Automating New Device Setup with NinjaRMM

Introduction

Setting up a new end-user laptop or workstation can cost IT anywhere from thirty minutes to three hours. On one end of the spectrum, the IT team my just join the device to the domain, install their antivirus, and hand it off to the end user; on the other end, you may have security-related configuration changes, multiple application deployments, and desktop personalization to perform before handing the device off.

Regardless of the number and complexity of steps taken before a new device is ready, this process is the first interaction IT will have with a new employee. Because of this, it is critical to the ongoing relationship between IT and the broader organization that the end-user have a positive onboarding experience.

Fortunately, for many organizations, new device setup is a highly standardized (or standardizable) task which lends itself to automation. Even if some customization is needed, automating the new device onboarding process can offer IT teams significant time savings. NinjaRMM recently conducted a survey of our customers which showed that our partners save 1.2 hours per endpoint on onboarding tasks when they automate with Ninja.

Whether you’re deploying from a golden image or from a clean Windows installation, Ninja can help automate personalized Windows setups at scale.

This guide walks you through some of the most common tasks you may perform when onboarding a device for a new employee and shows you how to automate that process with NinjaRMM.

Step 1

Document your endpoint setup process

Before you start setting up policies in NinjaRMM, you first need to identify which standard tasks, application deployments, and configuration changes you want to apply.

For example, you may want to:

- Join an Active Directory domain (or deploying a SaaS IAM product)
- Set up local users or local administrative accounts
- Uninstall unwanted applications
- Install productivity, security, management, or line of business applications
- Change device configurations like power management
- Personalize the user environment

If your new device setup process is already documented, you're all set. If not, you'll need to identify all the changes required on endpoints globally and on a client or role basis and document those steps. Using the activities tab, software inventory, and script repository in NinjaRMM may help you identify many tasks that can be standardized and rolled out during onboarding.

Each step then needs to be identified as global or role-specific. Global tasks may include installing Office 365 or joining the domain. Role-based tasks may include installing department-specific applications or mapping specific network drives.

You'll get greater time savings and have a greater impact on user satisfaction by really locking in the onboarding steps that impact every new employee, so time spent on global tasks is well spent. Functional or role-based automation can be incredibly impactful, but is secondary to a solid global onboarding automation.

Step 2

Write your scripts

While NinjaRMM provides some software installation and device configuration scripts out of box, you will need to write (or borrow) custom scripts to accomplish most steps in the device onboarding process. The NinjaRMM script share provides many great scripts you can borrow.

For each step in new device onboarding, we've curated several scripts from our shared library to help you get started:

Joining an Active Directory Domain
Join Active Directory Domain by Gabor Virag
Bulk Join PCs to Domain and Add to OU by Mason Schmitt

Setting up new users
Create a local admin account by Kelvin Tegelaar
Create a local user by Luc Blais

Uninstall unwanted applications
Uninstall Application (Windows) by Pedro Becker
Uninstall Application (Windows) by Leonard Wolf
Uninstall Application (Mac) by Justin Kikani

Install applications
Ninja provides a built-in software deployment script for MSI and EXE applications
Or script share includes dozens of custom software installation scripts

Manage Device Configurations
Change Registry Keys by Caleb Orviz
Encrypting drives by Kelvin Tegelaar
Changing power management settings by Clint Thomson
Deploy Wifi Profile by Kelvin Tegelaar
Renaming the device by Antonio Loffi-Lara
Enable Wake-on-Lan by Kelvin Tegelaar
Disable fast startup by Michael Muratovic

Personalize the user environment
Creating desktop shortcuts by Kelvin Tegelaar
Disabling or removing Cortana by Frank Marinex
Setting a default browser by Kelvin Tegelaar
Setting branded support information in Windows by Dallas Wilm

Please note: scripts in the NinjaRMM script share library are not supported or endorsed by NinjaRMM. Please take caution using scripts from any author you do not know and test scripts thoroughly before using them in production environments.

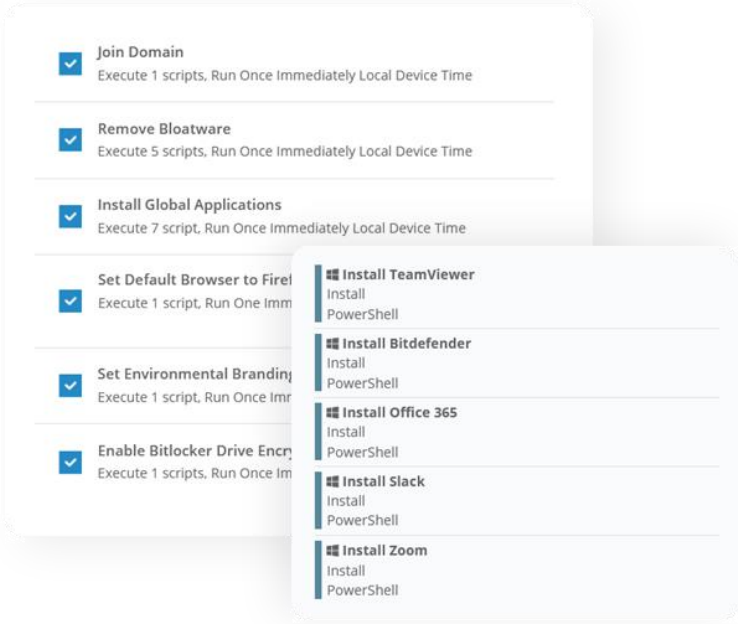
Step 3

Create a global device setup policy

From an ease-of-management perspective, we recommend separating your new device setup policies from your day-to-day management policies.

Your global device setup policy should include all the configuration changes, applications, and tasks you want to automate that are applicable to all endpoints. If a task is applicable to almost all endpoints, you can add it to the global device setup policy and disable it in child policies for the roles it is not applicable to.

- Create a new policy called Global Device Setup
- Add all the global configurations, applications, and tasks to the policy as scheduled scripts
- Set the script's schedule to Run Once Immediately – this forces the script to run as soon as the agent connects
- Add scripts in the order in which you want them to run. Scripts run in consecutive order.
- Save the policy



Step 4

Create role-based child policies

Role-based child policies allow you to add or remove automation steps from the global device setup policy. Child policies can personalize deployment based on user job function, location, or organization – whatever categorization makes sense for your business.

- Create a new policy and set the **Parent Policy** to **Global Device Setup** (created in the previous step)
- Add all the role-specific configurations, applications, and tasks to the policy as scheduled scripts
- Disable any configurations which are not relevant to the targeted role
- Save the policy

Master Onboarding Policy (Single-Org)

- Join Domain
- Uninstall Flash, Java, Silverlight, Bing Apps, Manufacturer Apps
- Install Applications: TeamViewer, Bitdefender, Office 365, Slack, Zoom, Firefox
- Set default browser to Firefox
- Set company wallpaper
- Enable drive encryption

Marketing Child Policy

Software
- Adobe Creative Suite
- Power BI

Configurations
- Map marketing drive

Engineering Child Policy

Software
- Notepad++
- AnyConnect VPN

Configurations
- Map dev drive

Finance Child Policy

Software
- Quickbooks
- NetSuite

Configurations
- Map finance drive

Master Onboarding Policy (Multi-tenant)

- Uninstall Flash, Java, Silverlight, Bing Apps, Manufacturer Apps
- Install Applications: TeamViewer, Bitdefender, Office 365, Slack, Zoom, Firefox
- Deploy backup
- Enable drive encryption

Client A Policy

- Join Client A domain
- Map network drives
- Deploy AutoCAD
- Deploy DeskTime

Client B Policy

- Join Client B domain
- Deploy WiFi profiles
- Deploy EHR
- Deploy Crowdstrike

Client C Policy

- Deploy JumpCloud
- Deploy WiFi profile
- Deploy VPN

Step 5

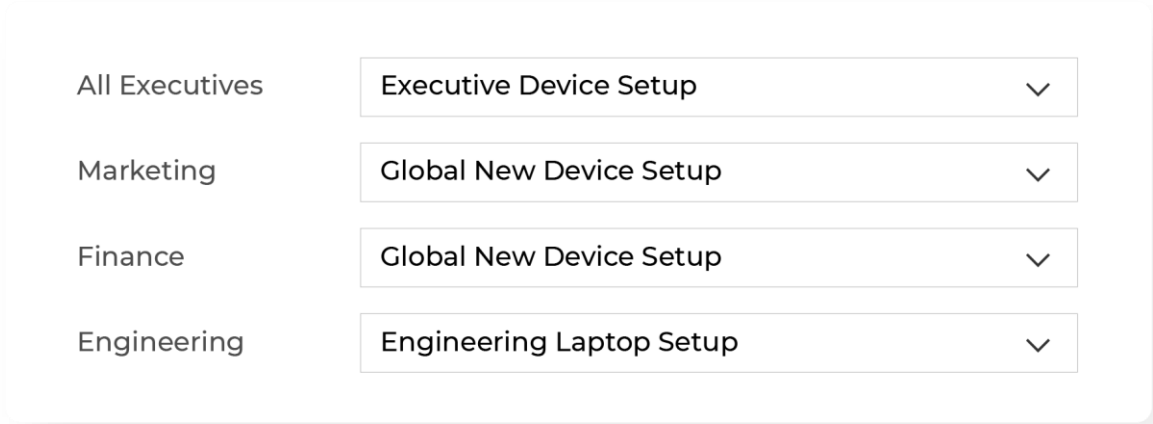
Test and deploy

Now that your policies are created it’s time to test your automated setup policy and deploy.

You’re going to want to test the policy and manually verify that all tasks were performed, applications deployed, and configurations changed with the expected results before deploying to production.

To automate deployment of these policies, you can create a new organization and assign policies based on role.

Once you’ve validated that the automation works on your golden image or devices in your organization, you can deploy to production.



About NinjaRMM

We are NinjaRMM

NinjaRMM is committed to building high-performance, scalable, secure, and easy-to-use IT management products that monitor, remediate, and enable MSPs and IT professionals to deliver business continuity and drive profitability. Our user experience was designed from the ground up to lower the costs of onboarding new users and maximize automation to deliver a modern IT management experience.

Easy to Use and to Work with

Industry-leading
Customer support

Fastest implementation
and pay-back time

Simple intuitive UI/UX

Talk with us

https://www.ninjarmm.com

sales@ninjarmm.com

USA: (888)-542-8339
DE: +49 (0)30-76758700
UK: +44 (0)20 3880 9027
FR: +33 (0)800 91 09 90