

SOP – Patch Management with NinjaOne

Purpose:

To define the standard process for managing, deploying, and reporting on operating system and third-party application patches using NinjaOne to maintain security, stability, and compliance across all managed endpoints.

Scope:

Applies to all Windows and macOS endpoints managed through NinjaOne, including servers and user workstations.

Pre-Requisites:

- NinjaOne agent installed on all endpoints.
- Admin-level access to NinjaOne Dashboard.
- Defined patch approval policy (e.g., automatic approval for critical patches).
- Backup and recovery plan in place.

How to Deploy the NinjaOne Agent:

To enable patch management and other remote functions, the NinjaOne agent must be installed on all target devices.

Step-by-Step Agent Deployment:

1. Log In to NinjaOne:

- Visit NinjaOne Portal and log in with admin credentials.

2. Navigate to the Agent Deployment Section:

- Click the “+ Add” button at the top-right corner of the dashboard.
- Select “**Device**” from the dropdown menu.

3. Select Device Type:

- Choose the appropriate device type from the following categories:
 - Computer (Windows, macOS, Linux)
 - Mobile Device (Apple, Android)
 - Virtual Infrastructure (Hyper-V, VMware)
 - Cloud Monitor (Ping, Port Scan, DNS, HTTP/HTTPS)

- Run Ad Hoc Network Discovery (Network Management System)

4. Windows OS Configuration (Example):

- Organization: Select the correct organization or department.
- Location: This will be auto-filled based on the organization.
- Device Role: Leave set to Auto (recommended for most cases).

5. Generate the Installer:

- Click “Generate Installer.”
- A confirmation popup will appear with the message: “**Successfully generated**”

6. Download or Copy Installation Link:

- From the popup window, either:
 - Download the installer directly to your local machine, or
 - Copy the installation URL to use in email or scripts.

7. Install the Agent (Manual Installation):

- Run the installer (.msi for Windows, .pkg for macOS) on the target device.
- Once installed, the device will automatically register in the NinjaOne dashboard.

8. Silent Install for Mass Deployment (Optional):

- Use the silent install command (example for Windows):

bash

CopyEdit

NinjaAgentSetup.exe /quiet /norestart /org=YourOrgID /group=GroupID

- Deploy via GPO, Intune, PDQ Deploy, or other tools.

9. Verify Agent Status:

- Navigate to Devices.
- Confirm the device appears and is marked as “**Online**” and “**Agent Connected.**”

10. Assign Tags or Move to Device Group:

- Tag or group the device appropriately to apply the correct patching policies.

Patch Management Workflow:

1. Accessing the NinjaOne Patch Dashboard

- Log in to the NinjaOne Portal.
- Navigate to **Dashboard > Patching**.
- Click the “**Patching**” dropdown menu then two patch types will appear:
 - Software Patches
 - OS Patches
- Select the patch type you want to view.

- Important: Check both Software Patches and OS Patches daily to stay on top of updates and vulnerabilities.

2. Patch Approval and Scheduling

- Navigate to Pending Patches.
- A list of available patches will be displayed.
- Review and verify whether each patch is valid and necessary (check version, description, severity, vendor, etc.).
- Select the patches that should be approved.

After selecting patches:

- Two buttons will appear above the patch list:
 - **“Approve for Policies”**
 - **“Reject for Policies”**

To approve:

- Click **“Approve for Policies.”**
- A popup will appear with the message:

“Confirm

The following policies will be modified:

Select all

Windows Workstation Policy

- Check both:
 - **Select all**
 - **Windows Workstation Policy”**
- Click **“Confirm”** to finalize patch approval and schedule deployment based on policy settings.

3. Monitoring Patch Deployment

- Go to **Dashboard > Activity**.
- Monitor patch progress and success/failure rates.
- Re-deploy failed patches or troubleshoot as needed.

4. Post-Deployment Checks:

- Confirm critical services are functioning as expected.
- Verify that endpoints remain connected and reporting to NinjaOne.
- Escalate unresolved post-patch issues to senior.