

AUTOMOX WORKLETS 101

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, macOS, and Linux 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:

01.

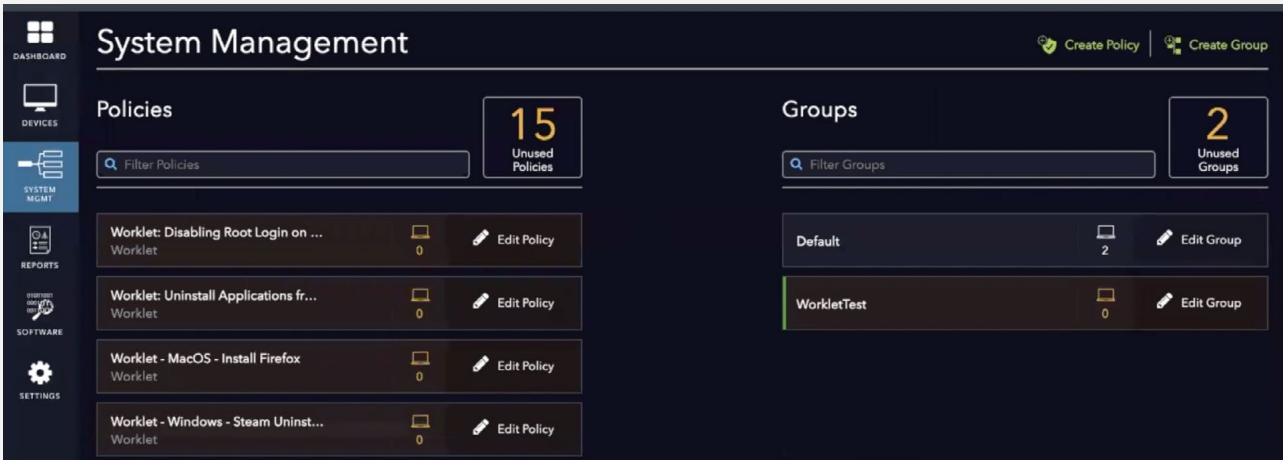
Applying configurations to devices that don't connect to the corporate network or aren't in Active Directory.

02.

Removing the hassle of establishing permissions to the endpoint.

03.

Automating the remediation of new vulnerabilities that aren't patchable.



The screenshot displays the Automox System Management interface. On the left is a navigation sidebar with icons for Dashboard, Devices, System Mgmt (selected), Reports, Software, and Settings. The main content area is titled 'System Management' and includes 'Create Policy' and 'Create Group' buttons. It is divided into two main sections: 'Policies' and 'Groups'. The 'Policies' section shows 15 'Unused Policies' and lists four worklets: 'Disabling Root Login on ...', 'Uninstall Applications fr...', 'MacOS - Install Firefox', and 'Windows - Steam Uninst...'. The 'Groups' section shows 2 'Unused Groups' and lists 'Default' and 'WorkletTest'.

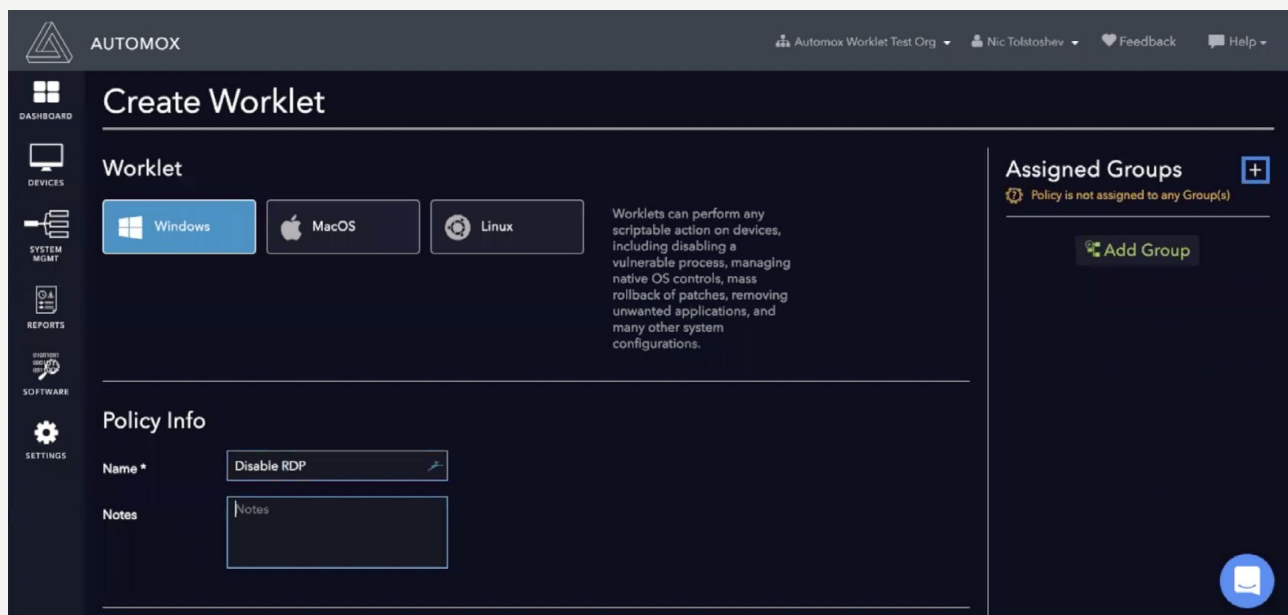
How do Automox Worklets work?

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 set up 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.



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:

```
```\n\n  code goes here\n\n```
```

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](#).

---

## 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.

---

### 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](#)

---

# Automox Worklets in action

Here are a few things Automox Worklets are doing today. You can access our full repository of worklets on the Automox Alive Community at:

[community.automox.com](https://community.automox.com)

---



## Disable Any Vulnerable Process

This RDP disabling worklet can be used as a mitigating control to protect impacted Windows systems from the BlueKeep vulnerability.

[See this worklet in action](#) →



## Manage Native OS Controls

Enforcing controls such as BitLocker are easy and can be automated with this simple policy.

[See this worklet in action](#) →



## Mass Rollback of Unwanted Patches

With a few clicks, an admin can deploy a worklet that will detect the presence of, and subsequently remove, the unwanted patch from any defined group of endpoints.

[See this worklet in action](#) →



## Support Legacy OS with Mass Deployment

This worklet allows you to quickly and simply deploy an emergency patch across legacy systems to ensure they are less of a risk for exploit.

[See this worklet in action](#) →

---

## ABOUT AUTOMOX

---

Facing growing threats and a rapidly expanding attack surface, understaffed and alert-fatigued organizations need more efficient ways to eliminate their exposure to vulnerabilities. Automox is a modern cyber hygiene platform that closes aperture of attack by more than 80% with just half the effort of traditional solutions.

Cloud-native and globally available, Automox enforces OS and third-party patch management, security configurations, and custom scripting across Windows, macOS, and Linux from a single intuitive console. IT and SecOps can quickly gain control and share visibility of on-prem, remote, and virtual endpoints without the need to deploy costly infrastructure.

Experience modern, cloud-native patch management today with a [15-day free trial](#) of Automox and start recapturing more than half the time you're currently spending on managing your attack surface. Automox dramatically reduces corporate risk while raising operational efficiency to deliver best-in-class security outcomes, faster and with fewer resources.

[Chat with Automox to set up a demo.](#)

[info@automox.com](mailto:info@automox.com)

720.440.2495