Getting Started: Fast-Track Your New Automox Environment

(reference material for onboarding)

➢ ***Introduction Slide***

Internet Access

- Agent Firewall Allow listing Rules - https://support.automox.com/help/agent-firewall-whitelisting-rules

- Using the Automox Agent With a Proxy Server - https://support.automox.com/help/using-the-automox-agent-with-a-proxy-server

Proxy notes

- *Tip:* Starting with agent version 29, Windows automatically identifies proxy settings if they are set per the current user or set for the system. Windows now require the system to have access through the proxy, or a policy configuration to lower the security to allow fallback to user.

- *Tip:* Devices behind a proxy may need a route to be configured (for example, pac file or proxy application permissions). Add routing, if needed.

- *Tip:* Add 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
```

EPP Trust

- Globally Trust-listing Automox Through EPP Application Control - https://support.automox.com/help/globally-trust-listing-automox-through-epp-application-control

Agent and Script Execution

- Location of Files Required by Automox - https://support.automox.com/help/location-of-files-required-by-automox

- Change Automox Script Execution Location - https://support.automox.com/help/change-automox-script-execution-location

- Agent may use C:\Windows\Temp for upgrades

****Additionally, a temporary working directory may be desired for some Worklet or Required Software Policies. Ensure these directories are also considered when setting up your trusts or exclusions. *Example →* C:\Windows\Temp or C:\MyOrg\ScriptDir

➢ ***Accessing Management Sites on the Web***

Automox API and S3

- Agent Firewall Allow listing Rules - https://support.automox.com/help/agent-firewall-whitelisting-rules
    - There are 2 Automox URLs that your agents will need to reach for the Automox agent to function correctly.
    - The api url provides your device access for the agent to communicate with the cloud Automox services. Uploaded files for Worklets and Required Software policies are stored in Automox's AWS s3 bucket.

Console

- To used the web console, you will need access to console.automox.com

- Best Browsers to use, current versions: Chrome, Edge, Firefox, Safari (c/c-1)
    - As of this date, the AX console does not officially or fully support mobile.

- *Tip:* All Automox communications over port 443

OS Patch Source

- Automox utilizes the built-in patch installation functionality from each operating system. Each of those update solutions will require access to the appropriate URLs for patching. Please see the Agent Firewall Allow Listing Rules Support document for additional instruction and resource links.

Other Sources

- Automox hosts a cache for a majority of the 3rd party patches we support at the console.automox.com site.

- Chrome Updates using its built-in updater.

- Account for any other applications that self patch by whitelisting the appropriate URLs

Automox Agent Enablement

Internet Access

- Agent Firewall Allow listing Rules - https://support.automox.com/help/agent-firewall-whitelisting-rules

- Using the Automox Agent With a Proxy Server - https://support.automox.com/help/using-the-automox-agent-with-a-proxy-server

Proxy notes

- *Tip:* Starting with agent version 29, Windows automatically identifies proxy settings if they are set per the current user or set for the system.

- Windows now require the system to have access through the proxy, or a policy configuration to lower the security to allow fallback to user.

- *Tip:* Devices behind a proxy may need a route to be configured (for example, pac file or proxy application permissions). Add routing, if needed.

- *Tip:* Add 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

EPP Trust

- Globally Trust-listing Automox Through EPP Application Control - https://support.automox.com/help/globally-trust-listing-automox-through-epp-application-control

Agent and Script Execution

- Location of Files Required by Automox - https://support.automox.com/help/location-of-files-required-by-automox\

- Change Automox Script Execution Location - https://support.automox.com/help/change-automox-script-execution-location

- Agent may use C:\Windows\Temp for upgrades

- Additionally, a temporary working directory may be desired for some Worklet or Required Software Policies. Ensure these directories are also considered when setting up your trusts or exclusions.

    - Example C:\Windows\Temp or C:\MyOrg\ScriptDir

➢ ***Takeaways***

Review Agent Requirements

- 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)

OS Source Assignment - *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.

- [OS Patch Management Settings for Groups]

Automox Best Practices

- 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.

- Define your method to set patch management settings. You can set this via Automox Groups, MDM or GPO as an example, but our best practice is to only use one method.

Group Structure

- It is possible to arrange groups by department, geography, or whatever makes sense for your organization. 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.

- Group Management Overview
  https://docs.automox.com/home/system-management/managing-groups#ManagingGroups-ViewingGroups

- Searching and Filtering Groups
  [Searching and Filtering for an Individual Policy or Group]

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 organization 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 msi installer switches and PowerShell bulk installer script to automatically add devices to a specific group at agent installation time.

Patch Policies and use cases

- Ask your CSM for the “Onboarding Jumpstart Guild - Patching” document for a deeper overview.

Agent Installation

- 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
    - Silent Agent Deployment on Windows
- Linux
  - Installing the Automox Agent on Linux
- Crowdstrike
  - Deploy Automox through CrowdStrike Falcon [Windows only]

Reboot Strategy

- Policy
- Worklet