

Nex Deployment, Security & Technical Guide

High-Level Product Reference

InvoScape | Nex Endpoint Management and orchestration platform

1. About This Guide

This guide provides a high-level technical overview of deploying and operating Nex. It is intended for organizations evaluating Nex and for administrators planning an initial deployment. Detailed day-to-day administration, Windows patching, Nex Agent deployment and software deployment are covered separately.

2. Deployment Overview

Nex uses a self-hosted server-and-agent architecture. The Nex Server is installed within the organization's environment and provides the management console, coordination services and database-backed operational data. The Nex Agent runs as a Windows service on each managed endpoint.

A typical high-level deployment sequence is:

1. Prepare a supported Windows environment for the Nex Server.
2. Provide the required Microsoft SQL Server instance.
3. Install and configure the Nex Server.
4. Configure DNS and HTTPS/certificate settings as required.
5. Activate or import the applicable Nex license.
6. Deploy the Nex Agent to managed Windows devices.
7. Verify endpoint registration and communication.
8. Begin managing devices through the Nex console.

3. Security & Architecture

Nex is designed as a self-hosted management platform. The organization operates the Nex Server and retains control of its management infrastructure and Nex operational data.

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.

- Nex Server provides the central management and coordination layer.
- Nex Agents communicate with the Nex Server from managed Windows endpoints.
- HTTPS/TLS can be used for protected server-agent communication.
- Certificate trust and DNS resolution must be appropriate for the chosen HTTPS deployment.
- Administrative access to Nex is authenticated.
- Nex operational data is stored in the organization's Microsoft SQL Server environment.

4. Network & Firewall Requirements

Managed endpoints must be able to reach the Nex Server across the internal network. Firewalls and network security controls must permit the Nex management ports used by the deployment.

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

DNS should allow managed endpoints to resolve the Nex Server name. Where HTTPS is used, endpoints must trust the certificate presented by the Nex Server.

Internet access is not required for Nex management traffic itself. Windows devices require access to the Microsoft services appropriate to their Windows Update configuration when obtaining updates from Microsoft.

5. Backup & Recovery

A Nex recovery plan should protect the components required to rebuild the management environment. Backup frequency and retention should follow the organization's own recovery objectives.

- Nex Microsoft SQL Server database.
- Nex Server configuration.
- Software package repository and associated deployment content.
- Certificates and certificate material required by the Nex Server.
- Any organization-specific deployment information required to reconnect managed endpoints.

At a high level, recovery consists of restoring the required server environment, database, configuration, package content and certificates, then validating Nex Server services and agent connectivity.

6. High-Level Troubleshooting

When Nex is not operating as expected, troubleshooting should begin with the communication path and the underlying Windows services rather than immediately changing the deployment.

- **Agent connectivity** - Confirm the Nex Agent service is running and that the endpoint can reach the configured Nex Server.
- **DNS** - Confirm the Nex Server hostname resolves to the expected address.
- **HTTPS/certificates** - Confirm the endpoint trusts the certificate presented by the Nex Server.
- **Firewall** - Confirm the required Nex management port is permitted between the endpoint and server.
- **SQL connectivity** - Confirm the Nex Server can connect to its configured Microsoft SQL Server instance.
- **Windows Update** - Confirm Windows Update and its required Windows components are healthy when investigating patching failures.
- **Logs** - Review Nex Server and Agent logs before making configuration changes.

7. Release, Compatibility & Known Issues

Nex release information should identify the product version, significant new functionality, fixes, compatibility changes and known limitations. Customers should review release information before upgrading production environments.

Known issues should be documented where they materially affect deployment or operation, together with a workaround where one has been validated.

8. Technical Reference

Item	High-Level Detail
Architecture	Self-hosted Nex Server with Nex Agent installed on managed Windows endpoints.
Database	Microsoft SQL Server.
Management HTTP	TBA
Management HTTPS	TBA
Agent	Windows service running on each managed endpoint.
Agent polling	Nex Agents periodically contact the Nex Server for management activity.
Endpoint platforms	Windows 10, Windows 11 and supported Windows Server releases.
Server compatibility target	Windows Server 2012 R2, 2016, 2019, 2022 and 2025 are current Nex compatibility targets; additional versions should be published only after validation.
Internet dependency	Nex management remains internal; Microsoft connectivity is required where Windows devices obtain updates from Microsoft services.

9. Capacity & Scaling

Nex Server capacity depends on endpoint count, polling activity, update operations, database growth, data retention and the resources assigned to the Nex Server and SQL Server.

Specific maximum endpoint counts and production sizing guarantees should be based on validated Nex load testing. Until formal scale testing is completed, published capacity information should be treated as deployment guidance rather than a guaranteed maximum.

10. Separate Operational Guides

The following subjects are intentionally maintained as separate documents because they require more detailed operational procedures than this high-level technical guide:

- Nex Administrator Guide
- Nex Windows Patching Guide
- Nex Agent Deployment Guide
- Nex Software Deployment Guide

11. Related Documentation

- Nex Product Overview
- Nex System Requirements