

Nex Administrator Guide

Operational Reference

InvoScape | Nex Endpoint Management and orchestration platform

1. About This Guide

This condensed guide provides administrators with a high-level reference for the routine operation of Nex. It focuses on the main areas used to view, organize and maintain managed Windows devices. Detailed deployment, patching, agent installation and software deployment procedures are covered in separate Nex documentation.

2. Nex Administration Console

The Nex Server provides the central administration interface for the managed Windows environment. Administrators use the console to review devices, organize endpoints, monitor update health, manage maintenance activity and review operational status.

Administrative access is authenticated. Administrators should use individual credentials and change initial or reset passwords as required by the organization's security practices.

3. Devices

Managed Windows workstations and servers appear in Nex after the Nex Agent has registered with the server. The Devices area provides the administrator with a central view of endpoints known to Nex.

- Confirm that expected devices are registered and reporting.
- Review device status and recent communication.
- Review available inventory and operating-system information.
- Identify devices that have stopped reporting or require attention.
- Use device information when investigating patching or maintenance problems.

4. Collections

Collections allow administrators to group devices for easier management. They can be used to organize endpoints by business function, location, operating-system role or another structure appropriate to the environment.

Administrators should keep collection membership deliberate and understandable, particularly where collections are used to target maintenance or deployment activity.

5. Update Health

Update Health provides visibility into whether a managed device is ready for Windows patching and whether conditions exist that may require administrator attention.

- Pending reboot state.
- Windows Update availability and health.
- Relevant Windows service state.
- Device readiness for patching.
- Compliance or conditions preventing normal update activity.

A device showing an unhealthy or blocked state should be investigated before repeatedly attempting update installation.

6. Maintenance Windows

Maintenance windows provide control over when managed maintenance activity is allowed to run. This allows administrators to align patching and related operations with approved business maintenance periods.

- Create maintenance windows appropriate to the devices or collections being managed.
- Confirm the intended schedule before enabling maintenance activity.
- Review device and job status after the maintenance period.
- Investigate endpoints that did not complete the expected maintenance workflow.

7. Jobs and Commands

Nex uses jobs and commands to coordinate management activity with endpoints. Administrators can use operational status and results to understand whether work is queued, in progress, completed or requires investigation.

Where a command fails, review the result and endpoint state before resubmitting work. Repeated execution without understanding the underlying failure can make troubleshooting more difficult.

8. Licensing

Nex Server licensing controls the authorized use of the Nex deployment, including license status, expiry and device entitlement. Licensing can be managed through the Nex Server registration and licensing functions.

Administrators should periodically confirm that the server license remains valid and that the licensed device capacity is appropriate for the environment. Nex also supports an offline licensing workflow for environments where direct licensing connectivity is not appropriate.

9. Routine Administrator Checks

A simple routine operational review should include:

- Confirm the Nex Server is operating normally.
- Check for devices that are no longer reporting.
- Review Update Health for blocked, unhealthy or pending-reboot endpoints.
- Review recent maintenance activity and failed jobs.
- Confirm expected devices remain in the correct collections.
- Review license status and device capacity.
- Review Nex logs when unexpected behavior is observed.

10. Basic Troubleshooting

Symptom	Initial Check
Device not reporting	Confirm the Nex Agent service is running and the endpoint can reach the Nex Server.
Device cannot reach Nex Server	Check DNS, network routing, firewall rules and the configured server address.
HTTPS communication problem	Check Nex Server name resolution and certificate trust on the endpoint.
Update activity not progressing	Review Update Health, pending reboot state, maintenance-window status and Windows Update health.
Job or command failed	Review the recorded result and relevant Nex Agent/Server logs before retrying.
Server database issue	Confirm the Nex Server can connect to its configured Microsoft SQL Server instance.

11. Administration Principles

- Investigate the cause of failures before repeatedly retrying operations.
- Use collections and maintenance windows consistently.
- Keep endpoint connectivity and update health visible.
- Review logs when behavior differs from the expected workflow.
- Maintain backups of the Nex database, configuration, package content and certificates.
- Apply Nex updates in accordance with published release information.

12. Related Documentation

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