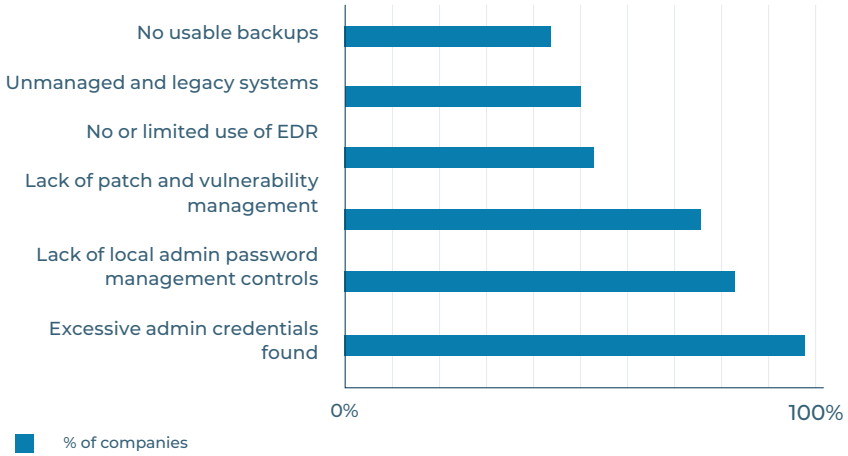
The Endpoint Defense Playbook: Locking Down Devices with NinjaOne

ninjaOne

Why is Endpoint Hardening Important?

At its core, endpoint (or device) hardening is the overarching concept of reinforcing security at the device level. Because securing your endpoints is fundamental to every other security action you take, the investment you make in it will have larger ROI than almost anything else. If you don't do it well, every other solution and step you take will have to be better, work harder, and have fewer gaps.

Unfortunately, according to Microsoft's 2022 Digital Defense Report, many organizations aren't taking the basic steps they need to support comprehensive endpoint hardening. Below are a few examples of key issues that have been negatively impacting cyber resiliency:



Though advanced security measures are important, it's critical to remember that the fundamentals still need work. In the same report, Microsoft found that basic security hygiene protects against 98% of attacks. By implementing good security practices, you can start building up those layers of security and give bad actors fewer opportunities to attack.

The chart below highlights the technical cybersecurity recommendations of major English-speaking governments for SMBs. Investments here (many of which are device hardening recommendations) provide the greatest 'bang for your buck' for most small and medium-sized businesses.

Guidance	Canada	Australia	UK	USA
Take regular backups	✓	✓	✓	✓
Patch OS and 3rd party applications	✓	✓	✓	✓
Configure and control application use	✓	✓	✓	✓
Encrypt drives and harden endpoint configurations	✓		✓	✓
Restrict user privileges	✓	✓	✓	✓
Enforce complex passwords and MFA	✓	✓	✓	✓
Enable AV / NGAV / antimalware solutions	✓		✓	✓
Secure portable media	✓		✓	
Enable the firewall on your devices			✓	✓

What Does Device Hardening Encompass?

Device hardening includes any changes you'd make to a device that helps improve the device's security. Here are a few examples:

Account Access Protection

- Enable and enforce MFA
- Remove extraneous accounts
- Change default admin accounts
- Enforce least privilege access across user accounts
- Block end-users from installing apps
- Enforce strong passwords

Device Configuration

- Enable secure boot
- Disable USB
- Encrypt disk
- Block net calls from applications (notepad, wscript, cscript, etc.)
- Reduce port exposure
- Enable and expand logging
- Disable insecure protocols like SMBv1, Telnet, and HTTP
- Password protect BIOS/UEFI

Software Management

- Remove potentially malicious apps
- Remove unsupported software
- Deploy antivirus / EDR
- Deploy password management solutions
- Enable firewall
- Remove old executables
- Prevent end users from installing apps

Auditing

- Audit device hardening

Note that this is not an exhaustive list, but a starting point for organizations looking for next steps in their endpoint hardening process. Not every device hardening activity will be applicable to every environment and many will need to be adapted to your own environment. And when improving endpoint security, remember that baselines are constantly changing, so security approaches should always be evaluated and refreshed on a regular basis.

It's also important to note that there are a number of critical actions that you may take to bolster your organization's security, but are not included in endpoint hardening, including:

- Identity and access management
- Advanced security solutions (SIEM, advanced AV, etc.)
- Security awareness training for end-users
- Network strategy
- Cloud application security
- Mobile threat defense

All of these actions are crucial to ensuring security, but don't specifically target security at the device level.

Automating Endpoint Hardening

Before we get into some examples of how organizations can use NinjaOne to strengthen and simplify their approach to endpoint hardening, let's talk a little more about automation.

In general, IT automation:

- Reduces the potential for human error
- Reduces the time investment in manual tasks
- Reduces costs
- Standardizes device management and service delivery
- Improves IT employee satisfaction
- Improves the end-user experience
- Helps to support compliance

By taking advantage of the benefits of automation, the endpoint hardening process becomes much simpler, more efficient, and cheaper in the long run. Additionally, since processes are set to run automatically, organizations can more quickly limit exposure to any potential vulnerabilities. The less time a device is exposed, the better off it'll be.

Within NinjaOne, there are various mechanisms that help organizations easily execute an automated IT workflow. In the next section, we'll be demonstrating five examples of how organizations can utilize Ninja's automation tools to improve device security, including:

1. Scheduled Scripts

When you want to take action against devices in a policy at a specific time or times

2. Scheduled Tasks

When you want to take action against devices in a group at a specific time or times

3. Script Result Conditions

When you want to regularly check information on a device and take action based on the returned results

4. Condition Triggered Script

When you want to respond immediately to a state change on a device

5. Custom-Field Triggered Scripts

When you need information Ninja doesn't collect by default or for multi-step / complex automations

Adding a Custom Script to NinjaOne

Because so many automations will need to be customized to individual environments, custom scripts are critical to automation in NinjaOne, so it's important to know how to add new scripts to your script library within the Ninja platform.

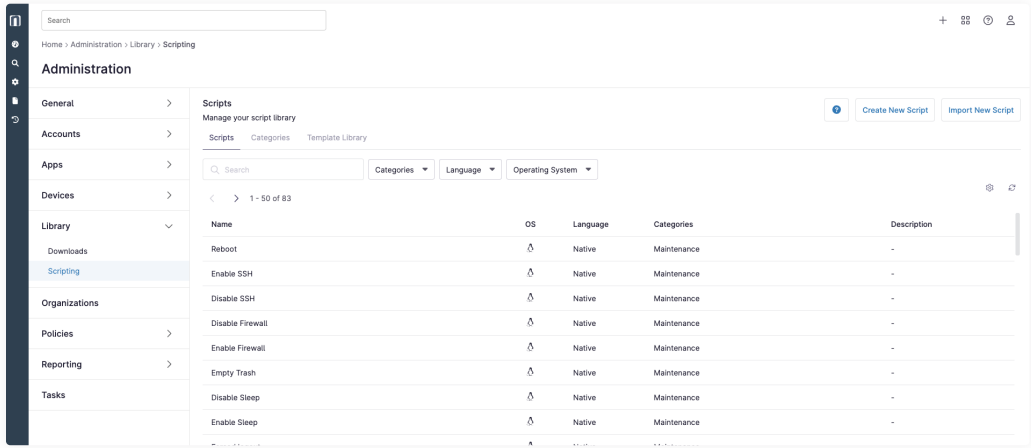
First, you'll head over to your Ninja dashboard and navigate to 'Administration' on the left-hand side. You'll click on 'Library' and 'Scripting' to access your script library (image 1):

To add a new script, you have a few different options. You can either:

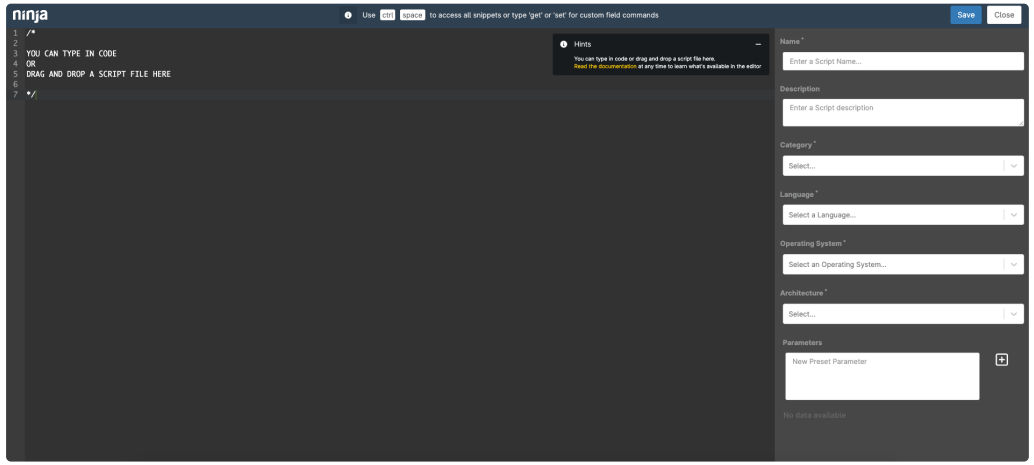
- Add a new script using the script editor (image 2):
- Import a new script using the template library
- Import a new script from your computer

For those of you looking for help with custom scripts, the Dojo (our Ninja customer community) is full of scripts uploaded by fellow Ninja users.

Note: Any scripts should be tested thoroughly before rolling out. Though the Ninja team does keep an eye on uploaded community scripts, they are not officially released by NinjaOne.



1. Script Library



2. Script Editor

ninjaOne

Five Ways to Automate Device Hardening

This list of five methods is far from exhaustive, but a good snapshot of what you can do within the NinjaOne console to help automate and support endpoint hardening.

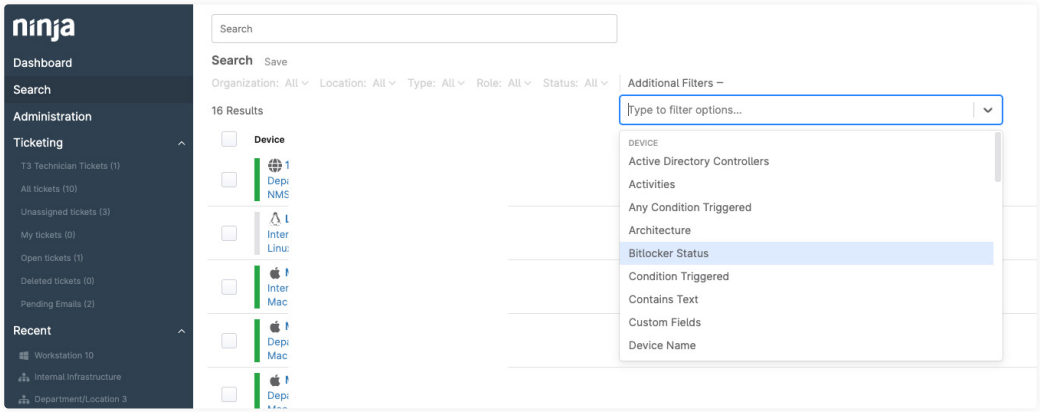
1. Deploy device security configurations on device setup

In this example we'll use the scheduled tasks mechanism to automate outside of policies.

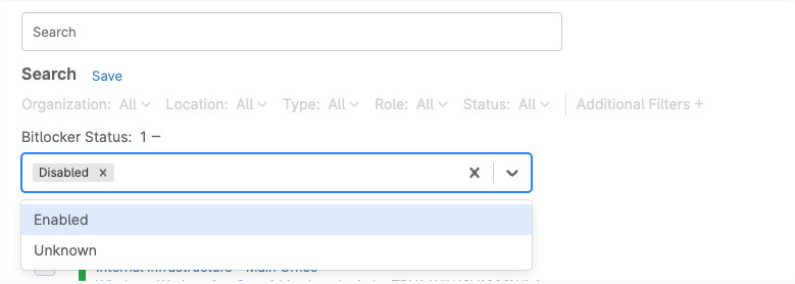
When setting up new devices, you can use tools that are automatically built into recent versions of Windows to improve device security. In this example, we're using Bitlocker, which is included on every Windows 10 and 11 workstation. With Ninja, you can natively track the status of Bitlocker, find devices that have Bitlocker disabled, and re-enable it using a custom script.

(If you do not already have the script to enable Bitlocker added to your console, follow the steps on Page 5 to add the script to your library. For this demonstration, we used this community PowerShell script. We would recommend naming it 'Enable Bitlocker' to easily find it during the scheduling process.)

In the Ninja console, you'll head over to 'Search' on the left-hand side and use the 'Additional Filters +' option to sort by Bitlocker Status (images 3 and 4):



3. Search



4. 'Bitlocker Disabled' Status Filter

ninjaOne

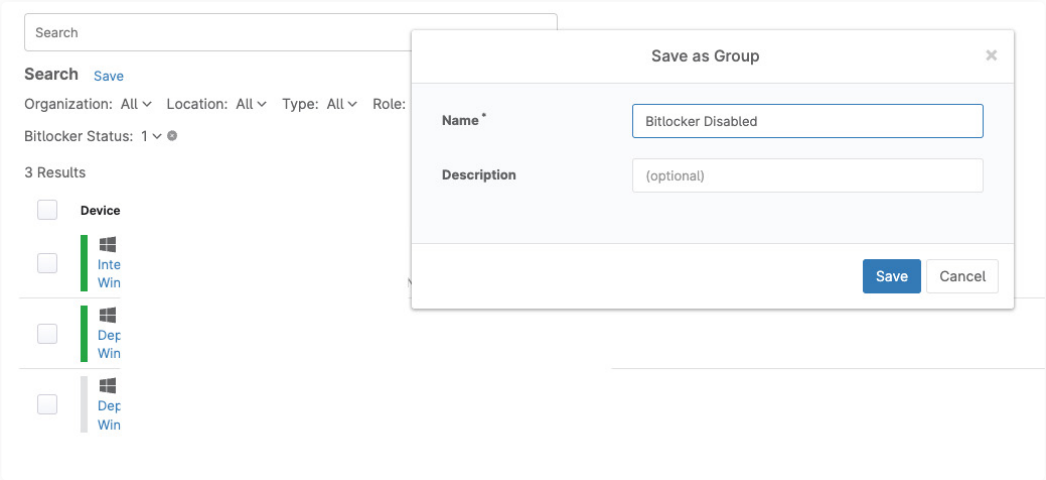
1. Deploy device security configurations on device setup *(cont.)*

You can also use the dropdowns to the left of the additional filters option to filter by organization, location, device type, role, and status. After filtering your desired endpoints, you can create a dynamic group with those that have Bitlocker disabled.

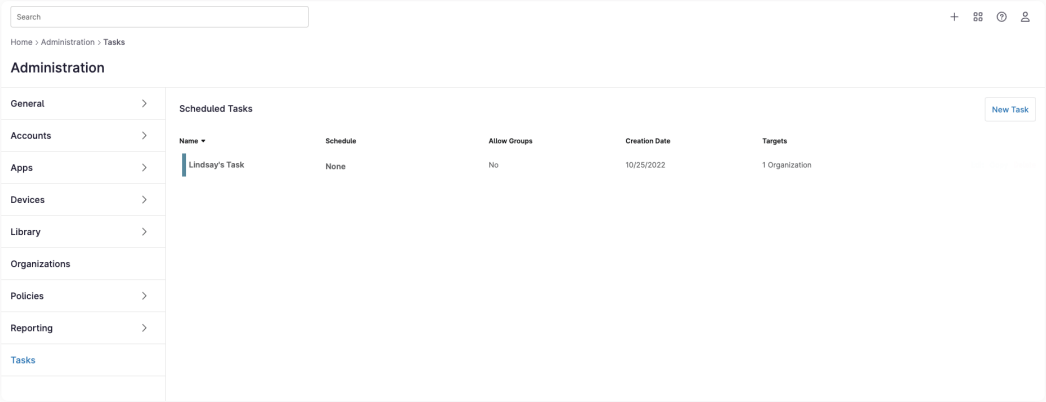
To create a dynamic group of these devices, you'll simply click on 'Save' above the filtering options and choose a name for your group (image 5):

Once your dynamic group is created, it will always show you up-to-date information. As you enable Bitlocker on these devices, it will fall out of this group. As you onboard new machines that don't have Bitlocker enabled, they'll show up in this group. Remember the name of the group you've created because we'll be searching for it in a minute.

You'll likely want to add some automated remediation to this process, so to do that, you'll head to 'Administration' on the left-hand sidebar and go down to 'Tasks' to add a New Task. The 'New Task' button will be on the top right-hand side of the Tasks page (image 6).



5. Dynamic Group with 'Bitlocker Disabled' Devices



6. Scheduled Tasks

ninjaOne

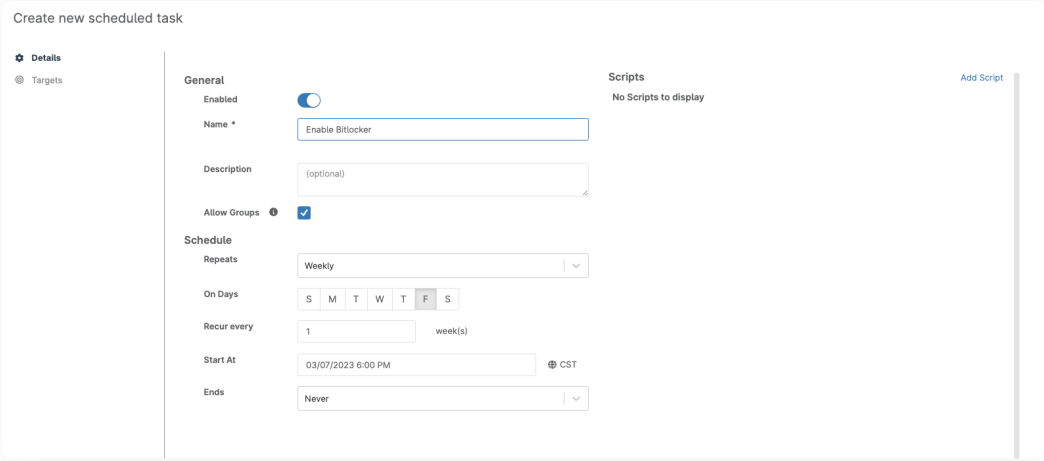
1. Deploy device security configurations on device setup *(cont.)*

After creating a new scheduled task, you'll add a name, your desired schedule (in this example, it's every Friday at 6pm CST), and a script on the right-hand side (Image 7).

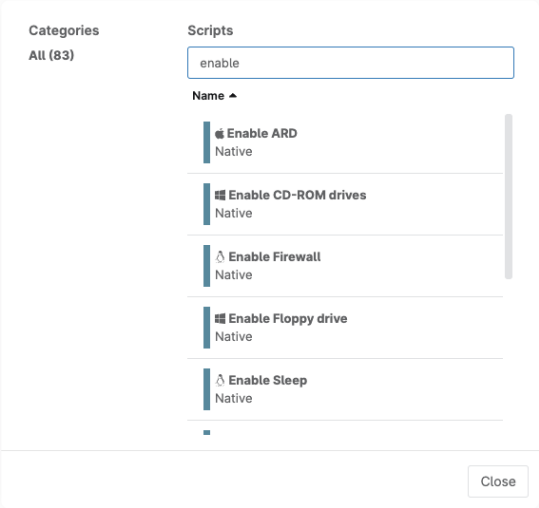
Once you have the 'Enable Bitlocker' script added to your library, you be able to search for it. This is what the available script list will look like (Image 8):

With the task schedule set and script chosen, you'll head down to 'Targets' and add a new target on the right-hand side. You can choose from organization, device, or group. In this case, we'll select Group and search for the 'Bitlocker Disabled' dynamic group that was created earlier (Image 9).

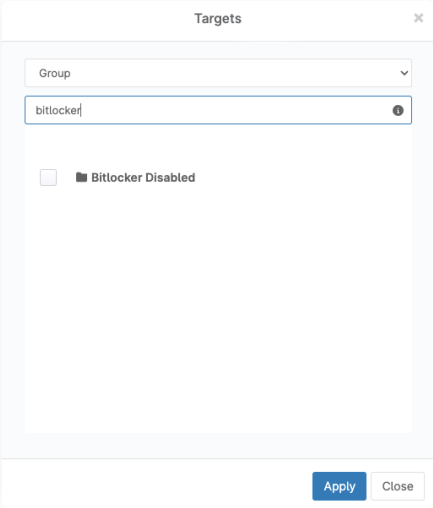
Some other examples of using dynamic groups with scheduled scripts include disabling mass storage devices, setting UAC, etc. Within the NinjaOne Template Library in the console, you'll find a number of ready-to-go script templates.



7. Creating a New Scheduled Task



8. Script List



9. 'Bitlocker Disabled' Dynamic Group TargetDynamic Group Target

ninjaOne

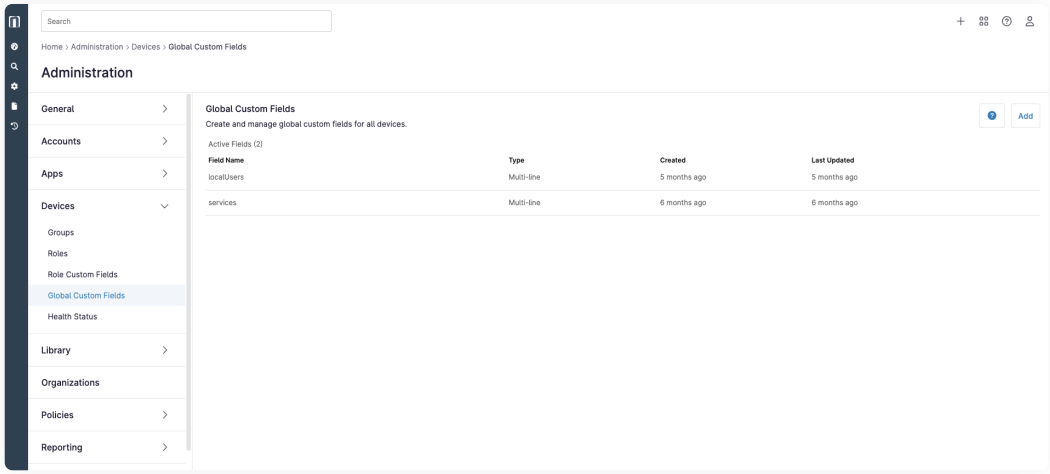
2. Enabling device firewall and blocking outbound net connections

In this example we'll use custom fields and policy conditions to detect a device state and trigger an automation.

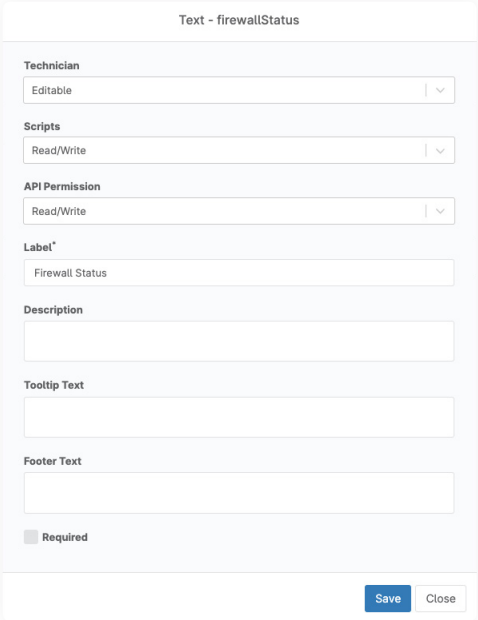
To check on the status of the device firewall in Ninja, we'll be focusing on the custom field and scheduled scripts mechanisms. Custom fields can be used in a variety of ways, but in this particular way, it will store the output of a PowerShell script.

To add a new custom field, you'll head over to the 'Administration' tab on the left-hand side of your dashboard and open up the 'Devices' section. Click on 'Global Custom Fields' and add a new custom field at the top right-hand side (image 10):

You'll create a new custom field called 'Firewall Status' and once created, it will pop up a new box giving you the option to change Technician access levels, script read and write capabilities, API read and write capabilities, a label, and additional text. You'll set the Scripts Permissions to Read/Write and hit Save. You'll also likely want the Technician field set to 'Read Only' (image 11):



10. Global Custom Fields



11. New Global Custom Field

ninjaOne

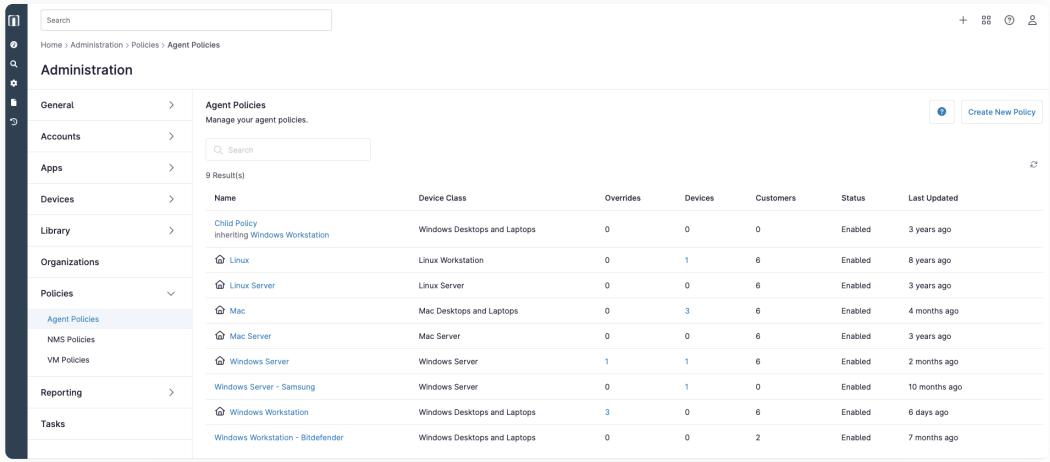
2. Enabling device firewall and blocking outbound net connections *(cont.)*

Once created, head over to your policies and choose the policy you'd like to manage. (If you're unfamiliar with policy setup, check out the NinjaOne policy efficiency webinar or Dojo KB article.) (image 12)

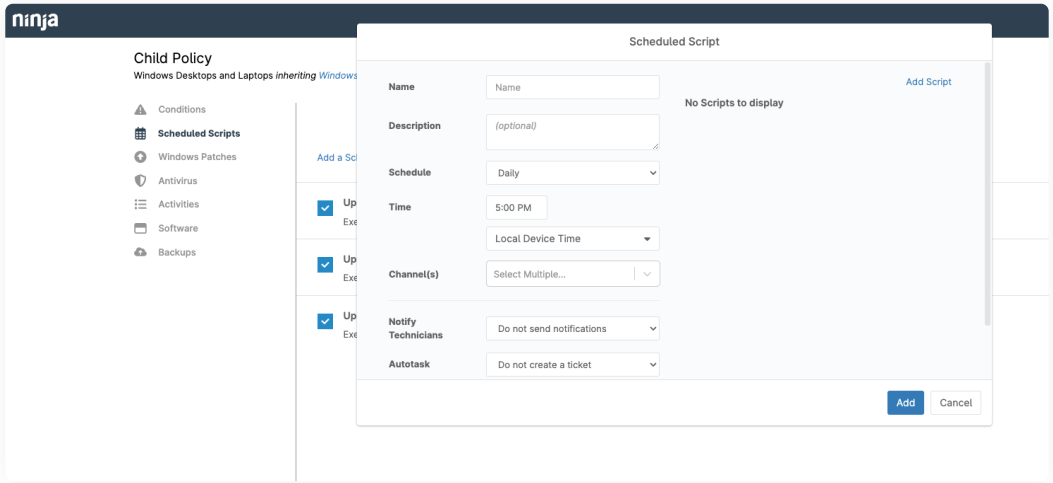
On the policy page, go down to 'Scheduled Scripts' and add a new scheduled script using the button above the list of scheduled scripts (image 13):

Once you have your script named and set a schedule, you'll add a script from your library on the right-hand side. In this case, we've used a basic Check Firewall Status PowerShell script located here. (This is not an official Ninja script, please test in your environment thoroughly before using! If you have not yet added a custom script for checking your firewall status, please follow the instructions to add a new script on Page 5 of this guide.)

Click Save and this will add the scheduled script to your policy. Next, you'll head up to the 'Conditions' section and add a new condition. In this new condition, you'll click on 'Select a condition' at the very top and choose 'Custom Fields' from the dropdown.



12. Agent Policies



13. New Scheduled Script

ninjaOne

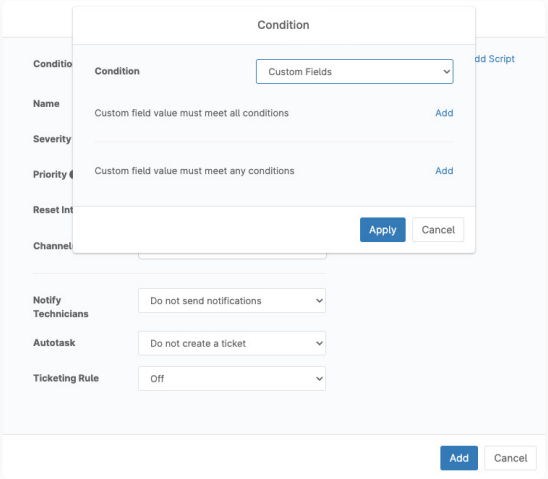
2. Enabling device firewall and blocking outbound net connections *(cont.)*

After choosing custom fields, you'll now have two different dropdowns under the 'Custom field value must meet all conditions' text (image 14):

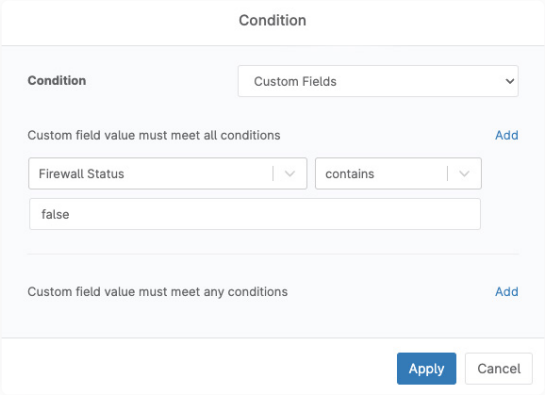
In the first dropdown, you'll select the Firewall Status custom field you created. In the second dropdown, you'll select 'contains' from the list. Below those two dropdowns, you'll type 'false' in the text box (meaning that the firewall is disabled) (image 15):

Once added, you should be able to now add a script on the right-hand side (image 16):

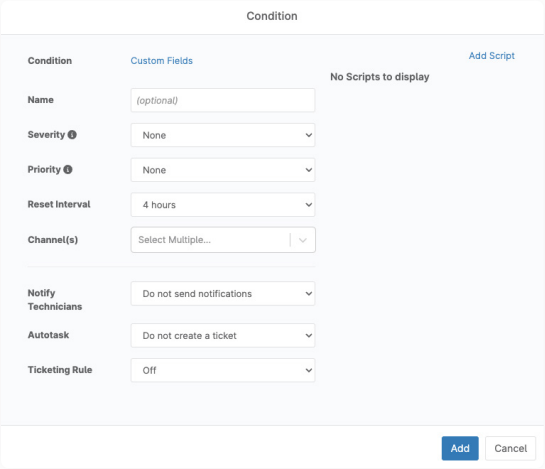
If you haven't yet added the Set-WindowsFirewall script to your Script Library, head over to the Administration page, go



14. Custom Field Conditions



15. Condition Parameters



16. Condition Details

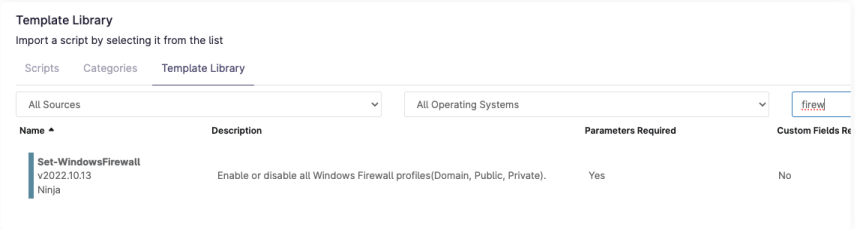
ninjaOne

to the 'Library' section and go to 'Scripting' to find your Script Library. The Set-WindowsFirewall script is baked-in to the Ninja platform, so you'll just have to go to the Template Library and import it (image 17):

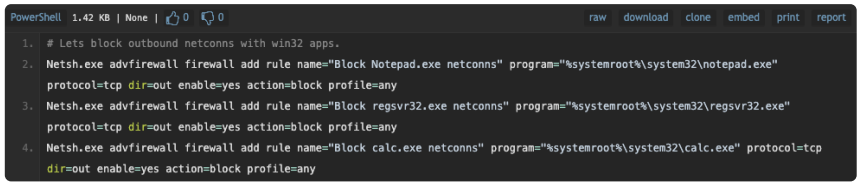
Once imported, it will appear in the dropdown to add as a script, and you can move forward with applying the condition to your policy.

To enhance firewall protection, you can also add a custom script to block outbound network communications. To add that script, you'll follow the same custom script instructions listed on Page 5. For this example, we used this Block Outbound NetConns for win32 PowerShell script. **(Again, this is not an official Ninja script, so please test extensively!)** (image 18)

Within that custom script, you'll add the desired applications you'd like to block internet access to. For example, it's unlikely that Windows calculator or Notepad will need internet access (but can be faked and used as vectors of attack), so you can add them to the list of any applications within the custom script itself. Once added to your Script Library, you can add the Block Outbound NetConns script to the same Check Firewall condition that you added the Set-WindowsFirewall script.



17. Set-WindowsFirewall Script in Template Library



18. Block Outbound NetConns for win32 PowerShell Script

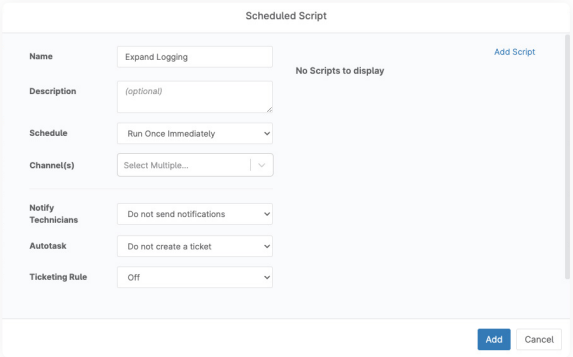
3. Enabling, expanding, and parsing logs

In this example we'll use custom fields and policy In this example we'll trigger an automation on device setup to change a device configuration.

Device configuration is only as good as the information that you're getting from it, which is where logs come in. Logs help you know what's happening on the device and certain logs may need to be expanded so you can get an accurate view of the health and security of your environment.

Before we take any additional steps, you'll want to add a new custom script to your library specifically for expanding those event logs. You'll follow the same custom script instructions listed on Page 5. We used this Expand Event Logging PowerShell script. (**Again, this is not an official Ninja script, so please test extensively!**)

Once you have your custom Expand Event Logging script added to your script library, you'll come back to your chosen policy page and navigating to 'Scheduled Scripts.' This scheduled script uses the 'Run Once Immediately' cadence, running on all of the devices within your chosen policy.



19. Expand Logging Scheduled Script

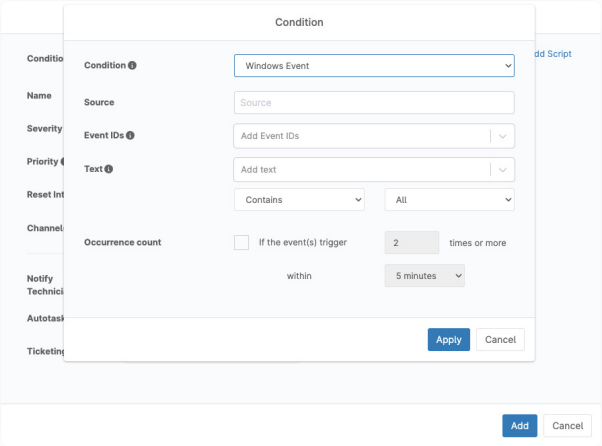
Run Once Immediately runs when devices are online, runs on any offline devices once they're back online, and runs on any new devices that join this policy (image 19).

Once you've chosen this cadence, add your Expand Event Logging custom script on the right-hand side. From there, you can apply this scheduled script to run immediately.

In addition to expanding logs, monitoring your event viewer from privilege escalation is another way to add a layer of endpoint security. This process will take place in the 'Conditions' tab where you can set up a new condition.

You'll add a new condition and choose 'Windows Event' to add a source and specific Event IDs that you want to monitor (image 20).

Once any of the Event IDs triggers, you'll be alerted of any changes in a particular user and be able to take action. There is no specific remediation in this guide, but you do have the option to add remediation into the automation steps using custom fields.



20. Windows Event Condition

ninjaOne

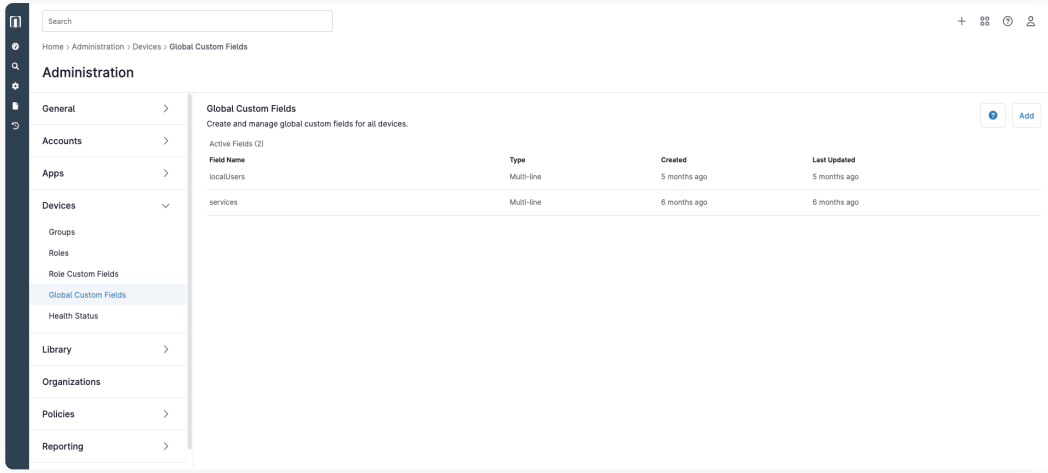
4. Creating a local admin account and automating password rotation

In this example we'll trigger an automation on device setup, then run a regular automation to change an admin password.

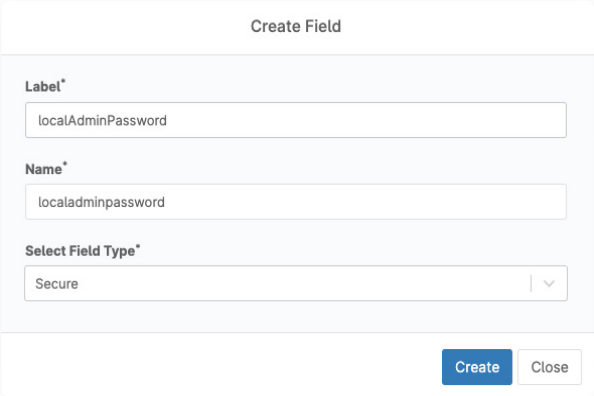
There is built-in functionality in Windows that you can take advantage of in Ninja to help with password rotation and protection. You'll follow the same steps of creating a custom script on Page 5 (we used this one in our example, but an additional reminder that **this is not a Ninja-created script, and you should test extensively before enabling**), add the script to a scheduled script in your chosen policy, and set it to run on your desired cadence.

For this, you'll go back into your Global Custom Fields menu (Administration > Devices) and add a new field (image 21).

In this new field, you'll label it the same thing that you set in the password rotation custom script (which is 'localAdminPassword' by default) and select the 'Secure' field type from the dropdown (image 22).



21. Global Custom Fields



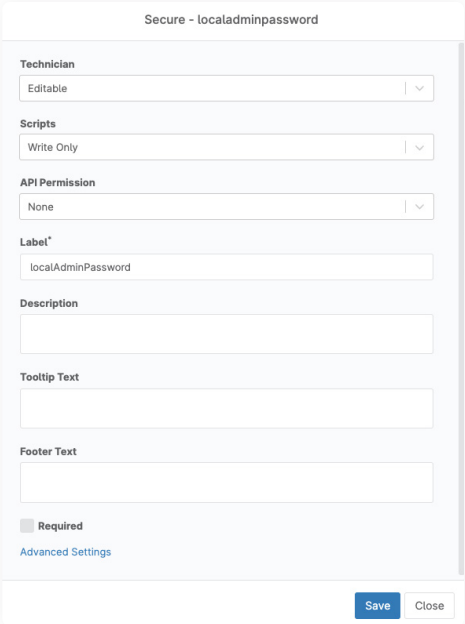
22. localAdminPassword Field

ninjaOne

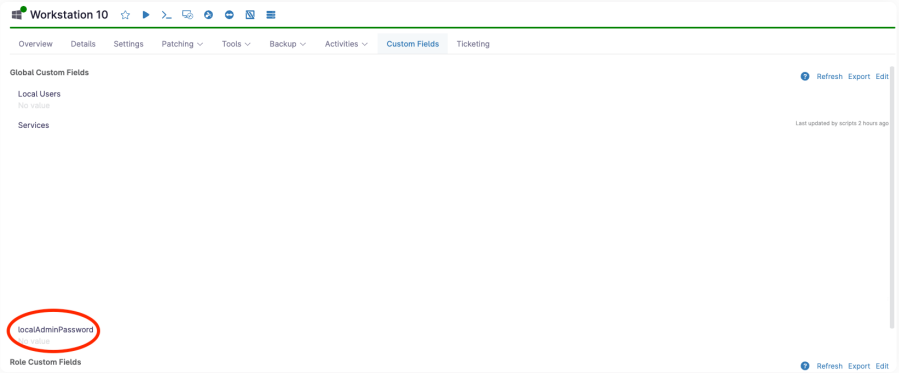
4. Creating a local admin account and automating password rotation *(cont.)*

A Secure field is specifically built for securely handling credentials - it is not visible in plain text, requires MFA to view, and is fully encrypted. There is also auditing to see who has access to the Secure field that's been added. Once you've clicked on 'Create,' you'll see a new box with some dropdown options. For this field, you'll want to set your Scripts to 'Write Only' and ensure the field is read only by technicians because this script creates a service account, generates a random alphanumeric character string as the password, and adds it as a Secure custom field. Once the password is generated, the script will write the password back into the Secure field (image 23).

This means that you don't have standardized passwords across the board and can go into the individual device to see the localAdminPassword in the Custom Fields section of the device page (image 24).



23. Secure Custom Field



24. Admin Password on Device Page

5. Detecting and removing potentially malicious software

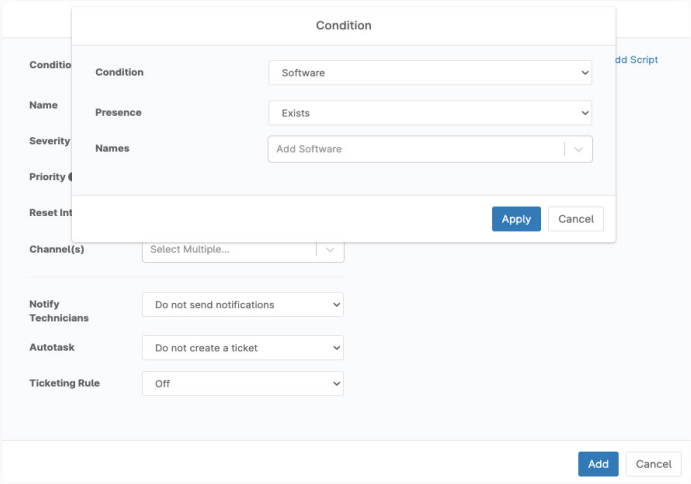
In this example, we'll use a policy condition to detect a state change (software installed) and trigger an automation to remediate the issue.

You can use Ninja's automation tools to detect and remove malicious or unwanted software easily from endpoints. Before you create the software detection condition, you'll need to add the Uninstall Application custom script to your library using the instructions on Page 5. The Uninstall Application PowerShell script we used in this example is located here. **(Again, this is not an official Ninja script, so please test extensively!)**

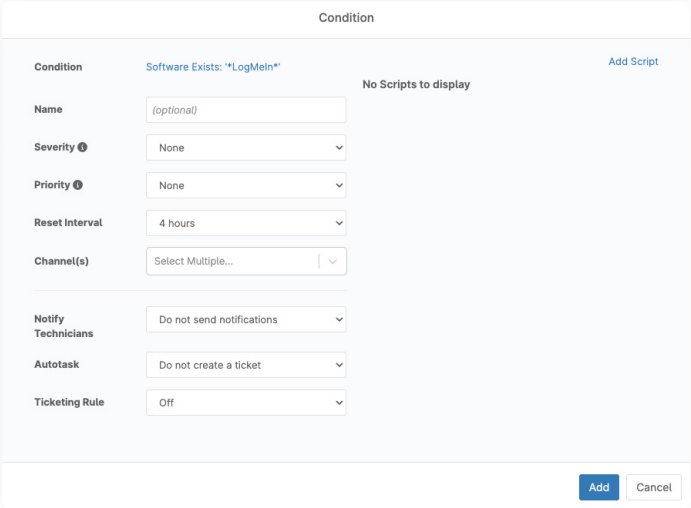
Once you've added that custom script to your library, you'll go back into the policy that you want to update, make your way back to the Conditions tab, and add a new condition. After choosing 'Select a condition' from the top, you'll choose 'Software' from the first dropdown and choose 'Exists' from the second dropdown (image 25):

After selecting both of those, you'll enter the name of the software that you'd like to detect. If you add asterisks around the software name, it will pull in anything that uses that name in the software title, not just exact matches. Once you've saved that information, you can add the script on the right-hand side (image 26):

To ensure you're fully remediating your issues, test and confirm that this PowerShell script or uninstaller will successfully remove the application before deploying fully.



25. Software Exists Condition



26. Condition Details

Resources

Endpoint hardening is essential, and with proper automation, it can be easy to implement and maintain. If you've been looking for a tool to help you automate your IT workflow, get access to a free NinjaOne trial here:

https://www.ninjaone.com/freetrialform/

We've also put together a list of a few security frameworks you can use when securing your network and devices:

- NIST Guide to General Server Security
- CIS Benchmarks for Microsoft Windows Desktop
- MITRE ATT&CK Security Knowledge Base

ninjaOne