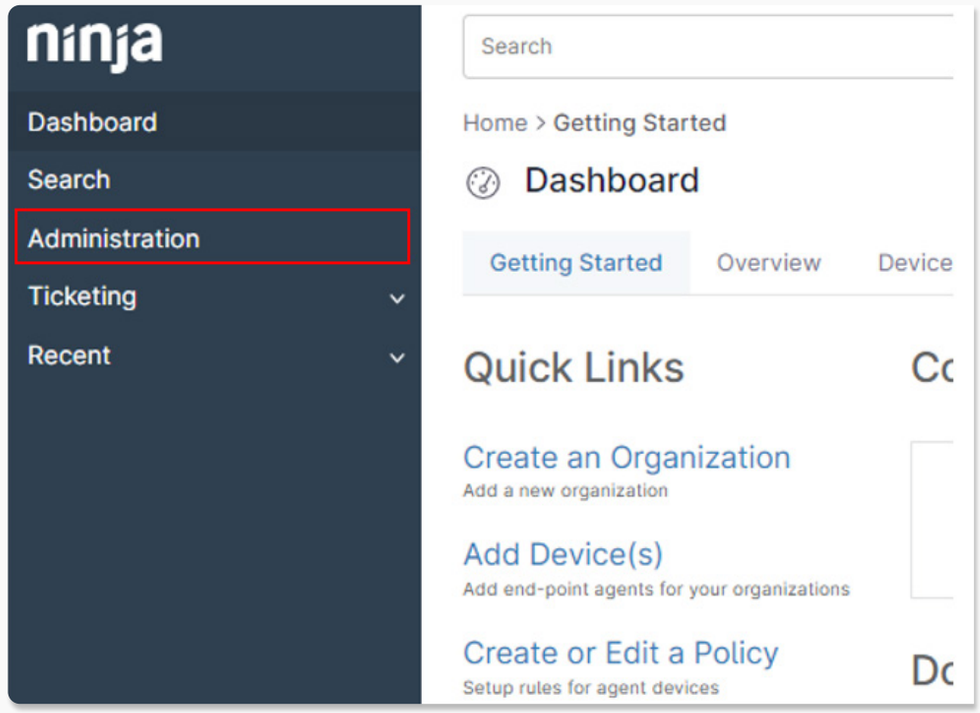
NinjaOne Onboarding Guide

ninjaOne

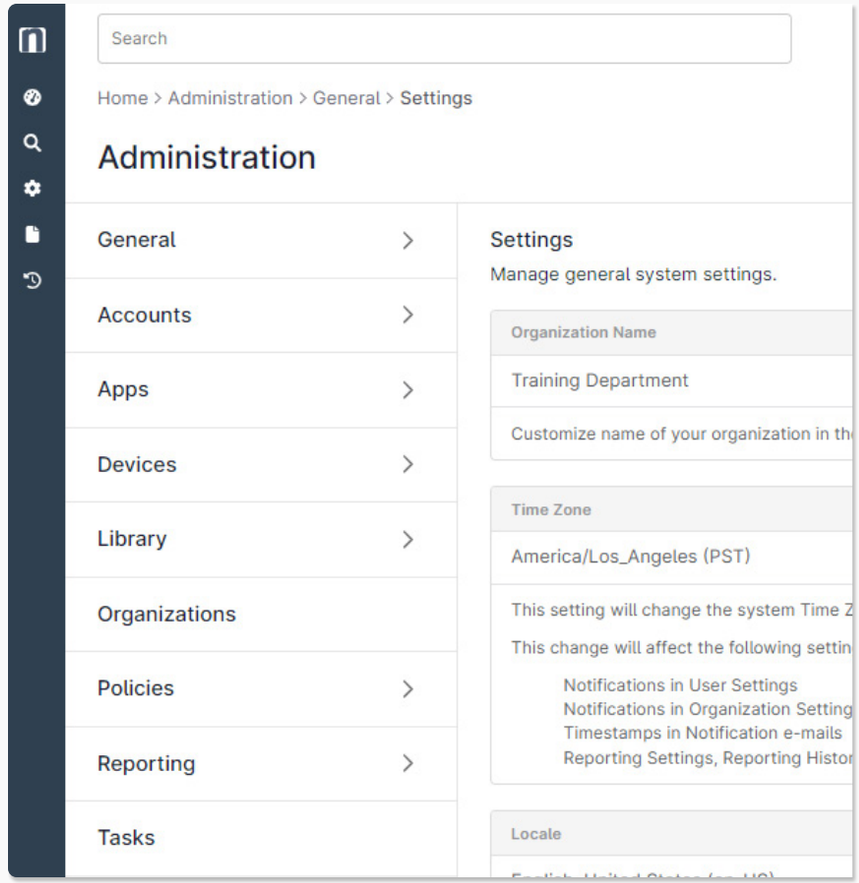
NinjaOne Onboarding Guide

You'll find that many of these settings can be created/edited from multiple sections of Ninja. For the purpose of this guide, however, we'll be focused on the Administration tab found in the left-hand side menu bar:



There are several sections under the **Administration** tab. In this guide, we'll be covering each of these sections:

- **General**
- **Accounts**
- **Apps**
- **Devices**
- **Library**
- **Organizations**
- **Policies**
- **Reporting**
- **Tasks**

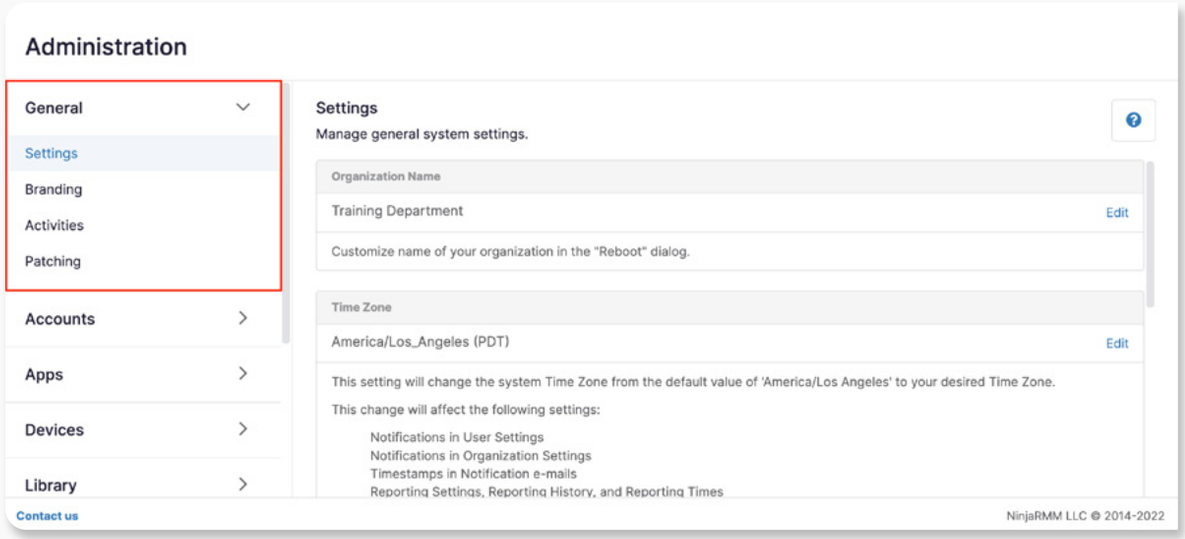


ninjaOne

General

The **General** tab includes a number of sub tabs:

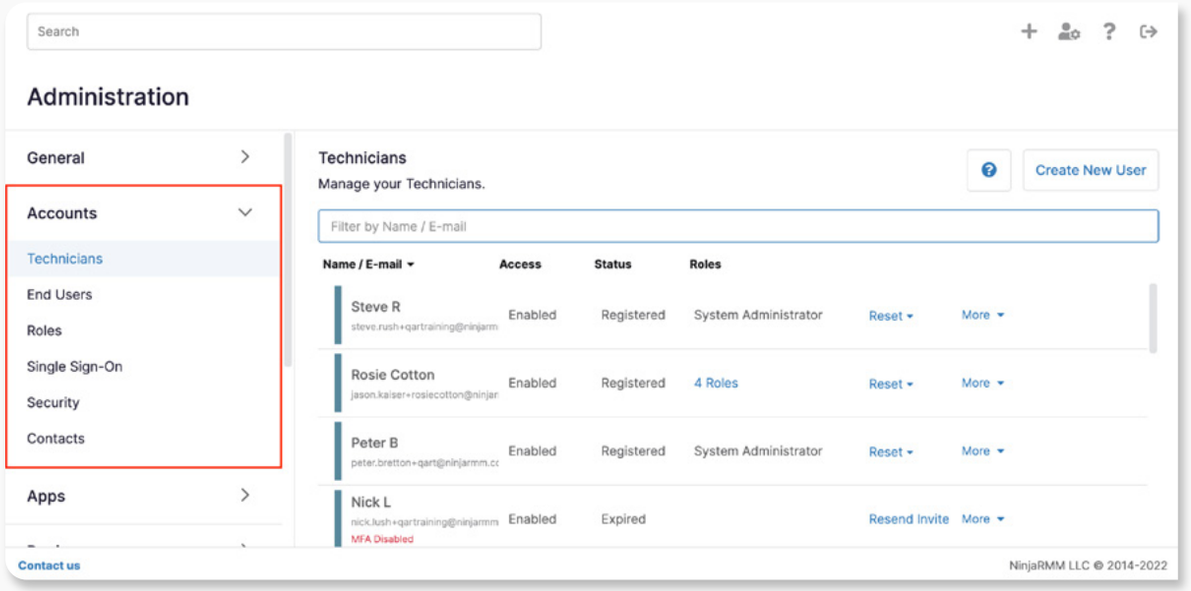
- **Settings -** This is where you can configure your organization name (as used in the dialog box any time you initiate a reboot on an endpoint), Time Zone Settings, locale settings, Ninja Agent Uninstall Prevention, advanced installer options, and deduplication.
- **Branding -** This is where you can configure your branded website and systray icon.
- **Activities -** Allows you to enable notifications and/or ticket creation for any system activities.
- **Patching -** This is where you can add preemptive patch approvals and rejections.



Accounts

The **Accounts** tab includes the following sub tabs:

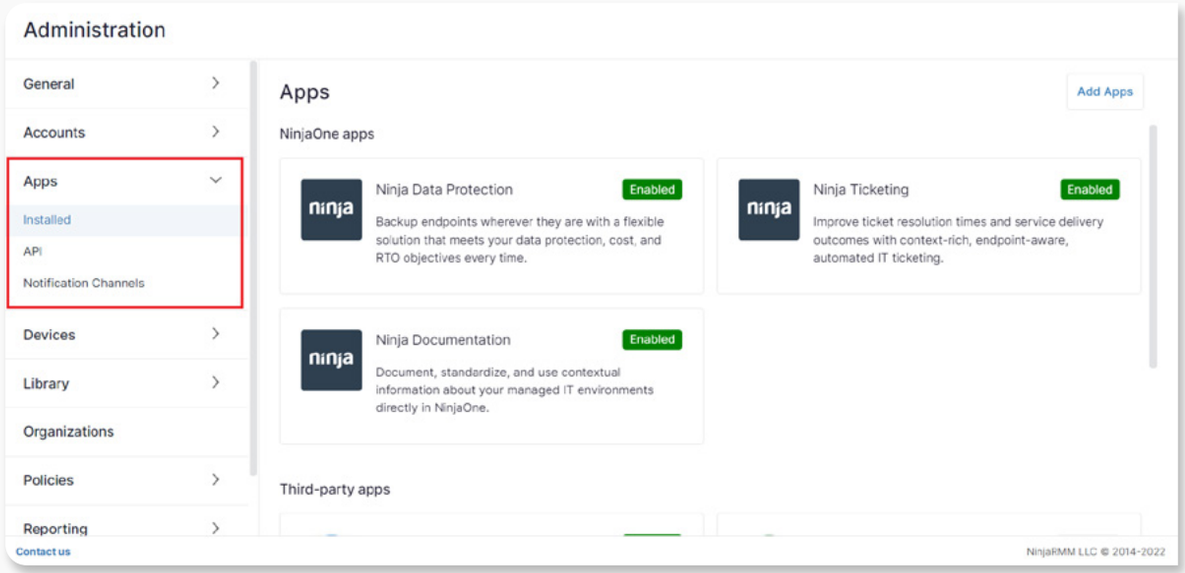
- **Technicians -** Allows Ninja system administrators to create, edit, and/or delete additional technicians.
- **End Users -** Allows Ninja system administrators to create, edit, and/or delete end users.
- **Roles -** Allows Ninja system administrators to create roles with specified User Permissions.
- **Single Sign-On -** This is where you can configure SAML for your account.
- **Security -** This is where you can set the MFA global administrative idle time security settings, as well as restrict user logins by IP addresses.
- **Contacts -** Allows Ninja system administrators to manage contacts for Ninja Ticketing.



Apps

The **Apps** tab allows you to set up any of the integrations that Ninja has to offer to increase your productivity and maximize your business potential.

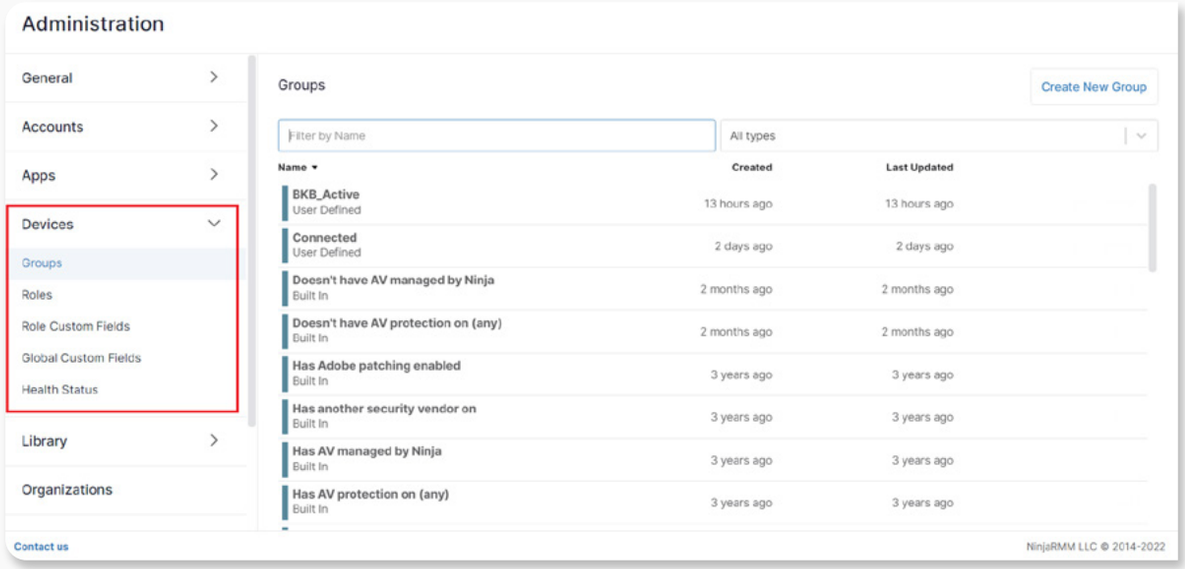
- **Installed -** This section contains apps which have been installed. They are broken into two groups, NinjaOne native apps, and Third-party apps.
- **API -** This section offers both documentation and examples of what can be done with Ninja's public API. Use this section to generate an API key or view the documentation and examples.
- **Notification Channels -** For information about setting up Notification Channels, please see **Notification Channels**



Devices

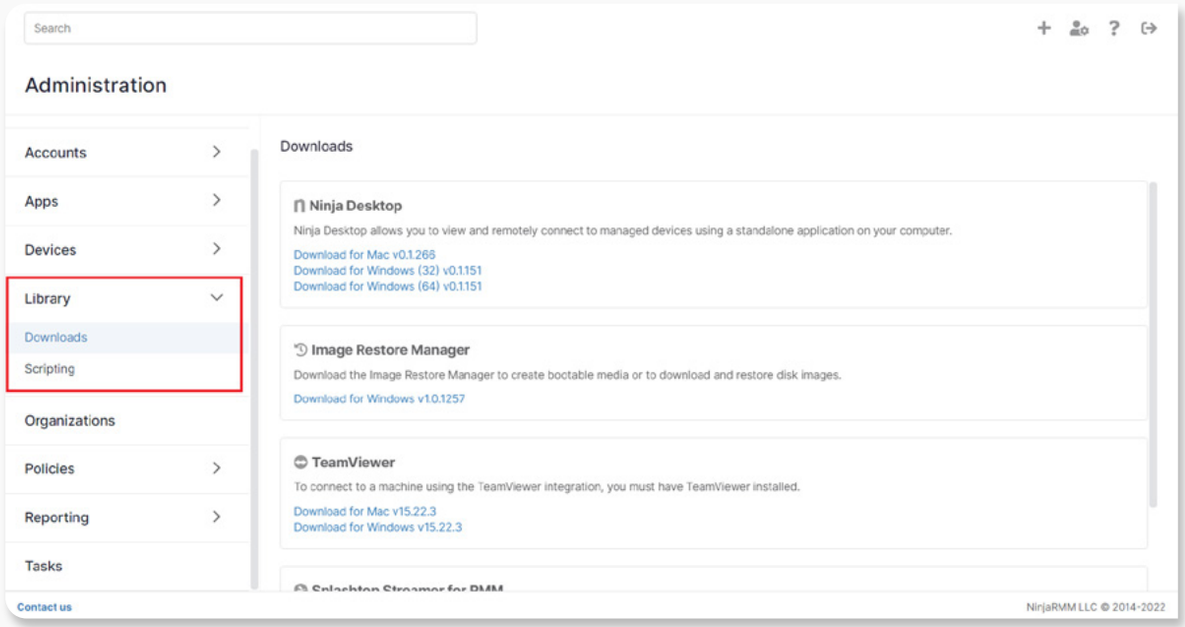
The **Devices** tab allows you to configure customized device roles, role custom fields, global custom fields and health statuses.

- **Groups -** This section provides a list of all groups which exist in Ninja.
- **Roles -** This section is where you can assign different Role Custom Fields to device roles which can then be applied to devices. For more information about setting up device roles, please see **Device Roles**.
- **Role Custom Fields -** This section allows you to create and keep track of Role Custom Fields. These fields can then be assigned to a role in order to be applied to specific devices. For more information about setting up custom fields, please see **Custom Fields (BETA)**
- **Global Custom Fields -** This is similar to the Role Custom Fields section, however, the fields created here will be global and as such will appear on all devices regardless of device role.
- **Health Status -** This section allows you to configure the different health statuses in Ninja. For more information about setting up health statuses, please see **Health Statuses**.



Library

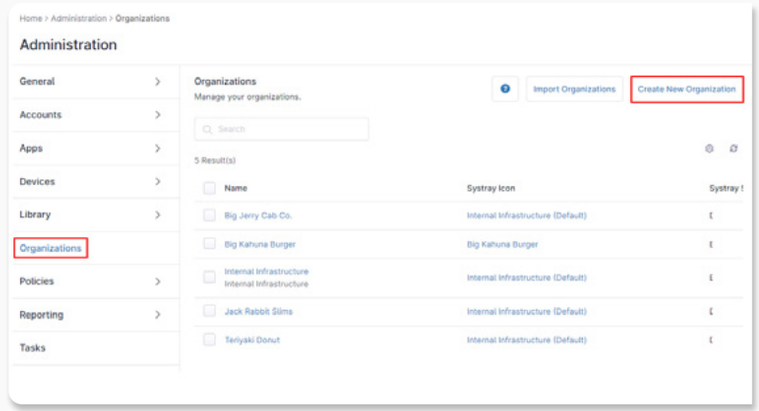
- **Downloads -** This section provides the download links for software within Ninja.
- **Scripting -** This section is where you can create and manage custom scripts in Ninja. For more information about the Script Library feature, please see our **Script Library** documentation.

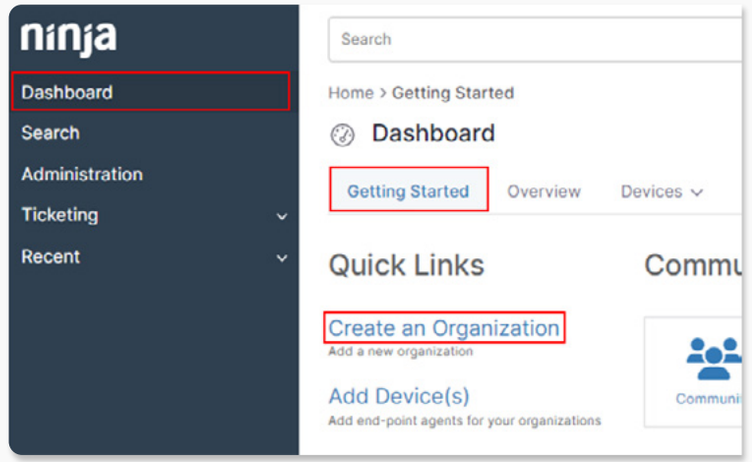


Organizations

The **Organizations** tab allows you to create and configure the customers that you wish to onboard and manage with Ninja; it is the shell in which you will assign policies.

1. There are multiple ways to create an organization:
    - Navigate to Dashboard and select the **Getting Started** tab. Select **Create Organization**.
    - Navigate to **Administration** and select **Organizations**.
    - Click on **Create New Organization** button.





ninjaOne

Organizations

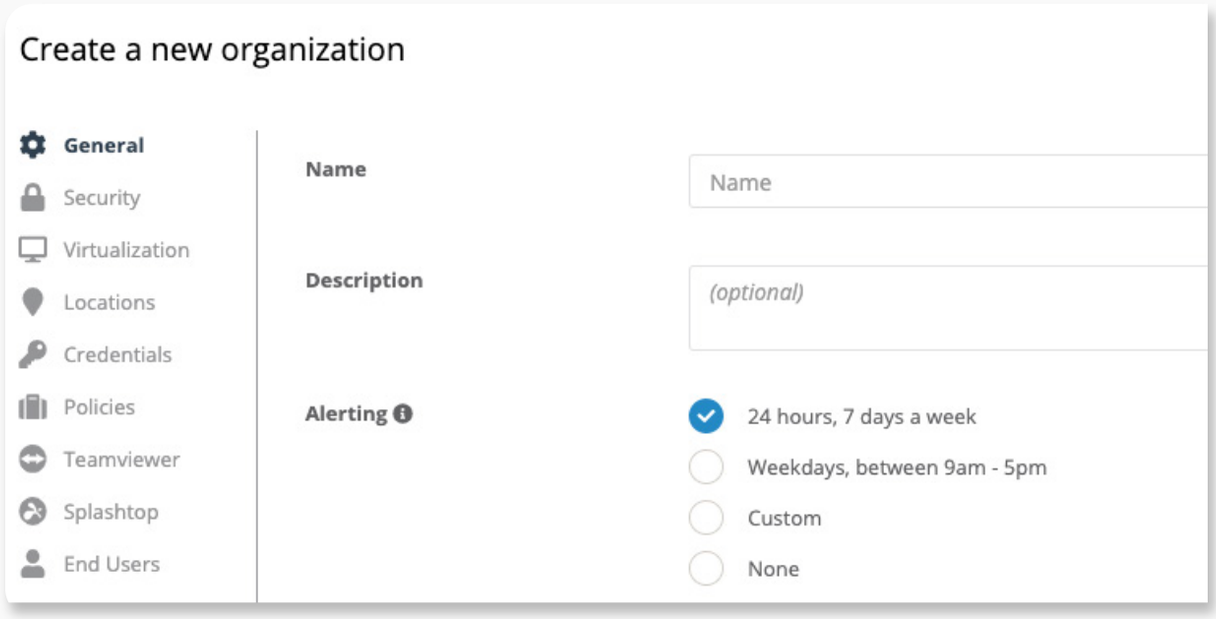
2. In the organization editor, you'll notice at least nine left-hand side tabs: General, Devices, Virtualization, Locations, Credentials, Policies, Splashtop, End Users, and Patching.

› General

- Type in the organization name and an optional description.
- Configure the time window in which you want to receive alerts for this organization (this may be based on the SLA agreement that you have with the client).
- Toggle the **systray icon** on/off for this organization.

› Security

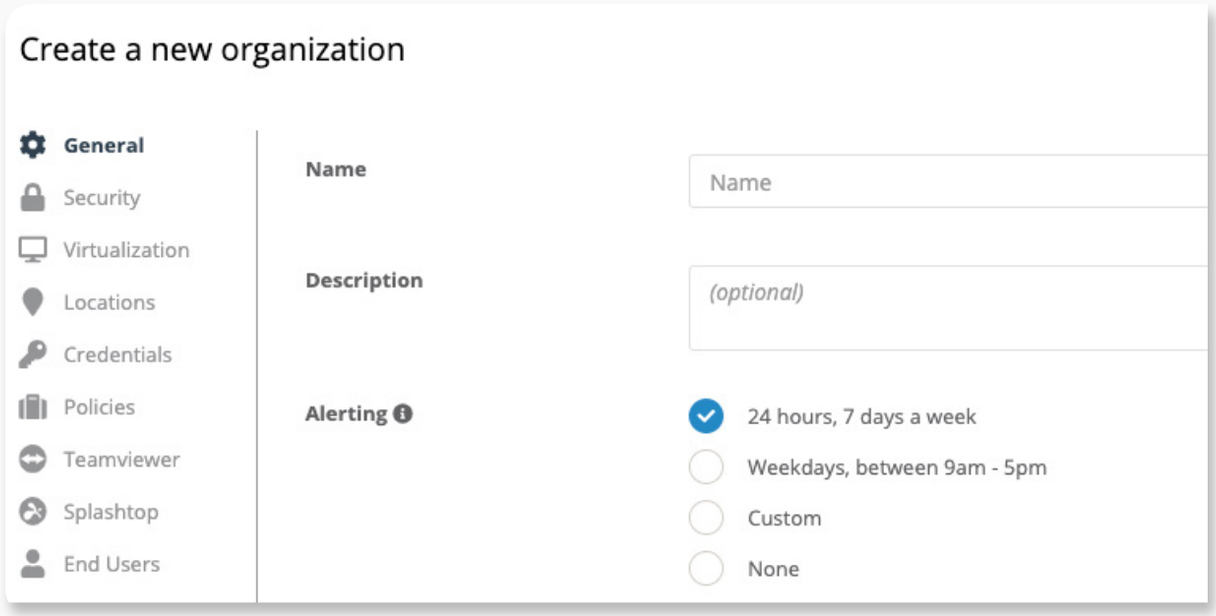
- Configure the approval settings for incoming devices under the organization.
- View any pending, approved, or rejected devices under the organization.
  (see: **Node Approval**)



Important Note: If you have other integrations enabled in Ninja, you may see additional tabs here (such as **TeamViewer** or **Backups**, as in the screenshot above).

Organizations

- **Virtualization**
  - Configure VMware monitoring for the organization. (see: **VMware Monitoring**)
- **Locations**
  - Create, edit, or delete different office locations under the organization.
  - Main Office is the default location. (see: **Locations**)
- **Credentials**
  - Add credentials to the organization's credential store.
  - Set the default credentials to be used for the devices under the organization. (see: **Credential Exchange**)



ninjaOne

Organizations

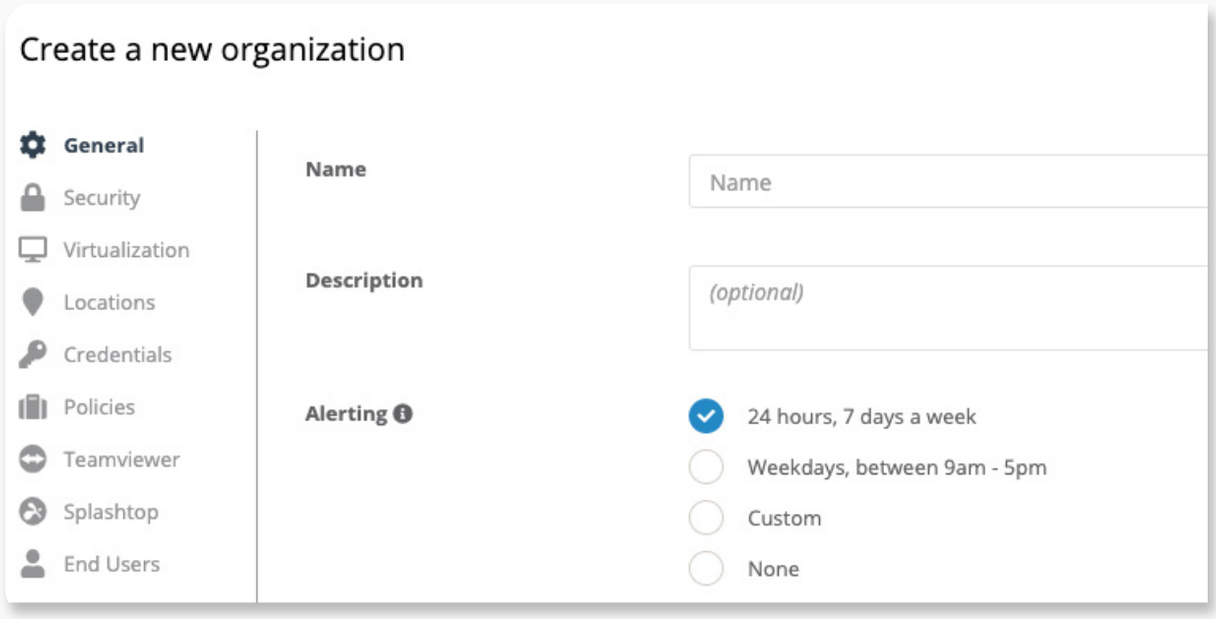
- **Policies**
  - Note that the Policies option in the Organization Editor has two tabs: Agent Policies and NMS Policies.

Agent Policies:

Select the policy that to be assigned to the devices under your organization by default.

NMS Policies:

NMS policies help you map the policies to different rules for networking devices. Choose this tab to review default NMS policies for each network component that can be monitored via the Ninja NMS agent.
(see: **NMS: Device Roles and Policies**)



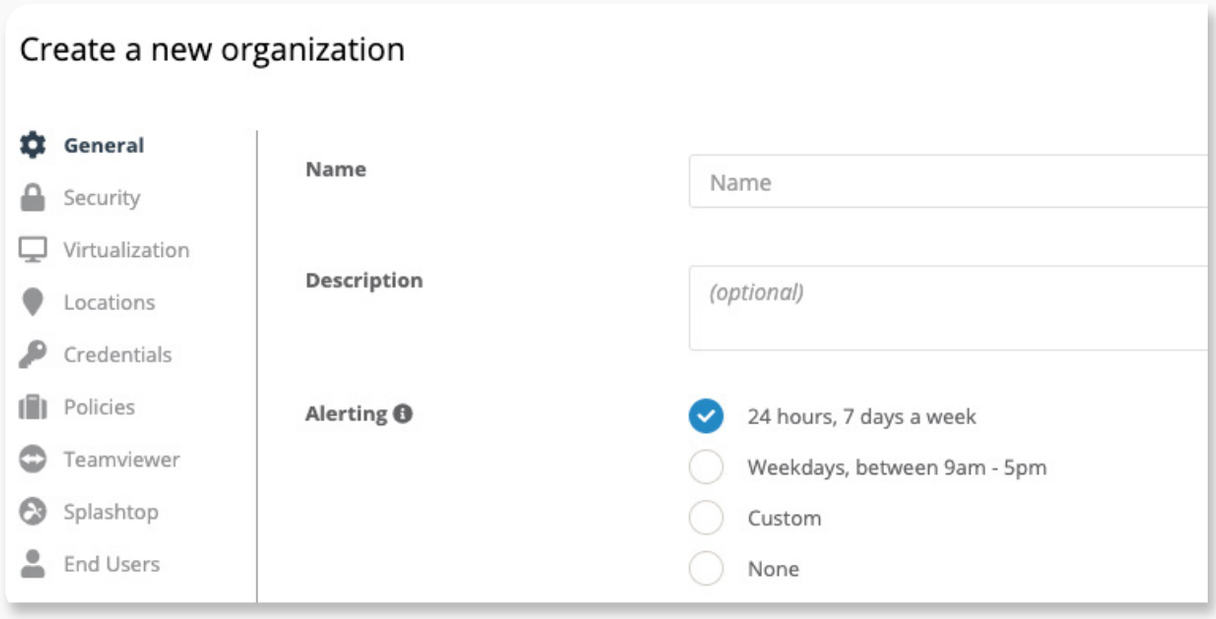
Important Note: Ninja automatically includes and assigns a default policy for Windows Workstation, Windows Server, and Mac. You can either edit these defaults or create new policies to meet the specific needs of this organization.

Organizations

- **Splashtop**
  - Splashtop is a remote connection tool, which features a lightweight agent and a highly secure encryption for screen sharing. (see: **Splashtop: Setup Guide**)
- **End Users**
  - Add and manage end users under the organization so that they can remotely access their devices. (see: **End User Sharing**)
- **Patching**
  - Add a WSUS server to use with OS patching for the organization. (see: Policies: Windows Patch Management)

3. Click **'Save'** in the top right corner and then close the organization editor to apply your settings.

> **Important Note:** Internal Infrastructure can now be edited or deleted as of the 5.2 release.



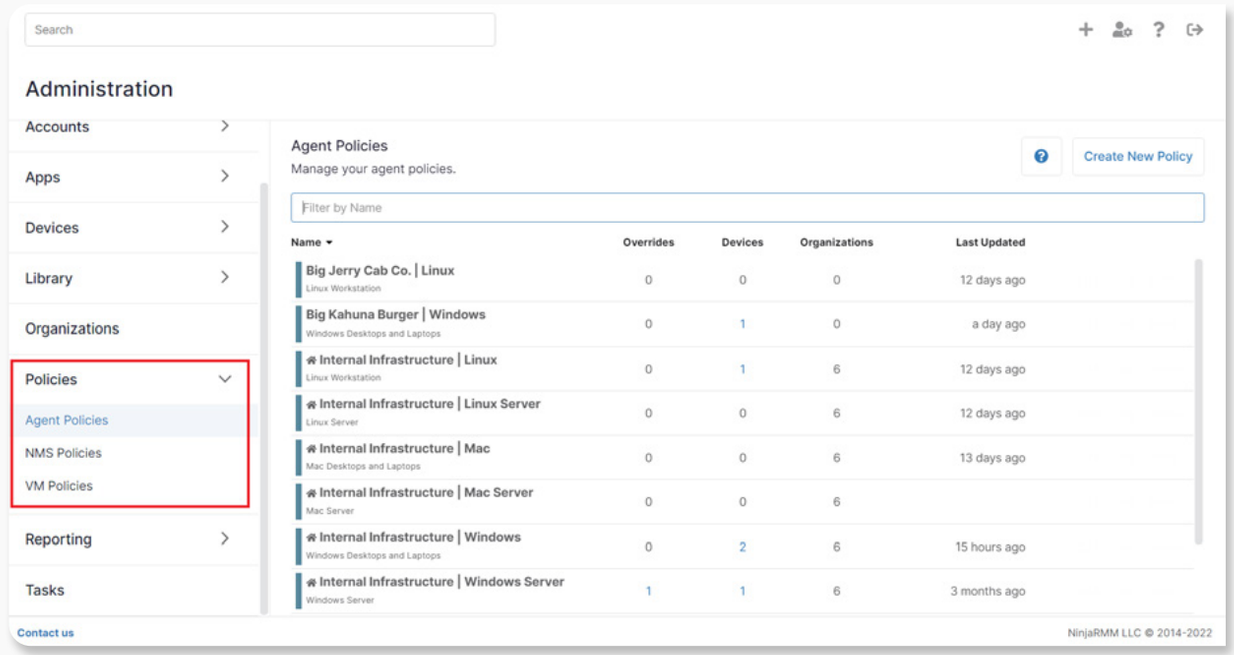
Important Note: The server must have Ninja installed in order to be available to select, and also must be under the organization in question (so, you will need to save the new organization and add devices to it prior to being able to configure the WSUS server).

Policies

Let's start off with an operational definition of a **Policy**: A **policy** is a set of conditions, scripts, and various settings like patching, remote access, and antivirus which can be collectively applied to a group of devices that are members of that policy.

Ninja provides a predefined list of default policies which include default condition monitoring. These default policies can be identified by the home symbol next to their names, which means that they are default and cannot be deleted. You can either edit the master policies or create brand new policies.

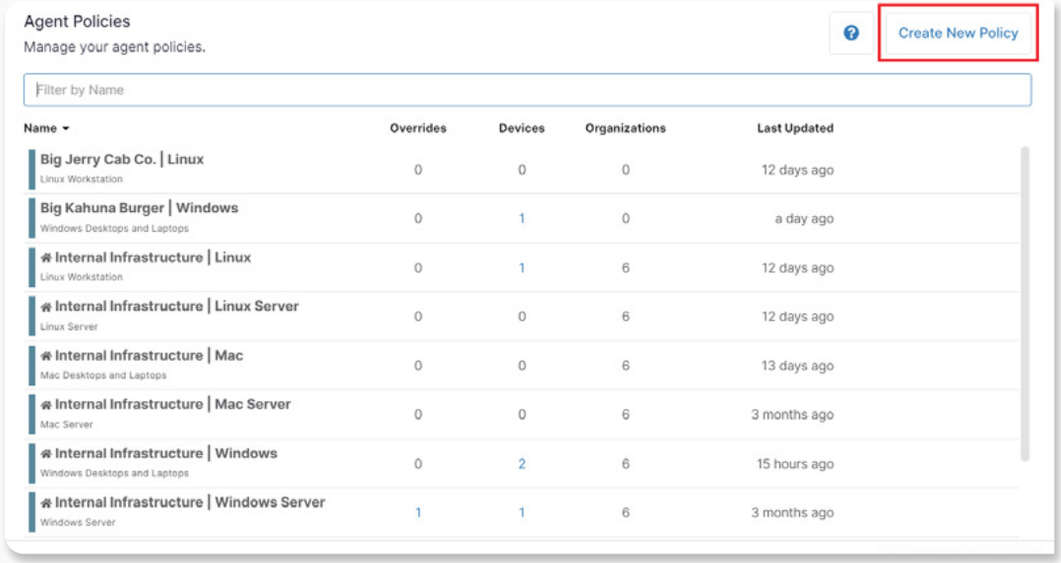
- **Agent Policies -** These policies govern devices which the Ninja agent is installed on and includes Windows, Mac, and Linux devices broken down by device type.
- **NMS Policies -** These policies govern your network devices including Firewalls, Dial Managers, Routers, and more.
- **VM Policies -** These policies govern Hyper-V and VMWare virtual machines and are broken down by Host and Guest policies.

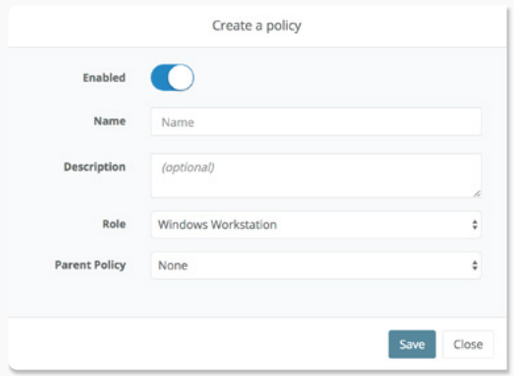


ninjaOne

Policies

1. Click '**Create New Policy**' in the top right corner.
2. Set up your policy shell.
   - **Toggle -** Enables/disables a policy. (Policy Conditions, Actions, and Antivirus settings will only be honored if the policy is enabled.)
   - **Name -** Set a name for your policy (i.e. "Workstation Policy - No AV")
   - **Description -** Enter a more robust description, if desired.
   - **Role -** Select one of the following roles for your policy:
     - Windows Desktops and Laptops
     - Windows Server
     - Mac Desktops and Laptops
     - Mac Server
     - Linux Desktops and Laptops
     - Linux Server
     - NMS
     - VMWare Virtual Machine Policy
     - VMWare Host Policy
   - **Parent Policy.** Using policy inheritance, you can make this a "child" of a "parent" policy. This means that the policy will follow all of the conditions, scheduled scripts, and other settings found in the parent policy, but will also include whatever changes/additions are made to this policy. This is helpful in situations where you want to set one master policy template that you can alter for specific client needs - without having to set the whole policy up from scratch. With the exception of any overrides, any change made to the parent policy will also populate down to children policies.





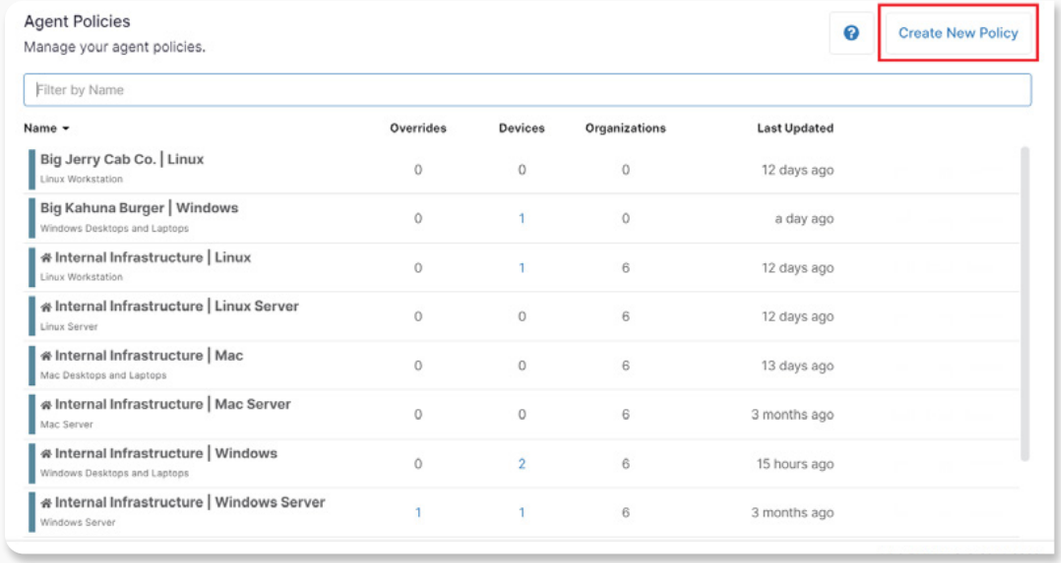
ninjaOne

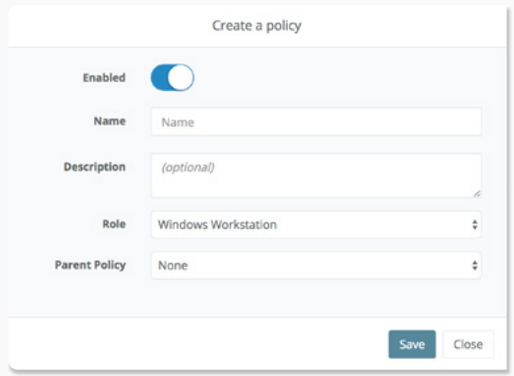
Policies

3. Once you click '**Save'**, the policy editor will automatically load. Note that several conditions are added to new policies by default. This is to ensure that bare-bones basic critical monitoring is happening for your customers out of the gate. You can add to, modify, or remove these conditions to meet your specific needs.

Please see the following documents for more granular details on each tab under the agent policy editor:

- Policies: Conditions
- Policies: Scheduled Scripts
- Policies: Windows Patch Management
- Integrated Antivirus: Webroot: Setup with a new account or Webroot: Setup with an existing account
- Integrated Antivirus: Bitdefender: Integration Guide
- Policies: 3rd Party Software Patch Management



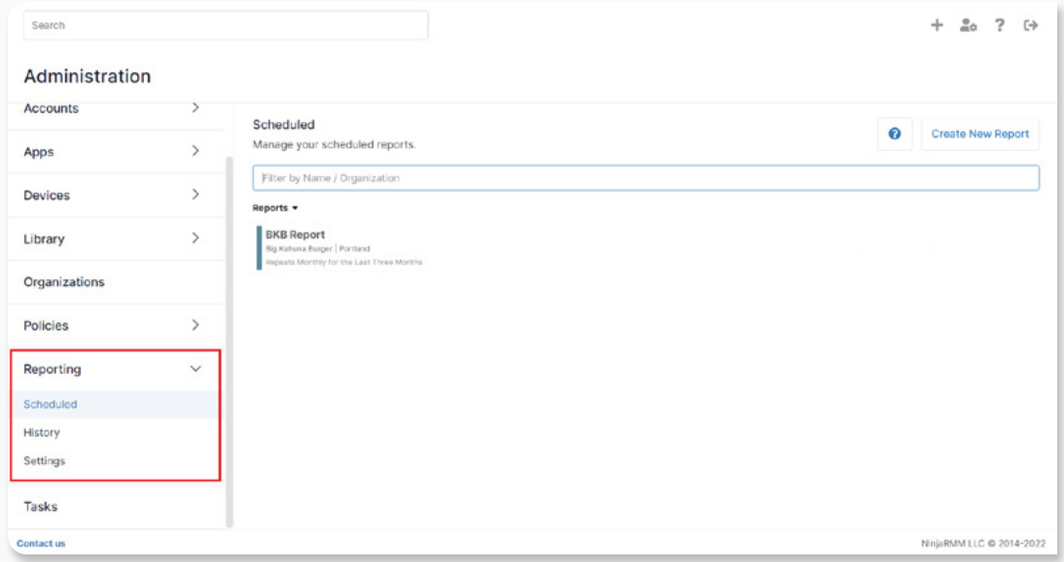


Reporting

The **Reporting** tab allows you to configure several out-of-box reports for your own and your customers' use.

- **Scheduled -** Allows you to create and schedule reports in Ninja. For more information about the different types of reports, please see Reporting: Types of Reports.
- **History -** This section allows you to view the history of run reports.
- **Settings -** This section allows you to set the reporting logo for your reports.

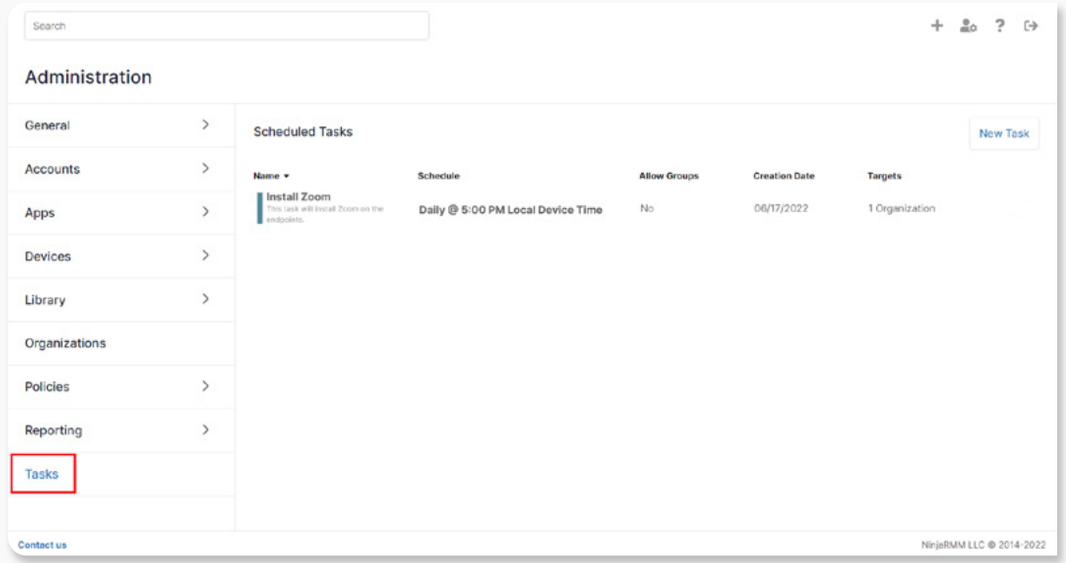
For more information about creating reports, please see **Reporting: Create and View Reports.**



Tasks

The **Tasks** tab allows you to create and manage scheduled tasks, wherein you may run scripts against a combination of devices, organizations, and/or groups.

For more information about **Scheduled Tasks**, please see our Scheduled Tasks documentation.



ninjaOne

ninjaOne