Deploying MDATP for Mac with MEM powershell scripts

Version 1.0

6th April 2020

Authored  
**Neil Johnson**, Microsoft Intune CxE

## MEM MDATP for Mac Deployment Script overview

The following PowerShell scripts are available to help with MDATP deployment for Mac from the [Microsoft graph GitHub repository](https://github.com/microsoftgraph/powershell-intune-samples/tree/master/MDATP).

|  |  |
| --- | --- |
| Script Name | Function |
| MacOS\_MDATP\_Deployment\_Add.ps1 | Creates all profiles and applications for MDATP for Mac in MEM but **does not assign** **them** to any groups. |
| MacOS\_MDATP\_Deployment\_Add\_Assign.ps1 | Creates all profiles and applications for MDATP for Mac in MEM and **assigns them to the group** that is specified. |

## Profiles Created

Both scripts will create the same five profiles. Four custom macOS | configuration profiles and one macOS | application profile.

|  |  |  |
| --- | --- | --- |
| Profile | Type | Purpose |
| macOS MDATP Kernel Extension | Custom | This is a custom *macOS | Configuration* profile that configures macOS to trust kernel extensions signed by Microsoft’s developer certificate. |
| macOS MDATP Notifications | Custom | This is a custom *macOS | Configuration* profile that configures macOS to allow MDATP to show the end user critical notifications when necessary. |
| macOS MDATP Full Disk Access | Custom | This is a custom *macOS | Configuration* profile that configures macOS to allow MDATP full access to the disk. |
| macOS MDATP Onboarding | Custom | This is a custom property list *macOS | Configuration* profile for MDATP which tells the MDATP application which tenant to connect to. |
| macOS MDATP System Extension | Custom | This is a custom *macOS | Configuration* profile that configures macOS to trust system extensions signed by Microsoft’s developer certificate. |
| macOS Microsoft Defender ATP | Application | This is a *macOS | app* profile that configures the client to download and install the MDATP binaries. |

## Command Line Arguments Description

The scripts take the following command line parameters:

* OnboardingXMLFilePath < file path>

This is the path to your MDATP **WindowsDefenderATPOnboarding.xml** file. To obtain this file, perform the following steps.

* From a browser, go to <https://securitycenter.windows.com/dashboard>
* Sign in with an administrator account
* Click **Settings** > **Onboarding**
* Select **macOS** from the dropdown for **onboarding process**
* Select **Mobile Device Management / Microsoft Intune** from the **deployment dropdown**
* Click **Download onboarding package**
* Inside the **WindowsDefenderATPOnboardingPackage.zip** make a copy of the **WindowsDefenderATPOnboarding.xml** file within the **Intune folder**.
* AADGroup <AzureAD Group Name>

This is the name of the Azure AD Group that the profiles will be assigned to. This is only available in the *MacOS\_MDATP\_Deployment\_Add\_Assign.ps1* script.

## Deployment Example

In this example I have saved my ***WindowsDefenderATPOnboarding.xml*** file in the same directory as the ***MacOS\_MDATP\_Deployment\_Add\_Assign.ps1*** script. Once the script is run it will create all five policies and assign them to the group provided.

Important:

If any users or devices are in the AAD Group, they will begin receiving the deployment profiles at their next check-in.

Graphical user interface, text

Description automatically generated

## MEM Policies

Once done, the following macOS | Configuration profiles will appear in your MEM console:

Graphical user interface, text, application

Description automatically generated

Once done, the following macOS | apps will appear in your MEM console:

A screenshot of a cell phone

Description automatically generated