Windows Embedded

Managing Windows Embedded 8 Devices

with System Center 2012 Configuration Manager

Version 1.0

January 2013

Introduction

Microsoft System Center 2012 Configuration Manager helps you to empower people to use the devices and applications they need to be productive, while maintaining corporate compliance and control. It accomplishes this with a unified infrastructure that gives a single pane of glass to manage physical, virtual, and mobile clients. It also provides tools and improvements that make it easier for IT administrators to do their jobs.

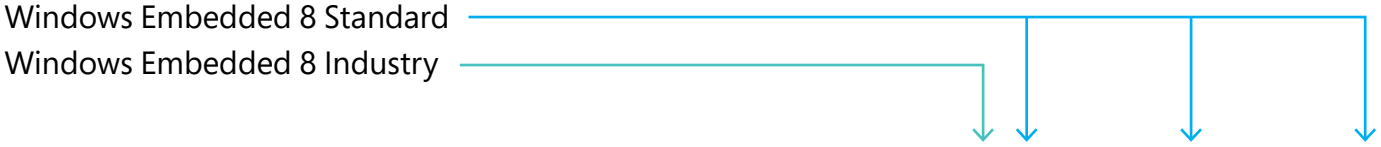
With Configuration Manager 2012 SP1, Windows Embedded 8 devices can be managed like any other IT asset. However, when a write filter is enabled on the device there are a few different scenarios to consider when managing the embedded device. This paper will focus on these scenarios.

First, let's take a brief look at what a write filter is and why it is used. A write filter intercepts writes to protected volumes, and redirects the writes to a different storage location called an overlay, which is discarded upon restart. By redirecting attempted writes to an overlay, write filters can make a write-protected volume appear to function as a writeable volume. This embedded functionality enables building of stateless (or semi-stateless) embedded devices, ensuring they are returned to the same known state on a restart for a predictable and reliable user experience. An additional benefit is the reduced wear on write-sensitive media such as compact USB flash devices.

Types of Write Filter

- Enhanced Write Filter (EWF). EWF intercepts writes to protected volumes at the sector level. Operating at the sector level means that EWF fully supports the NTFS file system. EWF does not allow file exclusions. You can enable registry exclusions by using Registry Filter. If a volume is protected by EWF, the entire volume is considered write-protected.
- File-Based Write Filter (FBWF). FBWF intercepts writes to protected volumes at the file level. This allows you to specify files or directories that are excluded from being filtered.
- Registry Filter. The Registry Filter enables you to persist specific registry keys or values when a device is shut down.
- Unified Write Filter (UWF). UWF operates at the sector level, intercepting all writes to a protected volume. However, you can specify that certain files, directories, or registry keys are excluded from being filtered. Excluded files and directories are tracked in a file exclusion list, and excluded registry entries are tracked in a registry exclusion list. Writes to items in an exclusion list are written directly to the protected volume.

Windows Embedded 8 Standard
Windows Embedded 8 Industry



Functionality	UWF	EWF	FBWF
File/folder exclusions	**Yes**	**No**	**Yes**
Registry key exclusions	**Yes**	**No***	**No***
Sector-based filtering	**Yes**	**Yes**	**No**
Supports Hibernate Once/Resume Many (HORM)	**Yes**	**No**	**No**
RAM-based overlay	**Yes**	**Yes**	**Yes**
Providers for Windows Management Instrumentation (WMI) version 2	**Yes**	**No**	**No**
Disk-backed overlay	**Yes**	**No**	**No**
Commit volume	**No**	**Yes**	**No**
Commit file	**Yes**	**No**	**Yes**

Figure 1 – Write filter summary

*You can use Registry Filter to make registry entries on volumes protected with EWF or FBWF persistent.

As you can see there are different types of write filters providing a variety of functionality. The benefits that come along with this, like ensuring the device starts into the same known state, come at a cost of added complexity when managing and deploying your device. You must consider your management, update, and deployment scenarios when you consider using write filters in your devices, in addition to the requirements and restrictions of each write filter. When write filters are not enabled on Windows Embedded 8 Standard or Windows Embedded 8 Industry then Configuration Manager 2012 SP1 can manage the device like any other IT asset. Just like a Window 8 client. This would be the same for Windows Embedded 8 Professional.

Management Capabilities Overview

Now that we know a little more about how write filters are used on embedded devices, let's take a look at the management scenarios for an embedded device using System Center Configuration Manager. Both Windows Embedded 8 Standard and Windows Embedded 8 Industry have the dependencies for Configuration Manager built into the core operating system. Combined with the Configuration Manager client, device builders and administrators have access to the following capabilities:

- Operating System Deployment
- Software Update Management
- Application Management
- Settings/Configuration Management
- Monitoring/Reporting
- Endpoint Protection

For information on these capabilities, click on the following link of System Center 2012 Configuration Manager capabilities:
www.microsoft.com/en-us/server-cloud/system-center/configuration-manager-2012-capabilities.aspx

The main challenge when managing devices that use write filters is that changes that are written to the overlay and not otherwise persisted will be lost upon restart. In most cases, that's why you use a write filter, but with some changes, such as software updates, or virus signature updates, you really would like to keep those changes past the restart. By not persisting the changes, you could end up with anything from performance issues as the server tries to redownload changes, to overall system instability. The key to managing write-filtered devices is to plan for what you want to persist and how you want to persist it.

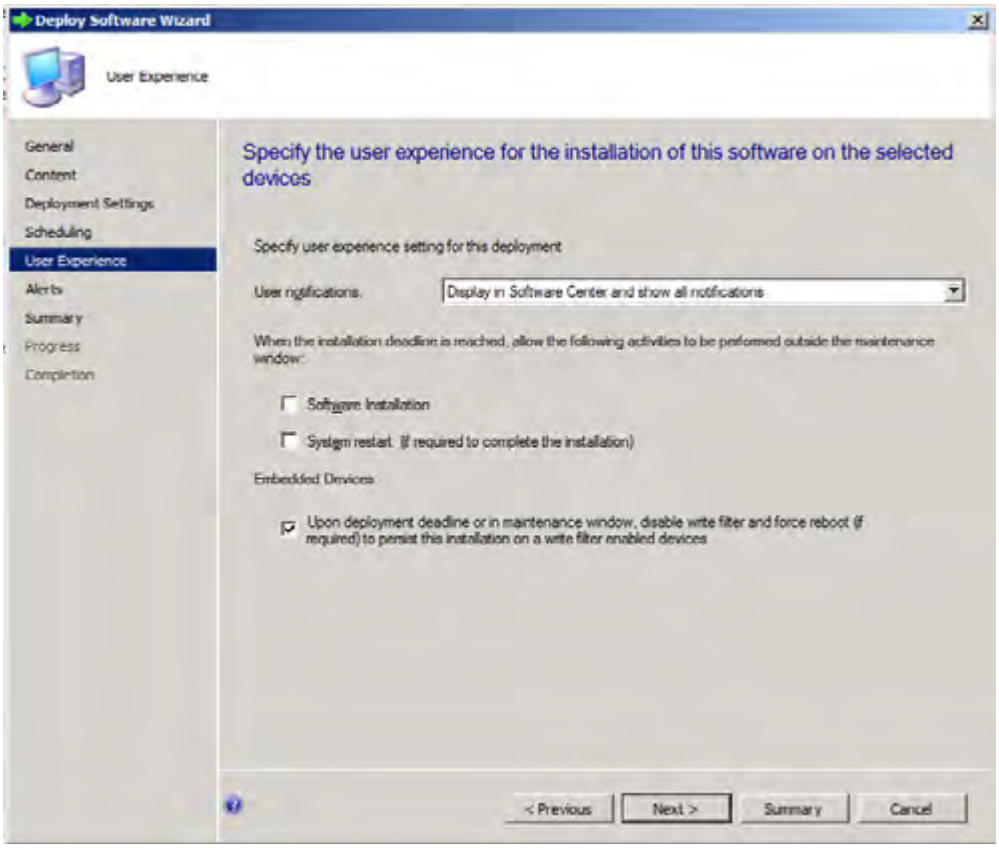
There are a couple of ways to persist changes on devices that use write filters. One is to disable the write filter, make the changes, and reenable the write filter. Another way is to use the exception capability that the FBWF and UWF write filters have. Exceptions allow you to specify files, folders, or registry keys that you want to persist through the write filter. Too many exceptions would defeat the purpose of the write filter, but targeted exceptions can be very useful in helping to persist the changes you need.

Configuration Manager 2012 SP1 is "write filter aware." What that means is that Configuration Manager has the ability to turn off the write filter on a device before any updates are downloaded, apply the updates, and then turn the write filter back on again. This "awareness" applies to a subset of the Configuration Manager features, which is summarized in the table below.

Windows Embedded 8 Standard with Write Filter Enabled

Management Capability	Write Filter Awareness	Maintenance Windows + Policy
Operating System Deployment	**X**	
Software Update Management	**X**	
Application Management	**X**	
Setting Configuration Management		**X**
Monitoring/Reporting		**X**
Endpoint Protection	**X**	

With write filter awareness, restarts and network traffic are minimized. For example, by using maintenance windows, Configuration Manager will only download updates during the maintenance window, while the write filter is off, rather than downloading them immediately into the overlay and then having to redownload them after a restart. Note that write filter awareness applies to the Enhanced Write Filter (EWF) and File-Based Write Filter (FBWF). We will cover Unified Write Filter (UWF) in the next section.



The figure on the left is an example of the UI experience in Configuration Manager for a feature that is write filter aware. In this case, when deploying software using the Deploy Software Wizard in Configuration Manager, the user sees a section called **Embedded Devices**. There they have an option to persist the software update (that is, restart, disable the write filter, and apply the update). The update will be processed as soon as the policy is ready for evaluation on the client device.

Figure 2 – Write filter aware example

Configuration Manager 2012 SP1 Embedded Device Support

Configuration Manager 2012 SP1 has native support for the key embedded scenarios listed in Figure 1. No additional software or licensing is required to manage the Windows 8 embedded device, which has all the dependencies for Configuration Manager included in the core embedded operating system.

Note: The Configuration Manger client is not included in the core embedded operating system. It can be deployed using various methods, including being installed automatically to assigned resources plus added to the image for Windows Embedded 8 Standard devices. Reference: Deploying the Configuration Manager Client to Windows Based Computers for additional client deployment options.

Configuration Manager 2012 SP1 supports write filter (FBWF and EWF) orchestration for Software Update Management, Application Management, Packages and Programs, and Task Sequences. System Center Endpoint Protection client installation and Endpoint Protection updates are also write filter aware.

Additional client improvements

- Non-admins cannot log on while the device is being serviced.
- Software Center blocks installation if write filters are enabled.
- Users cannot change their business hours.
- Users cannot postpone deployments to non-business hours.

Operating system deployment improvements

- "Apply operating system" from distribution point instead of running locally.
- New task sequence variable (SMSTSPostAction) that specifies a command line action to run after the task sequence completes.

"Write Filter Aware" System Center Endpoint Protection Use Case Example

Endpoint Protection installs are write filter aware. This means that when a System Center administrator pushes an Endpoint Protection install to client devices that have write filters, he can tell System Center to persist that installation through the write filter. Selecting the option below will cause the target devices to disable the write filter, restart, install the Endpoint Protection client, reenable the write filter, and restart again when the administrator pushes the Endpoint Protection client out to the devices.

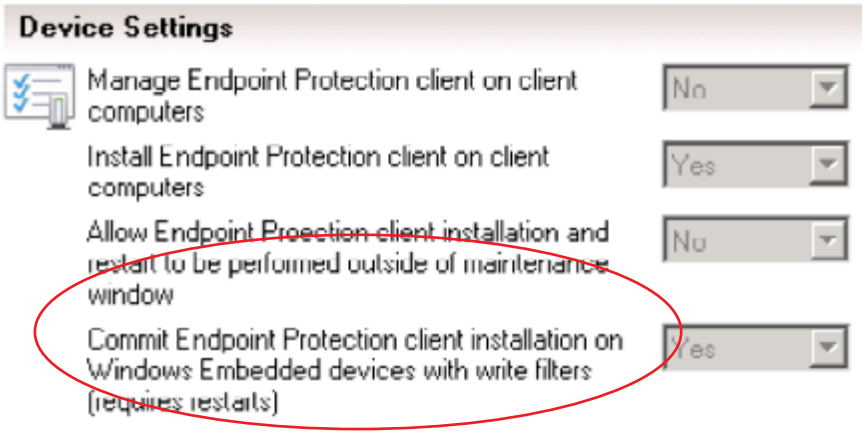


Figure 3 – Endpoint protection example

Universal Write Filter (UWF) Support

Configuration Manager 2012 SP1 does not natively support UWF. This doesn't mean that a System Center administrator cannot manage devices that use UWF, but it does mean that a little more planning is required in order to correctly manage the persistence of changes to devices.

Here's a brief example of deploying software updates to illustrate the difference:

With FBWF:

- The admin selects the updates to install.
- The admin selects the option in Configuration Manager to force-persist the changes.
- The admin selects the target devices and pushes the updates. Configuration Manager handles turning the write filters off/on and all associated restarts, in addition to applying the updates.

With UWF:

- The admin creates a task sequence that will turn off the write filter, restart, and install the updates. The task sequence uses a combination of native task sequence functions (for restarting and installing updates) and the uwfmgr.exe tool.
- The admin selects the task sequence and deploys it to the target devices.
- The devices are updated.

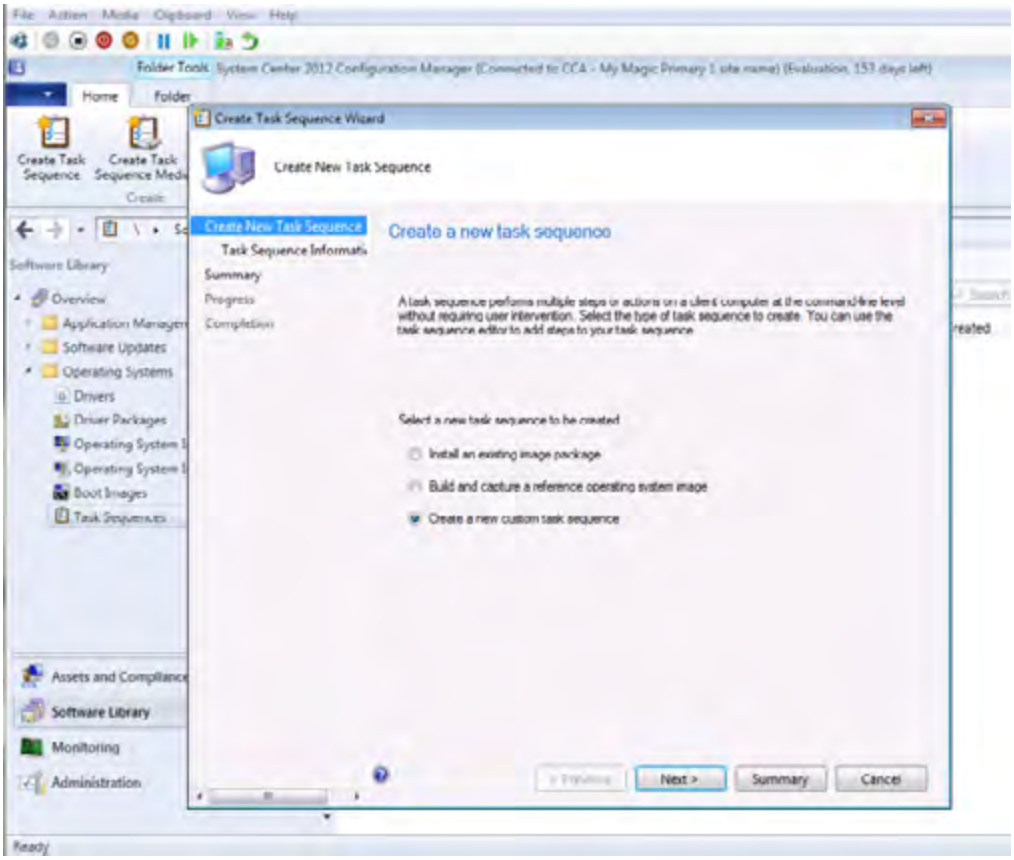
The table below illustrates the approach to managing Configuration Manager capabilities on a UWF device. The good news is you can use task sequences to handle any of the management functions yourself. For example, settings management in Configuration Manager is also not write filter aware. You could use a similar approach with task sequences to handle settings changes on write filter devices.

Windows Embedded 8 Standard or Window Embedded 8 Industry with Unified Write Filter Enabled

Management Capability	Task Sequence with Script	Maintenance Windows + Policy
Operating System Deployment	X	
Software Update Management	X	
Application Management	X	
Setting Configuration Management	X	X
Monitoring/Reporting	X	X
Endpoint Protection	X	

Figure 4 - Configuration Manager capabilities and UWF

Sample Process for Applying Software Updates

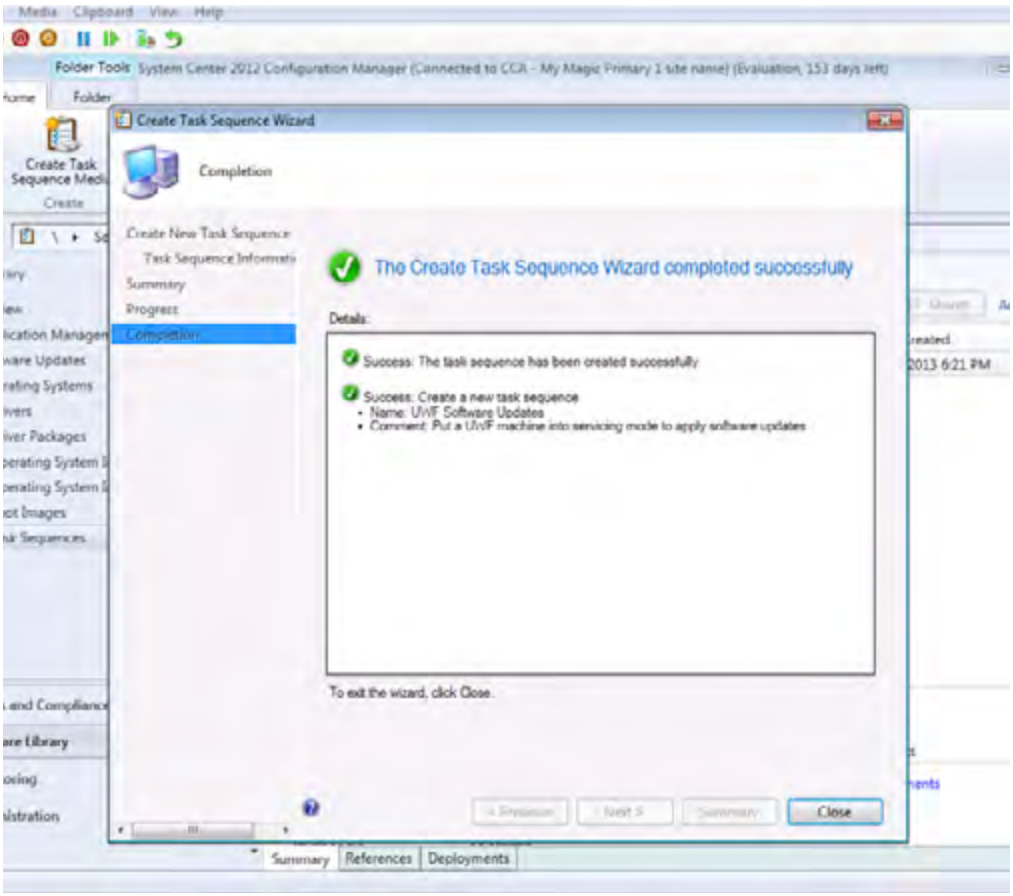


UWF ships with a command line utility known as uwfmgr.exe, which is a powerful tool for managing the configuration and state of the write filter. In this exercise, we will show you how easy it is to use uwfmgr.exe and tasks sequences in Configuration Manager to apply software updates to your operating system.

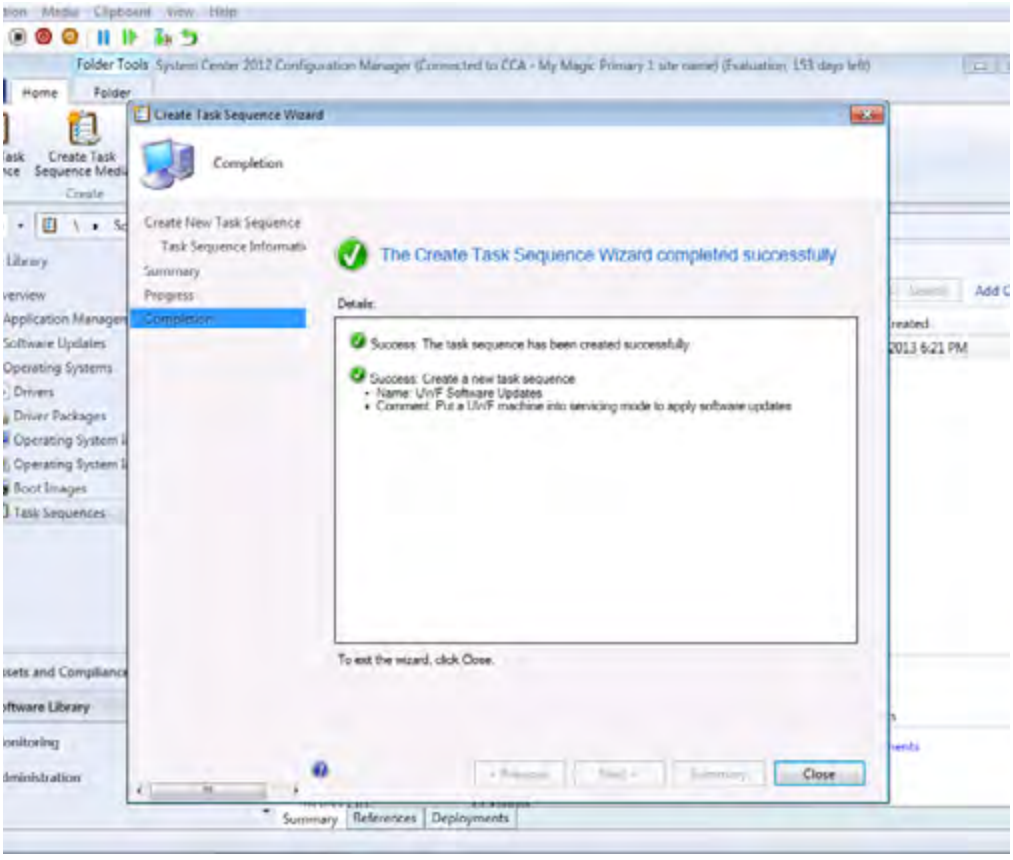
UWF servicing mode makes it easy to apply software updates to your operating system. This article goes into detail on how you would do that on a stand-alone device.

To manage the process with Configuration Manager, all you need to do is include uwfmgr.exe in a task sequence, and then deploy that task sequence to the devices you want to manage.

First, create a new, custom task sequence.

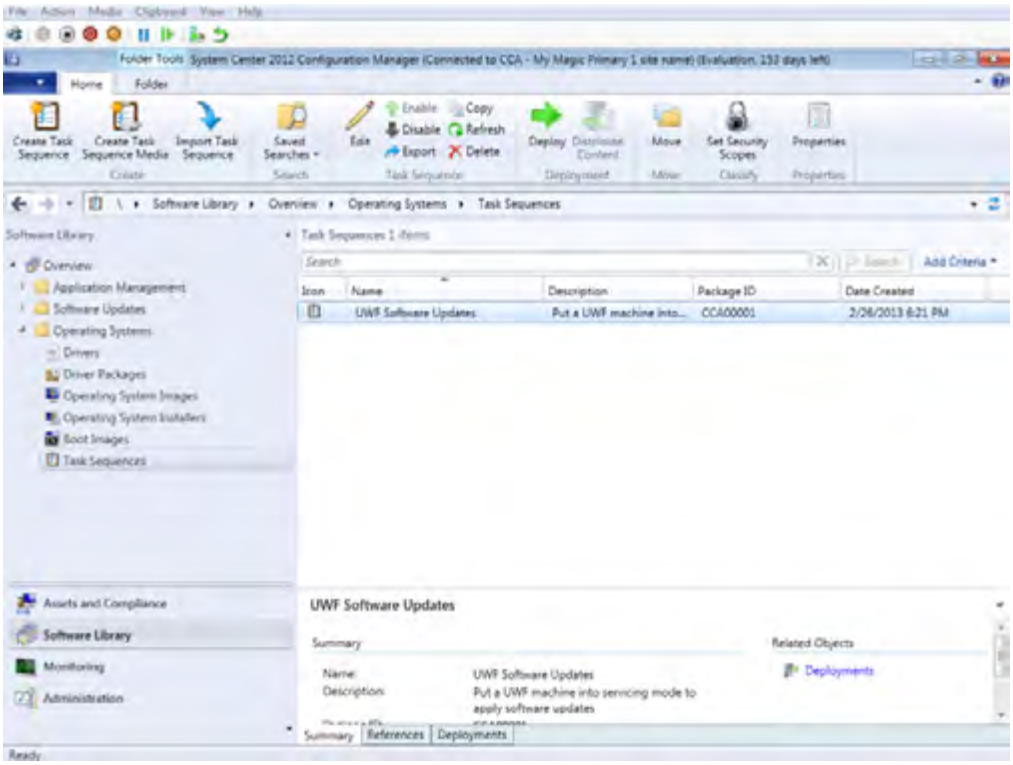


Name the task sequence something you can remember, like "UWF Software Updates." When it finishes, you'll see the pop-up to the left.

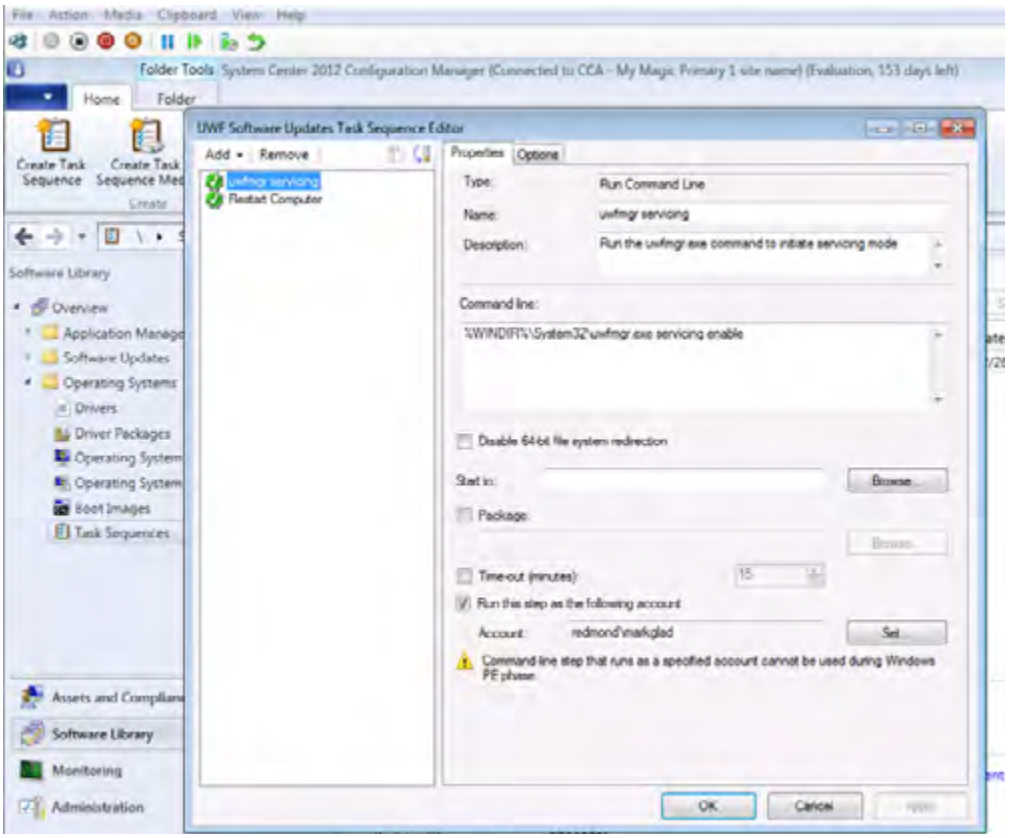


Creating a task sequence simply creates an empty placeholder. Now you need to edit the task sequence to tell it what to do. In this case it's really simple:

- Turn on UWF servicing mode.
- Restart the device.



You'll see your new task sequence in the list.



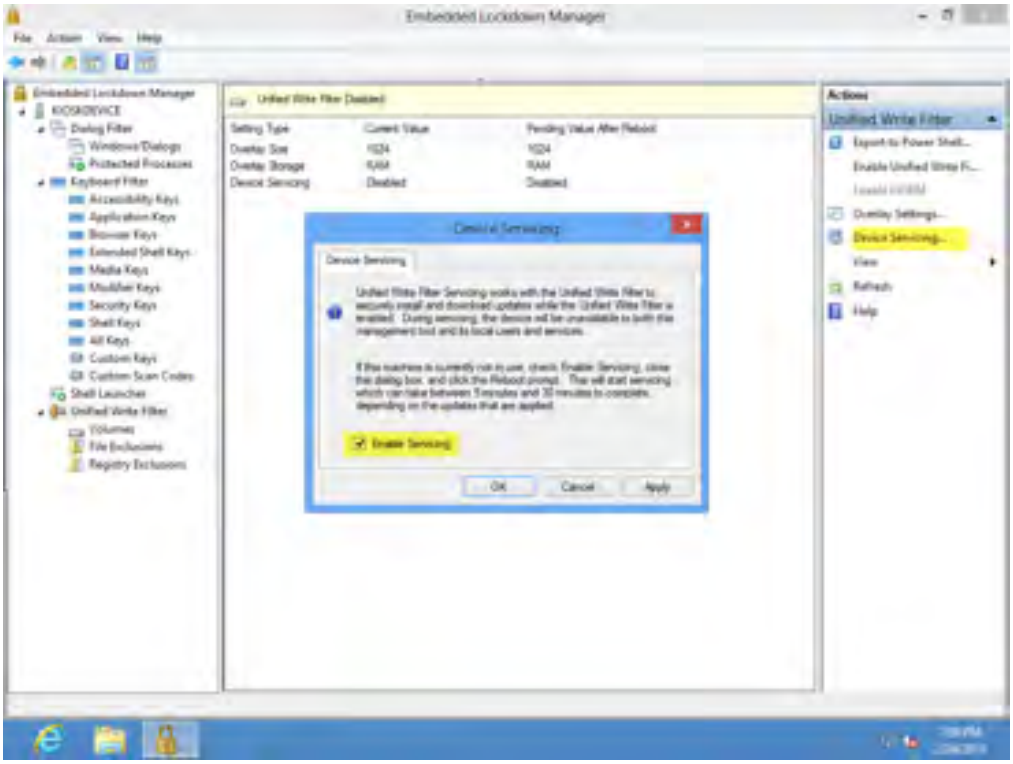
Right-click the task sequence, and select **Edit**. You will add the two tasks to the task sequence now. Both tasks are "general" tasks—a command line task, and a restart task.

To the left you can see the final product. We've added a command line task called "uwfmgr servicing," and in it you can see the command line syntax used to set the device up for UWF servicing. Notice that you can specify the account under which to run the command, which should be the admin account on your device. There are a number of advanced options available for more sophisticated setup and control.

"Restart Computer" is a standard task available within a task sequence. You don't need to write your own restart script or send another command line task. You just pick the "Restart Computer" task and add it to the task sequence, and your setup is complete.

All you have to do now is deploy this task sequence to the target devices, and you are all set. It will turn on UWF servicing mode and restart the device, which will then be in servicing mode. The UWF servicing mode will handle applying the available updates, and then it will do a final restart after that to turn off servicing mode and return the device to normal operations. All of that work is handled by the UWF servicing mode, so you don't need to include it in the task sequence.

Additionally, UWF can be configured outside of Configuration Manager with the Embedded Lockdown Manager (ELM) and the UWF servicing mode. This can be used for individual or a small number of embedded devices.



ELM is a snap-in to the Microsoft Management Console (MMC). You can use ELM remotely to connect to one or many devices. ELM automatically detects which lockdown features are installed on the device, and displays configuration options for those features. ELM uses Windows Management Instrumentation (WMI) to detect and change configuration settings. After modifying and testing settings on an embedded device, the new settings can be exported to a Windows PowerShell script.

Summary

Write filters are a key functionality for embedded devices, and management of these write filter–enabled devices is not significantly more complex than managing other IT assets. Many Configuration Manager features are already write filter aware. Plan for persistence, and use maintenance windows to optimize network utilization. Make deployments required instead of available. Use exceptions when you can to minimize restarts. Using the WMI provider you can manage the rest of the embedded-specific features (for example, Keyboard Filter) via Configuration Manager as well. Windows Embedded will continue to work closely with the Configuration Manager team to provide even richer integration between the products in the future.

Reference

Deploying the Configuration Manager Client to Windows-Based Computers
http://technet.microsoft.com/en-us/library/gg682132.aspx#BKMK_DeployClientEmbedded

Information on System Center Endpoint Protection Exception
http://blogs.msdn.com/b/windows-embedded/archive/2013/02/15/using-system-center-endpoint-protection-2012-sp1-on-windows-embedded-standard-7-and-posready-7-with-file-based-write-filters.aspx