SolarWinds

Network Operations Manager

Version 2016.2

Installation Guide

Last Updated: Tuesday, October 4, 2016
Retrieve the latest version from: *https://support.solarwinds.com/Success_Center/Network_Performance_Monitor_(NPM)/Documentation*

Table of contents

Requirements 4

Software requirements 4

Hardware requirements 5

Server port requirements 6

Database server (SQL Server) requirements 8

NTA Flow Storage database requirements 10

Additional monitoring requirements 11

Requirements to monitor Microsoft Hyper-V, VMware ESXi, and ESX Servers 12

Configure the SolarWinds Orion server to use the correct syslog port 13

Optional requirements 13

Agent requirements 13

Agent resource consumption 15

Agent port requirements on the remote computer 15

Certificates and the agent 16

Quality of Experience requirements 16

Network Packet Analysis Sensors (NPAS) 16

Server Packet Analysis Sensors (SPAS) 17

Remote computer port requirements 17

NetPath requirements 17

Probe computer 17

Ports 18

Database storage 18

Cloud environment 19

Scalability 19

Security enhancements and exceptions **21**

Enable secure channels with SSL 21

Configure the Orion Web Console for SSL 21

Configure the Orion Web Console to require SSL 22

Enable FIPS 22

Antivirus exclusions 23

Directories 23

Orion server 24

SQL Server 24

Deploy SolarWinds Network Operations Manager 25

Install SolarWinds Network Operations Manager 25

Upgrade to Network Operations Manager 25

License your product 26

Activate licenses with Internet access 26

Activate licenses offline 27

Sizing and Best Practices resources 28

Server sizing considerations 28

Recommendations 28

SQL Server configuration best practices 28

Maximizing SQL Server performance 29

Hardware settings for SQL Servers 29

Recommendations for maximum performance 29

Recommendations for four logical disks 29

Recommendations for three logical disks 30

Recommendations for two logical disks 30

Recommendations for multi-CPU systems and the optimal settings of the I/O subsystem 30

Database file setting recommendations 31

Memory setting recommendations 31

CPU setting recommendations 32

Requirements

Software requirements

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

- Do not install SolarWinds software on domain controllers.
- SolarWinds neither recommends nor supports the installation of any Orion product on the same server or using the same database server as a Research in Motion (RIM) Blackberry server.

SOFTWARE	REQUIREMENTS
Operating system	■ Windows Server 2008 R2 SP1, 64-bit ■ Windows Server 2012 and 2012 R2, 64-bit Windows Server 2012 R2 Essentials is not supported.
Operating system languages	■ English (UK or US) ■ German ■ Japanese ■ Simplified Chinese
IP address version	IPv4 IPv6 implemented as a dual stack. For more information, see RFC 4213 - Basic Transition Mechanisms for IPv6 Hosts and Routers. 1. CIDR notation is not supported for IPv6 addresses. 2. SolarWinds High Availability does not support IPv6 addresses.
Web server	Microsoft Internet Information Services (IIS), version 7.5 or later ■ DNS specifications require that host names be composed of alphanumeric characters (A–Z, 0–9), the minus sign (–), and periods (.). Underscore characters (_) are not allowed. For more information, see RFC 952 - DOD Internet Host Table Specification. ■ IIS is installed by the SolarWinds installer. You can install this software manually to reduce your installation time or network bandwidth.

SOFTWARE	REQUIREMENTS
.NET Framework	.NET 4.5 Compatible with 4.6.1
Web console browser	■ Microsoft Internet Explorer version 11 or later with Active scripting ■ Microsoft Edge ■ Firefox 45.0 or later (Toolset Integration is not supported on Firefox) ■ Chrome 49.0 or later ■ Safari for iPhone
Other	■ RabbitMQ (primary messaging service between the primary and additional polling engines) ■ MSMQ (fall back and legacy messaging)
Services	The following services must be running after installation is complete to collect syslog messages and traps: ■ SolarWinds Syslog Service ■ SolarWinds Trap Service
User privileges	SolarWinds recommends that administrators have local administrator privileges to ensure full functionality of local SolarWinds tools. Accounts limited to the Orion Web Console do not require administrator privileges.

Hardware requirements

The following table lists minimum hardware requirements and recommendations for your SolarWinds server on both physical and virtual computers.

Use the minimum hardware configuration if you are evaluating the product or do not anticipate heavy usage.

> SolarWinds strongly suggests using the recommended hardware configuration for production environments to avoid potential performance issues caused by a heavy load or custom configurations such as increased data retentions or more frequent polling intervals.

HARDWARE	REQUIREMENTS
CPU speed	Quad core processor or better ⚠ Do not enable Physical Address Extension (PAE).
Hard drive space	30 GB minimum

HARDWARE	REQUIREMENTS
	40 GB recommended Two 146 GB 15K (RAID 1/Mirrored Settings) hard drives are recommended with a dedicated drive for the server operating system and installation. During upgrades the installer needs 1 GB of free space. Some common files may need to be installed on the same drive as your server operating system. You may want to move or expand the Windows temporary directories.
Memory	16 GB minimum 32 GB recommended

Server port requirements

The following table lists the port requirements for Network Operations Manager.

Ports 4369, 25672, and 5672 are opened by default. These ports can be blocked by the firewall.

PORT	TYPE	PRODUCT/ FEATURE	DESCRIPTION
11	ICMP	NPM	Used by the NetPath probe to discover network paths.
21	TCP	VNQM	Used for CDR/CMR downloads through FTP.
22	TCP	VNQM	The default port for CDR/CMR downloads through SFTP and CLI operations through SSH.
23	TCP	VNQM	The default port for CLI operations using telnet.
25	TCP	NPM	The SMTP port used for non-encrypted messages.
43	TCP	NPM	Used by NetPath to query IP ownership and other information about the discovered IP addresses.
53	TCP/ UDP	NTA	The TCP and UDP port used for DNS queries.
80	TCP	All	The 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.

Port	Type	Product/ Feature	Description
			The port is also used for Cisco UCS monitoring.
135	TCP	Agents	Open on the remote computer (inbound) to deploy the agent from the SolarWinds server.
137	UDP	NTA	The port used 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. ⓘ 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.
161	UDP TCP	All	The default port for Polling Devices and Statistics Collection using SNMP.
443	TCP	All	The default port for https binding. It is also used for bi-directional ESX/ESXi server polling or Cisco UCS monitoring.
445	TCP	Agents	Used for Microsoft-DS SMB file sharing. This port must be open on the client computer (inbound) for remote deployment.
465	TCP	All	The port used for SSL-enabled email alert actions.
514	UDP	NPM	The Syslog Service uses this port to listen for incoming messages.
587	TCP	All	The port used for TLS-enabled email alert actions.
1433	TCP	All	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. The port used for communication between the NTA Flow Storage and the NPM SQL server.
1434	UDP	All	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.

PORT	TYPE	PRODUCT/ FEATURE	DESCRIPTION
1801	TCP	All	Used with MSMQ WCF binding (for more information see this KB: http://support.microsoft.com/kb/183293).
2055	UDP	NTA	The default port for receiving flows on any NTA collector. It must be open for receiving flows on additional polling engines.
5671	TCP	All	The port used for SSL encrypted RabbitMQ messaging from the additional polling engines to the main polling engine.
17777	TCP	All	Used for 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.
17778	HTTPS TCP	All	The port is required for access to the SWIS API and agent communication. It is also used by the NetPath probe.
17779	HTTP	All	Used for SolarWinds Toolset Integration over HTTP.
17780	HTTPS	All	Used for SolarWinds Toolset Integration over HTTPS.
17791	TCP	agents	Open for agent communication on any SolarWinds Orion server running Windows Server 2008 R2 SP1.
Device Specific		NTA	Cisco NetFlow Configuration: The port used for NetFlow traffic is specified in the configuration of your Flow-enabled Cisco appliance.

Database server (SQL Server) requirements

Network Operations Manager and your SolarWinds Orion database must use separate servers.

Multiple Orion server installations using the same database are not supported.

If you install on a virtual machine, you must maintain your SQL Server database on a separate, physical drive.

The following table lists software and hardware requirements for your SolarWinds Orion database server.

HARDWARE/ SOFTWARE	REQUIREMENTS
SQL Server	SolarWinds supports Express, Standard, or Enterprise versions of the following: ▪ SQL Server 2008, 2008 SP1, 2008 SP2, 2008 SP3, or 2008 SP4

Hardware/ Software	Requirements
	■ SQL Server 2008 R2, 2008 R2 SP1, 2008 R2 SP2, or 2008 R2 SP3 ■ SQL Server 2012, 2012 SP1, 2012 SP2, or 2012 SP3 ■ SQL Server 2014 or 2014 SP1 ■ SQL Server 2016 ■ SolarWinds strongly recommends using the 64-bit version of SQL Server. ■ The `FullWithSQL` installer package automatically installs SQL Server 2014 Express. This is recommended for evaluations. You must install .NET 3.5 manually with this option. ■ Due to latency effects, SolarWinds does not recommend installing your SQL Server and your Orion server or additional polling engine in different locations across a WAN. For more information, see Install SolarWinds software and SolarWinds database (SQL Server) across a WAN. ■ You can set the database recovery model to Full recovery mode only if you use Always On Availability. We strongly recommend Simple recovery mode due to ensure best performance. SolarWinds does not support Full recovery mode.
SQL Server collation	■ English with collation setting `SQL_Latin1_General_CP1_CI_AS` ■ German with collation setting `German_PhoneBook_CI_AS` ■ Japanese with collation setting `Japanese_CI_AS` ■ Simplified Chinese with collation setting `Chinese_PRC_CI_AS` We support CI database on an CS SQL Server. We do not support case-sensitive databases.
CPU speed	Dual quad core processor or better
Hard drive space	100 GB minimum 400 GB recommended SolarWinds recommends the following configuration: ■ A hardware RAID Controller with a battery backed-up write back cache ■ Disk Subsystem 1 Array 1: 2x 146 GB 15K disks RAID 1 (mirroring) for the OS ■ Disc Subsystem 2 Array 2: 2x 146 GB 15K disks RAID 1 (Pagefile + Extra Storage) ■ Disk Subsystem 3 Array 3: with 6x 15k 146 GB or 300 GB disks configured in a RAID 1+0 array for your SQL MDF and FILEGROUPS.

Hardware/ Software	Requirements
	■ Disk Subsystem 4 Array 4: with 4x 15k 146 GB or 300 GB disks configured in a RAID 1+0 array for your SQL LDF Transaction LOG file ■ Disk Subsystem 5 Array 5: with 4x 15k 146 GB or 300 GB disks configured in a RAID 1+0 array for your tempdb data file ■ Disk Subsystem 6 Array 6: with 4x 15k 146 GB or 300 GB disks configured in a RAID 0 array for your tempdb log file ■ Due to intense I/O requirements, a RAID 1+0 drive is strongly recommended for the SolarWinds database, data, and log files with a dedicated drive for the server operating system and tempdb files. ■ Other RAID configurations can negatively affect your SQL Server's performance. ■ Mirrored drives for the OS and RAID 1+0 for database data files are recommended. ■ Solid state drives (SSD) are recommended for all components. Per Windows standards, some common files may need to be installed on the same drive as your server operating system. You may want to move or expand the Windows or SQL temporary directories.
Memory	64 GB minimum 128 GB recommended
Authentication	Either mixed-mode or SQL authentication
Other software	If you are managing your SolarWinds Orion database, SolarWinds recommends you install the SQL Server Management Studio component. The Installation Wizard installs the following required x86 components if they are not found on your Orion database server: • SQL Server System Common Language Runtime (CLR) Types. Orion products use secure SQL CLR stored procedures for selected, non-business data operations to improve overall performance. • Microsoft SQL Server Native Client • Microsoft SQL Server Management Objects

NTA Flow Storage database requirements

The following table lists the minimum hardware requirements for the NTA Flow Storage database which is used for storing flow data in NTA.

- Install the NTA Flow Storage database on a different server than the SolarWinds Orion database so the high amount of incoming flows will not affect the performance.
- Do not install the NTA Flow Storage database on a polling engine (main or additional) because it might affect performance.
- Use a dedicated disk for storing your flows data.
- Do not run anti-virus software or any other file scanning application over data in the NTA Flow Storage database. File scanning applications affect the database performance and may even prevent the database from running properly.

Type	Requirements
CPU	Evaluation environments - 2 CPUs Production environments - 4 CPUs or more (4 - 16 CPUs)
RAM	Evaluation environments - 8 GB or more Production environments - 16 GB or more (16 - 128 GB) To ensure optimal performance, you should increase RAM together with the database size.
Hard drive space	20 GB on a 7200 RPM disk or more With the default 30-day retention period and default top talker optimization, plan at least 8 GB of additional storage capacity per sustained 1000 flows per second. However, the required hard drive space depends on your flow traffic, and SolarWinds recommends you provide more space accordingly. NTFS file system required ⚠ Use RAID 0 or 1+0 with NTA. Other RAID or SAN configurations are not recommended, as they can result in data loss and significantly decreased performance.
OS	Microsoft Windows Server 2008 SP2 and later, 64-biy
.NET Framework	4.5

Additional monitoring requirements

The `SysObjectID` on monitored devices must be also accessible from the Orion server.

Requirements to monitor Microsoft Hyper-V, VMware ESXi, and ESX Servers

Requirement	Description
SNMP	SNMP must be enabled on all ESXi and ESX servers. For more information, consult your ESX or ESXi server vendor documentation.
Virtualization software	ESXi and ESX Server version 4.1 or later VMware vSphere version 4.1 or later Microsoft Hyper-V Server versions 2008 R2, 2012, 2012 R2
VMware tools	VMware Tools must be installed on all virtual machines you want to monitor. If your virtual machines are on monitored ESXi and ESX servers, VMware Tools are not a requirement but provide access to additional information, such as IP addresses.

For more information about requirements, see VIM Minimum Requirements in the SolarWinds Virtual Manager documentation.

The following methods are used to monitor VMware ESX Servers and their component features.

Features	4	4i	5i	6.0
Datacenter	VMware API			
ESX cluster	VMware API			
Virtual Center	VMware API			
Detection as ESX server	VMware API			
Volumes	SNMP	N/A	SNMP	
Interfaces	SNMP	SNMP (partial)	SNMP	
CPU	VMware API			
Memory	VMware API			
Total CPU (ESX details view)	VMware API			
Total memory (ESX details view)	VMware API			
Network traffic utilization (ESX details view)	VMware API			
Guest VM list (ESX details view)	VMware API			

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.

Optional requirements

Some features have additional requirements on either the monitored computer or on the SolarWinds Orion server.

- Agent requirements
- Quality of Experience requirements
- NetPath requirements
- SolarWinds High Availability requirements

Agent requirements

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

Before you deploy agents to a target computer, review the following system requirements for the remote computer.

Type	Windows Requirements	Linux
Operating System	Windows Server 2008 Windows Server 2008 R2 Windows Server 2008 R2 SP1 Windows Server 2012 Windows Server 2012 R2 Windows 7, Windows 7 SP1 Windows 8, Windows 8.1 Windows 10	Red Hat Enterprise Linux 5 Red Hat Enterprise Linux 6 Red Hat Enterprise Linux 7 CentOS 5 CentOS 6 CentOS 7 SUSE Linux Enterprise Server 10

TYPE	WINDOWS REQUIREMENTS	LINUX
	⚠ Only Pro, Enterprise, and Ultimate workstation operating systems editions are supported.	- SUSE Linux Enterprise Server 11 - SUSE Linux Enterprise Server 12 - Ubuntu 14, 64-bit only - Amazon AMI, 64-bit only
Other Windows software	The following software packages are installed by the agent installer if necessary: - Microsoft Visual C++ 2013 Redistributable Package for 32-bit or 64-bit - .NET Framework 4.0 (You must install this manually if you are installing an agent on Windows Server 2008 R2 or earlier or Windows Core) - .NET Framework 4.5 (Required for Windows Server 2008 R2 SP1 and later)	You may need to install the following manually: - Python 2, versions 2.4.3 and later ⓘ Python 3 is not supported
Security	The VeriSign Root Certificate Authority (CA) must be current. This is required because the agent software is signed using a VeriSign certificate. To install a certificate, see Certificates and the agent. After the agent is installed, it runs as a Local System account and does not require administrative permissions to function.	
Account permissions	If you want to deploy agents from the Orion server, the following requirements must be met: - The account used for remote deployment must have access to the administrative share on the target computer: `\\<hostname_or_ip>\admin$\temp`. - User Account Control (UAC) must either be disabled on the target computer, or the built-in Administrator account must be used. ⓘ - You may need to disable UAC remote restrictions. - Other remote or mass deployment methods do not have the same requirements.	- An account that can connect remotely through SSH. - An account that can install software and create a user and group.
HDD	Approximately 100 MB of hard drive space on the target computer, for installation only	

Agent resource consumption

RESOURCE	CONSUMPTION
CPU	Less than 1% on average under normal operating conditions (0.24% on average)
Memory	10 - 100 MB, depending on the number and types of jobs
Bandwidth	Roughly 20% (on average) of the bandwidth consumed by the WMI protocol for transmission of the same information For example, Agent: 1.3 kB/s versus WMI at 5.3 kB/s
Storage	100 MB when installed

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

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

Agent port requirements on the remote computer

PORT	COMMUNICATION METHOD	OS	DESCRIPTION
17778	Agent-initiated	Windows Linux	Used continuously by the agent to communicate back to the Orion server. Also used to deploy the agent.
17791	Agent-initiated	Windows 2008 R2	Used continuously by the agent to communicate back to the Orion server. Also used to deploy the agent. This must be opened if the remote computers you monitor run Windows 2008 R2.
17790 (inbound)	Server-initiated	All	Used to communicate with the Orion server. This must be open on the remote computer.
135 (inbound)	Either	Windows	(DCE/RPC Locator service) Microsoft EPMAP. This port must be open on the client computer for remote deployment.
445 (inbound)	Either	Windows	Microsoft-DS SMB file sharing. This port must be open on the client computer (inbound) for remote deployment.
22	Either	Linux	(TCP) Used to install the agent on Linux computers through SSH and SFTP or SCP. TCP port 22 (outbound) must be open on the Orion server or additional polling engine and open (inbound) on the computer you want to

PORT	COMMUNICATION METHOD	OS	DESCRIPTION
			monitor.

Certificates and the agent

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

For more information, search for "Add the Certificates Snap-in to an MMC" at technet.microsoft.com.

Quality of Experience requirements

Before you deploy a Packet Analysis Sensor to a device to monitor QoE, review the following minimum system requirements for the remote computer.

You will need administrative privileges for each node or switch.

⚠ Sensors **cannot** be installed on 32-bit computers and do **not** support communication over https.

Network Packet Analysis Sensors (NPAS)

<table>
<tr><th>HARDWARE/SOFTWARE</th><th colspan="2">REQUIREMENTS</th></tr>
<tr><td>OS</td><td colspan="2">Windows 7 or later, 64-bit
Windows Server 2008 or later, 64-bit</td></tr>
<tr><td>CPU Cores</td><td colspan="2">2 CPU Cores + 1 CPU Core per 100 Mbps</td></tr>
<tr><td>Hard drive space</td><td colspan="2">500 MB</td></tr>
<tr><td>RAM</td><td colspan="2">1 GB + 1 GB per 100 Mbps
(2 GB + 1 GB per 100 Mbps recommended)</td></tr>
<tr><td>Network</td><td colspan="2">1Gbps maximum throughput</td></tr>
<tr><td rowspan="2">Port monitoring</td><td>For a physical monitored switch:
▪ SPAN
▪ Mirror port
▪ In-line tap</td><td>For a virtual monitored switch:
▪ Promiscuous port groups
▪ vTap</td></tr>
<tr><td colspan="2">Port monitoring requires at least one extra network interface to collect data from the managed network interface, a server to monitor the copied traffic, and a network cable to connect the mirrored port to the physical server.</td></tr>
</table>

HARDWARE/SOFTWARE	REQUIREMENTS
	View your vendor documentation for instructions about how to set up port mirroring. You can create port mirrors for both physical switches and virtual switches.

Server Packet Analysis Sensors (SPAS)

HARDWARE/SOFTWARE	REQUIREMENTS
OS	Windows 7 or later, 64-bit Windows Server 2008 or later, 64-bit ⓘ 32-bit operating systems are not supported.
CPU Cores	2 CPU Cores + 1 CPU Core per 100 Mbps
Hard drive space	500 MB
RAM	256 MB + 500 MB per 100 Mbps (256 MB recommended + 500 MB per 100 Mbps)
Network	1Gbps maximum throughput

Remote computer port requirements

See Agent requirements.

NetPath requirements

Probe computer

Probes are the source of network paths, and the paths are discovered by probes.

You create a probe on a source computer, which must meet the following requirements:

TYPE	REQUIREMENTS
Operating system (64-bit only)	Windows Server 2008 R2 SP1 Windows Server 2012 Windows Server 2012 R2 Windows 7 Windows 8 Windows 8.1 Windows 10 Professional and Enterprise

TYPE	REQUIREMENTS
	ⓘ Windows 10 Home edition is not supported.
CPU cores	2 CPU cores for 20 paths +1 CPU core per 10 additional paths
Hard drive space	1 GB
RAM	2 GB

Ports

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

PORT	PROTOCOL	SOURCE	DESTINATION	DESCRIPTION
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	TCP	Main polling engine	BGP data providers	Used by NetPath™ to query IP ownership and other information about the discovered IP addresses.

Database storage

When calculating the size requirements in SQL Server for NetPath™, you must account for the probing interval and the complexity of the network path from the probe to the monitored service. The complexity of the path is divided into three groups:

- Internal: services with fewer than 10 hops between the probe and the monitored service.
- Intermediate: multiple paths ending in a single endpoint node. Examples are github.com, linked.com, and visualstudio.com.
- Complex: multiple paths (over 20) ending in multiple endpoint nodes. Examples are google.com and yahoo.com.

This table provides an estimate in megabytes (MB) of the amount of storage consumed by SQL Server over a 30-day period (the default retention time) when monitoring a single service.

INTERVAL (IN MINUTES)	INTERNAL (IN MB)	INTERMEDIATE (IN MB)	COMPLEX (IN MB)
1	520	1105	1615
2	325	645	1145
3	200	445	915
4	170	350	750
5	135	265	480
10	80	175	470

Example storage requirement calculation

Your monitoring setup contains the following:

- Five internal monitors with a one-minute interval.
- Three intermediate monitors with a five-minute interval.
- Four complex monitors with a ten-minute interval.

The total storage requirement for SQL Server can be calculated as:

(5 × 520) + (3 × 265) + (4 × 470) = 5275 MB over a 30-day time period.

Cloud environment

When you place a probe in a public cloud, consider the following additional requirements:

PROVIDER	REQUIREMENTS
Amazon	■ Security group must be enabled on instances that host NetPath™ probes to allow inbound ICMP packets. ■ Probing services that host on Amazon Web Services (AWS) instances within the same cloud networks may not work.
Azure	■ Private Internet Protocol (PIP) must be enabled on instances that host NetPath™ probes. ■ Probing may work within VNET, but may not work if the path crosses the Azure Load Balancer.

Scalability

The scalability of NetPath™ depends on the complexity of the paths you are monitoring, and the interval at which you are monitoring them.

In most network environments:

- You can add up to 100 paths per polling engine.
- You can add 10 - 20 paths per probe.

  NetPath™ calculates the recommended path count based on the performance of each probe, and displays it each time you deploy a new path to the probe.

Security enhancements and exceptions

By default, SolarWinds uses the http protocol instead of https. You can increase the security of your data by using SSL or FIPS.

- Enable secure channels with SSL
- Enable FIPS

For best performance, SolarWinds also recommends creating an antivirus directory exclusion for the SolarWinds install folder.

Enable secure channels with SSL

SolarWinds products support the use of Secure Sockets Layer certificates to enable secure communications with the Orion Web Console.

Requirements

- Your server must have the required SSL certificate installed.
- Conduct secure SSL/TLS communications over port 443.

⚠ Due to security concerns, SolarWinds recommends that you disable SSL v3.0 and earlier.

1. Add a binding to https port 443 for the SolarWinds NetPerfMon site. For more information, consult the Microsoft online documentation on setting up SSL.
2. Enable the Orion Web Console for SSL.
3. You can also configure the Orion Web Console to require SSL.

Configure the Orion Web Console for SSL

1. Log in to your Orion server using an account with administrative rights.
2. Shut down all SolarWinds services. Start the Orion Service Manager in the SolarWinds Orion > Advanced Features program folder, and click Shutdown Everything.
3. Start the Database Manager from the SolarWinds Orion > Advanced Features program folder.
4. Expand the SQL servers, and navigate to SQL Servers > `your SolarWinds Orion database server` > SolarWindsOrion > Websites in the left pane.
   - If your SQL Server is not listed in the left pane, click Add Default Server.
   - If your Orion database is not listed in the left pane, add it:
     a. Click Add SQL Server.
     b. Using the format `Server\Instance`, select or provide the SQL Server instance you are using as your SolarWinds Orion database.
     c. Select the login method, providing credentials as required.
     d. Click Connect to Database Server.
5. Right-click the Websites table, and click Query Table.

6. Replace the default query with the following query, and click Refresh.

   ```
   UPDATE dbo.Websites SET SSLEnabled=1 WHERE WebsiteID=1
   ```

7. Switch to the Orion Service Manager, and click Start Everything.
8. Change the Orion Web Console port.
   a. Start the Configuration Wizard in the SolarWinds Orion > Configuration and Auto-Discovery program folder.
   b. Select Website, and click Next on the Welcome window.
   c. Enter the SSL port number, and click Next.

      > Port 443 is typically reserved for SSL traffic.

   d. Review the configuration summary, and complete the Configuration Wizard.

Configure the Orion Web Console to require SSL

1. In a text editor, open the web console configuration file, `web.config`, on your primary SolarWinds server.

   > The default location of web.config is `C:\Inetpub\SolarWinds\`.

2. In the `<system.web>` section, add the line:

   ```
   <httpCookies requireSSL="true" />
   ```

3. Locate the line:

   ```
   <forms loginUrl="~/Orion/Login.aspx" />
   ```

4. Edit it to `<forms loginUrl="~/Orion/Login.aspx" requireSSL=”true” />`.
5. To enable the HTTPOnly flag for added security, locate the `<httpCookies>` tag, and edit it to the following:

   ```
   <httpCookies httpOnlyCookies="true" requireSSL="true" />
   ```

6. Save and close web.config.

Enable FIPS

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

Monitored nodes and network discoveries must use FIPS-compliant authentication and privacy or encryption methods.

FIPS-Compliant Methods	
Authentication	SHA1
Privacy or encryption	AES128, AES192, AES256

> ⓘ SolarWinds recommends that you install all FIPS-compliant SolarWinds software on FIPS-compliant servers and maintain all non-compliant SolarWinds software on non-compliant servers.

1. Configure the Orion server for FIPS compliance. See the Microsoft Support knowledge base for more information.
2. Start the SolarWinds FIPS 140-2 Manager (`SolarWinds.FipsManager.exe`).

   > ⓘ By default, `SolarWinds.FipsManager.exe` is located in the `Install_Volume:\Program Files (x86)\SolarWinds\Orion` folder.

3. Read the welcome text, and click Next.
   The SolarWinds FIPS 140-2 Manager will confirm that the current configuration of your SolarWinds products is FIPS-compliant.
   - If an installed product is not FIPS-compliant, click Close, remove any non-compliant Orion Platform products from the FIPS-compliant server, and run the FIPS 140-2 Manager again.
   - If FIPS 140-2 is disabled, select Enable FIPS 140-2, and click Next.
   - If the FIPS Manager provides a list of objects or saved network discovery definitions that are not FIPS-enabled, complete the following steps.

     > ⓘ To refresh the list of non-compliant objects after editing the credentials, restart the FIPS 140-2 Manager.

     - Click the non-compliant monitored node, and edit its Polling Method to be FIPS-compliant.
       a. Select SNMPv3 as the SNMP Version.
       b. Select FIPS-compliant Authentication and Privacy/Encryption methods, and provide the passwords.
       c. Click Submit.
     - Click the non-compliant network discovery, and edit SNMP credentials to be FIPS-compliant.
       a. Confirm that all SNMP credentials are SNMPv3. Delete or edit any credentials that are not FIPS-compliant SNMPv3.
       b. Confirm that all SNMP credentials use FIPS-compliant Authentication and Privacy/Encryption methods, and provide the passwords.
       c. Complete the Network Sonar Wizard using the updated credentials.
4. Click Restart now to restart all relevant SolarWinds services.

Antivirus exclusions

To run SolarWinds products you may need to exclude certain directories and ports from your antivirus software and add service accounts.

Directories

Ensure that NPM has access to all required files by excluding the following directories from antivirus protection.

- Do not exclude executable files.
- SolarWinds assumes that C:\ is the default install volume.

Orion server

- `C:\Inetpub\SolarWinds\`
- `C:\ProgramData\SolarWinds\`
- `C:\Program Files (x86)\Common Files\SolarWinds\`
- `C:\Program Files (x86)\Microsoft SQL Server\`
- `C:\Program Files (x86)\SolarWinds\`
- `C:\Windows\Temp\SolarWinds\`
- `C:\Windows\Microsoft.NET\Framework\v2.0.50727\Temporary ASP.NET Files`
- `C:\Windows\Microsoft.NET\Framework\v4.0.30319\Temporary ASP.NET Files`
- `C:\Windows\Microsoft.NET\Framework64\v2.0.50727\Temporary ASP.NET Files`
- `C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Temporary ASP.NET Files`

If you are using NetFlow Traffic Analyzer, also exclude also the NTA Flow Storage Database directory and the appropriate backup directory from the antivirus protection.

SQL Server

- `C:\Program Files\Microsoft SQL Server\`
- `C:\Program Files (x86)\Microsoft SQL Server\`

Deploy SolarWinds Network Operations Manager

After you have reviewed and complied with the system requirements, install Network Operations Manager.

Install SolarWinds Network Operations Manager

⚠ Do not install SolarWinds products on a domain controller or use the same database server as a Research in Motion (RIM) Blackberry server.

1. Log in as an administrator to the server on which you are installing SolarWinds Network Operations Manager.
2. Extract the contents of the downloaded installation .ZIP file, including any .ZIP files included inside of the file.
3. Install SolarWinds NPM.

   ⓘ Downloading and installing Microsoft .NET Framework 4.5 can take more than 20 minutes. If your computer reboots, run the installation again.
4. Run the Configuration Wizard.
5. Install the following products in order. Do not run the Configuration Wizard until all products have been installed.
   a. NTA
   b. VNQM
   c. UDT
6. Run the Configuration Wizard.

Upgrade to Network Operations Manager

If you have one or more product modules included with Network Operations Manager, upgrade your products. Use the Multiple Products Upgrade Guide for an upgrade checklist, upgrade gotchas, and to build your upgrade path.

ⓘ You can skip checking the product requirements and use the Network Operations Manager system requirements instead.

After you have upgraded your previously installed product modules, install your new modules using the installation instructions. Skip any module that you have already upgraded.

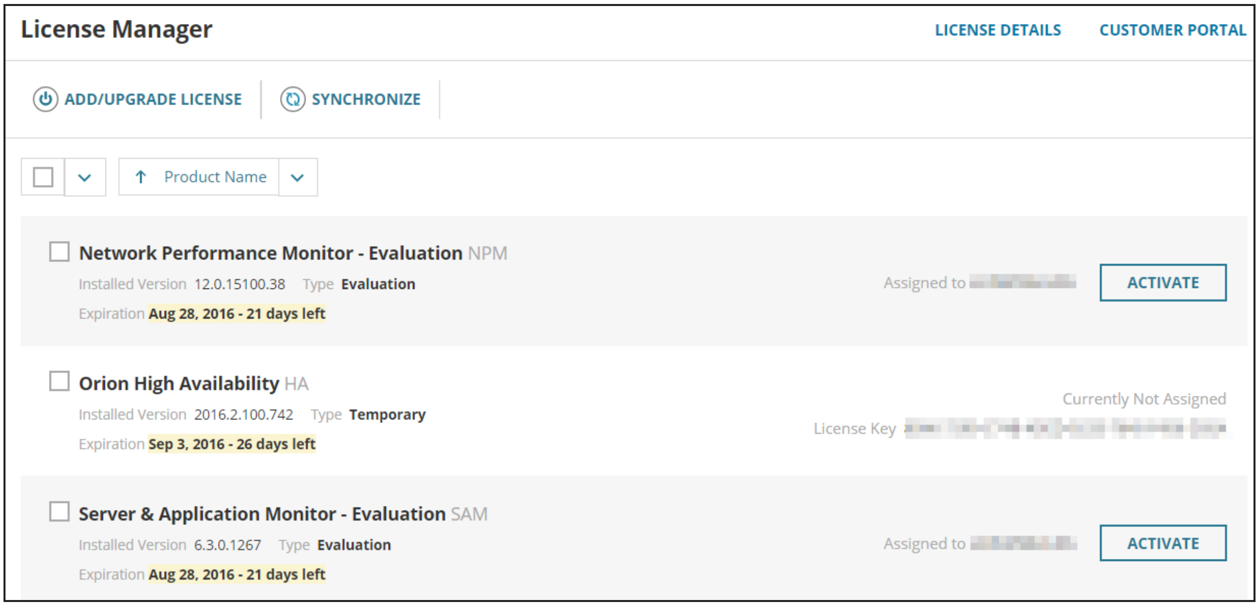
License your product

⚠ Activate your NPM license first before activating other licenses.

Activate licenses with Internet access

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

1. Open the Orion Web Console.
2. Click Settings > All Settings > License Manager.



□ **Network Performance Monitor - Evaluation** NPM
Installed Version 12.0.15100.38 Type **Evaluation**
Expiration **Aug 28, 2016 - 21 days left**
Assigned to [redacted]

□ **Orion High Availability** HA
Installed Version 2016.2.100.742 Type **Temporary**
Expiration **Sep 3, 2016 - 26 days left**
Currently Not Assigned
License Key [redacted]

□ **Server & Application Monitor - Evaluation** SAM
Installed Version 6.3.0.1267 Type **Evaluation**
Expiration **Aug 28, 2016 - 21 days left**
Assigned to [redacted]

3. Select each module installed with Network Operations Manager, click Activate.

   ⓘ If you are upgrading to Network Operations Manager, click Add/Upgrade License.

4. Enter the activation key.
   a. Click Customer Portal, and log in using your Customer ID and password, or your individual user account information.
   b. On the top menu bar, click License Management > License Management.
   c. Click the plus sign next to Network Operations Manager to display your activation keys.
   d. Copy the unregistered activation keys, 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 your product on a computer without Internet access, the web-based License Manager guides you through offline activation.

1. Open the Orion Web Console.
2. Click Settings > All Settings > License Manager.
3. Select a product, and click Activate.

   > ⓘ If you are upgrading to Network Operations Manager, click Add/Upgrade License.

4. Click Copy to Clipboard to copy the unique machine key.
5. Log in to the Customer Portal, and click License Management > License Management.
6. In the Customer Portal License Management, expand the product license to activate, and click Activate License Manually.
7. Paste the unique machine id from clipboard, and click Generate License File. Save the `.lic` file locally and transfer it to the offline computer.
8. 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.

Sizing and Best Practices resources

Server sizing considerations

Listed from the most important to the least important are the primary variables that affect scalability.

Number of monitored elements

> An element is defined as a single, identifiable node, interface, or volume. A single polling engine can monitor up to 12,000 elements. Monitoring some node types, such as routers, place more load on the system.

Polling frequency

> If you are collecting statistics every five minutes instead of the default nine minutes, the system will have to work harder and system requirements will increase.

Number of simultaneous users

> The number of simultaneous users accessing the Orion Web Console directly impacts system performance. We recommend limiting the number of simultaneous users to between 10 to 20 sessions per web site. You can install additional websites to handle larger user loads.

Recommendations

When planning a SolarWinds installation, there are four main factors that limit your polling capacity:

- CPU
- Memory
- Number of polling engines
- Polling engine settings

Be aware of these variables, and consider the following SolarWinds recommendation.

Use additional polling engines for 12,000 or more monitored elements

> If you plan to monitor 12,000 or more elements, SolarWinds recommends that you install additional polling engines on separate servers to help distribute the work load.

SQL Server configuration best practices

The standard SQL environment contains the following components:

- A dedicated SQL Standard or Enterprise Server
- Directly attached (DAS), RAID 10 storage (I/O subsystem)
- LAN attachment between the main Orion server and any additional components

If there are more databases on a given SQL Server, it is strongly recommended that you use dedicated hard drives for the tempdb database. Use at least one hard drive for data files, and one hard drive for the transaction log. All databases use the same tempdb, therefore the tempdb can be the biggest bottleneck in the I/O subsystem.

Maximizing SQL Server performance

When planning your SQL Server configuration, consider the following information:

- WAN connections should never be used between the SQL server and the Orion server. This includes any additional pollers.
- Do not install the SQL Server on the Orion server.
- The performance of the SQL Server is dependent on the performance of the I/O subsystem.
- The more disks there are in a RAID 10 array, the better.
- Many RAID controllers do not handle RAID 01 well.
- Solid state drives will improve performance.

Hardware settings for SQL Servers

The following section contains the recommended hardware settings for SQL Servers, taking into account different scenarios and the number of logical disks you use.

Recommendations for maximum performance

COMPONENT	RECOMMENDATION
Orion database	▪ A dedicated RAID 1+0 hard drive for data files (.mdf, .ndf). ▪ A dedicated RAID 1+0 hard drive with fast sequential writing for transaction files (.ldf).
SQL Server temporary directory (tempdb) database	▪ A dedicated RAID 1+0 hard drive for data files (.mdf, .ndf). ▪ A dedicated RAID 1+0 hard drive with fast sequential writing for transaction files (.ldf).
SQL Server host system (Windows)	▪ A dedicated hard drive of any type.

Recommendations for four logical disks

This configuration is recommended for medium deployments.

COMPONENT	RECOMMENDATION
Orion database	▪ A dedicated RAID 1+0 hard drive for data files (.mdf, .ndf). ▪ A dedicated RAID 1+0 hard drive with fast sequential writing for transaction files (.ldf).

COMPONENT	RECOMMENDATION
SQL Server temporary directory (tempdb) database	- A dedicated hard drive for data files (.mdf, .ndf) and the transaction log (.ldf)
SQL Server host system (Windows)	- A dedicated hard drive of any type. This hard drive should be the slowest of the four available disks.

Recommendations for three logical disks

COMPONENT	RECOMMENDATION
Orion database	- A dedicated RAID 1+0 hard drive for data files (.mdf, .ndf). - A dedicated RAID 1+0 hard drive with fast sequential writing for transaction files (.ldf).
SQL Server temporary directory (tempdb) database and SQL Server host system (Windows)	- A dedicated hard drive for tempdb data files (.mdf, .ndf), tempdb transaction log (.ldf), and host system.

Recommendations for two logical disks

- Use the disk with the faster sequential writing for the host system and for the transaction log files (.ldf).
- Use the other disk for data files (.mdf, .ldf), for the tempdb data files, and for the tempdb log files.

Recommendations for multi-CPU systems and the optimal settings of the I/O subsystem

On multi-CPU systems, the performance of some operations can be increased by creating more data files on a single hard drive.

> ⓘ Every logical CPU is considered to be one CPU.

The following example shows the original settings of a system with 16 CPU cores:

- One hard drive for data with the `SolarWindsOrionDatabase.MDF` file in the Primary filegroup.
- One hard drive for the transaction log with the `SolarWindsOrionDatabase.LDF` file.
- One hard drive for the tempdb data with the `tempdb.MDF` file in the Primary filegroup.
- One hard drive for the tempdb transaction log with the `tempdb.LDF` file.

The previous settings can be improved in the following way:

- One hard drive for data, with the following files in the Primary file group:
  - `SolarWindsOrionDatabase01.MDF`
  - `SolarWindsOrionDatabase02.NDF`
  - `SolarWindsOrionDatabase03.NDF`
  - `SolarWindsOrionDatabase04.NDF`
- One hard drive for the transaction log with the `SolarWindsOrionDatabase.LDF` file.
- One hard drive for tempdb data, with the following files in the Primary filegroup:
  - `tempdb01.MDF`
  - `tempdb02.NDF`
  - `tempdb03.NDF`
  - `tempdb04.NDF`
- One hard drive for the tempdb transaction log with the `tempdb.LDF` file.

> - Having more files in the filegroup help the SQL Server to distribute the load generated by multiple threads while working with files.
> - The recommended ratio between the number of cores and the files in the filegroup is typically 4:1 or 2:1 (for example, 16 cores and four files, or 16 cores and eight files).
> - The size and growth setting for all files in a filegroup must be set to identical values in order to distribute the load evenly.
> - For the transaction log, it is not effective to create more files, because the SQL Server can only use the first file.
> - For the tempdb database, a RAM disk or an SSD disk can be used.
> - An SSD disk can be used for data files, but it is not effective for the transaction log where sequential access is most important.

Database file setting recommendations

- Pre-allocate as much disk space as possible to save time.
- Define an absolute auto-growth setting with a reasonable size (500 MB, 1 GB, and so on), instead of an auto-growth percentage.

Memory setting recommendations

- Do not reserve all memory to the SQL Server, because this can lead to a lack of memory for the host operating system.
- Reserve 1 GB of memory to the host operating system if there are no additional services running on the given host system.
- If additional resource-intensive services are running on the host operating system, reserve sufficient memory for the host operating system. SolarWinds does not recommend such configuration.

CPU setting recommendations

- Ensure that power-saving technologies are disabled on the CPU.