

Nex Windows Patching Guide

Operational Overview

InvoScape | Nex Endpoint Management and orchestration platform

1. Overview

Nex centralizes Windows patch management so administrators can identify available updates, assess endpoint readiness, control when maintenance occurs and review the outcome from a single management platform.

The patching workflow is designed to reduce repetitive manual administration while keeping control of Windows maintenance within the organization's own environment.

2. Windows Update Scanning

Nex Agents check managed Windows devices for applicable updates and report the results to the Nex Server. This gives administrators visibility of updates detected across the managed environment.

- Identify endpoints requiring Windows updates.
- Record update scan results centrally.
- Provide administrators with visibility before installation activity begins.
- Support ongoing assessment of endpoint patching status.

3. Update Health

Before patching, Nex can assess conditions that influence whether an endpoint is ready for maintenance. Update Health helps administrators identify devices that may need attention rather than repeatedly attempting updates on an unhealthy endpoint.

- Pending reboot conditions.
- Windows Update readiness.
- Relevant Windows service health.
- Blocked or unhealthy update states.
- General readiness for patch installation.

4. Maintenance Windows

Maintenance windows allow patching activity to be aligned with approved business maintenance periods. Administrators can control when update installation and related maintenance operations are permitted to run.

This helps reduce disruption to users and business services while giving IT teams a predictable period in which to perform endpoint maintenance.

5. Patch Installation

When an endpoint is ready and the applicable maintenance conditions are met, Nex coordinates the installation of approved Windows updates through the Nex Agent.

At a high level, the workflow is:

1. Assess update health.
2. Check the endpoint for applicable Windows updates.
3. Determine the updates to be installed.
4. Wait for the applicable maintenance window where required.
5. Install updates.
6. Record the installation result.
7. Handle reboot requirements.
8. Re-check the endpoint following maintenance.

6. Reboot Management

Some Windows updates require a restart before maintenance is complete. Nex tracks reboot-required conditions and incorporates reboot handling into the patching workflow so that an endpoint is not incorrectly treated as fully complete while a restart remains outstanding.

After reboot activity, the endpoint can be checked again to confirm its resulting update and health state.

7. Monitoring and Compliance

Nex provides central visibility into update activity and endpoint state. Administrators can use this information to identify devices that completed maintenance, devices awaiting further action and endpoints requiring investigation.

- Review update scan and installation results.
- Identify pending-reboot devices.
- Review unhealthy or blocked endpoints.
- Confirm devices have returned to a healthy state after maintenance.
- Use collections to organize and review groups of managed endpoints.

8. When Patching Does Not Complete

Condition	Initial Check
Update scan not completing	Confirm the Nex Agent is communicating and Windows Update components are operational.
Endpoint blocked	Review Update Health and resolve the reported condition before retrying.
Pending reboot	Complete or schedule the required restart and allow Nex to reassess the endpoint.
Installation failure	Review the update result, Windows Update state and relevant Nex logs.
Maintenance did not run	Confirm the device or collection is associated with the intended maintenance window and review job status.

9. Business Benefits

Centralizing the Windows patching can reduce the administrative effort required to maintain individual systems, improve consistency across the environment and give the organization clearer visibility of devices that are not receiving expected maintenance.

Because Nex is self-hosted, patch-management control and Nex management traffic remain within the organization's environment. Nex does not require Azure or a cloud-hosted endpoint-management platform simply to centrally coordinate Windows patching.

10. Recommended Administrative Practice

- Review Update Health before investigating patch-installation failures.
- Use maintenance windows that reflect business operating requirements.
- Investigate repeated failures rather than continually resubmitting patch activity.
- Review pending-reboot devices after maintenance.
- Confirm endpoints continue to report to Nex after patching and reboot activity.
- Review Nex and Windows Update logs when behavior differs from the expected workflow.

11. Related Documentation

- Nex Product Overview
- Nex System Requirements
- Nex Deployment, Security & Technical Guide
- Nex Administrator Guide
- Nex Agent Deployment Guide