



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.

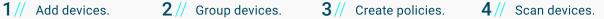


Browse our how-to videos and product demos for a walkthrough on the various things you can do in Automox. Or feel free to browse our user documentation by clicking **Help** in the upper right corner of the product console. Or, click our chat icon in the lower right corner of the product console to connect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











user key to complete.

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.

ADD DEVICES		×	
istall the Automox agent on each system you want to	o manage.		🚺 Automox Agent Setup
his is your unique user key. Keep it handy to use duri	ng the installation process.	_	Welcome to the Automox Setup Wizard
01. ^{3ef2-837b-46fc-ab02-4a39b9ea048e}		Ê	AUTOMOX Is incommended that you close all other applications before
Windows		•	Continuing Club Next to continue, or Cancel to exit Setur.
			0.2
▲ Download Installer 02.			03.
Then either double-click the installer, or run:			first Net Creat
Automox_Installer-1.0-31.msi ACCESSKE	Y=71de3ef2-837b-46fc-ab02-4a39b9ea04	Ē	
	ess, downloads, and installs the correct agent for	your OS.	
	ess, downloads, and installs the correct agent for	your OS.	
	ess, downloads, and installs the correct agent for	your OS.	
	ess, downloads, and installs the correct agent for	your OS.	
	ess, downloads, and installs the correct agent for	your OS.	
That's it! The agent guides you through the setup proc		your OS.	2// Open the installer file to
That's it! The agent guides you through the setup proc 1 // Select your OS and choose Installer.	ess, downloads, and installs the correct agent for $2//$ Download the installer file.	your OS.	3 // Open the installer file to begin the agent installation

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.

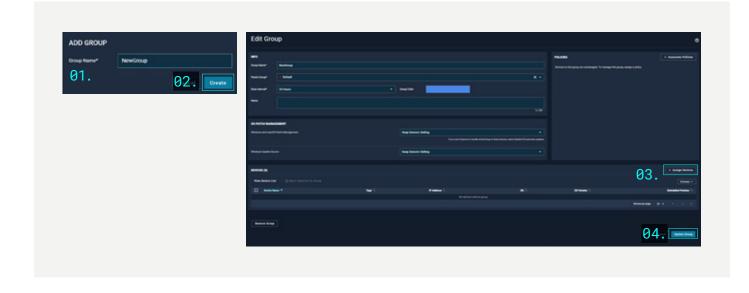




STEP 2: GROUP YOUR DEVICES

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.

					01																		
INFO																GROU	JPS				03.	+ A5	sociate Group
Policy Name*	4	ilcy Nam	•								Active	02	2.			This p	olicy is r	ut ensig	ned to any gr	oup(1).			
Notes										0	Inactive												
									1	-	ell Optione Yes	f and Roco	enmonded Windows Upde	Acra									
								0/500			No												
SCHEDULE																							
	🗆 sele															June 2021							
Months	JAN	FEB	MAR	APR	MAY	JUN	JUL	AUG	50P	00	T NOV	DEC				-							
		2ND	380	ATH	STH											0	4 8 11 12						
Webs	157																						

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.

INFO					STATUS 03.		
Host Name	AX-ADMIN-WIN/	Group	e Default	× •	Device	Connection	Policy
					цС	Ø	\oslash
Custom Name	Device Custom Name	Taga	Relet or Greate Tags				~
					Ready	Connected	Compliant
Exception	•	Last User Logged in	AUTOMOTIVAdministrator 2020-12-03 10:34 AM UTC-05				
System Details	a 10 753545	Network	Public IP 47.47.344.346		Last System Scan	2021-06-03 1:47 PM LDT	11 minutes ago
	FON AX-ADMIN-WIN7 automox.local		Device Local Area Connection		Next Patch Window	2021-06-04 12:00 AM EDT	10 hours from now
	 Serial Number VMware-42 Dt 27 84 d3 a5 d3 eb-a0 3d 19 8a 6b 10 29 9b 		MAC 00.50.56.8C.66.A4 Type ent		Last Disconnected		
	06 7 Enterprise (5.1.7501)		Private IP 10.101.101.41 (c80-3466.2420.7250.5615				
	• CPU Http:/// Xeon/H) CPU L5-2690 v2 (# 3.00GHz				Destart After Putch		
	• RAM 200				Device Requires Reboot	N0	
	Hard Disk - Local Disk 32 GB (17 GB Available)						
Automox Agent Version	1.931						

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.





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 7 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 NexGen, Highly Automated and User-Friendly solutions in partnership with IRONSCALES with the POWER OF NOW for Comprehensive NexGen Email Security, THREATX for NexGenWAAP (WAFF++) with an Attack-Centric approach and Cyber Security Training with Project Ares by CIRCADENCE CORPORATION for Online Simulation based Cyber Security Training.

You can view more information about plan pricing at : https://srccybersolutions.com/contact-us





For additional information, go to sales@srccybersolutions.com

+91 120 232 0960 / 1

www.srccybersolutions.com