(Windows) How to Deploy the CrowdStrike Falcon Sensor with Microsoft Intune

Created 7-20-21 by Anthony Mogannam (Amog)

Tested with Windows Sensor version 6.26.14003 and Microsoft Intune Service Release 2106

Best effort - CrowdStrike Support cannot assist with Microsoft Intune technical questions or troubleshooting. Use at your own risk

Introduction

Microsoft Intune is a fine solution for deploying and managing software packages however a few key caveats must be noted.

- The CrowdStrike Falcon Sensor is downloaded from within the Falcon Console in exe format.
- Microsoft Intune does not allow exe files to be deployed directly. Files must be converted to a supported format.
- This can be easily done by utilizing a Microsoft supplied utility known as the **Microsoft Win32 Content Prep Tool**, which available on GitHub here: https://github.com/microsoft/Microsoft-Win32-Content-Prep-Tool/blob/master/IntuneWinAppUtil.exe
    - This command line tool will archive and compress the Falcon Sensor exe file into a **.intunewim** file, which will be uploaded into Intune and deployed to selected endpoints.
- Once converted, the process of deploying with Intune is fairly straightforward and quick.
- The software package created here can be used for both **Installation and removal** of the sensor through Microsoft Intune.
- The CrowdStrike Sensor deploys silently on all endpoints and does not require a reboot.
- The same Falcon Sensor is used for Servers and Workstations alike.

Downloading the Falcon Sensor

The CrowdStrike Falcon Sensor for Windows is available for download directly within the Falcon Console. This can be found by navigating to ***Hosts Sensor Downloads***.

Take note of your Customer ID. This identifier is unique to your organization and is required during deployment to link each individual Sensor deployed to your individual instance of CrowdStrike Falcon.

Q Search

Share feedback on this menu

Bookmarks
Go to the pages, reports, and searches you use often and bookmark them.

Activity
Dashboard
Incidents
Detections
Quarantined Files
Remediation
Real Time Response
Firewall

Investigate
Host Search
Hash Search
User Search
IP Search
Hash Execution Search
Bulk Domain Search
Bulk Host Audit
USB Device Control
Event Search

Hosts
Dashboard
Host Management
Groups
Zero Trust Assessment New
Sensor Downloads
Installation Tokens

Configuration
Prevention Policies
Custom IOA Rule Groups
Detections Management
Exclusions
IOC Management New
Firewall Policies
Firewall Rule Groups
USB Device Policies
Response Policies
Response Scripts & Files
Containment Policy
Sensor Update Policies
General Settings
Notification Workflows
Activity Log
Audit Log

Dashboards
All Dashboards
Private Dashboards
Shared Dashboards
Preset Dashboards
Legacy Dashboards
Scheduled Reports New

Discover
Overview
Application Usa
Application Usa
Application Usa
Asset Inventory
MAC Address S
Managed Asset
System Resourc
Drive Encryptio
Account Monito
Account Search
Failed Logon At
Amazon Web Se

Cloud Security
Kubernetes Protection

Spotlight
Dashboard

Intelligence
Dashboard

MalQuery
Search

Falcon Users
User Management

CrowdStrike
All Apps

Sensor Downloads

Download Latest Sensor

HOW TO INSTALL
1. Download the latest sensor installer for your platform.
2. Copy your Customer ID checksum to enter during install:

XXXXXXXXXXXXXXXXXXXXXXXXXXXXXX-XX   Take note of your Customer ID

3. Run the installer on the endpoint.
For installing via systems management tool or reusable Virtual Machine images, see the Deployment Guides.

ADDITIONAL INFO
See Tool Downloads for uninstallers, SIEM connectors, and other tools.
Looking for an older version? See other supported versions.

Windows

Windows - 6.25.13909
Release date: Jul. 2, 2021
SHA256: 8ae9f2b6593bf0a2aebe200e98cbf82b421c057064deea054cff9ddf49eb21c8
Older versions   DOWNLOAD

Mac

macOS - 6.25.13807
Release date: Jul. 7, 2021
SHA256: a41bb75e4c78e35206e4888b771d9f12384a5d53ef608b49c59b259dd8f4f868
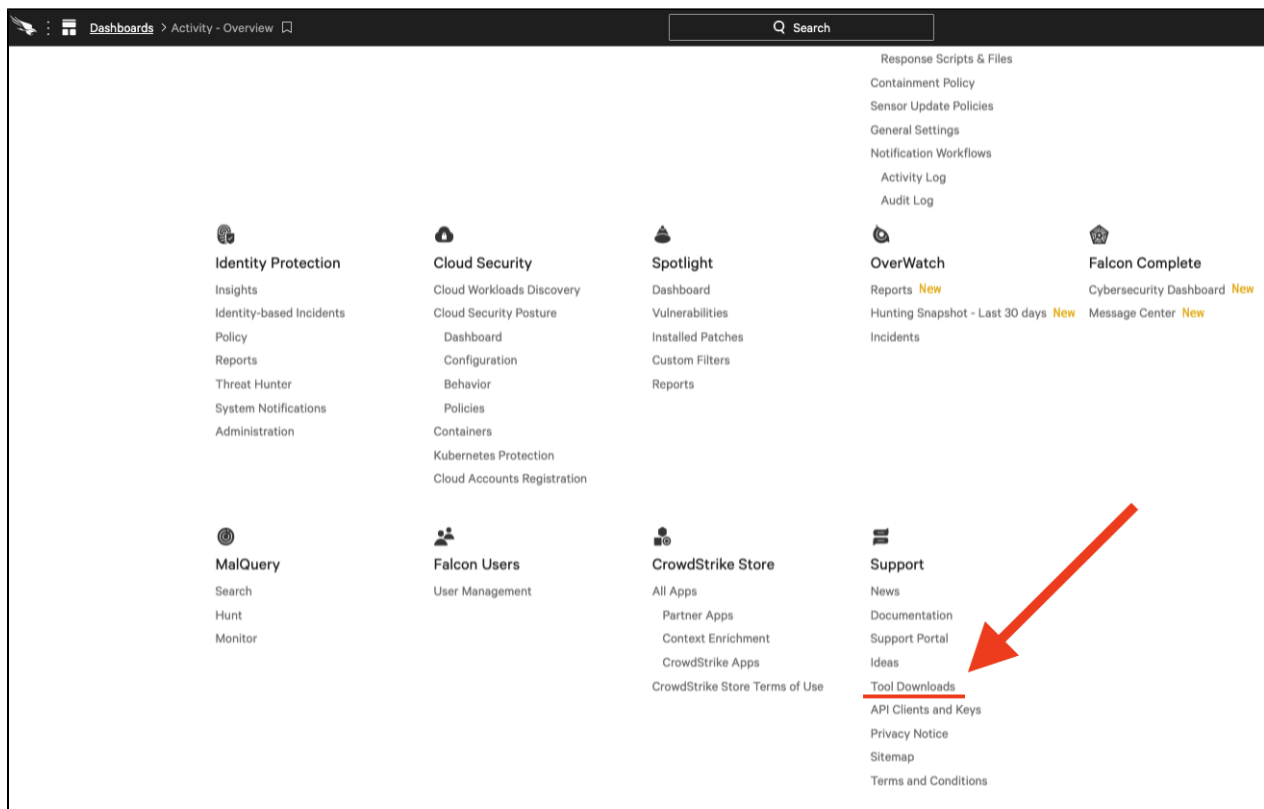Older versions   DOWNLOAD

Linux - Ubuntu

Downloading the Falcon Uninstall Tool (optional)

The software package created in the steps ahead can be used for installation and removal of the sensor through Microsoft Intune. **If you do not wish to use the same package for both installation and removal,** *skip this step.*

The Windows Sensor Uninstall Tool is available for download directly within the Falcon Console. This can be found by navigating to *Support Tool Downloads.*

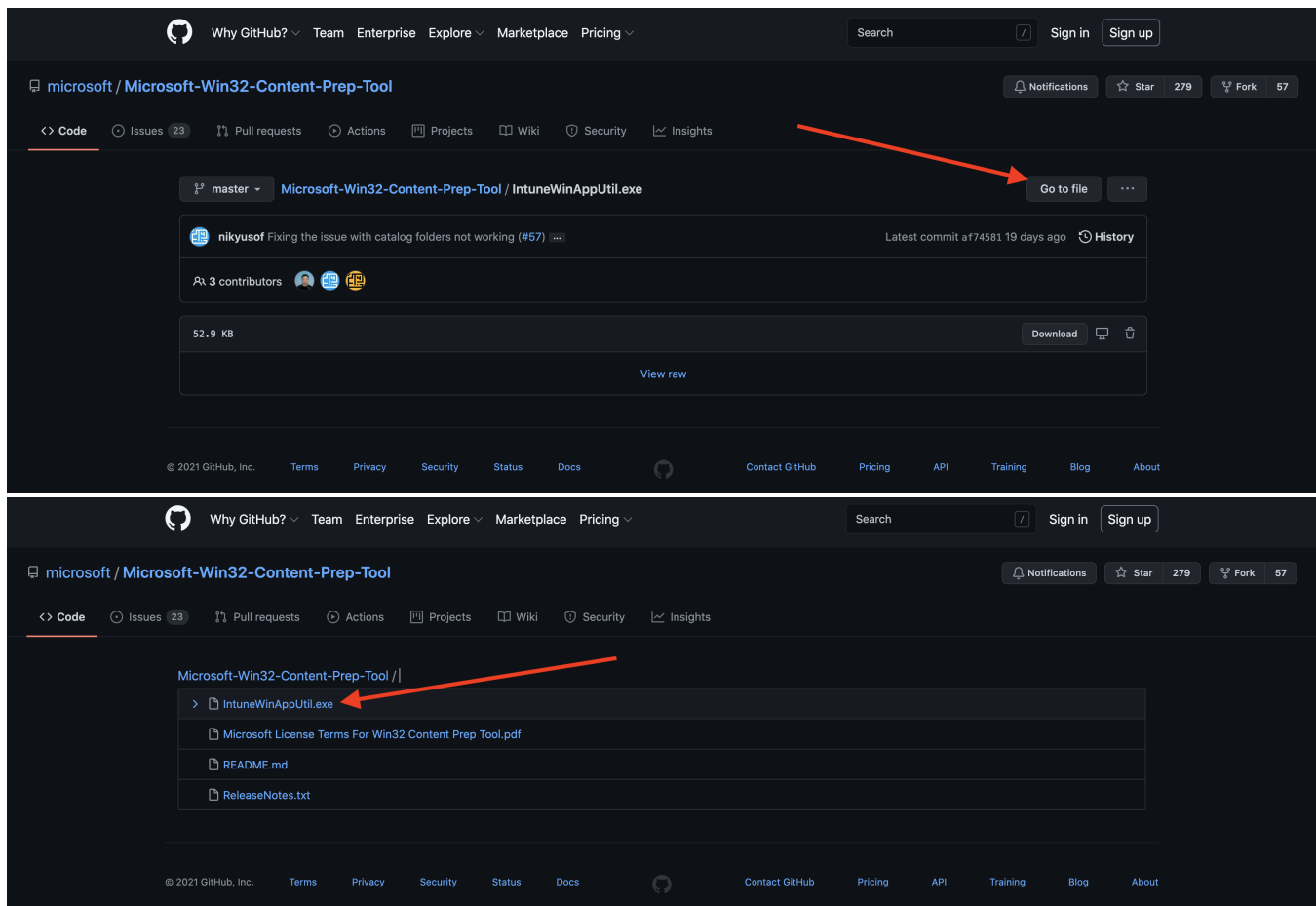The Falcon Windows Sensor Uninstall Tool is found at the bottom of the page.

Compressing and Archiving the exe Files into .intunewim

Navigate to the Microsoft GitHub and download the **Microsoft Win32 Content Prep Tool**

GitHub: https://github.com/microsoft/Microsoft-Win32-Content-Prep-Tool/blob/master/IntuneWinAppUtil.exe

Place _both_ the Falcon Sensor and the Uninstall Tool file into a dedicated folder together. (eg *Desktop\Falcon\FalconSensor.exe, *Desktop\Falcon\CSUninstallTool.exe). This is important as the entire contents of the selected folder will be archived.

From the Command Prompt, run IntuneWinAppUtil.exe and proceed through the following prompts, entering the appropriate information as needed.

- Source folder: The folder housing the Falcon Sensor and Uninstall Tool executables
- Setup file: The Falcon Sensor executable file (Only the Falcon Sensor itself, not the Uninstall Tool)
- Output folder: Location where the .intunewim file will be saved
- Specify catalog folder: Should be marked N. Only needed when deploying software to an endpoint running Windows 10 S mode

Once completed, you will be able to find the new .intunewim file in the folder you specified.

```
Administrator: Command Prompt - C:\Users\demo\Desktop\IntuneWinAppUtil.exe                    —   □   ✕

Microsoft Windows [Version 10.0.17763.1935]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\demo>C:\Users\demo\Desktop\IntuneWinAppUtil.exe
Please specify the source folder: C:\Users\demo\Desktop\Falcon
Please specify the setup file: C:\Users\demo\Desktop\Falcon\WindowsSensor.exe
Please specify the output folder: C:\Users\demo\Desktop
Do you want to specify catalog folder (Y/N)?N_
```

```
Select Administrator: Command Prompt                                                          —   □   ✕

INFO    Computed SHA256 hash for C:\Users\demo\AppData\Local\Temp\2\570c53cd-d836-4450-826c-b560e3888ffe\IntuneWinPackage
\Contents\IntunePackage.intunewin within 922 milliseconds
INFO    Copying encrypted file from 'C:\Users\demo\AppData\Local\Temp\2\570c53cd-d836-4450-826c-b560e3888ffe\IntuneWinPac
kage\Contents\c0c62102-1e1e-4faa-8fee-50d87591cc1e' to 'C:\Users\demo\AppData\Local\Temp\2\570c53cd-d836-4450-826c-b560e
3888ffe\IntuneWinPackage\Contents\IntunePackage.intunewin'
INFO    File 'C:\Users\demo\AppData\Local\Temp\2\570c53cd-d836-4450-826c-b560e3888ffe\IntuneWinPackage\Contents\IntunePac
kage.intunewin' got updated successfully within 153 milliseconds
INFO    Generating detection XML file 'C:\Users\demo\AppData\Local\Temp\2\570c53cd-d836-4450-826c-b560e3888ffe\IntuneWinP
ackage\Metadata\Detection.xml'
INFO    Generated detection XML file within 31 milliseconds
INFO    Compressing folder 'C:\Users\demo\AppData\Local\Temp\2\570c53cd-d836-4450-826c-b560e3888ffe\IntuneWinPackage' to
'C:\Users\demo\Desktop\Falcon\WindowsSensor.intunewin'
INFO    Calculated size for folder 'C:\Users\demo\AppData\Local\Temp\2\570c53cd-d836-4450-826c-b560e3888ffe\IntuneWinPack
age' is 63198012 within 1 milliseconds
INFO    Compressed folder 'C:\Users\demo\AppData\Local\Temp\2\570c53cd-d836-4450-826c-b560e3888ffe\IntuneWinPackage' succ
essfully within 674 milliseconds
INFO    Removing temporary files
INFO    Removed temporary files within 10 milliseconds
INFO    File 'C:\Users\demo\Desktop\Falcon\WindowsSensor.intunewin' has been generated successfully


[===============================================]   100%
INFO    Done!!!


C:\Users\demo>_
```

Configuring the Sensor Package within Microsoft Intune

Within Intune, Navigate to *Apps All Apps Add*. Under App Type, select Windows App (Win32). Select the App Package File you created in the previous step.

In the following screens, you are only required to fill in fields marked by * but should follow your organization's guidelines for software deployment.

In **App information**, enter a Name and Publisher for the sensor package, then click Next.

In **Program**, the Install Command and Uninstall Command must be entered.

- The default command for installation is as follows: ***<installer_filename> /install /quiet /norestart CID=XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX-XX***

- The default command for uninstall is as follows: ***CsUninstallTool.exe /quiet***

Install Behavior should be set to System. This executes the installation with administrative rights.

Device Restart Behavior should be set to No Specific Action. The Falcon Sensor does not require a reboot upon deployment.

Return Codes can be left as default.

- Your unique Customer ID (CID) can be found within the Falcon Console on the Sensor Downloads Page.
- For more information on the installation, uninstall, or general workings of the Falcon Sensor, please reference the **Falcon Sensor for Windows** guide located within the Falcon Platform at *Support Documentation Falcon Sensor for Windows*.

In **Requirements**, you will have to set <u>Operating System Architecture</u> and <u>Minimum Operating System</u> accordingly.

In Detection Rules, you will set a parameter for Intune to identify whether the Falcon Sensor is deployed on the endpoint.

Under **Rules Format**, select <u>Manually Configure Detection Rules.</u>

- Rule Type: File
- Path: C:\Program Files\CrowdStrike
- File or Folder: CSFalconController.exe
- Detection Method: File or Folder Exists

The **Dependancies** and **Supersedence** settings are not required and can be skipped.

In **Assignments**, choose to add an individual Asset Group or All Users under **Required.** This will force install the sensor on all included endpoints.

Review the sensor setting and confirm. Once confirmed, the .intunewim file will be uploaded and you will be notified when the app is ready.

The Sensor will be pushed to the endpoints automatically upon the next Intune Sync cycle. You can also choose to manually initiate a Sync.