

How to Use Worklets

This describes how you can use worklets to manage devices. In the console, Worklets are an option under **Manage > System Management > Policies**.

A **Worklet** is designed to be extremely flexible. It allows you to evaluate and enforce just about anything you can script. You can also upload files that can be used on the targeted device.

Script Languages

The Evaluation and Remediation code languages are specific to the OS and run in the version currently installed on the target machine.

Windows: PowerShell

Linux & OS X: Bash

It is possible to launch and run a script file in a different language in the remediation code by invoking the file from the native language script. This assumes that your target device is capable of running the uploaded script file.

Note: On 64-bit Windows, this runs in a 32-bit PowerShell session. You may need to plan around this for accessing 64-bit registry locations and filesystems. This is caused by 32-bit processes being redirected to 'Wow6432Node' or 'SysWoW64' in place of the native locations.

Evaluation Code

The evaluation code is intended to test a condition, and return an exit code based on that condition. The evaluation runs each time a device runs a scan and flags the device for remediation according to the exit code. If the exit code is 0, the evaluation is seen as successful and no remediation will take place. Any non-zero exit code flags the device for remediation. The remediation code will run when the worklet's scheduled time arrives.

Note that manually executing the worklet triggers the Remediation code regardless of the flagged exit code.

Remediation Code

The remediation code section is open ended and can be used to do basically anything you can script. For example, you can enforce a configuration setting, install an application or certificate, etc.

Any files you uploaded to the worklet are downloaded when the remediation code runs, and can then be called/invoked by your worklet.

Uploading Files

Any files you may need to reference in your remediation script can be uploaded as part of the policy. These files will download when the remediation runs and will be available in the current working directory of the script. As such, they can usually just be referred to by their file name, although some situations may require that you use the relative path. (./filename in Bash or .\filename in PowerShell).

Note: The current file size limit is 1 GB.

Executing Worklets

Scheduled Execution

As with all of the other policy types, worklets can be scheduled to run by Month, Day-of-Week, and Week-of-Month. Use this to customize the schedule on which the remediation script will run non-compliant devices.

Manual Execution

Manual Execution can be handled in two different ways: per device and per worklet.

On the **Device Details** page for every device in a Group that is associated with the worklet, there is an Associated Policies section where you can see the worklet name and a **Run On This Device** button. This button triggers the worklet to run immediately on the selected device.

On the **Manage > System Management** page, find the worklet from the list of Policies. From the Actions menu, select Run Policy. This triggers the worklet to run immediately on all devices in the associated groups.

Note: These methods trigger the remediation script regardless of the compliance status of the device. *Use these methods with caution.*

Related Topics:

- [Access Worklets in the Automox Community](#)
 - [What are Automox Worklets?](#)
-