



SECURITY WHITE PAPER

SolarWinds N-central

Version 11.2

Contents

Contents	3
Overview	5
Architecture	6
Probes and Agents	6
Probe and Agent Communications	6
Probe as a Cache	7
SolarWinds N-central Server	7
Port Access Requirements	7
The Upgrade Process	13
Agent and Probe Upgrade	13
Software Upgrades for Backup Manager and AV Defender	14
Remote Control	15
MSP Connect/MSP Anywhere	15
TCP Mode (Required)	16
UDP Mode (Optional)	17
MSP Anywhere	17
Other Remote Control Connections	18
Security Manager	20
Upgrades and Updates	20
Product Upgrades (Major Releases)	20
Product Updates (Hot Fixes)	21
Definition File Updates (Security Signatures)	23
More Information on Definition File Updates	23
Backup Management	25
SolarWinds Backup	25
Arcserve Backup	25
Mobile Device Management (MDM)	27

MDM Port Requirements27

Port Requirements27

Patch Management for Windows28

Managing Windows Updates28

Managing Third-Party Updates30

Monitoring for Missing Patches31

Scheduled Tasks32

Physical Security33

Security Implications34

Report Manager Integration34

LDAP Integration34

Overview

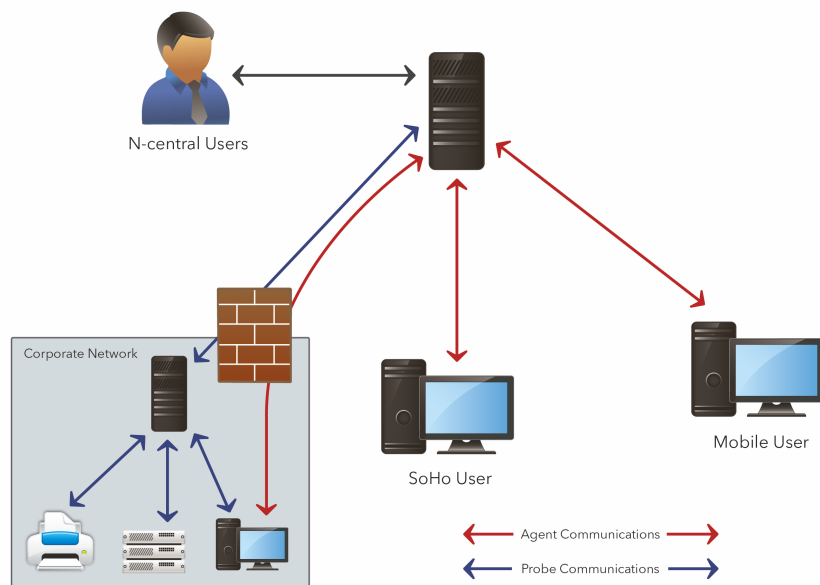
As an integral component of your IT management system, SolarWinds N-central® complements an organization's existing security policies and infrastructures. SolarWinds N-central consists of a number of components that were specifically designed to provide flexibility as well as to ensure the integrity of the security of the networks on which SolarWinds N-central operates.

The goal of this guide is to discuss each of the components of SolarWinds N-central at a high level.

Architecture

To better understand the impact that SolarWinds N-central may have on the security of the networks that it manages, it is necessary to have an understanding of its components and design.

SolarWinds N-central consists of three major components: Agents, Probes, and the SolarWinds N-central server.



Probes and Agents

A Probe is a Windows application that resides on a system within a customer's network, behind their firewall or within their private IP space. Probes provide network discovery, monitoring and management services for devices on that private network, leveraging industry standard protocols such as WMI, SNMP, ODBC, and others.

An Agent is an additional software component that may be installed on a Microsoft, Mac OS X, or Linux host device in order to gather data specific to that local device. Agents are typically installed on all Windows devices to provide full monitoring and management regardless of the logical placement of that device on the Internet.

Probe and Agent Communications

SolarWinds N-central Probes and Agents communicate with the SolarWinds N-central server using similar architecture and methods. The Probes and Agents leverage client-side initiated communications, where all data communications begin with an outbound call from the Agent or Probe.

As a direct result of this architecture, there is no public IP address or port forwarding required from the Internet to the devices running the Probes or Agents. The outbound communications from the Agents to the SolarWinds N-central server are based on SOAP and XMPP, and are transmitted using the HTTP or HTTPS protocols on the standard web ports. The nature of these communications allows for the support of standard proxies on the local network.

After the outbound session is established, the Agent receives a session ID that is used to identify that session and it persists until the session is closed. The Agents and Probes will open a second (asynchronous) signalling channel leveraging the XMPP protocol (on port 80/443) that is persistent to allow the SolarWinds N-central server to signal the Agents and Probes when actions are necessary (such as to initiate a remote control session). In cases where the XMPP session is terminated abnormally (for example, by a firewall cleaning open sessions), the Agent will re-create the session automatically.

SolarWinds N-central leverages the XMPP based communications for control purposes only, not for the transmission of monitored data. As an additional measure, the XMPP protocol can be turned off for individual devices or globally, however, this is not recommended as this will increase system load and will cause latency on certain SolarWinds N-central features.

By default, the SolarWinds N-central Agent, Probe, and XMPP-based communications use HTTPS with the data encrypted using TLS and the strongest cipher suite supported by both the client and the server.

Probe as a Cache

The Windows Probe also acts as a cache location for software installation files such as the Agent, AV Defender, Backup Manager, and Windows Patches. Agents communicate with the Probe over TCP 10004 using the .NET remote communication protocol.

SolarWinds N-central Server

The SolarWinds N-central server is the "brains" of the system and contains a number of components including the Web Interface, the SolarWinds N-central Administrator Console (NAC), Data Management System (DMS), Database, and other core system components. In addition to providing an interface for the Agents and Probes, the DMS is also the business logic layer of the application. All rules that govern how SolarWinds N-central deals with data are executed at this level. All physical data (configuration or monitored) is stored within the relational PostgreSQL database.

The SolarWinds N-central server is designed and secured so that it may be placed directly on the Internet, however, the recommended best practice is to place it in a restricted internet zone such as a DMZ.

For specific information on the ports that must be accessible for an SolarWinds N-central server, please refer to *"Port Access Requirements"* below, and also in the *"SolarWinds N-central System Requirements"* section of the Installation Guide.



Port Access Requirements



Access must be permitted to the following ports:

PORT NUMBER	PORT LOCATION				DESCRIPTION
	SOLARWINDS N-CENTRAL SERVER		MANAGED DEVICE		
	INBOUND	OUTBOUND	INBOUND	OUTBOUND	
20		√			Used for FTP connections, particularly when configured for backups.
21		√			Used for FTP connections, particularly when configured for backups.
22	√			√	SSH - used for remote control sessions. The firewall must be configured to allow access from the Internet to this port on the SolarWinds N-central server.
25		√			SMTP - used for sending mail.
53		√			Used for DNS.
80	√	√		√	<p>HTTP - used for communication between the SolarWinds N-central UI and Agents or Probes (including MSP Connect and MSP Anywhere).</p> <p>The firewall must be configured to allow access from the Internet to this port on the SolarWinds N-central server.</p> <p>This port must also be open for outbound traffic if the SolarWinds N-central server is monitoring the HTTP service on a managed device.</p>

PORT NUMBER	PORT LOCATION				DESCRIPTION
	SOLARWINDS N-CENTRAL SERVER		MANAGED DEVICE		
	INBOUND	OUTBOUND	INBOUND	OUTBOUND	
	<div><div><div><div><div></div><div>i</div></div></div><div>Inbound access to port 80 on the N-central server can be blocked provided that all Agents are configured to use HTTPS and the N-central server is accessed over port 443 using HTTPS.</div></div></div>				
123		√			Used by the NTP Date service which keeps the server clock synchronized. Normally using UDP (although some servers can use TCP).
135			√		Used by Agents and Probes for WMI queries to monitor various services. <div><div><div><div><div></div><div>i</div></div></div><div>Inbound from the Windows Probe to the Windows Agent.</div></div></div>
139			√		Used by Agents and Probes for WMI queries to monitor various services. <div><div><div><div><div></div><div>i</div></div></div><div>Inbound from the Windows Probe to the Windows Agent.</div></div></div>
443	√	√		√	HTTPS - used for communication between the SolarWinds N-central UI and Agents or Probes (including MSP Connect and MSP Anywhere).

PORT NUMBER	PORT LOCATION				DESCRIPTION
	SOLARWINDS N-CENTRAL SERVER		MANAGED DEVICE		
	INBOUND	OUTBOUND	INBOUND	OUTBOUND	
					<p>Port 443 is the TCP port needed for SSL (HTTPS) connections. The firewall must be configured to allow access from the Internet to this port on the SolarWinds N-central server.</p> <p>This port must also be open for outbound traffic if the SolarWinds N-central server is monitoring the HTTPS service on a managed device.</p> <p>Backup Manager relies on Port 443 TCP outbound. It is almost always open on workstations but may be closed on servers. This port must be open for outbound traffic on the SolarWinds N-central server.</p>
445			√		Used by Agents and Probes for WMI queries to monitor various services.
1234		√		√	Used by MSP Connect in UDP mode.
1235		√		√	
1433		*	*	*	Outbound on the SolarWinds N-central server, port 1433 is used by Report Manager for data export. On managed devices, it is also used by Agents (inbound) and Probes (out- bound) to monitor Backup Exec jobs.

PORT NUMBER	PORT LOCATION				DESCRIPTION
	SOLARWINDS N-CENTRAL SERVER		MANAGED DEVICE		
	INBOUND	OUTBOUND	INBOUND	OUTBOUND	
					<div> Inbound from the local LAN and not the Internet.</div> <div><p>* Port access is only required if you have installed the corresponding product. For example, access to port 1433 is only required if you have installed Report Manager or if you are managing Backup Exec jobs.</p></div>
5000		√			Backup Manager will use local port 5000. If this port is unavailable, Backup Manager will detect a free port automatically (starting from 5001, 5002 and up).
5280	√			√	Used by Agents and Probes for XMPP traffic.
8014			√		Backup Manager requires access to port 8014. This value cannot be modified. <div><div> Inbound from the local LAN and not the Internet.</div></div>
10000	√				HTTPS - used for access to the SolarWinds N-central Administration Console (NAC). The firewall must be configured to allow access from the Internet to this port on the SolarWinds N-central server.

PORT NUMBER	PORT LOCATION				DESCRIPTION
	SOLARWINDS N-CENTRAL SERVER		MANAGED DEVICE		
	INBOUND	OUTBOUND	INBOUND	OUTBOUND	
10004			√	√	<p>SolarWinds N-central Agents must be able to communicate with a Probe on the network over port 10004 in order for Probe caching of software updates to function properly.</p> <div> Inbound from the local LAN and not the Internet.</div>
15000			√	√	<p>For downloading software patches, port 15000 must be accessible for inbound traffic on the Probe device while it must be accessible for outbound traffic on devices with Agents.</p> <div> Inbound from the local LAN and not the Internet.</div>

The SolarWinds N-central server must be able to resolve (and access over FTP - TCP ports 20, 21, UDP ports above 1024 for Passive Transfer) the following domain name:

- `send.solarwinds.com`

The SolarWinds N-central server must be able to resolve (and access over HTTP TCP port 80) the following domain name:

- `sis.n-able.com`

The SolarWinds N-central server must be able to resolve (and access using HTTPS TCP port 443) the following domain names:

- `update.n-able.com`
- `feeds.n-able.com`

- servermetrics.n-able.com
- push.n-able.com
- scep.n-able.com
- licensing.n-able.com
- microsoft.com

The SolarWinds N-central server itself is based on the CentOS 6.x operating system which was fully patched at the time of the release. Additional updates are distributed as required through the standard SolarWinds N-central Hotfix or Service Pack process. This same process applies to all internal components such as the database and application servers. The SolarWinds N-central server includes an integrated firewall designed to secure the system from unwanted network traffic.

Internally, the system is built using industry standard best practices including:

- storage of all user passwords by first encrypting them using one-way encryption
- strong input type checking
- user access permissions
- protective support for cross site scripting (XSS) attacks

The Upgrade Process

Upgrading SolarWinds N-central involves not only upgrading the SolarWinds N-central server but also the Agents and Probes that communicate with it. For detailed instructions on how to perform an upgrade, refer to *"Upgrading to This Release"* in the Release Notes.

The upgrade process for SolarWinds N-central 11.2 consists of a number of elements including:


Agent and Probe Upgrade

1. The SolarWinds N-central server is upgraded.
2. The first time that the Probe connects to the SolarWinds N-central server after it has been upgraded, the Probe will detect the new version. The Probe will be updated automatically if it has been configured to do so.
3. After being upgraded, the Probe will automatically download the latest version of the Agent upgrade software and store it in the C:\Program Files (x86)\N-able Technologies\Windows Software Probe\cache directory.
4. If the Agents have been configured to upgrade automatically, they will:
 - a. Ping all of the Probes with which they can communicate to determine which Probe provides the fastest response time.
 - b. Download the Agent upgrade software from the fastest Probe they can communicate with using the .NET Remoting using TCP/IP via port 10004.
5. If the Agents cannot connect to a Probe, they will download the Agent upgrade software directly from the SolarWinds N-central server.

Software Upgrades for Backup Manager and AV Defender

Upgrades for Backup Manager and AV Defender follow the same procedure:


1. The Windows Probe will communicate with sis.n-able.com to determine the latest upgrade software every hour. If a new version is available, the Windows Probe will download the latest upgrade software.
2. If software is installed on a device (Backup Manager or AV Defender), the Agent will communicate via port 443 with the Windows Probe (or Probes) on the network to determine if it is running the latest version.
3. The Agent will download the upgrade software from the Probe using the .NET Remote API mechanism.

 For Backup Manager, if the Agent cannot download the upgrade software from a Probe, it will download it directly from <http://rmdmdownloads.ca.com>.

The SolarWinds N-central server will connect with sis.n-able.com on an hourly basis to check for new upgrades. If a newer version of the software is available, the appropriate service (for example, the AV Defender Status service for AV Defender) will transition to a Warning state until the software on that device is upgraded.


Remote Control

A key feature of SolarWinds N-central is the ability to remotely control any managed device, regardless of the user's location on the Internet. Remote control in SolarWinds N-central leverages the location of the SolarWinds N-central server on the Internet and the outbound communications model provided by Agents and Probes.

 Remote Control is available on SolarWinds N-central servers with a Professional license.

SolarWinds N-central uses the following methods to establish encrypted connections from the SolarWinds N-central server to the remote control target device:

- MSP Connect and MSP Anywhere, new remote management tool that replaces Direct Connect for devices upgraded with SolarWinds N-central 11.2 Agents.
- Other remote control types use connections established through one of SSH (Secure Shell) or HTTPS (Hypertext Transfer Protocol, Secure).

 In some circumstances, security scans performed on SolarWinds N-central servers may report vulnerabilities related to SSH that are based on the reported SSH version string (as the SSH version string is a truncated, high-level value). It is strongly recommended that you confirm that any reported vulnerabilities are fixed in that build of OpenSSH before further investigating the issue.

No matter which of the three protocols is used, you will need a user name and password in order to access the remote device.

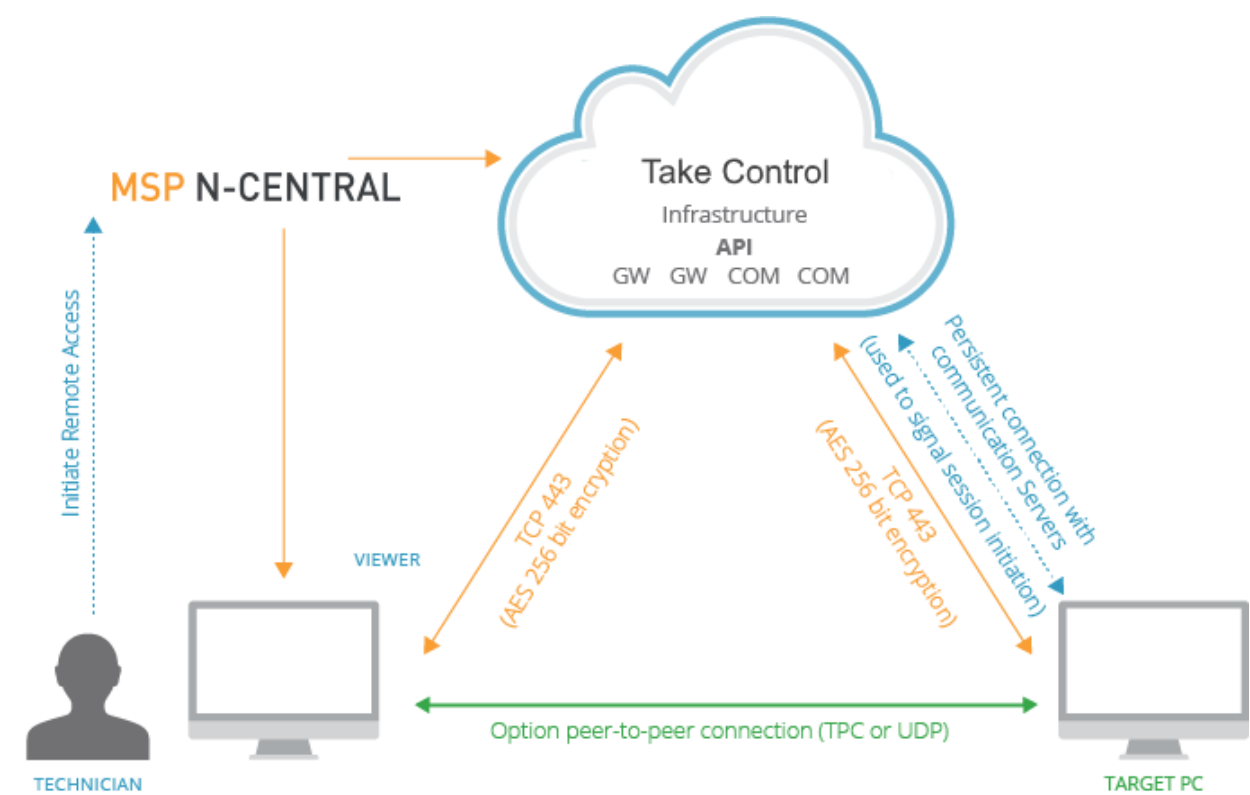
MSP Connect/MSP Anywhere

Take Control sessions are sheltered by a proprietary communication protocol with guaranteed global security by the Rijndael Advanced Encryption Standard (AES) using a 256-bit cipher (both when establishing or for the duration of the session). The key exchange is protected by an SSL based in AES-CBC with TLS v1.1. All commands, including keyboard and mouse strokes, file transfers and clipboard information are digitally signed.

Take Control does not have access to session content. All encryption is based on an end-to-end negotiation that does not intercept transferred information or decode the information in the gateway. Encryption keys are randomly generated for each session.

As an additional security measure, the client can configure an authentication method using a Master-Password or Windows Account and configure pre-authorization by the machine owner to launch the session.

Finally, all major features, including remote control, file transfer and chat conversations are logged in the Session details and can be video recorded.



The ports identified in the tables below must be accessible for Take Control and MSP Anywhere remote control connections.

💡 Mac OS uses TCP Mode only.

TCP Mode (Required)

If the agent has a direct TCP port configured, the same port must be open at the agent's firewall and be accessible by the viewer.

PORT NUMBER	PORT LOCATION			
	TAKE CONTROL VIEWER		TARGET DEVICE	
	INBOUND	O	I	O
		UTBOUND	NBOUND	UTBOUND
Port 80		✓		✓
Port 443		✓		✓
Port 3377		✓		✓
ⓘ Take Control fails over to this port as an alternative connection method.				

When using Take Control, the SolarWinds N-central server must be able to resolve the following domain names:

- *.mspa.n-able.com
- sis.n-able.com

When using MSP Anywhere, the SolarWinds N-central server must be able to resolve the following domain names:

- *.beanywhere.com
- mspa.n-able.com
- *.pubnub.com

UDP Mode (Optional)

Take Control can use the UDP transmission model to connect to devices in addition to TCP.

Initially, the Take Control viewer requires access to port 1234. After the system administrator modifies the firewall to enable the identified IP addresses to communicate with the server, the ports can be random.

PORT NUMBER	PORT LOCATION			
	TAKE CONTROL VIEWER		TARGET DEVICE	
	INBOUND	OUTBOUND	INBOUND	OUTBOUND
Port 1234		√		√
Port 1235		√		√

MSP Anywhere

To prevent AV Defender from blocking MSP Anywhere access, you need to configure AV Defender exclusions. Add the following components to the AV exclusion list:

- BASupApp.exe
- BASupTSHelper.exe

If after configuring these exclusions there are still issues establishing a connection, ensure that the following components are also excluded:

- agent.exe
- AgentMaint.exe
- NCentralRDViewer.exe
- BASEClient.exe

Should connection issues persist, re-install AV Defender and restart the system.

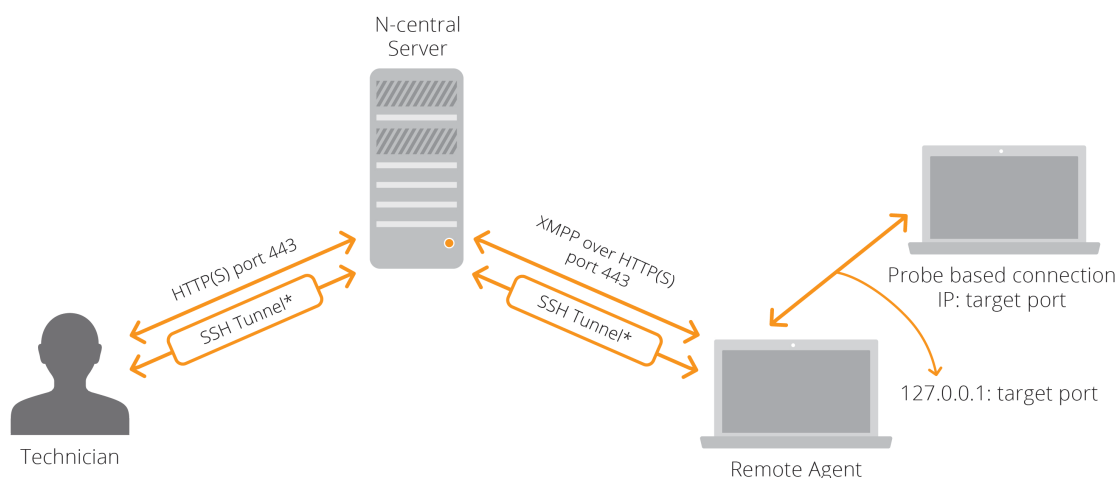
Other Remote Control Connections

For remote control types other than Direct Connect and Attended Remote Control, the first protocol attempted will be an SSH tunnel (TCP on port 22). Should the SSH connection attempt fail, the requesting user and the target system will again attempt to connect to each other through the SolarWinds N-central server using HTTPS on port 443.

PORT NUMBER	PORT LOCATION			
	SOLARWINDS N-CENTRAL SERVER		TARGET DEVICE	
	INBOUND	OUTBOUND	INBOUND	OUTBOUND
Port 22		√		√
Port 443		√		√

After the requesting user and the target system are connected, the remote control tools can then communicate over this encrypted connection as if they were located on the same network subnet. Since the remote control sessions originate outbound from the user's system, as well as from the device to be remotely controlled, there is no requirement for a public IP address, or inbound port forward for this remote control tool to work.

RC - Other Methods



Remote control in SolarWinds N-central uses several layers of security. The outbound request model ensures that there are no inbound reports required.

Data passed through SSH connections is encrypted using 128-bit AES-based encryption keys.

Data passed through HTTPS connections uses the HTTP (Hypertext Transfer Protocol) in combination with SSL (Secure Socket Layer) and TLS (Transport Layer Security). SSL and TLS are cryptographic protocols that provide secure communications on the Internet. HTTPS is designed for secure encrypted communication between different devices as well as secure identification and authentication of the remote device.

Security Manager

Security Manager is a fully integrated Antivirus/Anti-Malware engine designed to provide comprehensive protection to Windows Servers and Workstations. More information on this feature can be found in the SolarWinds N-central Online Help.

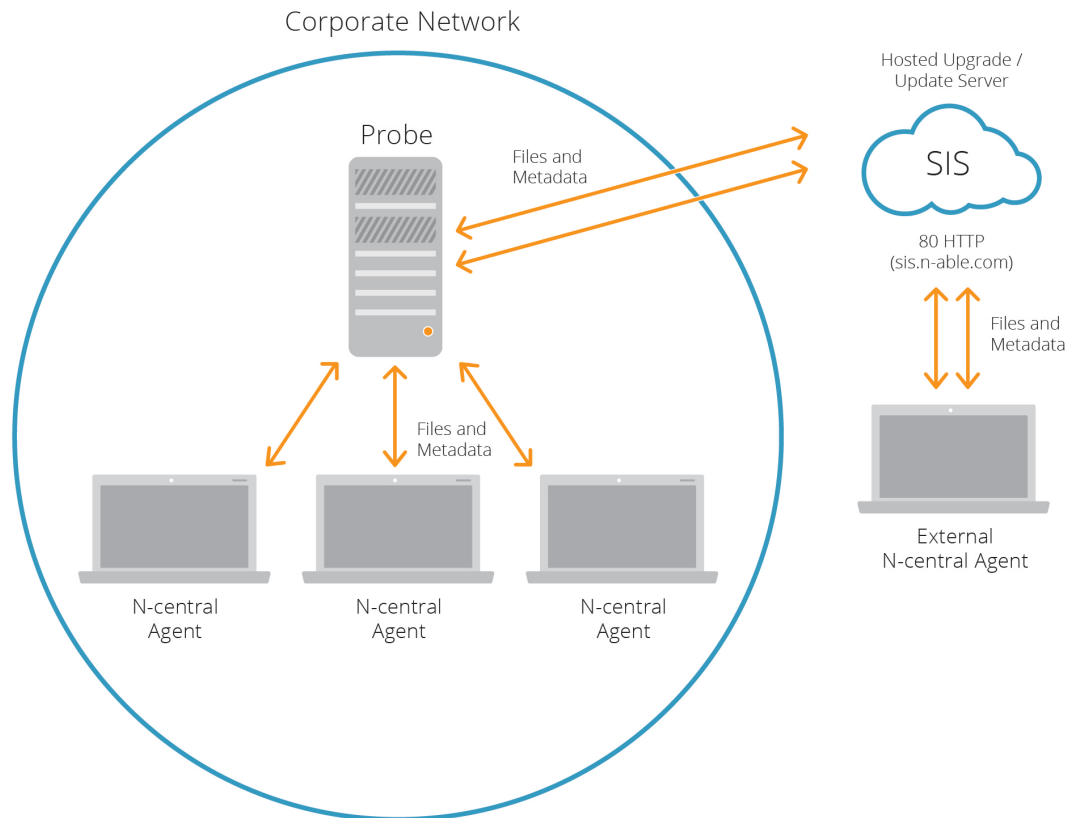
The security features of SolarWinds N-central provide for flexible deployment and updating without posing undue load on the service provider or end user networks. This is achieved through a distributed update architecture. This architecture is outlined below, and consists of the SolarWinds N-central server, Agents, Probes, and an SolarWinds MSP hosted update server.

Upgrades and Updates

Upgrades and updates to the Bitdefender software can be divided into three categories:

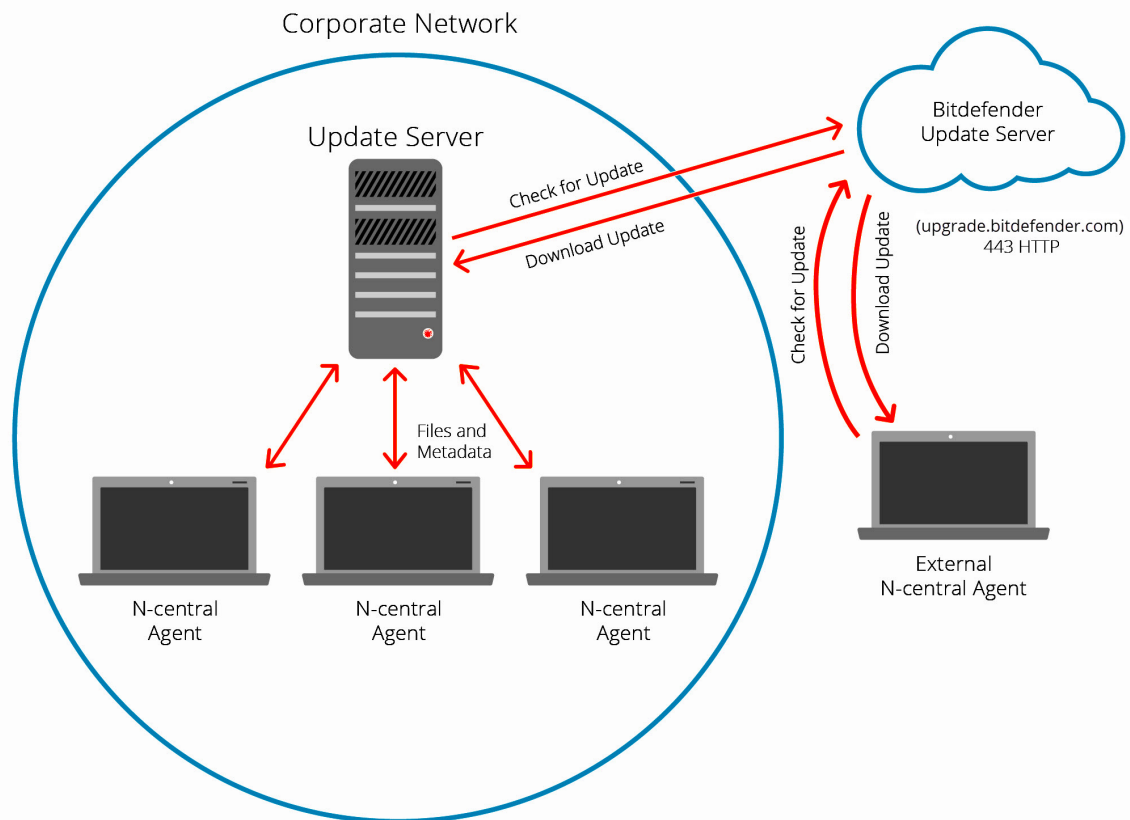
Product Upgrades (Major Releases)

1. The Agent will attempt to download the catalog file from sis.n-able.com every time that is specified in the Maintenance Windows usually every hour.
2. If an upgrade is available, the AV Defender Status service will transition to a Warning state to indicate that an upgrade is available.
3. AV Defender will download from the probe of and apply the upgrades as defined by the maintenance Window or when configured to do so from the All Devices View > Upgrade Monitoring Software. Re-starting devices is usually needed following a product upgrade and the AV Defender Status service will indicate that a restart is required and the Agent will initiate the restart once it is permitted by the Maintenance Window.

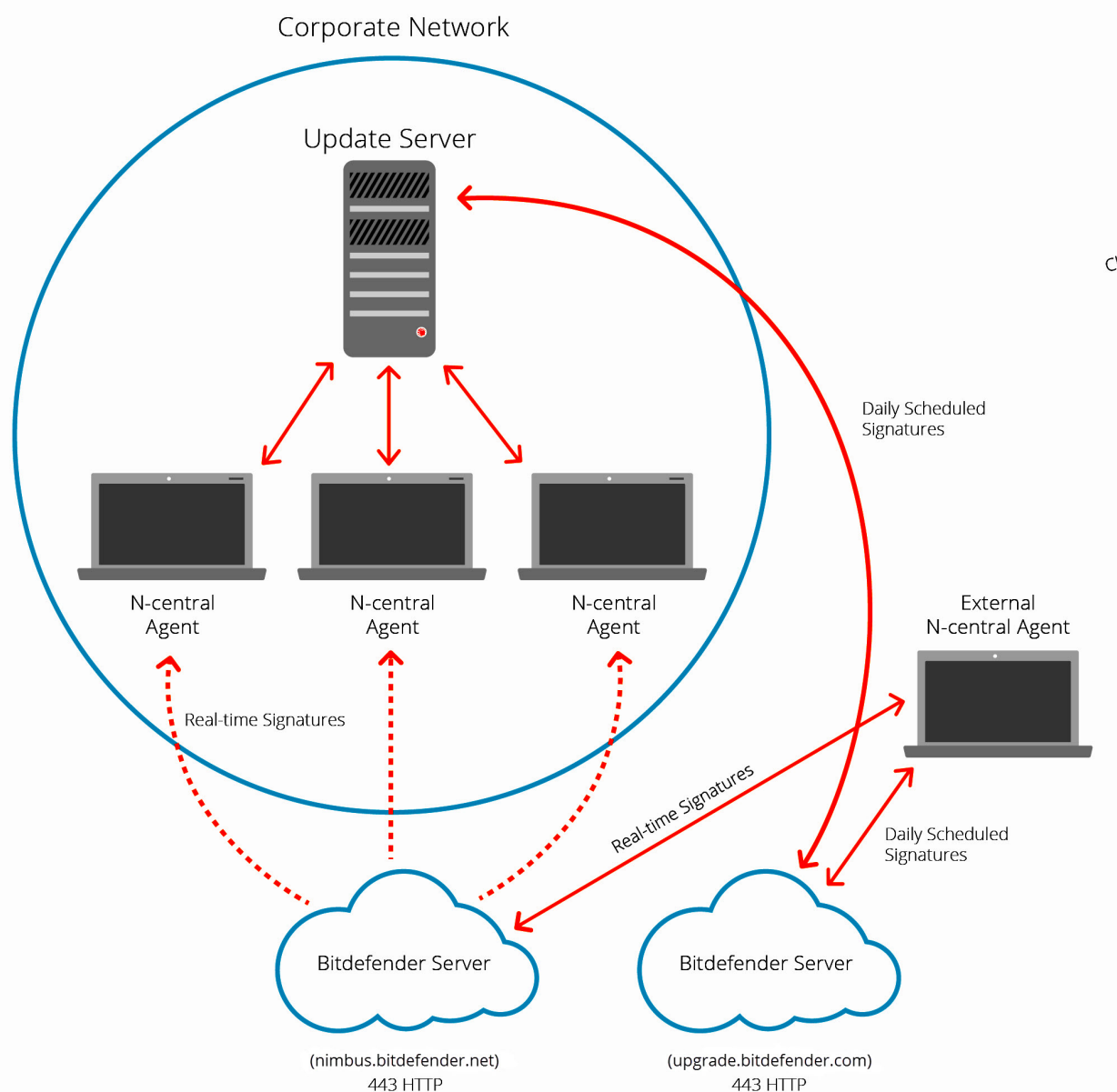


Product Updates (Hot Fixes)

1. AV Defender checks the local Update Server for Updates.
2. The Update Server checks upgrade.bitdefender.com for updates every half hour.
3. Agents outside of the corporate network checks upgrade.bitdefender.com directly for Updates.
4. AV Defender Status service will transition to a Warning state.
5. The Update is downloaded from the Update Server or upgrade.bitdefender.com.
6. AV Defender Updates are installed by the Maintenance Windows or manually.



Definition File Updates (Security Signatures)



More Information on Definition File Updates

Ensuring that your definition files are up to date is a critical aspect of managing AV Defender. Again, SolarWinds N-central leverages a distributed architecture to make distribution of these files fast and efficient.

- AV Defender Profiles in N-central allow the user to configure the update frequency as well as the failover behavior.

- Local Update Servers check for updates from the Bitdefender Update Server (upgrade.bitdefender.com) on a specific schedule.
- Definition File Updates are downloaded from the Update Server if available or directly from Bitdefender all using port 443.
- If an update server is configured for a Customer or Site, then AV Defender will use the local update server. If no update servers are selected, the AV Defender Status service will transition to a Warning state.
- If the Allow Failover to External Update Server property is enabled and Immediately is selected, AV Defender will obtain Definition file updates from upgrade.bitdefender.com.
- If the Allow Failover to External Update Server property is enabled and After <x> Hours is selected, AV Defender will then try to obtain updates from local update servers after every configured interval period has ended. If it is unable to check for updates for the configured number of hours, it will obtain the next update directly from the Bitdefender update server using port 443.

SECURITY MANAGER PROFILES - SETTINGS

Name: Default Profile - Laptops/Workstations High Protection

Description: Default AV Defender Profile with settings for Laptops/Workstations high protection

Settings

Associations

Display

Advanced

Update

SETTINGS DETAILED EXPLANATION [?]

Update Interval (Hours): 1

Proxy Settings: Use agent proxy

Server:

Port:

User Name:

Password: (unset)

☐ Show Password

Allow Failover to External Update Server: ☒

Failover to External Update Server if Local Server is Not Accessible: ☐ Immediately ☒ After 3 Hours

Backup Management

SolarWinds N-central backup management provides data backup and restore capabilities through bare metal restore and incremental snapshots in one package. You can do this on physical and virtual servers from local disk or off premise cloud storage.

With SolarWinds N-central backup management, with either Arcserve or SolarWinds Backup, you never have to do another full backup, greatly reducing network traffic, disk storage and load on production applications. Centralized deployment, management and reporting reduces implementation and management effort and provide status information directly to you for increased peace of mind.

Backup management relies on TCP outbound port 443 and local port 5000. If this port is not available, it automatically searches for a free port starting at port 5001 and continuing upward. In most cases, no additional firewall configuration is needed.

SolarWinds Backup

SolarWinds Backup is a hybrid cloud-based backup and recovery platform. SolarWinds Backup operates seamlessly in the background, storing data in reliable, secure data centers away from your customer's devices. Restoration of data can be for a single file or an entire system. SolarWinds N-central integrates with SolarWinds Backup to act as a conduit between SolarWinds Backup and the cloud storage to configure profiles and schedules.

SolarWinds Backup performs an initial full backup and then performs continual incremental backups. SolarWinds MSP uses True Delta(tm) deduplication and compression to transfer only blocks of data that have changed. This greatly reduces network traffic and the time required to backup data. Centralized deployment, management and reporting reduces implementation and management effort and provides status information directly to you. All backup data is encrypted locally using AES 256-bit encryption prior to transfer to the data center. Encryption uses an encryption key set by the service provider. Data is further protected in transit using TLS 1.2 and AES 256-bit encryption.

SolarWinds Backup provides an easy way to manage and control backups by:

- managing the deployment of tens or hundreds of devices,
- monitors backups to ensure they are working, and
- tests backups to ensure they are stable.

Arcserve Backup

Arcserve Backup provides a cost-effective, local solution that provides data backup and restore capabilities. It enables you to keep your customers' data safe using incremental snapshots and bare metal restore functionality.

Incremental backups require only one full backup and then continual incremental backups. This greatly reduces network traffic, disk storage and load on production applications. Centralized deployment, management and reporting reduces implementation and management effort and provides status information directly to you.

Arcserve Backup performs:

- A Full backup - a complete block-level backup,
- Incremental backups - a backup of only data that has been modified since the previous backup, and
- Verification- a re-synchronization of backups to ensure there has been no data loss or damage.

Mobile Device Management (MDM)

Managing mobile devices is performed using a connection to SolarWinds N-central's Mobile Device Management service. When SolarWinds N-central attempts to communicate with a mobile device, SolarWinds N-central sends a silent notification to the device prompting it to check in with the server. The device communicates with the server to see if there are tasks pending and responds with the appropriate actions. These tasks can include updating policies, providing requested device or network information, or removing settings and data.

MDM Port Requirements

Port Requirements

The table below outlines the TCP open port configurations required to send/receive push notifications.


PORT NUMBER	PORT LOCATION				DESCRIPTION
	SOLARWINDS N- CENTRAL SERVER		TARGET NETWORK SERVER		
	INBOUND	O UTBOUND	I NBOUND	O UTBOUND	
80		√	√		
443		√	√		
2195		√			Access to ports 2195 and 2196 must be granted to gateway.push-apple.com.akadns.net.
2196		√			
5222			√		
5223			√		
5228			√		TCP and UDP mode.

Patch Management for Windows

SolarWinds N-central includes a patch management solution that lets you provide service offerings to your customers. This section provides information for MS Windows Patch Management.

There are two aspects to N-central's patch management module:

- [Managing Windows updates](#)
- [Managing Third Party software patches](#)

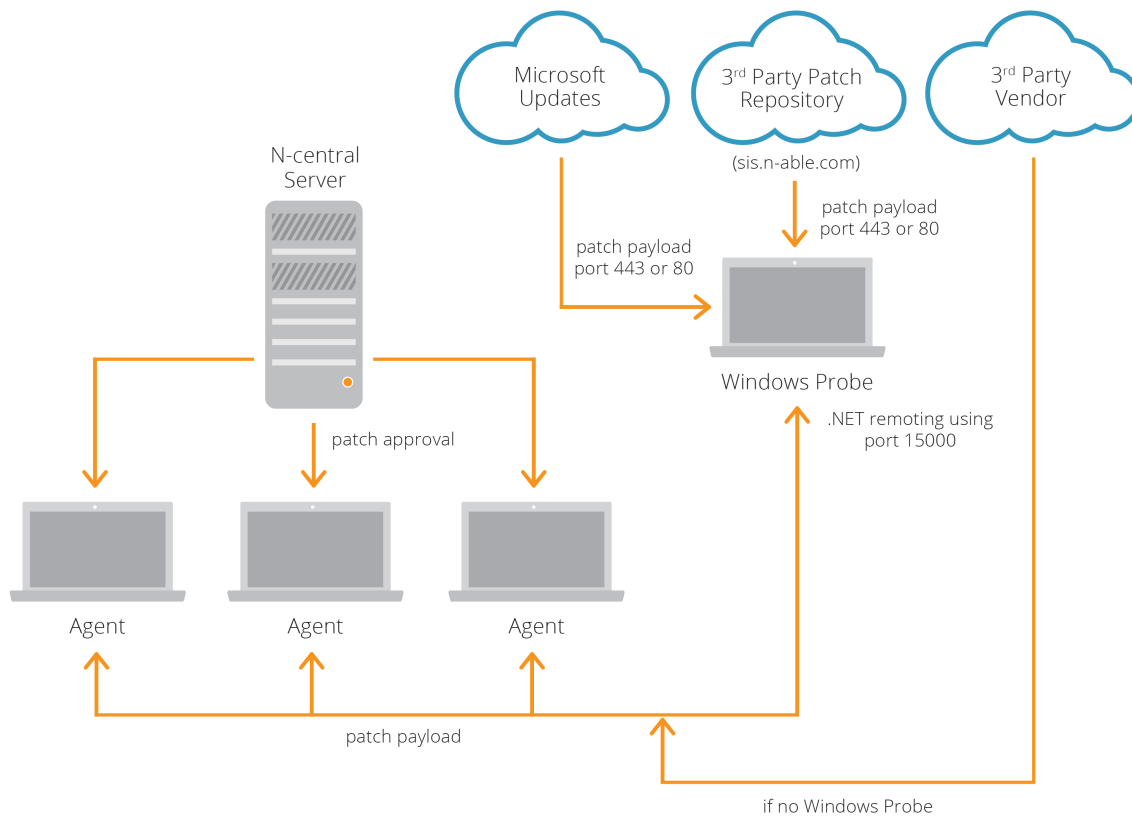
 SolarWinds N-central does not support uninstalling Microsoft patches for Windows Vista and Server 2008.

For devices using Windows 8 or Windows Server 2012 operating systems, Flash ActiveX is treated as a Windows Feature Update. Use Microsoft Patch Management to approve or decline Flash ActiveX updates for these devices.

Managing Windows Updates


1. The Windows Agent communicates with Windows Updates and requests a list of available updates.
2. The Windows Agent transmits this information to the SolarWinds N-central server.
3. The SolarWinds N-central administrator configures approvals for the list of updates.
4. The Windows Agent communicates with the Probe and requests the approved updates.
5. The Probe downloads the updates.
6. The Windows Agents download the updates from the Probe.
7. The Windows Agent applies the schedule for installing updates.

Patch Management

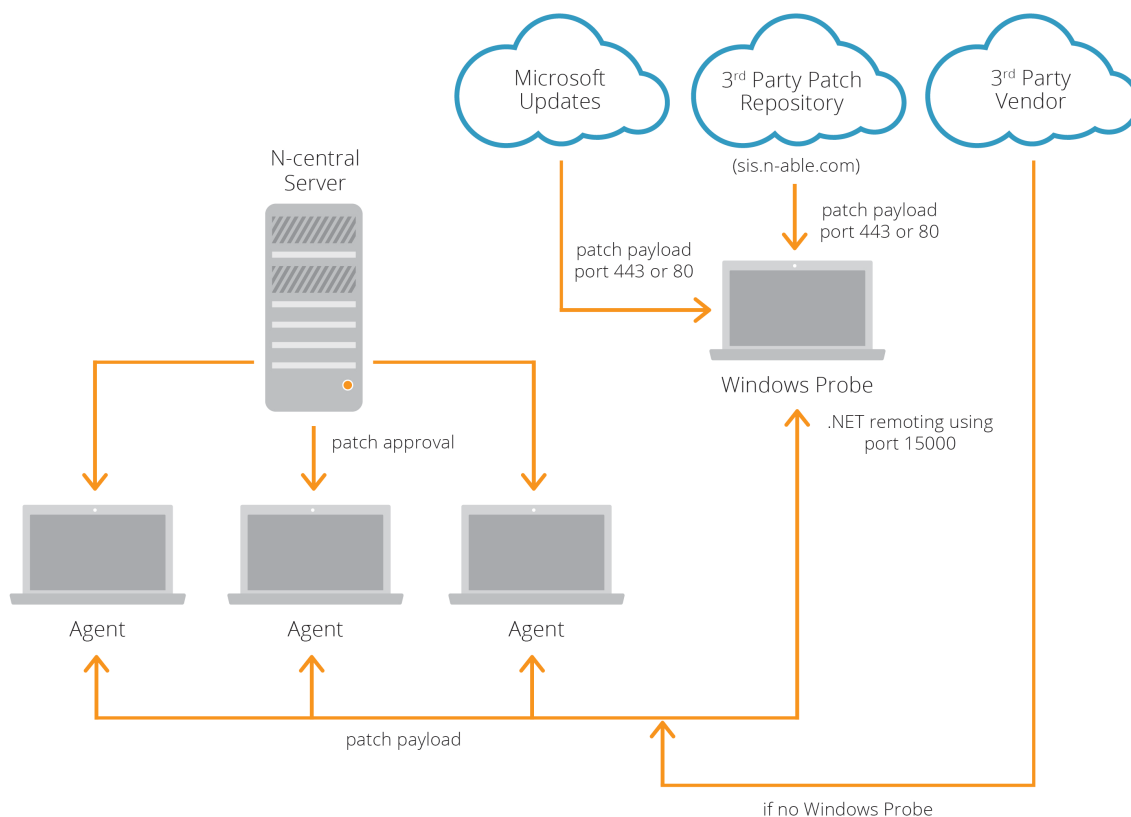


Managing Third-Party Updates

1. The Windows Agent downloads a list of third-party applications from the Probe that has already received a list of applications from `sis.n-able.com` and compares that list to the third-party applications installed on the device.
2. The Windows Agent transmits to SolarWinds N-central a list of the third-party applications that can be updated.
3. The SolarWinds N-central administrator configures approvals for the available patches.
4. The Windows Agent communicates with the Probe and requests the approved software patches.
5. Upon receiving the request, the Probe downloads the patch from the 3rd party software producer.
6. The Windows Agents download the patch from the Probe.
7. The Windows Agent applies the schedule for installing software patches.

 When Patch Cache is enabled N-central automatically tries to open port 15000.

Patch Management



Monitoring for Missing Patches

When a Windows Agent is installed on a device, the Patch Status service is automatically added to that device. The Patch Status service queries the Windows Update Agent (WUA) on the device to determine the Microsoft and third-party application patches that are missing.

The Patch Status service shows:

- total number of missing patches
- number of patches installed with errors
- missing patches by category
- missing patches older than a user-specified number of days

Scheduled Tasks

SolarWinds N-central provides the ability to create Scheduled Tasks for Windows devices. This feature allows you to create tasks that will install software remotely, execute scripts, copy files, and many others.

Scheduled Tasks are executed with the permissions used by the executing software (Agent or Probe). Agents use Agent credentials provided during discovery (or set individually on the Properties tab of the device) while the Probe typically uses domain administrator permissions.

In order for the Probe to execute remote scheduled tasks, the admin\$ share must be accessible to the domain administrator user account. As designed by Microsoft, only a Domain or Local Administrators can access the admin\$ share on a Windows operating system. This admin\$ share is accessed when deploying the SolarWinds N-central Agent, as well as during remote script or software deployment initiated by the SolarWinds N-central server.

Access to the root\cimv2 WMI namespace is required on all desktops and workstations to effectively monitor and manage a Windows operating system through WMI. A user account with the proper security accesses can be set on the cimv2 WMI namespace to allow non-domain administrator accounts to monitor and manage a Windows device through WMI as well.

Physical Security

While the SolarWinds N-central system was designed with security in mind, many software-level protections can be overcome or circumvented through physical access to the system.

To ensure the security of the system, it is important to use best practices for physical security in addition to network security. The physical security of the SolarWinds N-central server is the responsibility of the customer, however SolarWinds MSP promotes and advises customers to apply at least basic physical security precautions, which include the following:

SECURITY FEATURE	RESPONSIBILITY
BIOS authentication	Customer
Physical access control with access logging	Customer
Boot order security measures (CD boot not configured)	Customer

Security Implications

Using SolarWinds N-central includes a number of elements that may be affected by your existing security policies and systems.

Report Manager Integration

The following ports will need to be accessible to use Report Manager with SolarWinds N-central:

PORT NUMBER	PORT LOCATION				DESCRIPTION
	SOLARWINDS N-CENTRAL SERVER		REPORT MANAGER SERVER		
	INBOUND	OUTBOUND	INBOUND	OUTBOUND	
80	√	√	√	√	Communication between SolarWinds N-central and Report Manager. Port 80 must be available from the Internet to the Report Manager server to view reports.
443	√	√	√	√	Optionally used for SolarWinds N-central to Report Manager communication. Optionally used to view reports on the Report Manager server.
1433		√	√		SQL port used to send data from SolarWinds N-central to Report Manager.

LDAP Integration

SolarWinds N-central will need access to the following ports to integrate LDAP to query Active Directory:

PORT NUMBER	PORT LOCATION				DESCRIPTION
	SOLARWINDS N-CENTRAL SERVER		ACTIVE DIRECTORY SERVER		
	INBOUND	OUTBOUND	INBOUND	OUTBOUND	
389		√	√		Port 389 must be available from the Internet to the Active Directory Server to query AD. Unencrypted.
636		√	√		Optionally used for SolarWinds N-central to query AD. Encrypted (SSL).

© 2018 SolarWinds MSP Canada ULC. All rights reserved.

No part of this document may be reproduced by any means nor modified, decompiled, disassembled, published or distributed, in whole or in part, or translated to any electronic medium or other means without the written consent of SolarWinds MSP Canada ULC ("SolarWinds MSP"). All right, title, and interest in and to the software and documentation are and shall remain the exclusive property of SolarWinds MSP and its respective licensors.

SOLARWINDS MSP 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 MSP, ITS SUPPLIERS, NOR ITS LICENSORS BE LIABLE FOR ANY DAMAGES, WHETHER ARISING IN TORT, CONTRACT OR ANY OTHER LEGAL THEORY EVEN IF SOLARWINDS MSP HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

The SolarWinds MSP and N-CENTRAL marks are the exclusive property of SolarWinds MSP Canada ULC and its affiliates, are registered with the U.S. Patent and Trademark Office, and may be registered or pending registration in other countries. All other SolarWinds MSP trademarks, service marks, and logos may be common law marks, registered or pending registration in the United States or in other countries. All other trademarks mentioned herein are used for identification purposes only and may be or are trademarks or registered trademarks of their respective companies.

Feedback

SolarWinds MSP is a market driven organization that places importance on customer, partner and alliance feedback. All feedback is welcome at the following email address: n-ablefeedback@solarwinds.com.

About SolarWinds MSP

SolarWinds MSP empowers IT service providers with technologies that fuel their success. Solutions that integrate layered security, collective intelligence, and smart automation—both on-premises and in the cloud, backed by actionable data insights, help IT service providers get the job done easier and faster. SolarWinds MSP helps our customers focus on what matters most—meeting their SLAs and delivering services efficiently and effectively. For more information, visit solarwindsmsp.com.