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:

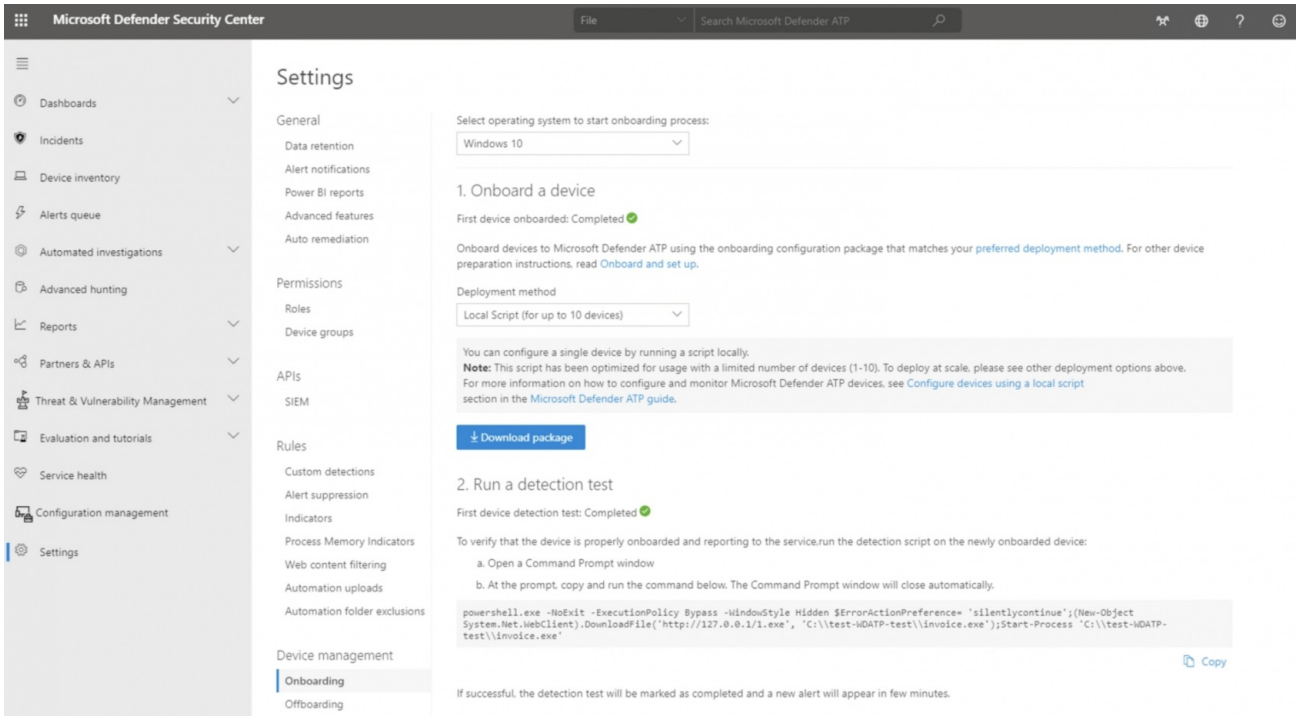
- Deployment Script: WindowsDefenderATPLocalOnboardingScript.bat
- Below provided Fileset

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\\\":\\\"
```

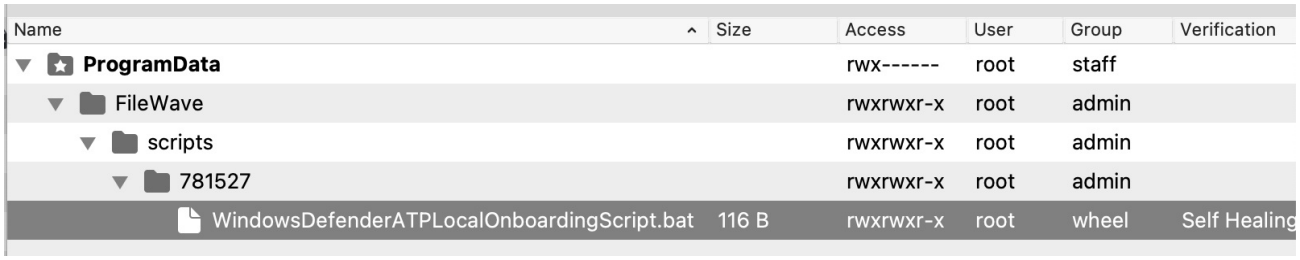
Directions

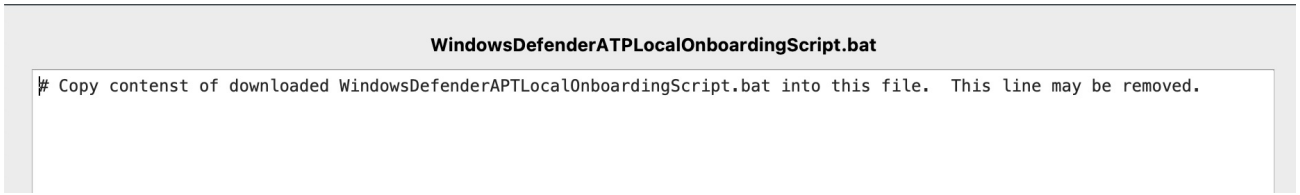
Download the example Fileset and import into FileWave

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:





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.

Revision #2
★Created 27 September 2023 07:49:44 by Sean Holden
Updated 2 November 2023 13:53:30 by Sean Holden