

Nex Agent Deployment Guide

Operational Overview

InvoScape | Nex Endpoint Management and orchestration platform

1. Overview

The Nex Agent is the Windows service installed on each workstation or server managed by Nex. It provides the communication layer between the endpoint and the Nex Server, allowing the server to coordinate management activity and receive endpoint status and results.

Agent deployment is intended to be lightweight and straightforward. Once installed and configured, the Agent operates in the background without requiring an interactive user session.

2. Before Deployment

Before installing the Nex Agent, confirm that:

- The Nex Server has been installed and configured.
- The endpoint is running a supported Windows operating system.
- The endpoint can reach the Nex Server across the organization's network.
- DNS can resolve the Nex Server name where a hostname is used.
- The required Nex management port is permitted through relevant firewalls.
- The endpoint trusts the Nex Server certificate where HTTPS is used.
- Administrative rights are available for Agent installation.

3. Supported Windows Environments

Nex is designed to manage Windows workstations and Windows Server systems. Current compatibility targets include:

- Windows 10
- Windows 11
- Windows Server 2012 R2
- Windows Server 2016
- Windows Server 2019
- Windows Server 2022
- Windows Server 2025

Additional Windows releases should be treated as supported only after compatibility testing for that release has been completed.

4. Agent Installation

The Nex Agent is installed on the endpoint using the Nex Agent installer. During deployment, the Agent is configured with the Nex Server information required to establish management communication.

At a high level, deployment consists of:

1. Run the Nex Agent installer with administrative rights.
2. Provide or apply the required Nex Server address.
3. Complete installation of the Nex Agent Windows service.
4. Allow the Agent to start and establish communication with the Nex Server.
5. Confirm that the endpoint registers and appears in the Nex administration console.

5. Agent Communication

The Nex Agent periodically contacts the Nex Server to receive management activity and return device information and command results. Nex management communication is designed to remain within the organization's network.

Function	Protocol	Default Port
Nex management - HTTP	TCP	TBA
Nex management - HTTPS	TCP/TLS	TBA

Nex supports a primary server connection with fallback communication capability. HTTPS should be used where the required DNS and certificate trust are available.

6. Registration and Initial Check

After installation, allow the Agent sufficient time to contact the Nex Server and register. The endpoint should then become visible in the Nex console.

Administrators should confirm:

- The device appears in Nex.
- The hostname and operating-system information are correct.
- The Agent continues to report to the Nex Server.
- Available device inventory is being received.
- Update Health and Windows Update information can be collected as expected.

7. Agent Service

The Nex Agent runs as a Windows service and is intended to start automatically with Windows. This allows management activity to continue regardless of whether a user is signed in.

Nex also uses a watchdog mechanism to help ensure the Agent service remains available. If a device stops reporting, checking the Nex Agent service should be one of the first troubleshooting steps.

8. HTTPS and Certificate Trust

Where HTTPS is used, the managed endpoint must trust the certificate presented by the Nex Server. The server name used by the Agent must also match the deployment's DNS and certificate configuration.

Certificate or DNS problems can prevent HTTPS communication even when the Nex Server itself is reachable. Administrators should validate name resolution and certificate trust before changing the Agent configuration.

9. Basic Troubleshooting

Symptom	Initial Check
Device does not appear in Nex	Confirm the Agent service is running and the configured Nex Server address is correct.
Server cannot be reached	Check DNS, routing, firewall rules and TCP connectivity to the Nex Server.
HTTPS fails	Confirm the endpoint trusts the Nex Server certificate and that the server name resolves correctly.
Agent stops reporting	Check the Nex Agent service, watchdog operation, network connectivity and Agent logs.
Inventory is missing	Confirm the Agent is reporting normally and review Agent logs and Windows inventory/WMI availability.
Update information is missing	Confirm Agent communication and the health of Windows Update components on the endpoint.

10. Deployment Principles

- Validate the Nex Server before deploying Agents widely.
- Test Agent deployment on a small group of representative Windows systems first.
- Confirm DNS, firewall and certificate trust before troubleshooting the application layer.
- Verify newly deployed devices are reporting before beginning maintenance activity.
- Expand deployment in controlled stages across the environment.
- Review Agent and Server logs when communication differs from the expected workflow.

11. Related Documentation

- Nex Product Overview
- Nex System Requirements
- Nex Deployment, Security & Technical Guide
- Nex Administrator Guide
- Nex Windows Patching Guide
- Nex Software Deployment Guide