

Software Updates (Windows)

The Software Updates (Windows) section provides essential information and guidance on keeping your Windows operating system and third-party software up to date. Stay informed about the latest updates, including security patches, bug fixes, and new features, to enhance the performance, stability, and security of your Windows devices. Learn how to check for and install updates, manage update settings, and optimize compatibility with third-party applications. By regularly updating your Windows operating system and software, you can ensure an optimized and secure computing experience while taking advantage of the latest improvements and enhancements.

- [Windows Software Update Reporting](#)
- [Installing Windows Updates that are not able to be automatically packaged](#)
- [Understanding and Utilizing the Windows Update Build Revision \(UBR\) Number](#)

Windows Software Update Reporting

What

Starting from FileWave version 14.7+ there is a better overview of updates that should be deployed to the Windows devices managed by FileWave so that you can easier identify possible risks and deploy needed patches.

- The number of missing updates is reported for each Windows device
- A list of all installed updates is reported for each Windows device
- A list of all requested updates is reported for each Windows device
- Regardless of the enrolment type, all devices are reporting the status

When/Why

Security is more important every day. Knowing the state of security of your endpoints is critical to protecting your environment so this enhancement will help with more detailed reporting around Microsoft patches. The data is collected every 1 hour from devices. Read the [OS Software Updates](#) article for more details on applying the updates to Apple or Microsoft Windows devices.

How

In the Native Admin, there is a new tab in the Client Info window, called "Software Updates"

- The Software Updates section displays all installed patches
- The Software Updates section displays all requested patches
- The device reports the status regardless of the way how it was patched (FW, manually, other tools)
- Additionally, a new property called Category is displayed to show what type of update is listed

It is possible to filter at the top of the table by:

- requested (default status), installed, all
- category (those with at least one result will be listed)
- critical (yes/no)

Win11-BETA1 - Client Info

Last Connected: 1/6/22 2:59 PM
From: 74.214.50.253
Free Space: 215.2 GB
Platform: Windows 11.0
Model: 318
Version: Not connected
Enrollment Type: Enrollment via fwcloud
Missing Updates: 3 | 0 Critical

Export Current Tab Client Monitor Get Log Verify Tools

Filesets Status Device Details Users Policies Software Updates

Status: Show All Category: Show All Critical: Show All 8 Updates

Name	Update ID	Size	Critical	Status	Update Assigned	Install Date	Category	Release Date	KB Article
2021-10 Update for Windows SV Versio...	831e2122-3a...	3.21 MB	Yes	Completed		12/7/21	Critical Upda...	11/4/21	KB4023057
2021-11 Cumulative Update Preview for...	2d1f8d5f-27...	45.0 MB	No	Unassigned			Updates	11/22/21	KB5007292
2021-12 Cumulative Update for Windo...	c44343a4-a...	1.86 GB	No	Completed		12/14/21	Security Upd...	12/14/21	KB5008215
Security Intelligence Update for Microso...	6545ff6b-b...	1.55 GB	No	Unassigned			Definition Up...	1/6/22	KB2267602
Security Intelligence Update for Microso...	1aab894d-7...	1.55 GB	No	Unassigned			Definition Up...	1/6/22	KB2267602
Update for Microsoft Defender Antivirus...	13c2493f-c...	7.8 MB	No	Completed		12/14/21	Definition Up...	12/13/21	KB4052623
Update for Windows Defender Antivirus...	c01629fc-6...	4.89 MB	No	Completed			Updates	5/1/20	KB4052623
Windows Malicious Software Removal T...	38db0ad6-2...	37.5 MB	No	Completed		12/14/21	Update Rollu...	12/14/21	KB890830

In the Web Admin, there are two new information items in the Software Updates section of Device Info.

- The overall number of missing and the number of (missing) critical updates are displayed
 - Both link to the Software Updates tab with the responding filter applied
 - In case of no results, the value "0" is displayed, but the link does not exist
- Regardless of the enrolment type, this section is available and functional for all Windows devices

Go to Dashboard

Devices

Payloads

Software Updates

Deployments

Device Info

Deployment

0% Completed

Completed : 0

Remaining : 1

Warning : 0

Error : 0

Software Updates

Missing: 1

Critical: 1/1

Device Info

Payloads

Software Updates

Applications

Users

Groups

Deployment

Software Updates

In the Web Admin when going to the Software Updates tab of a device there is additional filtering and reporting of missing and installed software updates.

- Filters can be applied to the whole table:
 - All / Missing / Installed
- Columns can be filtered:
 - Critical (dropdown)
 - Categories (multiselection)
 - Status (multiselection)

Win10-Lab1

Add to deployment

Verify

Device Actions

Device Info

Payloads

Software Updates

Applications

Users

Groups

Software Updates

Search list ...

Missing

Installed

All

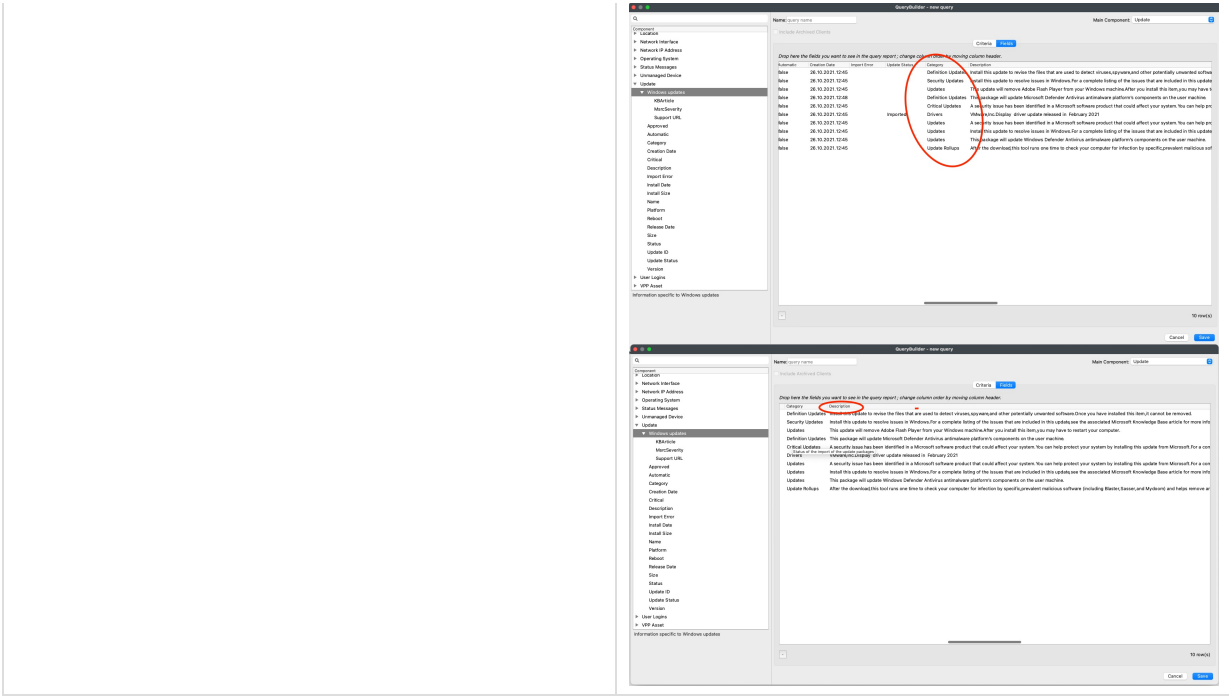
Name	Category ↑	Support URL	Release Date	Size	Critical	Status	Update ID
Security Intelligence Update for Microsoft...	Definition Updates	KB2267602	1/21/2022, 12:00:00 AM	1.48 GB	No	Unassigned Not Available ⓘ	e313c73f-5cfc-
Security Intelligence Update for Microsoft...	Definition Updates	KB2267602	1/23/2022, 12:00:00 AM	1.48 GB	No	Unassigned Not Available ⓘ	b1aaf9ea-7ede-
Security Intelligence Update for Microsoft...	Definition Updates	KB2267602	1/20/2022, 12:00:00 AM	1.55 GB	No	Unassigned Not Available ⓘ	0a0445f0-ef99-
Security Intelligence Update for Microsoft...	Definition Updates	KB2267602	1/22/2022, 12:00:00 AM	1.48 GB	No	Unassigned Not Available ⓘ	718f2eee-5d73-

In both the Native and Web Admins there are new fields that are usable for reporting on Windows patches.

As shown here KBArticle, MsrcSeverity, Support URL, Category, and Description are the new fields.

This is an example of Support URL, KBArticle, and MsrcSeverity used in a report.

These examples show Category and then Description.



Related Content

- [OS Software Updates](#)
- [Restart \(Windows\)](#)
- [Installing Windows Updates that are not able to be automatically packaged](#)

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

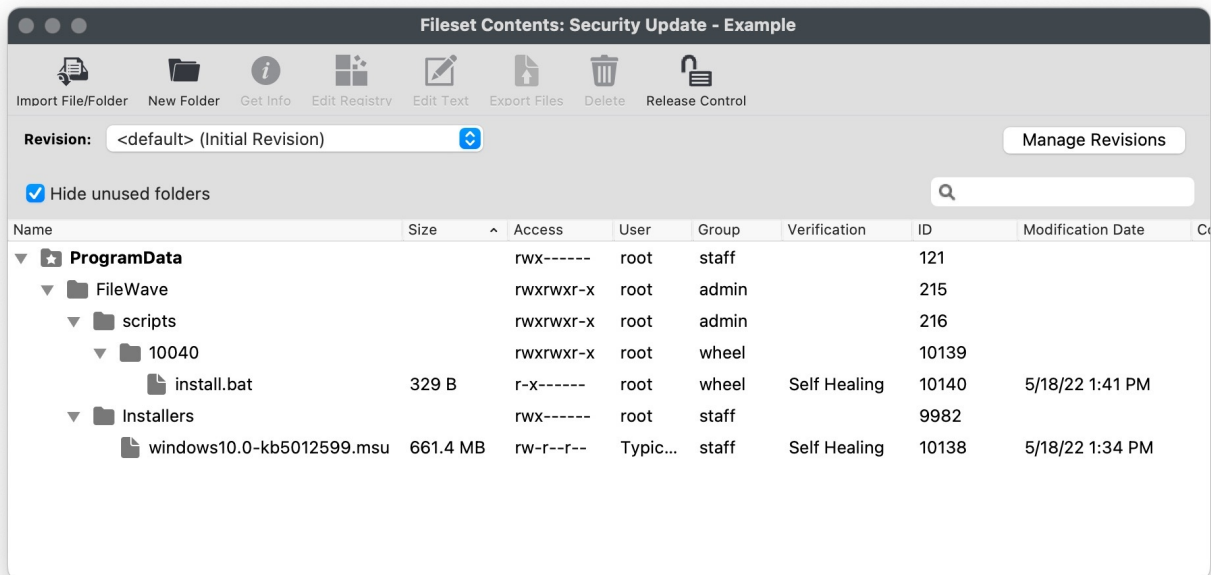
The first thing is to understand that Windows updates can come in .MSU files (Microsoft Standalone Updater). These updates can be processed by an exe %windir%\System32\Wusa.exe and installed.

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:

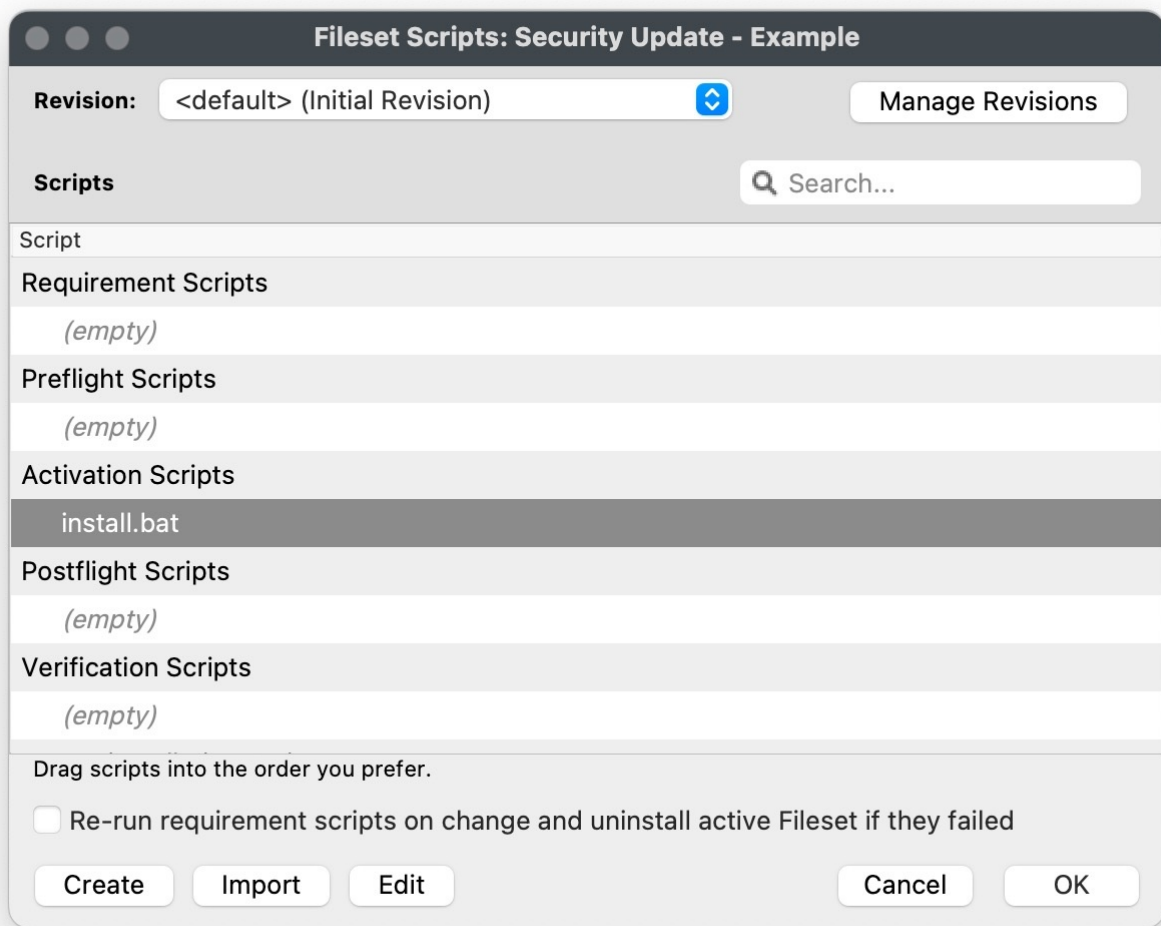
```
wusa.exe /quiet /norestart d:\934307\Windows6.0-KB934307-x86.msu
```

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.

Understanding and Utilizing the Windows Update Build Revision (UBR) Number

What

The Update Build Revision (UBR) number is a unique identifier for individual updates in Windows 10 and Windows 11 operating systems. It allows IT administrators to track, monitor, and ensure that their devices are up-to-date with the latest security patches, bug fixes, and feature improvements. The UBR number is not reported by FileWave by default; however, you can use Custom Fields in FileWave to collect and report on this information.

When/Why

Keeping devices updated is crucial for maintaining security, stability, and optimal performance. By monitoring UBR numbers, IT administrators can:

1. Identify devices that are not up-to-date with the latest updates.
2. Plan and execute update deployments effectively.
3. Verify the success of update installations.
4. Maintain compliance with internal and external policies or regulations.

This is particularly relevant for Education organizations, corporations, and state and local government agencies that rely on FileWave for their Unified Endpoint Management needs.

How

Using the below PowerShell code you can get the UBR from the Registry:

```
$ubr_version = (Get-ItemProperty "HKLM:\SOFTWARE\Microsoft\Windows NT\CurrentVersion").UBR
echo "$ubr_version"
exit 0
```

Using the below PowerShell code you can see how you can get both the OS version together with the UBR if that is desired:

```
$os_version = (Get-WmiObject -Class win32_OperatingSystem).Version
$sub_build_version = (Get-ItemProperty "HKLM:\SOFTWARE\Microsoft\Windows NT\CurrentVersion").UBR
echo "$os_version.$sub_build_version"
exit 0
```

To implement this very easily simply:

1. Download the below Custom Field file: [Windows UBR.customfields.zip](#)
2. Extract the zip archive
3. In FileWave Central go to Assistants → Custom Fields → Edit Custom Fields
4. Click Import and pick the file you extracted
5. Now make sure for one or both fields that you make sure to check the box to assign it to all devices so that they can report in their values. Then you can use the Custom Fields in any Query/Report/Smart Group

Related Content

- [Custom Fields](#)
- <https://www.vcloudinfo.com/2020/12/how-to-decode-windows-version-numbers.html>
- <https://superuser.com/questions/1287950/how-to-find-the-build-ubr-kernel-version-of-windows-10-using-command-line-c>
- <https://stackoverflow.com/questions/47859658/find-the-extended-ver-information-for-remote-windows-computer>