Windows 10 IoT Enterprise (14393): Turn Off Windows Update and Managing Updates

By Sean D. Liming and John R. Malin
Annabooks – www.annabooks.com

May 2018

Windows 10 Version 14393 Build 1607

Take Control

With clients shipping hundreds to thousands of systems worldwide, one of the topics we discuss with clients centers on system updates. Since support affects a company's bottom line, we need to ask the specific questions of: what, who, and how, with regards to the system maintenance in the field. Every company handles system maintenance differently. Some clients never update the system, some will only update the application and not the operating system, and others need to update everything. When it comes to installing Windows updates, our recommendation for most OEMs is to make sure that they control the updates. Windows comes with the Windows Update Service but relying on the service could be a hit or miss. Some systems might get all the updates and others might not, which could lead to different build configurations running in the field and many product support calls. Testing and verifying updates under controlled conditions, and then sending them out is as a controlled release is a cost-effective approach. To this end, in this paper we will discuss turning off Windows Update in the image and how to get operating system update files for your system.

Turning off Windows Update

The first thing to do is turn off Windows Update Service to keep it from running, but this has become a little more challenging in Windows 10. In our previous article, "Embedded/IoT OEMs and Windows as a Service (WaaS)", we discussed that Microsoft has different release strategies depending on the type of user or the system. Feature and system updates are pushed down at a bi-annual pace for most users. For Embedded/IoT OEMs who are on the LTSB/LTSC track, only security and hot fix updates are going to be downloaded, while feature updates are deferred for 10 years. This means that a system on the 14393 LTSB will remain on 14393 for an extended period of time. Irrespective of the branch or channel, Windows wants to keep itself up to date. We have had some clients tell us that they turn off Windows Update only to see that it has been turned on again at a later time. There are a couple of reasons for this. The first is that clones of a sysprep'd master image will turn Windows Update on again on first boot. The second is that there are a number of scheduled tasks that can kick off Windows Update at any time. **What we know at this time to turn off Windows Update completely is to do the following**:

In the sysprep unattended file add two Pass 7 OOBE synchronous commands to turn off Windows Update Services:

Stop Windows Update Service:

```
Sc.exe stop wuauserv
```

Disable Windows Update Service:

```
Sc.exe config wuauserv start= disabled
```

You will also want add the following as Pass 7 OOBE synchronous commands to disable scheduled tasks that might kick off Windows Update:

```
schtasks /Change /TN "\Microsoft\Windows\WindowsUpdate\sih" /Disable

schtasks /Change /TN "\Microsoft\Windows\WindowsUpdate\sihboot" /Disable
```

```
schtasks /Change /TN "\Microsoft\Windows\WindowsUpdate\Scheduled Start" /Disable
schtasks /Change /TN "\Microsoft\Windows\WindowsUpdate\Automatic App Update" /Disable
```

This means that each clone will have to boot to the administrator account to run the Pass 7 OOBE synchronous commands, thus completely disabling Windows Update. If you have a non-Admin account that you want the system to boot too, you can always add synchronous commands that change the auto-logon to the final user account and reboot the system

Managing Windows Updates

Windows updates are pushed out every month. Trying to supply updates every month is a bit challenging for any OEM and impacts customers as well. Depending on the customers that require updates, we recommend providing updates once or twice a year. Critical security updates would be an exception to that.

With Windows Update turned off, the next step is to figure out what Windows update files need to be applied to systems in the field. Microsoft has improved the general security patch updates. Each monthly update includes a cumulative update that contains all prior months since the release of the specific 10 versions. This means you can get the latest updates in one MSU/CAB file without having to go back through all previous months. Typically, there are 2 to 4 patches a month, one being the big cumulative update. Here are the steps to get the updates files:

1. Attach your target system to the Internet.
2. Enable Windows Update Service.
3. Run Windows Update to download and install the latest updates.
4. Once the updates have been installed, test the system to make sure everything is in working order.
5. Once the system has checked out, using the update history, you can go to the Microsoft Update Catalog site (https://www.catalog.update.microsoft.com/Home.aspx) to download the individual KB update files.

To speed things up a bit, you could download the latest cumulative update ahead of time from the "Windows 10 release information" page (https://www.microsoft.com/en-us/itpro/windows-10/release-information). The cumulative updates provide a sub-version of the version you are using. Once you download and install the cumulative update, you can go through the above steps to capture any other updates that get pulled down from Windows Update.

To apply the updates to individual systems in the field, you have two options. The first is to run WUSA.EXE or DISM to install each update package individually:

```
DISM.exe /Online /Add-Package /PackagePath:c:\<path to .msu file>
```

Or you can use System Image Manager to create a configuration set with the updates, and use DISM on the target system to apply the updates with one command:

```
Dism.exe /Online /Apply-Unattend:c:\Windows\ConfigurationSetRoot\AutoUnattend.xml
```

The book *Starter Guide for Windows® 10 IoT Enterprise* covers the details of how to create and apply a configuration set. You could, also, create a new master image that has all the updates and simply replace the whole image on each system. How you deploy and install the updates to the system in the field is up to you.

Summary

We cannot stress enough that OEMs should control how systems get updated in the field. Random updates that may or may not get applied can cause problems in the field that hurt the bottom line. Take control of the system by turning off Windows Update Service. Test Windows updates on a target system to be sure everything is in working order before deploying the updates to your systems in the field. Microsoft makes it easier to download updates from their catalog sight, so it is easy for you to create a custom update solution.