Onboarding Jumpstart Guide - Patching

As you begin to build out your new Automox organization, understanding what is available, and having access to best practices will help you to define your organization patch policy standards within the Automox console.

Each organization 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 organization.

Policy Overview - View and Create Policies

Managing Policies

Types of Patch Policies

- Patch All
- Patch All Except
- Patch Only

  Example of how to use Patch All Except and Patch Only policies: Using Policy Patch Filters
- Manual Approval
  - Enabling Manual Approval
- By Severity
  - Understanding Automox Severity Data
  - Patching When the Severity Level Is Unknown
- Advanced Policy
  - Using the Advanced Patch Policy

Notifications and Reboots

Windows and macOS patch policies have Reboot and Notification functionality built-in. They also have the ability to configure notifications and deferrals prior to patch installation, and before reboots.

- Notifications
  - macOS

    Allowing Automox Notifications on macOS Catalina

    Tip: To reset event notifications manually, use the following command.

    `sudo tccutil reset AppleEvents`
  - Security Approval for Microsoft Office Patches

    > **Caution**: If the amagent is not allowed to control Microsoft AutoUpdate, the latest version in the console will be empty and will not automatically update.

Set Security Approval for Microsoft Office Patches with an MDM Profile

- Reboot Notifications

  Tips:

  - If Automox reboot on a BitLocker managed device, BitLocker is bypassed for the managed reboot.
  - Reboot deferrals not applicable on Windows 7.
  - Notifications are currently not supported on Linux systems.

Third-Party Software Updates

- Supported Third-Party Software
- Best practices for patching third-party software

Patch Status

Status icons and messages found in the console can be very helpful when checking into device health, connection status, or the state of a policy that is attempting to run, or currently running. Here are a few examples:

- **Excluded From Reports**: This device is flagged as an exception and will not show up in reporting. We will still try to patch according to the policies assigned to the group that it is in.
- **Unmanaged**: This device has been added to Automox, but the group it is in does not have any policies assigned to it.

Patch Installation Methods

Scheduled Policy

- The policy will run at the local time of each device defined within the Policy.
- If notifications are configured, a notification and the defined deferral option will appear at the scheduled deployment time, allowing 15 minutes to respond.
  - If the Automatic Reboot option is enabled in the policy, and one or more patches require a reboot, the Reboot Message will be displayed. In any other scenario with Notifications, the Notification message will be displayed.
- If Automatic Reboot is configured, a final restart notification is displayed after patches are installed allowing 15 minutes, but only if a restart is required to complete the patch installation. The user can click Reboot now, or Close. If they select close, or do not respond to a reboot notification, the computer will reboot at the time specified.
  - If Reboot notification deferrals are enabled, the policy defined deferrals are displayed within the reboot notification.

- When the “If a device misses a patch window, patch it the next time the device checks in” checkbox is selected, as long as the machine has run a scan between the time the policy was created, and the policy schedule time, the policy will run when the device next communicates with Automox.
- Notifications are only displayed if there is an active user session (only if a user is logged on). If no user is logged in, installation and reboot actions will run automatically.

Manually Run Policy

You can manually run enabled and assigned policies at any time (this includes scheduled policies).

- You can trigger a manual policy run from Device Details (for an individual device) or from System Management (on all targeted computers at one time).
- Manually running a policy will honor the Automatic Reboot configuration, but will not display notifications.
- Manually running a Worklet policy will ignore evaluation, and immediately run the remediation code.
- Manually running a policy without a schedule set it the only way to trigger the policy to run.

Individually

You can install or uninstall (if applicable) updates from device details under the actions column drop-down menu.

- No notifications are displayed and no reboot will be forced when manually installing an individual patch from the Actions drop-down menu.
- **Note**: You can manually trigger a restart after the patch from Devices, or device details.

Patch all like OS devices where patch is missing

You can install a patch for all like OS devices where a patch is Awaiting installation. From the Software page, search for the patch of interest. One or more versions of the patch may be listed, as the software is displayed by OS as well as patch display name. You can see how many devices require the patch indicated in the “Impacted Devices” column. (The number in this column is also a hyperlink to the device list of impacted devices). To the right, there is an action drop-down button where you can install the patch on all impacted devices.

Patch Scenarios

Scenario: Patching Pilot - Policies and Groups

Patching a pilot group of systems before patching all production systems can help reduce potential risk incurred by installing updates to applications or operating systems. Here are a few tips:

- Build pilot group(s) that include like or similar systems to your production systems. Include devices with the same operating systems, applications, and similar patch levels. This will help to build confidence that your production patch deployment will work as expected when deployed to your production groups.

- Ensure that critical applications are reviewed after patching, allowing enough time to make adjustments should a patch negatively impact your app functionality.
- Provide enough time to evaluate the pilot devices, to keep the timing between pilot and production releases as short as possible to ensure dynamic rules do not modify the patch set between testing and production deployments.

Example (This is an example, used for demonstration purposes. Please adjust for your environment.)

Build the following groups:

- Pilot - Client Systems
- Pilot - Servers
- Production - Client Systems
- Production - Server Systems 1
- Production - Server Systems 2

Build the following policies:

- Pilot - Client Patch all except (or Advanced)
- Pilot - Server Patch All except (or Advanced)
- Servicing Stack Updates Pilot
- Servicing Stack Updates Client Production
- Servicing Stack Updates Server Production
- Production Client Patch all except (or Advanced)
- Production Server Patch all except (Saturday 10:00pm)
- Production Server Patch all except (Sunday 12:00am)

Scheduling:

- Schedule the Pilot policies to run every Wednesday at 12:00pm, with reboot.
- Schedule the Client Production policy to run Fridays at 10:00am, Notify users before patching and allow deferral for both patching and reboot. Install if the system is offline during scheduled time.
- Schedule Servicing Stack Update Pilot policy to install at 10:00am every day. Install if the system is offline during scheduled time. No reboot or notifications.
- Schedule the Servicing Stack Update Client Production policy to run Thursdays and Fridays at 9am. No reboot or notifications.
- Schedule the Servicing Stack Update Server Production policy to run on Saturday at 9pm. No reboot nor notification.
- Schedule the Production Server Patch all except (Saturday 10:00pm) policy to run every Saturday at 10:00pm. Include reboot without deferral.
- Schedule the Production Server Patch all except (Sunday at 12:00am) policy to run at 12:00am every

Sunday. Include reboot without deferral.

Logic in this scenario:

- The industry has determined that it takes an average of seven days for a bad character to take advantage of a new exploit. By patching weekly, you will test and deploy patches released within the previous 7 days.
- Pilot and production deployments are scheduled closely together. This allows dynamic policy rules to remain more relevant than scheduling them far apart. As patches are released or superseded, some patches may be added or removed from the dynamic policy patch set. This is a potential drawback to this scenario. The trade off is a set-it and forget-it rule set with the ability to keep your environment up to date with little manual administration effort.
- Patch schedules are simple and predetermined. This should simplify communications and employees can plan around the patch schedules.

Tips and Best Practices

What Are the Recommended Best Practices for Patching in Automox?

Tip: Policies are not inherited based on group hierarchy/structure. Policies must be directly assigned to each group where you want it to be applied.

Tip: Search filters are very helpful. 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 Software in the Policies filter, it will filter to that type of policy.

Tip: Each managed device will need access to all update sources when scans and policies run. Notable updates sources are:

- Windows Update troubleshooting
    - https://docs.microsoft.com/en-us/windows/deployment/update/windows-update-troubleshooting#device-cannot-access-update-files
- WSUS server (if used in your environment)

Templates

Here are API scripts (PowerShell) to create the patch policies from the previous Recommended Best Practices article:

- Primary Patch Policy

  https://github.com/AutomoxCommunity/Templates_And_Examples/blob/main/CreatePrimaryPatchPolicy.ps1

- Servicing Stack Update Policy

https://github.com/AutomoxCommunity/Templates_And_Examples/blob/main/CreateServicingStackPatchPolicy.ps1

- Windows 10 Feature Update Policy

  https://github.com/AutomoxCommunity/Templates_And_Examples/blob/main/CreateFeatureUpdatePatchPolicy.ps1

- Optional: Defender Definition Update Policy

  https://github.com/AutomoxCommunity/Templates_And_Examples/blob/main/CreateDefinitionUpdatePatchPolicy.ps1

Note: Policy rules are best suited for English-based systems. Use of Advanced policies may be more appropriate than Patch All Except policies when international language support is required (when standardized rule sets are preferred).

WSUS

- Configuring WSUS for Automox Integration
- OS Patch Management Settings for Groups

Integration with WSUS provides a way you can cache Microsoft updates on-premise to reduce download bandwidth. Third-party updates are not stored in WSUS, and will download from the internet directly.

When you set your Group's OS Patch Management "Windows Update Source" to WSUS, and you define your WSUS Server Address, your device will scan for Microsoft-based updates and determine compliance and applicability using your WSUS server as the update source. (**Note**: you can also use the “Keep Device Settings” options if WSUS policies are already applied and preferred).

Make sure to configure WSUS Products and Classifications to include everything needed, as only the patch metadata available in your WSUS DB (the patches included in the cab downloaded from WSUS) will be used to determine what patches are available for compliance or download.

At Scan Time

Automox will direct the device's WU agent to scan for updates against its update source. In this case it will scan against WSUS.

At Policy Run Time

Automox will direct the devices WU agent to download and install the updates it detected in a needed state. It will also verify third-party applications included in the patch policy, and will download them from the internet.

Tip: If you configure your group to use WSUS, your device MUST have access to your WSUS server when scans and policies run.

GPO vs Automox Group settings

GPO and Automox Group Patch Management settings can conflict. GPO Windows Update settings will apply based on the domain schedule (default every 90 minutes). Automox Patch Management Settings will apply based on the group defined scan interval. If they are different, your device could toggle between patch sources, or temporarily go to default. This can cause misalignment in needed patches and potentially install updates or feature updates directly from the internet. We suggest using the Automox group Patch Management Settings, and removing the WU settings from GPO to avoid this type of issue.

Troubleshooting

- WU Error codes

  Windows Update error code list by component - Windows Deployment

- Patch troubleshooting resources:

  Windows Update Troubleshooting Process

  Windows Update troubleshooting - Windows Deployment

- Windows Update Agent and WSUS troubleshooting

  Windows Update - Additional resources - Windows Deployment

Miscellaneous

- Patch rollbacks

  How to Rollback an Installed Patch on Devices

  Windows Patch Rollback Worklet

- Exclusion - Block list

  Adding Patches to the Block List in the Automox Console