AUTOMOX

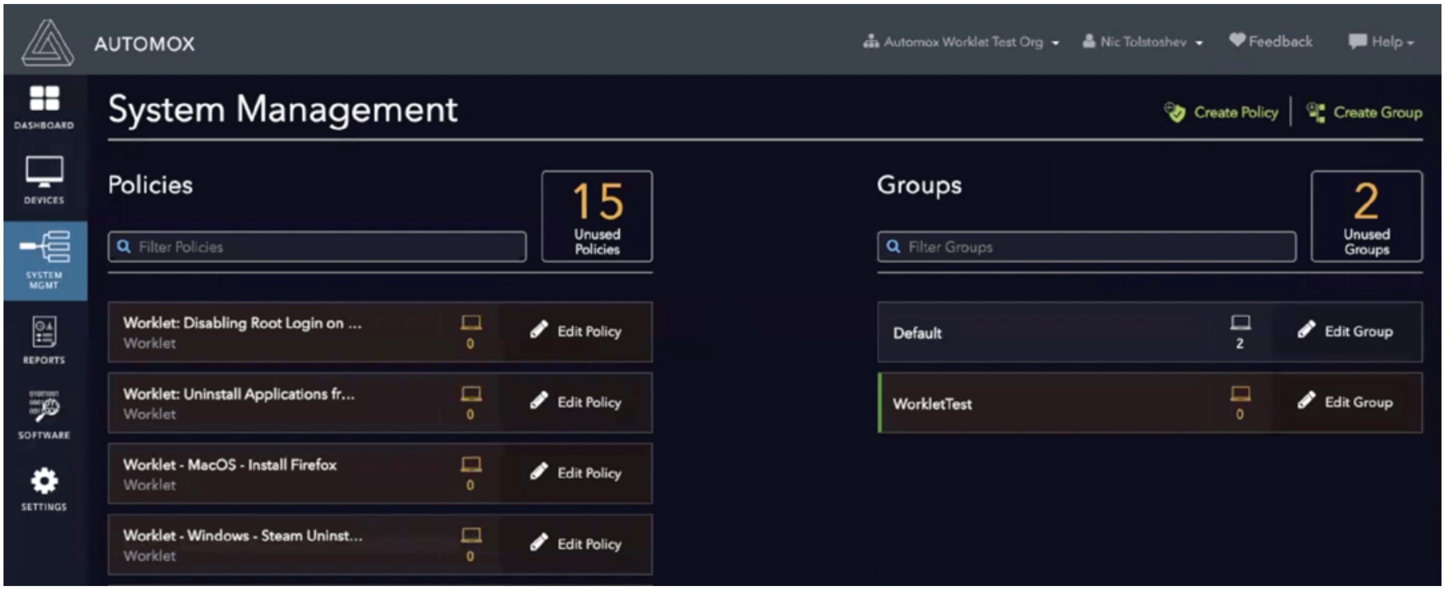
AUTOMOX WORKLET 101 RESOURCE GUIDE

Automox Worklets™ empower security and IT ops to create, automate, and enforce any custom task that they can imagine on endpoints. Based on PowerShell and Bash scripting, Worklets are reusable units of work that can be applied across Windows, Linux, and macOS devices irrespective of location or domain membership.

How useful are Automox Worklets?

Whatever you can script, you can turn into a worklet. And while the applications for worklets are essentially limitless, they are particularly useful for simplifying endpoint management at scale by:

1. Applying configurations to devices that don't connect to the corporate network or aren't in Active Directory.
2. Removing the hassle of establishing permissions to the endpoint.
3. Automating the remediation of new vulnerabilities that aren't patchable.



System Management

Policies — 15 Unused Policies

- Worklet: Disabling Root Login on ... — Worklet — 0
- Worklet: Uninstall Applications fr... — Worklet — 0
- Worklet - MacOS - Install Firefox — Worklet — 0
- Worklet - Windows - Steam Uninst... — Worklet — 0

Groups — 2 Unused Groups

- Default — 2
- WorkletTest — 0

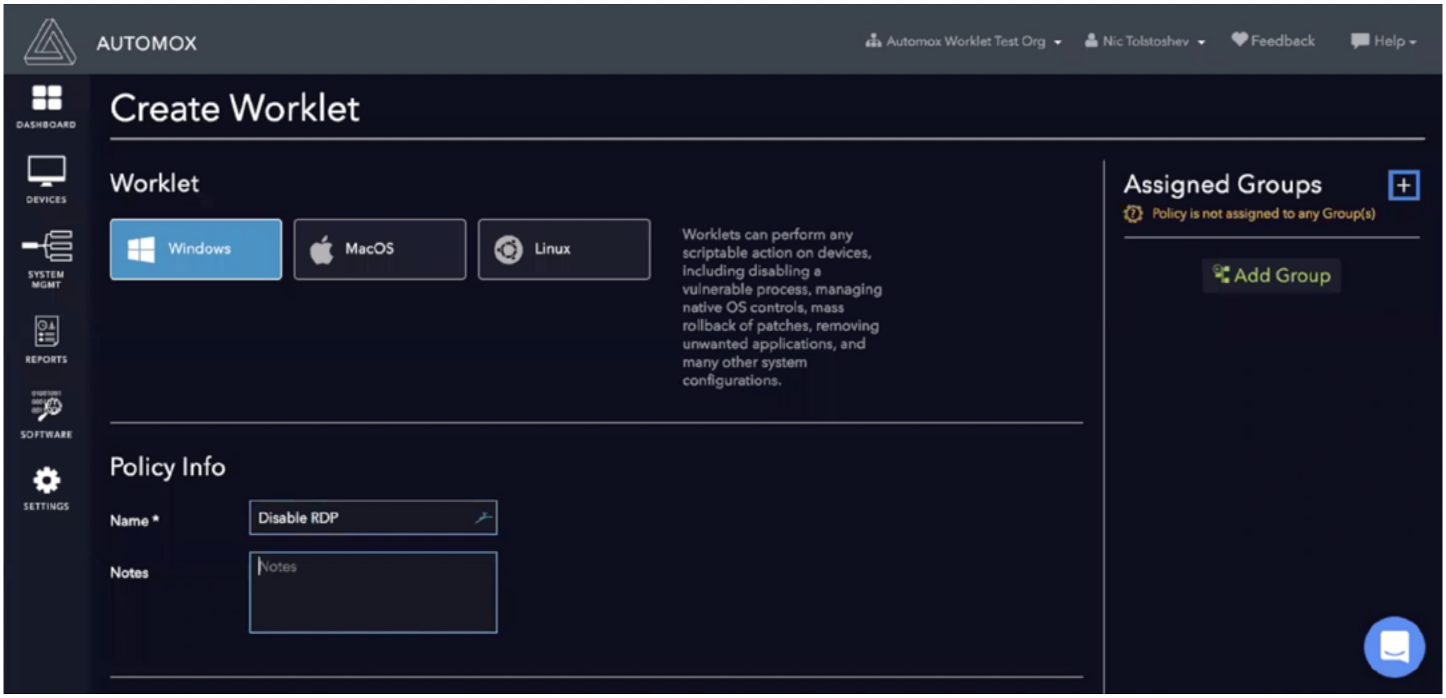
How do Automox Worklets work?

Worklets consist of two code blocks which have an If-Then relationship. The first block is called “evaluation” and the second is designated “remediation.” If the evaluation code block fails (returns non-zero), then the remediation block is run. Evaluation code executes every time an endpoint in an applicable group runs a scan. The remediation code runs according to the worklet policy schedule after the evaluation code has flagged the device as needing remediation. No code or variables is preserved between the evaluation code block and the remediation code block. The code blocks run as System in the **C:\ProgramData\amagent\**.

To impact local user settings, you’ll need to request the list of local users and loop through them in your code. If you use the Execute Now button on a policy, then only the remediation code runs. The result of the remediation code shows in the Activity Log report. You can upload files that you can reference in your code, like an MSI installer.

Getting setup to write your first worklet

Make sure you have a test group setup. Create your policy and select your operating system. Determine when you want the remediation to run. Make sure you have an endpoint with the agent installed, and that it has completed its first scan. Save your policy and connect it to the test group. Scan the endpoint to trigger the evaluation code and see the result on the device page. For testing purposes, run the remediation code manually. For local Windows testing of your PowerShell code, make sure to allow PowerShell code to run: **Set-ExecutionPolicy RemoteSigned** (run as admin). Any files uploaded can be referenced in your code in the current directory.



Create Worklet

Worklet

Worklets can perform any scriptable action on devices, including disabling a vulnerable process, managing native OS controls, mass rollback of patches, removing unwanted applications, and many other system configurations.

Assigned Groups

Policy is not assigned to any Group(s)

Policy Info

Name * Disable RDP

Notes

Tips for success

- Write and test your code on a local machine first.
- When migrating code over to a worklet, you might need to adjust for running as System instead of as the logged-in user.
- Check the results of your remediation code in the Activity Log report.
- Test your code out on different versions of each operating system. There may be changes in locations for settings or registry entries from one version to another.
- Search for code online that might already do what you need, with a little tweaking.

Where to get help

- Recorded tutorial webinar
- Automox Alive community
- Automox Support
- Stack Exchange or other code-focused community
- PowerShell documentation
- Bash resources

Downloading Worklets from the Automox Alive Community

Go to Automox Alive Community Worklets page. Copy over the code blocks by hand. Look through the documentation or description to see if any variables need configuration for your environment. Do a test scan and test remediation to make sure it's working. Keep an eye on it over time to ensure the activity logs continue to show success. If you make any improvements, please upload your version back to the community. Worklets are provided as-is, and there's no guarantee that they'll work in your particular environment.

Uploading Worklets to Automox Alive Community

Go to Automox Alive Community Worklets page. Include a description of what your worklet is and how it works. Call out any variables that need to be changed for other user environments.

Start and end your code blocks by putting three backticks in a row on a separate line:

~~~~
```
code goes here
```
~~~~

Submitted worklets go into a queue for review by the Community's moderation team. After the moderation team checks the code, the worklet is published live. If you've submitted a worklet and it doesn't go live in a timely manner, feel free to ping the moderation team.

- Do not include any API keys or credentials in your code.
- Use a placeholder to indicate where the downloader needs to put in their own API key or credentials.
- Feel free to upload your code to a repository such as Github and then link to that from your worklet post.
- All worklets uploaded and downloaded are covered by our Terms of Service.

List of current worklets:

1. Remove IE11 from Windows 10
2. Automatic Upgrade of Devices to Windows 10 version 1903
3. Get Hard Drive Free Space Percentage
4. Predictable Reboot Notifications for Windows
5. Invoke search repair troubleshooting pack
6. Invoke Troubleshootingpack Networking
7. Invoke Troubleshootingpack Bluetooth
8. Invoke Troubleshootingpack Audio
9. Execute Defender Quick or Full scan
10. Enable or disable Windows Defender
11. Suppress macOS Catalina Upgrade Notifications
12. Disabling Bluetooth on MacOS Endpoints IF No Connected Devices or Peripherals
13. IE11 Zero-day “One-Click” Remediation for Windows
14. Force password reset Windows
15. (macOS) Create a new user worklet
16. Installing CrowdStrike on MacOS
17. (macOS) enforce password policy for all users and not for exempt users
18. Remove Microsoft Mail App from Managed laptops - Windows 10
19. Disable PowerShell v2.0 on Windows 10
20. Reset Windows Update - Now with intensity
21. Installing Carbon Black on MacOS
22. Bitlocker Key ID and Recovery Key
23. Enable Gatekeeper on macOS
24. Disabling Root Login on Linux Devices
25. Less intense resetting of the Windows Update client
26. Uninstalling Applications on MacOS
27. Auto-Update Stale Docker Containers
28. Enable Firewall on macOS
29. Ensuring Firefox is installed on Mac devices
30. Enforced Application Uninstall
31. XP Patching
32. Install LogMeIn client on Mac
33. Install Discord client on Mac
34. Install Dashlane client on Mac
35. Legal Acknowledgement at Login
36. Enforce BitLocker Encryption
37. How to Disable Remote Desktop Protocol Connection
38. Windows Cleanup Tool
39. Install Box client on Mac
40. Windows Patch Rollback
41. Adobe Reader Install
42. Chrome Install
43. Dropbox Install
44. Evernote Install
45. Network Drive Mount
46. Set Windows Password Policy
47. Set Screensaver Settings
48. Skype Install
49. Slack Install