

Installing Windows Updates that are not able to be automatically packaged

What

As a Windows administrator, you want to install some Windows Updates where FileWave reports that the item is missing, but it's not a security update where FileWave could automatically create a Fileset for that update.

When/Why

Since 14.7.0 of FileWave, there has been additional reporting on missing updates for Windows. With the increased reporting many administrators have asked how to install an update when it is missing from a device but isn't seen as an update that FileWave is capable of turning into a Fileset on its own.

How

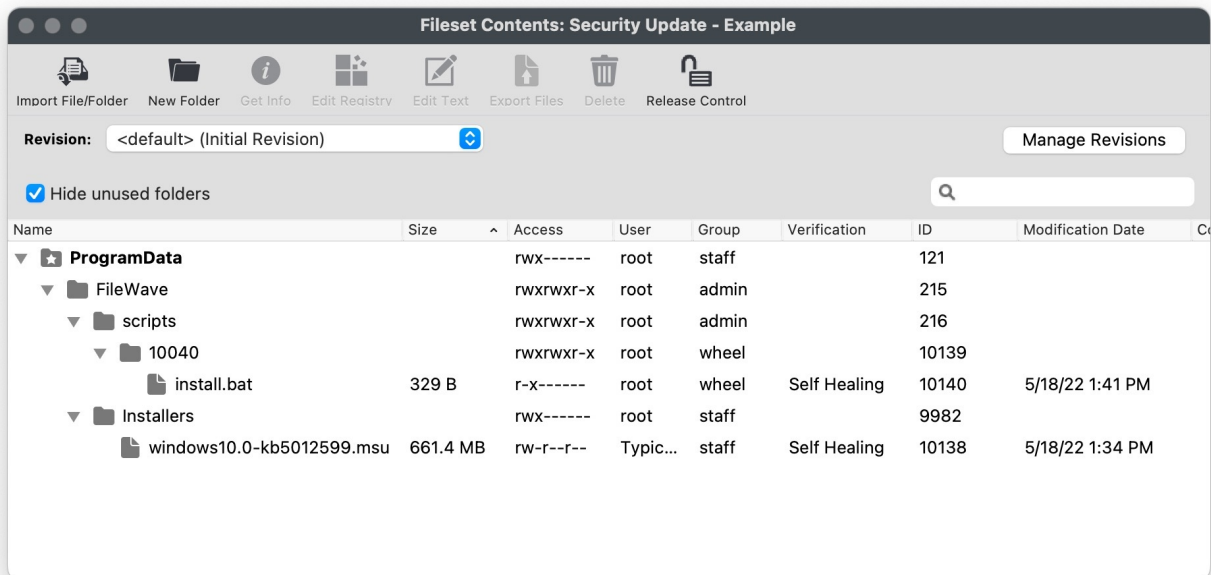
The first thing is to understand that Windows updates can come in .MSU files (Microsoft Standalone Updater). These updates can be processed by an exe %windir%\System32\Wusa.exe and installed.

For example, if the Windows6.0-KB934307-x86.msu file is in the D:\934307 folder, type the following command at a command prompt to install the update package:

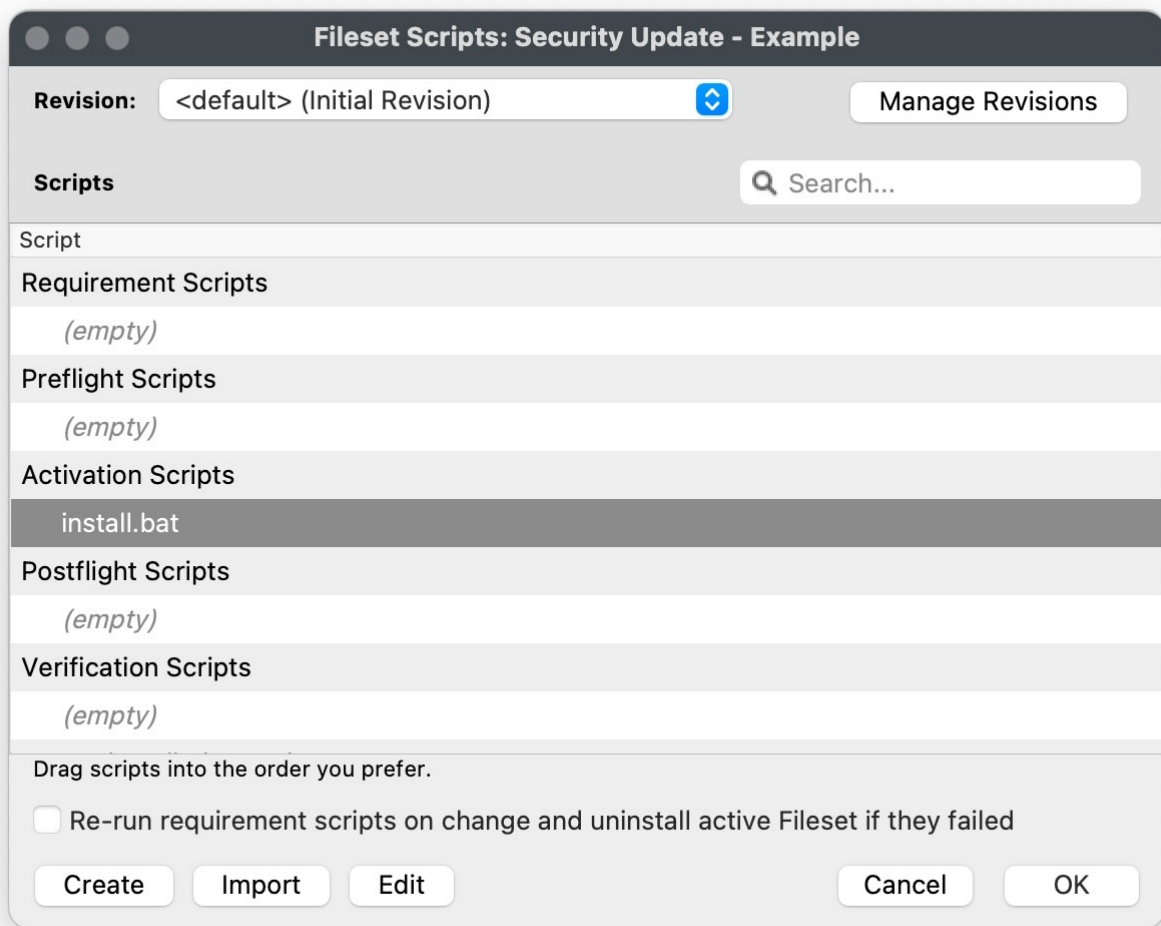
```
wusa.exe /quiet /norestart d:\934307\Windows6.0-KB934307-x86.msu
```

To accomplish this in FileWave let's take a real example. First, we will go to <https://www.catalog.update.microsoft.com/Home.aspx> to look for this update. Download the MSU file once you see it.

Next, create a Fileset by making an Empty Fileset and then add the update as seen here:



To install the MSU you will need to add an Activation Script to it.



Here is the text of install.bat.

i You'll notice in the images and script that I shortened the name of the MSU file. That's just to make it easier to read. If you keep the long name it downloads with then just be sure to copy the entire name if you do keep it long. Notice the " marks around the filename as well in case you have spaces in the path.

Install.bat

```
REM For all script types, returning an exit code of 0 (success) means the
REM script execution completed successfully.
REM Add the contents of your script below:

%windir%\System32\wusa.exe /quiet /norestart "c:\programdata\FileWave\Installers\windows10.0-kb5012599.msu"

exit 0
```

You may notice that this update has /norestart, but most security updates need a restart. You could go to Properties for the Fileset and have FileWave control the reboot as shown below.

Fileset Name: Security Update - Example

Revision: <default> (Initial Revision)
Manage Revisions

Properties
Requirements
Dependencies
Delete Files
Kiosk

☒ Requires Reboot
Message...
Color:

☐ Authenticated restart for devices with Full Disk Encryption and an escrowed Personal Recovery Key. MacOS 10.13+ APFS does not support the option for authenticated restart.

☐ Ignore Permissions on Existing Folders

Installation Priority:
Lowest
Highest

Verification settings

☒ Self Healing
☐ Download If Missing
☐ Ignore At Verify (Left Behind)

☐ Don't overwrite existing files upon deployment
☐ Overwrite only if the existing file is older

Apply Verification Settings

☐ Disable Windows 32-bit on Windows 64-bit redirection

Cancel
OK

It's important to note that wusa.exe is smart enough to not install an update that a device already has or an update that does not really apply to a device. You shouldn't have to worry about if someone already patched their machine. If you want to be a bit fancier you could make a Requirements script that would check if an update is installed and then exit if it is there.

Once an update is installed you would need the inventory to update for a client to see that the update is installed in the Software Updates section of the admin console. You can either wait for the verification to normally happen (once every 24 hours, or on restart) or send an explicit Verify command. That should be all you need to do. Repeat this process for any MSU file that you need to deploy via FileWave.

Related Content

- [Windows Software Update Reporting](#)
- [Fileset Creation and Deployment](#)

Digging Deeper

More information on wusa.exe is here:

<https://support.microsoft.com/en-us/topic/description-of-the-windows-update-standalone-installer-in-windows-799ba3df-ec7e-b05e-ee13-1cdae8f23b19>

When you are testing it may be difficult to repeat your testing once an update installs, but wusa has an /uninstall switch as well that

can save you time. Below is an example that would remove a patch. Another alternative is to use a Virtual Machine for testing and use snapshots to be able to install and then roll back to before the update was installed.

```
wusa /uninstall /kb: KB5000802 /quiet /promptrestart
```

For troubleshooting to view the Windows Update Standalone Installer event log on a client device, follow these steps:

1. Click Start, type event viewer in the Start Search box, and then click Event Viewer in the Programs list.
2. In Event Viewer, expand Windows Logs, and then click Setup.
3. Setup events appear in the middle pane.
4. In the Actions pane, click Filter Current Log.
5. In the Event sources list, click to select the WUSA check box, and then click OK.

🕒Revision #1

★Created 13 July 2023 19:59:58 by Josh Levitsky

✎Updated 13 July 2023 20:05:30 by Josh Levitsky