

SOLARWINDS TECHNICAL REFERENCE

Port Requirements for SolarWinds Products

Port Requirements for SolarWinds Products	1
Application Performance Monitor.....	1
Application Performance Monitor Component Monitors	1
Application Performance Monitor Templates.....	4
Application Performance Monitor WMI Requirements.....	4
ipMonitor	6
KiWi Syslog Server	9
LANsurveyor	9
NetFlow Collector Service ports	9
Orion IP SLA Manager.....	9
Orion IP Address Manager	9
Orion Enterprise Console.....	9
Orion Network Atlas	9
Orion Network Configuration Manager	9
Orion Network Performance Monitor	10
Orion Netflow Traffic Analyzer	10
Orion Additional Pollers	10
Storage Manager / Profiler.....	10
SolarWinds Engineer's Toolset.....	12
User Device Tracker	12
Virtualization Manager	12

Reference Guide for SolarWinds Products Port Requirements

Copyright© 1995-2010 SolarWinds. All rights reserved worldwide. No part of this document may 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 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 licensors. SolarWinds Orion™, SolarWinds Cirrus™, and SolarWinds Toolset™ are trademarks of SolarWinds and SolarWinds.net® and the SolarWinds logo are registered trademarks of SolarWinds All other trademarks contained in this document and in the Software are the property of their respective owners.

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 OR 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.

Microsoft® and Windows 2000® are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

Graph Layout Toolkit and Graph Editor Toolkit © 1992 - 2001 Tom Sawyer Software, Oakland, California. All Rights Reserved.

Portions Copyright © ComponentOne, LLC 1991-2002. All Rights Reserved.

Document Revised: 5/24/2011

About SolarWinds

SolarWinds, Inc develops and markets an array of network management, monitoring, and discovery tools to meet the diverse requirements of today's network management and consulting professionals. SolarWinds products continue to set benchmarks for quality and performance and have positioned the company as the leader in network management and discovery technology. The SolarWinds customer base includes over 45 percent of the Fortune 500 and customers from over 90 countries. Our global business partner distributor network exceeds 100 distributors and resellers.

Contacting SolarWinds

You can contact SolarWinds in a number of ways, including the following:

Team	Contact Information
Sales	sales@solarwinds.com www.solarwinds.com 1.866.530.8100 +353.21.5002900
Technical Support	www.solarwinds.com/support
User Forums	www.thwack.com

Conventions

The documentation uses consistent conventions to help you identify items throughout the printed and online library.

Convention	Specifying
Bold	Window items, including buttons and fields.
<i>Italics</i>	Book and CD titles, variable names, new terms
Fixed font	File and directory names, commands and code examples, text typed by you
Straight brackets, as in [value]	Optional command parameters
Curly braces, as in {value}	Required command parameters
Logical OR, as in value1 value2	Exclusive command parameters where only one of the options can be specified

Port Requirements for SolarWinds Products

The following reference provides a comprehensive list of port requirements for SolarWinds products. The ports will vary from product to product and on a per use basis. In some cases ports are configurable. Refer to your product Administrative Guide for more information.

Application Performance Monitor

TCP port 17777 must be open on both the Orion APM server and the website.

Application Performance Monitor Component Monitors

DHCP User Experience Monitor

- The UDP port used for the DHCP request. The default value is 67.
- The UDP port used for the DHCP response. The default value is 68.

Directory Size Monitor- See "WMI Requirements for APM Component Monitors and Templates " on page "4".

DNS Monitor – TCP The TCP port used for DNS queries. The default value is 53.

DNS Monitor – UDP The UDP port used for DNS queries. The default value is 53.

DNS User Experience Monitor- The port used for DNS queries. The default value is 53.

Download Speed Monitor- The port used for the character generator service. The default value is 19

File Age Monitor- This component monitor uses TCP/445 and UDP/445 ports.

File Change Monitor- This component monitor uses TCP/445 and UDP/445 ports

File Count Monitor See "WMI Requirements for APM Component Monitors and Templates " on page "4".

File Existence Monitor - This component monitor uses TCP/445 and UDP/445 ports.

Files Size Monitor- This component monitor uses TCP/445 and UDP/445 ports.

FTP Monitor- This field is the port number used for FTP sessions. The default value is 21.

FTP User Experience Monitor- This field is the port number used for FTP sessions. The default value is 21.

HTTP Form Login Monitor- This field is the port number used for HTTP forms-based login sessions. The default value is 80.

HTTP Monitor- The port used for the web site. The default value is 80.

HTTPS Monitor- The port used by the web site. The default value is 443.

IMAP4 Monitor uses port 143.

IMAP4 User Experience Monitor.

This component monitor uses the following ports when used with a Microsoft Exchange mail server:

- 102 X.400 MTA
- 110 POP3
- 119 NNTP

2 Port Requirements for SolarWinds Products

- 389 LDAP
- 563 POP3 over SSL.
- 636 LDAP over SSL.
- 993 IMAP4 over SSL.
- 995 POP3 over SSL.

IMAP4 Port

This field is the port number used for IMAP 4 sessions. The default value is 143. For Secure IMAP (IMAP4-SSL), use port 585. For IMAP4 over SSL (IMAPS), use port 993.

LDAP User Experience Monitor - The port used for LDAP connections. The default value is 389. For LDAP over SSL, use port 636.

Linux/Unix Script Monitor- This field allows you to specify the port number used for the SSH connection. The default value for this field is 22.

MAP4 User Experience Monitor.

This component monitor uses the following ports when used with a Microsoft Exchange mail server:

- 102 X.400 MTA
- 110 POP3
- 119 NNTP
- 389 LDAP
- 563 POP3 over SSL.
- 636 LDAP over SSL.
- 993 IMAP4 over SSL.
- 995 POP3 over SSL.
- **MAP4 SMTP Port** This field is the port number used for SMTP sessions. The default value is 25.

NNTP Monitor- This field is the port number used for NNTP connections. The default value is UDP 119.

ODBC User Experience Monitor- This component monitor uses port TCP/1630.

Oracle User Experience Monitor- This component monitor uses ports TCP/1521 and TCP/1526. The Oracle SQL*Net Listener allows Oracle client connections to the database over Oracle's SQL*Net protocol. You can configure it during installation. To reconfigure this port, use Net Configuration Assistant.

Performance Counter Monitor- This monitor uses RPC, requiring the following ports:TCP/135; RPC/named pipes (NP) TCP 139, RPC/NP TCP 445, RPC/NP UDP 137, RPC/NP UDP 138

POP3 Monitor- This field is the port number used for POP3 connections. The default value is 110. For Secure POP3 (SSL-POP) use port 995.

This component monitor uses the following ports when used with a Microsoft Exchange mail server:

- 102 X.400 MTA
- 110 POP3
- 119 NNTP
- 143 IMAP4
- 389 LDAP
- 563 POP3 over SSL.
- 636 LDAP over SSL.
- 993 IMAP4 over SSL.
- 995 Secure POP3 over SSL.

POP3 User Experience Monitor- This field is the port number used for POP3 sessions. The default value is 110. For Secure POP3 (SSL-POP) use port 995. It also uses an **SMTP Port** , port 25 for SMTP sessions.

Process Monitor -SNMP- component monitor uses SNMP communication

Process Monitor WMI- Uses WMI communication to test if the specified Windows process is running and uses RPC communication to test if the specified Windows process is running.

RADIUS User Experience Monitor- This field is the RADIUS protocol authentication port. The default value is 1812. Cisco devices may require port 1645. This field is the RADIUS protocol accounting port. The default value is 1813. Cisco devices may require port 1646.

RWHOIS Port Monitor- This template tests the ability of an RWHOIS server to accept incoming sessions on port 4321.

SMTP Monitor- This field is the port number used for SMTP connections. The default value is 25. For Secure SMTP (SSMTP), use port 465.

SQL Server User Experience Monitor- This component monitor only works if Microsoft SQL Server is using the default port 1433. If you have a Microsoft SQL Server database that uses a non-standard port, you cannot monitor it using the SQL Server User Experience monitor. You need to use the ODBC User Experience monitor instead to manually define a connection string that will allow you to talk to Microsoft SQL Server on its custom port.

TACACS+User Experience Monitor- This field is the TACACS+ protocol connection port. The default value is 49.

TCP Port Monitor- This uses the TCP protocol connection port. The default value is 80.

Tomcat Server Monitor- This field allows you to specify the port number used by the web site. The default value for this field is 8080.

VMware Performance Counter Monitor- Port number to use for VMware API. The default is 443.

Windows Event Log Monitor- This component monitor uses the following ports:

- TCP/135
- RPC/named pipes (NP) TCP 139
- RPC/NP TCP 445
- RPC/NP UDP 137
- RPC/NP UDP 138

POP3 User Experience Monitor **port 110**.

Application Performance Monitor Templates

Template port requirements will vary depending on how you utilize them. The following provides a list of monitor templates that use ports.

- **Blackberry Delivery Confirmation template** uses port 25 on the SMTP server for sending the test email. If the SMTP server uses a different port, change this value.
- **Finger Port Monitor** This template tests the ability of the Finger service to accept incoming sessions on port 79.
- **Gopher Port Monitor** This template tests the ability of a Gopher server to accept incoming sessions on port 70.
- **IRC Port Monitor** This template tests the ability of an IRC server to accept incoming sessions on port 6667.
- **Java Application Server (SNMP)** template is configured to send SNMP requests on port 1161.
- **SNPP Port Monitor** This template tests the ability of an SNPP server to accept incoming sessions on port 444.
- **Windows FTP Server** (via WMI) This template monitors the Windows FTP Publishing Service and tests the ability of the FTP server to accept incoming sessions on port 21.

Application Performance Monitor WMI Requirements

Microsoft Windows by default uses a random port between 1024 and 65535 for WMI communications. You must create firewall exceptions to allow TCP/UDP traffic on ports 1024 - 65535 or the component monitors and templates that use WMI will not work.

The following **component monitors** use WMI:

- Performance Counter Monitor
- Process Monitor – WMI (if script uses WMI access)
- Windows Event Log Monitor
- Windows PowerShell Monitor (if script uses WMI access)
- Windows Script Monitor
- Windows Service Monitor (if script uses WMI access)

The following **templates** use WMI:

- Active Directory

- Blackberry Enterprise Server
- Citrix XenApp 5.0 Core WMI Counters
- Citrix XenApp 5.0 ICA Session WMI Counters
- Citrix XenApp 5.0 Presentation Server WMI Counters
- Citrix XenApp 5.0 Services
- Errors in Application Event Log
- Exchange 2007
- Exchange 2007 Client Access Role Services
- Exchange 2007 Client Access Role WMI Counters
- Exchange 2007 Common WMI Counters
- Exchange 2007 Edge Transport Role Services
- Exchange 2007 Hub Transport Role Services
- Exchange 2007 Hub Transport Role WMI Counters
- Exchange 2007 Mailbox Role Services
- Exchange 2007 Mailbox Role WMI Counters
- Exchange 2007 Unified Messaging Role Services
- Exchange 2007 WMI Counters
- Exchange 2010 Client Access Role Services
- Exchange 2010 Common Performance Counters
- Exchange 2010 Edge Transport Role Services
- Exchange 2010 Hub Transport Role Services
- Exchange 2010 Mailbox Role Services
- Exchange 2010 Unified Messaging Role Services
- Exchange Server 2000 and 2003
- Internet Information Services
- Orion Server
- SharePoint Server (MOSS) 2007
- SharePoint Services (WSS) 3.0
- SQL Server 2005 Database
- SQL Server 2008 Database
- Windows Print Services
- Windows Server 2003-2008

ipMonitor

ipMonitor uses the following local Ports:

- HTTP Port (default is 8080 and TCP 443 for SSL or administrator assigned).

The following table provides the various ports that are utilized depending on which monitor is enabled.

Monitor	Type	Port	Parent Protocol
ACTIVE DIRECTORY	Active Directory	389	TCP
BANDWIDTH USAGE	Bandwidth	161	UDP
BATTERY	Battery	161	UDP
CPU USAGE	Processor Usage	161	UDP
DIRECTORY MONITOR	Directory Usage	n/a	SMB or NFS
Monitor	Type	Port	Parent Protocol
DNS-QA	Quality Assurance Domain Name Service	53	TCP
DNS-TCP	Domain Name Service - Transmission Control Protocol	53	TCP
DNS-UDP	Domain Name Service - User Datagram Protocol.	53	UDP
DRIVE SPACE	Drive Space Availability	161	UDP
EVENT LOG	NT Event Log Monitor	n/a	n/a
EXCHANGE SERVER	Microsoft® Exchange Server	n/a	n/a
EXTERNAL PROCESS	Executable File	n/a	n/a
FAN MONITOR	Fan Status	161	UDP
FILE PROPERTY	Any File Type	n/a	SMB or NFS
FILE WATCHING	Any File Type	n/a	SMB or NFS
FINGER	Finger Information Server	79	TCP
FTP	File Transfer Protocol	21	TCP
FTP-QA	Quality Assurance File Transfer Protocol	21	TCP
GOPHER	Menu driven front end to resource services such as anonymous FTP	70	TCP

HTML / ASP	HyperText Transfer Protocol	80	TCP
HTTP	HyperText Transfer Protocol	80	TCP
HTTP-QA	Quality Assurance HyperText Transfer Protocol	80	TCP
HTTPS	Hypertext Transfer Protocol Secure	443	TCP
HUMIDITY	Humidity Levels	161	UDP
IMAP4	Internet Message Access Protocol	143	TCP
IMAP4-QA	Quality Assurance Internet Message Access Protocol	143	TCP
IPMONITOR	ipMonitor	80, 443	TCP
IRC	Internet Relay Chat	6667	TCP
Monitor	Type	Port	Parent Protocol
KERBEROS 5	Kerberos 5	88	UDP
LDAP	Lightweight Directory Access Protocol	389	UDP
LINK-QA	Quality Assurance Link	80	TCP
LOTUS NOTES	Lotus Notes [™] Transport	1352	TCP
MAPI-QA	Microsoft Messaging Application Program Interface	n/a	n/a
MEMORY USAGE	Physical Memory (RAM)	161	UDP
NETWORK SPEED	Speed or Bandwidth Monitor	19	TCP
NNTP	Network News Transfer Protocol	119	TCP
NTP	Network Time Protocol	123	UDP
PING	Packet InterNet Groper	n/a	ICMP
POP3	Post Office Protocol	110	TCP
POP3-QA	Quality Assurance Post Office Protocol	110	TCP
RADIUS	Remote Authentication Dial-In User Service protocol	1812	UDP
RWHOIS	Recursive Whols Information Server	4343	TCP
SERVICE	Windows NT Service Monitor	n/a	NT Specific

8 Port Requirements for SolarWinds Products

SMTP	Simple Mail Transfer Protocol	25	TCP
SNMP	Simple Network Management Protocol	161	TCP
SNMP-QA	Quality Assurance Simple Network Management Protocol	161	UDP
SNMP TRAP-QA	Simple Network Management Protocol Traps	162	UDP
SNPP	Simple Network Pager Protocol	444	TCP
SQL: ADO	Structured Query Language: ActiveX Data Objects	n/a	NT Specific
SQL: ADO-QA	Structured Query Language: ActiveX Data Objects	n/a	NT Specific
SQL SERVER	Structured Query Language Server	n/a	NT Specific
TELNET	Remote Terminal Protocol	23	TCP
Monitor	Type	Port	Parent Protocol
TEMPERATURE	Temperature Levels	161	UDP
WHOIS	Whols Information Server	43	TCP

Note:

Any agent you configure to send Traps to ipMonitor must use this same IP Address and Port combination. If the Windows SNMP Trap Service is enabled on the ipMonitor host computer, it is very likely to conflict with ipMonitor's SNMP Trap Listener. Both are bound by default to port 162.

The **POP3 User Experience** monitor delivers an email to the SMTP server on port 25 for the recipient address you specify. The monitor then logs in to the POP3 Mail Server on port 110 and retrieves the LIST of queued mail.

KiWi Syslog Server

The following lists required ports needed for KiWi Syslog Server.

- TFTP Server uses Port 69.
- Syslog uses UDP port 514.

LANsurveyor

To ensure that LANsurveyor scans thoroughly, turn on file and print sharing services and configure your workstation firewall to allow connections to UDP 137, UDP 138, UDP 445, and TCP 139, and TCP 445 ports.

NetFlow Collector Service ports

- By default, Orion NTA listens for Flow data on port 2055, but some Flow-enabled devices, including some Nortel IPFIX-enabled devices, send Flow data on port 9995.
- **Cisco NetFlow Configuration:** The port used for NetFlow traffic is specified in the configuration of your Flow-enabled Cisco appliance.

Orion IP SLA Manager

- HTTP operation performs a TCP request to the HTTP server using port 80.
- TCP port 17777 must be opened for Orion module traffic.
- Secure SSL communications are conducted over port 443.
- SNMP port uses the Orion NPM default of UDP port 161.

Orion IP Address Manager

- SNMP port uses the Orion NPM default of UDP port 161.
- RPC Ports dynamically assigned above 1024. To configure RPC dynamic port allocations see: <http://support.microsoft.com/kb/154596>

Orion Enterprise Console

- Orion EOC Orion Information Service Protocol uses port 17777/tcp.
- Orion EOC Web Console typically uses port 80/tcp unless configured otherwise.

Orion Network Atlas

Orion Network Atlas requires the following port:

- Orion Information Service Protocol uses port 17777/tcp

Orion Network Configuration Manager

The following lists the ports that may be needed depending on how Orion NCM is designated to download and upload configurations.

- Telnet port 23.
- SSH port 22.
- TFTP port 69.
- FTP control (setup/teardown) on port 21, FTP data on port 20.

Orion Network Performance Monitor

The following list provides the various ports that are utilized by Orion NPM depending on which services are enabled.

- Orion NPM statistics collection uses UDP port 161.
- Orion NPM Syslog Service uses UDP port 514 for incoming messages.
- The Orion NPM Trap Server listens for incoming trap messages on UDP port 162.
- Access to the SWIS API requires port 17778 HTTPS.
- Polling ESX/ESXi servers requires port 443. This is bidirectional.
- 17779/HTTP and 17779/HTTPS for the SolarWinds Toolset Integration.
- 17777/TCP open for Orion module traffic.

Additional Web Server

If you have installed an additional web server:

- Default port 80.
- 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 `http://192.168.0.3:8080`.

Hot Standby Engine

If you have installed a Hot Standby Engine:

- Default port 80.
- 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 `http://192.168.0.3:8080`.

Orion Netflow Traffic Analyzer

- By default, Orion NTA listens for Flow data on port 2055 (UDP). Ensure that port 2055 is open for UDP communication on any Orion NTA collector.
- Orion Netflow Traffic Analyzer Flow-enabled devices send Flow data to the Orion NTA collector on port 2055.
- The Orion NTA collector polls CBQoS-enabled devices for traffic-shaping policies and results on port 161.
- Orion NTA requires that TCP port 17777 is opened both to send and to receive traffic between Orion NPM and any other Orion modules.

Orion Additional Pollers

Additional Pollers for NPM, APM and UDT, use TCP 17777.

Storage Manager / Profiler

The SolarWinds Storage Manager and Profiler products require the following ports.

- HTTP Port 4319 (configurable) – handles requests from Profiler Server Collector.

- UDP Port 162. By default if 162 is in use by Orion NPM for example, then Profiler will use 10162 or 20162 to register the agent, (also configurable) – SNMP traps are sent to the Profiler Server.

Profiler Web GUI

- The Profiler web interface is contacted via HTTP (configurable HTTP or HTTPS) on Port 9000 (configurable).

ProfilerCollector

- Handles the collection from Profiler Data Collectors/agents and also acts as a local data collector/agent. Communicates with data collectors/agents on HTTP Port 4319 (configurable).

AppProfiler Module Requirements

- Microsoft SQL 1433 or 1094 (depends on SQL configuration).

Profiler for VMware

- Virtual Center: HTTPS Port 443.

StorageProfiler - Fiber Channel Switches

- Cisco MDS, Brocade, McData, and QLogic Switches use 161 UDP on the switch.

StorageProfiler – NAS

- **EMC Celerra** Non-Configurable: 22 on the Control station.
- **NetApp** 80 (HTTP)/443 (HTTPS) on NetApp head/cluster node and any available for CIFS/NFS.

StorageProfiler – SAN

- **3PAR** Configurable: 5988 (HTTP) or 5989 (HTTPS) used by 3PAR provider.
- **Dell EqualLogic** 161 (UDP) on the EqualLogic Group IP.
- **EMC Symmetrix** Configurable: 5988 (HTTP) or 5989 (HTTPS) used by EMC Solutions Enabler.
- **HP EVA** Configurable: 5988 (HTTP) or 5989 (HTTPS) used by HP CommandView.
- **HP MSA** Non-configurable: 5989 (HTTPS) used by HP SMI-S Provider.
- **IBM DS 3K, 4K, 5K** Configurable: 5988 (HTTP) or 5989 (HTTPS) used by SMI-S provider .Non-Configurable: 2463 used to set RPC sessions to the storage controller from SMI-S provider.
- **IBM DS 6K, 8K** Configurable: 5988 (HTTP) or 5989 (HTTPS) used by SMI-S provider.
- **IBM SVC** Configurable: 5988 (HTTP) or 5989 (HTTPS) used by SMI-S provider.
- **LSI** Configurable: 5988 (HTTP) or 5989 (HTTPS) used by SMI-S provider. Non-Configurable: 2463 used to set RPC sessions to the storage controller from SMI-S provider.
- **NetApp** 80 (HTTP)/443 (HTTPS) on NetApp head/cluster node.
- **SUN/StorageTek** Configurable: 5988 (HTTP) or 5989 (HTTPS) used by SMI-S provider. Non-Configurable: 2463 used to set RPC sessions to the storage controller from SMI-S provider.

SolarWinds Engineer's Toolset

The following lists the required ports needed for the Engineer's Toolset.

Syslog Server

- Allows you to listen for incoming Syslog messages on UDP port 514.

WAN Killer

- Use port 7 to generate traffic going both ways. When data is sent to port 7 (echo), all traffic that is received by the target device will be sent back to WAN Killer. This will generate a load in both directions.
- Use port 9 (discard) to generate one-way traffic. Port 9 discards all data when received.

User Device Tracker

- Information Service uses TCP port 17777.
- Website uses TCP port 80.
- SQL uses TCP port 1433.
- SNMP uses port 161.

Virtualization Manager

Inbound TCP ports:

- 80
- 443
- 3389
- 5000

Optional inbound TCP ports:

- 22 (for SSH access to the virtual appliance)
- 5480 (for accessing the administration page)
- 8983 (for federated data collectors)
- 61616 (for federated data collectors)

Authentication Server

The Authentication Server configuration page lets you specify the servers used to authenticate Active Directory (AD) and/or LDAP users and uses the following ports:

- AD authentication (default is 389)
- LDAP authentication (default is 3268)