

This PDF is no longer being maintained at this location. View [Port requirements for all SolarWinds products](#) for the latest information.

SolarWinds

Port Requirements

Version 2016

For SolarWinds Products

© 2016 SolarWinds Worldwide, LLC. All rights reserved.

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

SOLARWINDS DISCLAIMS ALL WARRANTIES, CONDITIONS OR OTHER TERMS, EXPRESS OR IMPLIED, STATUTORY OR OTHERWISE, ON SOFTWARE AND DOCUMENTATION FURNISHED HEREUNDER INCLUDING WITHOUT LIMITATION THE WARRANTIES OF DESIGN, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE, AND NONINFRINGEMENT. IN NO EVENT SHALL SOLARWINDS, ITS SUPPLIERS, NOR ITS LICENSORS BE LIABLE FOR ANY DAMAGES, WHETHER ARISING IN TORT, CONTRACT OR ANY OTHER LEGAL THEORY EVEN IF SOLARWINDS HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

The SolarWinds and other SolarWinds marks, identified on the SolarWinds website, as updated from SolarWinds from time to time and incorporated herein, are registered with the U.S. Patent and Trademark Office and may be registered or pending registration in other countries. All other SolarWinds trademarks may be common law marks or registered or pending registration in the United States or in other countries. All other trademarks or registered trademarks contained and/or mentioned herein are used for identification purposes only and may be trademarks or registered trademarks of their respective companies.

Table of Contents

Port Requirements for SolarWinds Products	5
DameWare	5
Database Performance Analyzer (DPA)	7
Database Performance Analyzer on Orion (DPAO)	8
ipMonitor	8
Firewall Security Manager (FSM)	11
KiWi Syslog Server	11
LANsurveyor	11
Log & Event Manager (LEM)	12
Network Topology Mapper (NTM)	14
Orion Additional Poller	14
Orion Enterprise Console (EOC)	14
Orion Firewall Security Manage Module (Orion FSMM)	15
IP Address Manager (IPAM)	15
NetFlow Traffic Analyzer (NTA)	15
Orion Network Atlas	16
Network Configuration Manager (NCM)	16
Network Performance Monitor (NPM)	16
NetPath™ Ports	18
Additional Polling Engines	18
Additional Web Server	19
High Availability	19
Agents	19
Patch Manager (PaM)	20
Server & Application Monitor (SAM)	21
Server, Website, and Agent Ports	21

SAM Component Monitor Ports	21
SAM Templates	26
SAM WMI Requirements	26
Additional Polling Engines	28
Additional Web Server	28
Web Performance Monitor (formerly SEUM)	28
Toolset	28
Desktop Toolset	28
Web Toolset	29
Storage Manager (STM)	29
Storage Resource Monitor (SRM)	30
User Device Tracker (UDT)	31
Virtualization Manager (VMAN)	31
VoIP & Network Quality Manager (VNQM)	33
Web Help Desk (WHD)	34

Port Requirements for SolarWinds Products

Last Update: 12/7/2016

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 Administrator Guide for more information.

DameWare

PORT NUMBER	DESCRIPTION	USED WITH COMPONENT OR PRODUCT	CHANGE THE DEFAULT PORT IN...	MODIFY THE PORT SETTINGS ON...
443	DameWare Internet Proxy HTTPS - Used to connect computers through an Internet Session or download an MRC or Internet Session agent	DameWare Internet Proxy	The Configuration Wizard	N/A
6129	DMRC protocol - DameWare agents listen on this port for incoming remote desktop connections	DameWare Mini Remote Control	DameWare Mini Remote Control application	Mobile Client in Global Settings
6130	DameWare Mobile Client protocol - the Gateway service listens on this port for incoming mobile connections	DameWare Mobile Gateway	Administration Console or the Configuration Wizard	Mobile Client on the gateway login screen
6132	Internet Session data stream between MRC and the DameWare Internet Proxy	DameWare Central Server, DameWare Internet Proxy	The Configuration Wizard	N/A
6133	Communication requests for DameWare Central Server components	DameWare Central Server, DameWare Internet Proxy, DameWare Mobile Gateway	The Configuration Wizard	DRS, MRC, and Administration consoles on the login screen
Optional ports for specific DameWare features:				
UDP 137	Name Services port for File & Printer Sharing, User and Computer Authentication	DameWare Remote Support DameWare Mini Remote Support	Windows systems settings	N/A

PORT NUMBER	DESCRIPTION	USED WITH COMPONENT OR PRODUCT	CHANGE THE DEFAULT PORT IN...	MODIFY THE PORT SETTINGS ON...
		DameWare Central Server		
138	Datagram Services port for File & Printer Sharing	DameWare Remote Support DameWare Mini Remote Support	Windows systems settings	N/A
139	Session Services port for File & Printer Sharing, User and Computer Authentication	DameWare Remote Support DameWare Mini Remote Support DameWare Central Server	Windows systems settings	N/A
TCP and UDP 445	Direct Hosting, NetBIOS for File & Printer Sharing, User and Computer Authentication	DameWare Remote Support DameWare Mini Remote Support DameWare Central Server	Windows systems settings	N/A
5900	VNC default port	DameWare Mini Remote Support DameWare Central Server	MRC connection settings and in VNC configuration server	MRC connection settings and in VNC configuration server
88	Kerberos V5 port	DameWare Central Server	N/A	N/A
3389	RDP port	DameWare Mini Remote Support DameWare Central Server	MRC connection settings and in Windows registry	MRC connection settings and in Windows registry
Dynamic	NTLM port	DameWare Central Server	N/A	N/A

PORT NUMBER	DESCRIPTION	USED WITH COMPONENT OR PRODUCT	CHANGE THE DEFAULT PORT IN...	MODIFY THE PORT SETTINGS ON...
16993	Accessing Intel AMT secure(SSL)	DameWare Mini Remote Support	MRC connection settings and in Intel AMT server	MRC connection settings and in Intel AMT server
16992	Accessing Intel AMT	DameWare Mini Remote Support	MRC connection settings and in Intel AMT server	MRC connection settings and in Intel AMT server
UDP and TCP 389	For LDAP to handle normal queries from client computers to the domain controllers	DameWare Central Server	N/A	N/A
TCP and UDP 53	For DNS from client to domain controller and domain controller to domain controller	DameWare Central Server	N/A	N/A
TCP 636	Computer Authentication over SLL	DameWare Central Server	N/A	N/A

Database Performance Analyzer (DPA)

PORT	TYPE	DESCRIPTION	CHANGE THE DEFAULT PORT IN ...
8123	HTTP	Default HTTP port for web server	Can be changed according to changes in DPA server.xml
8124	HTTPS	Default HTTPS port for web server	Can be changed according to changes in DPA server.xml
8127	TCP	Internal Tomcat shutdown port	
80	HTTP	Default HTTP port for web server (Amazon AMI installs only)	
443	HTTPS	Default HTTPS port for web server (Amazon AMI installs only)	

Database Performance Analyzer on Orion (DPAO)

PORT	TYPE	DESCRIPTION	CHANGE THE DEFAULT PORT IN ...
80	TCP	Default HTTP port for IIS web server	Can be changed in IIS settings
443	TCP	Default HTTPS port for IIS web server	Can be changed in IIS settings
17776	TCP	Incoming HTTP port used for JSwis subscriptions	N/A
17777	TCP	Internal port for communication with SWIS	N/A
17778	TCP	Internal port for communication with SWIS (encrypted)	N/A
8124	TCP	Default HTTPS port for establish integration with DPA	Can be changed according to changes in DPA server.xml

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
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

MONITOR	TYPE	PORT	PARENT PROTOCOL
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
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

MONITOR	TYPE	PORT	PARENT PROTOCOL
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
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
TEMPERATURE	Temperature Levels	161	UDP
WHOIS	Whols Information Server	43	TCP

ipMonitor Traps

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.

Firewall Security Manager (FSM)

PORT	TYPE	COMPONENT	COMMENT
17778			For the NCM repository import method. FSM connects on this port to the Orion information service on the primary polling engine.
18184	TCP		For network connectivity between the Check Point management server and the FSM server.
18210	TCP	FW1_lca_pull (the Check Point internal CA pull service)	
18190	TCP	CPMI service	
18191	TCP	Check Point Daemon (CPD)	
21, 22	Telnet/SSH		For direct connection to firewalls to gather configs
3050	TCP	Firebird Database Manager	OFSMM, FSM server and FSM Client communication with Firebird DB
4568	TCP	License Manager Listener	
45680	TCP	License Manager Service	
48080	HTTP	FSM Web Server	
17784	HTTPS	Orion FSM Web Service	

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.

Log & Event Manager (LEM)

The following table provides a list of all of the ports needed for communication with SolarWinds LEM.

i In the table, "inbound" assumes that the LEM VM is behind the firewall, and that you are configuring firewall rules to allow network traffic through the firewall to the LEM VM.

PORT	PROTOCOL	SERVICE	DIRECTION	DESCRIPTION
22, 32022	TCP	SSH	Bidirectional	SSH traffic to the SolarWinds LEM VM. (Port 22 is not used prior to version 6.3.x.)
25	TCP	SMTP	Outbound	SMTP traffic from the SolarWinds LEM VM to your email server for automated email notifications.
80, 8080	TCP	HTTP	Bidirectional	Non-secure HTTP traffic from the SolarWinds LEM Console to the SolarWinds LEM VM. (LEM closes this port when activation completes, but you can re-open it with the CMC <code>togglehttp</code> command.)
139, 445	TCP	NetBIOS, SMB	Bidirectional	Standard Windows file sharing ports (NetBIOS Session Service, Microsoft SMB) that LEM uses to export debug files, syslog messages, and backup files. The LEM Remote Agent Installer also uses these ports to install agents on Microsoft Windows hosts across your network.
161, 162	TCP	SNMP	Bidirectional	SNMP trap traffic received from devices, and used by Orion to monitor LEM. (Monitoring LEM on port 161 is not used prior to version 6.3.x.)
389, 636	TCP	LDAP	Outbound	LDAP ports that the LEM Directory Service Connector tool uses to communicate with a designated Active Directory domain controller. The LEM Directory Service Connector tool uses port 636 for SSL communications to a designated Active Directory domain controller.
443, 8443	TCP	HTTPS	Bidirectional	HTTPS traffic from the SolarWinds LEM Console to the LEM VM. LEM uses these secure HTTP ports after LEM is activated.

PORT	PROTOCOL	SERVICE	DIRECTION	DESCRIPTION
(445)	TCP	SMB	Bidirectional	<i>See entry for port 139.</i>
514	TCP or UDP	Syslog	Inbound	Syslog traffic from devices sending syslog event messages to the SolarWinds LEM VM.
(636)	TCP	LDAP		<i>See entry for port 389.</i>
2100	UDP	NetFlow	Inbound	NetFlow traffic from devices sending NetFlow to the SolarWinds LEM VM.
6343	UDP	sFlow	Inbound	sFlow traffic from devices sending sFlow to the SolarWinds LEM VM.
(8080)	TCP	HTTP	Bidirectional	<i>See entry for port 80.</i>
(8443)	TCP	HTTPS	Bidirectional	<i>See entry for port 443.</i>
8983	TCP	nDepth	Inbound	nDepth traffic sent from nDepth to the LEM VM containing raw (original) log data.
9001	TCP	LEM Reports	Bidirectional	LEM Reports traffic used to gather LEM Reports data on the LEM VM.
(32022)	TCP	SSH	Bidirectional	<i>See entry for port 22.</i>
37890-37892	TCP	LEM Agents	Inbound	LEM Agent traffic sent from SolarWinds LEM Agents to the SolarWinds LEM VM. (These ports correspond to the destination ports on the LEM VM.)
37893-37896	TCP	LEM Agents	Outbound	LEM Agent return traffic sent from the SolarWinds LEM VM to the SolarWinds LEM Agents. (These ports correspond to the destination ports on the LEM agents.)

LEM no longer uses the port listed in the following table.

PORT	PROTOCOL	SERVICE	DIRECTION	DESCRIPTION
5433	TCP	LEM Reports	Inbound	Port 5433 is no longer used. Previously, this port carried traffic from SolarWinds LEM Reports to the SolarWinds LEM VM. This was used by versions prior to LEM 5.6, for which support ended December 2015.

In LEM 6.2 and later, LEM will need access to the following URLs to use the automatic connector update function and the Threat Feeds function:

- <http://downloads.solarwinds.com/solarwinds/Release/LEM/>
- <https://rules.emergingthreats.net/fwrules/>


Network Topology Mapper (NTM)

The following list provides the various ports that are used by Network Topology Mapper:

- SNMP uses the default UDP port 161.
- VMware objects are accessed over port 443.
- WMI communications use a random port between 1024 and 65535, per Microsoft Windows specifications. You must create firewall exceptions to allow TCP/UDP traffic on ports 1024 - 65535 or the monitored objects that use WMI will not be mapped.
- Access to the SWIS API requires port 17778 HTTPS.

Orion Additional Poller

The Additional Polling Engine will talk to the Primary Polling engine (and vice versa) on TCP port 17777 and TCP port 5671. It will also talk to the MS SQL DB server on port 1433.

-  Additional Polling Engines have the same port requirements as primary polling engines.
- Ports 4369, 25672, and 5672 are opened by default on the main server for RabbitMQ messaging. These ports can be blocked by the firewall.
 - Port 5672 (TCP) is required for RabbitMQ messaging between Orion servers for NPM 12.0 only (Orion Platform version 2016.1).

Orion Enterprise Console (EOC)

PORT	TYPE	DESCRIPTION
80	TCP	Access to the Web Console
17777	TCP	Information Service protocol

Orion Firewall Security Manage Module (Orion FSMM)

The default port number for the Firewall Security Manager database is 3050. If the Firewall Security Manager database port has not been changed, use the default. To be certain that 3050 is the correct port for your installation, see your SysAdmin or the person who installed the Firewall Security Manager database.


Option: On the Firewall Security Manager database host, at a command prompt, type `netstat -b` and press Enter. The result contains a list of port numbers, services, and executables. Find the executable `fbserver.exe` and confirm it is associated with port 3050.

IP Address Manager (IPAM)


- SNMP port uses the 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>
Port 53 (TCP) for zone transfers (DNS record polling).

NetFlow Traffic Analyzer (NTA)

The following table provides a list of all of the ports needed for communication with SolarWinds NTA.

PORT	TYPE	DESCRIPTION
53	TCP/ UDP	The TCP and UDP port used for DNS queries.
80	TCP	Default port used by the web console and any other additional web servers. 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 .
137	UDP	Port for outbound traffic if NetBIOS name resolution is turned on. When NTA is trying to resolve the NetBIOS names of servers in their conversations, you may find a large amount of outbound UDP 137 traffic from the NTA Collector to a number of external addresses. You can confirm the traffic by using the Flow Navigator to match the outbound connections to existing conversations. <div style="border: 1px solid #ccc; padding: 5px; background-color: #e6f2ff;"><p> This is normal behavior when NetBIOS is enabled. An easy way to demonstrate the behavior is to disable NetBIOS in NTA and watch all outbound connections terminate.</p></div>
161	TCP	The NTA collector uses this port for polling CBQoS-enabled devices for traffic-shaping policies and results using SNMP.

PORT	TYPE	DESCRIPTION
1433	TCP	The port used for communication between the NTA Flow Storage and the NPM SQL server.
2055	UDP	Default port for receiving flows on any NTA collector. It has to be open for receiving flows on additional polling engines.
17777	TCP	This port needs to be opened both to send and receive traffic between NPM and any other Orion modules.
17778	HTTPS and TCP	Open to access the SolarWinds Information Service API and agent communication
17791	TCP	Open for agent communication on any SolarWinds Orion server running Windows Server 2008 R2 SP1
Device Specific		Cisco NetFlow Configuration: The port used for NetFlow traffic is specified in the configuration of your Flow-enabled Cisco appliance

 If you store your flows data in a remote NTA Flow Storage database, you need to open ports 1433 (TCP) and 17777 (TCP) on the NTA Flow Storage server, too.

Orion Network Atlas

Orion Network Atlas requires the following port:

- Orion Information Service Protocol uses port 17777/tcp


Network Configuration Manager (NCM)

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

- FTP control (setup/teardown) on port 21, FTP data on port 20.
- 161 – default port for Polling Devices, Statistics Collection via SNMP
- 25 default port for e-mail sending via SMTP
- 22 - default port for Config transfer via SSH/ SCP server
- 23 – default port for Config transfer via Telnet
- 69 – port TFTP server listens on
- 8888 – default web server port
- 17777 – Information service port

Network Performance Monitor (NPM)

The following tables provide the ports that are used by NPM depending on which services are enabled.

 Ports 4369, 25672, and 5672 are opened by default on the main server for RabbitMQ messaging. These ports can be blocked by the firewall.

PORT	TYPE	DESCRIPTION
25	TCP	SMTP port for non-encrypted messages
80	TCP	Default additional web server port. If you specify any port other than 80, you must include that port in the URL used to access the web console. For example, if you specify an IP address of 192.168.0.3 and port 8080, the URL used to access the web console is http://192.168.0.3:8080 . Open the port to enable communication from your computers to the Orion Web Console. The port might also be used for Cisco UCS monitoring.
161	UDP	NPM statistics collection
162	UDP	NPM Trap Server listens for incoming messages
443	TCP	Default port for https binding. Also used for bi-directional ESX/ESXi server polling, or for Cisco UCS monitoring.
465	TCP	The port used for SSL-enabled email alert actions.
514	UDP	NPM Syslog Service listens for incoming messages
587	TCP	The port used for TLS-enabled email alert actions.
1433	TCP	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.
1434	UDP	The port used for communication with the SQL Server Browser Service to determine how to communicate with certain non-standard SQL Server installations. For more information, see this Microsoft Technet article .
1801	TCP	MSMQ WCF binding (for more information see this KB: http://support.microsoft.com/kb/183293).
5671	TCP	For encrypted RabbitMQ messaging (AMQP/TLS) into the main polling engine from all Orion servers.
17777	TCP	Orion module traffic. Open the port to enable communication from your poller to the Orion Web Console, and from the Orion Web Console to your poller. The port used for communication between the Orion Web Console and the poller.
17778	HTTPS	Required for access to the SWIS API and agent communication
17779	HTTP	SolarWinds Toolset Integration over HTTP

PORT	TYPE	DESCRIPTION
17780	HTTPS	SolarWinds Toolset Integration over HTTPS
17791	TCP	Open for agent communication on any SolarWinds Orion server running Windows Server 2008 R2 SP1

NetPath™ Ports

Open the following ports on your firewall for network connectivity used by NetPath™:

PORT	PROTOCOL	SOURCE	DESTINATION	DESCRIPTION
17778	TCP	NetPath™ probe	Polling engine	Used to send information back to your Orion server.
11 (ICMP Time Exceeded)	ICMP	Networking devices along your path	NetPath™ probe	Used by the NetPath™ probe to discover network paths.
User configured	TCP	NetPath™ probe	Endpoint service	Any ports of the monitored services that are assigned to the probe. Used by the NetPath™ probe to discover service status.
43 443	TCP	Main polling engine	BGP data providers and announcements, such as: <ul style="list-style-type: none"> ■ http://whois.arin.net/ui/ ■ https://stat.ripe.net/ 	Used by NetPath™ to query BGP information about the discovered IP addresses.

Additional Polling Engines

Additional Polling Engines used with NPM have the same port requirements as the [NPM primary polling engine](#). The following ports are the minimum required for an APE to ensure the most basic polling functions.

PORT	TYPE	DESCRIPTION
1433	TCP (outbound)	The port used for communication between the APE and the Orion database.
5671	TCP (AMQP/TLS - outbound)	For SSL encrypted RabbitMQ messaging from the Orion Web Console to the APE.
17777	TCP (bidirectional)	The port used for communication between the APE and the Orion Web Console.

Additional Web Server

PORT	TYPE	DESCRIPTION
80	TCP (inbound)	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 http://192.168.0.3:8080 .
1433	TCP (outbound)	The port used to send data from the Additional Web Server to the Orion database.
1801	TCP (outbound)	The port used for MSMQ messaging from the Additional Web Server to primary polling engine.
5671	TCP (AMQP/TLS - outbound)	For SSL encrypted RabbitMQ messaging from the Additional Web Server to the primary polling engine.
17777	TCP (bidirectional)	The port used for communication between the Additional Web Server and the primary polling engine.

High Availability

The following ports are used in addition to ports used by your primary products when you enable High Availability.

PORT	TYPE	DESCRIPTION
4369	TCP	Open on the main Orion server and its standby server for RabbitMQ clustering. This port exchanges EPMD and Erlang distribution protocol messages for RabbbitMQ. This port is not required when protecting additional polling engines.
5671	TCP	For encrypted RabbitMQ messaging (AMQP/TLS) into the main polling engine from all Orion servers.
25672	TCP	Open on the main Orion server and its standby server for RabbitMQ clustering. This port exchanges EPMD and Erlang distribution protocol messages for RabbbitMQ. This port is not required when protecting additional polling engines.

Agents

The following ports are used by the SolarWinds Orion agent.

PORT	TYPE	DESCRIPTION
17791	TCP	Allows agent communication on any SolarWinds Orion server running Windows Server 2008 R2 SP1.
17790	TCP	Open on the remote computer (inbound).
17778	TCP	Open on the SolarWinds Orion server (inbound).
135	TCP	Open on the remote computer (inbound) if you deploy the agent from the SolarWinds server.
445	TCP	Microsoft-DS SMB file sharing. This port must be open on the client computer (inbound) for remote deployment.

Patch Manager (PaM)


The following sections describe the ports used in the Patch Manager environment.

PORT	TYPE	DESCRIPTION
135	TCP	RPC Endpoint Mapper - The Patch Manager server uses this port to establish WMI connections to remote computers. It also uses this port to connect to the Service Control Manager (SCM) when it provisions the WMI providers dynamically on the remote computer.
389	TCP	Lightweight Directory Access Protocol - Patch Manager servers use this port for Active Directory authentication.
445	TCP	SMB over TCP - The Patch Manager server uses this port when it provisions the WMI providers to a remote computer.
4092		<p>Console-to-Server Communication - The Patch Manager console uses this port to communicate to an independent Patch Manager application server. This is a one-way communication channel, so it only requires inbound TCP traffic on the application server.</p> <p>Patch Manager servers in a distributed environment also use this port in the same manner for "downstream" communication. For example, the Patch Manager Primary Application Server (PAS) uses port 4092 to communicate with remote Patch Manager servers in secondary server roles.</p>
8787	TCP	Web Console Connections - By default, users connect to the Patch Manager web console server on port 8787.
17777	TCP	SolarWinds Information Service - The SolarWinds Information Service (SWIS) facilitates data exchange for the Patch Manager web console, along with the web console Application Programming Interface (API). Ensure this port is not blocked on servers running the Patch Manager web console server.

PORT	TYPE	DESCRIPTION
1024-65536	Dynamic Ports	DCOM or RPC - WMI technology is based on Distributed Component Object Model (DCOM)/RPC communication. DCOM/RPC allocates the ports used by the server within a dynamic port range. This range is typically between 1024 and 65536. To configure these ports using Windows Firewall on your managed computers, enable the Inbound Rules in the Windows Management Instrumentation (WMI) group

Server & Application Monitor (SAM)

Server, Website, and Agent Ports

PORT	TYPE	COMPONENT	DESCRIPTION
5671	TCP		RabbitMQ messaging
17791	TCP	Agents	Open for agent communication on any SolarWinds Orion server running Windows Server 2008 R2 SP1.
17777	TCP	SAM Server and Website	Must be open on both the SAM server and the website. <div style="border: 1px solid #ccc; padding: 5px; background-color: #e6f2ff;">  Additional polling engines will require access to the SQL database. </div>
135		Agents	Open Ports Requirements for Remote Deployment from the Orion Server - Microsoft EPMAP (DCE/RPC Locator service). This port is required to be open on the client computer (Inbound) for remote deployment.
445		Agents	Open Ports Requirements for Remote Deployment from the Orion Server - Microsoft-DS SMB file sharing. This port is required to be open on the client computer (Inbound) for remote deployment.

SAM Component Monitor Ports

COMPONENT/MONITOR	PORT	TYPE	DESCRIPTION
DHCP User Experience Monitor	67	UDP	The UDP port used for the DHCP request.
DHCP User Experience Monitor	68	UDP	The UDP port used for the DHCP response.
Directory Size Monitor			See "Application Performance Monitor WMI Requirements" on page "4".

COMPONENT/ MONITOR	PORT	TYPE	DESCRIPTION
DNS Monitor DNS User Experience Monitor	53	TCP/UDP	The TCP and UDP port used for DNS queries.
Download Speed Monitor	19		The port used for the character generator service.
File Age Monitor File Change Monitor File Existence Monitor Files Size Monitor	445	TCP/UDP	These components monitor uses TCP/445 and UDP/445 ports.
File Count Monitor			See "Application Performance Monitor WMI Requirements" on page "4".
FTP Monitor FTP User Experience Monitor	21		This field is the port number used for FTP sessions
HTTP Form Login Monitor HTTP Monitor TCP Port Monitor	80		This field is the port number used for HTTP forms-based login sessions.
HTTPS Monitor	443		The port used by the web site.
IMAP4 Monitor	143		
IMAP4 User Experience Monitor	143 and 993	IMAP4	This component monitor uses these ports when used with a Microsoft Exchange mail server.

COMPONENT/ MONITOR	PORT	TYPE	DESCRIPTION
IMAP4 User Experience Monitor	25	SMTP	This component monitor uses these ports when used with a Microsoft Exchange mail server.
IMAP4 Port sessions	143	IMAP4	This field is the port number used for IMAP 4 sessions.
IMAP4 Port sessions	585	IMAP4	For Secure IMAP (IMAP4-SSL), use port 585.
IMAP4 Port sessions	993	IMAP4	For IMAP4 over SSL (IMAPS), use port 993.
LDAP User Experience Monitor	389		The port used for LDAP connections.
LDAP User Experience Monitor	636		For LDAP over SSL, use port 636.
Linux/Unix Script Monitor Ports	22		This field allows you to specify the port number used for the SSH connection.
NNTP Monitor	119	UDP	This field is the port number used for NNTP connections.
ODBC User Experience Monitor	1630	TCP	This component monitor uses port TCP/1630.
Oracle User Experience Monitor	1521	TCP	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.
Oracle User Experience Monitor	1526	TCP	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	See description	TCP	This monitor uses RPC, requiring the following ports: <ul style="list-style-type: none"> ■ TCP/135 ■ RPC/named pipes (NP) TCP 139

COMPONENT/ MONITOR	PORT	TYPE	DESCRIPTION
			<ul style="list-style-type: none"> ■ RPC/NP TCP 445 ■ RPC/NP UDP 137 ■ RPC/NP UDP 138
POP3 Monitor POP3 User Experience Monitor	110 (default)		This field is the port number used for POP3 connections.
POP3 Monitor POP3 User Experience Monitor	995		For Secure POP3 (SSL-POP) use port 995.
POP3 User Experience Monitor SMTP Monitor	25	SMTP	This component uses port 25 for SMTP sessions.
SMTP Monitor	465	SSMTP	For Secure SMTP (SSMTP), use port 465.
POP3 Monitor	See Description		<p>This component monitor uses the following ports when used with a Microsoft Exchange mail server.</p> <ul style="list-style-type: none"> ■ 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	110 (default)		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.

COMPONENT/ MONITOR	PORT	TYPE	DESCRIPTION
Process Monitor		SNMP	This 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	1812 1645		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	4321		This template tests the ability of an RWHOIS server to accept incoming sessions on port 4321.
SQL Server User Experience Monitor	1433		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	49		This field is the TACACS+ protocol connection port. The default value is 49.
Tomcat Server Monitor	8080		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	443		Port number to use for VMware API. The default is 443.
ESX Hardware Monitoring	5989		Ensure port 5989 is open on the firewall.
Windows Event Log Monitor			This component monitor uses the following ports: <ul style="list-style-type: none"> ■ TCP/135 ■ RPC/named pipes (NP) TCP 139 ■ RPC/NP TCP 445

COMPONENT/ MONITOR	PORT	TYPE	DESCRIPTION
			<ul style="list-style-type: none"> ■ RPC/NP UDP 137 ■ RPC/NP UDP 138 ■ POP3 User Experience Monitor port 110

SAM Templates

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

TEMPLATE	PORT	DESCRIPTION
Blackberry Delivery Confirmation template	25	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	79	This template tests the ability of the Finger service to accept incoming sessions on port 79.
Gopher Port Monitor	70	This template tests the ability of a Gopher server to accept incoming sessions on port 70.
IRC Port Monitor	6667	This template tests the ability of an IRC server to accept incoming sessions on port 6667.
Java Application Server (SNMP) template	1161	This template is configured to send SNMP requests on port 1161.
SNPP Port Monitor	444	This template tests the ability of an SNPP server to accept incoming sessions on port 444.
Windows FTP Server (via WMI)	21	This template monitors the Windows FTP Publishing Service and tests the ability of the FTP server to accept incoming sessions on port 21.

SAM 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

Additional Polling Engines

Additional Polling Engines have the same port requirements as primary polling engines, as outlined above.

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>.

Web Performance Monitor (formerly SEUM)

The following list of ports is required for the WPM Player, Recorder and the Web Interface.

PORT	TYPE	DESCRIPTION
80 (or 8787)	TCP	Default web port. If you specify any port other than 80, you must include that port in the URL used to access the web console. For example, if you specify an IP address of 192.168.0.3 and port 8080, the URL used to access the web console is http://192.168.0.3:8080 . Open the port to enable communication from your computers to the Orion Web Console. depends on what the default port for the Orion web interface is.
443	TCP	Used when a certificate for encryption to the Orion web interface is installed (SSL/HTTPS)
1433	TCP	Used for communication between the SolarWinds server and the SQL Server. Open the port from your Orion Web Console to the SQL Server.
17777	TCP	Used for Orion WPM traffic.
17781	TCP	The default port the SEUM Player listens on. This port must be open between the Orion server and the WPM player for proper communications.
17782	TCP	Used for player-initiated communications mode

Toolset

Desktop Toolset

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

COMPONENT	PORT	TYPE	DESCRIPTION
Syslog Server	514	UDP	Allows you to listen for incoming Syslog messages on UDP port 514.

COMPONENT	PORT	TYPE	DESCRIPTION
WAN Killer	7 9		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.
Netflow Realtime	2055		Listens on Port 2055
TFTP Server	69	UDP	
SNMP Polling	161		
Sending emails	25		

Web Toolset

- Uses port 443 for Secured SSH Connection.

Storage Manager (STM)

PORT	TYPE	DESCRIPTION
22	TCP	Used on the control system for EMC Celerra Storage Devices.
80	TCP	Used on the NetApp head/cluster node and any available CIFS/NFS.
161	UDP	Used for polling of Fiber Channel Switches: Cisco MDS, Brocade, McData, and QLogic Switches. Used on the EqualLogic Group IP.
162	UDP	Agents use this port to notify Storage Manager Server when information is available to be retrieved from the agent. If port 162 is in use by Orion NPM, then Storage Manager will use 10162 or 20162 when SNMP traps are sent to the Storage Manager Server.
443	TCP	Storage Manager uses this port to communicate with VMware Virtual Center or ESX server. Used on the NetApp head/cluster node and any available CIFS/NFS.
1094	TCP	Used by MS SQL application module.
1433	TCP	Used by MS SQL application module.

PORT	TYPE	DESCRIPTION
1521	TCP	Used by Oracle application module.
2463	TCP	Used to set RPC sessions to the storage controller from the SMI-S provider for LSI and SUN StorageTek storage devices.
3306	TCP	Used by the Storage Manager Database.
4319	TCP	Handles the collection from Storage Manager Agents and also acts as a local data collector/agent. Storage Manager communicates with data collectors/agents.
5988	TCP	HTTP port used by SMI-S providers.
5989	TCP	HTTPS port used by SMI-S providers.
8443	TCP	HTTPS port used to communicate with the Storage Profiler Module
9000	TCP	Storage Manager Web Console
17778	TCP	Required for access to the SWIS API
43501	TCP	Java Management Extensions (JMX) if blocked can also use 43052, 43503, and 43504. Allows web server to obtain memory from STM services (collector, event receiver, maintenance, and poller).

Storage Resource Monitor (SRM)

PORT	TYPE	DESCRIPTION
25		SSL/TLS for email alert actions should be enabled
80	TCP	<p>Default web port. If you specify any port other than 80, you must include that port in the URL used to access the web console. For example, if you specify an IP address of 192.168.0.3 and port 8080, the URL used to access the web console is http://192.168.0.3:8080 . Open the port to enable communication from your computers to the Orion Web Console.</p> <p>Used on the NetApp head/cluster node and any available CIFS/NFS.</p> <p>Used by EMC VNX/Clariion for file side performance.</p>
161	UDP	<p>Used for polling storage arrays through SNMP</p> <p>Used on the EqualLogic Group IP.</p>
443	TCP	<p>Used on the NetApp head/cluster node and any available CIFS/NFS.</p> <p>Used by EMC VNX/Clariion for file side performance.</p>
1433	TCP	Used for communication between the SRM and the SQL Server.

PORT	TYPE	DESCRIPTION
1434	UDP	The port used for communication with the SQL Server Browser Service to determine how to communicate with certain non-standard SQL Server installations. For more information, see this Microsoft Technet article .
1801	TCP	MSMQ WCF binding (for more information see this KB: http://support.microsoft.com/kb/183293).
5988	TCP	HTTP port used by SMI-S providers.
5989	TCP	HTTPS port used by SMI-S providers.
8088	TCP	HTTP Backup port used for NetApp DFM management servers for 7-mode arrays
8443	TCP	HTTPS port used by Storage Profiler SWIS
8488	TCP	HTTPS Used for NetApp DFM management servers for 7-mode arrays
17777	TCP	Orion module traffic. Open the port to enable communication from your poller to the Orion Web Console, and from the Orion Web Console to your poller. The port used for communication between the Orion Web Console and the poller.
17778	HTTPS	Required for access to the SWIS API
17779	HTTP/HTTPS	SolarWinds Toolset Integration

User Device Tracker (UDT)

PORT	TYPE	DESCRIPTION
80	TCP	Used to access the website
161	UDP	Used for SNMP (polling) traffic
1433	TCP	Used to communicate with MS SQL
17777	TCP	Information Service Protocol

Virtualization Manager (VMAN)

The port requirements of SolarWinds Virtualization Manager depend on the features and components that are in use. The features and components on which the port requirements depend are the following:

- VMware data collection
- Hyper-V data collection
- AD/LDAP authentication
- Sending email notifications (used in alerting and reporting)
- Sending SNMP traps (used in alerting)

- Orion integration
- Federated collectors

The following inbound ports need to be configured for communication with the Virtualization Manager master appliance:

PORT	DESCRIPTION
80	For HTTP access to the Virtualization Manager user interface.
8983	For performing auto-upgrade after installing hotfixes on federated collectors, if federated collectors are configured.
443	For HTTPS access to the Virtualization Manager user interface.
5480	For HTTPS access to the Management Console.
61616	For Active MQ master-collector communication.
22	For SSH access to the virtual appliance.

The following outbound ports need to be configured, depending on the individual setup and the functions you use:

PORT	DESCRIPTION
162	For sending SNMP traps.
25	For sending emails through SMTP.
389	For Active Directory authentication.
3268	For LDAP authentication.
17778	For communication with the Orion server if the integration with Orion is enabled.
123	For using the NTP service.

If you use Virtualization Manager integrated with NPM or SAM in an environment with multiple polling engines and federated collectors, make sure that you open TCP port 17778 from the primary collector to every polling engine that is used to poll virtualization data.

The following inbound ports need to be configured on the federated collector:

PORT	DESCRIPTION
5480	For HTTPS access to the Management Console.
22	For SSH access to the federated collector.

The following outbound ports need to be configured on the federated collector:

PORT	DESCRIPTION
61616	For Active MQ master-collector communication.
443 or 80	For performing auto-upgrade or version upgrade.
8983	For performing auto-upgrade after installing hotfixes.

Depending on the environment that is polled, the following outbound ports need to be configured on the master or the collector for data collection:

PORT	DESCRIPTION
443	For data collection from ESX hosts and vCenters.
7	For access to Hyper-V hosts that were added by using a fully qualified domain name.
135	For WMI data collection from Hyper-V hosts or VMs.
Dynamic RCP ports	For WMI communication. The available ports can be configured on the WMI target/policy.

VoIP & Network Quality Manager (VNQM)

The following table provides a list of all of the ports needed for communication with SolarWinds VNQM.

PORT	TYPE	DESCRIPTION
21	TCP	FTP (CDR/CMR download)
22	TCP	SFTP (CDR/CMR download) SSH for CLI (operation polling)
23	TCP	TELNET for CLI (operation polling)
80	TCP	HTTP port Default port used by additional web servers. If you change this setting, you must include the port in the URL used to access the web console.
161	UDP	Default UDP port of NPM, used by SNMP.
443	TCP	Used for conducting secure SSL communications.
17777	TCP	Must be opened for Orion module traffic.

Web Help Desk (WHD)

The following table provides a list of all of the ports needed for communication with SolarWinds Web Help Desk.

PORT	TYPE	DESCRIPTION
25	TCP	Traffic from the SolarWinds WHD appliance to your email server for automated email notifications
80	TCP	Non secure connection to EWS
110	TCP	Non Secure POP3
135	TCP	Asset discovery via WMI
143	TCP	Non Secure IMAP
389	TCP	Traffic from the SolarWinds WHD appliance to a designated server (usually a domain controller) for use with the Directory Service tool (LDAP, AD)
443	TCP	Secure connection to EWS
636	TCP	Secure traffic from the SolarWinds WHD appliance to a designated server (usually a domain controller) for use with the Directory Service tool (LDAP, AD)
993	TCP	Secure IMAP
995	TCP	Secure POP3
1433	TCP	Microsoft SQL external database, Lansweeper, Microsoft SMS/SCCM, Solarwinds NCM/NPM/SAM
1521	TCP	Oracle JDBC for Asset discovery
3306	TCP	MySQL external database, LANrev, Casper 8 and lower
4445	TCP	Remote log server reader
5432	TCP	External PostgreSQL database
5433	TCP	Asset discovery Apple Remote 3.2
7100	TCP	Asset discovery Sybase
8081	TCP	Non-secure traffic from the SolarWinds Web Help Desk Console
8443	TCP	Secure traffic from the SolarWinds Web Help Desk Console
17778	TCP	SolarWinds Orion Integration
20293	TCP	Embedded PostgreSQL
61616	TCP	Web Help Desk Discovery Engine