N-ABLE™

N-central

Security White Paper

Version 2023.8

Contents

Overview

As an integral component of your IT management system, N-able N-central® complements an organization's existing security policies and infrastructures. N-able 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 N-able N-central operates.

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

Architecture

To better understand the impact that N-able 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.

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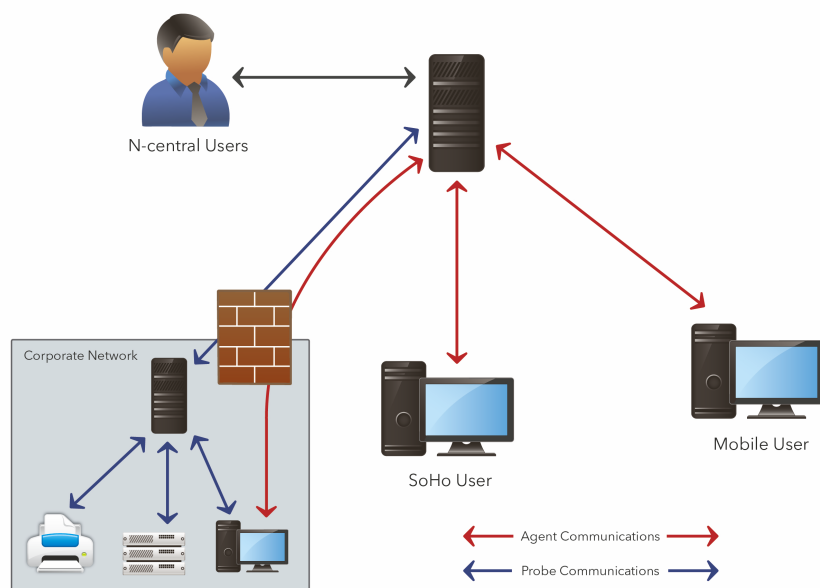
Probes and Agents

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, macOS, 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

N-able N-central Probes and Agents communicate with the N-able 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 N-able 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 5280 or 443) that is persistent to allow the N-able 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.

N-able 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 N-able N-central features.

By default, the N-able 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.

Security Profiles

Sometimes you have to work with older operating systems that use older security protocols. Security Profiles in N-able N-central enable you to select between modern security protocols, or legacy ones. The Modern security profile is enabled by default to block TLS 1.0 and 1.1. You can switch the network security profile to the Legacy Security Profile to use older TLS versions. To change Security Profiles, at the System level, click **Administration** > **Mail and Network Settings** > **Network Security**.

Because the Modern security profile is enabled by default, you need to ensure that Agents and Probes are at version 12.1 SP1 or higher. Version 12.1 SP1 and higher leverage TLS 1.2 properly and communicate with N-able N-central 12.2 and higher. This also applies to ReportManager; you need to upgrade it to version 5.0 SP5.

The differences between the profiles are:

Compatibility Security Profile

- The Compatibility security profile sits between the Legacy and Modern security profiles. It allows you to support older operating systems, such as Windows Server 2012 R2, but without allowing TLS 1.1 or 1.0.
- Does not support TLS 1.0 and 1.1.
- Disables weak SSH Ciphers, MACs and KEX Algorithms.
- Supports Modern Operating Systems (Windows 7/Server 2008 R2 and newer).
- Meets PCI requirements for TLS and ciphers.
- Support for only 2048 bit keys

> **ℹ** N-able strongly recommends that you choose between either the Compatibility or Modern security profile as we plan to deprecate the Legacy security profile in a future release of N-central.

Modern Security Profile:

- Configures N-central's UI so that it does not support TLS 1.0, 1.1, SHA1 and all weak ciphers and non-PFS ciphers.
- Supports TLS 1.3 on all UI, API, and Agent ports. The Web UI ports have further been enhanced with TLS ciphers that offer improved performance on mobile devices.
- Disables weak SSH Ciphers, MACs and KEX Algorithms.

- Will work with Modern Operating Systems (Windows 10/Server 2016 and newer).
- Meets PCI requirements for TLS and ciphers.
- Support for only 2048 bit keys

Legacy Security Profile:

- Configures N-central's UI to support TLS 1.0 and 1.1
- Not PCI/HIPPA/NIST compliant.
- Supports legacy operating systems (i.e. Windows Vista/Server 2008).

N-able N-central Server

The N-able N-central server is the "brains" of the system and contains a number of components including the Web Interface, 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 N-able N-central deals with data are executed at this level. All physical data (configuration or monitored) is stored within the relational PostgreSQL database.

The N-able 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 N-able N-central server, please refer to *"Port Access Requirements"* below, and also in the *"N-able 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
	N-able 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 N-able N-central server.
25		√			SMTP - used for sending mail.
53		√			Used for DNS.
80	√	√		√	HTTP - used for communication between the N-able N-central and agents or probes.

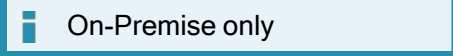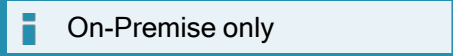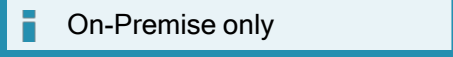| Port Number	Port Location				Description
	N-able N-central Server		Managed Device		
	Inbound	Outbound	Inbound	Outbound	
					N-able N-central recommends that you block all access from the internet to this port on the N-able N-central server, unless it is absolutely required. This port may be closed in a future release. This port must also be open for outbound traffic if the N-able N-central server is monitoring HTTP services on remote managed devices.
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. ℹ Inbound from the Windows Probe to the Windows Agent.
139			√		Used by Agents and Probes for WMI queries to monitor various services. ℹ Inbound from the Windows Probe to the Windows Agent.
443	√	√		√	HTTPS - used for communication between N-able N-central and Agents or Probes (including MSP Connect and MSP Anywhere). Your firewall must be configured to allow access from the Internet to this port on the N-able N-central server. This port must be open for outbound traffic if the N-able N-central server is monitoring HTTPS services on remote managed devices. Backup Manager on endpoint devices uses Port 443 TCP outbound. It is almost always open on workstations but may be closed on servers. Used by Agents and Probes as a failover for XMPP traffic when they cannot

Port Number	Port Location				Description
	N-able N-central Server		Managed Device		
	Inbound	Outbound	Inbound	Outbound	
					reach N-centralon port 5280. To activate EDR the N-able N-central server needs outbound HTTPS access to port 443 and the following domains: - *.sentinelone.net - sis.n-able.com - keybox.solarwindsmsp.com Pendo allows us to provide in-UI messaging and guides when there are important changes, new features onboarding, or other critical messages that we need to tell you about. You can gain access to these important messages, and help us make important design decisions from usage data, by allowing outbound HTTPS/443 access from your N-central server to the following URLs: ℹ Only windows agents will send data to the app.pendo.io URL. - app.pendo.io - cdn.pendo.io - data.pendo.io - pendo-io-static.storage.googleapis.com - pendo-static*.storage.googleapis.com
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 N-able 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 (outbound) to monitor Backup Exec jobs.

Port Number	Port Location				Description
	N-able N-central Server		Managed Device		
	Inbound	Outbound	Inbound	Outbound	
					ℹ️ Inbound from the local LAN and not the Internet.
	* 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.				
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. Outbound access to port 5280 for Managed Devices is recommended but not required.
8014			√		Backup Manager requires access to port 8014. This value cannot be modified. ℹ️ Inbound from the local LAN and not the Internet.
8443	√	√		√	The default port for the N-central UI. TCP port 8443 is used for TLS (HTTPS) connections to the N-central Web UI. Your firewall may be configured to allow access from the internet to this port on the N-able N-central server, if you require Web UI access outside of the network N-central is deployed to. You can change this port number in the N-central Administrator menu, under "Network Setup".
8800		√			The Feature Flag System in N-able N-central needs to talk to mtls.api.featureflags.prd.sharedsvcs.system-monitor.com. Used by N-able – generally during Early Access Preview and Release Candidate testing – to enable and disable features within N-able N-central.

Port Number	N-able N-central Server		Managed Device		Description
	Inbound	Outbound	Inbound	Outbound	
10000	√				HTTPS - used for access to the N-able N-central Administration Console (NAC). The firewall must be configured to allow access from the Internet to this port on the N-able N-central server.
					N-able recommends excluding all other inbound traffic to port 10000 except from N-able Ports for Support section below.
10004			√	√	N-able 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.
					ⓘ Inbound from the local LAN and not the Internet.
15000			√	√	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.
					ⓘ Inbound from the local LAN and not the Internet.

To ensure the flow of information between the N-able N-central server and outside sources, ensure the following domains and URLs are added to your firewall allow list. These domains are needed for outbound communication.

send.n-able.com	The N-able internal FTP server where a partner can upload and download files such as logs, executables and scripts.
	This is also the location where you download scripts from Scripto for additional troubleshooting tools for N-able N-central.
	Ports required: TCP 20 and 21, ports above UDP 1024 for passive transfer.
sis.n-able.com	A repository of XML files. Each XML lists download links for .exe, patches and so on.
	For example, when the agent is installed on a device and it needs to download AV Defender, the agent goes to http://sis.n-able.com/GenericFiles.xml and get the link to download the files compatible for the agent version.

	Port required: HTTP (80) and HTTPS (443)
All domains below require port TCP 443.	
update.n-able.com	The location where N-able N-central obtains the NSP file for upgrade. It also has .ISO, vdh.gz files for a N-able N-central installation. There is also an alias of this domain at releases.n-able.com.
feeds.n-able.com	The location where the N-able N-central gets RSS feeds.
sis.n-able.com	A repository of XML files. Each XML lists download links for .exe, patches and so on.
servermetrics.n-able.com **ⓘ On-Premise only**	When an N-able N-central server is installed, all information about it is sent to the N-able internal Activation Server.
licensing.n-able.com **ⓘ On-Premise only**	Once the N-able N-central server is validated, it communicates with the internal Activation Server to get the full license depending on the contract details.
push.n-able.com	Used for Apple Push Notification service (APN) and CSR certificate request for Mobile Device Management.
scep.n-able.com	Used for MDM installation, pushing profile to the target device
updatewarranty.com **ⓘ On-Premise only**	Used by N-able N-central to check the warranty expiration dates of managed devices.
microsoft.com	Used For Windows Update, which is needed for Patch Management or any other patch solution software.
https://keybox.n-able.com	Used with Netpath, EDR and future integrated components.
https://keybox.solarwindsmsp.com	Used with Netpath, EDR and future integrated components.
*.sentinelone.net	Used by EDR.
https://api.ecosystem-middleware.eu-central-1.prd.esp.system-monitor.com https://api.ecosystem-middleware.eu-west-1.prd.esp.system-monitor.com https://api.ecosystem-middleware.us-west-2.prd.esp.system-monitor.com https://api.ecosystem-middleware.ap-southeast-2.prd.esp.system-monitor.com https://ui.ecosystem-	Used by Microsoft Intune.

middleware.prd.esp.system-monitor.com/	
api.ecosystem-middleware.eu-east-1.prd.esp.system-monitor.com api.ecosystem-middleware.us-west-1.prd.esp.system-monitor.com	Middleware endpoints.
rest.ecosystem.ap-southeast-2.prd.esp.system-monitor.com rest.ecosystem.eu-east-1.prd.esp.system-monitor.com rest.ecosystem.eu-west-1.prd.esp.system-monitor.com rest.ecosystem.us-west-1.prd.esp.system-monitor.com	Rest endpoints.
grpc.ecosystem.ap-southeast-2.prd.esp.system-monitor.com grpc.ecosystem.eu-east-1.prd.esp.system-monitor.com grpc.ecosystem.eu-west-1.prd.esp.system-monitor.com grpc.ecosystem.us-west-1.prd.esp.system-monitor.com	GRPC endpoints.
cdn.pendo.io data.pendo.io pendo-io-static.storage.googleapis.com pendo-static*.storage.googleapis.com	Used by Pendo to receive data. Port required: HTTPS (443)
mtls.api.featureflags.prd.sharedsvcs.system-monitor.com	Used for Feature Preview.
assets.prd.esp.system-monitor.com	Used for Integrations like DNS Filter and EDR.

The N-able N-central server itself is based on the CentOS 7.x operating system which was fully patched at the time of the release. Additional updates are distributed as required through the standard N-able N-central Hotfix or Service Pack process. This same process applies to all internal components such as the database and application servers.

N-central server security

N-central incorporates the notion of IP blocking. If the server is hammered with too many invalid requests from the same IP address in a ten second period, N-central blocks the traffic for new requests on that IP. It does not block active requests on the same IP address. An example would be agents, which have valid session IDs or users logged

in the UI. Protections are in place to better manage the session to detect the offending IP address. To detect the correct IP address that is hammering the server, you will need to set up your firewall to allow the external IP address to be passed along. Some firewalls refer to this as *preserve the client IP*.

> **Server Security Management**
> The N-able N-central server includes an integrated firewall which blocks traffic on unused ports. It is recommended that you use your own IDS/IPS/IAV while following the minimum networking requirements to allow traffic, ports, and IP addresses documented in this Security White Paper and in Online Help.

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

Recommended exclusions for third party AV software

N-able N-central software (agents and probes) must be excluded from third party antivirus scans in order to function properly.

N-able recommends that you add the following path to the list of exclusions from security scans:

Folders

N-able N-central needs read/write access to following folders and their subfolders:

- `%Programfiles(x86)%\MspPlatform\PME`
- `%Programfiles(x86)%\MspPlatform\FileCacheServiceAgent`
- `%Programfiles(x86)%\MspPlatform\RequestHandlerAgent`
- `%ProgramData%\MspPlatform`

Applications

N-able N-central needs installation and access to following applications:

- `%Programfiles(x86)%\MspPlatform\FileCacheServiceAgent\FileCacheServiceAgent.exe`
- `%Programfiles(x86)%\MspPlatform\PME\ThirdPartyPatch\7z.exe`
- `%Programfiles(x86)%\MspPlatform\PME\Installers\CacheServiceSetup.exe`
- `%Programfiles(x86)%\MspPlatform\PME\Installers\RPCServerServiceSetup.exe`
- `%Programfiles(x86)%\MspPlatform\PME\Diagnostics\PME.Diagnostics.exe`
- `%Programfiles(x86)%\MspPlatform\RequestHandlerAgent\RequestHandlerAgent.exe`

Firewall

- Firewall must be not blocking following communication channels:
- HTTP and HTTPS communication (port 80 and port 443) between FileCacheServiceAgent windows service (`%Programfiles(x86)%\MspPlatform\FileCacheServiceAgent\FileCacheServiceAgent.exe`) and sis.n-able.com server

- If you use a probe, the firewall must not block communication between `FileCacheServiceAgent` windows service and the probe device on port 15000.

For a complete list of paths you can include to exclude from security scans, see Global Exclusions in the N-able N-central Online Help. This list includes folders excluded by AV Defender by default.

The Upgrade Process

Upgrading N-able N-central involves not only upgrading the N-able 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 N-able N-central 2021.3 consists of a number of elements including:

Agent and Probe Upgrade

The N-able N-central server is upgraded.

1. The first time that the Probe connects to the N-able 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.
2. 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.
3. 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.
4. If the Agents cannot connect to a Probe, they will download the Agent upgrade software directly from the N-able 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.

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

> 💡 Remote Control is available on N-able N-central servers with a Professional license.

N-able N-central uses the following methods to establish encrypted connections from the N-able 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 N-able N-central 2022.1 Agents.
- Other remote control types use connections established through one of SSH (Secure Shell) or HTTPS (Hypertext Transfer Protocol, Secure).

> ℹ️ In some circumstances, security scans performed on N-able 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.
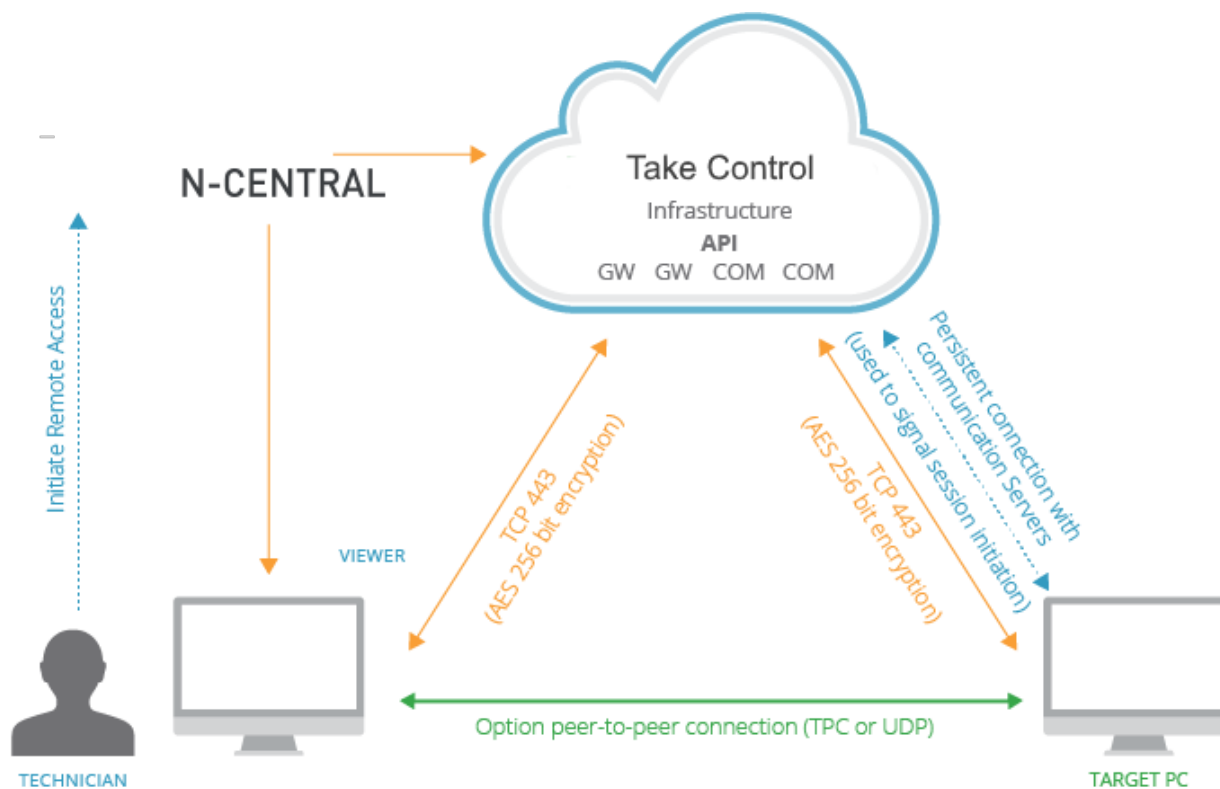
Take Control

Take Control sessions are sheltered by a proprietary communication protocol with guaranteed global security by AES using a 256-bit cipher when establishing, or for the duration, of the session. The key exchange is protected by an SSL based in AES-CBC with TLS 1.2. 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 (MSP Anywhere) remote control connections.

> 💡 macOS 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	Outbound	Inbound	Outbound
Port 80		√		√
Port 443		√		√
Port 3377 ℹ️ Take Control fails over to this port as an alternative connection method.		√		√

TCP Port usage in N-central is optional and used to directly connect a Technician's device to remote devices on the same local network instead of using the application's gateways (outside the local network) to broker the connection.

> **ℹ** Note: When any associated Firewall rules are disabled or removed, direct connection becomes unavailable and all connections are routed externally, even when both devices are in the same local network.

The *Attempt peer-to-peer connection first* option is meant only for peer-to-peer connections with devices outside the local network. The option attempts to make a P2P UDP connection to the device. It has no impact on peer-to-peer connections with local network devices, when traffic is allowed over TCP Port 5948. The option is not needed for remote control but the port will always be used unless it is disabled in the agent configuration file. In the rarest cases where the device is accessible on the internet it can also be used for P2P even not within the same LAN.

When using Take Control, the N-able N-central server, remote endpoints, and devices running the Viewer (those devices that are used to establish the remote session) must be able to resolve and reach hosts with the following domain names:

- `*.n-able.com`
- `sis.n-able.com`

The following domain also needs to be resolved for update downloads:

- `swi-rc.cdn-sw.net`

> **ℹ** IP addresses in the range 38.71.16.x are used to download product updates.

When using MSP Anywhere, the N-able 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 Location			
	Take Control Viewer		Target Device	
Port Number	Inbound	Outbound	Inbound	Outbound
Port 1234		√		√
Port 1235		√		√

- BASupApp.exe
- BASupTSHelper.exe
- agent.exe

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

Remote Desktop

With N-able N-central 2020.1, Remote Desktop uses a Custom Protocol Handler (CPH) to facilitate the connection to an RDP session. When launching a RDP session, N-able N-central will verify if the CPH application is installed on the host device. If CPH is not present on the system then you are prompted to download and install the application.

The handler will attempt to use a tunnel over SSH for the connection before failing over to HTTPS (443) to establish the connection. The CPH launcher opens a listening port randomly selected by N-central to start the RDP client.

> ⚡ **No CPH for Mac and Linux**
> Mac and Linux devices still use the Java implementation for Remote Desktop. SSH and Webpage require Java to run.

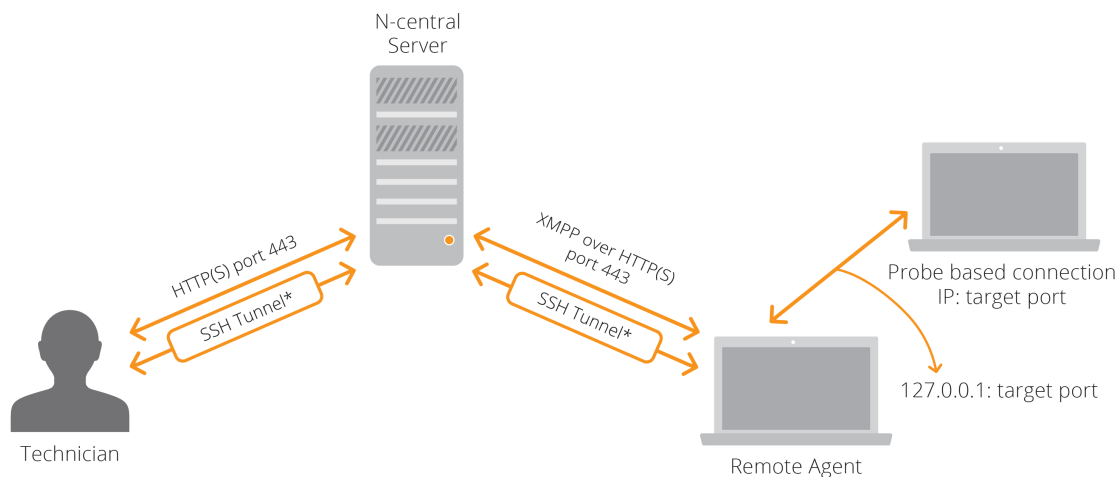# Other Remote Control Connections

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

	Port Location			
	N-able N-central Server		Target Device	
Port Number	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.

> ℹ️ In the diagrams below, the "SSH Tunnel*" notation indicates the first protocol attempted will be an SSH tunnel (TCP on port 22).

N-central
Server

HTTP(S) port 443

SSH Tunnel*

Technician

XMPP over HTTP(S)
port 443

SSH Tunnel*

Probe based connection
IP: target port

127.0.0.1: target port

Remote Agent

Remote control in N-able 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 N-able N-central Online Help.

The security features of N-able 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 N-able N-central server, Agents, Probes, and an N-able hosted update server.

Upgrades and Updates

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

Product Upgrades (Major Releases)

- 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.

- If an upgrade is available, the AV Defender Status service will transition to a Warning state to indicate that an upgrade is available.

- 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.
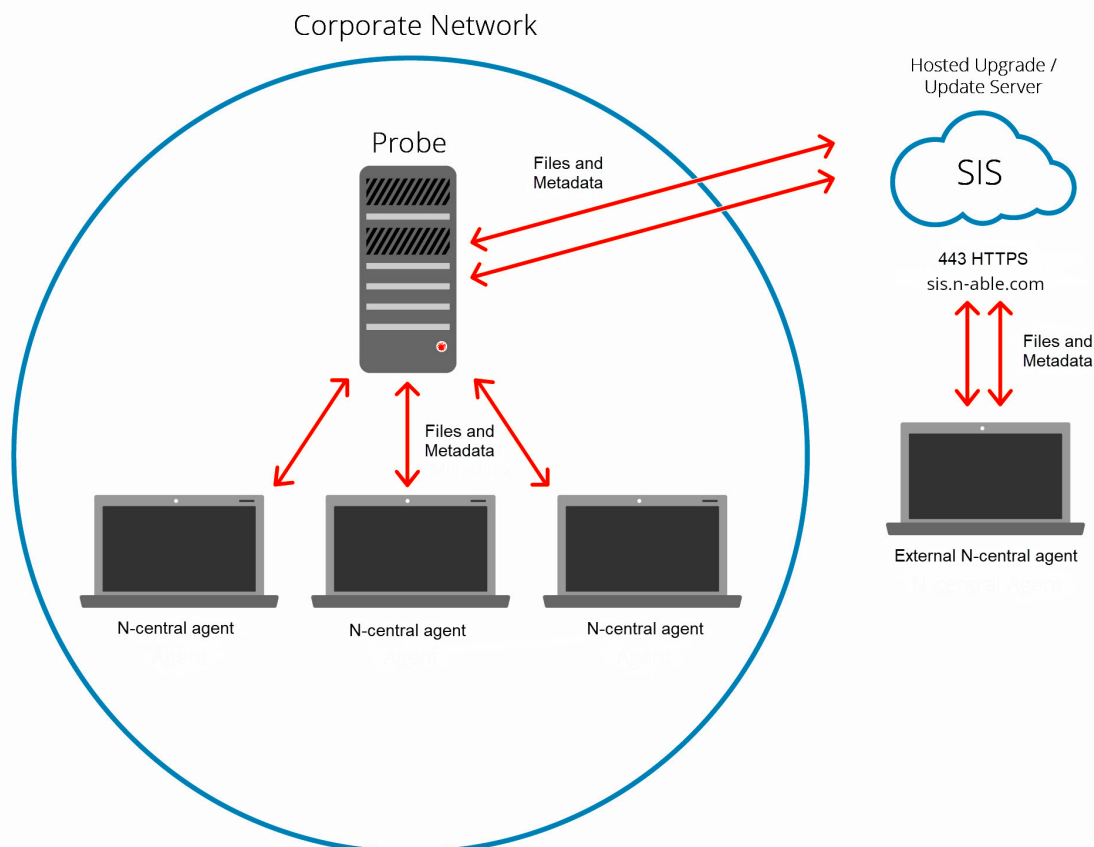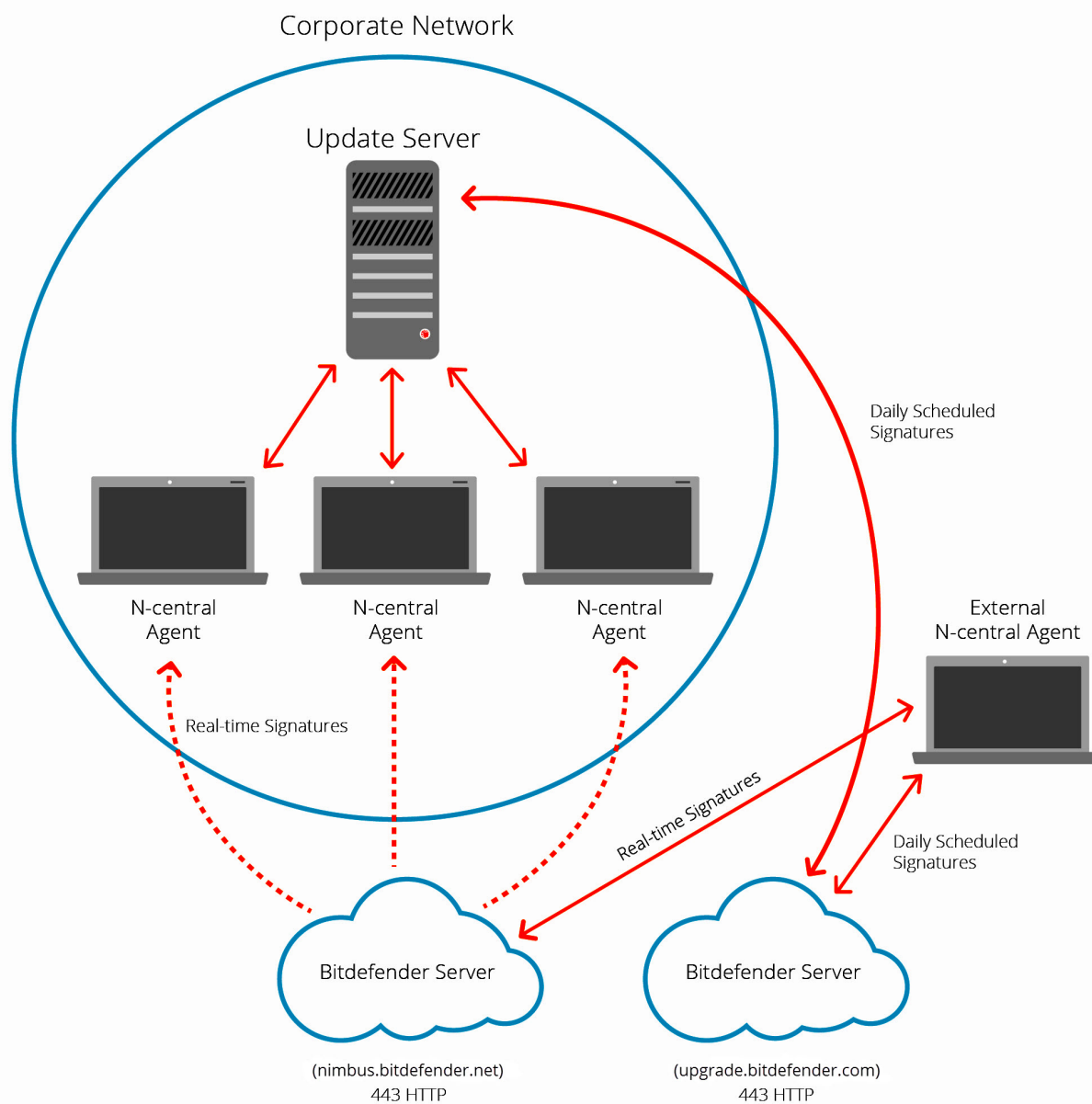
Product Updates (Hot Fixes)

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.
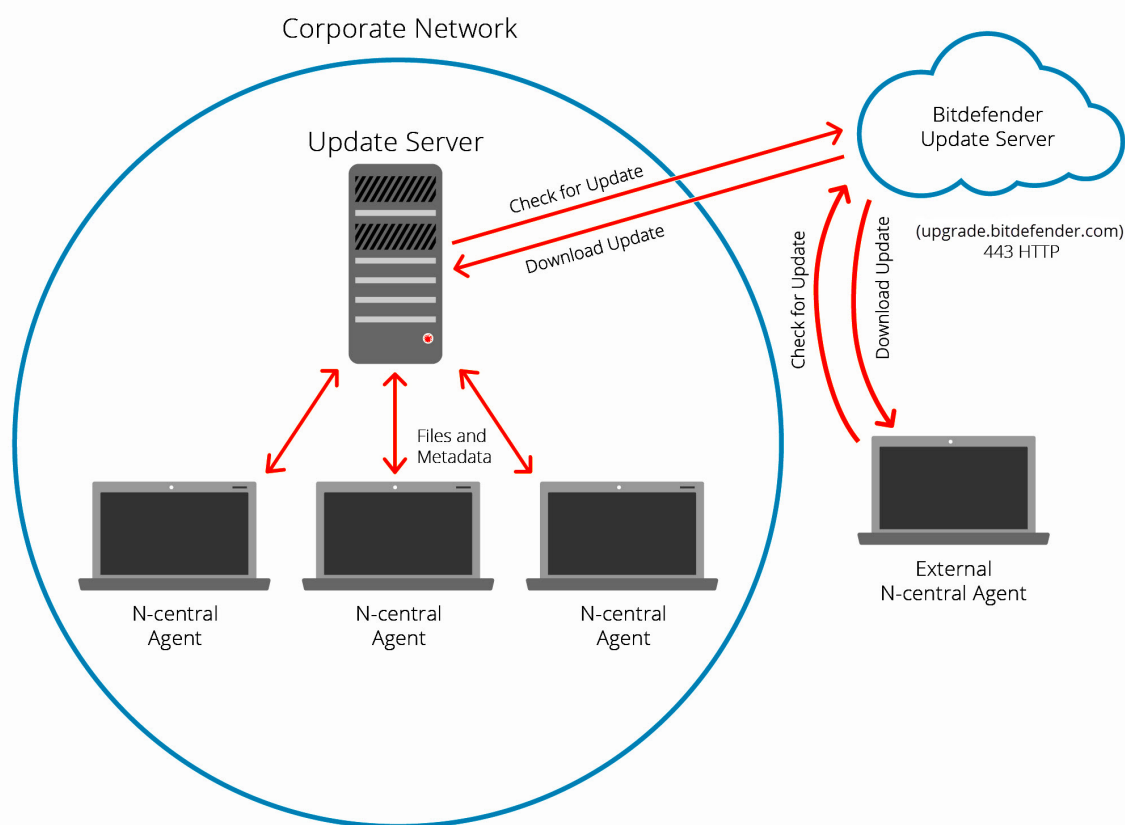
Definition File Updates (Security Signatures)

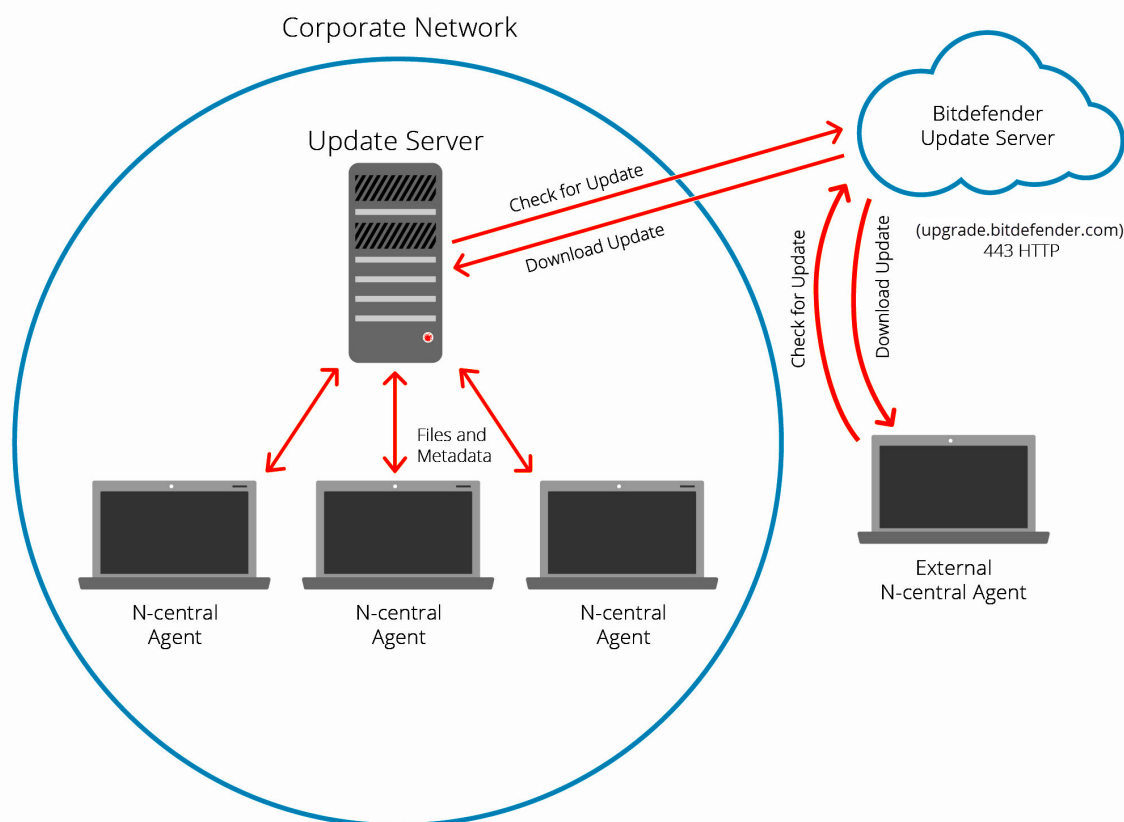## More Information on Definition File Updates

Ensuring that your definition files are up to date is a critical aspect of managing AV Defender. Again, N-able 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.
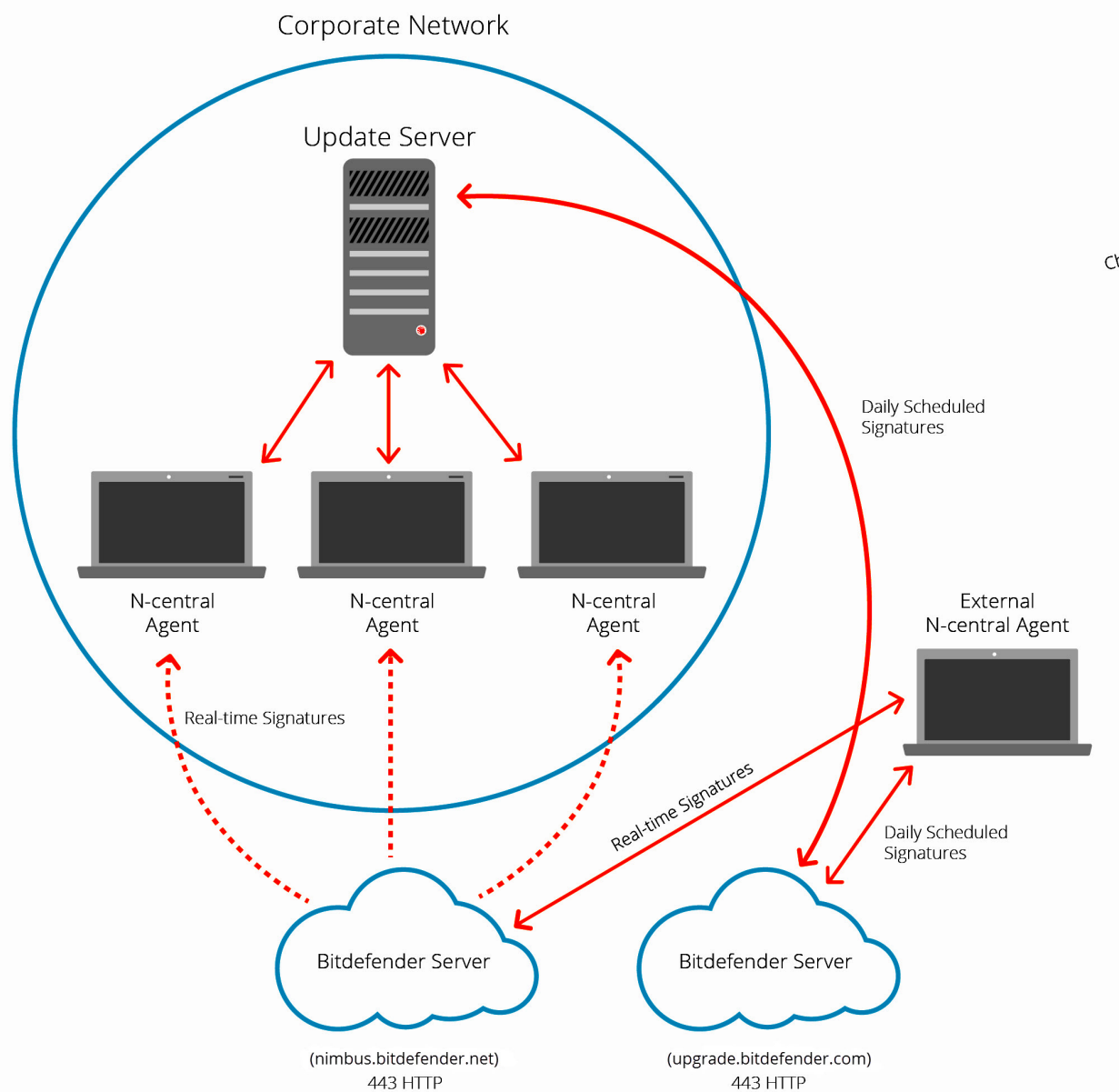
- Definition File Updates are downloaded from the Update Server if available or directly from Bitdefender all using port 443.

- 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.

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)

Corporate Network

Update Server

N-central Agent

N-central Agent

N-central Agent

External N-central Agent

Daily Scheduled Signatures

Real-time Signatures

Real-time Signatures

Daily Scheduled Signatures

Bitdefender Server

Bitdefender Server

(nimbus.bitdefender.net)
443 HTTP

(upgrade.bitdefender.com)
443 HTTP

More Information on Definition File Updates

Ensuring that your definition files are up to date is a critical aspect of managing AV Defender. Again, N-able 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

N-able 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 N-able N-central backup management, N-able 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 eff ort 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.

When using N-able Backup, the N-able N-central server must be able to resolve the following domain name:

- `*.cloudbackup.management`

N-able Backup

N-able Backup is a hybrid cloud-based backup and recovery platform. N-able 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. N-able N-central integrates with N-able Backup to act as a conduit between N-able Backup and the cloud storage to configure profiles and schedules.

N-able Backup performs an initial full backup and then performs continual incremental backups. N-able 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.

N-able 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.

Mobile Device Management (MDM)

Managing mobile devices is performed using a connection to N-able N-central's Mobile Device Management service. When N-able N-central attempts to communicate with a mobile device, N-able 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

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

| Port Number | Port Location | | | | Description |
| | N-able N-central Server | | Target Network Server | | |
	Inbound	Outbound	Inbound	Outbound	
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

N-able 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.

The Patch Management Engine (PME) on your devices requires that they have access to sis.n-able.com in order to update.

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

- Managing Windows updates
- Managing Offline Patches
- Managing Third Party software patches

> 💡 N-able 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 N-able N-central server.
3. The N-able 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 downloads the updates from the Probe.
7. The Windows Agent applies the schedule for installing updates.

Patch Management
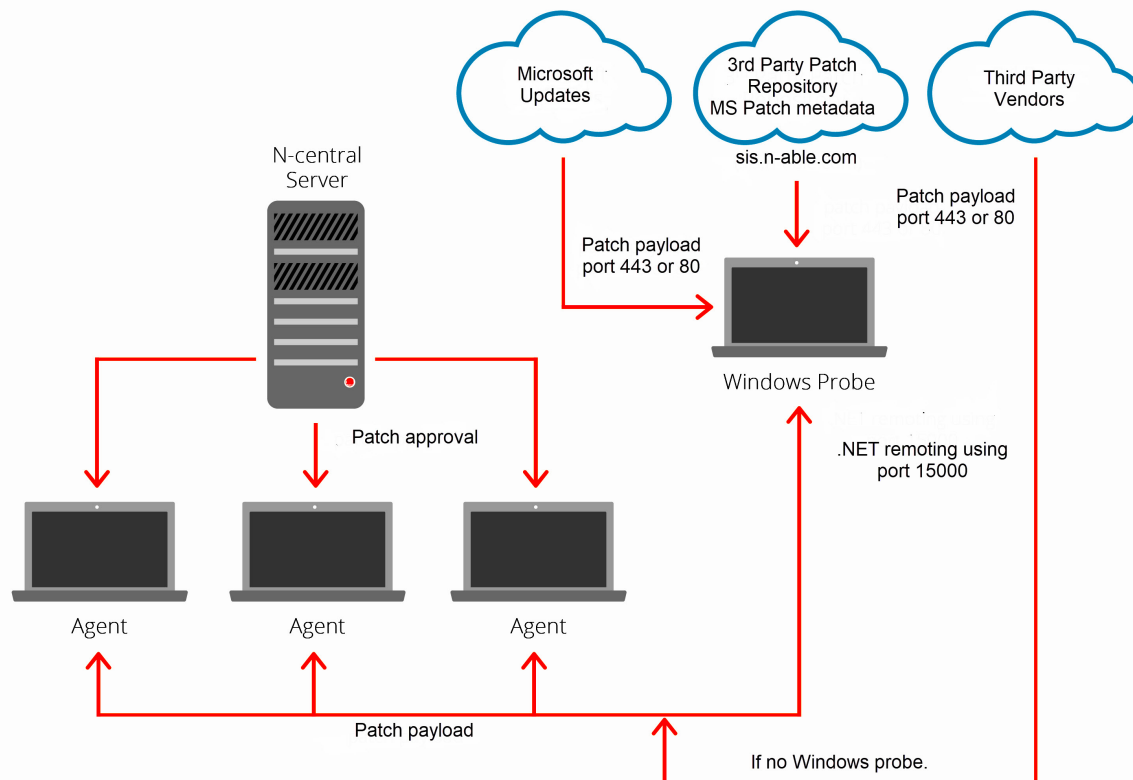
Managing Offline Patches

Archives of the metadata for offline patches is on `sis.n-able.com`, and installing offline patches behaves similarly to online patching through the Microsoft Update server.

Communication with `sis.n-able.com` uses port 443, but the data is also available through port 80. The Microsoft Update servers communicate using port 80.

Offline patching uses MSU installer files instead of the CAB installer files that are used with online patching, using the Microsoft Update server. The base URL of these files might also differ from those with online patching.

Patching data for offline devices is done through the probe using port 15000.

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

N-able 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 N-able N-central Agent, as well as during remote script or software deployment initiated by the N-able 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 N-able 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 N-able N-central server is the responsibility of the customer, however N-able 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 N-able 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 N-able N-central:

Port Number	Port Location				Description
	N-able N-central Server		Report Manager Server		
	Inbound	Outbound	Inbound	Outbound	
80	√	√	√	√	Communication between N-able 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 N-able N-central to Report Manager communication. Optionally used to view reports on the Report Manager server.
1433		√	√		SQL port used to send data from N-able N-central to Report Manager.

LDAP Integration

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

Port Number	Port Location				Description
	N-able 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 N-able N-central to query AD. Encrypted (SSL).

About N-able

N-able empowers managed services providers (MSPs) to help small and medium enterprises navigate the digital evolution. With a flexible technology platform and powerful integrations, we make it easy for MSPs to monitor, manage, and protect their end customer systems, data, and networks. Our growing portfolio of security, automation, and backup and recovery solutions is built for IT services management professionals. N-able simplifies complex ecosystems and enables customers to solve their most pressing challenges. We provide extensive, proactive support–through enriching partner programs, hands-on training, and growth resources–to help MSPs deliver exceptional value and achieve success at scale. For more information, visit www.n-able.com.