

Software Deployment Recipes (Microsoft)

The Software Deployment Recipes (Microsoft) section provides a curated collection of practical guides and step-by-step instructions for efficiently deploying software and applications in Microsoft environments. Discover proven techniques and best practices for automating software deployments, managing configurations, and optimizing compatibility on Windows devices. Whether you're a system administrator or an IT professional, these recipes offer valuable insights to streamline your software deployment processes, enhance productivity, and ensure a seamless experience across your Microsoft devices.

- [7zip \(Windows MSI\)](#)
- [Adobe Air \(Windows EXE\)](#)
- [CrowdStrike Falcon Protection \(Windows EXE\)](#)
- [Firefox Configuration Recipe \(Windows\)](#)
- [Google Chrome Extension Management \(Windows\)](#)
- [Installing SOLIDWORKS \(Windows EXE\)](#)
- [Java \(Windows EXE\)](#)
- [Microsoft Defender Recipe \(Win\)](#)
- [Office 2019 / Office 365 \(Windows\)](#)

7zip (Windows MSI)

Description

Example recipe for deploying 7zip with new MSI parameters in FileWave 15.2.0.

Ingredients

- FW Admin
- 7zip MSI installer

i Be sure to review 7zip FAQs to use the proper install path. FileWave will force a silent install when using MSI installers.

Directions

1. Download the 7zip MSI installer from 7zip: [Download](#)
2. Upload MSI installer by creating New Desktop Fileset and choose MSI / PKG to create
3. Highlight the newly created MSI Fileset, and select Properties
4. Scroll down to the Custom MSI install options
5. Enter in the desired path for 7zip

Fileset Name: MSI - 7zip

Revision: <default> (Initial Revision) [Manage Revisions](#)

Properties Requirements Dependencies Delete Files Kiosk

☐ Requires Reboot [Message...](#) Color: Color

☐ Force reboot

Device will force reboot 2 minutes after either activation or reboot deadline (if specified) when this fileset is deployed. Warning: Forced reboots can result in a loss of unsaved data on the device, and should be used sparingly.

☐ Authenticated restart

Applies to devices with Full Disk Encryption and an escrowed Personal Recovery Key.

☐ 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](#)

Custom MSI install options

☒ Use MSI uninstaller

Custom MSI uninstall options

(Un)install options may only include property assignments like PROPERTY=VALUE separated by space. [See details](#)

[Cancel](#) [OK](#)

- Example here is installing to C:\Program Files\7-Zip
6. Click OK to save

✓ Always test deployment for both successful installation and uninstallations. If you were assigning via Self Service Kiosk, and then end users decides to uninstall, want to be sure it does uninstall successfully.

Assign to Devices

Once testing has been completed and is successful, assign your Fileset to your devices. By way of either a 'Deployment' or 'Association' within FileWave, assign the Fileset to your devices.

Related Content

- [7zip Frequently Asked Questions](#)

Adobe Air (Windows EXE)

Description

Need to deploy Adobe Air onto your Windows machines? Here is what you need to know to make that fileset.

Ingredients

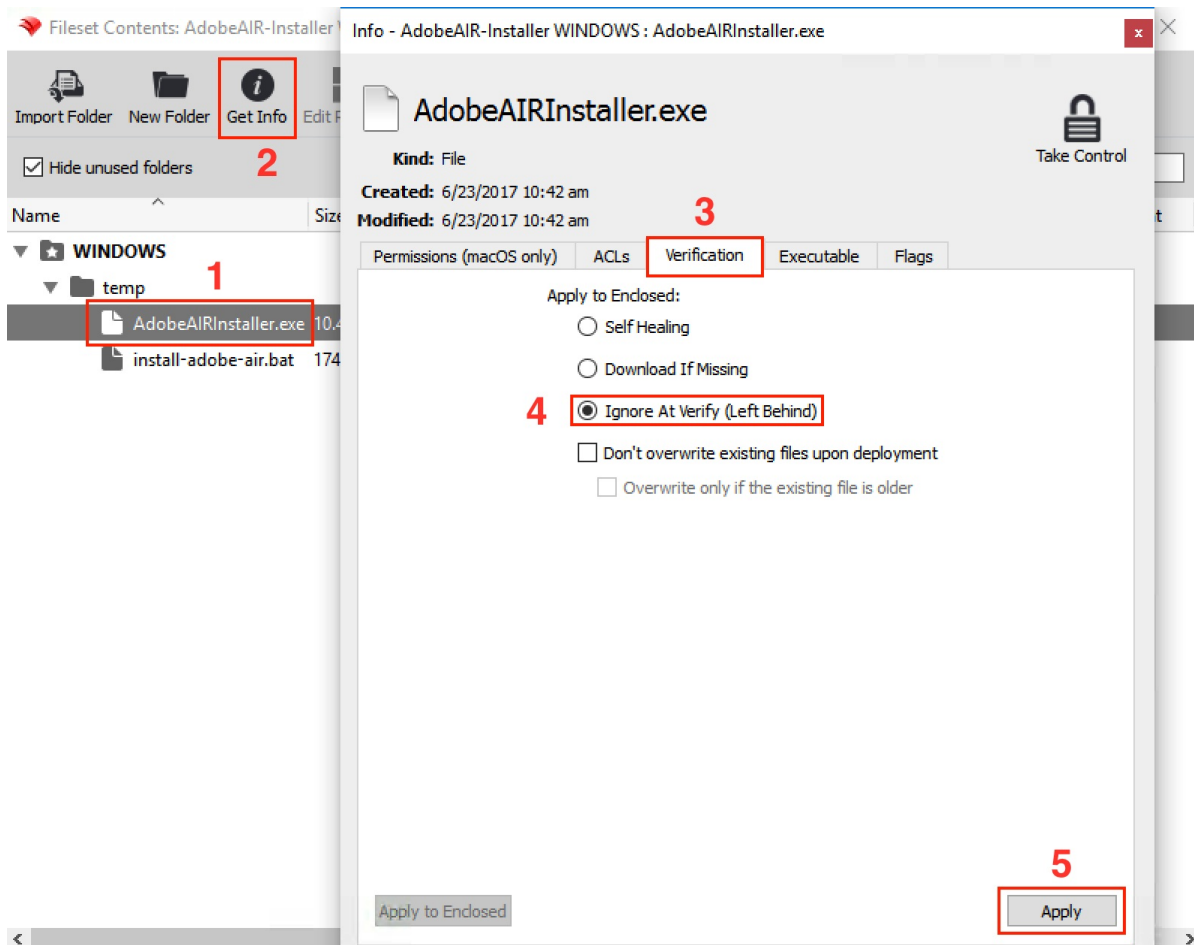
- Adobe Air installer
- FileWave Central

Directions

1. Download the most recent Adobe AIR Installer from <http://get.adobe.com/air/>
2. Extract and import the AdobeAIR-Installer.fileset.zip into FileWave Admin and open it. This fileset contains a script that calls the Adobe AIR Installer.
Starting the installation this way enables it to succeed even if no user is logged on at the target system.

```
start "" C:\Windows\temp\AdobeAIRInstaller.exe -silent
```

3. Import the "Adobe AIR Installer" into the C:\Windows\temp folder
4. Adjust the "Adobe AIR Installer.exe" verification settings to "Ignore at verify" using the "apply to enclosed" button as depicted below



5. Close the fileset and associate it to a test client

CrowdStrike Falcon Protection (Windows EXE)

Description

Needing to deploy to CrowdStrike Falcon antivirus to your Windows fleet? FileWave has you covered.

CrowdStrike's flagship product is called Falcon, which is a cloud-native platform that combines next-generation antivirus, endpoint detection and response (EDR), threat intelligence, and proactive threat hunting. Falcon aims to provide real-time visibility into endpoint activity, rapid threat detection, and automated response to security incidents.

Ingredients

- FileWave Admin Central
- CrowdStrike EXE installer
- CrowdStrike License code

Directions

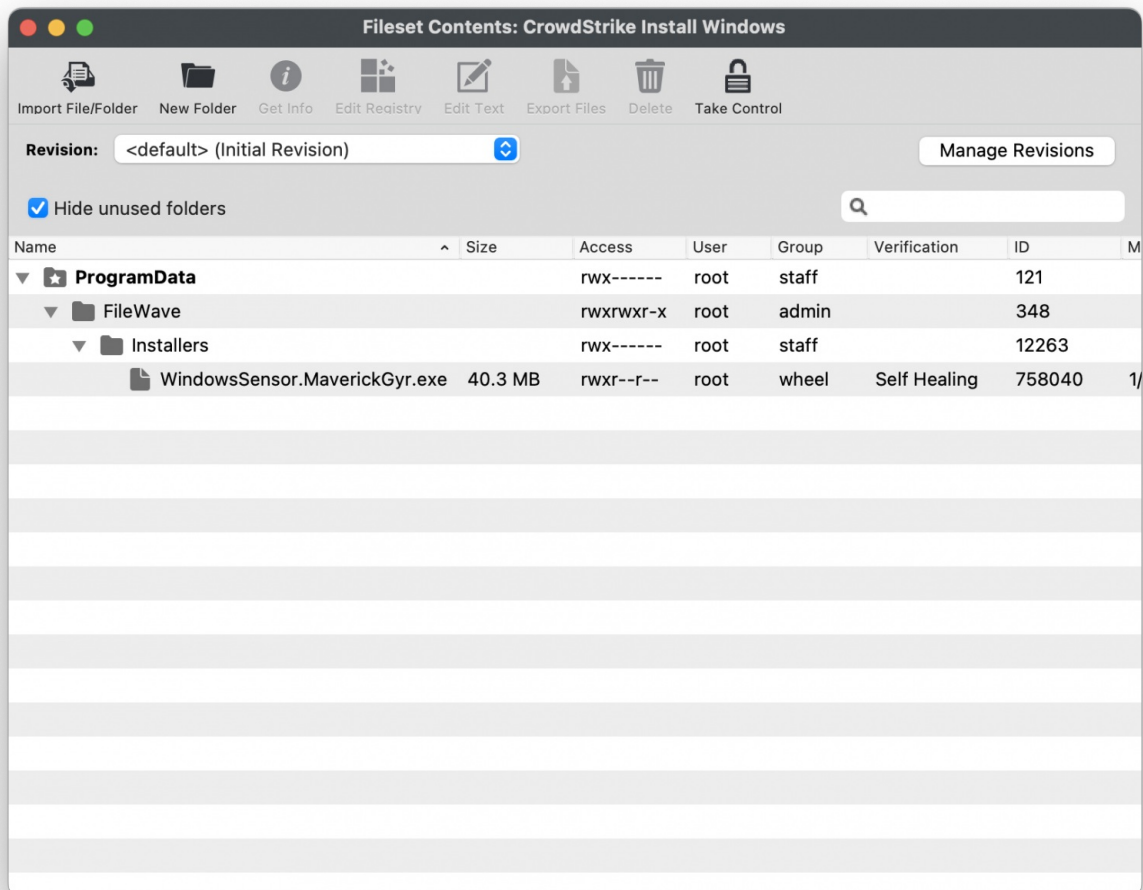
Deploying the CrowdStrike Falcon to your devices

CrowdStrike deployment for Windows devices has one Fileset. This Fileset includes an EXE with launch arguments to be customized with your CrowdStrike license code.



The Fileset included with the EXE installer is the latest version of CrowdStrike. If you have an EXE installer provided by CrowdStrike, you may replace with your own EXE installer version.

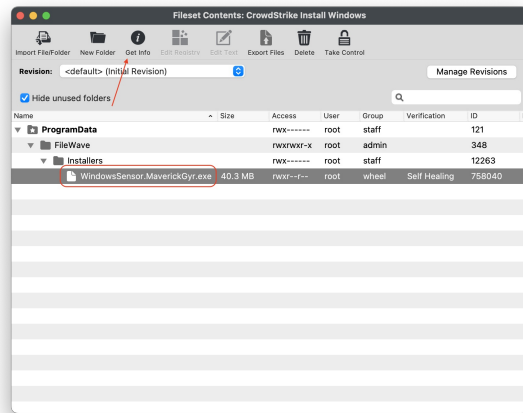
[CrowdStrike Windows Installation.fileset.zip](#)



Customizing the Installation EXE

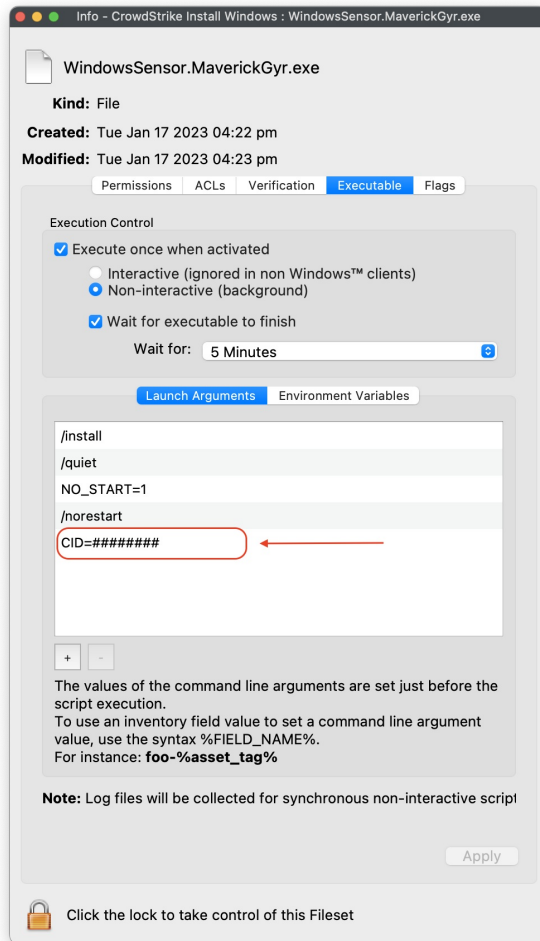
Editing the Fileset EXE

1. Highlight the CrowdStrike Windows Installation Fileset
2. Double-Click to open the Fileset Contents
3. Highlight and select the .exe file.
4. Click on 'Get Info'



Enter in your CrowdStrike License code

1. Select the tab 'Executable.'
2. Under the tab 'Launch Arguments' highlight CID=
3. Enter in your CrowdStrike License code.
4. Click the Apply to save your changes to the Launch Arguments
5. Close the Get Info Window to save your changes.



Please Note: Launch Argument NO_START=1 is intended if the desired outcome if you want CrowdStrike to start after the first reboot post-install. If not, remove NO_START=1 from the Launch Argument list.

Creating a Fileset Group

Keeping your Filesets organized is good practice, especially if there are multiple Filesets for software deployment or organization based on specific platform of deployment.

You may create a New Fileset Group, label it CrowdStrike Falcon (Windows 2023), and move the Fileset you created into this Group. Then associate the Fileset Group labeled CrowdStrike Falcon (Windows 2023) to your devices versus individual Filesets.

When ready, associate the Fileset Group labeled CrowdStrike Falcon (Windows 2023) to a few devices as a test. This is to verify and confirm that the software is installed properly based on your license code configured.

For best practice, always test a few devices before mass deployment.

Related Content

- [CrowdStrike Falcon Protection \(macOS\)](#)

Firefox Configuration Recipe (Windows)

Description

After installing Firefox, some configuration may be desirable, examples may include:

- Block auto updates
- Set home page
- Disable Mozilla First Run Pages

Firefox Documentation



The details of the Fileset are based upon: [Firefox Configuration](#)

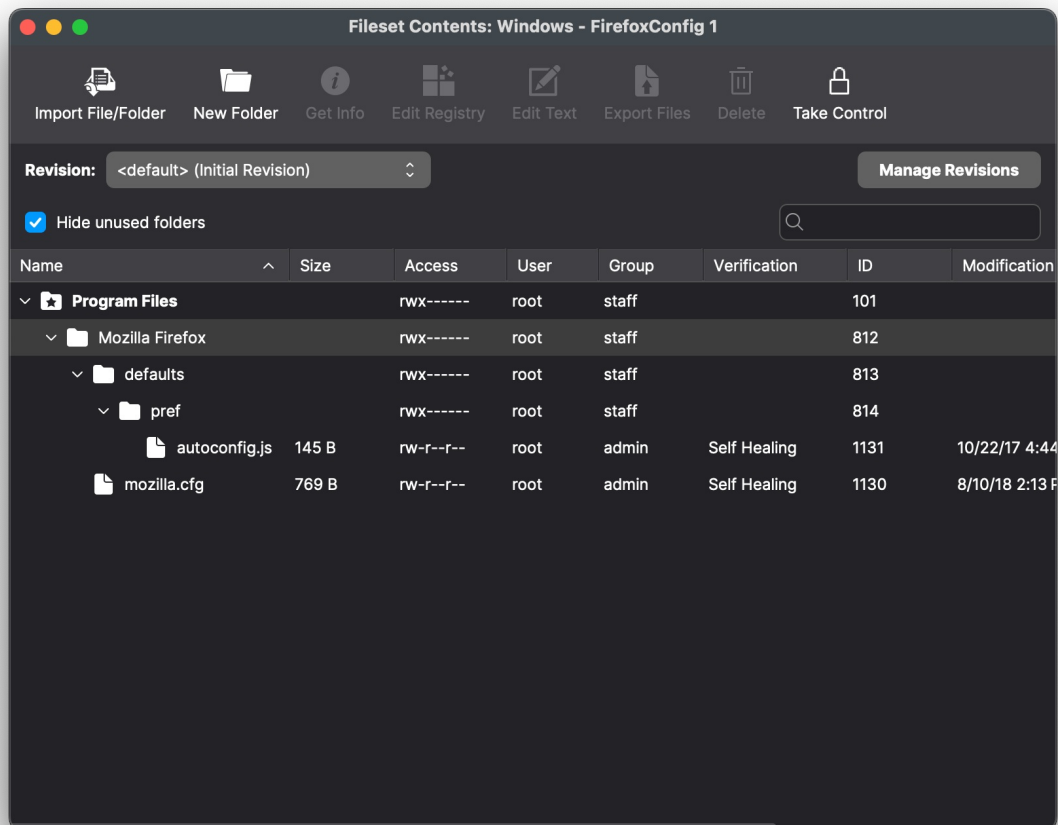
This is known to work with version 60, upwards. It may work with earlier versions, but testing on placement of files may vary with earlier versions.

Ingredients

- FW Admin
- Firefox installer application already as a Fileset
- The provided configuration Fileset: [Windows - FirefoxConfig.fileset.zip](#)

Directions

- Download the Fileset zip file, expand and drag into FileWave > Filesets
- Two files are present in the Fileset.



- The autoconfig.js file specifies the file to be used for configuration. In this Fileset the name of the file has been set to 'mozilla.cfg':

```
// Any comment. You must start the file with a comment!  
pref("general.config.filename", "mozilla.cfg");
```

```
pref("general.config.obscure_value", 0);
```

- To specify any desired settings, edit the mozilla.cfg file. The provided file is designed to prevent Firefox updates, disable privacy telemetry, disable the first run Mozilla home pages and set the user's homepage:

```
// Any comment. You must start the file with a comment!

// Disable updater
lockPref("app.update.enabled", false);
lockPref("app.update.auto", false);
lockPref("app.update.mode", 0);
lockPref("app.update.service.enabled", false);

// Set Homepage and stop Mozilla startup pages
lockPref("browser.startup.firstrunSkipsHomepage", false);
pref("browser.startup.homepage", "http://www.filewave.com");
lockPref("browser.startup.homepage_override.mstone", "ignore");

// Disable Privacy telemetry
lockPref("datareporting.policy.firstRunURL", );
lockPref("datareporting.healthreport.service.enabled", false);
lockPref("datareporting.healthreport.uploadEnabled", false);
lockPref("datareporting.policy.dataSubmissionEnabled", false);
lockPref("toolkit.telemetry.unified", false);
```

Preference Overview

Preference types can include: pref, defaultPref, lockPref, amongst others. Details can be found at: <https://support.mozilla.org/en-US/kb/customizing-firefox-using-autoconfig>

pref

This is used to set a preference that can be overridden by the user, but on next launch of the application it will revert back to the setting within the configuration file

lockPref

A lockPref cannot be overridden by the user

defaultPref

This is used to set a preference that can be overridden by the user. The user's setting will persist until the user resets them, at which point the defaultPref will be used on next launch of the application

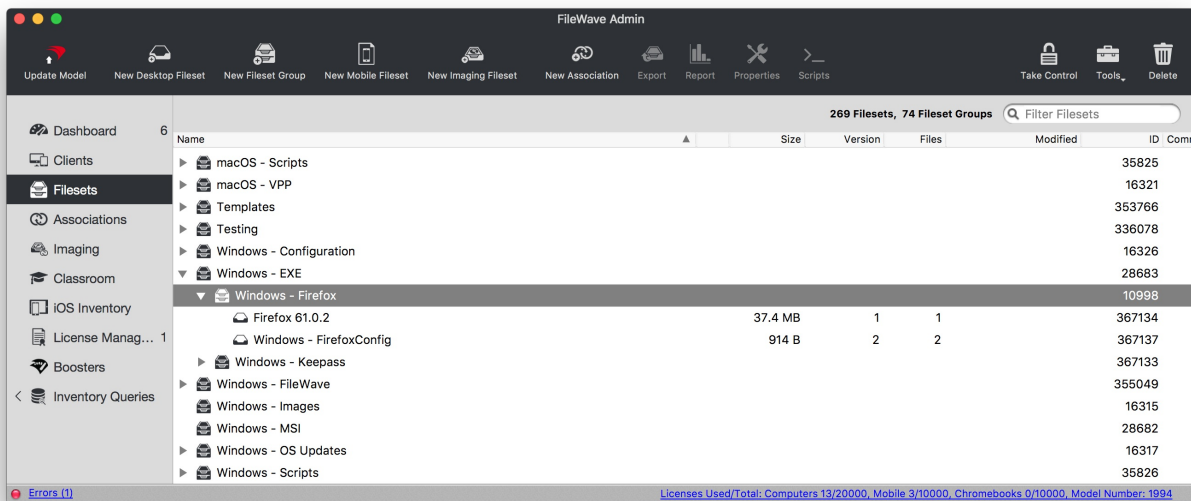


Preference Names

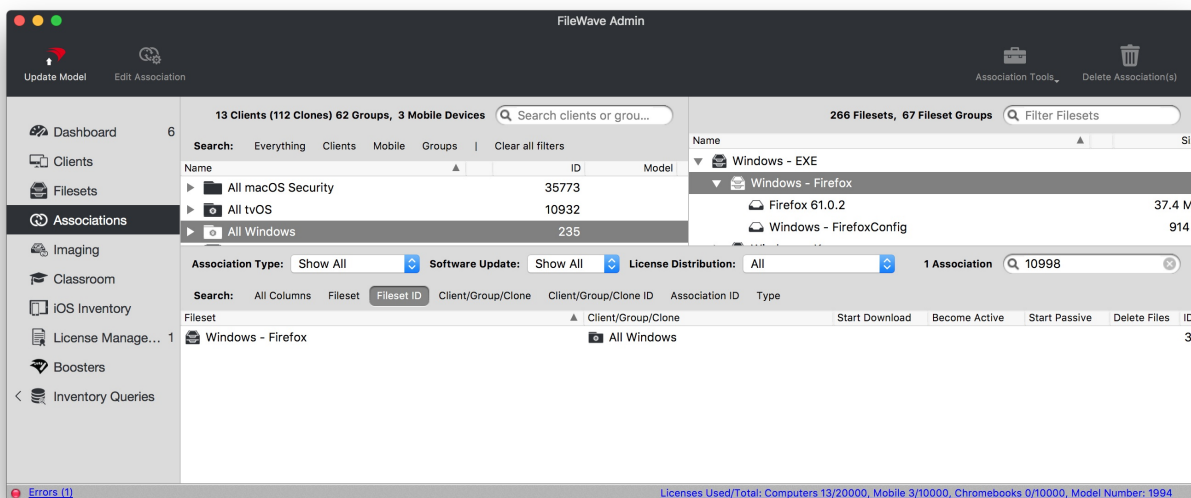
Navigating to 'about:config' in the Firefox URL bar will list all possible preference names and their values and types.

Association

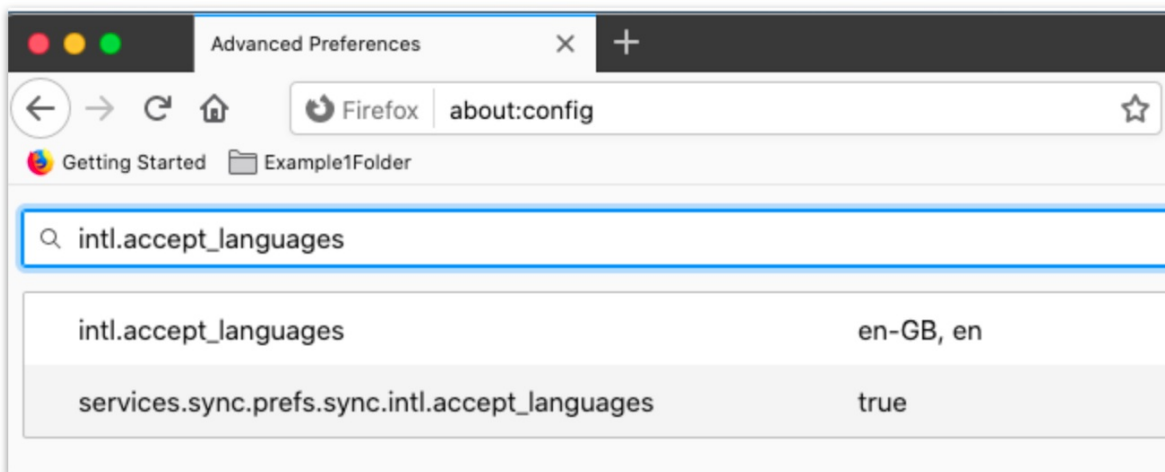
When associating, to ensure the configuration is installed with the Application, consider creating a Fileset Group:



Associating the 'Firefox' Fileset Group will ensure both the Application and Configuration are associated to devices.



When there is an update to Firefox, replace the version in the Fileset Group with the latest version after testing.



To ensure users may not circumvent management by changing the locale, enable 'BlockAboutConfig' (already set as TRUE in the template file)

Related Content

- [Firefox Configuration Recipe \(macOS\)](#)

Google Chrome Extension Management (Windows)

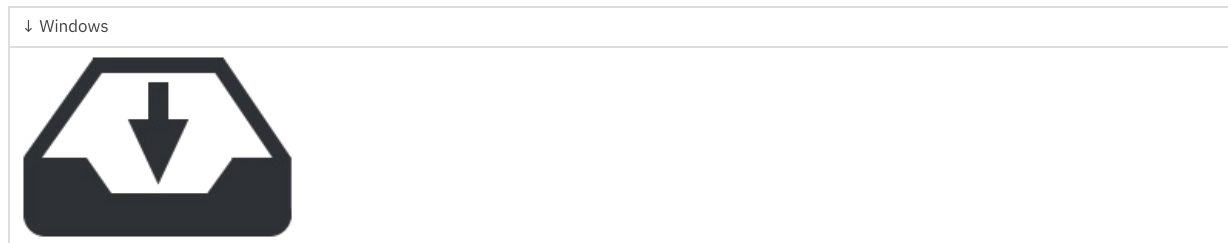
Description

Chrome Extensions, like [ClassSpaces](#), can be managed via FileWave on multiple device types.

If the Chrome browser is already managed using Google Admin Console, then all management may be applied to devices via the Google Admin Console. It is though possible to apply the management of Chrome to macOS and Windows devices via FileWave also.

Ingredients

- Chrome installation
- Provided downloads



Windows

The provided download is a basic example of a PowerShell Activation Script within a Fileset to apply ClassSpaces and block the user from other extensions. Drag and drop the Fileset into the Admin Console, associate to test devices and deploy once tested.

The script will create the necessary registry settings.

Contents of Script:

```
if ( -Not (Test-Path -Path "HKLM:\SOFTWARE\Policies\Google\Chrome\ExtensionSettings\*") ) {  
  
    New-Item -Path "HKLM:\SOFTWARE\Policies\Google\Chrome\ExtensionSettings\" -Name "*" -Force  
    New-ItemProperty -Path 'HKLM:\SOFTWARE\Policies\Google\Chrome\ExtensionSettings\*' -Name "installation_mode"  
-Value "blocked"  
  
    New-Item -Path "HKLM:\SOFTWARE\Policies\Google\Chrome\ExtensionSettings\" -Name  
"obeophmpnnhboefjagnpbllfbbaeodnn" -Force  
    New-ItemProperty -Path  
"HKLM:\SOFTWARE\Policies\Google\Chrome\ExtensionSettings\obeophmpnnhboefjagnpbllfbbaeodnn\" -Name "comment" -Value  
"ClassSpaces"  
    New-ItemProperty -Path  
"HKLM:\SOFTWARE\Policies\Google\Chrome\ExtensionSettings\obeophmpnnhboefjagnpbllfbbaeodnn\" -Name  
"installation_mode" -Value "force_installed"  
    New-ItemProperty -Path  
"HKLM:\SOFTWARE\Policies\Google\Chrome\ExtensionSettings\obeophmpnnhboefjagnpbllfbbaeodnn\" -Name "update_url" -  
Value "https://clients2.google.com/service/update2/crx"  
  
}
```



If there is already other extension management in place, the 'if' block may bypass the installation of the Extensions. If Extensions are already being managed, alter the conditions of the script appropriately.

Notes



As part of the example, an additional key has been added to block all other extensions. Remove or edit as desired

✔ If Chrome is already open, the settings will not be applied until after the browser has been restarted

Related Content

- [Google Chrome Extension Management \(macos\)](#)

Installing SOLIDWORKS (Windows EXE)

What

Need to deploy and install SolidWorks on Windows clients? Not a problem – FileWave has you covered. We need a few components from SolidWorks and some scripting tips to get deployment-ready.

Required components:

- FileWave Central
- SolidWorks Administrative Image Creator

When/Why

We will need to download and install the SolidWorks Administrative Image Creator on your Windows machine with FileWave Admin installed. This is to create the SolidWorks image that can be used for deployment and installation. You may review the SolidWorks documentation for further details on setting up and configuring here: [Creating an Administrative Image](#).

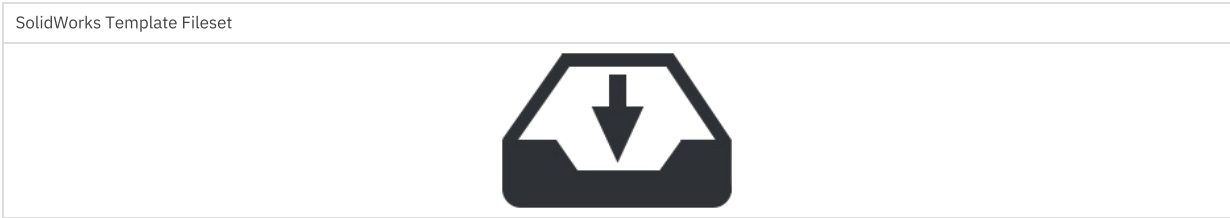
This “image” you created will be downloaded and placed onto the Windows machine under the default file path:

```
C:\SOLIDWORKS Admin\SOLIDWORKS 2022 SP2.0
```

Once completed, it will be ready to be uploaded into FileWave Admin.

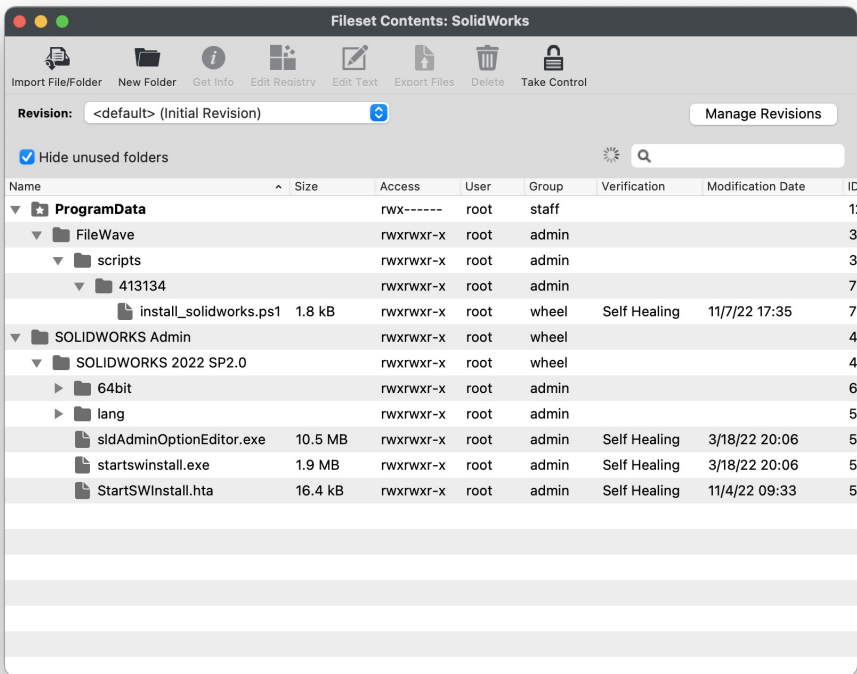
How

The SolidWorks image containing the contents of the installation will need to be uploaded into a Fileset. Below is a Fileset template with an included Powershell script to install SolidWorks and remove the shortcut links from the Users Desktop. More information on [Script Best Practices](#) and [Windows Software](#).



The

final version of the Fileset should be around 23Gb in size (with included SolidWorks image).



Here is the PowerShell script used in this Fileset.

```
#####
#SolidWorks Installation
#####

If ( [IntPtr]::Size * 8 -ne 64 )
{
    C:\Windows\SysNative\WindowsPowerShell\v1.0\PowerShell.exe -File $MyInvocation.MyCommand.Path
}
Else
{
    # Hide Wizard
    $regPath = 'Registry::HKEY_LOCAL_MACHINE\SOFTWARE\SolidWorks'
    New-Item $regPath -ErrorAction SilentlyContinue | Out-Null
    Set-ItemProperty -Path $regPath -Name UnattendedAccessWizardShown -Value 1 -Type DWord -ErrorAction
    SilentlyContinue | Out-Null
}

# Install MSI
$options = '/i', '/qb', '/s', '/v', '/qn', "C:\SOLIDWORKS Admin\SOLIDWORKS 2022 SP2.0\startswinstall.exe"

echo "Installing with options: $options"

Start-Process -FilePath "C:\SOLIDWORKS Admin\SOLIDWORKS 2022 SP2.0\startswinstall.exe" -ArgumentList $options -
NoNewWindow -Wait -PassThru

# Remove Desktop Icon
Remove-Item -Path "C:\Users\Public\Desktop\SOLIDWORKS 2022.lnk" -ErrorAction SilentlyContinue
Remove-Item -Path "C:\Users\Public\Desktop\eDrawings 2022 x64 Edition.lnk" -ErrorAction SilentlyContinue
Remove-Item -Path "C:\Users\Public\Desktop\SOLIDWORKS Composer 2022.lnk" -ErrorAction SilentlyContinue
Remove-Item -Path "C:\Users\Public\Desktop\SOLIDWORKS Composer Player 2022.lnk" -ErrorAction SilentlyContinue
Remove-Item -Path "C:\Users\Public\Desktop\SOLIDWORKS Electrical.lnk" -ErrorAction SilentlyContinue
Remove-Item -Path "C:\Users\Public\Desktop\SOLIDWORKS Manage 2022.lnk" -ErrorAction SilentlyContinue
Remove-Item -Path "C:\Users\Public\Desktop\SOLIDWORKS Visualize 2022.lnk" -ErrorAction SilentlyContinue

#####
#End
#####
```

Java (Windows EXE)

Description

This recipe shows you the steps you need to follow to make a Java Fileset for Windows.

Ingredients

- FileWave Central
- Java Installer (EXE)


Directions

1. Download the offline EXE update from: [Oracle Download Page](#)
2. Create an empty Fileset and drag the Java install EXE to an appropriate location, e.g. ProgramData > fwEXE
3. Select the EXE and choose Get Info > Executable
4. Set to 'Execute once when activated'
5. Add the below Launch Argument to silently instal and remove older installed versions

```
"/s REMOVEOUTOFDATEJRES=1"
```

6. Test

Info - Java 8u371 : jre-8u371-windows-x64.exe

 jre-8u371-windows-x64.exe

Kind: File

Created: Fri Jun 16 2023 02:59 pm

Modified: Fri Jun 16 2023 02:59 pm

PermissionsACLsVerificationExecutableFlags

Execution Control

☒ Execute once when activated

- ☐ Interactive (ignored in non Windows™ clie
- ☒ Non-interactive (background)
- ☐ Wait for executable to finish

Wait for: Infinite

Launch ArgumentsEnvironment Variables

```
"/s REMOVEOUTOFDATEJRES=1"
```


+

-

The values of the command line arguments are set just before the script execution.
To use an inventory field value to set a command line argument value. use the svntax

Note: Log files will be collected for synchronous non-

Apply

 Click the lock to take control of this Fileset

Digging Deeper

Oracle's Configuration Documentation

Applicable to online and offline installers only (.exe files and wrappers). Enables uninstallation of existing out-of-date JREs during JRE install.

REMOVEOUTOFDATEJRES

- REMOVEOUTOFDATEJRES=0 leaves all out-of-date Java versions on the system.
- REMOVEOUTOFDATEJRES=1 removes all out-of-date Java versions from the system.

For example, running jre1.8.0_60.exe /s REMOVEOUTOFDATEJRES=1 will remove all JREs below the security baseline.

JREs above the security baseline will not be uninstalled.



Details of baseline may be observed from Oracle's release notes:

<https://www.oracle.com/technetwork/java/javase/8all-relnotes-2226344.html>



Legacy Installers

Although recommendation is to always use the latest version, legacy versions are available from [Oracle's archive](#)

Microsoft Defender Recipe (Win)

Description

Example recipe for deploying Microsoft Defender.

Ingredients

On Windows devices this is relatively straight forward. Just a couple of items required:

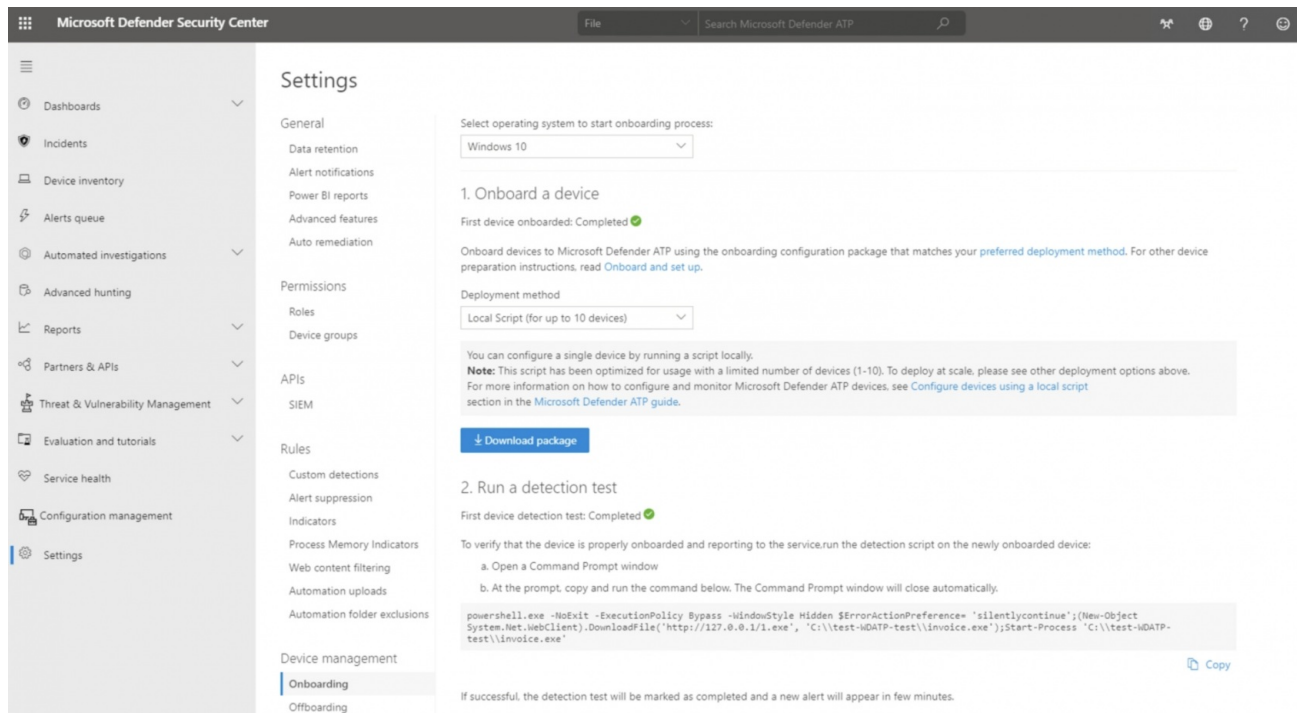
- Deployment Script: WindowsDefenderATPLocalOnboardingScript.bat
- Below provided Fileset

Downloads:

- [Microsoft Defender Installer/Uninstaller Filesets](#)

See below directions for deployment before associating with devices.

Microsoft Defender deployment script is available through the M365 Defender portal; [details in the Microsoft Deployment KB](#):



The 'WindowsDefenderATPLocalOnboardingScript.bat' is built by Microsoft with the appropriate licence code embedded into the script, such that the download is personal to the logged in account, when downloading.

It can be seen in the script from the line commencing as below:

```
REG add "HKLM\SOFTWARE\Policies\Microsoft\Windows Advanced Threat Protection" /v OnboardingInfo /t REG_SZ /f /d "{\body\": \"{{previousOrgIds\\\": [], \\\"orgId\\\": \\\"\"
```

Directions

Download the example Fileset and import into FileWave

Script: WindowsDefenderATPLocalOnboardingScript.bat

Edit the text of the provided 'WindowsDefenderATPLocalOnboardingScript.bat' file within the Fileset and paste in a copy of the script contents downloaded from Microsoft:

Name	Size	Access	User	Group	Verification
▼ ProgramData		rwx-----	root	staff	
▼ FileWave		rwxrwxr-x	root	admin	
▼ scripts		rwxrwxr-x	root	admin	
▼ 781527		rwxrwxr-x	root	admin	
WindowsDefenderATPLocalOnboardingScript.bat	116 B	rwxrwxr-x	root	wheel	Self Healing

WindowsDefenderATPLocalOnboardingScript.bat

Copy contenst of downloaded WindowsDefenderAPTLocalOnboardingScript.bat into this file. This line may be removed.

Assign to Devices

By way of either a 'Deployment' or 'Association' within FileWave, assign the Fileset to one or more test devices and once happy expand this to more devices.

Office 2019 / Office 365 (Windows)

Description

Need to deploy Microsoft Office 2019 or Office 365 onto your Windows machines? We've got you covered!

Note the Fileset below is based from the Microsoft Article listed here: <https://docs.microsoft.com/en-us/deployoffice/office2019/deploy>

Ingredients

- FileWave Central
- [Office Deployment Tool](#)
- [Office Config XML](#)
- [Office 2019 Fileset Template](#)

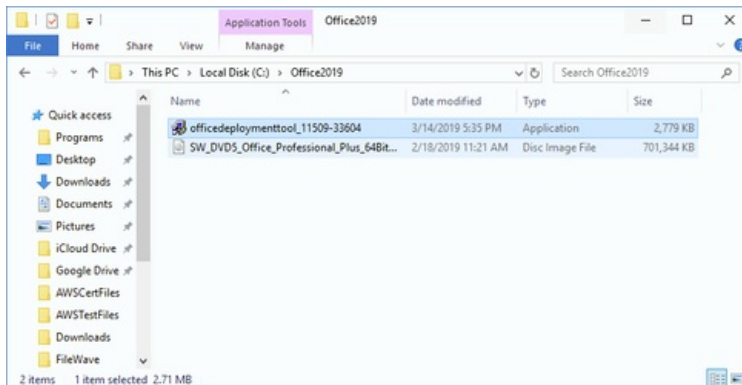
This Fileset utilizes scripts to install and uninstall Office. After the Fileset is deployed and activated it can take a few minutes for the Office installation to be completed. When the Office Fileset is removed from the device (by removing the association in FileWave) a script will start that will uninstall Office from the clients.

For Office 365 just substitute Office 365 in place of Office 2019 where it's mentioned below

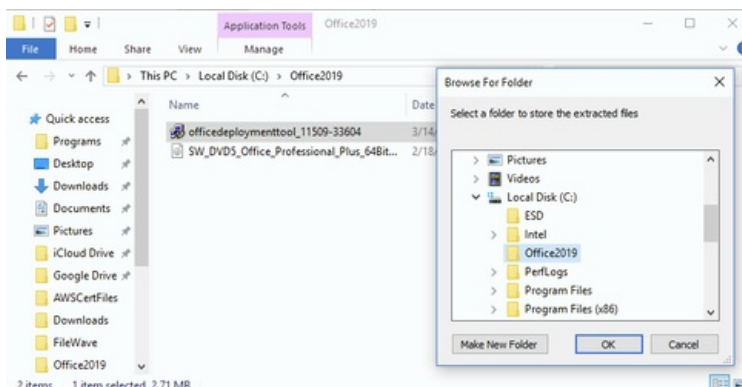
Directions

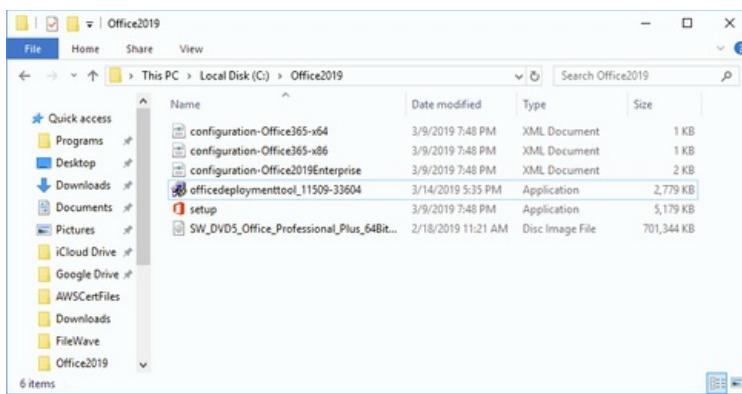
These directions assume you are creating an Office2019 folder on your local C:\ drive and you name the XML NewConfiguration. If you change the folder location, folder name, or XML name make sure you modify the steps below with your modifications.

- Download the Office Deployment Tool from the site below:
<https://www.microsoft.com/en-us/download/details.aspx?id=49117>

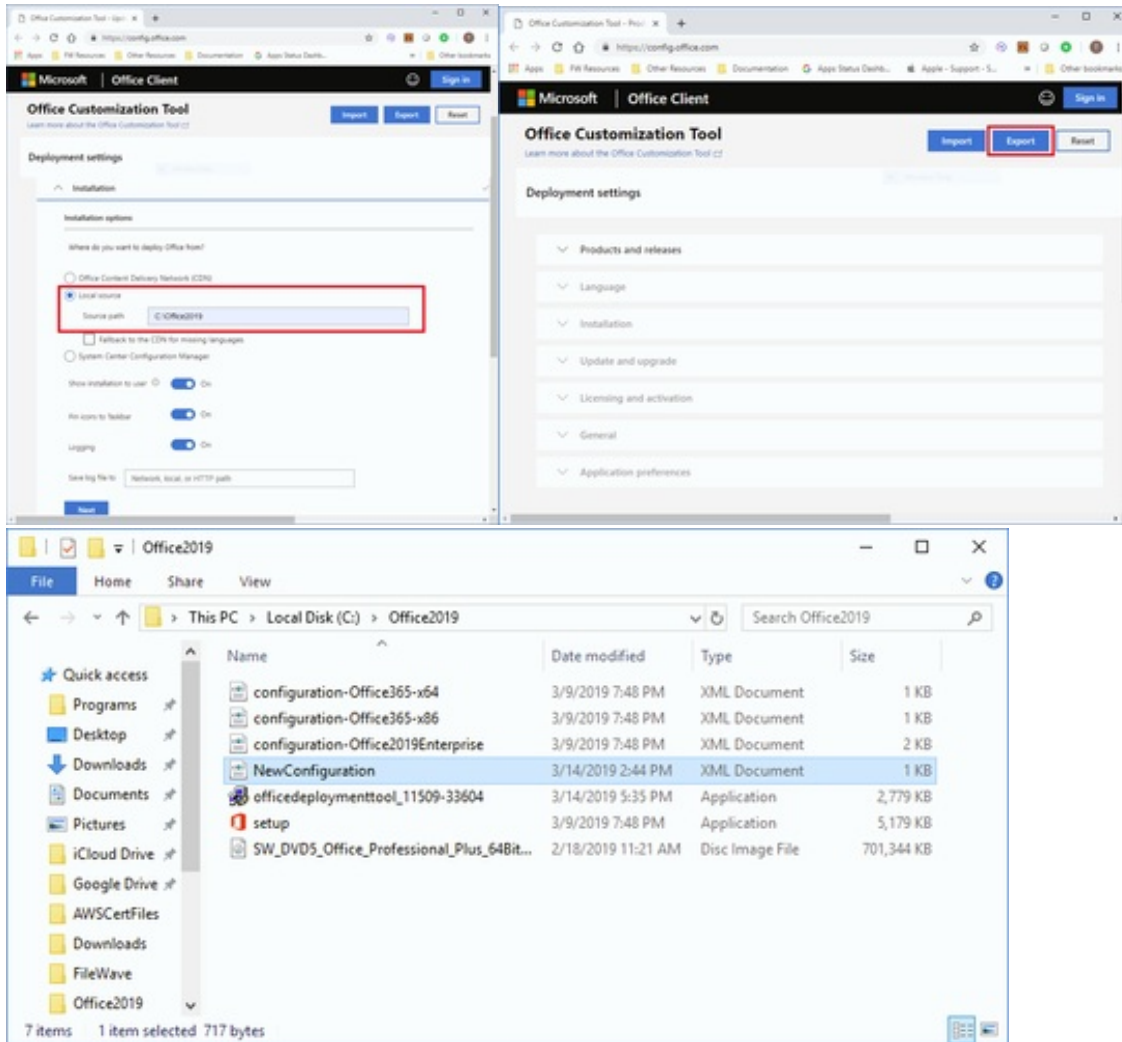


- Run the Office Deployment Tool to get the setup.exe and example configuration files





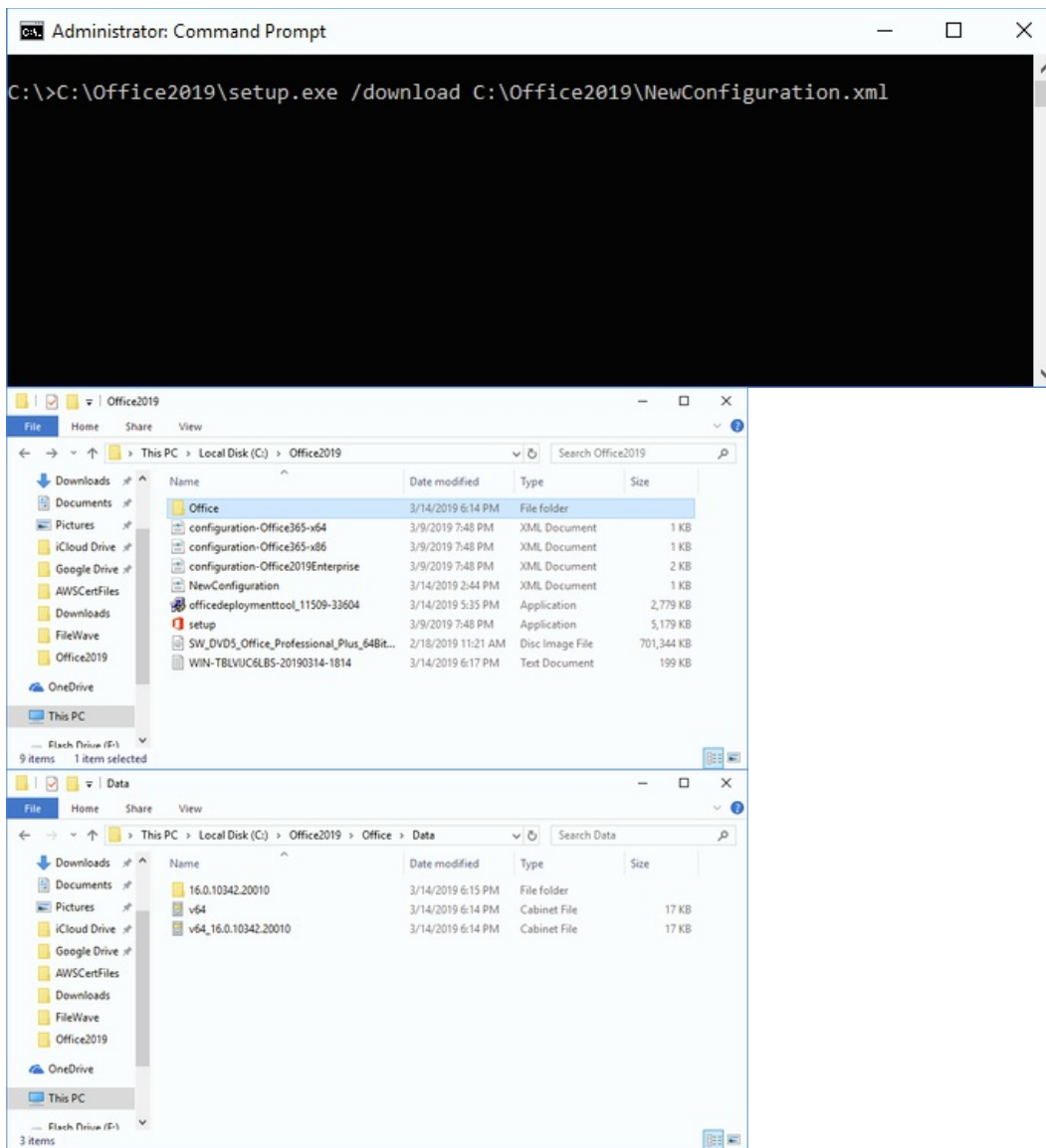
- Create a Configuration XML with information specific to your Office install. Make sure the source is not the CDN use local location C:\Office2019 and name the XML "NewConfiguration"
<https://config.office.com/>



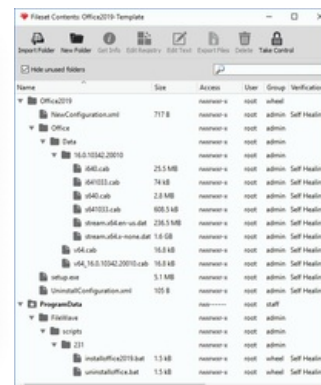
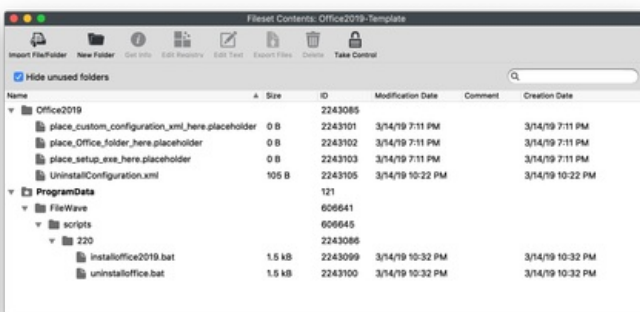
- Open command prompt and run the following command:

```
C:\Office2019\setup.exe /download C:\Office2019\NewConfiguration.xml
```

This is assuming you ran the deployment tool to a folder in the C:\ drive called Office2019 and you also added the xml to the same folder from earlier steps. This command will download from Microsoft a folder called "Office" with configuration files that you will need to install Office on your clients



- Download the [Office2019-Template.fileset.zip](#) from this KB and upload to FileWave
- Replace the placeholder files in the template with the Office folder and setup.exe you get from running the deployment tool in step 2. Also upload the XML you created in step 3 (if you did not name the xml NewConfiguration then you need to update the `instaloffice2019` script in the Fileset with that new name)



- Deploy the Office Fileset to your Windows devices and Office will be finished installing a few minutes after the Fileset activates
- If you delete the association for the Office2019 Fileset then the pre-uninstallation script will run and uninstall Office2019