

Nex System Requirements

High-Level Deployment Requirements

InvoScape | Nex Endpoint Management and orchestration platform

Overview

Nex is a self-hosted Windows endpoint management platform. A Nex deployment consists of a central Nex Server and the Nex Agent installed on each managed Windows endpoint. This document provides a high-level view of the infrastructure and connectivity required to deploy Nex.

Nex Server

The Nex Server is installed within the organization's own environment and provides the central management console, endpoint coordination and supporting services.

- A supported 64-bit Windows Server environment.
- A Microsoft SQL Server database instance available to Nex.
- Network connectivity between the Nex Server and managed endpoints.
- DNS name resolution appropriate to the deployment.
- A certificate is required when HTTPS management communication is enabled.
- Sufficient compute, memory and storage for the number of managed endpoints and retained operational data.

Database

Nex uses Microsoft SQL Server for its operational data. SQL Server Express can be used for smaller deployments, subject to Microsoft's edition limits. Larger environments may require a higher SQL Server edition depending on database size, workload and retention requirements.

Final deployment sizing should be based on the number of managed endpoints and the organization's operational and data-retention requirements.

Managed Endpoints

Each managed Windows device runs the Nex Agent as a Windows service. Nex is intended to manage supported Windows workstation and Windows Server operating systems.

Current Nex 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 Server versions should be listed as supported only after Nex compatibility testing for that release has been completed.

Network Requirements

Managed endpoints must be able to communicate with the Nex Server across the organization's network. Nex currently provides HTTP and HTTPS server endpoints, with deployments expected to use HTTPS where the required certificate trust is available.

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

Internet Access

Nex management traffic is designed to remain within the organization's network. Internet connectivity is required only where the managed Windows environment needs to access Microsoft services used to obtain Windows updates.

Nex is designed to operate entirely within your network. Internet access is only required for Microsoft services needed to obtain Windows updates; Nex management traffic remains internal.

DNS and Certificates

For HTTPS deployments, endpoints must be able to resolve the Nex Server name and trust the certificate presented by the server. Organizations may use an appropriate internally issued or otherwise trusted certificate consistent with their security architecture.

Administrative Requirements

- Administrative rights are required to install and configure the Nex Server.
- Administrative rights are required when deploying the Nex Agent to managed endpoints.
- The Nex Agent runs as a Windows service so that endpoint management can continue without an interactive user session.
- Firewall and security controls must permit the required Nex Server-to-endpoint communications.

Deployment Sizing

Nex Server hardware sizing depends on endpoint count, management activity, database growth and retention. Specific minimum and recommended CPU, memory and storage figures should be selected according to the intended deployment size.

Formal capacity guidance for larger deployments will be published from validated Nex load and scale testing. Until that testing is complete, unverified maximum endpoint or performance claims should not be treated as production sizing guarantees.

High-Level Checklist

- Supported Windows Server available for Nex Server.
- Microsoft SQL Server available.
- DNS configured for the Nex Server.
- HTTPS certificate available where HTTPS is used.
- Required Nex management ports permitted through internal firewalls.
- Managed Windows endpoints can reach the Nex Server.
- Managed devices have access to the Microsoft services required for Windows Update.
- Administrator access available for server and agent installation.

Related Nex Documentation

- Nex Product Overview
- Nex Deployment Guide
- Nex Security & Architecture Overview
- Nex Network & Firewall Requirements
- Nex Administrator Guide