Download and deploy Windows Defender Definitions for Windows 10 during OSD

When you are using Windows 10 and Windows Defender in Windows 10 then the definitions are as old as the .WIM file is. It is a good idea to update the definitions during OSD to make sure that the latest definitions are there.

I have used Chris Nackers post and script a lot for downloading and deploying the definitions for System Center Endpoint Protection during OS deployment in Windows 7, Windows 8. http://www.chrisnackers.com/2012/10/18/configuration-manager-2012-installing-endpoint-protection-during-a-task-sequence/

I also found this script in Technet Galleries also for downloading the Endpoint Protection definition files: https://gallery.technet.microsoft.com/scriptcenter/SCEP-Definition-Updates-to-fde57ebf

This post will cover how we can do the same for Windows Defender when deploying Windows 10, it is actually much easier as we don't have to install the Windows Defender client as it is already included in Windows 10. My colleague Johan Schrewelius and I put together this little script that can be run as a Schedule Task that download the definitions from Microsoft to the UNC path and update the package source files in a specific DP group.

The script can be downloaded from Technet Galleries: https://gallery.technet.microsoft.com/Windows-Defender-b15b8057

Here is how to use it:

1. To start with we create the following structure, "**Defender Definition**", with two underlying leaflets for each architecture, on our Package-share to which we can download the definition files:

2. Download the script from the link above and place the script in any folder, for example. “C:\Scripts”

3. Then we create the Package that will be used in Configuration Manager as wee need the PackageID in the powershell script to be able to update it when a new version is downloaded. Use the folder we created above as the package source, in this example:”\\CM2012R2\pkgshare$\Defender definitions”

4. Then we select a **Standard Program** as well, we need three more if both Windows 10 i386 and X64 is used as wee need two for each architecture

5. Use the following command for the first x86 program **“mpam-fe.exe”** with the command line **x86\mpam-fe.exe** as shown below, we cannot browse as we haven’t downloaded the files just yet. There are two files per architecture that needs to be installed.

6. Limit so that the application can only be run on 32-bit Windows 10.

7. Create three more programs one more for x86, the command line for the second x86 Program should be **x86\nis_full.exe.** Then it should look like this.

8. Then we create two more programs for X64 with the same commands but run from the **x64** folder instead. So it looks like this in the console.

9. Then we distribute the content to a **Distribution Point Group**

10. Now we can have a PackageID as well for the package which can be found in the Configuration Manager Admin Console, in this example 06000159

11. Now we edit the script that we placed in the **C:\Scripts** folder and change the following lines to reflect our environment.

12. Now we create a Schedule Task that will download the definition updates and update the package on the DP’s in the Distribution Point Group.

13. Schedule it to run it daily at **5 AM**

14. Use the task “**Start a program**“

Program: Powershell.exe

Arguments: -NoProfile-ExecutionPolicy ByPass-File C:\scripts\DownloadDefenderDefinitions.ps1

15. Then we can test the Schedule Task to make sure everything works by right-click the new event “Download Defender Definition” and select **Run**:

16. Examine the contents of both x 86 and x 64 leaflet under ‘**Defender Definition**“, they should now contain two files each with name as shown.

17. In the Configuration Manager Admin Console check the content status for the Package so that it was updated successful.

18. Then we add the steps to the Task Sequence to install the updated definitions
Add a new group “**Defender Definition Updates**” in the TS and restrict this to Windows 10 (32-and 64-bit).

19. Then we add the four programs that should be run, restrict them to run only on the correct architecture.

Then we are ready to deploy Windows 10 including the latest Windows Defender updates.

Unieke FAQ ID: #1065
Auteur: diode
Laatst bijgewerkt:09-07-2020 11:08