SRC CYBER SOLUTIONS LLP
CYBER RISK SOLUTIONS

AUTOMOX

QUICK START GUIDE

# Endpoint Management in Minutes With Automox

## TIPS FOR GETTING STARTED

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

**Browse our how-to videos and product demos** 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, click 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 management needs.

## STEP-BY-STEP: AUTOMOX ENDPOINT MANAGEMENT IN MINUTES

1 // Add devices.

2 // Group devices.

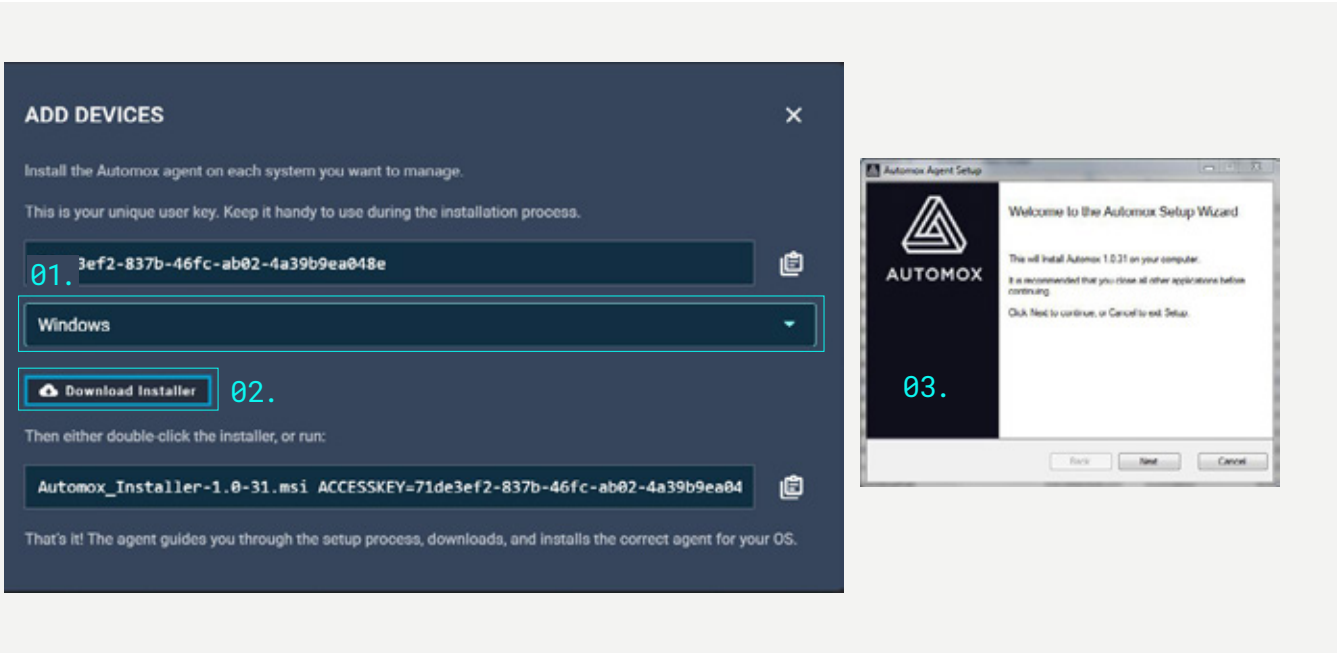
3 // Create policies.

4 // 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 your Microsoft® Windows®, macOS®, and Linux® systems. At under 10MB, 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**.




1 // Select your OS and choose **Installer.**

2 // Download the installer file.

3 // Open the installer file to begin the agent installation. You will need the unique user key to complete.

The Automox agent is installed using an easy-to-use 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.

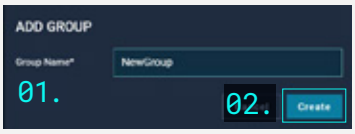
### Want to do more?

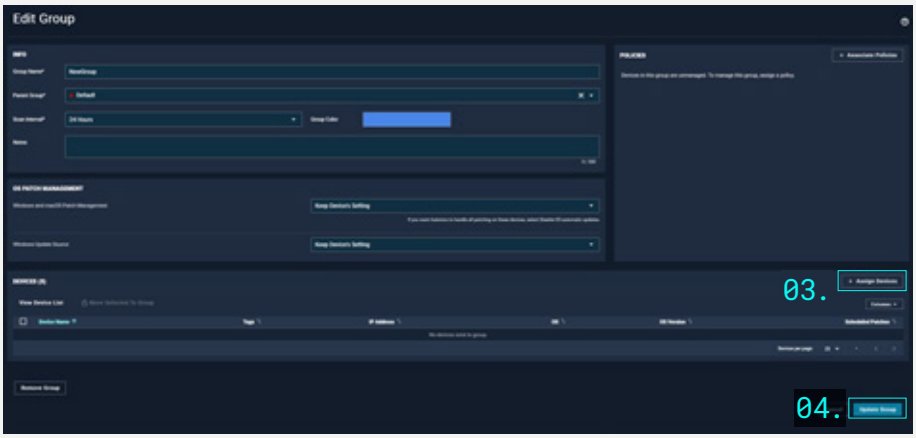
There are several methods to install our agent in bulk across multiple domains or servers. You can read more about bulk deployment and other product use cases in our Knowledge Base, accessible by clicking **the Question Mark icon** in the upper right corner of our console.

## STEP 2: GROUP YOUR DEVICES

Automox Groups enable you to segment your organization and simplify management. Whether you sort your devices by department, operating system, 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**.




1 // Enter **Group Name.** 2 // Click **Create.** 3 // Click **Assign Devices.** 4 // 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 the Automox solution, you can choose to customize your group settings.

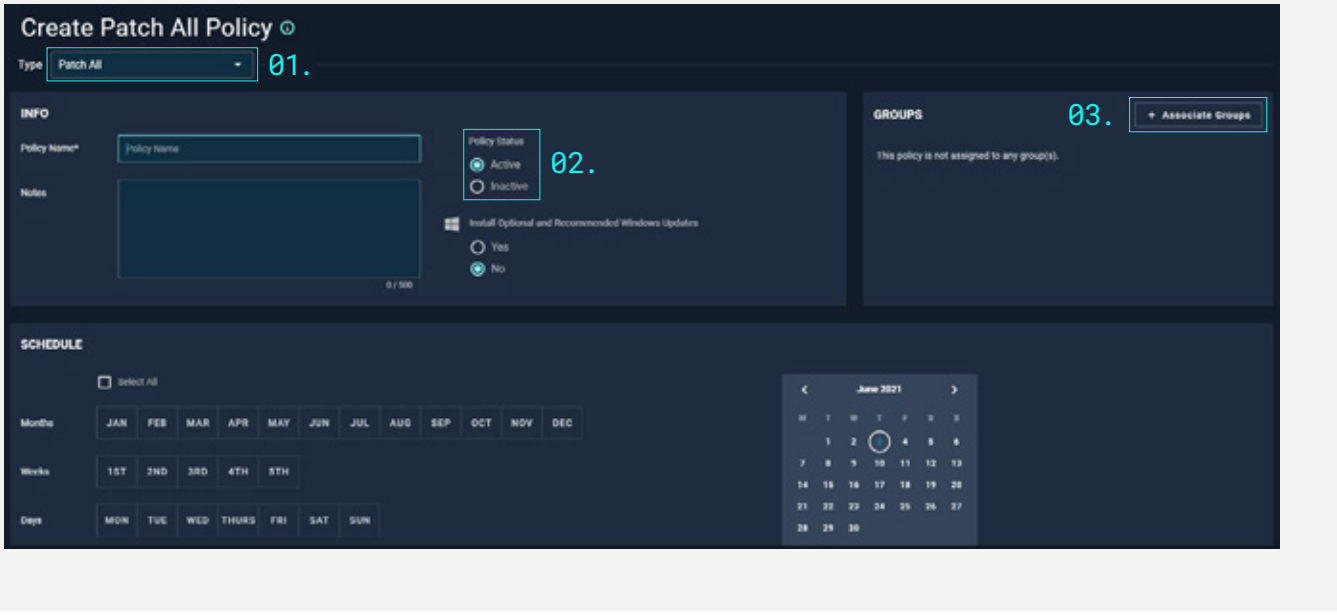
### Want to do more?

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, or create one policy to manage a mix of Microsoft Windows, macOS, and Linux devices. To get you started, let's create a **Patch All** policy:

Go to **Manage > Policies > Create Policy**.




1 // Select **Patch All.**

2 // Set **Policy Status to Active.**

3 // Add **Associate Groups.**

Click **Patch**, then **All**, then click **Next** on the lower right. Enter a **Name** for your new policy and set the **Policy Status** to "Active." 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 **Associate Groups** section in the upper right.

Scroll down to the bottom of the page past the "Deferral Settings" section and click on "Create Policy" to finalize.

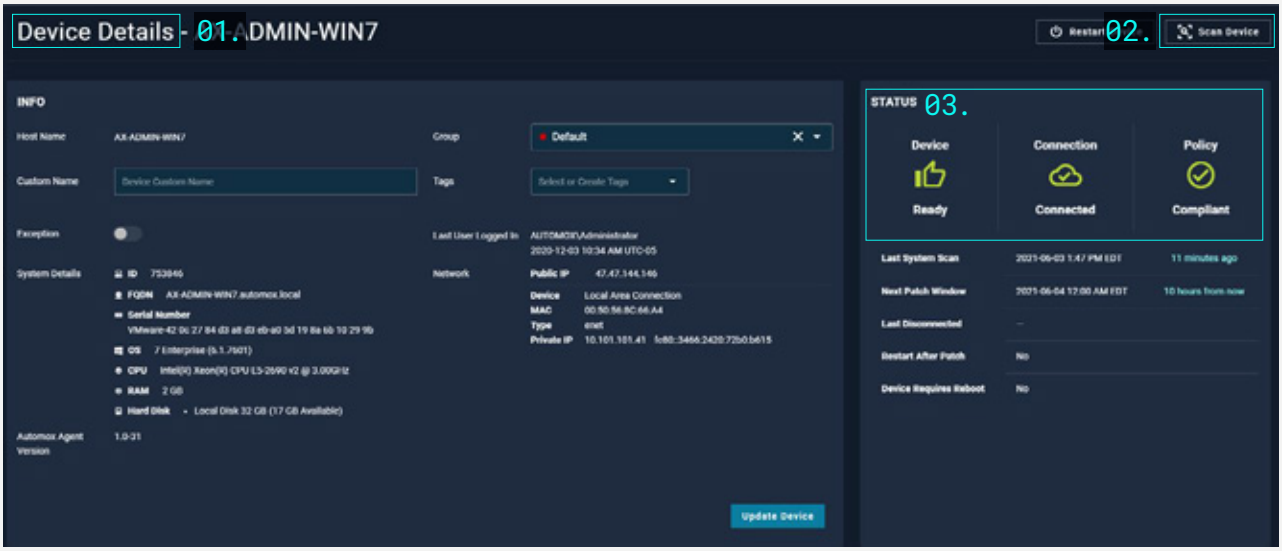
### Want to do more?

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




1 // From **Devices** view, select a device to open your **Device Details**.

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

3 // 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 the **Associated Policies** section, 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 would like Automox to scan the status of your devices. Be sure you check back regularly to see how your device statuses may have changed.

SRC CYBER SOLUTIONS LLP
CYBER RISK SOLUTIONS

AUTOMOX

## 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 management easier:

### Get familiar with the Automox dashboard.

Our dashboard view provides full visibility into the status 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, operating system, or region. The ability to group your devices allows you to enforce specific policies according to your business needs.

### Set a password policy across your available devices using an Automox Worklet™

We've leveraged cybersecurity best practices to create a Worklet that lets you enforce these password policies across your 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**.

## ABOUT SRC CYBER SOLUTIONS LLP

**At SRC Cyber Solutions LLP, we provide Next Generation, Automated and User-Friendly solutions in partnership with AUTOMOX for Patch and Endpoint Management, IRONSCALES for Comprehensive Email Security and Anti-Phishing Protection, THREATX for WAAP (WAF++) with an Attack-Centric approach for Web Application and API protection and Project Ares for Online Gamified Simulation-based Cyber Security Training.**

For additional information, please contact
sales@srccybersolutions.com

+91 120 232 0960 / 1

www.srccybersolutions.com