© 2017 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>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Get started</td>
<td>23</td>
</tr>
<tr>
<td>Introduction to UDT</td>
<td>23</td>
</tr>
<tr>
<td>New features in UDT 3.3</td>
<td>23</td>
</tr>
<tr>
<td>What Is a device?</td>
<td>23</td>
</tr>
<tr>
<td>What SolarWinds User Device Tracker offers</td>
<td>24</td>
</tr>
<tr>
<td>How does SolarWinds User Device Tracker work?</td>
<td>25</td>
</tr>
<tr>
<td>Install SolarWinds User Device Tracker</td>
<td>26</td>
</tr>
<tr>
<td>Scalability</td>
<td>26</td>
</tr>
<tr>
<td>Requirements for SolarWinds UDT</td>
<td>26</td>
</tr>
<tr>
<td>UDT server software requirements</td>
<td>27</td>
</tr>
<tr>
<td>SolarWinds Server Hardware Requirements</td>
<td>27</td>
</tr>
<tr>
<td>Requirements for Virtual Machines and Servers</td>
<td>28</td>
</tr>
<tr>
<td>Requirements for the Orion Platform database Server (SQL Server)</td>
<td>29</td>
</tr>
<tr>
<td>Additional SolarWinds UDT Requirements</td>
<td>31</td>
</tr>
<tr>
<td>Scalability</td>
<td>31</td>
</tr>
<tr>
<td>FIPS support</td>
<td>31</td>
</tr>
<tr>
<td>Server sizing</td>
<td>32</td>
</tr>
<tr>
<td>SNMP requirements for monitored devices</td>
<td>33</td>
</tr>
<tr>
<td>Install SolarWinds User Device Tracker</td>
<td>33</td>
</tr>
<tr>
<td>Install or upgrade SolarWinds User Device Tracker</td>
<td>33</td>
</tr>
<tr>
<td>Finish SolarWinds UDT installation</td>
<td>34</td>
</tr>
<tr>
<td>Moving SolarWinds UDT to a new server</td>
<td>34</td>
</tr>
<tr>
<td>Exclude Orion data directories from anti-virus scanning</td>
<td>36</td>
</tr>
<tr>
<td>Running SolarWinds UDT</td>
<td>36</td>
</tr>
<tr>
<td>Internet Explorer security settings</td>
<td>37</td>
</tr>
<tr>
<td>Configuring SolarWinds UDT</td>
<td>38</td>
</tr>
<tr>
<td>Port management</td>
<td>38</td>
</tr>
<tr>
<td>Track users and endpoints</td>
<td>38</td>
</tr>
</tbody>
</table>
UDT settings .......................................................................................................................... 39
License summary .................................................................................................................... 39
thwack community ................................................................................................................ 40
License Orion Platform products .......................................................................................... 40
Evaluate Orion Platform products ......................................................................................... 41
Activate licenses ................................................................................................................... 41
Assign licenses to a server .................................................................................................... 42
Upgrade licenses .................................................................................................................. 44
Maintain licenses with the stand-alone Windows License Manager ..................................... 45
Migrate licenses from one server to another ......................................................................... 46
Synchronize licenses ............................................................................................................ 48

Administer ................................................................................................................................ 49
Discovery Central .................................................................................................................. 49
Discover and add network devices ....................................................................................... 50
Discover your network with the Discovery Wizard ............................................................... 50
Add nodes using Active Directory ....................................................................................... 54
Credentials for Active Directory discovery ......................................................................... 55
Automatically add discovered nodes .................................................................................... 55
Add discovered devices to SolarWinds NPM ...................................................................... 57
Add a single node for monitoring ....................................................................................... 60
Import online and offline nodes from a file ......................................................................... 65
File requirements ................................................................................................................... 65
Import the nodes .................................................................................................................... 66
Map columns when importing nodes from a file ................................................................... 66
Reserved column names ....................................................................................................... 67
Edit node properties ............................................................................................................ 74
Edit the node name, web address, and which view opens when you double-click the node .. 75
Edit polling settings ............................................................................................................. 75
Edit dependencies or custom properties ................................................................. 76
Add what additional data you want to poll on the node ............................................ 76
Customize alerting thresholds .................................................................................. 76
Import nodes from a list of IP addresses .................................................................. 77
Manage scheduled discovery results ......................................................................... 77
Minimize SNMP processing load during discoveries using the Discovery Ignore List .................................................. 77
Add ignored devices back to discovery ....................................................................... 78
Choose the polling method to use ............................................................................ 78
External Node (No Status) ......................................................................................... 78
Status Only: ICMP ........................................................................................................ 78
Most Devices: SNMP & ICMP .................................................................................... 78
Windows Servers: WMI and ICMP ............................................................................. 79
Windows and Linux Servers: Agent ........................................................................... 79
User Device Tracker Port Discovery ........................................................................... 80
Add Orion Nodes to UDT .......................................................................................... 81
Event Notification for Nodes and Ports added to UDT ............................................... 81
Adding Active Directory Controllers and users ......................................................... 82
Managing Active Directory Credentials ..................................................................... 82
Adding a New AD Credential ...................................................................................... 82
Editing an AD Credential ......................................................................................... 83
Deleting an AD Credential ......................................................................................... 83
Domain controller configuration validation ................................................................. 83
Managing Active Directory Domain Controllers ....................................................... 84
Adding a new AD domain controller .......................................................................... 84
Edit an AD domain controller ................................................................................... 85
Assign a credential to an AD Domain Controller ....................................................... 85
Delete an AD Domain Controller ............................................................................... 85
Set up polling of user data across domains ............................................................... 86
Define credentials for polling across domains .........................................................86
Set WMI namespace security .......................................................................................87
Adding a new AD Credential .........................................................................................87
Enable DNS resolution for wireless nodes .................................................................88
Endpoints and the White List .........................................................................................89
Manage the UDT White List .........................................................................................89
Add endpoints to the White List .....................................................................................89
  Add endpoints to the DNA White List by adding rules .................................................90
  Add endpoints to the White List by enabling rules .....................................................90
Remove endpoints from the White List .......................................................................90
  Remove endpoints from the White List by editing rules .............................................90
  Remove endpoints from the White List by disabling rules .......................................91
Ignoring Endpoints in UDT .........................................................................................91
  Ignore endpoints in the White List by adding rules ..................................................91
  Ignore endpoints in the White List by enabling rules ................................................92
Delete White List rules ...............................................................................................92
Viewing Status: Device, Port, User, SSID .................................................................93
  Using the Device Tracker Summary ..........................................................................93
    Using the Device Tracker Port Details ......................................................................94
    Use the Device Tracker Access Point Details ...........................................................96
    Using the Device Tracker SSID Details ..................................................................97
    Use the Device Tracker User Details ......................................................................98
Manage SolarWinds UDT Polling Engines ...............................................................100
  View a polling engine status .....................................................................................100
  Configure polling engine settings ............................................................................100
  Update polling settings .............................................................................................100
    Configure polling interval settings .......................................................................100
    Configure polling statistics intervals ....................................................................102
Configure Database Settings ................................................................. 102
Configure network settings ................................................................. 105
Configure calculations and threshold settings ..................................... 106
Calculate node availability .................................................................. 107
Node Status ......................................................................................... 107
Percent Packet Loss ........................................................................... 107
Define baselines for nodes .................................................................. 108
Define a baseline for an individual node ............................................. 108
Define a baseline for multiple nodes .................................................. 108
Using the Polling Engine Load Balancer ............................................ 109
Set the node warning level .................................................................. 109
Set how many retries are necessary before packet loss is reported .... 110

Solutions ............................................................................................. 111
Finding the switch and port where a particular hostname, IP, or MAC address is or was connected .111
Display rogue endpoint connections in real-time ................................. 112
Track status for a group of ports .......................................................... 112
Shut down a network device port .......................................................... 114
Create and manage a Watch List ......................................................... 114
Find wireless endpoint connections .................................................... 114
Find a user's connections .................................................................... 115
Find endpoints in a subnet .................................................................... 115
Resolve IP address conflicts with IPAM and UDT integration .......... 117

The Orion Platform .............................................................................. 120
Manage the Orion Web Console ............................................................ 120
Log in to the Orion Web Console ........................................................... 120
Customize the Orion Web Console look, views, settings, charts, and maps ............................................................................ 120
My Dashboards ..................................................................................... 120
Change the Orion Web Console color scheme .................................... 124
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Change the Orion Web Console logo</td>
<td>125</td>
</tr>
<tr>
<td>Use Orion Web Console breadcrumbs</td>
<td>125</td>
</tr>
<tr>
<td>Customize resources</td>
<td>126</td>
</tr>
<tr>
<td>Filter nodes in resources using SQL queries</td>
<td>126</td>
</tr>
<tr>
<td>Specify what a Custom Object resource displays</td>
<td>126</td>
</tr>
<tr>
<td>Customize charts in the Orion Web Console</td>
<td>127</td>
</tr>
<tr>
<td>Create, delete, modify, or restrict views</td>
<td>130</td>
</tr>
<tr>
<td>Create new views</td>
<td>130</td>
</tr>
<tr>
<td>Add resources and columns to views, and define subviews</td>
<td>131</td>
</tr>
<tr>
<td>Create custom summary views</td>
<td>136</td>
</tr>
<tr>
<td>Add external website views</td>
<td>138</td>
</tr>
<tr>
<td>Optimize views for TV screens or mobile devices</td>
<td>139</td>
</tr>
<tr>
<td>Limit objects on a view</td>
<td>140</td>
</tr>
<tr>
<td>Use a view as a template</td>
<td>141</td>
</tr>
<tr>
<td>Delete views</td>
<td>141</td>
</tr>
<tr>
<td>Specify views for device types</td>
<td>141</td>
</tr>
<tr>
<td>Export views to PDF</td>
<td>141</td>
</tr>
<tr>
<td>Orion Web Console and chart settings</td>
<td>142</td>
</tr>
<tr>
<td>Web Console settings</td>
<td>142</td>
</tr>
<tr>
<td>Auditing settings</td>
<td>144</td>
</tr>
<tr>
<td>Chart settings</td>
<td>144</td>
</tr>
<tr>
<td>Discovery, Worldwide Map, and Active Alerts settings</td>
<td>144</td>
</tr>
<tr>
<td>Administrative functions</td>
<td>145</td>
</tr>
<tr>
<td>View secure data</td>
<td>145</td>
</tr>
<tr>
<td>Handle counter rollovers</td>
<td>145</td>
</tr>
<tr>
<td>Configure web proxy settings</td>
<td>146</td>
</tr>
<tr>
<td>Manage devices in the Orion Web Console</td>
<td>147</td>
</tr>
<tr>
<td>Edit node properties</td>
<td>147</td>
</tr>
</tbody>
</table>
Edit the node name, web address, and which view opens when you double-click the node ................................................................. 147
Edit polling settings ......................................................................................................................................................... 148
Edit dependencies or custom properties .......................................................................................................................... 148
Add what additional data you want to poll on the node ......................................................................................................... 149
Customize alerting thresholds ......................................................................................................................................... 149
Suspend collecting data or triggering alerts for nodes in Maintenance Mode ................................................................. 149
Mute alerts ........................................................................................................................................................................ 150
Resume alerts ................................................................................................................................................................... 150
Stop collecting statistics .................................................................................................................................................. 150
Start collecting statistics ................................................................................................................................................ 150
Schedule a maintenance period ...................................................................................................................................... 151
Change scheduled maintenance ..................................................................................................................................... 151
Cancel scheduled maintenance ...................................................................................................................................... 151
Poll and rediscover devices immediately .......................................................................................................................... 152
Stop monitoring devices ................................................................................................................................................ 152
Change the polling method for a node ............................................................................................................................. 152
Assign Universal Device Pollers (UnDPs) to monitored devices .......................................................................................... 153
Detect and predict possible duplex mismatches .............................................................................................................. 153
How do I resolve mismatches? ...................................................................................................................................... 154
Troubleshooting ............................................................................................................................................................... 154
Suspend collecting data for interfaces, or show interface as Unplugged ............................................................................. 155
Maintenance modes .......................................................................................................................................................... 155
Set the interface status as Unpluggable .............................................................................................................................. 155
Remotely manage monitored interfaces ............................................................................................................................ 155
Access nodes using HTTP, SSH, and Telnet .......................................................................................................................... 156
Web-based SSH .................................................................................................................................................................. 156
Monitor devices in the Orion Web Console .......................................................................................................................... 157
View properties of all monitored nodes and interfaces in the Network Overview ............................................................... 157
View the resources and statistics monitored on a node .................................................. 157
View events, alerts, traps, and syslogs in the Orion Web Console Message Center .............. 157
Edit node properties ......................................................................................................... 158
   Edit the node name, web address, and which view opens when you double-click the node ..... 158
Edit polling settings ......................................................................................................... 158
Edit dependencies or custom properties ........................................................................... 159
Add what additional data you want to poll on the node ..................................................... 160
Customize alerting thresholds ......................................................................................... 160
Customize the Manage Nodes view ................................................................................ 160
Search for devices ........................................................................................................... 161
Suspend collecting data or triggering alerts for nodes in Maintenance Mode ....................... 161
   Mute alerts .................................................................................................................. 161
   Resume alerts ............................................................................................................. 162
   Stop collecting statistics ......................................................................................... 162
   Start collecting statistics ......................................................................................... 162
   Schedule a maintenance period .............................................................................. 162
   Change scheduled maintenance ............................................................................ 163
   Cancel scheduled maintenance ............................................................................... 163
Poll and rediscover devices immediately ......................................................................... 163
Stop monitoring devices ................................................................................................. 164
Set the node warning level .............................................................................................. 164
Choose the polling method to use .................................................................................. 165
   External Node (No Status) ..................................................................................... 165
   Status Only: ICMP .................................................................................................. 165
   Most Devices: SNMP & ICMP ............................................................................... 165
   Windows Servers: WMI and ICMP ...................................................................... 165
   Windows and Linux Servers: Agent ..................................................................... 166
Change the polling method for a node .............................................................................. 166
Promote a node from ICMP to SNMP monitoring ......................................................... 167
Promoting a Node from ICMP to WMI Monitoring ....................................................... 168
Change polling engine node assignments ................................................................. 168
Access nodes using HTTP, SSH, and Telnet ................................................................. 168
Web-based SSH ........................................................................................................... 169
Managing Groups and Dependencies ......................................................................... 169
Managing Groups ......................................................................................................... 169
Creating Groups ........................................................................................................... 170
Editing Existing Groups ............................................................................................... 171
Managing Group Members ......................................................................................... 171
Deleting Groups ............................................................................................................ 171
Managing the Display of Group Status ........................................................................ 172
Managing Dependencies .............................................................................................. 173
Creating a New Dependency ........................................................................................ 174
Editing an Existing Dependency .................................................................................. 175
Deleting an Existing Dependency ................................................................................ 175
Viewing Alerts on Child Objects .................................................................................. 176
Manage Orion Polling Engines ..................................................................................... 176
Use additional polling engines to balance polling ...................................................... 176
Pre-flight checklist ........................................................................................................ 176
Port requirements for Additional Polling Engines ....................................................... 177
Install an Additional Polling Engine ............................................................................. 178
Activate Additional Polling Engine licenses ............................................................... 178
Use an Additional Web Server .................................................................................... 179
Requirements .............................................................................................................. 179
Download and install an Additional Web Server ....................................................... 180
Configure the Additional Web Server .......................................................................... 180
Activate your license ..................................................................................................... 181
View a polling engine status ......................................................................................................................... 181
Update polling settings ................................................................................................................................. 181
Configure polling interval settings .............................................................................................................. 181
Configure polling statistics intervals ........................................................................................................ 183
Configure the dynamic IP address and hostname resolution ................................................................. 183
Configure Database Settings ..................................................................................................................... 183
Configure network settings ......................................................................................................................... 186
Configure calculations and threshold settings ......................................................................................... 187
Calculate node availability ......................................................................................................................... 188
Node Status .................................................................................................................................................. 188
Percent Packet Loss .................................................................................................................................. 188
Define baselines for nodes ......................................................................................................................... 189
Define a baseline for an individual node .................................................................................................... 189
Define a baseline for multiple nodes .......................................................................................................... 189
Assign credentials to virtual servers ......................................................................................................... 189
Assign credentials to Hyper-V servers ...................................................................................................... 190
Assign credentials to VMware servers .................................................................................................... 190
Set general thresholds ............................................................................................................................... 190
Set the node warning level ......................................................................................................................... 190
Set how many retries are necessary before packet loss is reported ...................................................... 191
Delete polling engines ............................................................................................................................... 191
Thresholds .................................................................................................................................................. 192
Set general thresholds ............................................................................................................................... 193
Customize thresholds for single objects ................................................................................................. 193
Baselines and baseline calculations ....................................................................................................... 194
What data is subject to statistical baseline calculation? ........................................................................ 194
Use mean and standard deviations as thresholds .................................................................................... 194
Customize how the baseline is calculated .................................................................................................. 194
Maintain the SolarWinds Orion database ........................................................................................... 195
Additional resources .......................................................................................................................... 195
Database maintenance ......................................................................................................................... 196
  Check the database size ..................................................................................................................... 197
  Specify the time to run database maintenance ................................................................................. 197
  Adjust retention periods .................................................................................................................... 198
  Launch database maintenance manually ......................................................................................... 198
Back up and restore the database ...................................................................................................... 198
View database details and data in the Database Manager ................................................................. 199
  Add a server to Database Manager .................................................................................................. 199
  View database details ....................................................................................................................... 199
  Edit database fields ........................................................................................................................ 200
Update Orion Platform products to use the new database ............................................................... 200
Custom properties .............................................................................................................................. 201
  Create a custom property ................................................................................................................ 202
  Remove a custom property .............................................................................................................. 205
  Import custom property values ........................................................................................................ 205
  Export custom property data ........................................................................................................... 206
  Change custom properties values ................................................................................................... 207
    Edit values for custom properties ................................................................................................. 207
  Filter objects when assigning custom properties ............................................................................ 207
Manage Orion Web Console user accounts ..................................................................................... 208
  Create users ...................................................................................................................................... 208
    Create users based on existing Active Directory or local domain accounts ................................ 210
  Change account passwords ............................................................................................................. 212
  Enable users to authenticate through LDAP ................................................................................... 212
  Define what users can access and do ............................................................................................... 213
  Set default menu bars and views for users ...................................................................................... 215
Limit users to specific network areas ................................................................. 216
Restrict user access to network areas by applying limitations ............................ 216
Patterns for limitations ...................................................................................... 217
Create limitations based on custom properties .................................................. 217
Delete account limitations ................................................................................. 218
Configure automatic login ................................................................................. 218
Enable Windows Authentication with Active Directory ..................................... 219
Supported Active Directory scenarios ............................................................... 220
Log in with Windows pass-through security ....................................................... 221
Share views with non-Orion Web Console users .................................................. 222
Automatically login by passing your credentials through the URL ....................... 223
Group objects and mirror network dependencies in the Orion Web Console ...... 224
Group monitored objects ..................................................................................... 224
Mirror network object dependencies in the Orion Web Console ......................... 226
High Availability in SolarWinds products .......................................................... 231
How does it work? .............................................................................................. 231
Single subnet (LAN) .......................................................................................... 231
Multiple subnets (WAN) ..................................................................................... 232
When do I use a VIP or a virtual host name? ....................................................... 233
What is a Virtual IP address? .............................................................................. 233
What is a virtual host name? .............................................................................. 234
SolarWinds High Availability requirements ....................................................... 234
Supported products ............................................................................................ 234
Software and Hardware requirements ............................................................... 235
Port requirements .............................................................................................. 236
Networking requirements ................................................................................... 237
High Availability deployment walk-through ...................................................... 238
Set up the standby server .................................................................................. 238
Activate High Availability pool licenses ......................................................... 239
Set up an HA pool ......................................................................................... 240
Choose a preferred active service ................................................................. 242
Configure High Availability settings ............................................................. 242
Set up the default High Availability email ...................................................... 243
Manage HA pools ......................................................................................... 243
Disable HA pools ........................................................................................... 243
Remove HA pools .......................................................................................... 244
Force a manual failover ................................................................................ 244
View the pool member type ......................................................................... 244
How failovers work ....................................................................................... 245
References ..................................................................................................... 245
Which IP address is used as the source? ......................................................... 245
Why doesn’t the virtual host name resolve? .................................................. 246
What is a DNS Zone? .................................................................................... 247
What are Transaction Signatures (TSIG)? ..................................................... 247
Failover to a standby server ......................................................................... 248
Upgrade High Availability pool members ...................................................... 248
Use alerts to monitor your environment .......................................................... 249
Alert preconfiguration tasks ........................................................................ 249
Configure the default information in the email action ..................................... 249
Best practices and tips for alerting ................................................................. 250
Navigate to the Alert Manager ..................................................................... 251
Add an SMTP server ..................................................................................... 251
Create new alerts to monitor your environment ............................................ 251
Set alert properties ....................................................................................... 252
Define the conditions that must exist to trigger an alert ............................... 253
Define the conditions that must exist to reset an alert ................................. 255
Schedule when an alert monitors your environment .......................................................... 256
Define what happens when an alert is triggered ............................................................ 257
Define what happens when the alert is reset ..................................................................... 259
Review the alert’s configuration ....................................................................................... 260
Commonly created alerts ................................................................................................ 260
Alert me when a server goes down .................................................................................. 261
Discover network device failures ...................................................................................... 262
Alerting When an IP Address Changes ............................................................................ 263
Alerting on Metrics ......................................................................................................... 263
View triggered alerts in the Orion Web Console ............................................................... 263
Remove alerts from the Active Alerts list ....................................................................... 264
Test alert triggers and actions .......................................................................................... 264
  Test trigger conditions .................................................................................................... 264
  Test alert actions while creating or editing an alert ...................................................... 264
  Test alert actions in the Action Manager ...................................................................... 265
Modify multiple alerts or share alerts ............................................................................. 265
Add actions to alerts without opening the Alert Wizard ............................................... 265
Share alerts with others .................................................................................................. 265
Build complex conditions ............................................................................................... 266
  Wait for multiple objects to meet the trigger condition ............................................. 266
  Evaluate multiple condition blocks ........................................................................... 267
  Evaluate multiple object types .................................................................................... 267
Changes in the alerting engine ......................................................................................... 268
  Changed or removed functionality ............................................................................... 268
  Database changes ......................................................................................................... 268
  Macro or variable changes ............................................................................................ 269
Alert migration to the web ................................................................................................ 269
  Migration issues ............................................................................................................ 269
Limitations to migrated alerts ................................................................. 269
Share alerts with other SolarWinds products ........................................ 270
Integrate an Orion Platform product with ServiceNow ............................. 270
Before you begin ...................................................................................... 270
Install and configure the SolarWinds Alert Integration application in ServiceNow ......................................................... 271
Configure an Orion Platform product with ServiceNow ............................. 271
How conditions are evaluated .................................................................. 272
Manage alert actions ................................................................................ 273
Assign an action to an alert ..................................................................... 273
Enable and Disable Alerts ....................................................................... 273
Available alert actions ............................................................................ 273
Change a custom property ...................................................................... 273
Create a ServiceNow incident ................................................................ 274
Dial a paging or SMS service .................................................................. 276
Email a web page to users ...................................................................... 276
Execute an external batch file ................................................................. 277
Execute an external Visual Basic script .................................................. 277
Log the alert message to a file ................................................................. 278
Log the alert to the NPM event log ......................................................... 279
Change the resource allocation of a virtual machine ............................... 279
Delete a snapshot of a virtual machine ................................................... 280
Move a virtual machine to a different host .............................................. 281
Move a virtual machine to a different storage ........................................ 281
Pause a virtual machine ......................................................................... 282
Power off a virtual machine ................................................................... 283
Power on a virtual machine ................................................................... 284
Restart a virtual machine ...................................................................... 284
Suspend a virtual machine ..................................................................... 285
Take a snapshot of a virtual machine ................................................................. 285
Play a sound when an alert is triggered .......................................................... 286
Send a Windows Net message ........................................................................ 287
Restart IIS sites or application pools ............................................................... 288
Send an SNMP trap ......................................................................................... 288
Send a GET or POST request ......................................................................... 289
Send a syslog message .................................................................................... 290
Send an email or page ..................................................................................... 290
Manually set a custom status .......................................................................... 291
Use the speech synthesizer to read alerts ....................................................... 292
Log an alert to the Windows Event Log on a specific server ......................... 293

Variables and examples .................................................................................. 293
Variable construction ...................................................................................... 293
Variable modifiers .......................................................................................... 294
Alert variables ................................................................................................ 294
Status values ................................................................................................... 305
Example messages using variables ................................................................. 306
Syslog alert variables ...................................................................................... 307
Trap alert variables ........................................................................................ 310

Create and view reports .................................................................................. 315
Predefined reports ........................................................................................... 315
Manage reports in the Orion Web Console ..................................................... 315
Modify an existing web-based report .............................................................. 315
Create a web-based report ............................................................................... 316
Customize a web-based report layout ............................................................. 318
Add content to a web-based report ................................................................. 319
Add a custom chart or table to a web-based report ........................................ 319
Restrict who can access reports ..................................................................... 323
Generate reports on a schedule ................................................................. 324
Export and import reports ....................................................................... 326
Monitor Syslog messages .......................................................................... 327
Before you begin ...................................................................................... 328
Configure the SolarWinds Orion server to use the correct syslog port ....... 328
Syslog message priorities ........................................................................ 328
Syslog facilities ....................................................................................... 329
Syslog severities ..................................................................................... 329
View Syslog messages in the Orion Web Console ..................................... 330
Clear Syslog messages in the Orion Web Console ...................................... 331
View and clear Syslog messages in the Syslog Viewer ............................... 332
Search for Syslog messages in the Syslog Viewer ...................................... 332
Define the number of messages displayed, message retention, and the displayed columns in the Syslog Viewer .......................................................... 333
Trigger alerts when receiving specific Syslog messages ......................... 333
Forward syslog messages .......................................................................... 335
Syslog alert actions ................................................................................ 335
Monitor SNMP traps ................................................................................ 337
Before you begin ..................................................................................... 337
View SNMP traps in the Orion Web Console ........................................... 337
View current traps in the Trap Viewer ..................................................... 338
Search for traps in the Trap Viewer ........................................................ 338
Define how many traps to display, if you want to refresh the traps view, trap retention, and the information displayed in the Trap Viewer ...................................................... 339
Configure Trap Viewer filters and alerts ............................................... 339
What is a Trap Template? ...................................................................... 340
Additional Polling Engine and Web Console ........................................ 341
Additional Polling Engine Guidelines ..................................................... 342
Additional Polling Engine System Requirements ................................... 342
Use additional polling engines to balance polling ................................................................. 343
Pre-flight checklist .............................................................................................................. 343
Port requirements for Additional Polling Engines ............................................................. 344
Install an Additional Polling Engine .................................................................................. 344
Activate Additional Polling Engine licenses ..................................................................... 345
Use an Additional Web Server ............................................................................................ 345
Requirements ..................................................................................................................... 345
Download and install an Additional Web Server ............................................................... 346
Configure the Additional Web Server ................................................................................ 347
Activate your license .......................................................................................................... 348
Global Search View ........................................................................................................... 348
What else can I do in the Global Search View? .................................................................. 348
Search syslogs, traps and objects monitored in the Orion Web Console globally ............... 348
Install Orion Global Search ................................................................................................ 349
Uninstall Orion Global Search ............................................................................................ 349
Search with Orion Global Search ...................................................................................... 349
Execute a global search ...................................................................................................... 349
Orion Global Search query syntax ...................................................................................... 350
Auto-completing queries and properties in Orion Global Search ..................................... 350
Refining Global Search with available filters .................................................................... 351
Removing a property filter ................................................................................................. 351
Adding more properties for filtering search results .......................................................... 352
Troubleshooting slow Internet connectivity with Orion Global Search ......................... 352

References .......................................................................................................................... 354

Troubleshooting .................................................................................................................. 354
Check device compatibility ................................................................................................. 354
Scanning a Device .............................................................................................................. 354
Analyze test results .......................................................................................................... 355
Node discovery completely fails ................................................................. 356
Node Discovery Fails for Some Devices .................................................... 357
UDT missing user data ............................................................................. 357
UDT Polling Spikes CPU on Target Device(s) ........................................... 357
Wrong hostname reported for endpoint .................................................... 358
Wrong IP address reported for endpoint ................................................... 358
Wrong MAC Address Reported for Endpoint ........................................... 358
Wrong connection type reported for endpoint .......................................... 359
Wrong VLAN reported for endpoint ........................................................ 359
No DNS data for a device .......................................................................... 359
No Layer 3 Data for a Device .................................................................. 359
No Layer2 Data for a Device .................................................................... 360
No user data retrieved via WMI (Windows Server 2003) ........................... 360
UDT not receiving user data from domain controllers ............................... 361
  Event code setup .................................................................................... 361
  Add a deleted port back into UDT ........................................................... 361
Regular Expression Pattern Matching ...................................................... 362
  Characters .............................................................................................. 362
  Character classes or character sets [abc] ................................................. 362
  Anchors ................................................................................................. 364
  Quantifiers ............................................................................................ 365
  Dot ............................................................................................................ 366
  Word Boundaries ................................................................................... 367
  Alternation ............................................................................................. 367
  Regular expression pattern matching examples .................................... 367
Product updates .......................................................................................... 368
  Available product updates ..................................................................... 368
  SolarWinds product Team Blog ............................................................. 368
Get started

Introduction to UDT

SolarWinds User Device Tracker (SolarWinds UDT) allows you to monitor devices, ports, and users for your network. With SolarWinds UDT, you can analyze your port usage and capacity and be alerted to issues before or as soon as they occur.

SolarWinds UDT allows you to find where devices are connected in your network and offers detailed information about capacity analysis. UDT regularly polls switches and routers for information about what is connected to them. Based on this information, SolarWinds UDT stores current and historical information about where a device has been connected. It also provides alerts and reports about devices connected to the network. For capacity analysis, SolarWinds UDT can report on how many ports are used on switches currently, as well as over time, so you can better understand the true utilization of the ports on your switches.

UDT also polls Active Directory domain controllers event logs for user login activity and based on it provides current and historical views of endpoints to which users have been connected on the network.

New features in UDT 3.3

- UDT uses the new Orion Installer. This can be used to install the whole family of Orion products in a non-obtrusive way. Falcon installer will download the products the user has selected, install them and launch the configuration wizard.
- UDT polls Cisco ASA devices via CLI
  
  For instructions see the knowledge base article, Use UDT to poll Cisco ASA devices.

- UDT now uses web-based reports
- UDT now uses the alert manager within the SolarWinds Orion Web Console
- TLS 1.2 support

What Is a device?

A device is a MAC address, hostname, or IP Address. SolarWinds UDT allows you to search on this information to find where the device is connected in the network and where it has been connected in the past.

- What SolarWinds User Device Tracker offers
- How does SolarWinds User Device Tracker work?
What SolarWinds User Device Tracker offers

SolarWinds UDT provides focused device and port monitoring for network engineers. SolarWinds UDT provides many features to help, including:

- Discover IPv4 and IPv6 devices.
- Quickly find where a device (MAC address, hostname or IP Address) or user is connected on the network.
- Find out where a device or user has been connected in the past.
- Find out what has been connected to a port over time.
- Provides port capacity analysis for a switch (how many ports are being used, including both monitored and un-monitored ports).
- Provides global port capacity analysis for used/available ports and network capacity planning.
- Configure a watchlist to track when specific devices appear on the network and alert when the devices appear.
- Provides enhanced network topology mapping.
- Generates 7 new predefined reports on connected devices, device capacity, and AD users.
How does SolarWinds User Device Tracker work?

Using SNMP calls to your network framework, SolarWinds User Device Tracker provides real time feedback on your monitored devices and users and trending through statistics stored in the Orion Platform database. Keeping with 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 on a Web Console accessible from any supported browser.

The following diagram provides an overview of the current SolarWinds UDT architecture, including interactions among SolarWinds UDT components, the SolarWinds UDT database, Active Directory domain controllers, and the managed devices on your network.
Install SolarWinds User Device Tracker

If you have version 3.3 of UDT or higher, use the SolarWinds Orion Installer to install or upgrade one or more Orion Platform products simultaneously.

Installing SolarWinds User Device Tracker (SolarWinds UDT) is a wizard-driven process. Resource and space requirements are such that most deployments do not require hardware updates to your server.

SolarWinds UDT is a standalone product. It can be installed by itself or with other SolarWinds products (for example SolarWinds Network Performance Monitor) to provide an integrated experience.

UDT 3.3.0 is not compatible with NCM 7.6. To install UDT 3.3.0 or upgrade from 3.2.4 to 3.3.0, NCM 7.6 must be upgraded to 7.7 version.

Users with UDT 3.2.3 must first upgrade to UDT 3.2.4 and then to UDT 3.3.

- Requirements for SolarWinds UDT
- FIPS support
- Server sizing
- SNMP requirements for monitored devices
- Install SolarWinds User Device Tracker
- Activate your license
- Finish SolarWinds UDT installation
- Move SolarWinds UDT to a new server
- License Orion Platform products
- Exclude Orion data directories from anti-virus scanning
- Run SolarWinds UDT
- Internet Explorer security settings

Scalability

By adding individual polling engines, you can transparently scale your SolarWinds UDT installation to any environment.

For more information see Additional Polling Engine and Web Console

Requirements for SolarWinds UDT

SolarWinds recommends installing your SolarWinds product on its own server, with the Orion Platform database hosted separately, on its own SQL Server. Installations of multiple SolarWinds UDT servers using the same database are not supported.
UDT server software requirements

The following table lists minimum software requirements and recommendations for your UDT server.

<table>
<thead>
<tr>
<th>SOFTWARE</th>
<th>REQUIREMENTS</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>IIS must be installed. SolarWinds recommends that SolarWinds software</td>
</tr>
<tr>
<td></td>
<td>administrators have local administrator privileges to ensure full</td>
</tr>
<tr>
<td></td>
<td>functionality of local SolarWinds tools. Accounts limited to use of the</td>
</tr>
<tr>
<td></td>
<td>Orion Web Console do not require administrator privileges.</td>
</tr>
<tr>
<td>Notes:</td>
<td>• SolarWinds does not support production installations of SolarWinds</td>
</tr>
<tr>
<td></td>
<td>products on Windows XP, Windows Vista, or Windows 7 systems.</td>
</tr>
<tr>
<td>Web Server</td>
<td>Microsoft IIS, version 7.5 or later.</td>
</tr>
<tr>
<td></td>
<td>DNS specifications require that hostnames be composed of alphanumeric</td>
</tr>
<tr>
<td></td>
<td>characters (A-Z, 0-9), the minus sign (-), and periods (.). Underscore</td>
</tr>
<tr>
<td></td>
<td>characters (_) are not allowed. For more information, see RFC 952.</td>
</tr>
<tr>
<td>.NET Framework</td>
<td>Version 4.6 .NET Framework. This will be downloaded automatically if not</td>
</tr>
<tr>
<td></td>
<td>found when the installer is run.</td>
</tr>
<tr>
<td>SNMP Trap Services</td>
<td>Windows operating system management and monitoring tools component</td>
</tr>
<tr>
<td>Web Console Browser</td>
<td>• Microsoft Internet Explorer 11 or later</td>
</tr>
<tr>
<td></td>
<td>• Firefox 49 or later</td>
</tr>
<tr>
<td></td>
<td>• Google Chrome 54 or later</td>
</tr>
</tbody>
</table>

SolarWinds Server Hardware Requirements

The following table lists minimum hardware requirements and recommendations for your UDT server.
Hardware requirements are listed by SolarWinds license level.

<table>
<thead>
<tr>
<th>HARDWARE</th>
<th>UT2500, UT5000, or UT10000</th>
<th>UT25000 or UT50000</th>
<th>UTX</th>
</tr>
</thead>
<tbody>
<tr>
<td>CPU Speed</td>
<td>2.0 GHz</td>
<td>2.4 GHz</td>
<td>3.0 GHz</td>
</tr>
</tbody>
</table>

- Dual processor, dual core is recommended.

| Hard Drive Space | 2 GB | 5 GB | 20 GB |

- A RAID 1 drive for server operating system, SolarWinds installation, and tempdb files is recommended. The SolarWinds installer needs 1GB on the drive where temporary Windows system or user variables are stored. Per Windows standards, some common files may need to be installed on the same drive as your server operating system.

| Memory | 3 GB | 4 GB | 4 GB |

| Application Ports | 161/SNMP and 443/SNMP. VMware ESX/ESXi Servers are polled on 443. |
|                   | 17777/TCP open for Orion Platform traffic |
|                   | 17778/ HTTPS open to access the SolarWinds Information Service API |

Requirements for Virtual Machines and Servers

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

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

<table>
<thead>
<tr>
<th>VIRTUAL MACHINE CONFIGURATION</th>
<th>ORION REQUIREMENTS BY LICENSE LEVEL</th>
</tr>
</thead>
<tbody>
<tr>
<td>UT2500, UT5000, UT10000</td>
<td>UT25000 or UT50000</td>
</tr>
<tr>
<td>CPU Speed</td>
<td>2.0 GHz</td>
</tr>
</tbody>
</table>
### Orion Requirements by License Level

<table>
<thead>
<tr>
<th>Virtual Machine Configuration</th>
<th>UT2500, UT5000, UT10000</th>
<th>UT25000 or UT50000</th>
<th>UTX</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allocated Hard Drive Space</td>
<td>2GB</td>
<td>5GB</td>
<td>20GB</td>
</tr>
<tr>
<td>Notes:</td>
<td>Due to intense I/O requirements, SQL Server should be hosted on a separate physical server configured as RAID 1+0. RAID 5 is not recommended for the SQL Server hard drive.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Memory</td>
<td>3 GB</td>
<td>4 GB</td>
<td>4 GB</td>
</tr>
<tr>
<td>Network Interface</td>
<td>Each virtual machine on which Orion is installed should have its own, dedicated network interface card.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Notes:</td>
<td>Since Orion Platform SNMP to monitor your network, if you are unable to dedicate a network interface card to your Server, you may experience gaps in monitoring data due to the low priority generally assigned to SNMP traffic.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Requirements for the Orion Platform database Server (SQL Server)

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

<table>
<thead>
<tr>
<th>Requirements</th>
<th>UT2500, UT5000, or UT10000</th>
<th>UT25000 or UT50000</th>
<th>UTX</th>
</tr>
</thead>
<tbody>
<tr>
<td>SQL Server</td>
<td>SQL Server 2012, SP1, SP2, SP3</td>
<td>SQL Server 2014, SP1, SP2</td>
<td>SQL Server 2016, SP1</td>
</tr>
<tr>
<td></td>
<td>SQL Server 2017</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Notes:**
<table>
<thead>
<tr>
<th>REQUIREMENTS</th>
<th>UT2500, UT5000, OR UT10000</th>
<th>UT25000 OR UT50000</th>
<th>UTX</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Due to latency effects, SolarWinds does not recommend installing your SQL Server and your SolarWinds UDT server or additional polling engine in different locations across a WAN. For more information, see SolarWinds Knowledge Base article Can I install my Server or Additional Polling Engine and my Orion Platform database (SQL Server) in different locations across a WAN?</td>
<td>Either mixed-mode or SQL authentication must be supported.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Either mixed-mode or SQL authentication must be supported.</td>
<td>If you are managing your SolarWinds UDT database, SolarWinds recommends you install the SQL Server Management Studio component.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>If your SolarWinds UDT product installs SQL Server System CLR Types, a manual restart of the SQL Server service for your SolarWinds UDT database is required.</td>
<td>Use the following database select statement to check your SQL Server version, service pack or release level, and edition:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>select SERVERPROPERTY ('productversion'), SERVERPROPERTY ('productlevel'), SERVERPROPERTY ('edition')</td>
<td></td>
<td></td>
</tr>
<tr>
<td>CPU Speed</td>
<td>2.0 GHz</td>
<td>2.4 GHz</td>
<td>3.0 GHz</td>
</tr>
<tr>
<td>Hard Drive Space</td>
<td>2 GB</td>
<td>5 GB</td>
<td>20 GB</td>
</tr>
</tbody>
</table>

Due to intense I/O requirements, a RAID 1+0 drive is strongly recommended the SQL Server database and SolarWinds UDT data and log files. RAID 5 is not recommended for the SQL Server hard drive. The SolarWinds UDT installer needs at least 1GB on the drive where temporary Windows system or user variables are stored. Per Windows standards, some common files may need to be installed on drive as your server operating system.
The Configuration Wizard installs the following required x86 components if they are not found on your SolarWinds UDT database server:

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

### Additional SolarWinds UDT Requirements

Enterprise-level SolarWinds UDT deployments with the potential for more than 50,000 ports may need additional computing resources above the standards required for SolarWinds common components:

<table>
<thead>
<tr>
<th>Ports</th>
<th>Additional Requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td>Up to 50,000</td>
<td>No additional requirements</td>
</tr>
<tr>
<td>More than 50,000</td>
<td>8+ GB RAM</td>
</tr>
</tbody>
</table>

### Scalability

By adding individual polling engines, you can transparently scale your SolarWinds UDT installation to any environment.

For more information see [Additional Polling Engine and Web Console](#)

### FIPS support

FIPS (Federal Information Processing Standard) defines security and interoperability standards for computers used by the U.S. Federal Government.

To enable FIPS in the Local Security Policy on Windows:

1. Click Start > Control Panel > System and Security > Administrative Tools, and then double-click Local Security Policy.
2. Expand the Local Policies category in the left pane, and then click Security Options.
3. Right-click System cryptography: Use FIPS compliant algorithms for encryption, hashing, and signing.

4. In the context menu that is displayed, click Properties.

5. In the Local Security Setting tab, click Enabled and then click OK.

ℹ️ FIPS can also be enabled as part of Group Policy.

SolarWinds UDT installations on Windows Server 2008 R2 and Windows 7 (supported for evaluation purposes only) require a Microsoft hotfix to realize the FIPS-compatibility features of this release. For more information about this required Microsoft hotfix, see the article [http://support.microsoft.com/kb/981119](http://support.microsoft.com/kb/981119). As noted in the KB article, you need to enable FIPS first before applying the Microsoft hotfix.

### Server sizing

SolarWinds UDT is capable of monitoring networks of any size, ranging from small corporate LANs to large enterprise and service provider networks. Most SolarWinds UDT systems perform well on 3.0 GHz systems with 4 GB of RAM, using default polling engine settings. However, when monitoring larger networks, you should give additional consideration to the hardware used and the system configuration.

There are three primary variables that affect scalability. The most important consideration is the number of monitored ports, nodes, and users. Systems monitoring more than 50,000 elements require 8+ GB of RAM. The second variable to consider is polling frequency. For instance, if you are collecting statistics more frequently than the default, the system will have to work harder and system requirements will increase. Finally, the number of simultaneous users accessing SolarWinds UDT directly impacts system performance.

When planning an SolarWinds UDT installation, there are four main factors to keep in mind with respect to polling capacity: CPU, memory, number of polling engines, and polling engine settings. For minimum hardware recommendations, see [Requirements for SolarWinds UDT](http://support.solarwinds.com). For more information about polling engines, see [Additional Polling Engine and Web Console](http://support.solarwinds.com).

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

If you plan to monitor 150,000 or more ports, SolarWinds recommends that you install additional polling engines on separate servers to help distribute the work load. For more information about sizing SolarWinds UDT to your network, contact the SolarWinds sales team or visit [www.solarwinds.com](http://www.solarwinds.com). For more information about configuring additional pollers, see [Additional Polling Engine and Web Console](http://support.solarwinds.com).
SNMP requirements for monitored devices

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

- To properly monitor devices on your network, you must enable SNMP on all devices that are capable of SNMP communications
- If SNMPv2c is enabled on a device you want SolarWinds UDT to monitor, by default, SolarWinds UDT will attempt to use SNMPv2c to poll the device for performance information. If you only want SolarWinds UDT to poll using SNMPv1, you must disable SNMPv2c on the device to be polled.

Install SolarWinds User Device Tracker

SolarWinds User Device Tracker offers an intuitive wizard to guide you through installing and configuring the product.

SolarWinds User Device Tracker does not require SolarWinds NPM.

- Consult the SolarWinds Product Upgrade Advisor if you are installing or upgrading UDT with NPM or any other SolarWinds Orion product.
- If you have any additional SolarWinds UDT web consoles or pollers, you must upgrade them too by repeating this procedure for each additional SolarWinds UDT poller or web console. Be sure to use the correct installers for pollers or web consoles, since these are different from the standard installer package. For information about installing additional Orion Web Consoles or pollers, refer to the Chapter Additional Polling Engine and Web Console

Install or upgrade SolarWinds User Device Tracker

1. Using a local administrator account log on to the server where you want to install or upgrade SolarWinds UDT.
2. If you downloaded the product from the SolarWinds website, navigate to your download location and launch the executable.
3. If you are prompted to install requirements, click Install, and then complete the installation, including a reboot, if required.

Notes:
- Downloading and installing Microsoft .NET Framework 4.6. may take up to 20 minutes or more, depending on your existing system configuration.
- If a reboot is required, after restart, click Install to resume installation, and then click Next on the Welcome window.
4. If the Microsoft Installer Wizard detects that Microsoft Internet Information Services (IIS) version 7.5 is not installed, you will be given the option to allow the SolarWinds installer to install it, or to install it manually.

   ℹ️ The Orion Web Console requires that Microsoft IIS is installed on the SolarWinds UDT Server. If you do not install IIS at this point, you must install IIS later, and then configure a website for the Orion Web Console to use.

5. Read the message about the Orion Improvement Program. If you are willing to send anonymous data back to SolarWinds for product improvement, click Send data. Otherwise, click Do not send data.

   ℹ️ You can stop sending this data at any time by uninstalling the Orion Improvement Program using the Control Panel.

6. Read the welcome message, and then click Next.

7. If you are upgrading, type Yes that you acknowledge creating a database backup before installing the new version of UDT.

   ℹ️ For information on creating a database backup see Back up and restore the database.

8. Select I accept the terms of the License Agreement, and then click Next.

9. Select an Installation Folder or accept the default, and then click Next.

10. Click Next to begin the installation.

11. Click Finish when the setup completes.

Finish SolarWinds UDT installation

After activating your license, you are prompted to configure SolarWinds UDT. Doing so configures the SolarWinds UDT database, web site, and services to work in your specific Orion environment.

Follow the directions in the Orion Configuration Wizard:

1. Click Next on the Orion Configuration Wizard Welcome window.
2. Configure the Database Settings for the SQL Server, and then click Next.
3. Select the option to create a new database or to use an existing one, and then click Next.
4. Select the option to create a new account or to use an existing account, and then click Next.
5. Select the Website Settings, and then click Next.
6. Accept the SolarWinds services or plugins that are checked, and then click Next. If you have not installed other modules, the UDT Job Engine Plugin may be your only selectable option.
7. Review the configuration summary provided by the Configuration Wizard, and then click Next.
8. Click Finish when the Configuration Wizard completes.

Moving SolarWinds UDT to a new server

SolarWinds UDT encrypts your sensitive data with a security certificate stored on the original SolarWinds UDT server. To grant a new server access to this encrypted data, you must copy the original security certificate to the new server.
WARNING: If you do not replicate the original certificate, SolarWinds UDT on the new server cannot access any credentials used by your component monitors, and all of those component monitors will fail.

To replicate the original certificate:

1. Export the credential from the original server:
   a. On the Start Menu, click Run, type MMC, and then click OK.
   b. On the File menu, click Add/Remove Snapin, and then click Add.
   c. Select Certificates and then click Add.
   d. Select Computer account and then click Next.
   e. Select Local computer and then click Finish.
   f. Click Close.
   g. Click OK.
   h. Expand the Certificates (Local Computer) group.
   i. Expand the Personal group.
   j. Expand the Certificates group.
   k. Right-click SolarWinds Job Scheduler, point to All Tasks on the shortcut menu, and then click Export.
   l. Click Next in the Certificate Export Wizard.
   m. Select Yes, export the private key, click Next, and then click Next again.
   n. Type and confirm a password for this private key, and then click Next.
   o. Specify the file name to which you want to save the certificate, click Next, and then click Finish—the certificate is saved with a .pfx file name extension.

2. Copy the .pfx certificate file to the new server.
3. Import the certificate to the new server:

   a. On the Start Menu, click Run, type MMC, and then click OK.
   b. On the File menu, click Add/Remove Snapin, and then click Add.
   c. Select Certificates, and then click Add.
   d. Select Computer account, and then click Next.
   e. Select Local computer, and then click Finish.
   f. Click Close.
   g. Click OK.
   h. Expand the Certificates (Local Computer) group.
   i. Expand the Personal group.
   j. Expand the Certificates group.
   k. If there is a SolarWinds Job Scheduler Engine item in the list, right-click SolarWinds Job Scheduler Engine and select Delete from the shortcut menu.
   l. Right-click the Certificates-Personal-Certificates node, point to All Tasks in the shortcut menu, and then click Import.
   m. Click Next in the Certificate Import Wizard.
   n. Specify the .pfx certificate file you copied to the server and then click Next.
   o. Enter the password for the private key, check Mark this key as exportable, and then click Next.
   p. Select Place all certificates in the following store, and then select Personal as the Certificate Store.
   q. Click Next and then click Finish.

Exclude Orion data directories from anti-virus scanning

Anti-virus programs may lock files used by the SolarWinds Job Engine v2 during scanning. This can cause the SolarWinds Job Engine v2 services to stop and restart, causing delayed polling and gaps in data for a poll cycle.

SolarWinds recommends that you exclude certain Orion data directories (depending on your Windows platform) from your anti-virus scanning to improve performance and stability.

Exclude for Windows XP/Server 2003:

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

Exclude for Windows Vista/7/Server 2008:

   C:\ProgramData\SolarWinds

Running SolarWinds UDT

Click Start > All Programs > SolarWinds > Orion Web Console.
The Orion Web Console is displayed. You can login by default by entering the User name Admin and no password. Then click LOGIN.

Internet Explorer security settings

If you are using Internet Explorer, SolarWinds recommends that you add the URL of your Orion website (http://FullOrionServerName/), the URL of SolarWinds support (http://support.solarwinds.com), and about:blank to the list of trusted sites.

If you do not add these URLs to the list of trusted sites, you may see Internet Explorer dialogs that contain messages similar to the following regarding blocking website content:

Content from the website listed below is being blocked by the Internet Explorer Enhanced Security Configuration.

<website>

To add the specified URLs to your trusted sites list, click the Add... button in the Internet Explorer dialog.
Configuring SolarWinds UDT

You can configure SolarWinds UDT and its port information, watch list, and settings through the Orion Web Console by using the UDT Settings page.

Refer to the sections that follow for details about the administrative commands available in each category:

- **Port management**
- **Track users and endpoints**
- **UDT settings**
- **License summary**
- **thwack community**

Port management

The Port Management category gives you access to the commands that allow you to manage and discover ports. Keep in mind that for UDT a port is a physical connection on your network device.

Manage ports

Click Manage Ports in the UDT Settings section to add, configure, and delete ports.

User Device Tracker discovery

Click User Device Tracker Discovery in the UDT Settings section to discover ports.

For more information, see [User Device Tracker Port Discovery](#).

Track users and endpoints

The Track Users and Endpoints category gives you access to the commands that allow you to setup user tracking and manage a device watch list.

Manage the White List

Click the Manage White List option to add, edit, and delete rules for determining which endpoints on the network should be considered safe and which simply ignored.

For more information, see [Manage the UDT White List](#).

Manage Active Directory Domain Controller

Click Manage Active Directory Domain Controller option to add, edit, and delete AD domain controllers UDT uses to obtain user data.

For more information, see [Managing Active Directory Domain Controllers](#)
Manage Watch List

Click Manage Watch List in the UDT Settings section to add or delete endpoints and users to/from a Device Watch List.

UDT settings

The UDT Settings category gives you access to the commands that allow you to view and manage global UDT settings.

Polling interval

Click Polling Interval in the UDT Settings section to determine how frequently UDT polls a node for port status and what endpoints are connected to the port.

Data retention

Click Data Retention in the UDT Settings section to specify how long SolarWinds UDT keeps historical information in the database. By default this is 90 days.

Port thresholds

Click Thresholds in the UDT Settings section to set the level at which a port will be included in a High Port Utilization Report.

View UDT job status

Click View UDT Job Status in the UDT Settings section to view the status for the UDT jobs for each node, showing the node name and IP address, job type, date and time for the last time the job was run, date and time for the next time the job will be run.

Click Poll Now to immediately run the corresponding UDT job.

Advanced settings

Click Advanced Settings in the UDT Settings section to select more port types, review and change settings that determine how frequently UDT contacts AD domain controllers for user account updates, the overall limit for the number of rows UDT could return in search results, and timeouts for SNMP polling, port discovery, layer 3 device discovery, jobs (layer 2 and 3), DNS resolution jobs, cached DNS data.

Click SAVE whenever you make changes to settings on this page.

License summary

The License Summary category gives you access to the command that allows you to view the license information summary.
UDT license summary

Click UDT License Summary in the UDT Settings section to see a comparison between the current number of nodes and volumes and the limits allowed by your SolarWinds UDT license.

This page also displays the licensing information for both the Orion Platform and User Device Tracker and shows the version of the applications that you are running.

thwack community

The thwack Community category gives you access to the commands that allow you to view and download useful information from the thwack community for SolarWinds users.

UDT thwack forum

Click UDT thwack Forum in the UDT Settings section to browse the information provided in the UDT thwack Forum.

UDT credentials

UDT Credentials allows you to add, edit, or delete the credentials by which UDT will access AD domain controllers.

Manage Active Directory Administrator Credentials

Click Manage Active Directory Administrator Credentials in the UDT Settings section to create, edit, and delete credentials the UDT uses to communicate with AD domain controllers.

For more information, see Managing Active Directory Credentials

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.
If you licensed your products using the stand-alone License Manager tool, use the web-based License Manager for any product running on Orion Platform 2016.2 and later. SolarWinds recommends uninstalling the stand-alone tool if your product can be licensed through the Orion Web Console. If you run into licensing issues later, you can download the latest stand-alone License Manager tool from the Customer Portal.

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.
      i. 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 License Management > License Management.
   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.

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 License Management > License Management.
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.

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.

**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.

[ADD/UPGRADE LICENSE]

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.

**Maintain licenses with the stand-alone Windows License Manager**

After you install an Orion Platform product or other products such as DameWare, you are prompted to activate your license. To activate your product, go to the License Manager.

Orion Platform products with Core 2016.2 and later can use the web-based License Manager to manage licenses for all polling engines and additional websites from a single Orion Web Console page. Non-Orion Platform products use the stand-alone License Manager.

**What can you do with the Windows License Manager?**

- Deactivate licenses on one computer and activate them on another computer without contacting SolarWinds Customer Service.
- Upgrade production license levels.
- Upgrade from evaluation licenses to production licenses.
- Synchronize licenses with the licensing server.
You cannot activate the license for a product that is released after the end of your maintenance period. You can activate the license for a product released before the end of your maintenance period at any time.

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.
Administer

Discovery Central

Discovery Central provides a centralized overview of the types and number of network objects you are monitoring with your currently installed SolarWinds products. The Discovery Central view is subdivided into categories corresponding to the SolarWinds products you have installed.

For SolarWinds UDT, Discovery Central is divided into Network Discovery and User Device Tracker Port Discover; and each of these categories provides current information about the network objects currently being monitored. The Network Discovery category displays a count of network devices being monitored. The User Device Tracker Port Discovery category displays a count of Ethernet ports being monitored.

Clicking GO TO ORION HOME opens the Home view for your entire monitored network.

You must perform Network Sonar Discovery first before the Discovery Central becomes available to show the discovery status.

For more information about the DISCOVER MY PORTS option in the User Device Tracker Port Discovery category, refer to User Device Tracker (UDT) Scalability Engine Guidelines
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.

> With the release of UTD 3.3, highly secure Cisco ASA devices can now be monitored. For instructions see the knowledge base article, Use UDT to poll Cisco ASA devices.

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>IP Ranges</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>Subnets</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>IP Addresses</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>Active Directory</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**

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

- **IP RANGES**
  - Add Range

- **SUBNETS**
  - Add

- **IP ADDRESSES**
  - Write one IP address or hostname per line:
    - 10.199.8.1
    - 10.199.8.3
    - 10.199.8.5

- **ACTIVE DIRECTORY**
  - Add Active Directory Domain Controller to query...
4. If the Agents panel appears, you enabled the Quality of Experience (QoE) agent during installation. The QoE agent monitors packet-level traffic. If there are any nodes using agents, select the Check all existing nodes check box. This setting ensures that any agents you deploy, including the one on your Orion server, are up-to-date. If there are no nodes using agents, you can leave this option unchecked.

5. On the 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.

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

   SolarWinds recommends that you monitor Windows devices with WMI instead of SNMP.
8. On the Monitoring Settings panel, SolarWinds recommends manually setting up monitoring the first time you run discovery. This allows you to review the list of discovered objects and select the ones you want to monitor. When you scale monitoring, you can configure discovery to automatically start monitoring objects it finds.

![Monitoring Settings Panel]


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

![Discovery Scheduling Panel]

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

![Discovering Network Panel]

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.

   ![Available Organizational Units](image)

   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.

   ![Active Directory](image)

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.

![Image of 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.

![Image of interface selection]

**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 the types of volumes you want to monitor]

- Compact Disk
- Fixed Disk
- Flash Memory
- Floppy Disk
- Mount Point
- Network Disk
- Other
- RAM
- RAM Disk
- Removable Disk
- Unknown
- Virtual Memory

**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 the applications you want to monitor]

- Microsoft Exchange Server
- Microsoft IIS
- Microsoft SQL Server
- Windows Scheduled Tasks

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 NPM**

After the Network Sonar Wizard discovers your network, the Network Sonar Results Wizard opens, allowing you to import network elements into SolarWinds NPM your SolarWinds product. Nodes that are discovered do not count against your license count. Only nodes that you have added to the SolarWinds Orion database count against your license.
When you manually run discovery, by default, the system automatically selects all network elements to be monitored. You must clear the check boxes for elements you do not want monitored.

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

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

### Network Sonar Results Wizard

#### Device Types to Import
Select the device types to monitor.

<table>
<thead>
<tr>
<th>Count</th>
<th>Device Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>Catalyst 37xx Stack</td>
</tr>
<tr>
<td>1</td>
<td>Cisco 2821</td>
</tr>
<tr>
<td>1</td>
<td>net-snmp - Linux</td>
</tr>
<tr>
<td>1</td>
<td>VMware ESX Server</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.

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

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

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

- By default, SolarWinds NPM imports interfaces that are discovered in an Operationally Up state. However, because interfaces may cycle off and on, you can also select Operationally Down or Administratively Shutdown states for import.
4. Ensure the volume types you want to monitor are selected, and click Next.

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

   **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>✓ 11</td>
<td>RAM</td>
</tr>
<tr>
<td>✓ 12</td>
<td>Virtual Memory</td>
</tr>
<tr>
<td>✓ 3</td>
<td>Other</td>
</tr>
<tr>
<td>✓ 19</td>
<td>Fixed Disk</td>
</tr>
<tr>
<td>✓ 4</td>
<td>RAM Disk</td>
</tr>
</tbody>
</table>

   [NEXT]

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>SNMP</td>
<td></td>
</tr>
<tr>
<td>✓ 10.196.200.250</td>
<td>BROF-3750-CORE.demo.lab</td>
<td>Catalyst 37xx Stack</td>
<td>SNMP</td>
<td></td>
</tr>
<tr>
<td>✓ 10.196.202.1</td>
<td>BROF-2821-WAN.demo.lab</td>
<td>Cisco 2821</td>
<td>SNMP</td>
<td></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

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

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

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

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

To add a single node for monitoring:
1. Log in to the Orion Web Console as an administrator.
2. Click Settings > Manage Nodes, and then click Add a Node.
3. Specify the node, and click Next.
a. Provide the host name or IP address.

b. Select the polling method, and provide credentials.
4. Select the statistics and resources to monitor on the node, and click Next.

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

   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.

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

7. Click OK, Add Node.

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

Import online and offline nodes from a file

Add nodes from a file into your Orion server using an administrator account. Nodes that are imported and not attached to your network will be monitored automatically when they are online.

The Orion server stops importing nodes when the number of monitored elements, including offline nodes, in your server matches your license level. You will not be able to import more nodes than your license allows.

You need administrator rights to view this option and node management rights to perform this action.

Nodes added from a file use ICMP polling and monitor node status, response time, and packet loss. Use the Create Discovery Profile option at the end of the import wizard to change the polling method and monitored resources for the nodes you import.

File requirements

You can download sample files from Settings > All Settings > Import Nodes from File.
Files must meet the following guidelines:

- The file must be a CSV, TXT, or XLS file.
- The IP_Address column is required.
- All fields must have valid data based on the data type.
- Column names cannot be reserved.

Tip: You can add a column to your file, such as *Imported from File*, to use to group your nodes.

Import the nodes

1. Log in to the Orion Web Console as an administrator.
2. Click Settings > All Settings > Import Nodes from File.
3. Upload your CSV, TXT, or XLS file, and click Next.
4. **Map the column labels** from the file to columns in the Orion database. Unknown columns can be used to create new custom properties or ignored. You can ignore any column. Click Next when all columns are assigned.
5. All imported fields are validated based on the data type. Rows with invalid data are not imported into the database.

   Tip: SolarWinds recommends you browse through the node list to verify the data and note any nodes that cannot be imported due to data validation errors. You may want to correct the errors and try again.

6. Click Import to Database. All of the nodes are imported into the Orion database.
7. Select Create Discovery Profile if you want to change your polling methods or monitored resources.

You can view the nodes you imported in the Manage Nodes page. Group the nodes by Discovered Nodes - Imported on and choose the date you first imported the node. If a node was imported before, it will not appear in this grouping.

Create a Discovery Profile using the imported nodes to mass modify discovery settings

A **discovery profile** allows you to edit the polling and monitoring settings for the nodes you import from a file. You can change how you poll nodes, credentials you use for polling, or polling frequency.

Map columns when importing nodes from a file

When importing data from an external file, the wizard attempts to match the column labels in the file to the corresponding database columns. On the Map Columns step, columns that are read from the file are listed on the left. Match the columns from the file to columns in the Orion database.
Map unknown columns

If a column is not found in the Orion database, you can choose to create a new custom property. The wizard creates the new database column in the Orion database and values from the file are mapped to the new column. This option is selected by default. Some names are reserved and cannot be used as a new custom property.

Columns must be mapped to a single database column. You cannot map a column to multiple database columns.

You can edit properties created this way using the Custom Property manager and use them in the same way you would use any custom property that you created through the Custom Property manager.

Ignore columns

You can choose to ignore columns, and those values are not imported. You cannot ignore the IP Address column.

On the Preview step, the ignored column does not appear in any row.

Remember the column mapping for future imports

Files imported in the future default to the column mapping you select to remember. You still have the option of mapping the spreadsheet column to a different database column. The most recent column mapping that you choose to remember replaces the previous column mapping.

Troubleshooting column mapping

Check the following log files for errors related to importing items and mapping columns:

- ApolloWebApi.log
- NodeManagement.BusinessLayer.log

Reserved column names

The following is a list of reserved column names. You cannot create a custom property using any of these names.

<table>
<thead>
<tr>
<th>Reserved names</th>
<th>Reserved names</th>
</tr>
</thead>
<tbody>
<tr>
<td>ABSOLUTE</td>
<td>MachineType</td>
</tr>
<tr>
<td>ACTION</td>
<td>MAP</td>
</tr>
<tr>
<td>ADA</td>
<td>MATCH</td>
</tr>
<tr>
<td>ADD</td>
<td>MAX</td>
</tr>
<tr>
<td>ADMIN</td>
<td>MaxResponseTime</td>
</tr>
<tr>
<td>AFTER</td>
<td>MemoryUsed</td>
</tr>
</tbody>
</table>
• AgentPort
• AGGREGATE
• ALIAS
• ALL
• ALLOCATE
• Allow64BitCounters
• ALTER
• AND
• ANY
• ARE
• ARRAY
• AS
• ASC
• ASSERTION
• AT
• AUTHORIZATION
• AVG
• AvgResponseTime
• BACKUP
• BEFORE
• BEGIN
• BETWEEN
• BINARY
• BIT
• BIT_LENGTH
• BLOB
• BlockUntil
• BOOLEAN
• BOTH
• BREADTH
• BREAK
• BROWSE
• BufferBgMissThisHour
• BufferBgMissToday
• BufferHgMissThisHour
• BufferHgMissToday
• BufferLgMissThisHour
• MIN
• MinResponseTime
• MINUTE
• MODIFIES
• MODIFY
• MODULE
• MONTH
• NAMES
• NATIONAL
• NATURAL
• NCHAR
• NCLOB
• NEW
• NEXT
• NextPoll
• NextRediscovery
• NO
• NOCHECK
• NodeID
• NONCLUSTERED
• NONE
• NOT
• NULL
• NULLIF
• NUMERIC
• OBJECT
• ObjectSubType
• OCTET_LENGTH
• OF
• OFF
• OFFSETS
• OLD
• ON
• ONLY
• OPEN
• OPENDATASOURCE
• OPENQUERY
BufferLgMissToday
BufferMdMissThisHour
BufferMdMissToday
BufferNoMemThisHour
BufferNoMemToday
BufferSmMissThisHour
BufferSmMissToday
BULK
BY
CALL
Caption
CASCADE
CASCADED
CASE
CAST
CATALOG
CHAR
CHAR_LENGTH
CHARACTER
CHARACTER_LENGTH
CHECK
CHECKPOINT
ChildStatus
CLASS
CLOB
CLOSE
CLUSTERED
CMTS
CMTSImport
CMTSImportPending
CMTSImportStatus
CMTSPoll
CMTSPollStatus
COALESCE
COLLATE
COLLATION
COLUMN
OPENROWSET
OPENXML
OPERATION
OPTION
OR
ORDER
ORDINALITY
OUT
OUTER
OUTPUT
OVER
OVERLAPS
PAD
PARAMETER
PARAMETERS
PARTIAL
PASCAL
Password
PATH
PERCENT
PercentLoss
PercentMemoryUsed
PLAN
PollInterval
POSITION
POSTFIX
PRECISION
PREFIX
PREORDER
PREPARE
PRESERVE
PRIMARY
PRINT
PRIOR
PRIVILEGES
PROC
PROCEDURE
- COMMIT
- Community
- COMPLETION
- COMPUTE
- CONNECT
- CONNECTION
- CONSTRAINT
- CONSTRAINTS
- CONSTRUCTOR
- Contact
- CONTAINS
- CONTAINSTABLE
- CONTINUE
- CONVERT
- CORRESPONDING
- COUNT
- CPULoad
- CREATE
- CROSS
- CUBE
- CURRENT
- CURRENT_DATE
- CURRENT_PATH
- CURRENT_ROLE
- CURRENT_TIME
- CURRENT_TIMESTAMP
- CURRENT_USER
- CURSOR
- CustomPollerLastStatisticsPoll
- CustomPollerLastStatisticsPollSuccess
- CYCLE
- DATA
- DATABASE
- DATE
- DATETIME
- DAY
- DBCC
- PUBLIC
- RAISERROR
- READ
- READS
- READTEXT
- REAL
- RECONFIGURE
- RECURSIVE
- RediscoveryInterval
- REF
- REFERENCES
- REFERENCING
- RELATIVE
- REPLICATION
- ResponseTime
- RESTORE
- RESTRICT
- RESULT
- RETURN
- RETURNS
- REVOKE
- RIGHT
- ROLE
- ROLLBACK
- ROLLUP
- ROUTINE
- ROW
- ROWCOUNT
- ROWGUIDCOL
- ROWS
- RULE
- RWCommunity
- RWSNMPV3AuthKey
- RWSNMPV3AuthKeyIsPwd
- RWSNMPV3AuthMethod
- RWSNMPV3Context
- RWSNMPV3PrivKey
<table>
<thead>
<tr>
<th>SQL Keywords</th>
<th>SQL Keywords</th>
</tr>
</thead>
<tbody>
<tr>
<td>DEALLOCATE</td>
<td>RWSNMPV3PrivKeyIsPwd</td>
</tr>
<tr>
<td>DEC</td>
<td>RWSNMPV3PrivMethod</td>
</tr>
<tr>
<td>DECIMAL</td>
<td>RWSNMPV3Username</td>
</tr>
<tr>
<td>DECLARE</td>
<td>SAVE</td>
</tr>
<tr>
<td>DEFAULT</td>
<td>SAVEPOINT</td>
</tr>
<tr>
<td>DEFERRABLE</td>
<td>SCHEMA</td>
</tr>
<tr>
<td>DEFERRED</td>
<td>SCOPE</td>
</tr>
<tr>
<td>DELETE</td>
<td>SCROLL</td>
</tr>
<tr>
<td>DENY</td>
<td>SEARCH</td>
</tr>
<tr>
<td>DEPTH</td>
<td>SECOND</td>
</tr>
<tr>
<td>DEREF</td>
<td>SECTION</td>
</tr>
<tr>
<td>DESC</td>
<td>SELECT</td>
</tr>
<tr>
<td>DESCRIBE</td>
<td>SEQUENCE</td>
</tr>
<tr>
<td>Description</td>
<td>SESSION</td>
</tr>
<tr>
<td>DESCRIPTOR</td>
<td>SESSION_USER</td>
</tr>
<tr>
<td>DESTROY</td>
<td>SET</td>
</tr>
<tr>
<td>DESTRUCTOR</td>
<td>SETS</td>
</tr>
<tr>
<td>DETERMINISTIC</td>
<td>SETUSER</td>
</tr>
<tr>
<td>DIAGNOSTICS</td>
<td>Severity</td>
</tr>
<tr>
<td>DICTIONARY</td>
<td>SHUTDOWN</td>
</tr>
<tr>
<td>DISCONNECT</td>
<td>SIZE</td>
</tr>
<tr>
<td>DISK</td>
<td>SMALLINT</td>
</tr>
<tr>
<td>DISTINCT</td>
<td>SNMPV2Only</td>
</tr>
<tr>
<td>DISTRIBUTED</td>
<td>SNMPV3AuthKey</td>
</tr>
<tr>
<td>DNS</td>
<td>SNMPV3AuthKeyIsPwd</td>
</tr>
<tr>
<td>DOMAIN</td>
<td>SNMPV3AuthMethod</td>
</tr>
<tr>
<td>DOUBLE</td>
<td>SNMPV3Context</td>
</tr>
<tr>
<td>DROP</td>
<td>SNMPV3PrivKey</td>
</tr>
<tr>
<td>DUMMY</td>
<td>SNMPV3PrivKeyIsPwd</td>
</tr>
<tr>
<td>DUMP</td>
<td>SNMPV3PrivMethod</td>
</tr>
<tr>
<td>DYNAMIC</td>
<td>SNMPV3Username</td>
</tr>
<tr>
<td>DynamicIP</td>
<td>SNMPVersion</td>
</tr>
<tr>
<td>EACH</td>
<td>SOME</td>
</tr>
<tr>
<td>ELSE</td>
<td>SPACE</td>
</tr>
<tr>
<td>EnableLevel</td>
<td>SPECIFIC</td>
</tr>
<tr>
<td>EnablePassword</td>
<td>SPECIFICITY</td>
</tr>
<tr>
<td>END</td>
<td>SQL</td>
</tr>
<tr>
<td>Keywords</td>
<td>Keywords</td>
</tr>
<tr>
<td>----------------------------------</td>
<td>----------------------------------</td>
</tr>
<tr>
<td>GRANT</td>
<td>TRANSLATE</td>
</tr>
<tr>
<td>GROUP</td>
<td>TRANSLATION</td>
</tr>
<tr>
<td>GROUPING</td>
<td>TREAT</td>
</tr>
<tr>
<td>GroupStatus</td>
<td>TRIGGER</td>
</tr>
<tr>
<td>HAVING</td>
<td>TRIM</td>
</tr>
<tr>
<td>HOLDLOCK</td>
<td>TRUE</td>
</tr>
<tr>
<td>HOST</td>
<td>TRUNCATE</td>
</tr>
<tr>
<td>HOUR</td>
<td>TSEQUAL</td>
</tr>
<tr>
<td>IDENTITY</td>
<td>UNDER</td>
</tr>
<tr>
<td>IDENTITY_INSERT</td>
<td>UNION</td>
</tr>
<tr>
<td>INDENTITY_COL</td>
<td>UNIQUE</td>
</tr>
<tr>
<td>IF</td>
<td>UNKNOWN</td>
</tr>
<tr>
<td>IGNORE</td>
<td>Unmanaged</td>
</tr>
<tr>
<td>IMMEDIATE</td>
<td>UnManageFrom</td>
</tr>
<tr>
<td>IN</td>
<td>UnManageUntil</td>
</tr>
<tr>
<td>INCLUDE</td>
<td>UNNEST</td>
</tr>
<tr>
<td>INDEX</td>
<td>UPDATE</td>
</tr>
<tr>
<td>INDICATOR</td>
<td>UPDATETEXT</td>
</tr>
<tr>
<td>INITIALIZE</td>
<td>UPPER</td>
</tr>
<tr>
<td>INITIALLY</td>
<td>USAGE</td>
</tr>
<tr>
<td>INNER</td>
<td>USE</td>
</tr>
<tr>
<td>INOUT</td>
<td>USER</td>
</tr>
<tr>
<td>INPUT</td>
<td>Username</td>
</tr>
<tr>
<td>INSENSITIVE</td>
<td>USING</td>
</tr>
<tr>
<td>INSERT</td>
<td>VALUE</td>
</tr>
<tr>
<td>INT</td>
<td>VALUES</td>
</tr>
<tr>
<td>INTEGER</td>
<td>VARCHAR</td>
</tr>
<tr>
<td>INTERSECT</td>
<td>VARIABLE</td>
</tr>
<tr>
<td>INTERVAL</td>
<td>VARYING</td>
</tr>
<tr>
<td>INTO</td>
<td>Vendor</td>
</tr>
<tr>
<td>IOSImage</td>
<td>VendorIcon</td>
</tr>
<tr>
<td>IOSVersion</td>
<td>VIEW</td>
</tr>
<tr>
<td>IP_Address</td>
<td>WAITFOR</td>
</tr>
<tr>
<td>IP_Address_Type</td>
<td>WHEN</td>
</tr>
<tr>
<td>IPAddressGUID</td>
<td>WHenever</td>
</tr>
<tr>
<td>IS</td>
<td>WHERE</td>
</tr>
<tr>
<td>ISOLATION</td>
<td>WHILE</td>
</tr>
</tbody>
</table>
Edit node properties

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

You need **Node Management Rights**.

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

1. Click Settings > Manage Nodes.
2. Locate the node for which you want to edit properties.
   
   To find the node, use the filter and search tools above the nodes list.

3. Select the node, and click Edit Properties.

- IsServer
- ITERATE
- JOIN
- KEY
- KILL
- LANGUAGE
- LARGE
- LAST
- LastBoot
- LastSync
- LastSystemUpTimeUtc
- LATERAL
- LEADING
- LEFT
- LESS
- LEVEL
- LIKE
- LIMIT
- LINENO
- LOAD
- LOCAL
- LOCALTIME
- LOCALTIMESTAMP
- Location
- LOCATOR
- LOWER
- WirelessAP
- WirelessLastStatPoll
- WirelessPollInterval
- WirelessStatBlockUntil
- WITH
- WITHOUT
- WORK
- WRITE
- WRITETEXT
- YEAR
- ZONE
Edit the node name, web address, and which view opens when you double-click the node

1. To rename the node, type the new name in the Name field. 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.
2. To change the view which displays details about this node, select the View Type from the list.
3. To change the template for the address used in the Node Details resource that allows you to navigate to the node from the resource, scroll down to Web Browse Template, and change the default http://{{HrefIPAddress}}.
4. Click Submit.

Edit polling settings

1. To change the polling IP address, type the new IP address, or click Select IP Address and select the new IP address.

   ![Warning]
   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.

   ![Info]
   If the device is dual-stack, IPv4 resolution will be 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. If you have high-speed interfaces, and you are experiencing frequent counter rollovers, confirm that the monitored device supports 64-bit counters, and select Allow 64-bit Counters.

   ![Info]
   Some vendor implementations of 64-bit counters produce faulty data. If you notice erratic 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).

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

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

   d. Click Test to test your provided SNMP settings.
5. To change the existing polling intervals, provide new intervals in the Node Status Polling, Collect Statistics and Poll for Topology Data fields.
6. If there are multiple polling engines in your environment and you want to change the polling engine that polls the node, click Change Polling Engine.

7. Click Submit.

## Edit dependencies or custom properties

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

## Add what additional data you want to poll on the node

1. 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.

2. 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.

3. 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.
      
      Administrator credentials are needed only for installing agents.
   
   b. Click Test to validate.
   
   c. Enter the Domain Controller Polling Interval to be used. The default is 30 minutes.

4. To poll for VMware, select Poll for VMware, provide the vCenter or ESX Server credentials, and click Test.

5. If the node is an F5 device and you want to monitor load balancers, select Poll for i5 Control, and provide the credentials.

6. Click Submit.

## Customize alerting thresholds

Be informed when polled values for a metric on the node reach unwanted values by specifying custom thresholds for the node.

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

See the Network Performance Monitor Getting Started Guide for more information about network discovery.

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.

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
User Device Tracker Port Discovery

When you have finished discovering network devices and importing them into the Orion Platform database, you must discover the Ethernet ports on those devices whose connections you want SolarWinds UDT to monitor.

To do this, you use the DISCOVER MY PORTS option in Discovery Central.

To discover ports:

1. Click Settings near the top right of the application window.
2. Click Discovery Central in the Getting Started with Orion category, and then click DISCOVER MY PORTS.
3. Select the desired device classification in the Group By list.
4. Select the desired devices in the tree and then click NEXT. The discovery begins.

   If you install SolarWinds UDT on a machine that already has NPM installed (same DB), then you will be able to add ports from any of those existing here.

5. The Advanced Filtering Options are displayed to reduce the number of ports to actively monitor.
6. Expand the Advanced Filtering Options tree and select the desired options:
   a. Check Active Status or Inactive Status depending on whether you want to actively monitor the ports or not.
   b. Check Trunk if you only want to select trunk (uplink) ports in the filter. If Trunk is not checked, then both trunk ports and access ports will be selected in the filter.
   c. Specify Port Range using values separated by commas. HP uses a convention of 1-48. Cisco uses a row/port notation (and a switch/row/port notation for stacked switches). An example for Cisco is: 0/1-48, 1/1-48,1/1-24 etc.
   d. Specify VLAN as an integer ranging from 1-4095. You can provide a comma-separated list or range. For example: 1,2,5,6-20,66.
   e. Specify Port Description for each port by specifying a different description on each line using strings, *, or regular expressions. For information about using regular expressions, refer to Appendix C, "Regular Expression Pattern Matching".

7. Expand the Device tree at the bottom of the page and select the desired ports:
8. Click Filter All Ports Below to apply the selected filtering options to the selected ports. If you want to undo the filtering, deselect the Advanced Filtering Options chosen previously and click Filter All Ports Below. Then click the check box next to the Name column (or the check box next to each desired device name) to restore all the discovered ports.
9. Click NEXT to begin monitoring the selected ports.
10. If you want to setup devices on a Watch List, so that you are alerted when they are seen on the network, click Next.
11. Click Add Device.
12. Add the MAC address, IP address, or hostname.
13. Give the device a descriptive name by which to recognize it in alerts.
14. Click OK.
15. Click OK, I'M DONE to return to Home, or click SETUP WATCH LIST to set up a watch list for selected hostnames and MAC addresses on your monitored ports.

Add Orion Nodes to UDT

User can display and monitor Orion Nodes with UDT by following the steps below.

1. Go to Settings near the top right of the application window.
2. Select UDT Setting under Product Specific Settings.
3. Under Port Management, choose show Nodes and filter to UDT Unmonitored Nodes.
4. Select the Nodes that need to be monitored by UDT and click Monitor with UDT.
5. A notification banner appears: "New Ports will be imported to UDT by next polling interval".

Event Notification for Nodes and Ports added to UDT

To know whether an Orion node was added to UDT, event notifications are triggered and can be found in the Last 25 Events resource in the UDT summary page.

Types of Event Notifications:

- When adding a group of nodes, event notification appears for the entire group and not for each node.
- The event message notification for a successful importation of a single node is "Ports of the node [node name] have been imported. [Reason is stated if known]."
- The event message notification for a failed general importation of a single node is "Ports of the node [node name] have not been imported. [Reason is stated if known]."
- The event message notification for a failed importation due to license limit of a single node is "Some ports of node [node name] have been imported as unmonitored due to license limit."
- The event message notification for a successful importation of multiple nodes is "Ports for [number of nodes] have been imported."
- The event message notification for a failed general importation of multiple nodes is "Ports for [number of nodes] have not been imported. [Reason is stated if known]."
- The event message notification for a failed importation due to license limit of a single node is "Some ports for [number of nodes] have been imported as unmonitored due to license limit."
- All event notifications related to nodes importation are displayed in the UDT Events resource.
Adding Active Directory Controllers and users

The following topics describe the process of adding an Active Directory domain controller into UDT and using it to track the activity of AD-associated users on your network.

UDT tracks user activity by reading an event log on the AD domain controller. Reading that log requires UDT to have the Event LogReader permission on each AD controller through which it is tracking user activity.

Before you add an AD domain controller, and begin tracking the user accounts that are associated with it, you must first create appropriate credentials for UDT to use in interacting with it.

- Managing Active Directory Credentials
- Managing Active Directory Domain Controllers
- Setting Up Polling of User Data Across Domains
- Defining Credentials for Polling Across Domains
- Setting WMI Namespace Security
- Adding a New AD Credential

Managing Active Directory Credentials

AD credentials are used in conjunction with the AD domain controllers you add into UDT.

The following sections explain how to add, edit, and delete AD credentials. We will also discuss the possible scenarios UDT will report when validating AD credentials.

Notes:

- The domain credential used by UDT for communications with the Domain Controller should have the following permission:
  - Event Log Readers
- The domain credentials should also have access to the WMI namespaces listed below:
  - CIMV2
  - directory
  - RSOP

Adding a New AD Credential

Follow these steps to add a new AD credential into UDT.

1. Click Manage Active Directory Administrator Credentials in the UDT Credentials area in UDT Settings (Settings > UDT Settings).
2. Click Add UDT Credential.
3. Enter a Credential Name. For example, if this credential were the one that you want UDT to use in retrieving event log data from an AD domain controller, you might call it Event Log Reader.

4. Enter a User Name (Domain\Username) that is known within a specific domain.

5. Enter and confirm the appropriate password, then click OK.

Editing an AD Credential

Follow these steps to edit an AD credential into UDT.

1. Click Manage Active Directory Administrator Credentials in the UDT Credentials area in UDT Settings (Settings > UDT Settings).
2. Click the Credential Name in the list, then click Edit Credential.
3. Make your changes.
   a. Enter a Credential Name. For example, if this credential were the one that you want UDT to use in retrieving event log data from an AD domain controller, you might call it Event Log Reader.
   b. Enter a User Name (Domain\Username) that is known within a specific domain.
   c. Enter and confirm the appropriate password, then click OK.

Deleting an AD Credential

Follow these steps to delete a credential.

You cannot delete a credential if it is currently associated with one or more domain controllers. You can check if a credential is currently assigned by referring to the Assigned to DC(s) column in the credentials list.

1. Click Manage Active Directory Administrator Credentials in the UDT Credentials area in UDT Settings (Settings > UDT Settings).
2. Click the Credential Name in the list, then click Delete Credential.

Domain controller configuration validation

The domain controller configuration validation is done on the following pages:

- Add node
- Manage domain controller
- UDT discovery (import Domain Controller page)

The following table shows possible scenarios that might be encountered when editing or entering AD credentials into UDT.

<table>
<thead>
<tr>
<th>Scenario</th>
<th>Result in UDT</th>
</tr>
</thead>
</table>
| WMI services is not running on the Domain Controller | UDT displays the warning message "WMI
service is not running"

| UDT credential does not have rights to the required WMI namespaces (CIMV2, directory and RSOP) | UDT displays the warning message "WMI service is running but user does not have enough permissions"

| If the audit account logon event is configured to the state "No Auditing" or "Failure" and the UDT credential does not have event log read access | UDT displays the error message "2 connection error"

| The audit account logon event is configured as expected but the UDT credential does not have event log read access | UDT displays the error message "1 connection error"

| The audit account logon event is not configured but the UDT credentials have event log read access | UDT displays the error message "1 connection error"

| If everything is set up as expected | UDT displays "Successful"

| If the supplied credentials are wrong | UDT displays "Test Failed"

---

**Managing Active Directory Domain Controllers**

UDT uses Active Directory domain controllers to retrieve information about user activity on network devices.

The following topics explain how to discover, add, edit and delete AD domain controllers from within UDT:

- Adding a new AD domain controller
- Edit an AD domain controller
- Assign a credential to an AD Domain Controller
- Delete an AD Domain Controller

**Adding a new AD domain controller**

Follow these steps to add a new AD [domain controller](#) into UDT.

1. Click Manage Active Directory Domain Controller in the Track Users and Endpoints area in UDT Settings (Settings > UDT Settings).
2. Click Add AD Domain Controller.
3. Enter a hostname or IP address under Define Node.
5. Select the appropriate credential for UDT to use with this AD domain controller. The UDT software automatically populates User Name and Password based on the values you entered when you created the credential. For information of credentials see [Managing Active Directory Credentials](#)
6. Click Next.
7. Select the node resources to monitor, then click Next.
8. Check Scan device for ports if you want to monitor the ports on this AD domain controller.
9. Review the properties you defined. When you are ready, click OK, ADD NODE.

The Domain Controller Polling Interval indicates how often UDT updates its information about user activity within the domain.

10. Click Advanced Settings under UDT Settings on the User Device Tracker Settings page (Settings > UDT Settings).
11. Review and adjust as needed the AD User Update Interval to match the rate at which AD user information is updated. This setting determines how often UDT polls the AD domain controller for user information.
12. After the polling interval, review the user information available from this AD domain controller in the All User Logins resource on the UDT Summary view.

Edit an AD domain controller

Follow these steps to edit an AD domain controller.

1. Click Manage Active Directory Domain Controller in the UDT Credentials area in UDT Settings (Settings > UDT Settings).
2. Select the AD domain controller in the list.
3. Click Submit.

Assign a credential to an AD Domain Controller

Follow these steps to assign a credential to an AD Domain Controller.

1. Click Manage Active Directory Domain Controller in the UDT Credentials area in UDT Settings (Settings > UDT Settings).
2. Select one or more AD domain controllers in the list.
3. Click Assign security log access credentials.
4. Select the relevant credential.
   For information about credentials see Managing Active Directory Credentials
5. If you are ready to assign the credential to the selected node(s), click OK.

Delete an AD Domain Controller

Follow these steps to delete a Domain Controller.

1. Click Manage Active Directory Domain Controller in the UDT Credentials area in UDT Settings (Settings > UDT Settings).
2. Select one or more AD domain controllers in the list.
3. Click Delete.
4. If you want to delete the node from UDT, select Delete node and data from UDT only.
5. If you want to delete the node from all SolarWinds products, select Delete node from all modules.
6. Click Delete.

**Set up polling of user data across domains**

Enabling UDT to poll user data, essentially by retrieving event log data, on an AD domain controller outside the local domain of the UDT server requires setup both in UDT and the AD domain controller. UDT supports the following methods for getting event log data from another domain:

**Eventing6**
- This is the preferred method and depends on the AD domain controller running Windows 2008 R2.

**WMI**
- This method is supported across Windows platforms.

UDT collects user information through a scheduled job (REL).

See also: [Define credentials for polling across domains](#)

**Define credentials for polling across domains**

Keep in mind these requirements when you set up your credentials for accessing an AD domain controller outside the local UDT server domain:

- The UDT user account must be a member of the target domain.
- The UDT user account must either be a member of the Administrators group on the target domain controller or a limited account with privileges to access the remote security event log and directory service on the remote domain controller. If UDT is using a limited account the account must be a member of these groups:
  - Domain Users
  - Distributed COM Users
  - Event Log Readers
  - Remote Desktop Users
- The domain credentials should also have access to the WMI namespaces listed below:
  - CIMV2
  - directory
  - RSOP

<i>You can use these instructions to give the account the relevant privileges.</i>

See also: [Set up polling of user data across domains](#)
Set WMI namespace security

You configure access to WMI namespaces through these steps on the target AD domain controller.

1. Open Administrative Tools (Control Panel > Administrative Tools)
2. Double-click Computer Management.
3. Expand the Services and Applications and double-click WMI Control.
4. Right-click WMI Control, and then select Properties.
5. On the Security tab, expand the tree under Root.
6. Select CIMv2 and then click Security.
7. Click Advanced.
8. Click Add.
9. Enter the account name in the text box and then click OK.
10. Confirm that Apply to is set to This namespace and subnamespaces.
11. Select the Allow check boxes for Execute Methods, Enable Account, and Remote Enable.
12. Click OK.
13. Select directory and then click Security.
14. Repeat steps 7-12.

The Custom Security Descriptor (CustomSD) in Windows 2003 Server may obstruct retrieval of user data even though the connection is open.

After you have the desired account setup for WMI access on the AD domain controller, you can add the account credentials to UDT. To do that, see Managing Active Directory Credentials.

Adding a new AD Credential

Follow these steps to add a new AD credential into UDT.

1. Click Manage Active Directory Administrator Credentials in the UDT Credentials area in UDT Settings (Settings > UDT Settings).
2. Click Add UDT Credential.
3. Enter a Credential Name. For example, if this credential were the one that you want UDT to use in retrieving event log data from an AD domain controller, you might call it Event Log Reader.
4. Enter a User Name (Domain\Username) that is known within a specific domain.

Whatever account you enter must have appropriate permissions on the AD domain controller for the tasks for which UDT would use it. The permission required to access the Event Log is Event Log Reader. See the section on Define credentials for polling across domains if the AD domain controller for which you are setting up UDT credentials resides in a domain outside the domain of the UDT server.

See also: Set WMI namespace security
Enable DNS resolution for wireless nodes

UDT uses the Orion Platform wireless component to manage wireless devices. By default, the wireless component does not resolve a wireless node's IP address into a hostname. To enable that, you must adjust a setting in the config file SolarWinds.Wireless.Collector.dll.config.

2. Modify the value of <add key="RDNSTimeout" value="0" />, changing the "0" to "1".
3. Save the change and restart the Orion Web Console.

See also: Manage the UDT White List
Endpoints and the White List

Manage the UDT White List

The White List enables you to tell UDT which endpoints on your network you consider safe. Using that list UDT can report a list of endpoints on the network that you do not consider safe, and these endpoints appear in the Rogue Devices resource.

The White List also enables you to tell UDT which endpoints on your network to ignore altogether. Any endpoint that you want UDT to ignore becomes completely invisible to all its resources.

Rules determine how the White List influences UDT’s endpoint monitoring behavior. By default UDT creates and enables three rules in the White List during software installation: Any Hostname, Any IP Address, and Any MAC Address.

With default rules enabled, all endpoints connected to your monitored UDT devices are placed on the UDT White List list; and as a result no endpoints appear on the list in the Rogue Devices resource.

UDT treats an endpoint’s MAC address, IP address, and hostname as separate objects. Depending on white list inclusion rules, one or more of those objects could possibly appear in the Rogue Devices resource at the same time.

See also:

- Enable DNS resolution for wireless nodes
- Add endpoints to the White List
- Remove endpoints from the White List
- Ignore endpoints in UDT
- Delete White List rules

Add endpoints to the White List

UDT uses inclusion rules to determine which endpoints connected to UDT-monitored devices are safe and unsafe. Endpoints UDT determines are unsafe, in that they are not covered by White List rules, appear in the list on the Rogue Devices resource.

Through its rules the UDT White List determines which endpoints connected to UDT enables three self-explanatory white list inclusion rules by default: Any Hostname, Any IP Address, and Any MAC Address. With these rules enabled, all endpoints connected to your monitored UDT devices are placed on your white list.

You add endpoints to the White List by adding or enabling rules:
Add rules
Enable rules

Add endpoints to the DNA White List by adding rules

You can add endpoints to the White List by adding rules (described below) or by enabling rules.

Follow these steps to add endpoints to the White List by adding rules.

1. Click Add New on Included.
2. Click a Selection Method and add the appropriate information.
   - Device (to add endpoints associated with a UDT device)
     - Enter the appropriate string. Click Add More to add another device, as needed.
   - IP Range or MAC Range (to add multiple endpoints)
     - Enter the Start address and End address. Click Add More to add another range, as needed.
   - Subnet (to add endpoints on an entire subnet)
     - Click the plus icon (+) and, in Add New Subnet, enter strings for the Subnet Address and Subnet Mask. Then click ADD.
   - Custom
     - Select a target and enter appropriate patterns. Enter each one on a separate line.
3. Click Next.
4. Optionally, enter a name for and description to help track why you added the device(s) to the white list.
5. Click FINISH.

Add endpoints to the White List by enabling rules

You can add endpoints to the White List by adding rules or by enabling rules. To enable a rule or rules:

1. Select the rule in the list.
2. Click Enable.

Remove endpoints from the White List

You remove endpoints from the White List by modifying or disabling inclusion rules:

- Edit rules
- Disable rules

Remove endpoints from the White List by editing rules

You can remove endpoints from the white list by editing rules (described below) or by disabling rules.
Follow these procedures to remote endpoints from your White List by editing existing rules.

1. Click Included.
2. If you need to modify an existing rule, select the rule and click Edit.
3. Modify the information under Input (which displays one of the following depending on how you initially defined the rules).
   - Device: Enter the appropriate string. Click Add More to add another device, as needed.
   - IP Range or MAC Range: Enter the Start address and End address. Click Add More to add another range, as needed.
   - Subnet: Click the plus icon (+) and, in Add New Subnet, enter strings for the Subnet Address and Subnet Mask. Then click ADD.
   - Custom: Select a target and enter appropriate patterns. Enter each one on a separate line.
4. Click Next.
5. Optionally, enter a name for and description to help track why you added the device(s) to the white list.
6. Click FINISH.

Remove endpoints from the White List by disabling rules

You can remove endpoints from the white list by editing rules or by disabling rules (described below).

To remove endpoints from your White List by disabling existing rules:

1. Select the rule in the list.
2. Click Disable.

**Ignoring Endpoints in UDT**

UDT uses ignore rules to determine which endpoints connected to UDT-monitored devices are irrelevant to tracking. Endpoints UDT determines are irrelevant, in that they are covered by white list rules, do not appear in UDT resources.

You ignore endpoints in UDT by adding or enabling rules:

- Adding Rules
- Enabling Rules

Wireless endpoints cannot be ignored. Exclusion rules do not apply to them.

**Ignore endpoints in the White List by adding rules**

You can ignore endpoints in the white list by adding rules (described below) or by enabling rules.
Follow these steps to ignore endpoints in UDT by adding new rules.

1. Click Add New on Ignored.
2. Click a Selection Method and add the appropriate information.
   - Device (to add endpoints associated with a UDT device)
     - Enter the appropriate string. Click Add More to add another device, as needed.
   - IP Range or MAC Range (to add multiple endpoints)
     - Enter the Start address and End address. Click Add More to add another range, as needed.
   - Subnet (to add endpoints on an entire subnet)
     - Click the plus icon (+) and, in Add New Subnet, enter strings for the Subnet Address and Subnet Mask. Then click ADD.
   - Custom
     - Select a target and enter appropriate patterns. Enter each one on a separate line.
3. Click Next.
4. Optionally, enter a name for and description to help track why you added the device(s) to the white list.
5. Click FINISH.

Ignore endpoints in the White List by enabling rules

You can ignore endpoints in the white list by adding rules or by enabling rules (described below).

To ignore endpoints in UDT by enabling existing rule:

1. Select the rule in the list under Ignored.
2. Click Enable.

Delete White List rules

To delete a White List rule, select the rule in the list and then click Delete.
Viewing Status: Device, Port, User, SSID

The following sections provide a short list and overview of the views and resources provided with User Device Tracker that reveal status information.

For information on customizing a view, editing or deleting resources, see [Create, delete, modify, or restrict views](#).

- **Using the Device Tracker Summary**
- **Using the Device Tracker Port Details**
- **View node and port data in tooltips**
- **Use the Device Tracker Access Point Details**
- **Use the Device Tracker SSID Details**
- **Use the Device Tracker User Details**
- **View User Data in Tooltips**

**Using the Device Tracker Summary**

The Device Tracker Summary view provides the following resources. You can customize which of these resources appear on the page by clicking Customize Page.

<table>
<thead>
<tr>
<th>RESOURCE</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>All UDT Nodes</td>
<td>The All UDT Nodes resource provides a list of nodes, grouped by node property, with a status icon and the node name displayed for each node. Expanding a node displays the ports for the node with a status icon and the port name displayed for each port.</td>
</tr>
<tr>
<td>Total Ports Currently Used</td>
<td>Provides a chart with the total number and percentage of used and free ports.</td>
</tr>
</tbody>
</table>
| All User Log Ins | Provides a list of users logged in within the footprint of the monitored network. Logins are listed by most to least recent.

User Search (type in a username) to limit the list to the logins by a specific user. |
| Active Alerts | Provides a list of the active alerts associated with UDT devices and ports. |
| Top XX Nodes by Percent Ports Use | Provides a list of the nodes with the highest percent of ports used. Because comparing disparate statistic measurements is of limited use, we suggest you create Statistic Data resource containing filters to limit the statistic sources. |
## Rogue Devices
The Rogue Devices resource provides a list of endpoints that fall outside the rules defined to determine which endpoints are on the White List and are considered safe.

## Device Watch List
Displays the Device Watch List.

## Ethernet Ports Used Over Time
Provides a chart of the ethernet ports used over time with a menu of view options for:
- Last 7 days
- Last 30 days
- Edit Chart
- View Chart Data
- View Chart Data in Excel

## Last 25 Events
Provides a list of the last twenty-five events associated with UDT. For more information about creating alerts for these events, see [Use alerts to monitor your environment](#).

## Top 10 SSIDs by Current # of Endpoints
Shows the 10 Service Set Identifiers (SSIDs) with the most current endpoint connections. The information is presented in a table by SSID and the number of Current Endpoint Connections.

## Top 10 Access Points by Current # of Endpoints
Shows the 10 wireless access points with the most current endpoint connections. The information is presented in a table by Access Point and the number of Current Endpoint Connections.

### Using the Device Tracker Port Details

The Device Tracker Port Details view opens when you click on a specific port on a node in UDT Nodes, and provides the following resources. You can customize which of these resources appear on the page by clicking Customize Page. You may see different resources depending on the item you are viewing.

#### Port Details

Provides a list of port properties, including the port name, port number, MAC addresses of the devices connected to the port, VLANs, and Duplex mode.

Click EDIT to specify the following port details information:
- **Maximum Number of IPV4 Addresses to Display** - specifies the maximum number of connected IPV4 addresses to display in the GUI.
- **Maximum Number of IPV6 Addresses to Display** - specifies the maximum number of connected IPV6 addresses to display in the GUI.
- **Maximum Number of MACs to Display** - specifies the maximum number of connected MAC addresses to display in the GUI.

**Port History**

Provides a table of port history information, including the time period, connected IP addresses, connected MAC addresses, and hostnames.

Click EDIT to specify the following port history information:

- **Maximum Number of Rows to Display** - specifies the maximum number of rows to display in the history table for the GUI.

View node and port data in tooltips

Node and port tooltips in SolarWinds UDT provide immediate status overviews of monitored nodes and ports. To view a quick overview of any monitored node or port in the web console, hover over a node or port. Depending on the selected device, the information in the following tables is displayed immediately.

### Node tooltips

<table>
<thead>
<tr>
<th>HOVER OVER...</th>
<th>TO SEE...</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>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>
Port tooltips

<table>
<thead>
<tr>
<th>Hover Over...</th>
<th>To See...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port Name</td>
<td>Name of the port.</td>
</tr>
<tr>
<td>Oper Status</td>
<td>Operational status of the port (up, down).</td>
</tr>
<tr>
<td>Admin Status</td>
<td>Administrative status of the server (up, down, warning, unplugged, or unmanaged).</td>
</tr>
<tr>
<td>Interface Type</td>
<td>The interface type of the port.</td>
</tr>
<tr>
<td>Active Connection</td>
<td>Whether the connection is active or not.</td>
</tr>
<tr>
<td>VLAN</td>
<td>Displays information about the VLAN.</td>
</tr>
<tr>
<td>Duplex</td>
<td>Displays the Duplex mode: FullDuplex, HalfDuplex, or Unknown.</td>
</tr>
<tr>
<td># of connected IPs</td>
<td>Number of connected IP addresses</td>
</tr>
<tr>
<td># of connected MACs</td>
<td>Number of connected MAC addresses</td>
</tr>
</tbody>
</table>

Use the Device Tracker Access Point Details

The Device Tracker Access Point Details view opens when you click on a specific access point in Top 10 Access Points on the Device Tracker Summary view, and it provides the following resources. You can customize which of these resources appear on the page by clicking Customize Page. You may see different resources depending on the item you are viewing.

**Current Endpoint Connections**

Shows all endpoint connections on a specific access point or SSID. The information is presented in a table by Endpoint Name, Last User Login, Connection Duration (in minutes), and the name of the SSID (only if the resource is displayed on an Access Point Details view).

Click EDIT to specify the following information:

- Title - specifies the title of the resource.
- Subtitle - specifies a subtitle of the resource.
- Maximum Number Endpoint Connections to Display - specifies the maximum number to display of the endpoints connected to the access point.

**All Endpoint Connections**
Shows all endpoint connections on a specific access point or SSID. The information is presented in a table by Endpoint Name, Last User Login, Connection Duration (in minutes), and the name of the SSID (only if the resource is displayed on an Access Point Details view).

Click EDIT to specify the following information:

- Title - specifies the title of the resource.
- Subtitle - specifies a subtitle of the resource.
- Maximum Number of Endpoint Connections to Display - specifies the maximum number to display of the endpoints connected to the access point.

**Wireless Access Point Details**

Shows information about a specific wireless access point. The information is presented in a table that indicates the access point Status (Up/Down), Access Point Name, Access Point IP Address, the access point Type (Thin/Autonomous), and the wireless Controller.

Click EDIT to specify a different title for the resource or to add/edit a subtitle.

**All SSIDs**

Shows all Service Set Identifiers (SSIDs) associated with a wireless access point. The information is presented in a table by SSID, Channel, and the number of Current Endpoint Connections.

Click EDIT to specify the following information:

- Title - specifies the title of the resource.
- Subtitle - specifies a subtitle of the resource.
- Maximum Number of SSIDs to Display - specifies the maximum number to display of the endpoints connected to the access point.

**Using the Device Tracker SSID Details**

The Device Tracker SSID Details view opens when you click on a specific SSID in Top 10 SSIDs on the Device Tracker Summary view, and it provides the following resources. You can customize which of these resources appear on the page by clicking Customize Page. You may see different resources depending on the item you are viewing.

**Current Endpoint Connections**

Shows all endpoint connections on a specific access point or SSID. The information is presented in a table by Endpoint Name, Last User Login, Connection Duration (in minutes), and the name of the SSID (only if the resource is displayed on an Access Point Details view).

Click EDIT to specify the following information:
- Title - specifies the title of the resource.
- Subtitle - specifies a subtitle of the resource.
- Maximum Number Endpoint Connections to Display - specifies the maximum number to display of the endpoints connected to the access point.

All Endpoint Connections

Shows all endpoint connections on a specific access point or SSID. The information is presented in a table by Endpoint Name, Last User Login, Connection Duration (in minutes), and the name of the SSID (only if the resource is displayed on an Access Point Details view).

Click EDIT to specify the following information:

- Title - specifies the title of the resource.
- Subtitle - specifies a subtitle of the resource.
- Maximum Number of Endpoint Connections to Display - specifies the maximum number to display of the endpoints connected to the access point.

All Access Points

Shows a table of all Access Points, the Channel on which they are broadcasting a signal, and the number of Current Endpoint Connections.

Click EDIT to specify the following information:

- Title - specifies the title of the resource.
- Subtitle - specifies a subtitle of the resource.
- Maximum Number of Access Points to Display - specifies the maximum number of access points to display.

Use the Device Tracker User Details

Device Tracker User Details view opens when you click on a specific user listed under All User Log Ins, and provides the following resources. You can customize which of these resources appear on the page by clicking Customize Page. And you can export the view to a PDF file by clicking Export to PDF.

User Details

Provides a list of details associated with the user account, including the user's display name, first and last name, title, department, office, company, manager, assistant, email addresses, group memberships, phone number, street address, city, state, zip code and country/region.

Click EDIT to specify the maximum number of email addresses or groups to display for this user and the maximum number or details (rows) to display for from the user record.
Note: the UDT database receives all the information from the AD domain controller that the administrator has not blocked due to internal or other policies.

All Endpoint Log-ins

Provides a searchable list of endpoints on which this specific user has logged in, including the endpoint name, most recent log in time.

Use the Search window to see data only related to a specific endpoint.

Click Show All to see a complete list for this user that extends beyond the row limit set for the resource display.

Click EDIT to specify the number of rows to display.

View user data in tooltips

User tooltips in SolarWinds UDT provide immediate status overviews of monitored users. To view a quick overview of any monitored user in the web console, hover over a user in the list. Depending on the selected user, and the policies on the AD domain controller, the information in the relevant user record is displayed. This table includes an example of the information commonly available; most fields are self-explanatory.

User tooltips

<table>
<thead>
<tr>
<th>Hover over...</th>
<th>To see...</th>
</tr>
</thead>
<tbody>
<tr>
<td>User</td>
<td>The user name on the relevant AD domain controller.</td>
</tr>
<tr>
<td>Title</td>
<td>The user's title within the company.</td>
</tr>
<tr>
<td>Office</td>
<td>The user's home office within the company.</td>
</tr>
<tr>
<td>Department</td>
<td>The user's department within the company.</td>
</tr>
<tr>
<td>Company</td>
<td>The user's company.</td>
</tr>
<tr>
<td>Address</td>
<td>The user's company address.</td>
</tr>
<tr>
<td>City</td>
<td>The city in which the user's office is located.</td>
</tr>
<tr>
<td>State</td>
<td>The state in which the user's office is located.</td>
</tr>
<tr>
<td>Zip Code</td>
<td>The relevant USPS postal code.</td>
</tr>
<tr>
<td>Country/Region</td>
<td>The country in which the user is based.</td>
</tr>
</tbody>
</table>
Manage SolarWinds UDT Polling Engines

To ensure that your polling engines are optimized to run at peak performance, you will need to occasionally tune them. If you use more than one polling engine, you will need to balance the load so that each engine can perform optimally.

- View Polling Engine Status in the Web Console
- Configure Polling Engine settings
- Orion Platform Polling settings
- Calculate node availability
- Calculate a baseline
- Use the Polling Engine Load Balancer
- Set the node warning level
- Manage packet loss reporting

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.

Configure polling engine settings

Click Settings > All Settings, and in the Thresholds & Polling group, click Polling Settings to configure your polling engine.

For information about the options you can configure, see Update polling settings.

Update polling settings

Click Settings > All Settings, and in the Thresholds & Polling group, click Polling Settings to configure your polling engine.

Depending on the Orion Platform products you have installed, additional polling settings may be available. See your SolarWinds Orion Administrator Guide for more information about the settings.

Configure polling interval settings

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 Interface Poll Interval (SolarWinds NPM)**

The interval for polling the status and response time of monitored interfaces. By default, this interval is 120 seconds. Available only if SolarWinds NPM is installed.

**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](#).

- 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.

- 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 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.
Interface Baseline Calculation Frequency
Specify how often the interface baseline calculation runs.

Detailed Interface Availability Statistics Retention
Specify the number of days until the detailed interface availability statistics in the SolarWinds Orion database are summarized into hourly statistics. By default, this period is seven days.

Hourly Interface Availability Statistics Retention
Specify the number of days until the hourly interface availability statistics are summarized into daily statistics. By default, this period is 30 days.

Daily Interface Availability Statistics Retention
Specify the number of days until the daily interface availability statistics are deleted from the database. By default, this period is 365 days.

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.

Detailed UnDP Statistics Retention
Specify the number of days until the detailed UnDP statistics are summarized into hourly statistics.

Hourly UnDP Statistics Retention
Specify the number of days until the hourly UnDP statistics are summarized into daily statistics.

Daily UnDP Statistics Retention
Specify the number of days until the daily UnDP statistics are deleted from the database.

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.

![Warning]

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.

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.
Using the Polling Engine Load Balancer

The Polling Engine Load Balancer is a useful tool for reassigning nodes to a new polling engine, deleting an unused polling engine, and performing load balancing between multiple polling engines. The tool is available within the Monitor Polling Engines application, which is an advanced feature of SolarWinds Orion Platform products. Reassigning nodes to new polling engines may be required in the following situations:

- Moving or renaming your SolarWinds Orion server
- Merging two or more SolarWinds Orion servers

If these or any other conditions present the need for reassignment, complete the following procedure to reassign nodes to a new polling engine.

1. Click Start > All Programs > SolarWinds Orion > Advanced Features > Orion Service Manager.
2. Click Shutdown Everything.
   
   **Info:** Confirm that you stop the SolarWinds Network Performance Monitor Service on all polling engines.

3. Click Start > All Programs > SolarWinds Orion > Advanced Features > Monitor Polling Engines.
4. Click Servers > Poller Load Balancing.
5. Select the nodes you want to reassign.

   **Info:** Use Shift + click to highlight multiple consecutive rows, and use Ctrl + click to highlight multiple non-consecutive rows.

6. Click Polling Engines > Move Selected Nodes to *, substituting the target polling engine for *. The node is reassigned, and it reflects the name of the polling engine in the polling engine column.
7. Click Start > All Programs > SolarWinds Orion > Advanced Features > Orion Service Manager to restart Orion services.

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.

**Info:** 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.

**Tip:** 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.

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.

   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.
Solutions

Finding the switch and port where a particular hostname, IP, or MAC address is or was connected

Scenario: I need to find the switch and port where a particular hostname, IP, or MAC address is now connected or was connected in the past in order to respond to a security or network problem.

1. Click the DEVICE TRACKER tab, if not already selected.
2. Locate UDT Search (just below the menu bar near the top right of the page).
3. Click the menu button in the search box, and select the desired option(s) for the search.

- MAC addresses are stored without formatting; you can successfully search for a MAC address with format xxxx.xxxx.xxxx or xx-xx-xx-xx-xx-xx or xx:xx:xx:xx:xx:xx.

4. Enter the desired term for the search.
   This example uses IP address '10.199.0.3' as the target device.
   In general, specific matches are required sought unless wildcards are used in the search term. This means that if you search for laptop and there is a machine named laptop01, you will not find it unless you search for laptop01 or laptop* (or other valid wildcard search).

5. Press Enter or click the search button to begin the search.
   The search results are displayed in a scrollable, tabular view. For each item, the following information is displayed in columns:
   - Match Item
   - Match Type
   In this example, searching on subnet '10.199.*', we get a list of one item and the software automatically navigates to the Device Tracker Endpoint Details for '10.199.0.3', showing us:

<table>
<thead>
<tr>
<th>NODE PORT</th>
<th>NODE NAME</th>
<th>CONNECTION DURATION</th>
<th>CONNECTION TYPE</th>
</tr>
</thead>
<tbody>
<tr>
<td>A1</td>
<td>Core-4500</td>
<td>24 days, 8 hours, 5 minutes</td>
<td>Endpoint IP Address</td>
</tr>
<tr>
<td>(Router)</td>
<td>Core-4500</td>
<td>24 days, 8 hours, 5 minutes</td>
<td>Endpoint IP Address</td>
</tr>
</tbody>
</table>

- Search returns a separate row each for active and inactive connections. If you cannot find a device, but know that it is connected, search using the MAC address to find the port that points to a physical location. MAC addresses are stored without formatting. You can successfully search for a MAC address with format xxxx.xxxx.xxxx or xx-xx-xx-xx-xx-xx or xx:xx:xx:xx:xx:xx.
6. To monitor this endpoint as a node, click Start monitoring as a node under Endpoint details.

**Display rogue endpoint connections in real-time**

Scenario: I have my White List set up but I want real-time or near real-time alerts when a rogue device connects to the network.

To cover this scenario, you will need to set up your devices to send connection-related traps to the UDT server. UDT checks the database for trap-related information at set intervals. If an endpoint connects to a UDT device, and the endpoint is not on the White List, UDT posts an alert in the web console.

- The following instructions are for Cisco devices only
- You can remove device configurations by running a given command with 'no' in front of it; for example, no set logging server ip_address removes that target from the remote logging stream.

To enable your Cisco devices to send trap messages:

1. Open a command line in config mode on your device.
2. Execute the commands from the examples, changing the IP address to match your UDT server.

   **Traps (IOS)**
   - snmp-server host 10.110.68.33 public config
   - snmp trap mac-notification change added
   - snmp trap mac-notification change removed

   **Traps (CatOS)**
   - set snmp trap 10.110.68.33 public config
   - snmp trap mac-notification change added
   - snmp trap mac-notification change removed

3. Open the UDT Settings on the UDT server (Settings > UDT Settings).
4. Click Advanced Settings.
5. Enter a value (in seconds) under MAC Notification Processing Inverval for the frequency with which you want UDT to check for new trap messages.
6. Click Save.
7. To verify your setup, connect a device to the network that is not on the UDT White List.
8. Wait for the time you allotted in Step 5 and then check the Active Alerts and All Triggered Alerts resources for an entry that shows the MAC address of the device you just connected.

**Track status for a group of ports**

Scenario: I need to track port usage for all of my Cisco devices.
To cover this scenario, you will need to create an Orion Platform group containing the relevant ports and then select that group in UDT resources.

1. Click Start > All Programs > SolarWinds > Orion Web Console.
2. Click Settings in the top right of the web console.
3. Click Manage Groups in the Node & Group Management grouping of the Orion Website Administration page.
4. Click Add New Group.
5. Enter a name for the group (for example, "Cisco Ports") in the Name field, and then expand Advanced.
6. If you want the group to roll up the worst status of the group members, select Show Worst Status.
7. If you want the group to roll up the best status of the group members, select Show Best Status.
8. If you want the group to display a warning status if the group members have a mixture of different statuses, select Mixed Status shows warning.
9. Click Next.
10. Click Add dynamic query.
   a. Type a name for the query in the Dynamic query object name field.
   b. Select Port in the Orion Object is list.
   c. Click Add Condition and build the following condition with the three drop-down lists: Port Operational Status is 1.
      This condition limits the group membership to operational ports.
   d. Click Add Condition again and build the following condition with the three drop-down lists: Port Vendor is Cisco.
      This condition limits the group membership to ports on Cisco devices.
   e. Click Preview to verify that the dynamic query is selecting your intended objects.
   f. Click Save.
11. Click Create Group.
    This group is now available for you to use in a UDT port resource.
12. Click Customize Page on the UDT Summary view.
13. Click the plus (+) above the column in which you want the new port status resource to appear.
14. Select Total Ports Currently Used under UDT Port Charts and then click Done.
15. Click Edit in the new Total Ports Currently Used resource.
    Give the resource an appropriate title (for example, "Cisco Ports Usage").
16. Under Groups select the name of the group you created (for example, "Cisco Ports").
17. Click Submit.

The chart now shows you the percentage of usage for all grouped ports on your Cisco devices.
Shut down a network device port

Scenario: UDT is listing an endpoint on my network as rogue. I want to shut down access to the endpoint immediately while I investigate.

1. Click the endpoint in the Rogue Devices resource.
2. Click the node port in the Current Network Connections resource on Endpoint Details.
3. Click the Shutdown button in the Port Details resource.

Create and manage a Watch List

Scenario: I need to create a watch list to be alerted when certain IP or MAC addresses, or a certain user, connects to the network.

This scenario assumes that you have already discovered appropriate nodes and ports, and that you have added an Active Directory domain controller and appropriate credentials for UDT to use in retrieving user information. For more information on discovery, see Discover and add network devices; for more information on adding a domain controller and credentials, see Adding Active Directory Controllers and users.

1. Click the DEVICE TRACKER tab, if not already selected.
2. Click MANAGE LIST on the Device Watch List resource.
3. Click Add Device/User.
4. Select an object type (MAC address, IP address, hostname, or username) and enter a valid string.
5. Optionally, give this item a name and description.
6. Click Submit.
7. Repeat 1-6 for all objects you want added to the Watch List.

Find wireless endpoint connections

Scenario: I need to find the endpoint(s) currently connected to the wireless network through a particular SSID.

1. Click the DEVICE TRACKER tab, if not already selected.
2. Click the relevant node (wireless controller) in the UDT node list.
3. In the Node Details view locate the relevant SSID by clicking + as needed to expand the list of SSIDS related to the access points in the All Access Points and SSIDS resource.
4. Click the SSID.
   The Current Endpoint Connections resource shows the endpoints currently connected to the wireless network through the specific SSID and the All Endpoint Connections shows all endpoints connected via the SSID during a specified period (for example, Last 7 Days).
5. If you do not see an endpoint that you expect to see, you can search for it by IP address, hostname, or MAC address in either the Current Endpoint Connections or the All Endpoint Connections resource.

Find a user's connections

Scenario: I need to find the endpoint(s) where a specific user is or has been connected to the network.

1. Click the DEVICE TRACKER tab, if not already selected.
2. Locate UDT Search (just below the menu bar near the top right of the page).
3. Click the menu button in the search box, and select user name.
4. Enter the user name to search (in this example, "Maxine.Tarnow") press Enter or click the search button to begin the search.

With a successful search the software automatically navigates to the Device Tracker User Details for domain\Anais.Nin, showing us the user's connections in the All Endpoint Log Ins resource:

<table>
<thead>
<tr>
<th>ENDPOINT NAME</th>
<th>MOST RECENT LOG IN TIME</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.110.67.21</td>
<td>12/14/2016 4:24:15 PM</td>
</tr>
<tr>
<td>10.110.67.68</td>
<td>12/13/2016 1:02:00 PM</td>
</tr>
</tbody>
</table>

Find endpoints in a subnet

Scenario: I need to find all endpoints currently on a subnet.

1. Click the DEVICE TRACKER tab, if not already selected.
2. Locate UDT Search (just below the menu bar near the top right of the page).
3. Click the menu button in the search box, and select the desired option(s) for the search.

MAC addresses are stored without formating; you can successfully search for a MAC address with format xxxx.xxxx.xxxx or xx-xx-xx-xx-xx-xx or xx:xx:xx:xx:xx:xx.
4. Enter the desired term for the search.
   This example uses IP address '10.199.3.*' as the target subnet.
   In this case we are searching for an exact match. In general, specific matches are required sought unless wildcards are used in the search term. This means that if you search for laptop and there is a machine named laptop01, you will not find it unless you search for laptop01 or laptop* (or other valid wildcard search).
   More wildcard examples:
   - Fa1* - (when used with Port Number search option) matches any port number that begins with Fa1 followed by any characters.
   - MAC Address: 00:0C*
   - IP Address: 10.10.10.*
   - Cisco3750-* (assuming each of three stacked switches were added as individual devices, using a common naming convention like Cisco3750-1, Cisco3750-2, Cisco3750-3; in this search you would select the 'Connected To' drop-down list beside Search).

5. Press Enter or click the search button to begin the search. The search results are displayed in a scrollable, tabular view:

<table>
<thead>
<tr>
<th>MATCH ITEM</th>
<th>MATCH TYPE</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.199.3.1</td>
<td>Endpoint IP Address</td>
</tr>
<tr>
<td>10.199.3.10</td>
<td>Endpoint IP Address</td>
</tr>
<tr>
<td>10.199.3.100</td>
<td>Endpoint IP Address</td>
</tr>
<tr>
<td>10.199.3.101</td>
<td>Endpoint IP Address</td>
</tr>
<tr>
<td>10.199.3.102</td>
<td>Endpoint IP Address</td>
</tr>
<tr>
<td>10.199.3.103</td>
<td>Endpoint IP Address</td>
</tr>
<tr>
<td>...</td>
<td>...</td>
</tr>
</tbody>
</table>

6. From the search results, you can select an item and then click Add To Watch List in order to add the item to the device watch list.
Resolve IP address conflicts with IPAM and UDT integration

Integration with UDT and IPAM is available with UDT v 3.2 and IPAM v 4.3 or higher. If you are running both products, the built-in integration provides a view of end-to-end mapping of an IP address to any connected user/device, along with the device port and connection details all in the same window. If you are running UDT v 3.2 and IPAM v 4.3 or higher, no steps are needed for integrating the two products. IPAM will automatically detect if UDT is installed and add UDT users and switch port columns to your IP address view. The following screen shot shows the display presented in the IPAM "Manage Subnets & IP Address" resource.

Integrating IPAM with UDT can help you troubleshoot in the following ways:

- Find out which user or device is accessing a particular IP address
- Drill down to get network connection history for an IP address
- See port and user information related to an IP address or host DNS assignment
- View port usage and capacity on every switch
- Detect endpoint devices having IP address conflicts
- Shutdown a port through the web interface
IPAM can detect IP Address conflicts (both IP static and DHCP environments) and help you to troubleshoot the problem by simply drilling down to the actual switch port and shutting it down.

Once you see an IP Address conflict event/alert, simply click on the IP or MAC address info in the alert message and it will take you to the IP Address Details view, where you can see the MAC address assignment history.

If you determine you need to resolve the conflict on the spot, you can administratively shutdown the port using UDT.

IP address conflicts will trigger an event displaying the MAC addresses in conflict. The following screen shot shows an example of what to look for:

![IPAM displays the IP address history along with the MAC address of the IP address in conflict.](image)

To shut down the conflicting port:
1. Click on the node port in the IPAM "Current Network Connections" resource on "Endpoint Details".
2. Click Shutdown in the "Port Details" resource.
The Orion Platform

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.

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.

   **DEFAULT MENU BAR AND VIEWS**
   Select the menu bar for this account. To view the contents of each
   Home Tab Menu Bar  New York ▼
   Network Tab Menu Bar  Network_TabMenu ▼

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.

![Menu bars and order selection](image)

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.

![Menu Bar: New York](image)

3. Drag available items from the left-hand column to Selected Items on the right.

![Available and selected items](image)

1. Hover over any view title to read the description.
   To change the order of menu items, drag and drop items in the Selected column.
4. Click Submit to save your changes.

You can also add links to node details views for specific nodes, or to external Internet pages as a menu item.

a. Click Add below the Available items list, provide a name, URL and description for the menu item, and click add.
b. Drag the new item to the Selected items column.

Users who can see the menu bar in My Dashboards will see the added items.

Add menu bars

When you have a list of items you want users to access from My Dashboards, create a menu bar.

1. Click My Dashboards > Configure.
2. Scroll to the bottom of the page, and click New Menu Bar.
3. Name the menu bar.
4. Drag views from the Available items column into Selected items.

5. Click Submit.

The new menu bar is created. You can now assign it to users who will see the items in My Dashboards.

Change the Orion Web Console color scheme

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

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. For a list of database changes from Orion Platform version 2014.2 to version 2016.1, including new tables, column changes, or data constraint or data type changes, see the Database Changes spreadsheet.

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.
   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.

   Defined custom properties are listed for all grouping types.

   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.

Customize charts in the Orion Web Console

Use the customization options available in the chart to customize the data, layout and time frame shown by the chart.

Available customization options depend on the chart.

Drop-down customization options

Some charts have drop-down menus that include the following options:

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

Edit Resource page

If a chart has an Edit button, click it to get to the Edit Resource page. Edit titles, time periods, or other details, and click Submit to go back to the view and see the changes applied in the chart.

**Titles and subtitles**

You can customize the title and subtitle for the resource and for the chart.
To change the chart labels, click Advanced, and enter a text or variable that displays as the chart title or subtitle.

The default for the chart subtitle is \$\{ZoomRange\}, which shows the selected zoom range.

Other options depend on the chart type.

**Calculated series: Show a trend line**

Select the box to display a trend line on the graph. This shows potential future results as extrapolated from collected historical data.

The trend lines are intended only as approximate predictions of future data.

**Calculated series: Show the sum of all data series**

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

**Calculated Series: Show the 95th percentile line**

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

**Maximum Number of Items to Display:**

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

**Time periods: Default zoom range**

Select the default range of data to be displayed from the drop-down list.

**Time periods: Amount of historical data to load**

Select the amount of historical data to load from the drop-down list.

**Time periods: Sample interval**

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

Custom Chart page

Click Export or click the chart to open the Custom Chart page in a new tab. You can change the chart settings and click Refresh to see the changes applied in the same tab.

If the chart has a drop-down menu, you can also access the custom chart page by selecting the Edit chart option.
Title, Subtitle, Subtitle #2

Enter a title and optional subtitles to be displayed above the chart.

Time Period: Select a Time Period

Select the time period that you want the chart to cover.
Alternatively, you can enter a specific time period for the chart.

Time Period: Beginning Date/Time

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

Time Period: Ending Date/Time

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

Sample Interval

Select the sample interval. Each sample interval is represented on a chart by a single point or bar. Data within a selected sample interval is summarized automatically.

Chart Size: Width

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

Chart Size: Height

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

Font Size

Select the font size for the chart from the drop-down list.

Trend Line: Show Trend

Select the box to display a trend line on the graph. This shows potential future results as extrapolated from collected historical data.

Due to the broad array of factors that can affect the performance of devices, trend lines are intended as approximate predictions of future data only.

Display Chart Data: Raw Data

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

Display Chart Data: Chart Data

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

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 for creating 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>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.

   ![Note on Type of View](image)

   The Type of View affects how the view is made accessible to users, and your choice may not be changed later. For more information, see Specify views for device types.

   After you have created a new view, the Customize page opens.

**Add resources and columns to views, and define subviews**

Administrators can edit views on the Customize page for the view. Click Customize Page on the view, or access the page through Manage Views.

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 resources to the view**

![Check out this video on adding and customizing resources](image)

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

![Add Resources to Column](image)

   ![Tip](image)

   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 in the Search box.
3. Use the arrow icons next to the columns to move resources between columns.

4. Click Done.

   The view should now be populated with the resources 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.
Add columns

Resources on views are divided into columns. 

On the Customize Page, click Add New Column.

You do not have to add resources here. You can click Done, and drag resources between the columns on the view.

Change column width

To change a column width, position the cursor between the columns and drag the column border to achieve the appropriate width.

Change column width

To change a column width, position the cursor between the columns and drag the column border to achieve the appropriate width.

Move resources on views

To move resources within a column or between columns on a subview, drag the handle at the top of the resource to the new location.

Divide content into subviews

If there is too much information on the view, group and divide resources into subviews.

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.
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.

To save space on the views, click the double arrow button to minimize subviews.

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.

```
Title: Average Response Time
Subtitle: Custom object resource
Choose Object Type: Nodes
```

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.

```
Select a Chart: Average Response Time
Select object: 
Limit Series: 
Show Sum in Data Series: Don't show the sum
Time Period: 
Sample Interval: 
Auto-Hide Resource: 
```

The fields displayed and information required depend upon the object type selected.
Add external website views

You can select any external website and add it to the Orion Web Console as a view.

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:
   \texttt{http://domain\_name}
7. Select the Menu Bar to which you want to add the website link.
   \textcolor{red}{\textbf{Important}}: 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.
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 Enable Drag&Drop / Pause.
2. Drag and drop resources within the selected pane.
3. When you have finished repositioning the resources, click the Settings icon again, and select Disable Drag&Drop / Resume.

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.

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

   You can also open the Customize View page from the view, by clicking Customize Page.
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.

Export views to PDF

The Export to PDF button on dashboards is deprecated as of this release and will be removed in a future release. SolarWinds recommends that you use the Save as PDF functionality built into your browser.
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.

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.

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

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.

Administrative functions

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).

   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.

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.

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
   - Access the product blog
   - Check for maintenance updates
   - Access the ServiceNow® instance you integrated with your SolarWinds Orion server. For information about integrating SolarWinds Orion with ServiceNow, see Integrate an Orion Platform product with ServiceNow.

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.
Manage devices in the Orion Web Console

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

💡 You need node management rights.

Access the Node Management view in two ways:

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

💡 The All Nodes resource is included on the Orion Summary Home view by default, but you can include it on any other view.

Edit node properties

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

💡 You need Node Management Rights.

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

1. Click Settings > Manage Nodes.
2. Locate the node for which you want to edit properties.

💡 To find the node, use the filter and search tools above the nodes list.

3. Select the node, and click Edit Properties.

Edit the node name, web address, and which view opens when you double-click the node

1. To rename the node, type the new name in the Name field. 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.
2. To change the view which displays details about this node, select the View Type from the list.
3. To change the template for the address used in the Node Details resource that allows you to navigate to the node from the resource, scroll down to Web Browse Template, and change the default `http://{{HrefIPAddress}}`.
4. Click Submit.
Edit polling settings

1. To change the polling IP address, type the new IP address, or click Select IP Address and select the new 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 will be 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. If you have high-speed interfaces, and you are experiencing frequent counter rollovers, 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 erratic or incorrect data, clear the box to disable 64-bit counters.

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

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

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

   d. Click Test to test your provided SNMP settings.

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

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

7. Click Submit.

Edit dependencies or custom properties

1. To add, edit, or delete an existing dependency that includes the node, 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.
Add what additional data you want to poll on the node

1. 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.

2. 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.

3. 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.
      
      - Administrator credentials are needed only for installing agents.

   b. Click Test to validate.

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

4. To poll for VMware, select Poll for VMware, provide the vCenter or ESX Server credentials, and click Test.

5. If the node is an F5 device and you want to monitor load balancers, select Poll for i5 Control, and provide the credentials.

6. Click Submit.

Customize alerting thresholds

Be informed when polled values for a metric on the node reach unwanted values by specifying custom thresholds for the node.

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

2. Click Submit.

Suspend collecting data or triggering 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.
The following maintenance options are available:

- **Mute alerts**: data for the node, interfaces, and volumes on the node is 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 is **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.

**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 Now.

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 again.

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, start polling the node again.

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

NPM collects performance and availability data again, 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 - data for the node is collected, but alerts do not trigger.
   - Stop polling the node - data for the node is not collected and alerts do not trigger.
4. Specify the maintenance period, and click Schedule.

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, select the nodes, and click Maintenance Mode > Schedule.

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

You can cancel the maintenance schedule at any time.

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.
To cancel scheduled maintenance from the Manage Nodes view, select the node and click Maintenance Mode > Manage Again or Resume Alerts, according to the maintenance settings.

Poll and rediscover devices immediately

Devices are polled for statistics and status regularly, as specified in the Polling Settings. Discoveries run according to their schedule.

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

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 node or interface you want to poll or rediscover.
4. To poll the selected node or interface, click More Actions > Poll Now.
5. To rediscover the selected node, click More Actions > Rediscover.

Stop monitoring devices

Deleting a node also deletes 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 object, and click Delete.
   - To find a monitored application, interface, or volume, expand the parent node, and select the object.
   - To find a node, use the filter and search tools above the node list.
   - To group found nodes, select a property in the Group By list.
   - To delete multiple interfaces on different nodes, use the search tool above the table to find the nodes, and select the interfaces.
4. Click OK to confirm deletion.

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.

Assign Universal Device Pollers (UnDPs) to monitored devices

SolarWinds NPM provides both a selection of predefined pollers and the Universal Device Poller utility for defining your own pollers to monitor specific aspects of your network devices.

If you do not see a poller that meets your monitoring needs, use the Universal Device Poller to create your own poller. See Monitoring MIBs with Universal Device Pollers.

1. Log in to the Orion Web Console as an administrator.
2. Click Settings > Manage Nodes.
3. Select the node, interface or volume you want to assign Universal Device Pollers to.

   - The list only includes nodes polled through SNMP. If you cannot see a node, check the polling method, and change it to SNMP.

   - See Add a single node for information about adding nodes, interfaces or volumes for monitoring.

4. Click Assign Pollers in the Node Management toolbar.
5. Expand the poller group, and select pollers to be assigned.
6. Click Submit, and click OK to confirm the assignment.

   The selected pollers will now be polled on the node, interface or volume.

Detect and predict possible duplex mismatches

One of the most common causes of performance issues on 10/100 or 100/1000 Mbit Ethernet links occurs when one port on the link operates at half-duplex while the other port operates at full-duplex.

1. Log into the Orion Web Console.
2. Go to the node details view for the parent node of the interface you want to check for duplex problems.
3. Consult the Possible Duplex Mismatches resource. If there are no errors, the resource is hidden.
The resource lists all duplex interfaces on the node, percentage of transmit and receive errors, the neighboring node and interface. If the neighboring interface or node is not monitored, the appropriate columns are empty. The last column displays the duplex mode issue - Mismatch, or Unknown.

**Duplex Mismatch**

To be able to detect duplex mismatches, your nodes need to meet the following requirements:

- The nodes must be monitored by NPM.
- The nodes must be in the up state during the discovery.
- The nodes must support topology and be interconnected.
- Duplex of both devices must be identified as Full or Half.

The resource shows all duplex mismatches, not only 100% duplex mismatches. These are reported on by the Duplex Mismatch alert.

**Possible Duplex Mismatch**

If at least one of the link interfaces has the duplex mode defined as half or full, the resource helps you identify possible mismatch.

Possible duplex mismatches are visible in the duplex mode column as the Unknown duplex mode. They are identified in the following cases:

- If the switch port reports more than 0.5% receive or transmit errors.
- If the switch port reports CRC errors.
- If the switch port reports Late Collision errors.

**How do I resolve mismatches?**

To resolve a duplex mismatch, make sure your hardware is working, and unify the duplex mode configuration on neighboring interfaces.

**Troubleshooting**

**The Possible Duplex Mismatches does not display on Node Details view**

If the resource does not appear on the node details view, there might be a performance issue due to the amount of interfaces and topology connections. Check the following logs for the occurrence of mismatch information:

C:\ProgramData\SolarWinds\Logs\Orion\OrionWeb.log

C:\ProgramData\SolarWinds\InformationService\v3.0\Orion.InformationService.log
The Possible Duplex Mismatches resource does not display percentage of errors

Possible causes:

- No statistical data for these interfaces.
- A performance issue connected with getting statistic information for the resource.

Suspend collecting data for interfaces, or show interface as Unplugged

Monitored interfaces are regularly polled for operational status, and collected statistics are displayed in the Orion Web Console.

Maintenance modes

To temporarily stop collecting data or triggering alerts for interfaces, put the interface or the parent node into a maintenance mode.

1. Go to Manage Nodes, and navigate to the interfaces.
2. Select the interfaces, and select a maintenance mode option:
   - Mute alerts: data for the interface is collected, but alerts do not trigger.
   - Stop collecting data: data for the interface is not collected and alerts do not trigger.
   - Schedule a maintenance period: specify a period of time to stop collecting data or mute alerts for the interface.

   The interface is in maintenance mode according to your settings. For information about resuming alerts, starting collecting statistics, or editing the scheduled maintenance, see the section on Maintenance Mode for nodes.

Set the interface status as Unpluggable

If it is not relevant when an interface is down, you can specify that the interface is "unpluggable", and the interface status will not be reflected in the status of the parent node and in alerts.

1. On the Node Management view, select the interface, and click Edit Properties.
2. Select Display Interface as Unplugged Rather Than Down, and click Submit.

The interface status is not reflected in the status of the parent node and in alerts.

Remotely manage monitored interfaces

Using the Node Management utility, you can shut down or enable interfaces, and override configured EnergyWise power settings remotely.

To remotely manage interfaces, the parent node must have not only Community String, but also Read/Write Community String set correctly. See Edit polling settings.
1. Log in to the Orion Web Console as an administrator.
2. Click Settings > Manage Nodes.
3. Locate the parent node of the interface, and expand the parent node.
   - To find the node, use the filter and search tools above the nodes list.
4. Select the interfaces to manage.
5. To shut down the interfaces, click More Actions > Shut Down, and click OK to confirm.
6. To enable the interfaces, click More Actions > Enable.
7. If the selected interface is EnergyWise-enabled, you can override the current power level setting. Click More Actions > Override Power Level, set the power level, and click OK.
   - Remote overrides are temporary and will be reset in accordance with your configured EnergyWise policy for the selected interface. See Managing EnergyWise interface entity power levels.

Access nodes using HTTP, SSH, and Telnet

The Orion Web Console supports the use of HTTP, SSH, and Telnet protocols for remote device access if associated applications like PuTTY and FiSSH on your Orion server are properly registered.

For more information, search the MSDN online help for "Registering an Application to a URI Scheme".

- To use the remote access applications, web browser integration for the user account must be enabled. Navigate to the user account, and ensure Allow Browser Integration is set to Yes.

Launch remote access applications from any Details view.

Web-based SSH

You can access network devices and servers using SSH through a web-based feature. Through the node details page, locate the Management resource, and click SSH. A web-based terminal launches providing an SSH direct terminal connection. You can use SSH commands to modify device settings and troubleshoot server issues.

The web-based SSH supports all servers with SSH access capable and configured, including Linux hosts, virtual machines, switches, routers, and firewalls.

- The server or network device must be reachable by the Orion server.
Monitor devices in the Orion Web Console

Like all Orion Platform products, SolarWinds NPM offers immediate insight into the performance of your network.

Devices you want to monitor must be added to the SolarWinds Orion database. See Discover and add network devices.

View properties of all monitored nodes and interfaces in the Network Overview

1. Log in to the Orion Web Console, and click My Dashboards > Network > Overview.
2. Select the node property you want to view in the Nodes field, and select the interface property in the Interfaces field.
3. Click Refresh to show the updated overview.

The Network Overview provides a list of monitored nodes and interfaces. The list is sorted alphabetically, and you can select which property you want to see for nodes and interfaces.

Hover over any icon, IP address, or node name to open a tooltip with the current status information about the node or interface.

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, and expand the group including the node to view.
3. Select the node, and click List Resources on the Node Management toolbar.

The interfaces and volumes for this nodes are displayed, showing which are being currently monitored.

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.

### Edit node properties

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

**Info** You need **Node Management Rights**.

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

1. Click Settings > Manage Nodes.
2. Locate the node for which you want to edit properties.

   - To find the node, use the filter and search tools above the nodes list.
3. Select the node, and click Edit Properties.

#### Edit the node name, web address, and which view opens when you double-click the node

1. To rename the node, type the new name in the Name field.
   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.
2. To change the view which displays details about this node, select the View Type from the list.
3. To change the template for the address used in the Node Details resource that allows you to navigate to the node from the resource, scroll down to Web Browse Template, and change the default `http://{{HrefIPAddress}}`.
4. Click Submit.

#### Edit polling settings

1. To change the polling IP address, type the new IP address, or click Select IP Address and select the new IP address.

   **Warning** 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 will be 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. If you have high-speed interfaces, and you are experiencing frequent **counter rollovers**, 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 erratic or incorrect data, clear the box to disable 64-bit counters.

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

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

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

   d. Click Test to test your provided SNMP settings.

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

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

7. Click Submit.

**Edit dependencies or custom properties**

1. To add, edit, or delete an existing dependency that includes the node, 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.
Add what additional data you want to poll on the node

1. 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.

2. 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.

3. 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.
      - Administrator credentials are needed only for installing agents.
   b. Click Test to validate.
   c. Enter the Domain Controller Polling Interval to be used. The default is 30 minutes.

4. To poll for VMware, select Poll for VMware, provide the vCenter or ESX Server credentials, and click Test.

5. If the node is an F5 device and you want to monitor load balancers, select Poll for i5 Control, and provide the credentials.

6. Click Submit.

Customize alerting thresholds

Be informed when polled values for a metric on the node reach unwanted values by specifying custom thresholds for the node.

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

Customize the Manage Nodes view

The Manage Nodes view is the primary view for device management in the Orion Web Console.

Find the node or interface you want to manage, select it, and use the management functions in the toolbar.

You can manage more nodes or interfaces at the same time.

- To select all items in the table, select the box to the left of the Name column.
Search for devices

1. Type a search string into the Search field above the results table, and click Search.
   - The search is only performed on properties displayed in the table.
   To add a property, click >> at the far right of the title row of the table, and select system or custom properties which should be displayed and searched.

   If you are looking for interfaces, consider selecting Interfaces next to the Search field.

2. If the list of found devices is too long, select a Group By option in the left section, and select a group. Nodes in the group display in the results table.
   - The Group By list includes custom properties.

3. If you see a parent object in the table, expand it, and select the node or interface which you want to edit.

Suspend collecting data or triggering 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.

The following maintenance options are available:

- **Mute alerts**: data for the node, interfaces, and volumes on the node is 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 is 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.

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 Now.

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 again.

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, start polling the node again.

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

NPM collects performance and availability data again, 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 - data for the node is collected, but alerts do not trigger.
   - Stop polling the node - data for the node is **not** collected and alerts do not trigger.
4. Specify the maintenance period, and click Schedule.
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.

   ![Image]

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

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

You can cancel the maintenance schedule at any time.

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

   ![Image]

   The scheduled maintenance is canceled.

   ![Image]

   To cancel scheduled maintenance from the Manage Nodes view, select the node and click Maintenance Mode > Manage Again or Resume Alerts, according to the maintenance settings.

Poll and rediscover devices immediately

Devices are polled for statistics and status regularly, as specified in the Polling Settings. Discoveries run according to their schedule.

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

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 node or interface you want to poll or rediscover.
4. To poll the selected node or interface, click More Actions > Poll Now.
5. To rediscover the selected node, click More Actions > Rediscover.

Stop monitoring devices

Deleting a node also deletes 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 object, and click Delete.

   - To find a monitored application, interface, or volume, expand the parent node, and select the object.
   - To find a node, use the filter and search tools above the node list.
   - To group found nodes, select a property in the Group By list.

4. Click OK to confirm deletion.

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.
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

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.

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

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

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

11. For SNMPv3, provide the credentials and click Test to validate the credentials. See the vendor documentation for your network device for further information.
12. Click Submit.
Promoting a Node from ICMP to WMI Monitoring

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.

Access nodes using HTTP, SSH, and Telnet

The Orion Web Console supports the use of HTTP, SSH, and Telnet protocols for remote device access if associated applications like PuTTy and FiSSH on your Orion server are properly registered.

For more information, search the MSDN online help for "Registering an Application to a URI Scheme".

To use the remote access applications, web browser integration for the user account must be enabled. Navigate to the user account, and ensure Allow Browser Integration is set to Yes.
Launch remote access applications from any Details view.

**Web-based SSH**

You can access network devices and servers using SSH through a web-based feature. Through the node details page, locate the Management resource, and click SSH. A web-based terminal launches providing an SSH direct terminal connection. You can use SSH commands to modify device settings and troubleshoot server issues.

The web-based SSH supports all servers with SSH access capable and configured, including Linux hosts, virtual machines, switches, routers, and firewalls.

- The server or network device must be reachable by the Orion server.

**Managing Groups and Dependencies**

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

**Managing Groups**

Groups contain Orion Platform objects that report a status such as nodes, volumes, applications, interfaces, ports, and even other groups. You create, delete, and modify groups from the Manage Groups page.

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

To access the Manage Groups page:

1. Log on to the Orion Web Console.
2. Click Settings in the top right of the web console.
3. Click Manage Groups in the Node & Group Management grouping of the Orion Website Administration page.

The following sections provide more information about creating and managing groups in Orion Platform:

- [Creating Groups](#)
- [Editing Existing Groups](#)
- [Managing Group Members](#)
- [Deleting Groups](#)
- [Managing the Display of Group Status](#)
Creating Groups

Creating a group is a straightforward process of selecting the Orion objects you want the group to contain. At creation time, you can also decide how you want SolarWinds to roll up the status of the group members.

It is also possible to specify group members on the basis of shared properties by adding them with a dynamic query. Orion Platform objects added through dynamic queries are automatically added or removed from the group.

To create a new group:

1. Click Start > All Programs > SolarWinds > Orion Web Console.
2. Click Settings in the top right of the web console.
3. Click Manage Groups in the Node & Group Management grouping of the Orion Website Administration page.
4. Click Add New Group.
5. Enter a name for the group in the Name field, and then expand Advanced.
6. If you want the group to roll up the worst status of the group members, select Show Worst Status.
7. If you want the group to roll up the best status of the group members, select Show Best Status.
8. If you want the group to display a warning status if the group members have a mixture of different statuses, select Mixed Status shows warning.
9. Click Next.
10. If you want to individually select group members, follow these steps:
    a. In the Show Only list, select the type of Orion Platform object you want to add as a group member.
    b. Check the checkbox of the Orion Platform object and then click Add to Group.
11. If you want to dynamically select group members based on shared properties, follow these steps:
    a. Click Add dynamic query.
    b. Type a name for the query in the Dynamic query object name field.
    c. Select an Orion Platform object type in the Orion Object is list.
    d. Click Add Condition to specify further selection properties.
    e. Click Preview to verify that the dynamic query is selecting your intended objects.
    f. Click Save.
12. Continue adding individual Orion Platform objects or dynamic queries until you have finished building your group.
13. Click Create Group.
Editing Existing Groups

You can edit the properties of an existing group or add and remove objects. These are separate editing tasks.

To edit properties of an existing group:

1. Click Start > All Programs > SolarWinds > Orion Web Console.
2. Click Settings in the top right of the web console.
3. Click Manage Groups in the Node & Group Management grouping of the Orion Website Administration page.
4. Check the group you want to edit, and then click Edit Properties.
5. Edit the Name and Description of the selected group, as appropriate.
6. If you want to manage the members of the selected group, click Add & Remove Objects. For more information about managing group members, see Managing Group Members.
   ▪ Expand the Contains summary for the selected group to see all member objects in the group.
7. If you want to configure the calculation of displayed group status or the frequency with which group status is refreshed, expand Advanced, select a Status rollup mode, and then provide a Refresh frequency.
   ▪ For more information about status rollup for groups, see Managing the Display of Group Status.
8. Click Submit.

Managing Group Members

The following procedure manages the objects included within a defined group.

1. Click Start > All Programs > SolarWinds > Orion Web Console.
2. Click Settings in the top right of the web console, and then click Manage Groups in the Node & Group Management grouping of the Orion Website Administration page.
3. Check the group you want to edit, and then click Add & Remove Objects.

Deleting Groups

Complete the following steps to delete an existing group.

1. Click Start > All Programs > SolarWinds > Orion Web Console.
2. Click Settings in the top right of the web console, and then click Manage Groups in the Node & Group Management grouping of the Orion Website Administration page.
3. Check the group you want to delete, and then click Delete.
Managing the Display of Group Status

The status of any particular group is determined by the status of the members of the group. There are three methods for determining the status displayed for a selected group of monitored objects:

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

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

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

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

- **Mixed Status** shows Warning ensures that the status of a group displays the worst warning-type state in the group. If there are no warning-type states, but the group contains a mix of up and down states, then a Mixed Availability (⚠️) warning status is displayed for the whole group. The following table indicates how the Mixed Status shows Warning option operates:

<table>
<thead>
<tr>
<th>Object States</th>
<th>Group Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>![Critical]</td>
<td>![Critical]</td>
</tr>
<tr>
<td>![Critical]</td>
<td>![Critical]</td>
</tr>
<tr>
<td>![Mixed Availability]</td>
<td>![Mixed Availability]</td>
</tr>
</tbody>
</table>

The following procedure configures the method used to determine group status.

1. Click Start > All Programs > SolarWinds > Orion Web Console.
2. Click Settings in the top right of the web console, and then click Manage Groups in the Node & Group Management grouping of the Orion Website Administration page.
3. Check the group you want to edit, and then click Edit Properties.
4. Expand Advanced, and then select a Status rollup mode, as follows:
   a. If you want the group to roll up the worst status of the group members, select Show Worst Status.
   b. If you want the group to roll up the best status of the group members, select Show Best Status.
   c. If you want the group to display a warning status if the group members have a mixture of different statuses, select Mixed Status shows warning.
5. Click Submit.

Managing Dependencies

Dependencies in Orion Platform allow you to account for topological constraints on your network. These constraints may be either the result of the design of a specific device, as in the case of interfaces on a switch or router, or the result of the physical architecture of your network itself. Orion Platform offers an Unreachable status to account for the case when a device may appear to be down when its status is actually indeterminate, due to another device being down or unresponsive.

For example, in the case of a typical switch monitored by SolarWinds NPM, when the switch itself goes down or becomes unresponsive, all interfaces on the switch will also be unresponsive, even though they may functioning perfectly well. By default, in SolarWinds NPM these child interfaces display as Unreachable because their parent node is reporting as down.

Likewise, Orion Platform also makes it possible to define dependencies among distinct devices, as in the case of a subnet of devices on your network that depends on a single WAN link to connect with the rest of your network. In this case, if you have defined a group consisting of the devices in this dependent subnet, you can then define a dependency where the dependent subnet is a child group to the parent router that is serving as the WAN link to the rest of your network. For more information about groups, see Managing Groups.

The power of dependencies becomes evident when considering alerts. If you have an alert configured to trigger when a monitored object is down, you only want that alert to trigger if a monitored objects is positively down. In other words, you do not want an down object alert to trigger for an object that is not actually down. Without dependencies, all monitored objects on a monitored node that is unresponsive to ICMP queries will also report as down. With dependencies in use, these child objects will instead display as Unreachable, saving you the hassle of sorting through numerous false alerts resulting from the failure of a single node to respond promptly to a status query.

> Interfaces may be defined as parent objects, but they cannot be defined as child objects. SolarWinds NPM determines interface status directly by polling parent nodes. If the node on which an interface exists goes down, SolarWinds NPM automatically reports any and all interfaces on that node as unreachable.
Creating a New Dependency

Creating a new dependency is a straightforward process of selecting the parent and children objects, as shown in the following procedure.

1. Click Start > All Programs > SolarWinds > Orion Web Console.
2. Click Settings in the top right of the web console, and then click Manage Dependencies in the Node & Group Management grouping of the Orion Website Administration page.
3. Click Add new dependency.
4. On the Select Parent page, complete the following steps:
   a. Use the Show only: and Group by: selection fields to customize the list of displayed objects and groups.
   i. The properties listed in the Group by selection field are dynamic.
   b. Select the parent object or group in the main pane, and then click Next.
   i. If you want to define a dependency so that the reported states of child objects are dependent on the status of multiple parent objects, create a group including all parent objects, and then select it on this view. For more information, see Creating Groups.
5. On the Choose Child page, complete the following steps:
   a. Edit the Dependency name, as appropriate.
   b. Use the Show only: and Group by: selection fields to customize the list of displayed objects and groups.
   i. Properties listed in the Group by: selection field are dynamically dependent on the selection in the Show only: field.
   c. Select the child object or group in the main pane, and then click Next.
   i. If you want to define a dependency so that the reported states of multiple child objects are dependent on the status one or more parent objects, create a group including all child objects, and then select it on this view. For more information, see Creating Groups.
6. On the Review Dependency view, review the current settings for the configured dependency.
   Notes:
   • If any advanced alerts are configured on parent or child objects, they will be listed on this view. Click + to expand alert details.
   • In the event that a parent object is down, all alerts configured on any child objects in a dependency on the down parent object are automatically suppressed.
7. Click Submit to accept the dependency definition.
Editing an Existing Dependency

Editing an existing dependency is a straightforward process, as shown in the following procedure.

1. Click Start > All Programs > SolarWinds > Orion Web Console.
2. Click Settings in the top right of the web console, and then click Manage Dependencies in the Node & Group Management grouping of the Orion Website Administration page.
3. Check the dependency you want to edit, and then click Edit.
4. On the Select Parent page, complete the following steps:
   a. Use the Show only: and Group by: selection fields to customize the list of displayed objects and groups.
      
      Properties listed in the Group by: selection field are dynamically dependent on the selection in the Show only: field.

   b. Select the parent object or group in the main pane, and then click Next.
      
      If you want to define a dependency so that the reported states of child objects are dependent on the status of multiple parent objects, create a group including all parent objects, and then select it on this view. For more information, see Creating Groups.

5. On the Choose Child page, complete the following steps:
   a. Edit the Dependency name, as appropriate.
   b. Use the Show only: and Group by: selection fields to customize the list of displayed objects and groups.
      
      Properties listed in the Group by: selection field are dynamically dependent on the selection in the Show only: field.

   c. Select the child object or group in the main pane, and then click Next.
      
      If you want to define a dependency so that the reported states of multiple child objects are dependent on the status one or more parent objects, create a group including all child objects, and then select it on this view. For more information, see Creating Groups.

6. On the Review Dependency view, review the current settings for the configured dependency.
   Notes:
   
   • If any advanced alerts are configured on parent or child objects, they will be listed on this view. Click + to expand alert details.
   • If a parent object is down, all alerts configured on any child objects in a dependency on the down parent object are automatically suppressed.
7. Click Submit to accept the dependency definition.

Deleting an Existing Dependency

Deleting an existing dependency is a straightforward process, as shown in the following procedure.
1. Click Start > All Programs > SolarWinds > Orion Web Console.
2. Click Settings in the top right of the web console, and then click Manage Dependencies in the Node & Group Management grouping of the Orion Website Administration page.
3. Check the dependency you want to delete, and then click Delete.
4. Click Yes to confirm deletion of the selected dependency.

Viewing Alerts on Child Objects

In the event that a parent object is down, all advanced alerts configured on any child objects in a dependency on the down parent object are automatically suppressed. The following procedure displays all advanced alerts currently configured on any child objects in a selected dependency.

1. Click Start > All Programs > SolarWinds > Orion Web Console.
2. Click Settings in the top right of the web console.
3. Click Manage Dependencies in the Node & Group Management grouping of the Orion Website Administration page.
4. Check the dependency that includes the child object on which the alerts you want to view are configured, and then click Alerts on Child.

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.

<table>
<thead>
<tr>
<th>PORT</th>
<th>PROTOCOL</th>
<th>SERVICE/PROCESS</th>
<th>DIRECTION</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>1433</td>
<td>TCP</td>
<td>SolarWinds Collector Service</td>
<td>Outbound</td>
<td>The port used for communication between the APE and the Orion database.</td>
</tr>
<tr>
<td>1801</td>
<td>TCP</td>
<td>Message Queuing</td>
<td>Inbound</td>
<td>The port used for MSMQ messaging from the Orion Web Console to the Additional</td>
</tr>
<tr>
<td>Port</td>
<td>Protocol</td>
<td>Service/Process</td>
<td>Direction</td>
<td>Description</td>
</tr>
<tr>
<td>------</td>
<td>----------</td>
<td>-----------------</td>
<td>-----------</td>
<td>-------------</td>
</tr>
<tr>
<td>5671</td>
<td>TCP</td>
<td>RabbitMQ</td>
<td>Bidirectional</td>
<td>The port used for SSL-encrypted RabbitMQ messaging from the Orion Web Console to the Additional Polling Engine.</td>
</tr>
<tr>
<td>17777</td>
<td>TCP</td>
<td>SolarWinds Information Service</td>
<td>Bidirectional</td>
<td>The port used for communication between the Additional Polling Engine and the Orion Web Console.</td>
</tr>
</tbody>
</table>

Install an Additional Polling Engine

1. Click Settings > All Settings > Polling Engines.
2. Click Download Installer Now.
3. Run the installer on the computer you want to use as your additional polling engine or website.
4. Enter the main Orion server credentials.
5. Choose either Additional Polling Engine or Additional Website. If you want to install a backup server for High Availability, view SolarWinds High Availability requirements first. The packages are downloaded from the main Orion server.
6. Follow the onscreen instructions to complete your installation and configuration.

The Additional Polling Engine or Additional Web Server is installed, together with all hotfixes for products released later than September 2016.

For example, when installing or upgrading to SAM 6.3 and IPAM 4.3.2, any hotfixes for SAM 6.3 are installed. You must install the hotfix for IPAM manually.

Repeat installing on all Additional Polling Engines and then on all Additional Web Servers in your environment.

Activate the Additional Polling Engine licenses

1. In the Orion Web Console, click Settings > All Settings > License Manager.
2. Locate the license in the License Manager, click Activate, and complete the activation.

The Additional Polling Engine license is activated. Review the polling engine it is assigned to, and re-assign the license if necessary.

When finished, specify nodes to be polled by the Additional Polling Engine.
Use an Additional Web Server

With an Additional Web Server, you can access the Orion Web Console remotely, from a location other than your primary Orion server. You can view the primary Orion Web Console without deploying an entire Orion installation or excessively taxing the resources of your primary SolarWinds server.

Requirements

- Matching version of Additional Web Server and your product installed on the main polling engine
- 64-bit operating system:
  - Windows Server 2008 R2 SP1 or
  - Windows Server 2012 and 2012 R2
  - Windows Server 2016
- Matching version of .NET 4.5 installed on the main polling engine
- Minimum hardware requirements
  - CPU speed: Quad core processor, 2.5 GHz or better
  - Hard drive space: 2.5 GB minimum
  - Memory: 4 GB minimum, 8 GB recommended

A higher number of concurrent users may change the requirements.

Port requirements

<table>
<thead>
<tr>
<th>PORT</th>
<th>PROTOCOL</th>
<th>SERVICE /PROCESS</th>
<th>DIRECTION</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>80</td>
<td>TCP</td>
<td>World Wide Web Publishing Service</td>
<td>Inbound</td>
<td>Default additional web server port. Open the port to enable communication from your computers to the Orion Web Console. If you specify any port other than 80, you must include that port in the URL used to access the web console. For example, if you specify an IP address of 192.168.0.3 and port 8080, the URL used to access the web console is <a href="http://192.168.0.3:8080">http://192.168.0.3:8080</a>.</td>
</tr>
<tr>
<td>1433</td>
<td>TCP</td>
<td>SolarWinds Collector Service</td>
<td>Outbound</td>
<td>The port used for communication between the SolarWinds server and the SQL Server. Open the port from your Orion Web Console to the SQL Server.</td>
</tr>
<tr>
<td>1801</td>
<td>TCP</td>
<td>Message queuing</td>
<td>Outbound</td>
<td>The port used for MSMQ messaging from the Additional Web Server to the Main Polling Engine.</td>
</tr>
<tr>
<td>5671</td>
<td>TCP</td>
<td>RabbitMQ</td>
<td>Outbound</td>
<td>The port used for SSL-encrypted RabbitMQ messaging from</td>
</tr>
</tbody>
</table>
Before you begin, prepare:

- Hostname or IP address of your main polling engine
- Orion Web Console user name and password with administrative rights
- To use SQL authentication, prepare the SQL server credentials
- SQL database name

Download and install an Additional Web Server

1. In the main Orion Web Console, click Settings > All Settings > Web Console Settings.
2. Click Download Installer Now.
3. Run the installer on the computer you want to use as your Additional Web Server.
4. Enter the main Orion server Orion server credentials.
5. Choose Additional Website.
   The packages are downloaded from the main Orion server.
6. Follow the onscreen instructions to complete your installation.

Configure the Additional Web Server

1. If the Configuration Wizard does not start automatically, click Start > All Programs > SolarWinds Orion > Configuration and Auto-Discovery > Configuration Wizard.
2. Click Next on the Welcome tab of the Configuration Wizard.
3. Select or type the SQL Server used by your primary Orion server.
4. If you are using Windows NT Integrated Security, select Use Windows Authentication, and click Next.
5. If you are using a SQL Server login and password, complete the following steps:
   a. Select Use SQL Server Authentication.
   b. Provide your Login and Password, and click Next.
6. Select or type the Database Name that is connected to your Orion server, and click Next.
7. If a dialog appears that says that multiple polling engines have been detected, click OK to continue database upgrade/verification.
8. When the database structure validation completes, click Next.
9. Specify a SQL account User Name and Password for the polling engine and web site to use to access the database, and click Continue.

   - If you already have a SQL account, you can specify the credentials for that account.

10. To set up the web console, click Next on the Create Website tab, and then complete the following procedure:

   a. Specify the IP Address of the local server on which you are installing the new web-only interface.

   b. Specify the TCP Port through which you want to access the web console.

      - If you specify any port other than 80, you must specify that port in the URL that is used to access the web console. For example, if you specify an IP address of 192.168.0.3 and port 8080, your URL is http://192.168.0.3:8080.

   c. Specify the volume and folder in which you want to install the web console files, and then click Continue.

11. If you are asked to overwrite an existing website, click Yes.

12. When the new web console has been created, click Continue.

You can now use the additional Orion Web Console to access your Orion Platform product.

Activate your license

- To evaluate an Additional Web Server, just install it.
- To activate a production license for an Additional Web Server, log in to the Orion Web Console on your main polling engine, and activate the license.

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.

- Depending on the Orion Platform products you have installed, additional polling settings may be available. See your SolarWinds Orion Administrator Guide for more information about the settings.

Configure polling interval settings

- 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 Interface Poll Interval (SolarWinds NPM)**

The interval for polling the status and response time of monitored interfaces. By default, this interval is 120 seconds. Available only if SolarWinds NPM is installed.

**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.

Interface Baseline Calculation Frequency

Specify how often the interface baseline calculation runs.

Detailed Interface Availability Statistics Retention

Specify the number of days until the detailed interface availability statistics in the SolarWinds Orion database are summarized into hourly statistics. By default, this period is seven days.

Hourly Interface Availability Statistics Retention

Specify the number of days until the hourly interface availability statistics are summarized into daily statistics. By default, this period is 30 days.

Daily Interface Availability Statistics Retention

Specify the number of days until the daily interface availability statistics are deleted from the database. By default, this period is 365 days.

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.

Detailed UnDP Statistics Retention

Specify the number of days until the detailed UnDP statistics are summarized into hourly statistics.

Hourly UnDP Statistics Retention

Specify the number of days until the hourly UnDP statistics are summarized into daily statistics.

Daily UnDP Statistics Retention

Specify the number of days until the daily UnDP statistics are deleted from the database.

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.

ℹ️ 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.

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 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.

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.

   Specify your own custom values for Maximum, CurrentValue, and DefaultValue.

   INSERT INTO [OrionDatabaseName].[dbo].[Settings] (SettingID, Name, Description, Units, Minimum, Maximum, CurrentValue, DefaultValue) VALUES ('SWNetPerfMon-Settings-Response Time Retry Count', 'Response Time Retry Count', 'Number of times Orion retries ICMP pings on a monitored device before reporting packet loss', '', 1, Maximum, CurrentValue, DefaultValue)

5. To start the Orion Service Manager, click SolarWinds Orion > Advanced Features program folder.
6. Click Start Everything.

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.

- **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.

- **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.
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.
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.

**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.

![Database Manager screenshot](image)

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.

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.

   You can also adjust retention periods for other statistics.

   ![Table of retention periods]

   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.

**Edit database fields**

You can edit database fields in the Database Manager. We do not recommend changing values directly in the database unless clearly directed to do so by Support or as completed by a DBA. As you make changes and capture data through the Orion Web Console, this data saves safely to the database.

`Table editing should only be performed by a database administrator (DBA) or other expert user. Changes made directly in your database can jeopardize the integrity of your data. SolarWinds recommends that you change database settings and values using the Settings with your Orion Web Console.`

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. See [Add a server to Database Manager](#).
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. Right-click a table, and click Table Details.
5. 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 edit the data in a table, click Enable Table Editing, and edit the fields in the table.

**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.

**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.

a. Edit the Property Name and Description fields.

- Property names are not case-sensitive, and must be unique for each object type. For example, you can have separate Comment properties for Nodes, Volumes, and other object types.

b. Select the Format for the property.

- We recommend that you limit the string length for text properties. The string length can affect SQL performance, especially when custom properties are used in limitations. The shorter the string length, the faster the queries.

To limit the string length, click Edit, and provide the maximum number of characters.

```plaintext
Format: Text
```

To limit the string length, click Edit, and provide the maximum number of characters.

- Restricting values helps to maintain the consistency of values for individual custom properties.

c. Create a drop-down menu with specific values for the property by selecting Restrict values, and adding the values.

- Restricting values helps to maintain the consistency of values for individual custom properties.

d. If you want to limit how the custom property for nodes should be used, clear boxes in the Usage section.

- When you select a Usage option, you cannot clear the option after you submit the custom property. This prevents you for example from disabling a custom property for reports in case it is already used in a report.

- Alerts: the custom property is offered only in alerts.
- Filtering: the custom property is offered when adding Filter Properties in AppStack Environment.
- Grouping: the custom property is offered in Group by drop-down lists.
- Reports: the custom property is offered when designing the layout for web-based reports.
- Object Details Views: the custom property appears in the Custom Properties [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.

   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.

<table>
<thead>
<tr>
<th>SPREADSHEET COLUMN</th>
<th>ORION DATABASE COLUMN</th>
</tr>
</thead>
<tbody>
<tr>
<td>Caption</td>
<td>Caption</td>
</tr>
<tr>
<td>IP Address</td>
<td>IP_Address</td>
</tr>
</tbody>
</table>

   - Select Imports To to import the data in the spreadsheet column to the selected SolarWinds Orion database column.

     ![Select Imports To Image]

     This option overwrites any existing data in the corresponding custom properties.

     ![Select Imports To Options Image]

   - 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.

   ![Export Custom Property Data Image]

   You can only select custom properties for a single object type.

1. Log in to the Orion Web Console as an administrator.
2. Click Settings > All Settings in the menu bar.
3. In the Node & Group Management grouping, click Manage Custom Properties.
4. Select the custom properties you want to export, and click Export Values. You can Filter objects to find the custom properties more easily.
5. To export custom property data for specific objects, click Select <Objects>, and select the objects.
6. Select the database columns you want to export. You can also change which custom properties you want to export.
7. Select the file type for the exported data. This can be .csv, .txt, .html or xls.
8. Click Export.
The exported file is downloaded to your browser's default download location.

**Change custom properties values**

You can change the value of a custom property from the Manage Custom Properties page or bulk edit the values of a custom property assigned to objects.

- You can only edit properties of one object type at a time.

**Edit values for custom properties**

When you are entering a large amount of data, it can be easier to [import the values from a spreadsheet](#).

1. Log in to the Orion Web Console as an administrator.
2. Click Settings > All Settings in the menu bar.
3. In the Node & Group Management grouping, click Manage Custom Properties.
4. Select the custom properties, and click View / Edit Values. You can [filter objects](#) to find the custom properties more easily.
5. To add or change a value for a property, enter the value into the field.
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.

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.

<table>
<thead>
<tr>
<th>TASK</th>
<th>ACCESS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add and edit user accounts and reset passwords.</td>
<td>Allow Administrator Rights</td>
</tr>
<tr>
<td><strong>TASK</strong></td>
<td><strong>ACCESS</strong></td>
</tr>
<tr>
<td>------------------------------------------------------------------------</td>
<td>---------------------------------------------------------------------------</td>
</tr>
<tr>
<td>SolarWinds recommends that you do not allow users to change their own Orion Web Console account passwords.</td>
<td></td>
</tr>
<tr>
<td>Add, edit, and delete nodes.</td>
<td>Allow Node Management Rights</td>
</tr>
<tr>
<td>Enable/disable monitoring elements.</td>
<td>Allow Account to Unmanage Objects</td>
</tr>
<tr>
<td>Add, edit, schedule, and delete reports.</td>
<td>Allow Report Management Rights</td>
</tr>
<tr>
<td>Add, edit, and delete alerts.</td>
<td>Allow Alert Management Rights</td>
</tr>
<tr>
<td></td>
<td>To only allow some actions, keep No in Allow Alert Management rights and Allow items in the Alerts section as appropriate.</td>
</tr>
<tr>
<td>Customise views.</td>
<td>Allow Account to Customize Views</td>
</tr>
<tr>
<td>Access only a set of devices (type, location, department, and so on).</td>
<td>Click Add Limitation and define the limitation.</td>
</tr>
</tbody>
</table>

---

*SolarWinds does not recommend enabling Alert Management Rights when a user account is set to expire. When the account expires, any alert the account created will behave erratically.*
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]

3. Select Orion individual account, and click Next.

![I would like to create:]

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.

```
Add New Account

I would like to create:

- Orion individual account
  Add a new SQL-based account. Learn more

- Windows individual account
  Add existing Active Directory or local accounts to Orion. Learn more

- Windows group account
  Add existing Active Directory or local group accounts to Orion. Learn more
```

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.

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.

   ![Note] 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>1. Disabling an account does not delete it. Account definitions and details are stored in the SolarWinds Orion database and can be enabled later.</td>
</tr>
<tr>
<td></td>
<td>2. When you disable an account that was used to create alerts, the alerts' Owner field is permanently cleared, but the alerts operate as normal.</td>
</tr>
<tr>
<td>Should the user be able to log in only temporarily?</td>
<td>Specify the expiration date.</td>
</tr>
<tr>
<td>Should the user be logged in indefinitely even if the browser is closed?</td>
<td>Select Yes for the Disable Session Timeout option. Session timeouts are global and set in Web Console Settings. By default, new user 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>
<tbody>
<tr>
<td>Add and edit user accounts and reset passwords.</td>
<td>Allow Administrator Rights Granting administrator rights does not assign the Admin menu bar to a user. For more information, see Set default menu bars and views for users.</td>
</tr>
<tr>
<td></td>
<td>SolarWinds recommends that you do not allow users to change their own Orion Web Console account passwords.</td>
</tr>
<tr>
<td>Add, edit, and delete nodes.</td>
<td>Allow Node Management Rights</td>
</tr>
<tr>
<td>Create, edit, and delete maps in the Network Atlas.</td>
<td>Allow Map Management Rights</td>
</tr>
<tr>
<td>Add, edit, schedule, and delete reports.</td>
<td>Allow Report Management Rights To only allow access to some reports, select the report category the user can access.</td>
</tr>
<tr>
<td>Add, edit, and delete alerts.</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>SolarWinds does not recommend enabling Alert Management Rights when a user account is set to expire. When the account expires, any alert the account created will behave erratically.</td>
</tr>
<tr>
<td>Customize views.</td>
<td>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.</td>
</tr>
<tr>
<td>Enable/disable monitoring elements.</td>
<td>Allow Account to Unmanage Objects</td>
</tr>
<tr>
<td>Acknowledge and clear events, advanced alerts, and Syslogs.</td>
<td>Allow Account to Clear Events, Acknowledge Alerts and Syslogs.</td>
</tr>
</tbody>
</table>
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.

   DEFAULT MENU BAR AND VIEWS

   Select the menu bar for this account. To view the contents of each

   HomeTab Menu Bar       New York  
   NetworkTab Menu Bar     Network_TabMenu  

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. For greater flexibility, you can create your own account limitations in the Account Limitation Builder, based on custom properties.

**Restrict user access to network areas by applying limitations**

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

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

*Pattern limitations can have a negative impact on performance and are error prone.*
If the default limitations are not enough, you can create limitations based on custom properties, and apply them on user accounts.

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

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

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

Patterns for limitations

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

Patterns are not case sensitive.

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

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

Create limitations based on custom properties

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

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

1. Click Start > All Programs > SolarWinds Orion > Grouping and Access Control > Account Limitation Builder.
2. Click Start on the splash screen.
3. Click Add Limitation.
4. Select a Custom Property. The fields are populated automatically based on your selection.
5. Choose a Selection Method.
   - This is the selection format that will appear when you are choosing values for the account limitation in the Orion Web Console.
   - Pattern matching is the most powerful selection, but it is also the selection most prone to errors when restricting access and impacts performance.
6. Click OK.

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

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.

- This procedure requires access to the computer that hosts the Orion server.

1. Start the Account Limitation Builder in the SolarWinds Orion > Grouping and Access Control program folder.
2. Click Start on the splash screen.
3. Click the row of the limitation that you want to delete.
   - Use <Shift+Click> to highlight multiple consecutive rows or <Ctrl+Click> to highlight multiple non-consecutive rows.
4. Click Edit > Delete Selected Limitations.

The limitation is now unavailable for limiting user accounts in the Orion Web Console.

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.

- 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 (NTSF) or share drive. Download it for free from here: http://www.solarwinds.com/products/freetools/permissions_analyzer_for_active_directory/

Authenticate users through MSAPI

1. Enable the Orion Web Console to use automatic Windows Authentication.
   a. Start the Configuration Wizard in the SolarWinds Orion > Configuration and Auto-Discovery program folder.
   b. Select Website, and click Next.
c. Provide the appropriate IP Address, Port, and Website Root Directory, and select Yes - Enable Automatic Login Using Windows Authentication.

d. Click Next, and complete the Configuration Wizard.

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>
<tr>
<td>Scenario</td>
<td>Web Console Login Supported?</td>
<td>Local Login Required?</td>
<td>Network Atlas and Unmanage Utility Login Supported?</td>
</tr>
<tr>
<td>-------------------------------------------------------------------------</td>
<td>------------------------------</td>
<td>-----------------------</td>
<td>-----------------------------------------------------</td>
</tr>
<tr>
<td>Login with trusted domain AD user</td>
<td>No</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Login with trusted domain AD Group User</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Login with &quot;Orion Server&quot; domain Group AD account (group user belongs to trusted domain)¹</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Login with trusted domain Group AD account (group user belongs to &quot;Orion Server&quot; domain)²</td>
<td>No</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Login with AD user or Group user from a foreign AD forest</td>
<td>Yes, when LDAP is enabled</td>
<td>No, without an Additional Website³</td>
<td></td>
</tr>
</tbody>
</table>

Enable LogonFallback

LogonFallback must be enabled when the Active Directory user of the Orion Web Console does not have local login rights to the web server.

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

Log in 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.

```
```

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.

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

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

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

Delete groups

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

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

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

<table>
<thead>
<tr>
<th>OBJECT STATES</th>
<th>GROUP STATUS</th>
</tr>
</thead>
<tbody>
<tr>
<td>(Up, Warning, Down)</td>
<td>(Up)</td>
</tr>
<tr>
<td>(Up, Down)</td>
<td>(Up)</td>
</tr>
<tr>
<td>(Warning, Down, Unknown)</td>
<td>(Warning)</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>OBJECT STATES</th>
<th>GROUP STATUS</th>
</tr>
</thead>
<tbody>
<tr>
<td>(Up, Warning, Down)</td>
<td>(Down)</td>
</tr>
<tr>
<td>(Warning, Up)</td>
<td>(Warning)</td>
</tr>
<tr>
<td>(Warning, Down, Unknown)</td>
<td>(Down)</td>
</tr>
</tbody>
</table>

The Mixed Status Shows Warning selection ensures that the status of a group displays the worst warning-type state in the group. If there are no warning-type states, but the group contains a mix of up and down states, then a Mixed Availability (●) warning status is displayed for the whole group.

<table>
<thead>
<tr>
<th>OBJECT STATES</th>
<th>GROUP STATUS</th>
</tr>
</thead>
<tbody>
<tr>
<td>! ●</td>
<td>(Critical)</td>
</tr>
<tr>
<td>! ● ●</td>
<td>(Critical)</td>
</tr>
<tr>
<td>● ●</td>
<td>(Mixed Availability)</td>
</tr>
</tbody>
</table>
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.
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. Type a Dependency Name, select the child entities, and click Next.

<table>
<thead>
<tr>
<th>Dependency name:</th>
<th>New York IT Department Router</th>
</tr>
</thead>
<tbody>
<tr>
<td>Parent:</td>
<td>HQDC-3750-CORE</td>
</tr>
</tbody>
</table>

**SHOW ONLY:**
- Groups

**GROUP BY:**
- [No Grouping]

<table>
<thead>
<tr>
<th>Display Name</th>
<th>New York IT Department</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>HQDC-3750-CORE</td>
</tr>
</tbody>
</table>

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

ℹ️ 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.

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.

**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 it 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 host name](#) to route incoming requests and messages to the current, active server. All single subnet HA pools must use a VIP.

![Diagram of High Availability setup](image)
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 attempts to restart the service. If the service goes down a second time within a set amount of time, 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 primary server, including receiving syslogs, SNMP traps, and NetFlow information through the VIP or virtual host name. You can manually failover to your primary server to return it to active service.

Multiple subnets (WAN)

When you configure your environment for SolarWinds High Availability over a WAN (Disaster Recovery), place your secondary server on a different subnet in the same DNS zone. 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 host name to route incoming requests and messages to the current, active server. You can have only two servers in a pool.
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 host name. You can manually failover to your primary server to return it to active service.

When do I use a VIP or a virtual host name?

Use a VIP to reference your protected servers when you are protecting a server on a single subnet. Use a virtual host name either on a single subnet or across multiple subnets.

<table>
<thead>
<tr>
<th></th>
<th>SINGLE SUBNET</th>
<th>MULTIPLE SUBNETS</th>
</tr>
</thead>
<tbody>
<tr>
<td>VIP</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Virtual host name</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.

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 host name?

A virtual host name is shared by both members of the HA pool. Only the active member of the HA pool responds to the virtual host name. Use a virtual host name to connect to your Orion server or additional polling engine HA pools when they span two different subnets.

You can use a virtual host name when configuring an HA pool on a single subnet or over two subnets.

How do I choose a virtual host name?

You can create a new virtual host name on the fly when you create an HA pool or create a virtual host name before creating your HA pool.

While you can use your original Orion server’s host name as the virtual host name, this is not recommended. This method requires the same steps as migrating your main server to a new hostname, but allows devices that you have configured for limited access to specific hosts to continue to send information to the same host name.

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.

You cannot enable an HA pool for a server that includes non-supported products.

Visit SolarWinds KB MT6886 to build an upgrade path.

Supported products

<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>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 7.0 and later</td>
</tr>
<tr>
<td>NetFlow Traffic Analyzer 4.2.1 and later</td>
<td>NetFlow Traffic Analyzer 4.2.2 and later</td>
</tr>
<tr>
<td>Network Configuration Manager 7.5.1 and later</td>
<td>Network Configuration Manager 7.7 and later</td>
</tr>
<tr>
<td>IP Address Manager 4.3.2 and later</td>
<td>IP Address Manager 4.5 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>
</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 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</td>
</tr>
<tr>
<td>HARDWARE/SOFTWARE</td>
<td>REQUIREMENTS FOR BOTH SERVERS</td>
</tr>
<tr>
<td>-------------------</td>
<td>------------------------------</td>
</tr>
<tr>
<td></td>
<td>on the primary server or closely match the primary server</td>
</tr>
<tr>
<td></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 host names)</td>
<td>Windows or BIND DNS administrative server credentials</td>
</tr>
<tr>
<td></td>
<td>- You can use other DNS servers using your own scripts.</td>
</tr>
<tr>
<td></td>
<td>- Primary and secondary server can be joined to a Windows domain</td>
</tr>
</tbody>
</table>

### 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>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 during installation when you use the Scalability Engines Installer from the Customer Portal instead of the installer downloaded from the Orion Web Console.</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.

- All pool members must be able to resolve the host names of all additional pollers, additional websites, and the main Orion server. Pool members must also be able to resolve the host names of members in the same pool.
- 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 host name 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 host name. 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 host name.

1. Build a standby server as the server you want to protect.
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 host name.

Optional deployment steps

Depending on your network and device configuration, you may need to perform some or all of the following steps.

- Modify the firewall settings to allow communication to and from the VIP address or virtual host name 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 devices that send syslog messages, SNMP traps, or NetFlow data to your Orion server to use the VIP or virtual host name. 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 host name? for more information.

- Modify devices’ SNMP settings to accept requests from the VIP address and the primary and secondary IP addresses or from the virtual host name.
- Modify devices’ SNMP settings to send requests to the primary and secondary IP addresses.

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 on 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 products installed on the secondary server must match your primary server, including the version numbers and any hotfixes.
You can open the main server's Orion Web Console while logged in to the secondary server to download the server software instead of moving the installer to the secondary server. You may need to install hotfixes manually on pool members.

Before you begin, you need the credentials for your SolarWinds Orion SQL database.

1. Open the Orion Web Console.
2. Click Settings > All Settings > High Availability Deployment Summary.
3. Click Setup a new HA server.
4. On the dialog, click Get started setting up a server.
5. Activate your HA pool license.
6. On the Setup a High Availability Server dialog, click Download installer now.
7. Move the downloaded installer to your secondary server and run it.
   - Select which type of backup server you want to install under High Availability.
   - Enter your SQL 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 more 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 host name, 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 host name (for multiple subnets installations)
- The secondary HA server
- An available HA pool license

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 and the virtual IP (VIP) address or virtual host name. The VIP must be unassigned and on the same subnet as the primary and secondary servers.
5. Optionally, if you prefer the main server in the pool to be the active server, expand Preferred Server Settings, and choose the main server. By default, no server is preferred.
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. A failover 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 will be 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

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 host name.
5. Optionally, if you prefer the main server in the pool to be the active server, expand Preferred Server Settings, and choose the main server. By default, no server is preferred.
6. Click Next.
7. Select the DNS type.
   - Microsoft DNS
     1. Enter the IP address of your DNS server.
     2. Enter the DNS Zone.
     3. Enter administrative credentials for the DNS server.
   - BIND DNS
     1. Enter the IP address of your DNS server.
     2. Enter the DNS Zone.
     3. Enter the TSIG secret key name and the TSIG shared secret key value.
8. Click Create Pool to complete the pool setup.

If the virtual host name already has a DNS entry, you are reminded that the DNS entry will be overwritten.

Your main server or additional polling engine is now highly available and can failover to the standby server across subnets. A failover audit event is logged when you create the pool and the DNS entry points to the standby server.

When the pool is created, the High Availability Deployment Summary displays the active and standby servers grouped under the pool name. Failover events will be 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.

Choose a preferred active service

When a preferred active server fails over to the standby server, it will failback to the preferred server when the 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 to failback to.

When a failover occurs, the active server fails back to the preferred server when the preferred server is UP.

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 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 there is a network connection available and your SMTP server is up.

Separate email addresses with a semicolon.

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
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.

Manage HA pools

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.

Remove HA pools

You may need to delete 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 active when you delete the pool.

   1. In the Orion Web Console, click Settings > All Settings > High Availability Deployment Summary.
   2. Select the pool you want to delete.
   3. Click Commands on the Pool Details section.
   4. Click Remove Pool.

A failover audit event is logged when you remove a pool.

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.

ℹ️ Failover can only occur when both pool members are up, the pool is enabled, and High Availability is enabled.

   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.

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.
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 restart 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.

References

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 00001010-11000111-00001111-00000001</td>
<td></td>
</tr>
<tr>
<td>VIP</td>
<td>10.199.15.20 00001010-11000111-00001111-00010100</td>
<td>27</td>
</tr>
<tr>
<td>Primary pool member</td>
<td>10.199.15.61 00001010-11000111-00001111-00111101</td>
<td>26</td>
</tr>
<tr>
<td>Secondary pool member</td>
<td>10.199.15.62 00001010-11000111-00001111-00111110</td>
<td>26</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 00001010-11000111-00001111-00000001</td>
<td></td>
</tr>
<tr>
<td>VIP</td>
<td>10.199.15.82 00001010-11000111-00001111-01010010</td>
<td>25</td>
</tr>
<tr>
<td>Primary pool member</td>
<td>10.199.15.61 00001010-11000111-00001111-00111101</td>
<td>26</td>
</tr>
<tr>
<td>Secondary pool member</td>
<td>10.199.15.62 00001010-11000111-00001111-00111110</td>
<td>26</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.

Why doesn't the virtual host name resolve?

If your virtual host name does not resolve, use the following to troubleshoot this issue.
Are you using the correct IP address of the DNS server?

Ensure you are using the correct IP address of the DNS server for your DNS zone.

Do your credentials have sufficient privileges?

Your credentials must be able to add or update host entries on the selected DNS server.

Can you connect to the DNS server?

You must be able to connect to the DNS server so the software can resolve the virtual host name.

Do your firewall settings allow connections between your DNS server and your Orion server, including any Additional Web Servers?

You must be able to connect to the DNS server from your Orion server and any Additional Web Servers.

Can your web server resolve entries from the DNS server?

Verify that your Orion server or Additional Web Server is allowed to resolve host entries from your selected DNS server.

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 (TSIG)?

Instead of administrator credentials, we require transaction signatures when interacting with BIND DNS. TSIG grants greater security when updating the DNS server.

You must configure your BIND DNS name server in the DNS zone to use TSIG you use when creating the HA pool.

The TSIG shared secret key name is the name you gave the key in the configuration file.

The TSIG shared key value is the contained in the .private file created when you generate the TSIG secret. Use the string after Key: in the file.
Failover to a standby server

Use this alert action in conjunction with SolarWinds High Availability. You can use alerts to refine your monitoring and force a failover when specific conditions exist.

For example, if you want to force a failover to your secondary server when the primary server's CPU load is more than 85% for more than 20 minutes, create an alert that monitors the primary server and choose the Failover Action in the trigger action. You can then use the Failover Action as the reset action to set the primary server as active server.

- An HA pool must be set up to configure this action.

1. When editing or adding an alert, click Add Action in the Trigger or Reset Action section of the Alert Wizard.
2. Select the Failover Action, and then click Configure Action.
3. Select the pool you want to use to failover to the backup server.
4. Schedule the action by selecting Time of Day > Use special Time of Day schedule for this action. This schedule only applies to the alert action you are editing.
   - This is often used to prevent an action from occurring during specific windows.
5. Select how frequently this action occurs for each triggered alert in Execution Settings.
6. Click Add Action.

The action is added to the trigger or reset action list, and you can test the action using the Simulate button. When the trigger or reset conditions of the alert are met, the HA pool you selected fails over to the secondary server.

Upgrade High Availability pool members

Pool members must have the same SolarWinds products and product versions installed, including hotfixes.

When you upgrade a product that is installed on a pool member, the pool is disabled and cannot be enabled until that product is also upgraded on the other pool member.

1. Log in to the Orion Web Console from the standby server.
2. Click Settings > All Settings > High Availability Deployment Summary > Set up a new HA server > How do I set it up > Download the Orion HA Installer.
3. Run the installer on the standby server.

The installer downloads all products installed on main or additional web server and then installs it.

If you view a pool when one member has not been upgraded, it appears as if there are multiple product mismatches. For example, Orion Platform, VIM, and the product you are upgrading may all appear out of sync. When you upgrade the product on the other pool member, the products and product versions should all match.
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.

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

   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 exist 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.

Before you click Submit, review the information box above it. This box lists the number of objects that will trigger the alert immediately based on your current trigger condition.

Modify any section by clicking Edit next to that section.

You can integrate your alerts with other SolarWinds' products, such as AlertCentral or Web Help Desk, by expanding Alert Integration.

Once you have created an alert, it is added to the list of available alerts in the Alert Manager. When the alert is enabled, it immediately monitors your environment for the conditions necessary to trigger it.

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.

   a. Enter the location of the log. For example, enter C:\ExampleAlertLog.txt in the Alert Log Filename Field.
   b. In the Message text box, type Node $\{N=SwisEntity;M=Caption\}$ is currently down.
   c. Click Add Action.
11. Click Add Escalation Level, and enter 5 minutes to wait for 5 minutes before escalating to the next level.
12. Click Add Action in Escalation Level 2, and select Send an Email/Page. Click Configure Action.
   a. Enter your email as the recipient.
   b. Add a message.
      
      You can use variables to customize your message. You can also use a variable that allows you to acknowledge an alert from email (${N=Alerting;M= AcknowledgeUrl}).
      
      c. Enter your SMTP server information if you have not already done so.
         You can enter a default SMTP server that is used for all your email in the Configure Default Send Email Action setting.
      
      d. Go to Execution settings to click Add Action.

13. Click Copy Actions to Reset Actions Tab, and then click Next.

14. Click Edit next to your logging action, and modify your message to Node
    ${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.

Discover network device failures

With alerting, Orion Platform products give you the ability to immediately discover whenever any device on your network is experiencing a problem.

Alert on custom properties to alert you to a node failure on your monitored network.

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.

   i The ${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 ${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.

Alerting When an IP Address Changes

Alerting on Metrics

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.

Tip: 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.

Tips: 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**

### 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:

- Alert can be triggered if more or equal [ ] 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.

4. Choose how long to wait before evaluating the next section.
5. Create the next condition block.

How condition blocks are evaluated

The condition blocks are evaluated at the same time. If they are all true based on the conditions, the alert triggers. For example, condition A, B, and C must be true in order for the alert to trigger.

(Condition A) & (Condition B) & (Condition C)

Condition blocks are evaluated using variations of AND, so the trigger condition in each section must be met.

A condition block can be evaluated at a different time than other condition blocks. For example, if you want to be alerted if the backup system is active for more than an hour, you can choose to wait an hour after the primary condition block, where the application going down is the trigger condition, before evaluating whether the backup system is still active.

Evaluate multiple object types

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.

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
- AlertConfigurations
- AlertHistory
- AlertHistoryView (introduced in 2015.1.3)
- AlertMigrationLog
- AlertObjects
- AlertSchedules
For a list of database changes from Orion Platform version 2014.2 to version 2016.1, including new tables, column changes, or data constraint or data type changes, see the online Database Changes spreadsheet.

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.
- `${AlertStartTime}` - When the alert active. You can use the Time of Day scheduler to control when the alert is active.
- `${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.
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.

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.
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.

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: (Node Status = Up) AND (Percent Loss >= 75) AND (CPU Load >= 85)

**At least one child condition must be satisfied (OR)**

At least one child condition must be true before the alert is triggered.

In this example the alert trigger reads:

Alert when: (Node Status = Up) OR (Percent Loss >= 75) OR (CPU Load >= 85)

In this situation, if any of the three conditions become true, the alert will trigger.

**All child conditions must NOT be satisfied**

Every child condition must be false before the alert is triggered.

In this example the alert trigger reads:

Do not alert when: (Node Status = Down) AND (Percent Loss <= 75) AND (CPU Load <= 85)

Alternatively, you can think of the trigger as:

Alert when: (Node Status != Down) AND (Percent Loss > 75) AND (CPU Load > 85)

The conditions have been inverted (Node Status = Down instead of Node Status = Up).

**At least one child condition must NOT be satisfied**

Any child condition must be false before the alert is triggered.
In this example the alert trigger reads:

Do not alert when: (Node Status = Down) OR (Percent Loss <= 75) OR (CPU Load <= 85)

Alternatively, you can think of the trigger as:

Alert when: (Node Status != Down) OR (Percent Loss > 75) OR (CPU Load > 85)

The conditions have been inverted (Node Status = Down instead of Node Status = Up).

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.

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 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.
   
   ![Tip](image)
   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.
   
   ![Tip](image)
   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.

![Tip](image)
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 trigger 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
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.
   - If the option is not selected, the action will be performed live on the virtual machine.
6. Under Specify New Resources, specify whether you want to add more resources to the virtual machine, or replace the existing resources with new resources, and then specify the parameters of the new resource or resources.
   a. Select Number of processors, and specify the number of processors to allocate.
   b. Select Memory, and specify the memory capacity to allocate.

7. Schedule the action by selecting Time of Day > Use special Time of Day schedule for this action. This schedule only applies to the alert action you are editing.
   ![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.
      - 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.

   ![This option is only available if the alert is built to trigger for virtual machines.]

   b. To power off a different virtual machine, click Select specific VM, and search for a virtual machine.

4. Schedule the action by selecting Time of Day > Use special Time of Day schedule for this action. This schedule only applies to the alert action you are editing.

   ![This is often used to prevent an action from occurring during specific windows.]

5. Select how frequently this action occurs for each triggered alert in Execution Settings.

6. Click Add Action.

The action is added to the trigger or reset action list, and you can test the action using the Simulate button. When the trigger or reset conditions of the alert are met, the specified virtual machine will be powered off.
Power on a virtual machine

If a virtual machine is powered off, you can have an alert trigger the virtual machine to be powered on. This alert management action is only available if the integration with Virtualization Manager is enabled.

1. When editing or adding an alert, click Add Action in the Trigger or Reset Action section of the Alert Wizard.
2. Select Manage VM - Power On, and click Configure Action.
3. Under Select Virtual Machine, specify the virtual machine that you want to power on.
   a. To power on the virtual machine that triggered the alert, click Execute this action.
   
   ![This option is only available if the alert is built to trigger for virtual machines.]
   
   b. To power on a different virtual machine, click Select specific VM, and search for a virtual machine.
4. Schedule the action by selecting Time of Day > Use special Time of Day schedule for this action. This schedule only applies to the alert action you are editing.
   
   ![This is often used to prevent an action from occurring during specific windows.]
5. Select how frequently this action occurs for each triggered alert in Execution Settings.
6. Click Add Action.

The action is added to the trigger or reset action list, and you can test the action using the Simulate button. When the trigger or reset conditions of the alert are met, the specified virtual machine will be powered on.

Restart a virtual machine

If a virtual machine is experiencing issues, you can have an alert trigger the virtual machine to be restarted. This alert management action is only available if the integration with Virtualization Manager is enabled.

1. When editing or adding an alert, click Add Action in the Trigger or Reset Action section of the Alert Wizard.
2. Select Manage VM - Reboot, and click Configure Action.
3. Under Select Virtual Machine, specify the virtual machine that you want to reboot.
   a. To reboot the virtual machine that triggered the alert, click Execute this action.
   
   ![This option is only available if the alert is built to trigger for virtual machines.]
   
   b. To reboot a different virtual machine, click Select specific VM, and search for a virtual machine.
4. Schedule the action by selecting Time of Day > Use special Time of Day schedule for this action. This schedule only applies to the alert action you are editing.
This is often used to prevent an action from occurring during specific windows.

5. Select how frequently this action occurs for each triggered alert in Execution Settings.
6. Click Add Action.

The action is added to the trigger or reset action list, and you can test the action using the Simulate button. When the trigger or reset conditions of the alert are met, the specified virtual machine restarts.

Suspend a virtual machine

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.
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.

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.
      
      ![Note] 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.

   ![Note] This is often used to prevent an action from occurring during specific windows.

7. Select how frequently this action occurs for each triggered alert in Execution Settings.

8. Click Add Action.

The action is added to the trigger or reset action list, and you can test the action using the Simulate button. When the trigger or reset conditions of the alert are met, the SNMP trap message is sent.

**Send a GET or POST request**

SolarWinds can be configured to communicate alerts using HTTP GET or POST functions. As an example, a URL may be used as an interface into a trouble ticket system, and, by correctly formatting the GET function, new trouble tickets may be created automatically.

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.

4. Schedule the action by selecting Time of Day > Use special Time of Day schedule for this action. This schedule only applies to the alert action you are editing.

   ![Note] This is often used to prevent an action from occurring during specific windows.

5. Select how frequently this action occurs for each triggered alert in Execution Settings.

6. Click Add Action.
The action is added to the trigger or reset action list, and you can test the action using the Simulate button. When the trigger or reset conditions of the alert are met, the GET or POST request is sent to the server. You can view the server logs to confirm that the action occurred.

Send a syslog message

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 investigation into the cause of the alert.

Before configuring this alert you must first configure the default SMTP server the product uses to send email. You can change the default SMTP server later or use different SMTP servers for specific alerts.

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 with 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 SNMP 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 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.

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:
      The server with the Windows Event Log that the alert writes to must be monitored by your Orion server.
   b. Enter the Message of your alert trigger.
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.

Variables and examples

Orion Platform products, including the Alert Manager, the Traps Viewer, the Syslog Viewer, and Network Atlas can employ Orion variables. These variables are dynamic and, in the case of alerts, parse when the alert is triggered or reset.

As of Orion Platform version 2015.1, variables have changed to a more flexible format. The previous implementation was SQL based, and the new version is based on SolarWinds Information Service (SWIS). For example, the variable \${ResponseTime} is now \${N=SwisEntity;M=ResponseTime}.

Variables are designated by a $ and enclosed in {brackets}. There are three attributes per variable, but only two are necessary.

All variables are available in the variable picker in the Orion Web Console. You do not need to create or enter variables manually.
This is the context of the variable and required. You can use the following contexts:

- Alerting - uses variables specific to alerting
- OrionGroup - uses variables specific to groups
- SwisEntity - uses variables specific to the objects you monitor in the context of the alert
- Generic - uses variables specific to general environmental properties

This is the variable or macro name and required. You can use entity names from the SWIS.

This converts the data to a user-friendly format. Use formats that correlate to the data. For example, use DateTime with AcknowledgedTime, not with ObjectType. You can convert data to specific formats using the variable picker.

Variable modifiers

Variables can be modified by using any of the variable modifiers in the following table.

<table>
<thead>
<tr>
<th>VARIABLE MODIFIER</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>-Raw</td>
<td>Displays the raw value for the statistic. For example, if Transmit Bandwidth is set to 10 Mbps, then the raw value would be “10000000”. The cooked value would be “10 Mbps”.</td>
</tr>
<tr>
<td>-Previous</td>
<td>Displays the previous value for the statistic before the Alert was triggered</td>
</tr>
<tr>
<td>-Cooked</td>
<td>Displays the cooked value for the statistic. For example, if Transmit Bandwidth is set to 10 Mbps, then the raw value would be “10000000” and cooked value would be “10 Mbps”.</td>
</tr>
<tr>
<td>-PreviousCooked</td>
<td>Displays the previous cooked value for the statistic before the Alert was triggered</td>
</tr>
</tbody>
</table>

Add modifiers to variables by the following examples below:

```
${N=Alerting;M=Previous(AcknowledgedBy)}
```

Alert variables

General alert variables

The following are valid, general alert variables.
<table>
<thead>
<tr>
<th><strong>GENERAL VARIABLE</strong></th>
<th><strong>DESCRIPTION</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><code>${N=Alerting;M=AlertID}</code></td>
<td>The ID of the alert</td>
</tr>
<tr>
<td><code>${N=Alerting;M=AlertName}</code></td>
<td>The name of the alert from the alert field Name of alert definition in Alert Properties</td>
</tr>
<tr>
<td><code>${N=Alerting;M=AlertDescription}</code></td>
<td>The description of the alert from the alert field Description of alert definition in Alert Properties</td>
</tr>
<tr>
<td><code>${N=Alerting;M=AlertDetailsURL}</code></td>
<td>The URL used to get more information about the triggered alert</td>
</tr>
<tr>
<td><code>${N=Alerting;M=AlertMessage}</code></td>
<td>The alert message from the alert field Message displayed when this alert is triggered in Trigger Actions</td>
</tr>
<tr>
<td><code>${N=Alerting;M=DownTime}</code></td>
<td>The amount of time the alert has been active</td>
</tr>
<tr>
<td><code>${N=Alerting;M=ObjectType}</code></td>
<td>The object type that the alert is monitoring</td>
</tr>
<tr>
<td><code>${N=Alerting;M=Severity}</code></td>
<td>The severity of the alert from the alert field Severity of Alert in Alert Properties</td>
</tr>
<tr>
<td><code>${N=Alerting;M=LastEdit}</code></td>
<td>The last time the alert definition has been edited</td>
</tr>
<tr>
<td><code>${N=Alerting;M=Acknowledged}</code></td>
<td>Acknowledged status</td>
</tr>
<tr>
<td><code>${N=Alerting;M=AcknowledgedBy}</code></td>
<td>Who the alert was acknowledged by</td>
</tr>
<tr>
<td><code>${N=Alerting;M=AcknowledgedTime}</code></td>
<td>Time the alert was acknowledged</td>
</tr>
<tr>
<td><code>${N=Alerting;M=Notes}</code></td>
<td>Information from the Notes field when you acknowledge alerts through the Web Console</td>
</tr>
<tr>
<td><code>${N=Alerting;M=AlertTriggerCount}</code></td>
<td>Count of triggers</td>
</tr>
</tbody>
</table>
| `${N=Alerting;M=AlertTriggerTime}` | Date and time of the last event for this alert. (Windows control panel defined “Short Date” and “Short Time”)
| `${N=Generic;M=Application}` | SolarWinds application information |
| `${N=Generic;M=Copyright}` | Copyright information |
| `${N=Generic;M=Release}` | Release information |
| `${N=Generic;M=Version}` | Version of the SolarWinds software package |

It is possible to use previous generation variables, for example `${NodeName}`. However, when using the variable picker, the new format is displayed by default. Previous generation variables can only be entered manually.
Some variables are no longer valid.

Date and time variables
The following are valid date and time variables.

<table>
<thead>
<tr>
<th>DATE/TIME VARIABLE</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>${N=Generic;M=AMPM}</td>
<td>AM/PM indicator</td>
</tr>
<tr>
<td>${N=Generic;M=AbreviatedDOW}</td>
<td>Current day of the week. Three character abbreviation.</td>
</tr>
<tr>
<td>${N=Generic;M=Day}</td>
<td>Current day of the month</td>
</tr>
<tr>
<td>${N=Generic;M=Date;F=Date}</td>
<td>Current date. (Short Date format)</td>
</tr>
<tr>
<td>${N=Generic;M=DateTime;F=DateTime}</td>
<td>Current date and time. (Windows control panel defined “Long Date” and “Long Time” format)</td>
</tr>
<tr>
<td>${N=Generic;M=DayOfWeek}</td>
<td>Current day of the week.</td>
</tr>
<tr>
<td>${N=Generic;M=DayOfYear}</td>
<td>Numeric day of the year</td>
</tr>
<tr>
<td>${N=Generic;M=Hour}</td>
<td>Current hour</td>
</tr>
<tr>
<td>${N=Generic;M=HH}</td>
<td>Current hour. Two digit format, zero padded.</td>
</tr>
<tr>
<td>${N=Generic;M=Past2Hours}</td>
<td>Last two hours</td>
</tr>
<tr>
<td>${N=Generic;M=Past24Hours}</td>
<td>Last 24 hours</td>
</tr>
<tr>
<td>${N=Generic;M=Last7Days;F=Date}</td>
<td>Last seven days (Short Date format)</td>
</tr>
<tr>
<td>${N=Generic;M=PastHour}</td>
<td>Last hour</td>
</tr>
<tr>
<td>${N=Generic;M=LocalDOW}</td>
<td>Current day of the week. Localized language format.</td>
</tr>
<tr>
<td>${N=Generic;M=LocalMonthName}</td>
<td>Current month name in the local language.</td>
</tr>
<tr>
<td>${N=Generic;M=LongDate}</td>
<td>Current date. (Long Date format)</td>
</tr>
<tr>
<td>${N=Generic;M=Month}</td>
<td>Current numeric month</td>
</tr>
<tr>
<td>${N=Generic;M=MM}</td>
<td>Current month. Two digit number, zero padded.</td>
</tr>
<tr>
<td>${N=Generic;M=AbbreviatedMonth}</td>
<td>Current month. Three character abbreviation.</td>
</tr>
<tr>
<td>${N=Generic;M=MonthName}</td>
<td>Full name of the current month</td>
</tr>
<tr>
<td>${N=Generic;M=MediumDate}</td>
<td>Current date. (Medium Date format)</td>
</tr>
<tr>
<td>${N=Generic;M=Minute}</td>
<td>Current minute. Two digit format, zero padded.</td>
</tr>
</tbody>
</table>
# Date/Time Variable

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>${N=Generic;M=Second}</td>
<td>Current second. Two digit format, zero padded.</td>
</tr>
<tr>
<td>${N=Generic;M=Time}</td>
<td>Current Time. (Short Time format)</td>
</tr>
<tr>
<td>${N=Generic;M=Today;F=Date}</td>
<td>Today (Short Date format)</td>
</tr>
<tr>
<td>${N=Generic;M=Year}</td>
<td>Four digit year</td>
</tr>
<tr>
<td>${N=Generic;M=Year2}</td>
<td>Two digit year</td>
</tr>
<tr>
<td>${N=Generic;M=Yesterday;F=Date}</td>
<td>Yesterday (Short Date format)</td>
</tr>
</tbody>
</table>

## Group variables

The following are valid group variables.

<table>
<thead>
<tr>
<th>Group Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>${N=OrionGroup;M=GroupDetailsURL}</td>
<td>URL of the Group Details view for a selected group</td>
</tr>
<tr>
<td>${N=OrionGroup;M=GroupFrequency}</td>
<td>Interval on which group membership is evaluated and group snapshots are taken.</td>
</tr>
<tr>
<td>${N=OrionGroup;M=GroupID}</td>
<td>Designated identifier for a defined group</td>
</tr>
<tr>
<td>${N=OrionGroup;M=GroupMemberDisplayName}</td>
<td>Display name of group member type: Node, Volume, Component, Application, etc.</td>
</tr>
<tr>
<td>${N=OrionGroup;M=GroupMemberDisplayNamePlural}</td>
<td>Display name of multiple group members of a type: Nodes, Components, Applications, etc.</td>
</tr>
<tr>
<td>${N=OrionGroup;M=GroupMemberFullName}</td>
<td>Full name of a group member, including location</td>
</tr>
<tr>
<td>${N=OrionGroup;M=GroupMemberName}</td>
<td>Name of a group member</td>
</tr>
<tr>
<td>${N=OrionGroup;M=GroupMemberPercentAvailability}</td>
<td>Percent availability of a group member when group member status is Up, Warning, or Critical and 0% if status is anything else.</td>
</tr>
<tr>
<td>${N=OrionGroup;M=GroupMemberSnapshotID}</td>
<td>Unique identifier of group member snapshot.</td>
</tr>
<tr>
<td>${N=OrionGroup;M=GroupMemberStatusID}</td>
<td>Identifier assigned to a group member indicating its status. For more information see Status values.</td>
</tr>
<tr>
<td>${N=OrionGroup;M=GroupMemberStatusName}</td>
<td>Name of group member status. For more information see Status values.</td>
</tr>
</tbody>
</table>
### Group Variable

<table>
<thead>
<tr>
<th>Group Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>${N=OrionGroup;M=GroupMemberUri}</td>
<td>Uri used by SolarWinds Information Service (SWIS) to refer to the selected group member within the web console.</td>
</tr>
<tr>
<td>${N=OrionGroup;M=GroupName}</td>
<td>Name of the group.</td>
</tr>
<tr>
<td>${N=OrionGroup;M=GroupOwner}</td>
<td>Orion product appropriate to the group type</td>
</tr>
<tr>
<td>${N=OrionGroup;M=GroupPercentAvailability}</td>
<td>100% when group status is Up, Warning, Critical and 0% if status is anything else.</td>
</tr>
<tr>
<td>${N=OrionGroup;M=GroupStatusCalculatorID}</td>
<td>Name of roll-up logic calculator that evaluates status of group based on member statuses. (0 = Mixed, 1 = Worst, 2 = Best)</td>
</tr>
<tr>
<td>${N=OrionGroup;M=GroupStatusCalculatorName}</td>
<td>Name of roll-up logic calculator that evaluates status of group based on member statuses. (Mixed, Worst, Best)</td>
</tr>
<tr>
<td>${N=OrionGroup;M=GroupStatusID}</td>
<td>Identifier assigned to a group indicating its status. For more information see <a href="#">Status values</a>.</td>
</tr>
<tr>
<td>${N=OrionGroup;M=GroupStatus}</td>
<td>Name of group status. For more information see <a href="#">Status values</a>.</td>
</tr>
<tr>
<td>${N=OrionGroup;M=GroupStatusRootCause}</td>
<td>A list of all group members that are not Up</td>
</tr>
</tbody>
</table>

### Status Variables

When using the `${Status}` variable with a monitored object, status values are returned, as appropriate. The following table provides a description for each status value.

<table>
<thead>
<tr>
<th>STATUS VALUE</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>Unknown</td>
</tr>
<tr>
<td>1</td>
<td>Up</td>
</tr>
<tr>
<td>2</td>
<td>Down</td>
</tr>
<tr>
<td>3</td>
<td>Warning</td>
</tr>
<tr>
<td>4</td>
<td>Shutdown</td>
</tr>
<tr>
<td>5</td>
<td>Testing</td>
</tr>
<tr>
<td>6</td>
<td>Dormant</td>
</tr>
</tbody>
</table>
### STATUS VALUE | DESCRIPTION
---|---
7 | Not Present
8 | Lower Layer Down
9 | Unmanaged
10 | Unplugged
11 | External
12 | Unreachable
14 | Critical
15 | Mixed Availability
16 | Misconfigured
17 | Could Not Poll
19 | Unconfirmed
22 | Active
24 | Inactive
25 | Expired
26 | Monitoring Disabled
27 | Disabled
28 | Not Licensed

Important: As of Orion Platform version 2015.1, SolarWinds alerts use a new variable format. See [Alert variables](#) for more information.

**Node variables**
The following are valid node variables.

<table>
<thead>
<tr>
<th>Node Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>${N=SwisEntity;M=AgentPort}</td>
<td>Node SNMP port number</td>
</tr>
<tr>
<td>${N=SwisEntity;M=Node.Allow64BitCounters}</td>
<td>Node allows 64-bit counters (1), or not (0)</td>
</tr>
<tr>
<td>${N=SwisEntity;M=AvgResponseTime}</td>
<td>Average node response time, in msec, to ICMP requests</td>
</tr>
<tr>
<td>Node Variable</td>
<td>Description</td>
</tr>
<tr>
<td>---------------</td>
<td>-------------</td>
</tr>
<tr>
<td>${N=SwisEntity;M=BlockUntil}$</td>
<td>Day, date, and time until which node polling is blocked</td>
</tr>
<tr>
<td>${N=SwisEntity;M=BufferBgMissThisHour}$</td>
<td>Device-dependent count of big buffer misses on node in current hour, queried with MIB 1.3.6.1.4.9.2.1.30</td>
</tr>
<tr>
<td>${N=SwisEntity;M=BufferBgMissToday}$</td>
<td>Device-dependent count of big buffer misses on node in current day, queried with MIB 1.3.6.1.4.9.2.1.30</td>
</tr>
<tr>
<td>${N=SwisEntity;M=BufferHgMissThisHour}$</td>
<td>Device-dependent count of huge buffer misses on node in current hour, queried with MIB 1.3.6.1.4.9.2.1.62</td>
</tr>
<tr>
<td>${N=SwisEntity;M=BufferHgMissToday}$</td>
<td>Device-dependent count of huge buffer misses on node in current day, queried with MIB 1.3.6.1.4.9.2.1.62</td>
</tr>
<tr>
<td>${N=SwisEntity;M=BufferLgMissThisHour}$</td>
<td>Device-dependent count of large buffer misses on node in current hour, queried with MIB 1.3.6.1.4.9.2.1.38</td>
</tr>
<tr>
<td>${N=SwisEntity;M=BufferLgMissToday}$</td>
<td>Device-dependent count of large buffer misses on node in current day, queried with MIB 1.3.6.1.4.9.2.1.38</td>
</tr>
<tr>
<td>${N=SwisEntity;M=BufferMdMissThisHour}$</td>
<td>Device-dependent count of medium buffer misses on node in current hour, queried with MIB 1.3.6.1.4.9.2.1.22</td>
</tr>
<tr>
<td>${N=SwisEntity;M=BufferMdMissToday}$</td>
<td>Device-dependent count of medium buffer misses on node in current day, queried with MIB 1.3.6.1.4.9.2.1.22</td>
</tr>
<tr>
<td>${N=SwisEntity;M=BufferNoMemThisHour}$</td>
<td>Count of buffer errors due to low memory on node in current hour</td>
</tr>
<tr>
<td>${N=SwisEntity;M=BufferNoMemToday}$</td>
<td>Count of buffer errors due to low memory on node in current day</td>
</tr>
<tr>
<td>${N=SwisEntity;M=BufferSmMissThisHour}$</td>
<td>Device-dependent count of small buffer misses on node in current hour, queried with MIB 1.3.6.1.4.9.2.1.14</td>
</tr>
<tr>
<td>Node Variable</td>
<td>Description</td>
</tr>
<tr>
<td>---------------</td>
<td>-------------</td>
</tr>
<tr>
<td>${N=SwisEntity;M=BufferSmMissToday}</td>
<td>Device-dependent count of small buffer misses on node in current day, queried with MIB 1.3.6.1.4.9.2.1.14</td>
</tr>
<tr>
<td>${N=SwisEntity;M=Caption}</td>
<td>User friendly node name</td>
</tr>
<tr>
<td>${N=SwisEntity;M=Community}</td>
<td>Node community string</td>
</tr>
<tr>
<td>${N=SwisEntity;M=Contact}</td>
<td>Contact information for person or group responsible for node</td>
</tr>
<tr>
<td>${N=SwisEntity;M=CPULoad}</td>
<td>Node CPU utilization rate at last poll</td>
</tr>
<tr>
<td>${N=SwisEntity;M=CustomPollerLastStatisticsPoll}</td>
<td>Day, date, and time of last poll attempt on node</td>
</tr>
<tr>
<td>${N=SwisEntity;M=CustomPollerLastStatisticsPollSuccess}</td>
<td>Day, date, and time that node was last successfully polled</td>
</tr>
<tr>
<td>${N=SwisEntity;M=NodeDescription}</td>
<td>Node hardware and software</td>
</tr>
<tr>
<td>${N=SwisEntity;M=DNS}</td>
<td>Fully qualified node name</td>
</tr>
<tr>
<td>${N=SwisEntity;M=DynamicIP}</td>
<td>If node supports dynamic IP address assignment via BOOTP or DHCP (1); static IP address return (0)</td>
</tr>
<tr>
<td>${N=SwisEntity;M=EngineID}</td>
<td>Internal unique identifier of the polling engine to which node is assigned</td>
</tr>
<tr>
<td>${N=SwisEntity;M=GroupStatus}</td>
<td>Filename of status icon for node and, in NPM, its interfaces</td>
</tr>
<tr>
<td>${N=SwisEntity;M=IOSImage}</td>
<td>Family name of Cisco IOS on node</td>
</tr>
<tr>
<td>${N=SwisEntity;M=IOSVersion}</td>
<td>Cisco IOS version on node</td>
</tr>
<tr>
<td>${N=SwisEntity;M=IP_Address}</td>
<td>Node IP address</td>
</tr>
<tr>
<td>${N=SwisEntity;M=IPAddressType}</td>
<td>Node IP address version (IPv4 or IPv6)</td>
</tr>
<tr>
<td>${N=SwisEntity;M=LastBoot}</td>
<td>Day, date and time of last node boot</td>
</tr>
<tr>
<td>${N=SwisEntity;M=LastSync}</td>
<td>Time and date of last node database and memory synchronization</td>
</tr>
<tr>
<td>${N=SwisEntity;M=Location}</td>
<td>Physical location of node</td>
</tr>
<tr>
<td>Node Variable</td>
<td>Description</td>
</tr>
<tr>
<td>---------------</td>
<td>-------------</td>
</tr>
<tr>
<td><code>${N=SwisEntity;M=MachineType}</code></td>
<td>Node manufacturer or distributor and family or version information</td>
</tr>
<tr>
<td><code>${N=SwisEntity;M=MaxResponseTime}</code></td>
<td>Maximum node response time, in msec, to ICMP requests</td>
</tr>
<tr>
<td><code>${N=SwisEntity;M=MemoryUsed}</code></td>
<td>Total node memory used over polling interval</td>
</tr>
<tr>
<td><code>${N=SwisEntity;M=Stats.MinResponseTime}</code></td>
<td>Minimum node response time, in msec, to ICMP requests</td>
</tr>
<tr>
<td><code>${N=SwisEntity;M=NextPoll}</code></td>
<td>Day, date and time of next scheduled node polling</td>
</tr>
<tr>
<td><code>${N=SwisEntity;M=NextRediscovery}</code></td>
<td>Time of next node rediscovery</td>
</tr>
<tr>
<td><code>${N=SwisEntity;M=NodeID}</code></td>
<td>Internal unique identifier of node</td>
</tr>
<tr>
<td><code>${N=SwisEntity;M=PercentLoss}</code></td>
<td>ICMP packet loss percentage when node last polled</td>
</tr>
<tr>
<td><code>${N=SwisEntity;M=PercentMemoryUsed}</code></td>
<td>Percentage of total node memory used over polling interval</td>
</tr>
<tr>
<td><code>${N=SwisEntity;M=PollInterval}</code></td>
<td>Node polling interval, in seconds</td>
</tr>
<tr>
<td><code>${N=SwisEntity;M=RediscoveryInterval}</code></td>
<td>Node rediscovery interval, in minutes</td>
</tr>
<tr>
<td><code>${N=SwisEntity;M=ResponseTime}</code></td>
<td>Node response time, in milliseconds, to last ICMP request</td>
</tr>
<tr>
<td><code>${N=SwisEntity;M=SNMPv3Credentials.RWAuthenticationKey}</code></td>
<td>SNMPv3 read/write credential authentication key</td>
</tr>
<tr>
<td><code>${N=SwisEntity;M=SNMPv3Credentials.RWAuthenticationKeyIsPassword}</code></td>
<td>States if the SNMPv3 read/write credential authentication key is the password</td>
</tr>
<tr>
<td><code>${N=SwisEntity;M=SNMPv3Credentials.RWAuthenticationMethod}</code></td>
<td>SNMPv3 read/write credential authentication method</td>
</tr>
<tr>
<td><code>${N=SwisEntity;M=SNMPv3Credentials.RWContext}</code></td>
<td>SNMPv3 read/write security context information</td>
</tr>
<tr>
<td><code>${N=SwisEntity;M=SNMPv3Credentials.RWPrivacyKey}</code></td>
<td>SNMPv3 read/write credential key</td>
</tr>
<tr>
<td>Node Variable</td>
<td>Description</td>
</tr>
<tr>
<td>---------------</td>
<td>-------------</td>
</tr>
<tr>
<td>N=SwisEntity;M=SNMPv3Credentials.RWPrivacyKeyIsPassword</td>
<td>States if the SNMPv3 read/write credential privacy key is the password</td>
</tr>
<tr>
<td>N=SwisEntity;M=SNMPv3Credentials.RWPrivacyMethod</td>
<td>SNMPv3 read/write credential privacy encryption method</td>
</tr>
<tr>
<td>N=SwisEntity;M=SNMPv3Credentials.RWUsername</td>
<td>User friendly name for SNMPv3 read/write credential</td>
</tr>
<tr>
<td>N=SwisEntity;M=Severity</td>
<td>A network health score determined additively by scoring the status of monitored objects. In NPM 1 point is provided for an interface in a warning state, 1000 points for a down interface, and 1 million points for a down node. In SAM, 100 points is provided for an application in a warning state, 200 points for an application in critical state, 500 is status is unknown, and 1000 for a down application.</td>
</tr>
<tr>
<td>N=SwisEntity;M=SNMPv3Credentials.AuthenticationKey</td>
<td>SNMPv3 authentication key</td>
</tr>
<tr>
<td>N=SwisEntity;M=SNMPv3Credentials.AuthenticationKeyIsPassword</td>
<td>States if node SNMPv3 authentication key is password</td>
</tr>
<tr>
<td>N=SwisEntity;M=SNMPv3Credentials.AuthenticationMethod</td>
<td>SNMPv3 authentication type</td>
</tr>
<tr>
<td>N=SwisEntity;M=SNMPv3Credentials.Context</td>
<td>Group or domain of user with SNMPv3 access to node</td>
</tr>
<tr>
<td>N=SwisEntity;M=SNMPv3Credentials.PrivacyKey</td>
<td>SNMPv3 credential key</td>
</tr>
<tr>
<td>N=SwisEntity;M=SNMPv3Credentials.PrivacyKeyIsPassword</td>
<td>States if node SNMPv3 credential key is the password</td>
</tr>
<tr>
<td>N=SwisEntity;M=SNMPv3Credentials.PrivacyMethod</td>
<td>SNMPv3 credential key type</td>
</tr>
<tr>
<td>N=SwisEntity;M=SNMPv3Credentials.Username</td>
<td>User friendly name for SNMPv3 credential</td>
</tr>
</tbody>
</table>
### Node Variable Description

<table>
<thead>
<tr>
<th>Node Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Username}</td>
<td></td>
</tr>
<tr>
<td>${N=SwisEntity;M=SNMPVersion}</td>
<td>States the version of SNMP used by the node</td>
</tr>
<tr>
<td>${N=SwisEntity;M=StatCollection}</td>
<td>Statistics collection frequency, in minutes</td>
</tr>
<tr>
<td>${N=SwisEntity;M=Status;F=Status}</td>
<td>Numerical node status. For more information, see <a href="#">Status Variables</a>.</td>
</tr>
<tr>
<td>${N=SwisEntity;M=StatusDescription}</td>
<td>User friendly node status</td>
</tr>
<tr>
<td>${N=SwisEntity;M=StatusLED}</td>
<td>Filename of node status icon</td>
</tr>
<tr>
<td>${N=SwisEntity;M=SysName}</td>
<td>String reply to SNMP SYS_NAME OID request</td>
</tr>
<tr>
<td>${N=SwisEntity;M=SysObjectID}</td>
<td>Vendor ID of the network management subsystem in OID form. Clearly determines the type of node.</td>
</tr>
<tr>
<td>${N=SwisEntity;M=SystemUpTime}</td>
<td>Time, in hundredths of a second, either since network monitoring started (WMI) or since the monitored device rebooted (SNMP).</td>
</tr>
<tr>
<td>${N=SwisEntity;M=TotalMemory}</td>
<td>Total node memory available</td>
</tr>
<tr>
<td>${N=SwisEntity;M=UnManaged}</td>
<td>States if node is currently unmanaged</td>
</tr>
<tr>
<td>${N=SwisEntity;M=UnManageFrom}</td>
<td>Day, date, and time when node is set to “Unmanaged”</td>
</tr>
<tr>
<td>${N=SwisEntity;M=UnManageUntil}</td>
<td>Day, date, and time when node is scheduled to be managed</td>
</tr>
<tr>
<td>${N=SwisEntity;M=Vendor}</td>
<td>Node manufacturer or distributor</td>
</tr>
<tr>
<td>${N=SwisEntity;M=VendorIcon}</td>
<td>Filename of node vendor logo</td>
</tr>
</tbody>
</table>

#### SQL queries

Any value you can collect from the database can be generated, formatted, or calculated using a SQL query as a variable. To use a SQL query as a variable in Orion Platform products, use `${SQL: {query}}` as shown in the following example that returns the results of the SQL query:

```
Select Count(*) From Nodes:
```

[i] SolarWinds does not support SQL queries directly. Visit our user forums on [THWACK](#) for help from our community.
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.
- **${AlertStartTime}** - When the alert is active. You can use the Time of Day scheduler to control when the alert is active.
- **${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.

Status values

When using the `${N=SwisEntity; M=Status}` variable with a monitored object, status values are returned, as appropriate. The following table provides a description for each status value.

<table>
<thead>
<tr>
<th>STATUS VALUE</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>Unknown</td>
</tr>
<tr>
<td>1</td>
<td>Up</td>
</tr>
<tr>
<td>2</td>
<td>Down</td>
</tr>
<tr>
<td>3</td>
<td>Warning</td>
</tr>
<tr>
<td>4</td>
<td>Shutdown</td>
</tr>
<tr>
<td>5</td>
<td>Testing</td>
</tr>
<tr>
<td>6</td>
<td>Dormant</td>
</tr>
<tr>
<td>7</td>
<td>Not Present</td>
</tr>
<tr>
<td>8</td>
<td>Lower Layer Down</td>
</tr>
<tr>
<td>9</td>
<td>Unmanaged</td>
</tr>
<tr>
<td>10</td>
<td>Unplugged</td>
</tr>
<tr>
<td>11</td>
<td>External</td>
</tr>
<tr>
<td>12</td>
<td>Unreachable</td>
</tr>
<tr>
<td>14</td>
<td>Critical</td>
</tr>
</tbody>
</table>
### Status Value Description

<table>
<thead>
<tr>
<th>Status Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>15</td>
<td>Partly Available</td>
</tr>
<tr>
<td>16</td>
<td>Misconfigured</td>
</tr>
<tr>
<td>17</td>
<td>Could Not Poll</td>
</tr>
<tr>
<td>19</td>
<td>Unconfirmed</td>
</tr>
<tr>
<td>22</td>
<td>Active</td>
</tr>
<tr>
<td>24</td>
<td>Inactive</td>
</tr>
<tr>
<td>25</td>
<td>Expired</td>
</tr>
<tr>
<td>26</td>
<td>Monitoring Disabled</td>
</tr>
<tr>
<td>27</td>
<td>Disabled</td>
</tr>
<tr>
<td>28</td>
<td>Not Licensed</td>
</tr>
<tr>
<td>29</td>
<td>Other</td>
</tr>
<tr>
<td>30</td>
<td>Not Running</td>
</tr>
</tbody>
</table>

#### Example messages using variables

The following examples illustrate messages that you can create using variables. You can use variables in the message body or the subject. You can also use variables in alert conditions.

SolarWinds recommends using the variable picker by clicking Insert Variable.

<table>
<thead>
<tr>
<th>Message with variables</th>
<th>Message with resolved variables</th>
</tr>
</thead>
<tbody>
<tr>
<td>Previous reboot was at ${N=SwisEntity;M=Previous (LastBoot)}.</td>
<td>Previous reboot was at 10/29/2014 12:02:00 PM.</td>
</tr>
<tr>
<td>Alert: The SNMP Community string used to query ${N=SwisEntity;M=Caption} has been changed from ${N=SwisEntity;M=Previous(Community)} to ${N=SwisEntity;M=Community}.</td>
<td>Alert: The SNMP Community string used to query Houston_backup has been changed from 1234 to 5678.</td>
</tr>
<tr>
<td>Alert: ${N=SwisEntity;M=Caption} has exceptionally high response time. Average Response Time is ${N=SwisEntity;M=AvgResponseTime} and is varying from ${N=SwisEntity;M=MinResponseTime} to ${N=SwisEntity;M=MaxResponseTime}.</td>
<td>Alert: DevOP_VMs has exceptionally high response time. Average Response Time is 1200 ms and is varying from 500 ms to 1700 ms.</td>
</tr>
</tbody>
</table>
You can also manually add a repeater when you expect multiple objects to be included in an alert. For example, if you have an alert set up to notify you when 5 nodes go down, you can use <<< >>> to repeat both text and variables. See the examples below.

This message with no repeater displays every node that is down in a separate sentence: 

\[
\text{Current packet loss for } \{N=\text{SwisEntity};M=\text{Caption}\} \text{ is } \{N=\text{SwisEntity};M=\text{PercentLoss}\}. \text{ Average Response time is } \{N=\text{SwisEntity};M=\text{AvgResponseTime}\} \text{ and is varying from } \{N=\text{SwisEntity};M=\text{MinResponseTime}\} \text{ to } \{N=\text{SwisEntity};M=\text{MaxResponseTime}\}. \\
\]

This message displays only the text included in the repeater, in this case each node that is down: 

\[
\text{MainWebServer is } 43\%. \text{ Average Response time is } 500 \text{ ms and is varying from } 200 \text{ ms to } 800 \text{ ms.}
\]

This message displays each node that is down and the status of each node: 

\[
\text{<<< } \{N=\text{SwisEntity};M=\text{Caption}\} \text{ is } \{N=\text{SwisEntity};M=\text{Status};F=\text{Status}\}. \text{ >>>
\]

\[
\text{SYSLOG ALERT VARIABLES}
\]

The following variables can be used in syslog alert messages. Each variable must begin with a dollar sign and be enclosed in curly braces as, for example, \(\{\text{VariableName}\}\). Syslog alerts also support the use of Node alert variables.

For more information on the use of variables, see Variables and examples.
Syslog date and time variables
<table>
<thead>
<tr>
<th>SYLOG DATE/TIME VARIABLE</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>${AbbreviatedDOW}</td>
<td>Current day of the week. Three character abbreviation.</td>
</tr>
<tr>
<td>${AMPM}</td>
<td>AM or PM corresponding to current time (before or after noon)</td>
</tr>
<tr>
<td>${D}</td>
<td>Current day of the month</td>
</tr>
<tr>
<td>${DD}</td>
<td>Current day of the month (two digit number, zero padded)</td>
</tr>
<tr>
<td>${Date}</td>
<td>Current date. (Short Date format)</td>
</tr>
<tr>
<td>${DateTime}</td>
<td>Current date and time. (Windows control panel defined &quot;Short Date&quot; and &quot;Short Time&quot; format)</td>
</tr>
<tr>
<td>${DayOfWeek}</td>
<td>Current day of the week.</td>
</tr>
<tr>
<td>${DayOfYear}</td>
<td>Numeric day of the year</td>
</tr>
<tr>
<td>${H}</td>
<td>Current hour</td>
</tr>
<tr>
<td>${HH}</td>
<td>Current hour. Two digit format, zero padded.</td>
</tr>
<tr>
<td>${Hour}</td>
<td>Current hour. 24-hour format</td>
</tr>
<tr>
<td>${LocalDOW}</td>
<td>Current day of the week. Localized language format.</td>
</tr>
<tr>
<td>${LongDate}</td>
<td>Current date. (Long Date format)</td>
</tr>
<tr>
<td>${LocalMonthName}</td>
<td>Current month name in the local language.</td>
</tr>
<tr>
<td>${LongTime}</td>
<td>Current Time. (Long Time format)</td>
</tr>
<tr>
<td>${M}</td>
<td>Current numeric month</td>
</tr>
<tr>
<td>${MM}</td>
<td>Current month. Two digit number, zero padded.</td>
</tr>
<tr>
<td>${MMM}</td>
<td>Current month. Three character abbreviation.</td>
</tr>
<tr>
<td>${MediumDate}</td>
<td>Current date. (Medium Date format)</td>
</tr>
<tr>
<td>${Minute}</td>
<td>Current minute. Two digit format, zero padded.</td>
</tr>
<tr>
<td>${Month}</td>
<td>Full name of the current month</td>
</tr>
<tr>
<td>${N}</td>
<td>Current month and day</td>
</tr>
<tr>
<td>${S}</td>
<td>Current second.</td>
</tr>
<tr>
<td>${Second}</td>
<td>Current second. Two digit format, zero padded.</td>
</tr>
</tbody>
</table>
### Syslog Date/Time Variable

<table>
<thead>
<tr>
<th>Syslog Date/Time Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>${Time}</td>
<td>Current Time. (Short Time format)</td>
</tr>
<tr>
<td>${Year2}</td>
<td>Two digit year</td>
</tr>
<tr>
<td>${Year}</td>
<td>Four digit year</td>
</tr>
</tbody>
</table>

Other Syslog variables

<table>
<thead>
<tr>
<th>Syslog Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>${Application}</td>
<td>SolarWinds application information</td>
</tr>
<tr>
<td>${Copyright}</td>
<td>Copyright information</td>
</tr>
<tr>
<td>${DNS}</td>
<td>Fully qualified node name</td>
</tr>
<tr>
<td>${Hostname}</td>
<td>Host name of the device triggering the alert</td>
</tr>
<tr>
<td>${IP_Address}</td>
<td>IP address of device triggering alert</td>
</tr>
<tr>
<td>${Message}</td>
<td>Status of device triggering alert</td>
</tr>
<tr>
<td>${MessageType}</td>
<td>The name of the triggered alert</td>
</tr>
<tr>
<td>${Severity}</td>
<td>A network health score indicating node states as follows:</td>
</tr>
<tr>
<td></td>
<td>INTERFACE_UNKNOWN = 1</td>
</tr>
<tr>
<td></td>
<td>INTERFACE_WARNING = 1</td>
</tr>
<tr>
<td></td>
<td>INTERFACE_DOWN = 1000</td>
</tr>
<tr>
<td></td>
<td>NODE_UNKNOWN = 1000000</td>
</tr>
<tr>
<td></td>
<td>NODE_WARNING = 1000000</td>
</tr>
<tr>
<td></td>
<td>NODE_DOWN = 1000000000</td>
</tr>
</tbody>
</table>

The Up score for Nodes and Interfaces is zero.

<table>
<thead>
<tr>
<th>Syslog Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>${Version}</td>
<td>Version of the SolarWinds software package</td>
</tr>
</tbody>
</table>

### Trap alert variables

The following variables can be used in trap alert messages with the Orion Trap Server. Each variable must begin with a dollar sign and be enclosed in curly braces as, for example, ${>VariableName>}. 
Trap alerts may also use any valid node variable.
Trap date and time variables
<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>${\text{AbbreviatedDOW}}$</td>
<td>Current day of the week. Three character abbreviation.</td>
</tr>
<tr>
<td>${\text{AbbreviatedMonth}}$</td>
<td>Current month of the year. Three character abbreviation.</td>
</tr>
<tr>
<td>${\text{AMPM}}$</td>
<td>AM or PM corresponding to current time (before or after noon)</td>
</tr>
<tr>
<td>${D}$</td>
<td>Current day of the month</td>
</tr>
<tr>
<td>${DD}$</td>
<td>Current day of the month (two digit number, zero padded)</td>
</tr>
<tr>
<td>${Date}$</td>
<td>Current date. (MM/DD/YYYY format)</td>
</tr>
<tr>
<td>${DateTime}$</td>
<td>Current date and time. (MM/DD/YYYY HH:MM format)</td>
</tr>
<tr>
<td>${Day}$</td>
<td>Current day of the month</td>
</tr>
<tr>
<td>${DayOfWeek}$</td>
<td>Current day of the week.</td>
</tr>
<tr>
<td>${DayOfYear}$</td>
<td>Numeric day of the year</td>
</tr>
<tr>
<td>${H}$</td>
<td>Current hour</td>
</tr>
<tr>
<td>${HH}$</td>
<td>Current hour. Two digit format, zero padded.</td>
</tr>
<tr>
<td>${Hour}$</td>
<td>Current hour. 24-hour format</td>
</tr>
<tr>
<td>${LocalDOW}$</td>
<td>Current day of the week. Localized language format.</td>
</tr>
<tr>
<td>${LongDate}$</td>
<td>Current date. (DAY NAME, MONTH DAY, YEAR format)</td>
</tr>
<tr>
<td>${LongTime}$</td>
<td>Current Time. (HH:MM:SS AM/PM format)</td>
</tr>
<tr>
<td>${M}$</td>
<td>Current numeric month</td>
</tr>
<tr>
<td>${MM}$</td>
<td>Current month. Two digit number, zero padded.</td>
</tr>
<tr>
<td>${MMM}$</td>
<td>Current month. Three character abbreviation.</td>
</tr>
<tr>
<td>${MMMM}$</td>
<td>Full name of the current month</td>
</tr>
<tr>
<td>${MediumDate}$</td>
<td>Current date. (DD-MMM-YY format)</td>
</tr>
<tr>
<td>${MediumTime}$</td>
<td>Current time. (HH:MM AM/PM format)</td>
</tr>
<tr>
<td>${Minute}$</td>
<td>Current minute. Two digit format, zero padded.</td>
</tr>
<tr>
<td>${MonthName}$</td>
<td>Full name of the current month</td>
</tr>
<tr>
<td>${S}$</td>
<td>Current second.</td>
</tr>
</tbody>
</table>
### Trap Date/Time Variable Description

<table>
<thead>
<tr>
<th>Trap Date/Time Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>${Second}</td>
<td>Current second. Two digit format, zero padded.</td>
</tr>
<tr>
<td>${Time}</td>
<td>Current Time. (HH:MM format)</td>
</tr>
<tr>
<td>${Year}</td>
<td>Four digit year</td>
</tr>
<tr>
<td>${Year2}</td>
<td>Two digit year</td>
</tr>
</tbody>
</table>

### Other Trap Variables

<table>
<thead>
<tr>
<th>Trap Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>${Application}</td>
<td>SolarWinds application information</td>
</tr>
<tr>
<td>${Community}</td>
<td>Node community string</td>
</tr>
<tr>
<td>${Copyright}</td>
<td>Copyright information</td>
</tr>
<tr>
<td>${DNS}</td>
<td>Fully qualified node name</td>
</tr>
<tr>
<td>${Hostname}</td>
<td>Host name of the device triggering the trap</td>
</tr>
<tr>
<td>${IP_Address}</td>
<td>IP address of device triggering alert</td>
</tr>
<tr>
<td>${Message}</td>
<td>Message sent with triggered trap and displayed in Trap Details field of Trap Viewer</td>
</tr>
<tr>
<td>${MessageType}</td>
<td>Name or type of trap triggered</td>
</tr>
<tr>
<td>${Raw}</td>
<td>Raw numerical values for properties sent in the corresponding incoming trap.</td>
</tr>
<tr>
<td>${RawValue}</td>
<td>Raw numerical values for properties sent in the corresponding incoming trap. The same as ${Raw}.</td>
</tr>
<tr>
<td>${vbData1}</td>
<td>Trap variable binding value</td>
</tr>
<tr>
<td>${vbName1}</td>
<td>Trap variable binding name</td>
</tr>
</tbody>
</table>
Create and view reports

SolarWinds provides predefined reports for each Orion Platform product. Use the web-based interface to customize these predefined reports and create your own reports.

You must use the Orion Report Writer to maintain legacy reports created with Orion Report Writer.

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.

Manage reports in the Orion Web Console

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

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

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

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

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. You can also modify the layout.
   a. Click Add content to add resources to your report. For more information, see Add content to a web-based 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](image)

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...
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.
     
     **This is the most straightforward selection method, and recommended for new users. It is also the preferred method for relatively permanent network objects.**
   - Dynamic Query Builder - use to select objects based on object properties.
     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.
     
     **This is the preferred selection method for groups of objects of a specified type that may change over time. "All Cisco nodes in Austin" is an example of a group best defined using the Dynamic Query Builder.**
   - Advanced DataBase Query (SQL, SWQL) - only use if you are comfortable querying your SolarWinds database directly using SQL or SWQL.
     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.

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.
   
   Click Add Time to select additional dates and times.

   - To delay when the report runs, select Specific Date in the Starting On field, and then select the date and time when you want the schedule to start.
   - To stop the report from running automatically, select Ending On, and then select the date and time when you want the schedule to end.

4. Click Add Frequency.
5. Click Add Action, and select the action (Email, Print, or Save to Disk) to be executed on the configured schedule.
6. Click Configure Action.
   - For email actions, enter the recipients, the message, and the SMTP server.
     Select Include Report’s URL to allow recipients to access the report remotely.
   - For print actions, enter the Windows credentials necessary to access your printer, the printer, and print settings.
   - For save actions, enter the location you want to save the report to, the credentials in domain\username format, and the file type you want to save the report as. The location must be accessible from the Orion Web Console server.

7. Click Add Action.

The action is added to the Actions list. You can add multiple actions.

Create and assign report schedules in Report Manager

The Report Manager provides a list of all reports that have been set up for your SolarWinds Orion web-based reports. You can create schedules and assign reports to schedules.

Create a report schedule

1. Select a report.
2. Click on Schedule Report > Create New Schedule to display the Properties view.
3. Add additional reports to this schedule by clicking Assign another Report.
4. Click Assign Webpage to include a snapshot of the selected website, and enter the URL in the field displayed. You can assign multiple webpages.
   - Start each URL with http:// or https://.
5. Expand Advanced Settings to specify a user account so that its limitations are applied to this schedule. Click Another User, and enter the User name or Account ID and Password.
6. Click Next to display the Frequency view.
7. Click Add Frequency, and then select when you want to run the report.
   - Click Add Time to select additional dates and times.
   - To delay when the report runs, select Specific Date in the Starting On field, and then select the date and time when you want the schedule to start.
   - To stop the report from running automatically, select Ending On, and then select the date and time when you want the schedule to end.
8. Click Add Frequency, and then click Next to display the Actions view.
9. Click Add Action, and select the action (Email, Print, or Save to Disk) to be executed on the configured schedule.
10. Click Configure Action.
   - For email actions, enter the recipients, the message, and the SMTP server. Select Include Report's URL to allow recipients to access the report remotely.
   - For print actions, enter the Windows credentials necessary to access your printer, the printer, and print settings.
   - For save actions, enter the location you want to save the report to, the credentials in domain\username format, and the file type you want to save the report as. The location must be accessible from the Orion Web Console server.

11. Click Add Action.
12. Click Next to display the Summary view.
13. If the schedule summary is correct, click Create Schedule.

The schedule is displayed in the Schedule Manager.

Assign a report to a schedule or multiple schedules

1. Select one or more reports.
2. Click Schedule Report > Assign Existing Schedule.
3. Select the schedule or schedules in the Assign existing schedule list and clicking Assign Schedule(s) to confirm that you want to assign the report.

Schedule 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.

Report Writer is a legacy feature that you can access on your Orion server.

<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>
</tbody>
</table>

page 326
<table>
<thead>
<tr>
<th>Supported Formats</th>
<th>Orion Web Console</th>
<th>Report Writer</th>
</tr>
</thead>
<tbody>
<tr>
<td>Excel</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>PDF</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>HTML and MHTML</td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>Image (BMP, GIF, JPG, PNG, etc.)</td>
<td></td>
<td>✓</td>
</tr>
</tbody>
</table>

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.

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:

\[ \text{Priority} = \text{Facility} \times 8 + \text{Severity} \]
Syslog facilities

The facility value indicates which machine process created the message. The Syslog protocol was originally written on BSD Unix, so Facilities reflect the names of UNIX processes and daemons.

If you are receiving messages from a UNIX system, consider using the User Facility as your first choice. Local0 through Local7 are not used by UNIX and are traditionally used by networking equipment. Cisco routers, for example, use Local6 or Local7.

<table>
<thead>
<tr>
<th>NUMBER</th>
<th>SOURCE</th>
<th>NUMBER</th>
<th>SOURCE</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>kernel messages</td>
<td>12</td>
<td>NTP subsystem</td>
</tr>
<tr>
<td>1</td>
<td>user-level messages</td>
<td>13</td>
<td>log audit</td>
</tr>
<tr>
<td>2</td>
<td>mail system</td>
<td>14</td>
<td>log alert</td>
</tr>
<tr>
<td>3</td>
<td>system daemons</td>
<td>15</td>
<td>clock daemon</td>
</tr>
<tr>
<td>4</td>
<td>security/authorization messages</td>
<td>16</td>
<td>local use 0 (local0)</td>
</tr>
<tr>
<td>5</td>
<td>messages generated internally by Syslog</td>
<td>17</td>
<td>local use 1 (local1)</td>
</tr>
<tr>
<td>6</td>
<td>line printer subsystem</td>
<td>18</td>
<td>local use 2 (local2)</td>
</tr>
<tr>
<td>7</td>
<td>network news subsystem</td>
<td>19</td>
<td>local use 2 (local3)</td>
</tr>
<tr>
<td>8</td>
<td>UUCP subsystem</td>
<td>20</td>
<td>local use 2 (local4)</td>
</tr>
<tr>
<td>9</td>
<td>clock daemon</td>
<td>21</td>
<td>local use 2 (local5)</td>
</tr>
<tr>
<td>10</td>
<td>security/authorization messages</td>
<td>22</td>
<td>local use 2 (local6)</td>
</tr>
<tr>
<td>11</td>
<td>FTP daemon</td>
<td>23</td>
<td>local use 2 (local7)</td>
</tr>
</tbody>
</table>

Syslog severities

The following table provides a list of Syslog severity levels with descriptions and suggested actions for each.
<table>
<thead>
<tr>
<th>Number</th>
<th>Severity</th>
<th>Suggested Actions</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>Emergency</td>
<td>A &quot;panic&quot; condition affecting multiple applications, servers, or sites. System is unusable. Notify all technical staff on call.</td>
</tr>
<tr>
<td>1</td>
<td>Alert</td>
<td>A condition requiring immediate correction, for example, the loss of a backup ISP connection. Notify staff who can fix the problem.</td>
</tr>
<tr>
<td>2</td>
<td>Critical</td>
<td>A condition requiring immediate correction or indicating a failure in a primary system, for example, a loss of a primary ISP connection. Fix CRITICAL issues before ALERT-level problems.</td>
</tr>
<tr>
<td>3</td>
<td>Error</td>
<td>Non-urgent failures. Notify developers or administrators as errors must be resolved within a given time.</td>
</tr>
<tr>
<td>4</td>
<td>Warning</td>
<td>Warning messages are not errors, but they indicate that an error will occur if required action is not taken. An example is a file system that is 85% full. Each item must be resolved within a given time.</td>
</tr>
<tr>
<td>5</td>
<td>Notice</td>
<td>Events that are unusual but are not error conditions. These items might be summarized in an email to developers or administrators to spot potential problems. No immediate action is required.</td>
</tr>
<tr>
<td>6</td>
<td>Informational</td>
<td>Normal operational messages. These may be harvested for network maintenance functions like reporting and throughput measurement. No action is required.</td>
</tr>
<tr>
<td>7</td>
<td>Debug</td>
<td>Information useful to developers for debugging an application. This information is not useful during operations.</td>
</tr>
</tbody>
</table>

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.
   - 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.

ℹ️ 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.

ℹ️ 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.

ℹ️ 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.

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.

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.
   - To designate a specific IP address or hostname as the Syslog source, select Retain the Original Source Address of the Message, select Use a Fixed Source IP Address, and provide the IP address or hostname.
   - To keep the original IP address of the syslog source device, select Retain the Original Source Address of the Message, select Spoof Network Packet, and select the Network Adapter.
4. Click OK to complete the configuration.

You have defined the destination, port for sending the syslog message, and the source IP of the device in the syslog message used in the alert action.

**Syslog alert actions**

**Discard the Syslog Message**

Delete unwanted Syslog messages sent to the Syslog server.

**Tag the Syslog Message**

Add a custom tag to received Syslog messages. Ensure you include the Tag column in the viewer when assigning a tag.

**Modify the Syslog Message**

Modify the severity, facility, type, or contents of a Syslog message.
Log the Message to a file

Specify a file and a series of variables with which to tag Syslog messages sent to the file. Ensure you have already created the log file you want to use. The alert cannot create a file.

Windows Event Log

Write a message to local or remote Windows Event Logs.

Forward the Syslog message

Specify the IP address or hostname and the port to forward a Syslog event.

Send a new Syslog message

Trigger a new Syslog message, sent to a specific IP address or hostname, on a specific port, with a customizable severity, facility, and message.

Send an SNMP Trap

Send a trap to an IP address following a specific trap template and using a specific SNMP community string.

Play a sound

Play a sound when a matching Syslog message is received.

Text to Speech output

Define the speech engine, speed, pitch, volume, and message to read.

Execute an external program

Allows you to specify an external program to launch using a batch file. This action is used when creating real-time change notifications in Orion.

Execute an external VB Script

Launch a VB Script using the selected script interpreter engine and a saved script file.

Send a Windows Net Message

Send a net message either to a specific computer or to an entire domain or work group.

Send an E-mail / Page

Send an email from a specified account to a specified address, using a specific SMTP server, and containing a customizable subject and message.

Stop Processing Syslog Rules

Stops the processing of Syslog rules for the matching Syslog message.
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

You can also search trap messages using the Global Search feature. For more information, see Search syslogs, traps and objects monitored in the Orion Web Console globally.

1. Log in 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.
- Click Start > All Programs > SolarWinds Orion > Syslog and SNMP Traps > Trap Viewer.
- Click View > Current Traps.
- Click a column header to order listed traps by the selected trap characteristic.
- 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.

   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.

   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:
The following table describes the OIDs section of the Orion Generic Alert trap template. This is the section you modify to display the information you want in your trap messages.

<table>
<thead>
<tr>
<th>TEMPLATE OID LINE</th>
<th>INFORMATION RETURNED</th>
</tr>
</thead>
<tbody>
<tr>
<td>OID: OID=&quot;1.3.6.1.2.1.1.3.0&quot; MIB=&quot;RFC1213-MIB&quot; Name=&quot;sysUpTime.0&quot; Value=&quot;0&quot; DataType=&quot;67&quot; ValueName=&quot;0&quot; HexValue=&quot;&quot;</td>
<td>This line displays how long the device has been up.</td>
</tr>
<tr>
<td>OID: OID=&quot;1.3.6.1.6.3.1.1.4.3.0&quot; MIB=&quot;SNMPv2-MIB&quot; Name=&quot;snmpTrapEnterprise.0&quot; Value=&quot;1.3.6.1.4.1.11307&quot; DataType=&quot;6&quot; ValueName=&quot;enterprises.11307&quot; HexValue=&quot;&quot;</td>
<td>This line displays the enterprise associated with the trap.</td>
</tr>
<tr>
<td>OID: OID=&quot;1.3.6.1.4.1.11307.10.1&quot; MIB=&quot;SNMPv2-SMI&quot; Name=&quot;enterprises.11307.10.1&quot; Value=&quot;${AlertMessage}&quot; DataType=&quot;4&quot; ValueName=&quot;${AlertMessage}&quot; HexValue=&quot;&quot;</td>
<td>When the template is used in an alert, this line displays the alert message associated with the triggered alert.</td>
</tr>
</tbody>
</table>

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

### Additional Polling Engine and Web Console

Installing additional pollers and Web Consoles help you extend your Orion User Device Tracker (UDT) implementation. You can install additional polling engines to aid you in load balancing and configure additional websites to ensure redundant access through more than one web server. By sharing the same database, you can also share a unified user interface, making the addition of polling engines transparent to your staff.

The following topics provide descriptions and installation procedures for adding polling engines and websites. These components are licensed and purchased separately from your main Orion User Device Tracker install and require the installation of the SolarWinds UDT Additional Polling Engine. For more information about purchasing licenses, contact your sales representative (sales@solarwinds.com) or customer service.

- Additional Polling Engine Guidelines
- Additional Polling Engine System Requirements
- Use additional polling engines to balance polling
- Use an Additional Web Server
**Additional Polling Engine Guidelines**

The following table provides guidance for SolarWinds NPM installations that use scalability engines to expand monitoring capacity.

<table>
<thead>
<tr>
<th><strong>NETWORK PERFORMANCE MONITOR (NPM) SCALABILITY ENGINE GUIDELINES</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Stackable Pollers Available?</strong></td>
</tr>
<tr>
<td><strong>Poller Remotability Available?</strong></td>
</tr>
</tbody>
</table>
| **Primary Poller Limits** | ~12k elements at standard polling frequencies:  
  - Node and interface up/down: 2 minutes/poll  
  - Node statistics: 10 minutes/poll  
  - Interface statistics: 9 minutes/poll  
  25-50 concurrent Orion Web Console users  
  SNMP Traps: ~500 messages per second (~1.8 million messages/hr)  
  Syslog: 700-1k messages/second (2.5 - 3.6 million messages/hr)  
  Note: If you are monitoring more than ~100,000 elements, consider using SolarWinds Enterprise Operations Console. |
| **Scalability Options** | One polling engine for every ~12k elements  
  Maximum of 100k elements per primary SolarWinds NPM server (i.e. 1 NPM server + 9 APEs). For more information about licensing, see "How is SolarWinds NPM licensed?" |
| **WAN and/or Bandwidth Considerations** | Minimal monitoring traffic is sent between the primary NPM server and any APEs that are connected over a WAN. Most traffic related to monitoring is between an APE and the SolarWinds database. |

**Additional Polling Engine System Requirements**

System requirements for an Additional Polling Engine are the same as system requirements for your Main Polling Engine.
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.

<table>
<thead>
<tr>
<th>PORT</th>
<th>PROTOCOL</th>
<th>SERVICE/PROCESS</th>
<th>DIRECTION</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>1433</td>
<td>TCP</td>
<td>SolarWinds Collector Service</td>
<td>Outbound</td>
<td>The port used for communication between the APE and the Orion database.</td>
</tr>
<tr>
<td>1801</td>
<td>TCP</td>
<td>Message Queuing WCF</td>
<td>Inbound</td>
<td>The port used for MSMQ messaging from the Orion Web Console to the Additional Polling Engine.</td>
</tr>
<tr>
<td>5671</td>
<td>TCP</td>
<td>RabbitMQ</td>
<td>Bidirectional</td>
<td>The port used for SSL-encrypted RabbitMQ messaging from the Orion Web Console to the Additional Polling Engine.</td>
</tr>
<tr>
<td>17777</td>
<td>TCP</td>
<td>SolarWinds Information Service</td>
<td>Bidirectional</td>
<td>The port used for communication between the Additional Polling Engine and the Orion Web Console.</td>
</tr>
</tbody>
</table>

Install an Additional Polling Engine

1. Click Settings > All Settings > Polling Engines.
2. Click Download Installer Now.
3. Run the installer on the computer you want to use as your additional polling engine or website.
4. Enter the main Orion server credentials.
5. Choose either Additional Polling Engine or Additional Website. If you want to install a backup server for High Availability, view SolarWinds High Availability requirements first. The packages are downloaded from the main Orion server.

6. Follow the onscreen instructions to complete your installation and configuration. The Additional Polling Engine or Additional Web Server is installed, together with all hotfixes for products released later than September 2016.

For example, when installing or upgrading to SAM 6.3 and IPAM 4.3.2, any hotfixes for SAM 6.3 are installed. You must install the hotfix for IPAM manually.

Repeat installing on all Additional Polling Engines and then on all Additional Web Servers in your environment.

Activate the Additional Polling Engine licenses.

Activate Additional Polling Engine licenses

1. In the Orion Web Console, click Settings > All Settings > License Manager.
2. Locate the license in the License Manager, click Activate, and complete the activation. The Additional Polling Engine license is activated. Review the polling engine it is assigned to, and re-assign the license if necessary.

When finished, specify nodes to be polled by the Additional Polling Engine.

Use an Additional Web Server

With an Additional Web Server, you can access the Orion Web Console remotely, from a location other than your primary Orion server. You can view the primary Orion Web Console without deploying an entire Orion installation or excessively taxing the resources of your primary SolarWinds server.

Requirements

- Matching version of Additional Web Server and your product installed on the main polling engine
- 64-bit operating system:
  - Windows Server 2008 R2 SP1 or
  - Windows Server 2012 and 2012 R2
  - Windows Server 2016
- Matching version of .NET 4.5 installed on the main polling engine
- Minimum hardware requirements
  - CPU speed: Quad core processor, 2.5 GHz or better
  - Hard drive space: 2.5 GB minimum
  - Memory: 4 GB minimum, 8 GB recommended

A higher number of concurrent users may change the requirements.
Port requirements

<table>
<thead>
<tr>
<th>PORT</th>
<th>PROTOCOL</th>
<th>SERVICE /PROCESS</th>
<th>DIRECTION</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>80</td>
<td>TCP</td>
<td>World Wide Web Publishing Service</td>
<td>Inbound</td>
<td>Default additional web server port. Open the port to enable communication from your computers to the Orion Web Console. If you specify any port other than 80, you must include that port in the URL used to access the web console. For example, if you specify an IP address of 192.168.0.3 and port 8080, the URL used to access the web console is <a href="http://192.168.0.3:8080">http://192.168.0.3:8080</a>.</td>
</tr>
<tr>
<td>1433</td>
<td>TCP</td>
<td>SolarWinds Collector Service</td>
<td>Outbound</td>
<td>The port used for communication between the SolarWinds server and the SQL Server. Open the port from your Orion Web Console to the SQL Server.</td>
</tr>
<tr>
<td>1801</td>
<td>TCP</td>
<td>Message queuing</td>
<td>Outbound</td>
<td>The port used for MSMQ messaging from the Additional Web Server to the Main Polling Engine.</td>
</tr>
<tr>
<td>5671</td>
<td>TCP</td>
<td>RabbitMQ</td>
<td>Outbound</td>
<td>The port used for SSL-encrypted RabbitMQ messaging from the Additional Web Server to the Additional Polling Engine.</td>
</tr>
<tr>
<td>17777</td>
<td>TCP</td>
<td>SolarWinds Collector Service</td>
<td>Outbound</td>
<td>Orion module traffic. Open the port to enable communication from your polling engine to the web server, and from the web server to your polling engine.</td>
</tr>
</tbody>
</table>

Before you begin, prepare:

- Hostname or IP address of your main polling engine
- Orion Web Console user name and password with administrative rights
- To use SQL authentication, prepare the SQL server credentials
- SQL database name

Download and install an Additional Web Server

1. In the main Orion Web Console, click Settings > All Settings > Web Console Settings.
2. Click Download Installer Now.
3. Run the installer on the computer you want to use as your Additional Web Server.
4. Enter the main Orion server Orion server credentials.
5. Choose Additional Website.
The packages are downloaded from the main Orion server.

6. Follow the onscreen instructions to complete your installation.

Configure the Additional Web Server

1. If the Configuration Wizard does not start automatically, click Start > All Programs > SolarWinds Orion > Configuration and Auto-Discovery > Configuration Wizard.
2. Click Next on the Welcome tab of the Configuration Wizard.
3. Select or type the SQL Server used by your primary Orion server.
4. If you are using Windows NT Integrated Security, select Use Windows Authentication, and click Next.
5. If you are using a SQL Server login and password, complete the following steps:
   a. Select Use SQL Server Authentication.
   b. Provide your Login and Password, and click Next.
6. Select or type the Database Name that is connected to your Orion server, and click Next.
7. If a dialog appears that says that multiple polling engines have been detected, click OK to continue database upgrade/verification.
8. When the database structure validation completes, click Next.
9. Specify a SQL account User Name and Password for the polling engine and web site to use to access the database, and click Continue.
   If you already have a SQL account, you can specify the credentials for that account.
10. To set up the web console, click Next on the Create Website tab, and then complete the following procedure:
    a. Specify the IP Address of the local server on which you are installing the new web-only interface.
    b. Specify the TCP Port through which you want to access the web console.
       If you specify any port other than 80, you must specify that port in the URL that is used to access the web console. For example, if you specify an IP address of 192.168.0.3 and port 8080, your URL is http://192.168.0.3:8080.
    c. Specify the volume and folder in which you want to install the web console files, and then click Continue.
11. If you are asked to overwrite an existing website, click Yes.
12. When the new web console has been created, click Continue.

You can now use the additional Orion Web Console to access your Orion Platform product.
Activate your license

- To evaluate an Additional Web Server, just install it.
- To activate a production license for an Additional Web Server, log in to the Orion Web Console on your main polling engine, and activate the license.

Global Search View

The Global Search view allows you to search for information in your syslogs, traps, events, alerts, and for information about nodes, interfaces, and volumes monitored in NPM.

Simply enter an appropriate string into the global search field and click Search. For more information, see Search syslogs, traps and objects monitored in the Orion Web Console globally.

What else can I do in the Global Search View?

- Specify the search by a query, using the auto-suggest function. For more information, see Orion Global Search query syntax and Auto-completing queries and properties in Orion Global Search.
- Specify the time period relevant for the search. For more information, see Adjust the time period.
- Refine the search with available default filters. For more information, see Refining Global Search with available filters.
- Add properties to search for. For more information, see Adding more properties for filtering search results.
- Remove a property used in the current search.
  Locate the property which you want to remove from the search below the search line and click x to remove it.
- Display more information about results.
  - To display information about an object in the results list, position the cursor over it. A tooltip displays with relevant information about the object. For nodes, relevant details might include the status, polling IP address, machine type, average response time, packet loss, and CPU load.
  - To view events and alerts concerning the object, click the + before the item in the results list.

Search syslogs, traps and objects monitored in the Orion Web Console globally

SolarWinds NPM 11.5 introduces the technical preview of Orion Global Search. This feature provides a global search interface in the Orion Web Console and allows you to search for information contained in traps, syslogs, alerts, events and in the database of objects monitored in SolarWinds Orion.

This feature is Technical Preview. Any functionality in this feature may be subject to change upon official release. This feature is not fully supported at this time and should be used carefully.
Install Orion Global Search

1. Go to your installation folder, run the Orion Global Search executable, and complete the installation.
   By default, you can find the executable using the following path:
   `<ProgramData Folder>\Solarwinds\Installers\OGSinstaller.msi`

2. Run the Configuration Wizard.

   If you want to also search through historical syslogs and traps, select the option to index existing entries.

   If historical syslogs and traps are not relevant for you, you do not have to index syslogs and traps.

   Indexing runs in the background, and can be time-consuming, depending on the amount of data being indexed.

Uninstall Orion Global Search

- Go to Program Features (for example, navigate through Start > Control Panel > Program Features), right-click SolarWinds Orion Global Search, and select Uninstall.

Search with Orion Global Search

- When you are notified about an event or issue, search for textual keywords from the notification, such as a user name, application impacted, IP address, remote site name, performance counters or error message.

  **Example Use Case**

  When a user reports poor connectivity, you can search for his computer name or IP address.

Execute a global search

1. Log in to the Orion Web Console.

2. Enter a keyword into the Search Orion box in the top right corner of the Orion Web Console, and click the Search icon.
   This will open the results of the basic search in the Global Search view.

   - Orion Global Search performs a full text search of the string you enter into the search field. If you want to search for a certain sequence of words, enclose the phrase by quotation marks (" ").
   - You can also use auto-complete of search queries and properties.
3. Refine the search to narrow down items you are interested in.

   **Adjust the time period**
   - To prolong or shorten the time period which is relevant for your search, select the appropriate item in the Time Period list below the search line.
   - To specify a precise time period, click the links next to From and To items to define start and end date of the period you are interested in.

   **Refine filters**
   - Refine the search with filters available by default.

   **Add filters**
   - Add more filters.

   **Remove filters**
   - Remove an already applied filter.
   - Locate the property which you want to remove from the search below the search line and click x to remove it.

4. Display information about individual search result items:

   - To display information about an object in the results list, position the cursor over it. A tooltip displays with relevant information about the object. For nodes, relevant details might include the status, polling IP address, machine type, average response time, packet loss, and CPU load.
   - To view events and alerts concerning the object, click the + before the item in the results list.

**Orion Global Search query syntax**

Orion Global Search allows you to specify the information you are looking for by entering a query into the search box.

Supported queries consist of database field names (also called properties) and database field values. These can be further connected by logical operators.

The Orion Global Search field requires the following syntax:

```
[database field name]:[field value] [LOGICAL OPERATOR] [database field name]:[field value]
```

Example:

```
```

This query returns all Cisco nodes that are down.

For more information about automatic suggestions provided for any input into the global search field, see [Auto-completing queries and properties in Orion Global Search](#).

**Auto-completing queries and properties in Orion Global Search**

Orion Global Search has a powerful auto-complete feature which helps you specify what information you are looking for in logs and NPM. The auto-complete feature suggests available properties and modifiers which you can use to tailor a query to suit your needs.
Auto-suggestions include:

- Field names from the Orion database. These are object properties that can be used to design a search query for Orion Global Search.
- Logical operators that allow you to combine multiple properties, such as AND, OR, or NOT.

Auto-suggestions only include available properties, not values available for them. To be able to use auto-suggestions, you need to add an appropriate value to limit the search results by.

To specify a search using auto-complete:

1. Log on to the Orion Web Console and execute an Orion Global Search.
2. Now in the Global Search view, start typing a value or property you want to search for. A list of suggestions will display below the search field.
3. Use the arrow keys to move in the list and press <Enter> to add the selected suggestion into the search field.
4. Fill in the required field value to be searched for.
5. If you want to further specify your query, use a logical operator, such as AND. Then you can add another field name and value that you are interested in finding.

Refining Global Search with available filters

The Refine Further section in the Orion Global Search view provides default filtering options based on the keyword you entered. You can find their properties and their values available in the results of the current search.

In most cases, default filters include the object type (for example Nodes, Interfaces, Components, SqlServerApplication, and so on), and their status (for example Disabled, Down, Up, Unknown).

To refine search results:

1. Log into the Orion Web Console and execute a global search.
2. In the Refine Search section, select the items which you want to have in the results.
3. Click Update results.

The results will now only show items corresponding with the selected properties. Applied properties display below the search field.

Removing a property filter

If you have refined your filter too much, or need to apply a different approach to filtering, you can remove properties used for filtering.

To remove a filter, locate the filter below the search field, and click x for property filters that you do not want to apply on the search results any more.
Adding more properties for filtering search results

You can further limit Orion Global Search results to display information related only to objects with specified properties. This can be done by adding a filter property and specifying values which should be included in the results.

For example, you might want to see log and NPM information only for loopback interfaces.

1. Log on to the Orion Web Console and execute an Orion Global search.
2. Now in the Global Search view, click Add Filter Property.
3. Select the appropriate Orion Object in the Available Columns list, and then select the required property in the Database Column name table.
   Example: To search for loopback interfaces information, select Interface in the Orion Object list, and then select Interface Type Description.
4. Click Add Filter Property.
   The selected property with available values will display in the Refine Further area.
   Example: If you selected Interface Type Description, it will display in the Refine Further area, with all available values, such as loopback, Ethernet, ppp, and so on.
5. Select one or more property values by which you want to limit the search results, and then click Update Results.
   Example: If you are interested only in results concerning loopback interfaces, select loopback below Interface Type Description, and update the results.

The selected filters display below the search field. If you want to exclude the selected property from filtering the results again, click x next to the appropriate property.

The Refine Further area displays only the properties and values that are available in your SolarWinds Orion database and in your logs.

Troubleshooting slow Internet connectivity with Orion Global Search

This feature is Technical Preview. Any functionality in this feature may be subject to change upon official release. This feature is not fully supported at this time and should be used carefully.

If an end user notifies you that the connection to the Internet is really slow, you can search for items related to this user with Orion Global Search to address this issue.

You need to find any occurrence of the user's computer in any of your log files, such as SNMP syslog and traps.

You also need to find out the relationship of the end user log entry occurrences to your network monitoring system (NPM) and to network devices, such as routers and switches and whether they were impacted at the time of the incident on the network.

As a result, you expect to find the cause of the issue either in a log file, or deduce what the cause is from the correlation of log messages for the particular end user and historical data provided by NPM, such as router availability status, port utilization, latency, packet loss, restart of a device, flapping routes, and so on.
Once you identify what caused the issue, you can take measures to resolve it.

To troubleshoot poor Internet connectivity with Orion Global Search:

1. Log into the Orion Web Console.
2. Enter the user's computer name or IP address into the Orion Global Search field and click Search.
3. The Global Search Results view will display any occurrence of the computer in your Syslogs, traps, and in NPM in chronological order.
4. If necessary, adjust the default time period to cover the time the user is complaining about. Select the appropriate time period in the drop-down list above, or click the From and To links to specify the time in more detail.
5. Review the log and NPM data together and try to find a dependency between them to identify the cause of the issue.
Troubleshooting

The following topics address some issues that users of UDT have encountered and resolved.

- Check device compatibility
- Scan a device
- Analyze test results
- Node discovery completely fails
- Node discovery fails for some devices
- UDT missing user data
- UDT polling spikes CPU on target device(s)
- Wrong hostname reported for endpoint
- Wrong IP address reported for endpoint
- Wrong MAC address reported for endpoint
- Wrong connection type reported for endpoint
- Wrong VLAN reported for endpoint
- No DNS data for a device
- No Layer 3 data for a device
- No Layer 2 data for a device
- No user data retrieved via WMI (Windows Server 2003)
- UDT not receiving user data from domain controllers
- Add a deleted port back into UDT
- Orion platform components

Check device compatibility

UDT Compatibility Checker is a standalone application that, like UDT, polls selected devices for data but presents the results in a raw format, facilitating investigation when something is not the way customer expects. This tool is located in the installation subdirectory.

Scanning a Device

Use these steps to poll a UDT device.
1. Open the UDT Compatibility Check (by default, "<installed path>\SolarWinds\Orion\UDT").
2. Click New. This opens a wizard that guides you and where you configure what device to poll and what data to collect.
3. If you select Orion Node, provide the requested information.
   - Enter credentials you use to login on the UDT server.
   - Select the Orion Node.
   - Select a connection type.
4. If you select Manual, enter the IP address of the device, the credential type (SNMPv1, SNMPv2c, SNMPv3, or REL), the connection port, and the device vendor.
   - For SNMPv1 and SNMPv2, enter the community string.
   - For SNMPv3, enter the user name and context.
   - For REL, enter the user name and password to access the remote event log.
5. Click Next.
6. Select the test targets for this session and then click Finish.

Results display in the session data window.

Analyze test results

After you scan a device, the following sections guide you in understanding the results for the different test targets.

Discovery, Layer 2, Layer 3, and DNS

In the Session Data menu you can find some items with Job Statistics suffix. If you select one of those, it will display an overview of the selected job where you can verify how the device responds to UDT requests for specific OIDs (Type and Status) and how long it takes (Duration). This way you can easily identify if the device is currently not supported by UDT or it timeouts on some requests.

The other items in the Session Data menu give detailed information about the selected object (OID) and what data it returned. The item always belongs to the nearest Job Statistics parent above.

Below is a very brief description of some of the objects UDT query to get the data. To get more details and understand what the individual values mean use the Cisco SNMP Object Navigator.

Discovery and Layer 2 Job Statistics

These two jobs query similar OIDs.

Consult these objects about ports (port index, name, ifType, speed, trunk mode etc.) if you think the data UDT displays for the device ports are incorrect.
Consult these objects about endpoints (MAC addresses) and to which ports they are connected if UDT is not displaying a specific endpoint.

- dot1dTpFdbTable
- dot1dBasePortTable

Layer 3 Job Statistics

Consult these objects about endpoints (IP addresses) and their mapping to corresponding MAC addresses to find what the device whose IP address UDT cannot see is returning for the IP-MAC.

- ipNetToMediaTable
- ipNetToPhysicalTable

If the device does not support those objects, UDT cannot get any layer 3 information.

DNS Job

The table shows the IP addresses for discovery and the names to which they resolve.

Node discovery completely fails

Issue: Device discovery fails regardless of the devices selected.

These are the paths to resolving this issue:

- UDT Discovery always runs on main poller even if the nodes are affiliated with additional poller. Make sure the machine where main poller is installed has access to the selected device (try ping etc.),
- Make sure the SNMP requests/responses are not blocked by a firewall.
- Verify that job engine services (JobEngine v2, Collector Polling Controller, Collector Data Processor, Collector Management Agent) are running.
- Check the UDT.Jobs log to see if the discovery job finished successfully or shows an error.
- Check the UDT.BusinessLayer log to see if the discovery job's results were processed successfully or shows an error,
Node Discovery Fails for Some Devices

Issue
Device discovery fails if done for specific devices.

Solution
These are the paths to resolving this issue:

- UDT Discovery runs on the poller the nodes are affiliated with (i.e. it respects main and additional polling engines) since UDT 2.5. Make sure the machine where appropriate poller is installed has access to the selected device (try ping etc.)
- Run UDT Compatibility Checker (discovery target) from machine with the right polling engine against the device and check the results
- Increase Port/Layer3 Discovery Job Timeout (Advanced Settings page)
- Increase SNMP Timeout (Advanced Settings page)

UDT missing user data

Issue: UDT is set up to retrieve user data from domain controllers but no user data is displayed in the UDT web console.

To verify that assigned credentials have sufficient privileges, attempt to re-add the domain controller into UDT.

To verify credential privileges:

1. Click UDT Settings in the web console.
2. Click Manage Domain Controllers under Track Users and Endpoints.
3. Click Add AD Domain Controller.
4. Enter the hostname or IP address.
5. Check Active Directory Domain Controller.
6. Choose your credential from the list.
7. Enter and re-enter the password.
8. Click Test.

If the test succeeds, the credentials are valid for the purposes of retrieving user data from the domain controller. If not, see Managing Active Directory Credentials to edit the credentials or create another set.

UDT Polling Spikes CPU on Target Device(s)

Issue
CPU utilization spikes on a device when UDT polls it.
**Solution**

Try one or more or these things:

- Adjust the SNMP Pacing Delay setting on Advanced settings page (Settings > UDT Settings > Advanced Settings) from 0 to 1 or 1 to 2.
  
  Keep in mind this setting affects all UDT jobs and so may increase the time to complete them.
  
  If possible, set your polling mode to SNMPv1 because some devices do not handle GetBulk requests very well.

- Check the length of the SNMP queue on relevant devices.

**Wrong hostname reported for endpoint**

**Issue:** The data returned for an endpoint has an incorrect hostname.

Keep in mind that the Endpoint Details view displays both current and historical data.

Use nslookup to verify the hostname associated with the IP address.

Connect the relevant network device and verify in the ARP table that the IP address is associated with the correct MAC address.

**Wrong IP address reported for endpoint**

**Issue:** The data returned for an endpoint has incorrect IP address. Since data is being returned we know the Layer 3 job is running.

Keep in mind that the Endpoint Details view displays both current and historical data.

Connect to the relevant network device and check the ARP table to verify that the MAC address for the endpoint is correct.

**Wrong MAC Address Reported for Endpoint**

**Issue**

The data returned for an endpoint has incorrect MAC address. Since data is being returned we know the Layer 2 job is running.

**Solution**

Keep in mind that the Endpoint Details view displays both current and historical data.

Connect to the relevant network device and check the MAC address table; verify that the MAC address for the endpoint is correct.

Check the ARP table to verify that the MAC address for the endpoint is correct.
Wrong connection type reported for endpoint

Issue: The data returned for an endpoint has an incorrect connection type.

Solution

Try these things:

- Verify the endpoint is not connected to a trunk port. (Trunk ports are excluded by design from direct connection reporting.)
- Connect to the relevant network device to which you think the endpoint is actually connected; check the value for the endpoint in the MAC address table.
- Connect to the relevant network device to which UDT says the endpoint is connected; check the MAC address routing table.

Wrong VLAN reported for endpoint

Issue: The data returned for an endpoint has incorrect VLAN information. Since data is being returned we know the Layer 2 job is running.

Connect to the relevant network device and correct any error in its MAC address routing table for the endpoint.

No DNS data for a device

Issue: A device is added to UDT but does not display data (DNS).

Verify that:

- Device supports all relevant OIDs
- Layer 3 job exists for the node (Settings > UDT Settings > Job Status)
- UDT ports are being monitored (Settings > UDT Settings > UDT Port Management page)
- In UDT.Jobs log the job completes successfully; verify job's duration and adjust timeout if necessary (Settings > UDT Settings > Advanced Settings)
- In UDT.BusinessLayer log verify the job's results are processed successfully
- Use nslookup from the UDT server to get DNS information on the device.

No Layer 3 Data for a Device

Issue

A device is added to UDT but doesn't display data (Layer3).

Solution
Verify that:

- Device supports all relevant OIDs
- Layer3 job exists for the node (Settings > UDT Settings > Job Status)
- UDT ports are being monitored (Settings > UDT Settings > UDT Port Management page)
- In UDT.Jobs log the job completes successfully; verify job's duration and adjust timeout if necessary (Settings > UDT Settings > Advanced Settings)
- In UDT.BusinessLayer log verify the job's results are processed successfully
- Connect to the device and verify ARP address table (e.g. sh arp)

No Layer2 Data for a Device

**Issue**

A device is added to UDT but doesn't display data (Layer2).

**Solution**

Verify that: Device supports all relevant OIDs

- Layer2 job exists for the node (Settings > UDT Settings > Job Status)
- UDT ports are being monitored (Settings > UDT Settings > UDT Port Management page)
- In UDT.Jobs log the job completes successfully; verify job's duration and adjust timeout if necessary (Settings > UDT Settings > Advanced Settings)
- In UDT.BusinessLayer log verify the job's results are processed successfully
- Connect to the device and verify MAC address table (e.g. sh mac address-table)

No user data retrieved via WMI (Windows Server 2003)

Issue: If you are running UDT on Windows Server 2003, and setup WMI retrieval of user data from a Active Directory domain controller outside of the local UDT server's domain, and using an account with limited permissions, UDT is able to connect to the remote AD controller but does not retrieve user data. Data retrieval is blocked by an implementation of the Custom Security Descriptor (CustomSD).

The only identified workaround involves a registry edit on the domain controller, as follows:

1. Open RegEdit from the Run line.
2. Locate the CustomSD key (KEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Eventlog\Security)
3. Add to the existing string the extra ACL: (A;;0x1;;S-1-5-32-573).
4. Save and exit.
UDT not receiving user data from domain controllers

Issue: UDT credentials are managing relevant domain controllers and the credentials for accessing them are valid. AD polling, however, is not working.

In some cases this problem has been traced to the wrong event codes being generated on the domain controller(s). UDT cannot display any user related data without event codes 4768/4769 and without a result code of 0x0; any other event or result codes result in UDT ignoring the log data.

Event code setup

Use Group Policy Manager to review and edit the default local policy on the domain controller(s). Check that the "Audit account logon events" policy is enabled on the domain controller; since event 4768 belongs to this category.

Add a deleted port back into UDT

Re-run UDT Port Discovery.

To add a UDT port:

1. Open the Orion Web Console.
2. Click Settings > UDT Settings > User Device Tracker Discovery.
3. Select the node(s) from which you deleted the port(s).
4. Click Next to run the discovery.
5. Select the ports to actively monitor in IMPORT PORTS.
6. Click + to expand Advanced Filtering Options.
7. Select 'Show Deleted Ports'.
8. Click 'FILTER ALL PORTS BELOW >', then click + next to the node(s) on which you deleted the ports. (You should see all ports including the deleted ones.)
9. Click the deleted ports. They are added back into UDT.
10. Click Submit.
Regular Expression Pattern Matching

When editing comparison criteria, the following regular expressions can be used for pattern matching. Examples are provided at the end of this section.

Characters

<table>
<thead>
<tr>
<th>CHARACTER</th>
<th>DESCRIPTION</th>
<th>EXAMPLE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Any character except (\text{[^}])</td>
<td>All characters except the listed special characters match a single instance of themselves.</td>
<td>a matches a</td>
</tr>
<tr>
<td>\ (backslash) followed by any of (\text{[^}])</td>
<td>A backslash escapes special characters to suppress their special meaning.</td>
<td>+ matches +</td>
</tr>
<tr>
<td>(\text{\x\x}) where (\text{\x}) are 2 hexadecimal digits</td>
<td>Matches the character with the specified ASCII/ANSI value, which depends on the code page used. Can be used in character classes.</td>
<td>\xA9 matches © when using the Latin-1 code page.</td>
</tr>
<tr>
<td>(\text{n, r and t})</td>
<td>Match an LF character, CR character and a tab character respectively. Can be used in character classes.</td>
<td>\n\n matches a DOS/Windows CRLF line break.</td>
</tr>
</tbody>
</table>

Character classes or character sets [abc]

<table>
<thead>
<tr>
<th>CHARACTER CLASSES OR SETS</th>
<th>DESCRIPTION</th>
<th>EXAMPLE</th>
</tr>
</thead>
<tbody>
<tr>
<td>[ (opening square bracket)</td>
<td>Starts a character class. A character class matches a single character out of all of the possibilities offered by the character class. Inside a character class, different rules apply. The rules in this section are only valid inside character classes. The rules outside this section are not valid in character classes, except \n, \r, \t and \xFF</td>
<td></td>
</tr>
<tr>
<td><strong>CHARACTER CLASSES OR SETS</strong></td>
<td><strong>DESCRIPTION</strong></td>
<td><strong>EXAMPLE</strong></td>
</tr>
<tr>
<td>-------------------------------</td>
<td>----------------</td>
<td>-------------</td>
</tr>
<tr>
<td>Any character except ^,-,\</td>
<td>All characters except the listed special characters.</td>
<td>[abc] matches a, b or c</td>
</tr>
<tr>
<td>\ (backslash) followed by any of ^,-,\</td>
<td>A backslash escapes special characters to suppress their special meaning.</td>
<td>[^]] matches ^ or ]</td>
</tr>
<tr>
<td>- (hyphen) except immediately after the opening [</td>
<td>Specifies a range of characters. (Specifies a hyphen if placed immediately after the opening [])</td>
<td>[a-zA-Z0-9] matches any letter or digit</td>
</tr>
<tr>
<td>^ (caret) immediately after the opening [</td>
<td>Negates the character class, causing it to match a single character not listed in the character class. (Specifies a caret if placed anywhere except after the opening [])</td>
<td>[^a-d] matches x (any character except a, b, c or d)</td>
</tr>
<tr>
<td>\d, \w and \s</td>
<td>Shorthand character classes matching digits 0-9, word characters (letters and digits) and whitespace respectively. Can be used inside and outside character classes</td>
<td>[\d\w] matches a character that is a digit or whitespace</td>
</tr>
</tbody>
</table>
## Anchors

<table>
<thead>
<tr>
<th>Anchors</th>
<th>Description</th>
<th>Example</th>
</tr>
</thead>
</table>
| ^ (caret) | Matches at the start of the string to which the regular expression pattern is applied. Matches a position rather than a character. Most regular expression flavors have an option to make the caret match after line breaks (i.e. at the start of a line in a file) as well. | ^ \. matches `a` in `abc\ndef`.
Also matches `d` in "multi-line" mode. |
| $ (dollar) | Matches at the end of the string to which the regular expression pattern is applied. Matches a position rather than a character. Most regular expression flavors have an option to make the dollar match before line breaks (i.e. at the end of a line in a file) as well. Also matches before the very last line break if the string ends with a line break. | $. matches `f` in `abc\ndef`.
Also matches `c` in "multi-line" mode. |
| \A | Matches at the start of the string to which the regular expression pattern is applied to. Matches a position rather than a character. Never matches after line breaks. | \A . matches `a` in `abc` |
| \Z | Matches at the end of the string to which the regular expression pattern is applied. Matches a position rather than a character. Never matches before line breaks, except for the very last line break if the string ends with a line break. | \Z . matches `f` in `abc\ndef` |
| \z | Matches at the end of the string to which the regular expression pattern is applied. Matches a position rather than a character. Never matches before line breaks. | \z . matches `f` in `abc\ndef` |
## Quantifiers

<table>
<thead>
<tr>
<th><strong>Quantifiers</strong></th>
<th><strong>Description</strong></th>
<th><strong>Example</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>? (question mark)</td>
<td>Makes the preceding item optional. The optional item is included in the match, if possible.</td>
<td>abc? matches ab or abc</td>
</tr>
<tr>
<td>??</td>
<td>Makes the preceding item optional. The optional item is excluded in the match, if possible. This construct is often excluded from documentation due to its limited use.</td>
<td>abc?? matches ab or abc</td>
</tr>
<tr>
<td>* (star)</td>
<td>Repeats the previous item zero or more times. As many items as possible will be matched before trying permutations with fewer matches of the preceding item, up to the point where the preceding item is not matched at all.</td>
<td>.* matches &quot;def&quot; &quot;ghi&quot; in abc &quot;def&quot; &quot;ghi&quot; jkl</td>
</tr>
<tr>
<td>*? (lazy star)</td>
<td>Repeats the previous item zero or more times. The engine first attempts to skip the previous item before trying permutations with ever increasing matches of the preceding item.</td>
<td>.*? matches &quot;def&quot; in abc &quot;def&quot; &quot;ghi&quot; jkl</td>
</tr>
<tr>
<td>#NAME?</td>
<td>Repeats the previous item once or more. As many items as possible will be matched before trying permutations with fewer matches of the preceding item, up to the point where the preceding item is matched only once.</td>
<td>.+ matches &quot;def&quot; &quot;ghi&quot; in abc &quot;def&quot; &quot;ghi&quot; jkl</td>
</tr>
<tr>
<td>+? (lazy plus)</td>
<td>Repeats the previous item once or more. The engine first matches the previous item only once, before trying permutations with ever increasing matches of the preceding item.</td>
<td>.+? matches &quot;def&quot; in abc &quot;def&quot; &quot;ghi&quot; jkl</td>
</tr>
<tr>
<td>QUANTIFIERS</td>
<td>DESCRIPTION</td>
<td>EXAMPLE</td>
</tr>
<tr>
<td>--------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>------------------</td>
</tr>
<tr>
<td>{n} where n is an integer &gt;= 1</td>
<td>Repeats the previous item exactly n times.</td>
<td>a(3) matches aaa</td>
</tr>
<tr>
<td>{n,m} where n &gt;= 1 and m &gt;= n</td>
<td>Repeats the previous item between n and m times. Will try to repeat m times before reducing the repetition to n times.</td>
<td>a(2,4) matches aa, aaa or aaaa</td>
</tr>
<tr>
<td>{n,m}? where n &gt;= 1 and m &gt;= n</td>
<td>Repeats the previous item between n and m times. Will try to repeat n times before increasing the repetition to m times.</td>
<td>a(2,4)? matches aaaa, aaa or aa</td>
</tr>
<tr>
<td>{n,} where n &gt;= 1</td>
<td>Repeats the previous item at least n times. Will try to match as many items as possible before trying permutations with fewer matches of the preceding item, up to the point where the preceding item is matched only m times.</td>
<td>a(2,)? matches aaaaa in aaaaa</td>
</tr>
<tr>
<td>{n,}? where n &gt;= 1</td>
<td>Repeats the previous item between n and m times. The engine first matches the previous item n times before trying permutations with ever increasing matches of the preceding item.</td>
<td>a(2,)? matches aa in aaaaa</td>
</tr>
</tbody>
</table>

**Dot**

<table>
<thead>
<tr>
<th>DOT CHARACTER</th>
<th>DESCRIPTION</th>
<th>EXAMPLE</th>
</tr>
</thead>
<tbody>
<tr>
<td>. (dot)</td>
<td>Matches any single character except line break characters \r and \n.</td>
<td>. matches x or most any other character</td>
</tr>
</tbody>
</table>
Word Boundaries

<table>
<thead>
<tr>
<th>WORD BOUNDARY</th>
<th>DESCRIPTION</th>
<th>EXAMPLE</th>
</tr>
</thead>
<tbody>
<tr>
<td>\b</td>
<td>Matches at the position between a word character (anything matched by \w) and a non-word character (anything matched by [\W] or \W) as well as at the start and/or end of the string if the first and/or last characters in the string are word characters.</td>
<td>abc\b</td>
</tr>
<tr>
<td>\B</td>
<td>Matches at the position between two word characters (i.e. the position between \ww) as well as at the position between two non-word characters (i.e. \W\W).</td>
<td>\B\B</td>
</tr>
</tbody>
</table>

Alternation

<table>
<thead>
<tr>
<th>ALTERNATION CHARACTER</th>
<th>DESCRIPTION</th>
<th>EXAMPLE</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>(vertical bar or &quot;pipe&quot;)</td>
<td>Causes the regular expression engine to match either the part on the left side or the part on the right side. Can be strung together into a series of options.</td>
</tr>
<tr>
<td></td>
<td>(vertical bar or &quot;pipe&quot;)</td>
<td>The vertical bar has the lowest precedence of all operators. Use grouping to alternate only part of the regular expression.</td>
</tr>
</tbody>
</table>

Regular expression pattern matching examples

The following examples illustrate uses of regular expression pattern matching.

snmp-server community public

Finds any line that includes the text snmp-server community public. There can be text before and/or after the string on the same line.

service tcp-keepalives-in.*\n(.*\n)*.*service tcp-keepalives-out

Finds the first line service tcp-keepalives-in and then looks for service tcp-keepalives-out on any line after that. The regular expression string .*\n(.*\n)*.* is used to search any number of lines between strings.

access-list 105 deny.*tcp any any eq 139 log
Finds the line with access-list 105 deny, followed by any number of characters of any type, followed by tcp any any eq 139 log on the same line. The regular expression string .* finds any character and any number of characters on the same line. This expression can be used to find spaces, tabs, numbers, letters, or special characters.

ntp clock-period \d*

Finds any line that includes ntp clock-period, followed by any number. The regular expression string \d* will find any number at any length, such as 3, 48, or 2394887.

user \x2a

Finds any line that includes user *. The regular expression string \x, followed by a hexadecimal value, specifies an individual character. In this example, \x2a represents the asterisk character, which has a hexadecimal value of 2a.

**Product updates**

The Product Updates category provides commands to get up-to-date information about using and upgrading SolarWinds UDT.

**Available product updates**

Click Available Product Updates on the Settings page to configure regular checks for SolarWinds UDT updates that can include version upgrades and service packs.

**SolarWinds product Team Blog**

Click SolarWinds product Team Blog on the Settings page to view regular posts from members of the SolarWinds product team to help you take full advantage of features provided by SolarWinds UDT and other SolarWinds products.

**User Device Tracker (UDT) Scalability Engine Guidelines**

<table>
<thead>
<tr>
<th>User Device Tracker (UDT) Scalability Engine Guidelines</th>
</tr>
</thead>
<tbody>
<tr>
<td>Stackable Pollers Available?</td>
</tr>
<tr>
<td>Poller Remotability Available?</td>
</tr>
<tr>
<td>Primary Poller Limits</td>
</tr>
<tr>
<td>Scalability Options</td>
</tr>
</tbody>
</table>
### User Device Tracker (UDT) Scalability Engine Guidelines

<table>
<thead>
<tr>
<th>Category</th>
<th>Guidelines</th>
</tr>
</thead>
<tbody>
<tr>
<td>Maximum of 500k port per instance (1 main poller and 4 additional)</td>
<td>Maximum of 500k port per instance (1 main poller and 4 additional)</td>
</tr>
<tr>
<td>WAN and/or Bandwidth Considerations</td>
<td>None</td>
</tr>
<tr>
<td>Other Considerations</td>
<td>UDT version 3.1 supports the ability to schedule port discovery.</td>
</tr>
<tr>
<td></td>
<td>In UDT version 3.1 the Max Discovery Size is 2,500 nodes/150,000 ports</td>
</tr>
</tbody>
</table>