Onboarding Jumpstart Guide - Manage Your Environment

Overview

As you begin to organize your new Automox account and zones, understanding what is available, and having access to best practices will help you to define your group structure and configure standards within the Automox console.

Each company account has its own unique challenges, and there is no one-plan-fits-all solution. This guide is designed to provide you with resources and recommendations to help you define the best use of Automox for your company.

Automox Documentation

Automox has created content in several different formats. Here are the primary links to find that information and documentation:

- Automox Home: Automated Patch Management + Better Cyber Hygiene
- Automox Community: Community for Automox customers
- Documentation Help Center: https://support.automox.com/
- API: Automox API Reference Guide
- Blog: The Automox Blog
- How-to Videos: Automox Videos
- Quick Start Guide: Learn the Basics in Minutes

Console Overview

The console is your primary user interface to interact with Automox. Hopefully you have had an opportunity to explore the console during your trial and initial setup. Due to the intuitive and ease of use of the console's design, this section provides resources for additional information and detail rather than a detailed walkthrough.

Link to console: Console

Dashboard

This is your landing page in the console. You will find an overview of your environment and links to actions you may be interested in to manage your zone. Automox Console Dashboard

Devices

- Device Filter Panel: Search, sort, and filter devices
- Device Details and Status
- What the Statuses Found in the Automox Console Mean

- Managing Devices: Manage group placement, view/export inventory, scan/reboot/remove devices
- Software Inventory
- Automox Compliance

Manage

This is where groups and policies are managed. (These topics are discussed again later in the document and/or document series.)

Reports

Overview of reports and how to export data from the console: Automox Reports

Software

This section provides topics with tips and links related to the Software page.

Filtering and Searching

- Filtering and Searching on the Software Page

Exclusions/blocklist

- Adding Patches to the Block List in the Automox Console

> **Tip:**
> Some columns contain drill-down links or additional information when you click on them. As an example, some items in the **Severity** column are blue. If you click on them, a related CVE number appears.
> If you click on the blue number under the **Impacted** or **Updated** column, you are presented with a list of devices that have available updates or have already applied that patch. You can export these lists.

Software Info

- We scan for software listed here in addition to a few unique paths for the third-party software supported by Automox (for example: Zoom, OneDrive)
- **macOS**
  - /Applications/*.app
  - /Applications/**/*.app
  - /System/Applications/*.app
  - /System/Applications/**/*.app
- **Windows**
  - HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall*
  - HKEY_LOCAL_MACHINE\Software\wow6432node\Microsoft\Windows\CurrentVersion\Uninstall*.
  - Program Files

    - Program Files (x86)
- **Linux**

  Query the package manager using the appropriate language for OS.

    - dnf/yum
    - Aptitude
    - zypper

Settings

- Settings Overview
    - **Profile:** Manage your user information, password, and notifications (email or Slack)

      Tip: If you forget your password, you can reset it from the console login page. Type in your email address and you will see a link to reset your password by entering your email address. Link: https://console.automox.com/forgot-password
    - **User Accounts and Roles**
    - **Keys - API:** see Managing Keys.

      Tip: API key access rights are based on the account the key is created for. It allows the same rights as the user assigned role. You can limit the available actions an API key can make by generating a key for a user assigned the appropriate role. As an example, use a key generated for a read-only user to collect report details. This key does not allow the user to make changes in the environment.
      Tip: You can only create a new API key for yourself. Zone Administrators can manage existing keys for their zone(s).

    - **Security:** Two-factor Authentication, Define Login Attempts, SAML, and Enforce Zone-Wide Two-factor Authentication **Setting up SAML for multiple zones SSO**

Tip: Request Automox support from within the console. You can access support by clicking **Contact Support** in the lower-right corner. From here you can start a support request live. Responses are interactive, and are forwarded to email should you log off or close the console.
In the upper-right corner of the console you can also click the **?** to view resources such as our Help Center and Community.

Agents

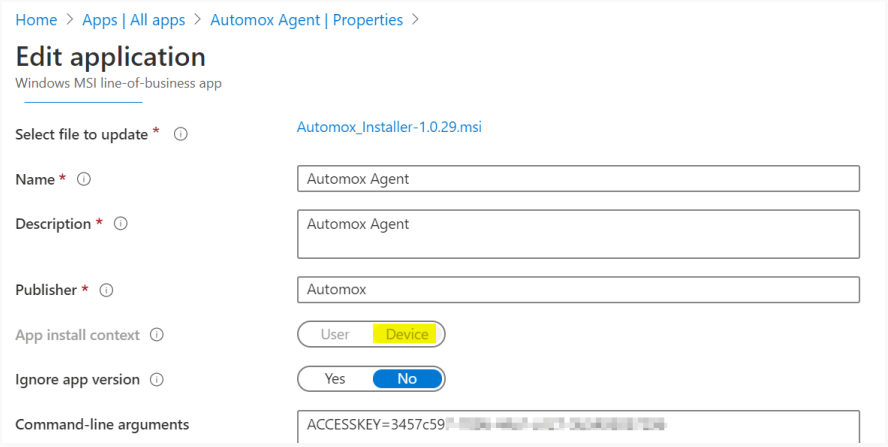
Managing your devices from the cloud is pretty amazing. It also comes with a few considerations when moving from traditional on-premise solutions. You will need a plan to deploy your agents if your clients are dispersed. It is also a good time to ensure your environment is set up for success. Follow the information here to ensure your devices can connect to the needed internet points, so

that the Automox agent can do its job efficiently.

TL;DR
Ensure that your devices can reach the Internet and devise a plan to get your agents deployed. Ensure that your devices are manageable and that your current security tools allow Automox to do what it needs to do.

System Requirements	Automox Agent Requirements Windows • The built-in Windows Update Agent\Service must be healthy and enabled. • .NET Framework 3.5 or later • PowerShell 2.0 or later • x86 and x64 based processor (ARM processors not yet supported)
	• EPP Application Control - Globally Trust-listing Automox • Local Agent and Log directories are useful for configuring antivirus rules. See Location of Files Required By Automox **Tip**: To ensure uninterrupted functionality, please consider if EPP (endpoint protection platform)/antivirus rules are required in your environment. • Customize Script Execution Location: This is useful if you need to control where processes run on your devices. Change Automox Script Execution Location • Update Sources: Each managed device requires access to all update sources when scans and policies run. Notable update sources are: ◦ Windows Update sites ◦ WSUS (if used in your environment) ◦ See list of Internet URLs in the Miscellaneous > Important URLs section at the end of this document for a more detailed list of URLs to allow access. • Firewall considerations: **Tip:** ◦ All managed systems require access (and potential defined routing) to api.automox.com* port 443 ◦ IP addresses for the API change often and dynamically. If an IP address list is required by your company, the following article provides a suggestion about how to identify the current list. Make sure to keep firewall exceptions up-to-date.

Environmental Considerations	◦ Uploaded content for Required Applications or Worklets is stored in Amazon s3. A rule should be configured to allow access to automox-policy-files.s3.us-west-2.amazonaws.com* See Agent Firewall Allowlisting Rules • Important URLs • Proxy and routing **Tip**: Starting with agent version 29, Windows automatically identifies proxy settings if they are set per the current user or set for the system. **Tip**: Devices behind a proxy may need a route to be configured (for example, pac file or proxy application permissions). Add routing, if needed. • Ubuntu and CentOS (Debian and YUM) Proxy configuration Adjust `/etc/init.d/amagent` daemon by adding the following settings if missing just after the variable definitions: # PATH should only include `/usr/*` if it runs after the mountnfs.sh script PATH=/sbin:/usr/sbin:/bin:/usr/bin DESC="Automox agent" NAME=amagent DAEMON=/opt/amagent/amagent DAEMON_ARGS="" PIDFILE=/var/run/$NAME.pid # Proxy settings export HTTP_PROXY="Proxy server" export HTTPS_PROXY="PROXY server" # Exit if the package is not installed [-x "$DAEMON"] || exit 0
	Where to find the agent: Download Links for the Latest Automox Installers Installation Methods: Here are several examples including manual installation, bulk deployments, group policies, and use of automation tools to get your agents deployed. • Bulk agent installation options (includes command lines for each OS): Deploying the Automox Agent in Bulk • GPO options: Deploying the Automox Agent Using Windows GPO - for Remote Users Deploying the Automox Agent Using Windows GPO • Windows installation tips: Modify the MSI to include your access key Embedding Your Access Key into the Automox MSI Windows silent install switches

Agent Installation	Silent Agent Deployment on Windows • Linux: Installing the Automox Agent on Linux • Intune: Example of how to configure a msi line-of-business app 
Agent: Various topics	• Move device to another zone: Moving Devices From One Zone to Another • Remove agents: Removing the Agent Using the Console (Recommended) Manual agent removal instructions in article above (best practice, remove from console) • Gold Image: Best Practices **Tip**: If you apply your image with a step-by-step or scripted process, consider disabling the Automox agent in your image and later enabling it in your deployment process when you are ready for Automox to become active.
Troubleshooting	Agent Initialization • Cert (Unknown Authority): Agent Error: x.509 Certificate Signed By Unknown Authority • macOS: Troubleshooting the Automox Agent Installation on macOS Tips for troubleshooting agent installation: • See Location of Files Required By Automox. The amagent.log can be reviewed to help identify a cause for agent initialization issues. • Check the Device Status, Connection Status and the Troubleshooting section of the device details in the console. This can help detect issues with the following: Connection to the API, identify if a reboot is

	needed, identify low disk space (less than 3 GB), and if patch source is unreachable. • If you deregister an agent manually, ensure you do it as an administrator. If you run it without administrator rights, it can orphan the agent certificate.

Groups

It is possible to arrange groups by department, geography, or whatever makes sense for your zone. You can use groups to efficiently manage patching, required software, and Worklet policies across your devices. You also use groups to define scan interval, and OS Patch Management configurations. Refer to the following:

- Group Management Overview
- Searching and Filtering for an Individual Policy or Group
- Here are some helpful group management tips:
    - This is a prime opportunity for you to simplify your administration tasks by applying a functional group structure. Groups can be based on OS, Test/Production, or a business case such as zone administration or location and department.
    - Parent groups are for organizational purposes ONLY.
    - Policies are not inherited based on group hierarchy/structure. Policies must be directly assigned to each group where you want it to be applied.
    - Use a predetermined naming convention for your groups and policies to get quick views of relevant objects. If you search for Worklet, Patch, or Required in the policies filter, it will filter to that type of policy.
    - You can use the Windows PowerShell bulk installer script to automatically add devices to a specific group at agent installation time.

Scan

Scans evaluate the status of your device and return hardware, software, and patch inventory. A scan returns the compliance state for Patch, Required Software, and Worklet policies assigned to the group. Scans also check if a reboot is needed.

Scan Interval

- You can set the scan interval per group from 6-24 hours (default is 24 hours).

- Groups - Best Practices

Define your scan interval

- In most cases, setting the scan interval to 24 hours is ideal. This will return policy compliance and inventory 1 time per day.
- If you are onboarding and bringing your devices up to a current patch compliance state, you might want to shorten the scan interval temporarily for a current group-level compliance view.

- Automox best practice:
  - Scan Interval - 24 hours*

    * If you have a reason to shorten the time, then set this based on your needs.

> **Note**: A scan runs after each policy runs.

Set your OS Patch Management Settings

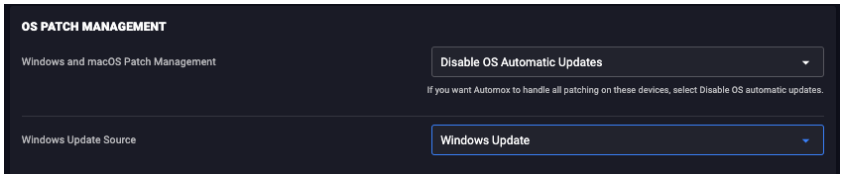
The OS Patch Management settings are key in controlling your patching process. Take a moment to consider these settings and configure them appropriately. This is one of the Automox configurations that may help shape your group structure. See OS Patch Management Settings for Groups.

Automox best practice

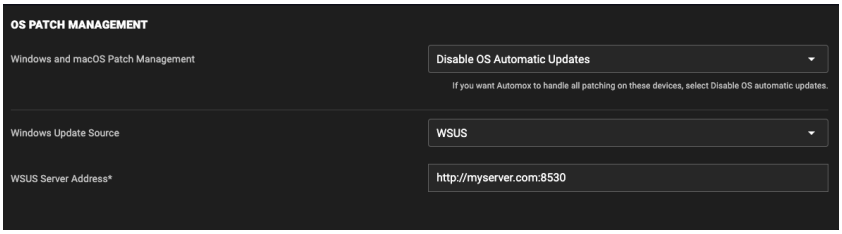
- **Windows and macOS Patch Management - Disable OS automatic updates**

  This option will prevent the device from automatically installing updates outside of your defined patch policies. Your patch policy defines when the device will pull updates from Microsoft Updates (or WSUS) and what patches to install.
- **Windows Update Source - Windows Update - or - WSUS**
  - **If the devices in this group will not download content from a local WSUS server, set this to Windows Update.**

    > **Note**: This is the Automox Best Practice

  - If the devices in this group leverage a local WSUS server, set this to WSUS and enter your WSUS server address (for example, http://myserver.com:8530).



Manage non-Automox patch configurations

- GPOs - Remove settings or set to “Not Configured”
    - Behavior: Automox applies OS Patch Management settings when a scan runs. GPOs will apply based on the policy refresh settings (default every 90 minutes). If they are set differently, your device WU agent might toggle patch source and potentially download content at unexpected times.
    - Allow Automox to manage the WU settings when you are managing patching through Automox.
- **Default Group**

  All new devices are assigned the Default group. Defining the settings and policies targeting the Default group can add to your device management strategy. Here are a few concepts for the Default group configuration.

  > **Note**: Policy overview and best practices provided in the Worklet and Patching Jumpstart guides.

  #### Scenario 1 - Soft Landing

  Intent - Get the agent installed, but don’t enforce any changes until the device is moved to its proper management group.

  Suggested settings: OS Patch Management

    - Windows and macOS Patch Management - Keep Device’s Setting
    - Windows Update Source - Keep Device’s Setting

- Policy Assignment: None

  Outcome: When the agent initializes and the object is added to the Default group, the device settings remain unmanaged. The devices can then be moved into another group, which will define the patch setting and become managed based on the policies assigned to the new group.

  #### Scenario 2 - Standardize

Intent - Bring devices to a known standardized state as the devices are added to Automox management. This is ideal for a managed new computer setup, but without a current user.

Suggested settings: OS Patch Management

  - Windows and macOS Patch Management - Disable OS automatic updates
  - Windows Update Source - Windows Update (or alternatively WSUS with defined WSUS server address)

- Policy Assignment:
  - Assign Patch policies with the Schedule “Select All” checkbox selected, the “Missed Patch Window” checkbox selected, and Automatic Reboot enabled.
    - Optional - Create multiple Patch policies as defined above and schedule every few hours.
  - Assign Required Software and Worklet policies to install line of business applications and configure your device to bring your device to standard

- Outcome: Device patch settings are configured for Automox management. Patch state is brought to current, and required configurations and software are installed when devices are added to the Automox environment.

Group Structure

Groups provide two primary functions and one major setting.

1. They provide an organizational structure for your devices.
2. They provide a way to organize policy assignments.
    - The OS Patch Management Settings define your patch source.

- Automox is built with simplicity in mind. We hope this motivates you to build your group structure in a way that simplifies your administration when using Automox to manage your devices.

> **Tips for group structures**:
>
> - Policies are not inherited through parent groups at this time, although the policy assignment is per group. Use this to help determine your hierarchy.
> - Groups are sorted alphabetically by hierarchy. A naming convention will help with organization.

Group Structure Examples

Scenario 1 - Simplified Group Structure

This scenario is ideal for simplifying administrative tasks. All OS versions can be placed in the same groups as only the proper policies will apply. Here you can easily control your deployment

times and verify deployments to pilot groups prior to production. The server groups demonstrate a way to separate your systems by a maintenance window based on your environmental needs.

Miscellaneous

- Automox Product Portal: Request new functionality or features
- Release Notes
- Automox Status: Operational status board for Automox services

  RSS Feed: https://status.automox.com/history.rss

- Important URLS (for firewall and routing rules):

  Windows URL's (TCP/80-443)

  microsoft.com
  windowsupdate.com
  nsatc.net
  phicdn.net
  windows.com

  All Windows updates URL

  *.delivery.dsp.mp.microsoft.com.nsatc.net
  .dl.delivery.mp.microsoft.com
  *.wac.phicdn.net
  .windowsupdate.com
  *dsp.mp.microsoft.com
  *dsp.mp.microsoft.com.nsatc.net
  emdl.ws.microsoft.com
  geo-prod.do.dsp.mp.microsoft.com
  prod.do.dsp.mp.microsoft.com
  wac.phicdn.net
  windowsupdate.com
  au.download.windowsupdate.com*
  cs9.wac.phicdn.net download.windowsupdate.com*
  fe2.update.microsoft.com*
  fe3.*.mp.microsoft.com.*
  fe3.delivery.dsp.mp.microsoft.com.nsatc.net
  fe3.delivery.mp.microsoft.com*
  fe3cr.delivery.mp.microsoft.com
  fe2cr.update.microsoft.com
  v10.events.data.microsoft.com
  v20.events.data.microsoft.com
  fe3.update.microsoft.com

geo-prod.do.dsp.mp.microsoft.com
sls.update.microsoft.com*
sls.update.microsoft.com*
slscr.update.microsoft.com
slscr.update.microsoft.com*
Tsfe.trafficshaping.dsp.mp.microsoft.com
sls.update.microsoft.com
fe2.update.microsoft.com
fe3.delivery.mp.microsoft.com
au.download.windowsupdate.com
sls.update.microsoft.com.nsatc.net
fe2.update.microsoft.com.nsatc.net
fe3.delivery.dsp.mp.microsoft.com.nsatc.net
audownload.windowsupdate.nsatc.net

Delivery Optimization (DO) URLs for Split-Tunneling VPN

Delivery Optimization for Windows 10 updates - Windows Deployment

From this Microsoft solutions content, you can find further relevant URLs under the following sections:

- Delivery Optimization service endpoint:
  https://*.prod.do.dsp.mp.microsoft.com

- Delivery Optimization metadata:
  http://emdl.ws.microsoft.com
  http://*.dl.delivery.mp.microsoft.com

- Windows Update and Microsoft Store backend services and Windows Update and Microsoft Store payloads:
  http://*.windowsupdate.com
  https://*.delivery.mp.microsoft.com
  https://*.update.microsoft.com