Microsoft Defender Recipe (macOS)

Description

Example recipe for deploying Microsoft Defender.

Ingredients

The list is actually quite extensive, due to the necessary payloads:

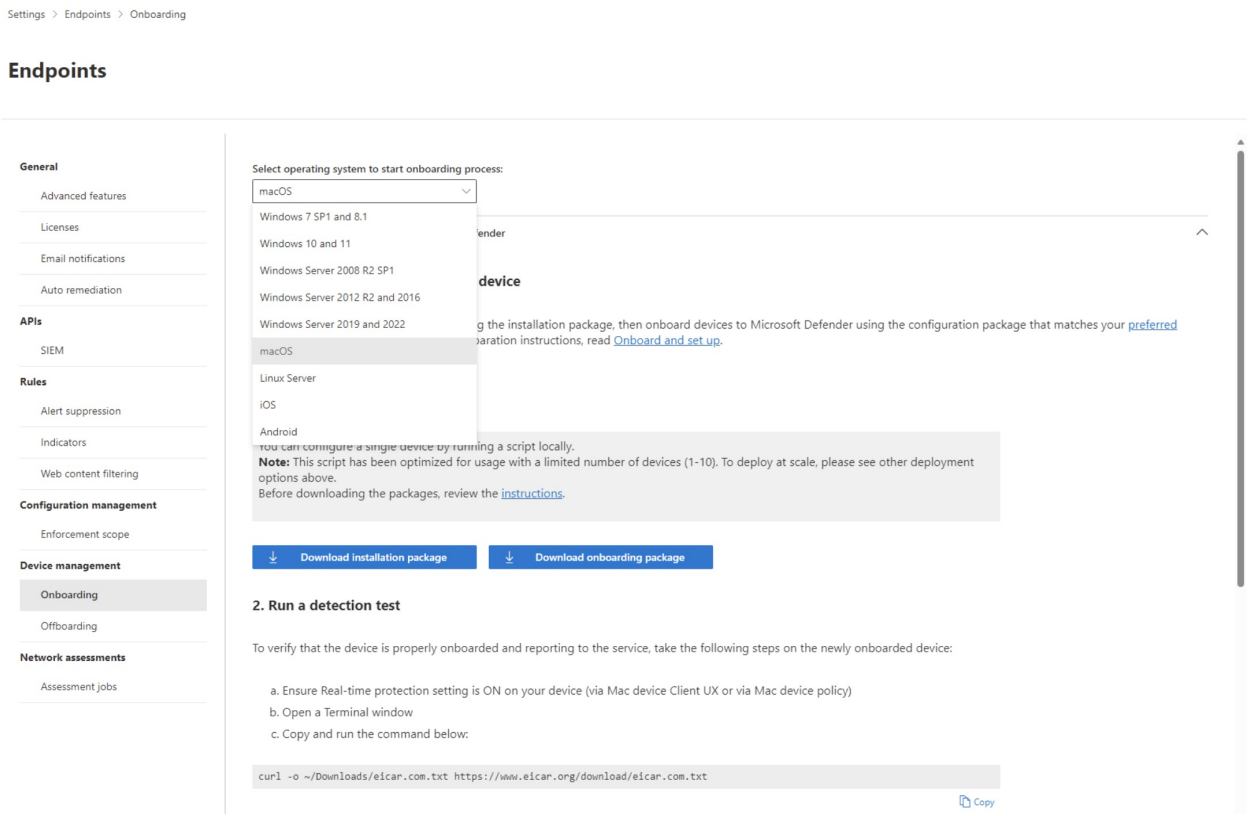
- Microsoft Defender PKG
- Deployment Script: MicrosoftDefenderATPOnboardingMacOs.sh
- Below provided Fileset
- Profiles for:
  - Web Content Filter
  - TCC allowances
  - Notifications
  - Data Acceptance & Autoupdater
  - System and Kernel Extensions

Downloads:

- Microsoft Defender Installer/Uninstaller Filesets
- Microsoft Defender Profiles

> See below directions for deployment before associating with devices.

Microsoft Defender PKG and deployment script are available through the M365 Defender portal; details in the Microsoft Deployment KB:



> The 'MicrosoftDefenderATPOnboardingMacOs.sh' 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.

```
            <key>OrgId</key>
             <string>[licence code here]</string>
```

The 'OnboardingInfo' key also has this code burnt into its value.

Directions

Download all of the above provided Filesets. Note the Kernel Extension should only be required for legacy devices.

Fileset Group

Create a Fileset Group in which to add each of these.

Profiles should be installed firsts. The Installer Fileset has a requirement script to ensure Profiles are installed, before commencing with download and activation of the Installer.

The requirement script is designed to confirm ALL profiles are installed in advance, with the exception of the Kernel Extension, since this is legacy. The Profile ID of the Kernel Extension may be added to the list within the Fileset. If this is requirement, but are unsure how to approach this, just ask in either the Discord, Alliance or Slack FileWave forums. Links available through the 'Resources' of the FileWave Website.

Installer: 'wdav.pkg'

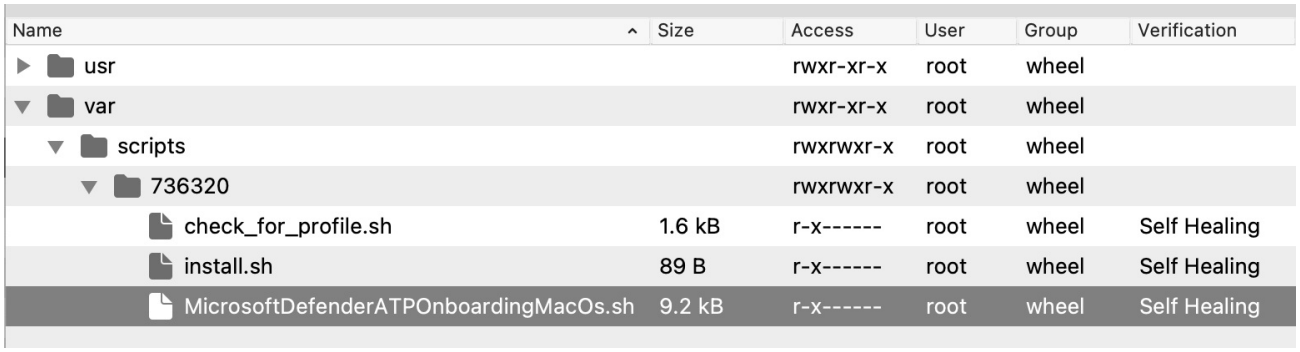
The 'Microsoft Defender Installer macOS' Fileset requires the downloaded PKG. Open the Fileset and drag the PKG into the same location as the '.placeholder' file; this placeholder file may be deleted.

Name	Size	Access	User	Group	Verification
usr		rwxr-xr-x	root	wheel	
local		rwxr-xr-x	root	wheel	
etc		rwxr-xr-x	root	wheel	
MicrosoftDefender		rwxr-xr-x	root	wheel	
.placeholder	0 B	rw-r--r--	Typic...	staff	Self Healing

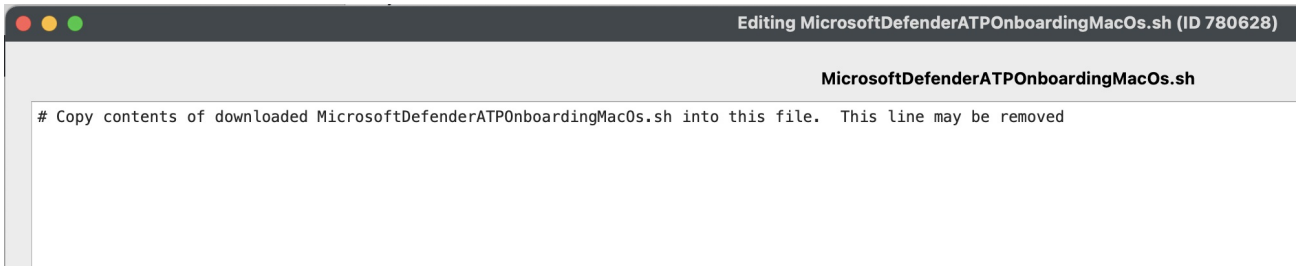
Name	Size	Access	User	Group	Verification
usr		rwxr-xr-x	root	wheel	
local		rwxr-xr-x	root	wheel	
etc		rwxr-xr-x	root	wheel	
MicrosoftDefender		rwxr-xr-x	root	wheel	
wdav.pkg	269.6 MB	rw-r--r--	root	wheel	Self Healing

Script: MicrosoftDefenderATPOnboardingMacOs.sh

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



Name	Size	Access	User	Group	Verification
usr		rwxr-xr-x	root	wheel	
var		rwxr-xr-x	root	wheel	
scripts		rwxrwxr-x	root	wheel	
736320		rwxrwxr-x	root	wheel	
check_for_profile.sh	1.6 kB	r-x------	root	wheel	Self Healing
install.sh	89 B	r-x------	root	wheel	Self Healing
MicrosoftDefenderATPOnboardingMacOs.sh	9.2 kB	r-x------	root	wheel	Self Healing



Profile Payload Values

The Profiles to manage the AutoUpdater and Notifications are configured with default values, consider confirming an internal desired process and adjust to match.

> The 'AcknowledgedDataCollectionPolicy' key prevents a user notification pop-up from showing. Recommendation is to leave this value as set.

All other profile payload values should be correct at the time of writing, however, Microsoft may make changes over time which could require alteration of one or more of these.

Details pertaining to the contents of the payloads may be viewed in Microsoft's Defender Policies documentation; scroll down past the initial unnecessary information until you reach Step 4.

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.

Additional Information

The requirement script within the Installer Fileset is designed to ensure all profiles are in place before downloading and commencing with the installation. Script output from the Client Info > Fileset Status displays logged information.

Example:

First time the script ran, the Profiles were not yet installed. On next run profiles were installed and the requirement script exited with a value of 0.

Script Log:

```
---------------------- HEADER - Date: (Mon Sep 25 2023) - Time: (13:36:40) ----------------------
Set to match all profile IDs

Looking for profile: ml1063.local.5b1e7237-2773-4d3a-9627-361c4dd8a9b0.Configuration.5b1e7237-2773-4d3a-9627-361c4dd8a9b0
Profile found: FALSE

Looking for profile: ml1063.local.bd9007c3-41d6-45bb-a2bf-774ec901e4c2.Configuration.bd9007c3-41d6-45bb-a2bf-774ec901e4c2
Profile found: FALSE

Looking for profile: ml1063.local.7f249c3c-f79a-48cf-952c-dd178a00a5a6.Configuration.7f249c3c-f79a-48cf-952c-dd178a00a5a6
Profile found: FALSE

Looking for profile: ml1063.local.f68916cf-c1e0-47e2-a73c-700678267fe8.Configuration.f68916cf-c1e0-47e2-a73c-700678267fe8
Profile found: FALSE

Looking for profile: ml1063.local.4726b0a7-4f74-4369-8aeb-2450e4f0f935.Configuration.4726b0a7-4f74-4369-8aeb-2450e4f0f935
Profile found: FALSE
Only found 0 profiles from the supplied list of 5
```

```
---------------------- FOOTER - Date: (Mon Sep 25 2023) - Time: (13:36:41) - Exit code: (1) ----------------------
--

---------------------- HEADER - Date: (Mon Sep 25 2023) - Time: (13:39:31) ----------------------
Set to match all profile IDs

Looking for profile: ml1063.local.5b1e7237-2773-4d3a-9627-361c4dd8a9b0.Configuration.5b1e7237-2773-4d3a-9627-
361c4dd8a9b0
Profile found: TRUE

Looking for profile: ml1063.local.bd9007c3-41d6-45bb-a2bf-774ec901e4c2.Configuration.bd9007c3-41d6-45bb-a2bf-
774ec901e4c2
Profile found: TRUE

Looking for profile: ml1063.local.7f249c3c-f79a-48cf-952c-dd178a00a5a6.Configuration.7f249c3c-f79a-48cf-952c-
dd178a00a5a6
Profile found: TRUE

Looking for profile: ml1063.local.f68916cf-c1e0-47e2-a73c-700678267fe8.Configuration.f68916cf-c1e0-47e2-a73c-
700678267fe8
Profile found: TRUE

Looking for profile: ml1063.local.4726b0a7-4f74-4369-8aeb-2450e4f0f935.Configuration.4726b0a7-4f74-4369-8aeb-
2450e4f0f935
Profile found: TRUE
All profiles found.  Exiting 0

---------------------- FOOTER - Date: (Mon Sep 25 2023) - Time: (13:39:33) - Exit code: (0) ----------------------
--
```

Subsequently, the Fileset downloaded and activated:

Client Log:

```
2023-09-25 13:39:34.758|main|INFO|CLIENT|about to downloadAllFileset files for Fileset MicroSoft Defender
Installer macOS Installer Included, ID 736320, revision ID 736320
2023-09-25 13:39:35.697|main|INFO|CLIENT|Downloading Fileset MicroSoft Defender Installer macOS Installer
Included, ID 736320, revision ID 736320
2023-09-25 14:03:49.650|main|INFO|CLIENT|finished downloadFileset files for Fileset MicroSoft Defender Installer
macOS Installer Included, ID 736320, revision ID 736320
2023-09-25 14:03:50.285|main|INFO|CLIENT|Create all folders of fileset ID Fileset MicroSoft Defender Installer
macOS Installer Included, ID 736320, revision ID 736320, version 4
2023-09-25 14:03:50.289|main|INFO|CLIENT|Activate all files of Fileset MicroSoft Defender Installer macOS
Installer Included, ID 736320, revision ID 736320, version 4
2023-09-25 14:03:50.465|main|INFO|CLIENT|Done activating all 4 files of Fileset MicroSoft Defender Installer macOS
Installer Included, ID 736320, revision ID 736320, version 4
```

Revision #7
★Created 22 September 2023 16:02:27 by Sean Holden
✎Updated 2 November 2023 13:53:55 by Sean Holden