AUTOMOX

QUICK START GUIDE

PATCH MANAGEMENT IN MINUTES WITH AUTOMOX

Tips for getting started

You can be up and running using Automox patching policies in less than 30 minutes. Check out our step-by-step instructions to get you patching devices in no time.

Browse our how-to videos and product demos at atmx.io/how-to-videos for a walkthrough on the various things you can do in Automox. Or, feel free to browse our user documentation by clicking **Help** in the upper right corner of the product console. Or, clicking our chat icon in the lower right corner of the product console to connect with a support representative.

If you have any issues or would like to connect directly with an Automox expert, contact support@automox.com. We're happy to guide you through some best practices for your patching and endpoint hardening needs.

STEP-BY-STEP: AUTOMOX PATCH MANAGEMENT IN MINUTES

01. Add devices

02. Group devices

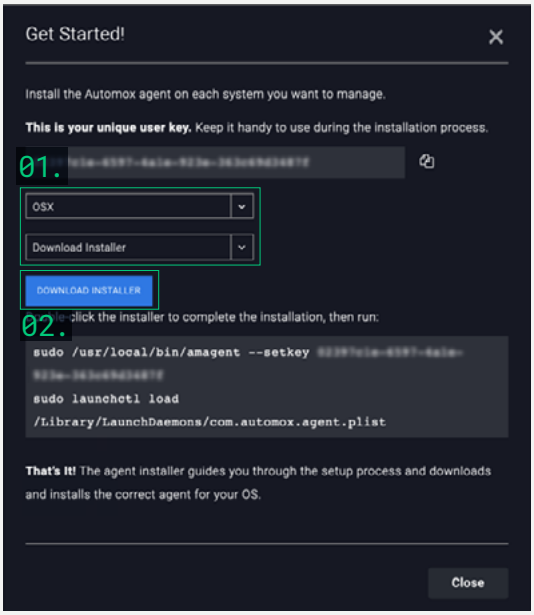
03. Create policies

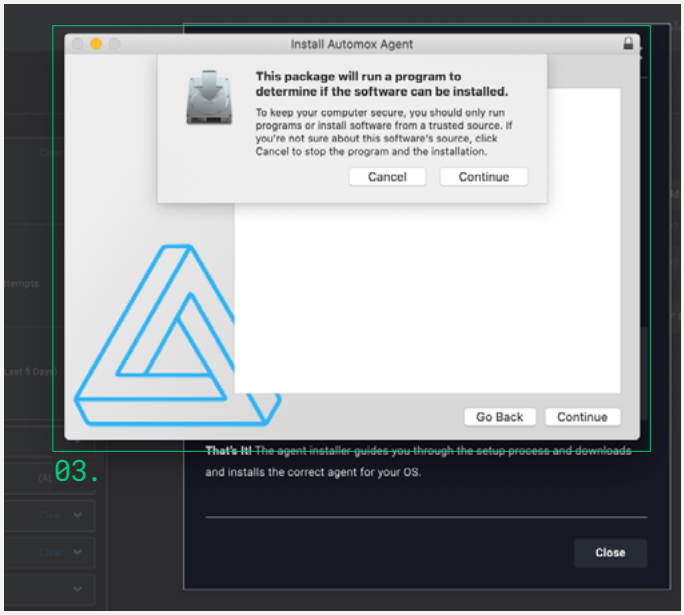
04. Scan devices

Step 1: Add devices

Before you can use the Automox console to manage devices in your organization, you need to install the Automox agent. You can download and install a single agent for all of your Windows, macOS, and Linux systems. At under 20MB, the Automox agent is highly efficient with low I/O and CPU overhead. A persistent encrypted session with the Automox cloud securely manages your device. To install the Automox agent and add your devices:

Go to **Devices > Add Devices**.





01.

Select your OS and choose **Installer**.

02.

Download the installer file.

03.

Open the installer file to complete agent installation.

You can install the agent through an onboarding wizard. After adding your devices, Automox inventories all hardware, software, patches, and configuration details — which is visible from the **Devices** page. You can continue adding devices right from the dashboard.

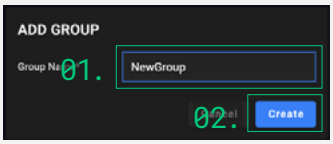
WANT TO DO MORE?

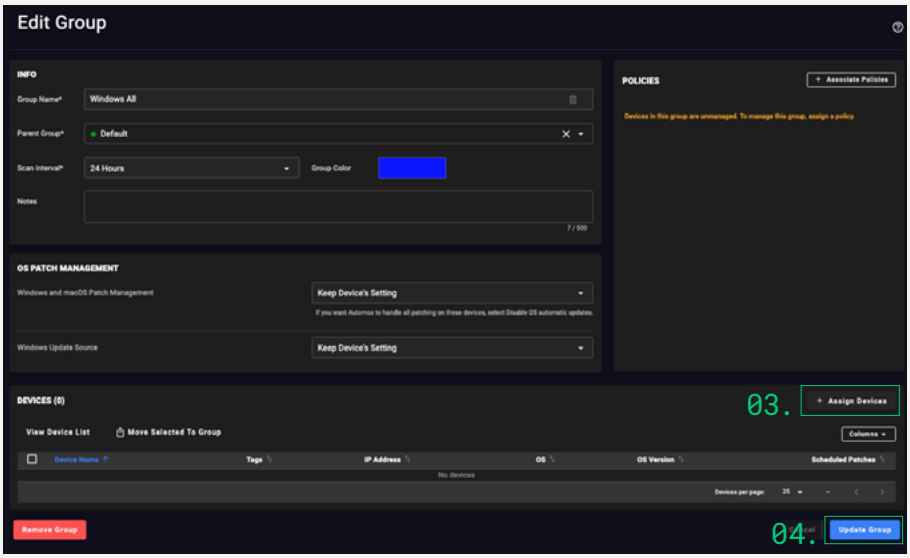
We have multiple methods to install our agent in bulk across multiple domains or servers. You can read more about bulk deployment and other product use cases in our user documentation, accessible by clicking **Help** in the upper right corner of our console.

Step 2: Group your devices

Automox Groups enable you to segment your organization and simplify management. Whether you sort your devices by department, OS, or region, groups simplify the management of your security infrastructure. Do the following to add a group, and assign devices:

Go to **Devices > Create Group**.





01.

Enter **Group Name**.

02.

Click **Create.**

03.

Click **Assign Devices**.

04.

Click **Update Group**.

Enter a **Group Name** for your new group and click **Create**. In the Edit Group screen, click **Assign Devices** to assign the devices to the group. You can accept all other defaults for your new group. Click **Update Group** to save your group settings. Once you create more than one group, you can look at the options that help you identify groups for easier management. And, as you become more familiar with our product you can choose to customize your group settings.

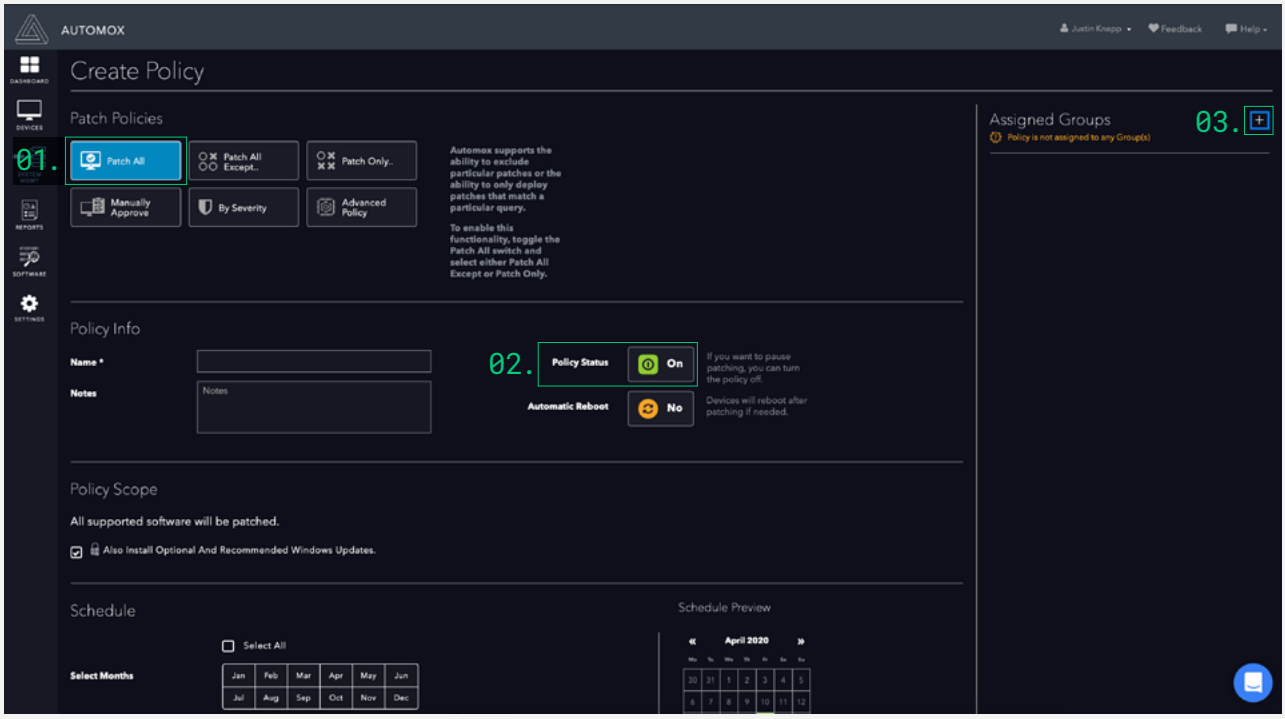
WANT TO DO MORE?

Consider how you want to group and segment your devices for patching and endpoint hardening. You can create and assign policies to one group or multiple groups, and you also can choose to create sub-groups under a **Parent Group** for easier management.

Step 3: Create a policy

Policies automate cyber hygiene, helping you patch systems, ensure the right software is installed, and maintain configurations. You can create policies once and assign them to multiple groups of devices, quickly update policies for every device without the need to touch code or hardware, create one policy to manage a mix of Windows, macOS, and Linux devices. To get you started, let's create a **Patch All** policy:

Go to **System Management > Create Policy > Patch All.**



01.

Select **Patch All**.

02.

Set **Policy Status** to **On**.

03.

Add **Assigned Groups**.

Enter a **Name** for your new Policy and toggle the **Policy Status** to "On." This enables patching. You can accept all other defaults for your new policy. Before saving the policy, assign a group by clicking the plus sign in the **Assigned Groups** section.

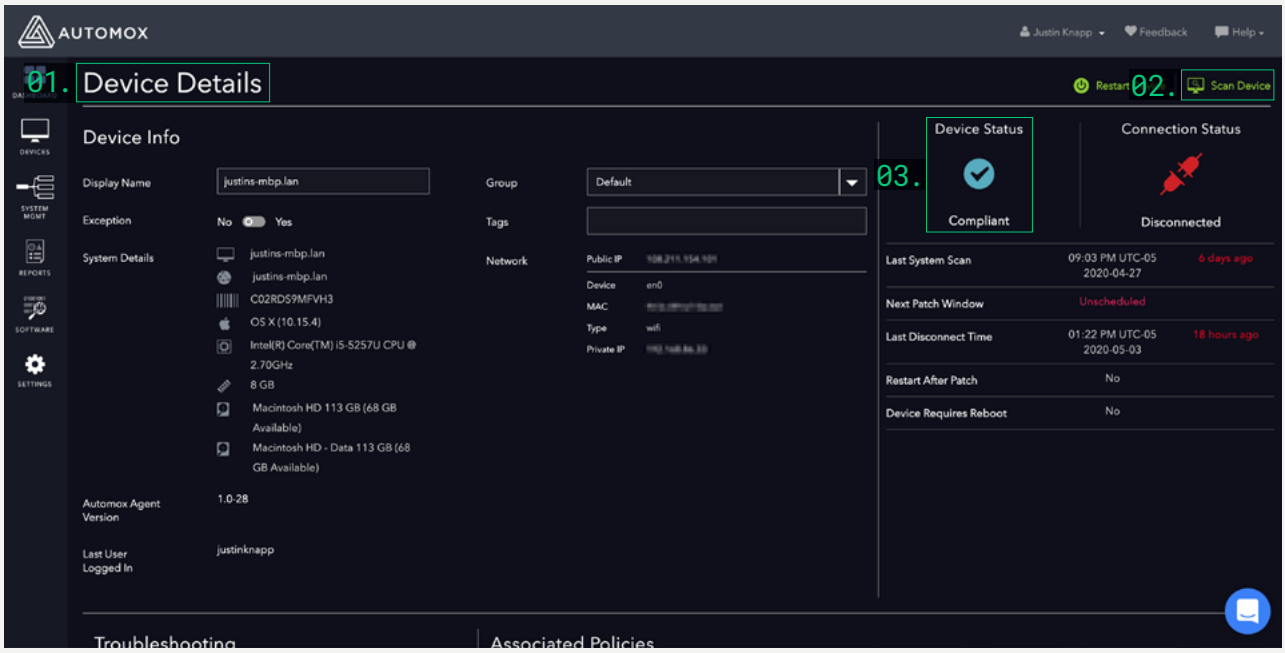
WANT TO DO MORE?

You can choose to configure the other policy settings at a later time — such as for automatic reboot, scheduling, and user notifications. These settings are not required for this quick start configuration, but key to how you want to manage your devices long term based on your patching requirements.

Step 4: Scan devices and run policies, as needed

Now that you've added your devices and assigned a policy to your specific group, let's manually scan your devices to determine their patching status.

Go to **Devices > [Your Named Device] > Scan Device.**



01.

From **Devices** view, select and open your **Device Details**.

02.

Click **Scan Device** to determine if compliant with policy.

03.

The **Device Status** displays if compliant with all policies.

After scanning: if your device status is non-compliant with the latest patches, a **Needs Attention** status displays. If your device status is compliant, then you're all set.

Under Associated Policies, you can choose to run a policy to put your devices in compliance with the latest patch updates. Click **Run On This Device** next to the associated policy.

WANT TO DO MORE?

You can customize the device scan interval to between 6–24 hours. You pick how frequently or infrequently you'd like Automox to scan the status of your devices. Be sure you check back regularly to see how your device statuses may have changed.

There's so much more you can do in Automox

You've got the basics covered. Pretty simple, right? Here's a quick list of what more you can do to realize how Automox can make patching and endpoint hardening easier:

Get familiar with the Automox dashboard.
Our dashboard view provides full visibility into the statuses of your devices, allowing you to quickly identify misconfigured systems, missing patches, or compliance issues.

Check for a software version in your application inventory.
Because Automox provides access and visibility of all your endpoints, you can confirm that they are running the latest version of a specific software to keep them better protected and secure from known vulnerabilities.

Add more devices and begin grouping them according to your patch management policies or organizational architecture.
For example, group by department, OS, or region. The ability to group your devices allows you to enforce specific policies according to these groupings.

Set a password policy across your available devices using an Automox Worklet.
We've leveraged cyber hygiene best practices to create a worklet that lets you enforce these password policies across your corporate endpoints: see Automox Worklet - Set Password Policies to create and run this worklet in your environment. You can learn more about Automox Worklets at: automox.com/use-cases/worklet.

Manage your Automox subscription

Go to the **Settings** page in the Automox console, navigate to the **Billing** page, and **pick the plan** that works best for you. You can view more information about plan pricing at: automox.com/pricing.

If you prefer, feel free to connect directly with your Automox sales representative to discuss the available subscriptions and discuss the best plan for you. You also can connect with Automox Sales at: sales@automox.com.