EMEA CONTACT
support@10zig.eu
+44(0) 116.214.8650

AMERICAS CONTACT
support@10zig.com
866.865.5250

Unified Write Filter Configuration

In Windows Embedded Standard 8, Unified Write Filter (UWF) protects volumes from write operations. UWF intercepts write actions and redirects them to overlay storage. With UWF, you can do stateless operations by creating a protected OS image, and you reduce the wear on flash media. UWF supports RAM- and disk-based overlays. Both types of overlay discard all changes on restart. UWF also provides the ability to perform *dynamic protection*, which means adding and removing volumes at run time.

One of the important features of UWF is *intelligent filtering*, which enables specified files and folders as well as certain registry keys to be persisted, while protecting the rest of the volume. The list of these specified files, folders, and registry keys is known as the *exclusion list*. You can use intelligent filtering to persist changes to an antivirus signature file or to a directory such as a user's Documents folder within the protected volume. You can also use intelligent filtering to persist a registry key, such as the Domain Secret key, in a protected system.

You can configure UWF at run time by using either of the following methods:

- UWF manager, a command-line configuration utility (Uwfmgr.exe).
- UWF Windows Management Instrumentation (WMI) provider that uses WMI properties and
  1 GB of operating system memory (32-bit system) or 2 GB of operating system memory (64-bit system)

UWF manager provides many options and configuration tasks that do not exist in Enhanced Write Filter (EWF) manager or File-based Write Filter (FBWF) manager, such as adding registry exclusions and adding volumes. UWF manager syntax is very different from both EWF manager and FBWF manager, because it categorizes configuration into six high-level parameters to simplify configuration and avoid parameter or argument overloading.

Lab Exercise Purpose

In this lab exercise, you will learn how to configure UWF at run-time by using UWF manager (Uwfmgr.exe).

Prerequisites

Important Most UWF configuration commands are executed when the next restart happens, so the system must be restarted for the command to take effect.

To perform the steps in this lab exercise, the following hardware and software are required:

- Hardware that meets Standard 8 requirements.
- An installed Standard 8 image that includes UWF.

Note By default, UWF is disabled and there are no protected volumes, files, or folders in the exclusion list.

For more information, see *Media and Requirements* in the Standard 8 documentation.

Step 1: Ensure that your device will start and perform well after UWF is enabled

In this step, you will change system settings that can prevent your device from starting after UWF is enabled or that can cause poor performance.

1. On the embedded device, open a command prompt as an administrator. For Windows Shell, to open a command prompt, do the following:

    a. In Windows Explorer, navigate to \Windows\System32,right-click cmd.exe, and then click **Run as Administrator**.

    b. Accept the User Account Control (UAC) prompt.

2. To change UWF so that it does not prevent your device from starting, at the command prompt, type the following command:

```
bcdedit /set {current} bootstatuspolicy ignoreallfailures
```

3. To disable indexing service, type the following command:

```
sc config cisvc start= disabled
```

4. To disable Prefetch/SuperFetch services, type the following command:

```
sc config sysmain start= disabled
```

5. To disable system restore, run the following Visual Basic script:

```
strComputer = "."
Set objWMIService = GetObject("winmgmts:" _
    & "{impersonationLevel=impersonate}!\\" _
    & strComputer & "\root\default")

Set objItem = objWMIService.Get("SystemRestore")
errResults = objItem.Disable("")
```

Step 2: Protect a volume on a Standard 8 system

In this step, you will use UWF to protect a volume on a Standard 8 system.

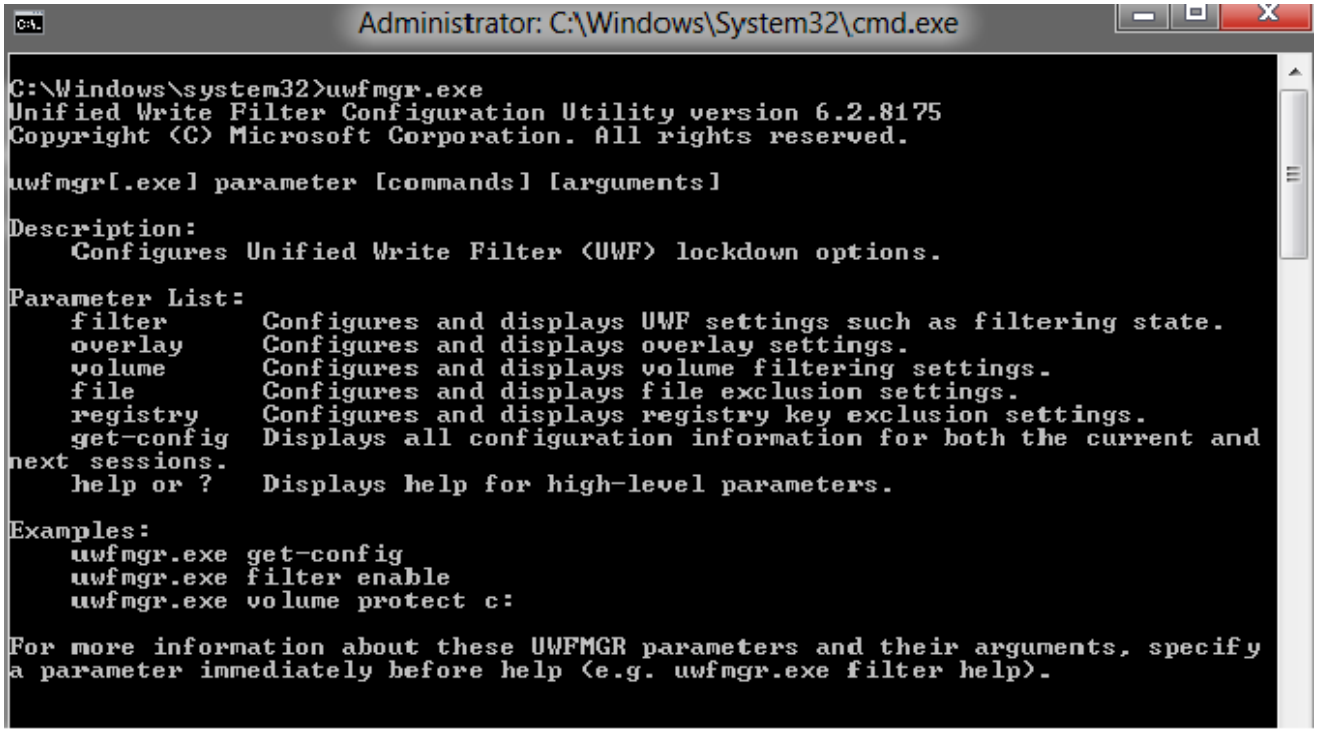
1. On the embedded device, open a command prompt as an administrator. For Windows Shell, to open a command prompt, do the following:

    a. In Windows Explorer, navigate to \Windows\System32, right-click cmd.exe, and then click **Run as Administrator**.

    b. Accept the UAC prompt.

2. To get UWF help, at the command prompt, type `uwfmgr.exe`.

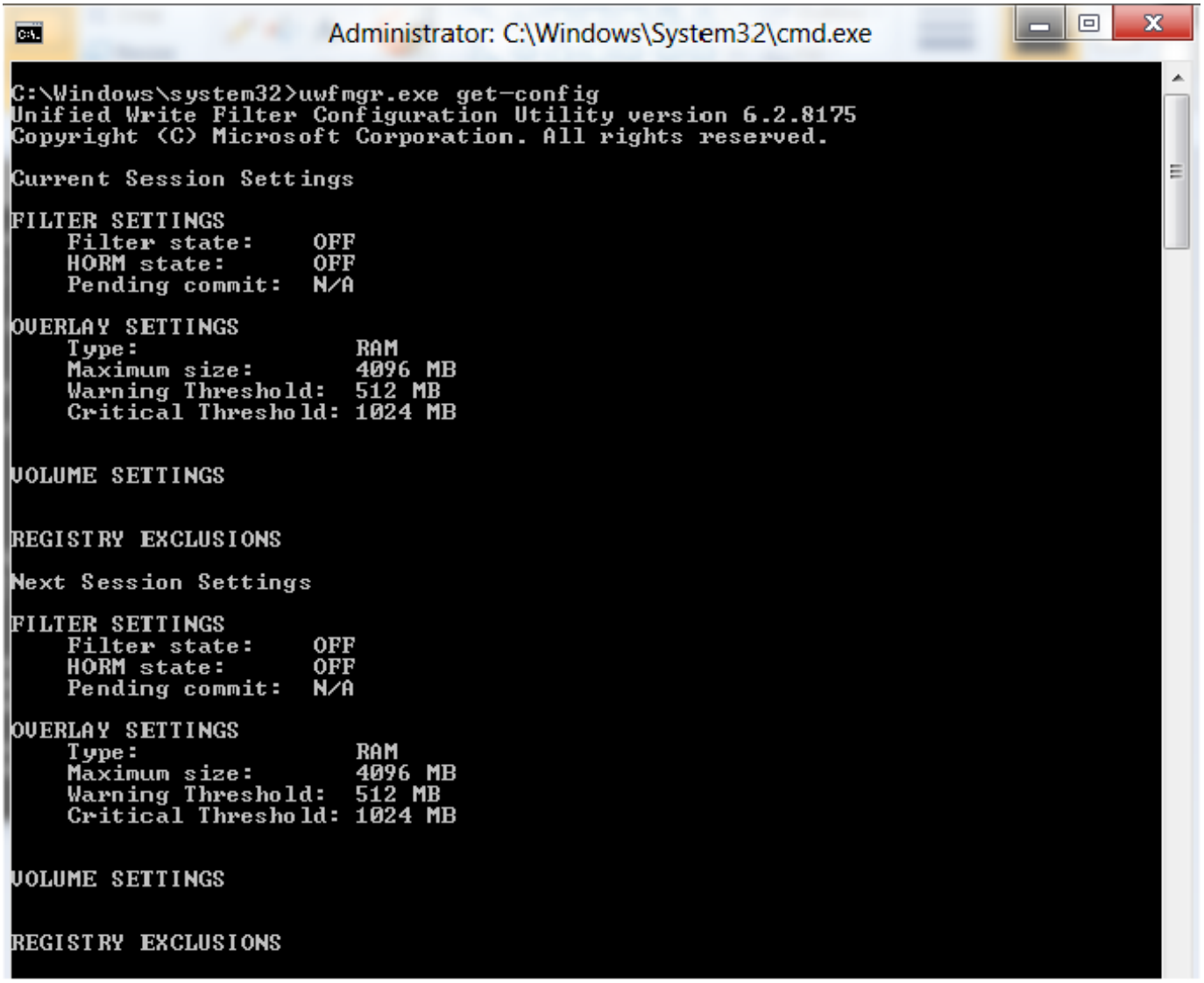
    The following help and usage information for high-level parameters appears.



Note To get help and usage information for any high-level parameter, run `uwfmgr.exe %parameter_name%` without any arguments, for example, `uwfmgr.exe filter`.

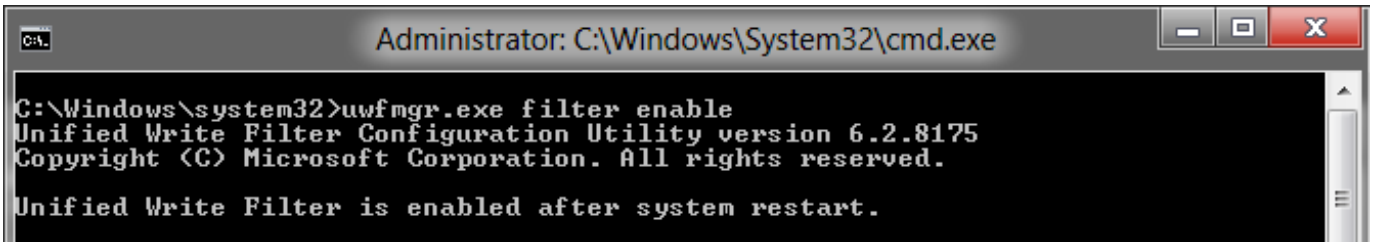
3. To check UWF settings, type `uwfmgr.exe get-config`.

    The configuration status for the current session and the next session after restarting appears, including outcome information includes the Filter status, Overlay settings, Volume protection settings including file exclusion, and registry exclusion settings as shown in the following figure.

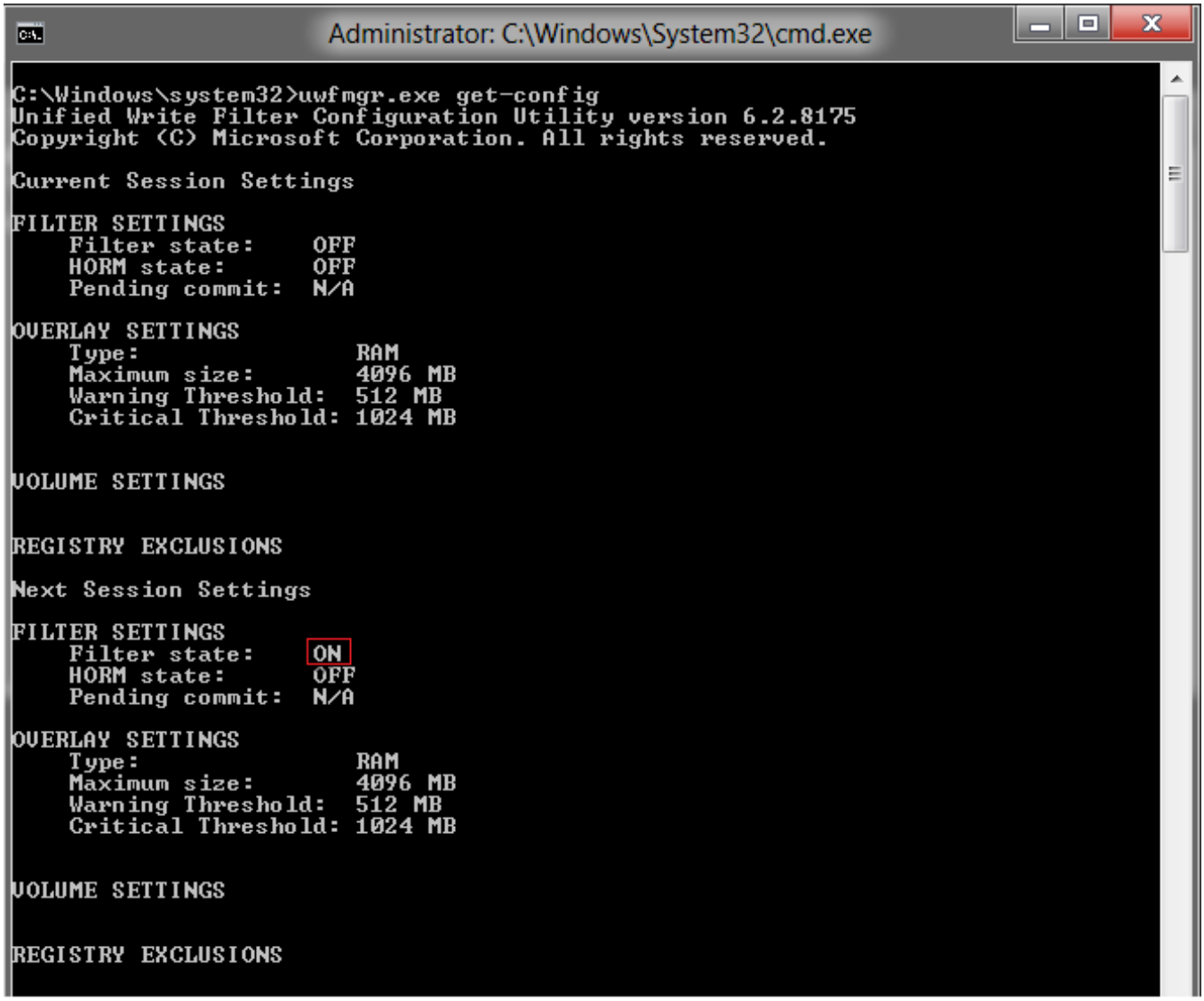


4. To enable UWF, type `uwfmgr.exe filter enable`.

After you restart, the filter is enabled for the next session as shown in the following figure.



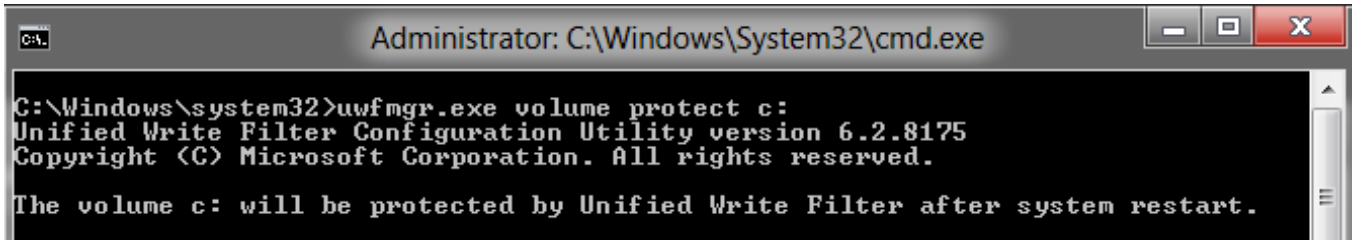
5. To check UWF status, type `uwfmgr.exe get-config`.



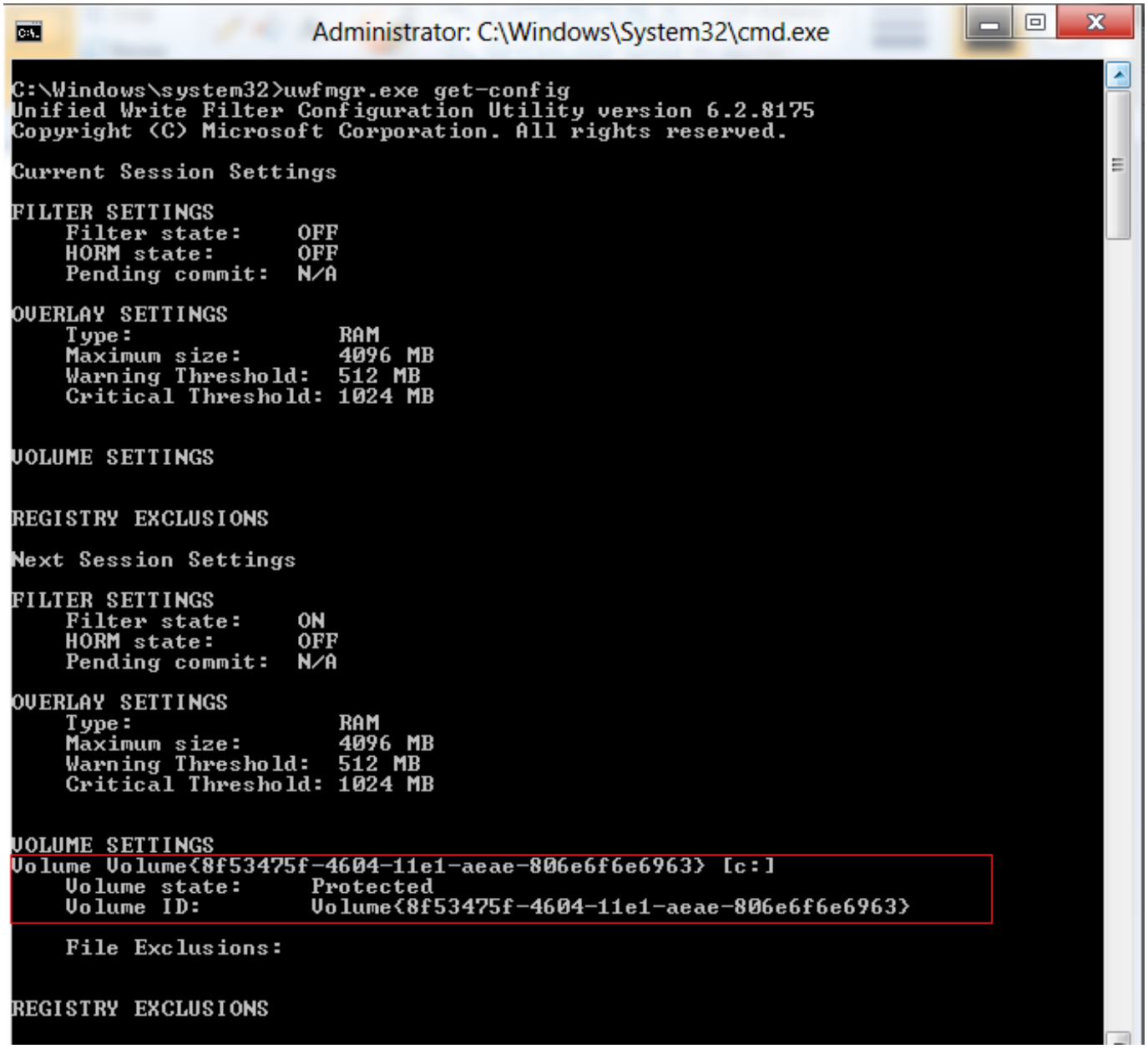
6. To protect a volume with UWF, type `uwfmgr.exe volume protect C:`.

   Note This command adds only volumes that exist in the system.

   After you restart, the volume is added to the list of protected volumes in the next session, as shown in the following figure.



7. To check UWF status, type `uwfmgr.exe get-config`.



8. Restart the system.

Step 3: Add file and registry exclusions to a UWF-protected Standard 8 system

In this step, you will add file and registry exclusions to a UWF-protected Standard 8 system.

1. On the embedded device, open a command prompt as an administrator. For Windows Shell, to open a command prompt, do the following:

    a. In Windows Explorer, navigate to \Windows\System32,right-click cmd.exe, and then click **Run as Administrator**.

    b. Accept the UAC prompt.

2. To create sample folders and files to exclude, do the following:

    a. At the command prompt, type the following commands:

    ```
    md C:\aa\documents

    md C:\mydir

    notepad.exe C:\mydir\myfile.txt
    ```

    b. Save the text file and then close Notepad.

    Note Uwfmgr.exe does not support adding files and folders that do not exist yet to the exclusion list.

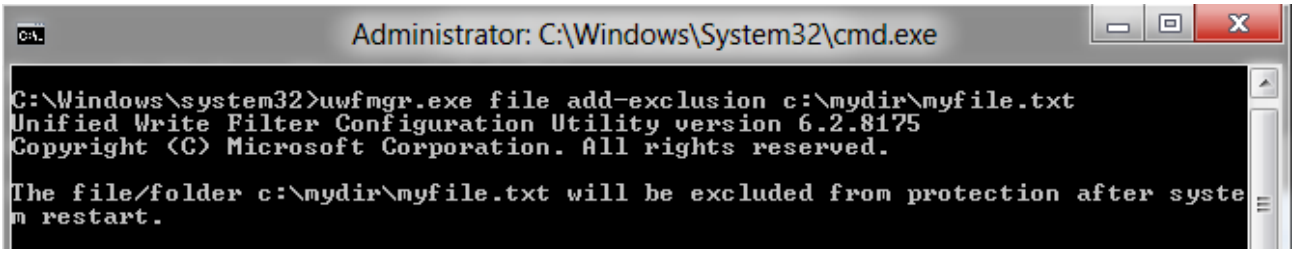
3. To add file and folder exclusions, do the following:

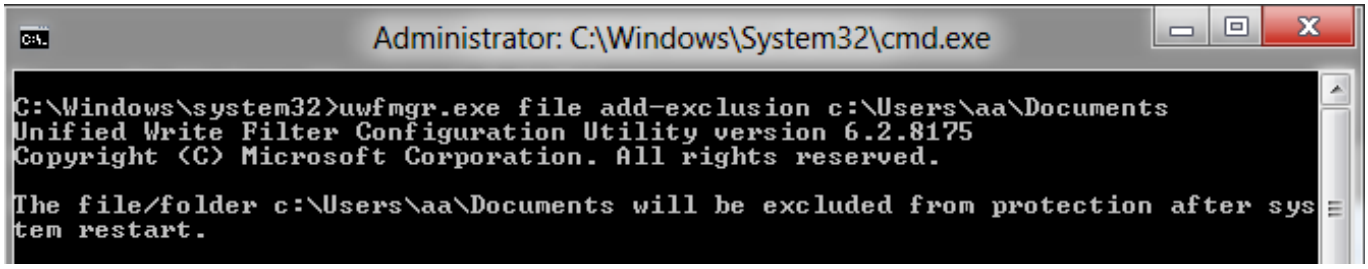
    a. At the command prompt, type the following commands:

    ```
    uwfmgr.exe file add-exclusion C:\mydir\myfile.txt

    uwfmgr.exe file add-exclusion C:\aa\documents
    ```

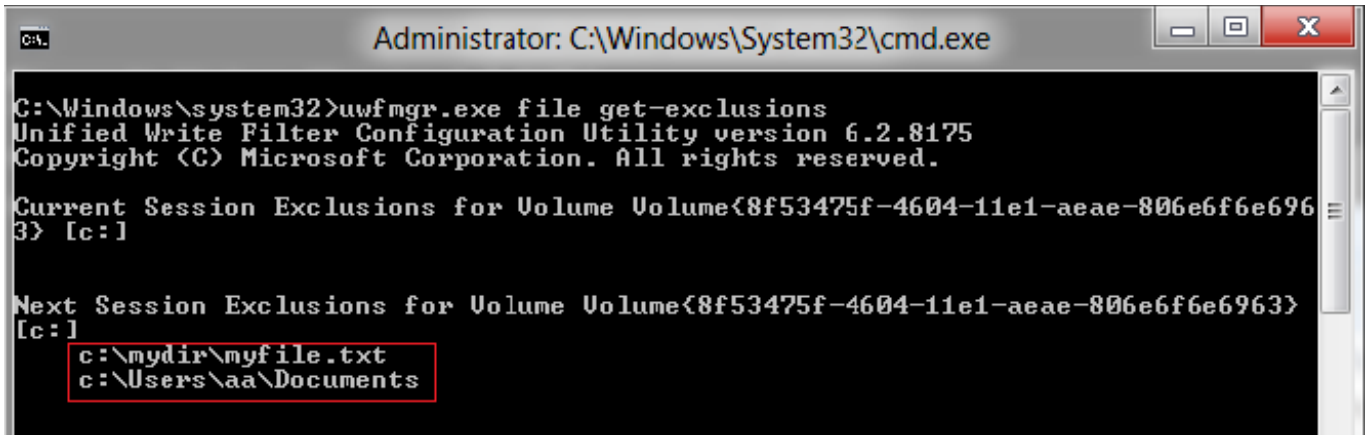
    Note To add an exclusion for a file or a folder that includes a space in the path, enclose the path in quotation marks, for example, "c:\My Files".

    After you restart, the specified files and directories are added to the exclusion list in the next session as shown in the following figures.





b. To check file exclusion status, type `uwfmgr.exe file get-exclusions`.

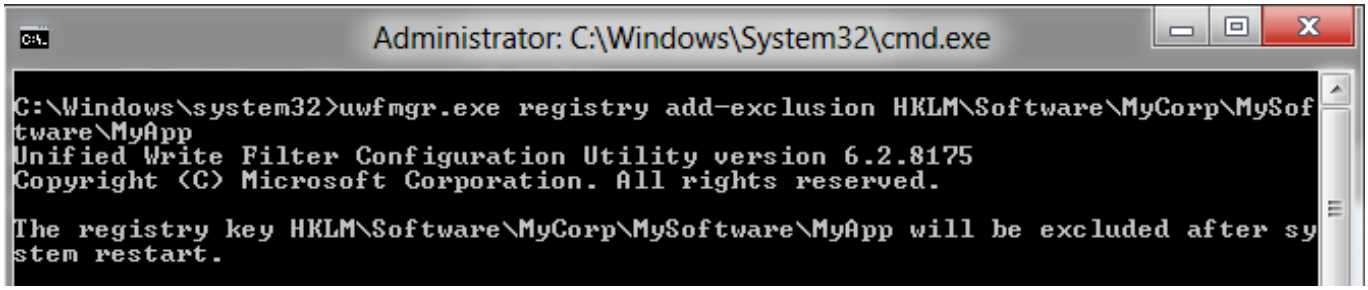


4. To add a registry key exclusion, do the following:

   a. At the command prompt, type
   `uwfmgr.exe registry add-exclusion HKLM\Software\MySoftware\MyApp`.

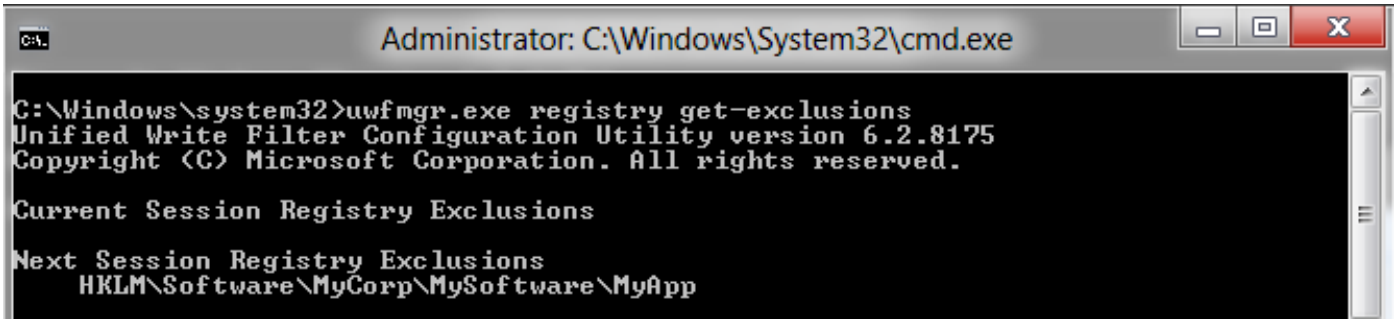
   Note To add exclusion for a registry key that includes a space, enclose the registry key name in quotation marks.

   After you restart, the specified registry key is added to the exclusion list in the next session as shown in the following figure.

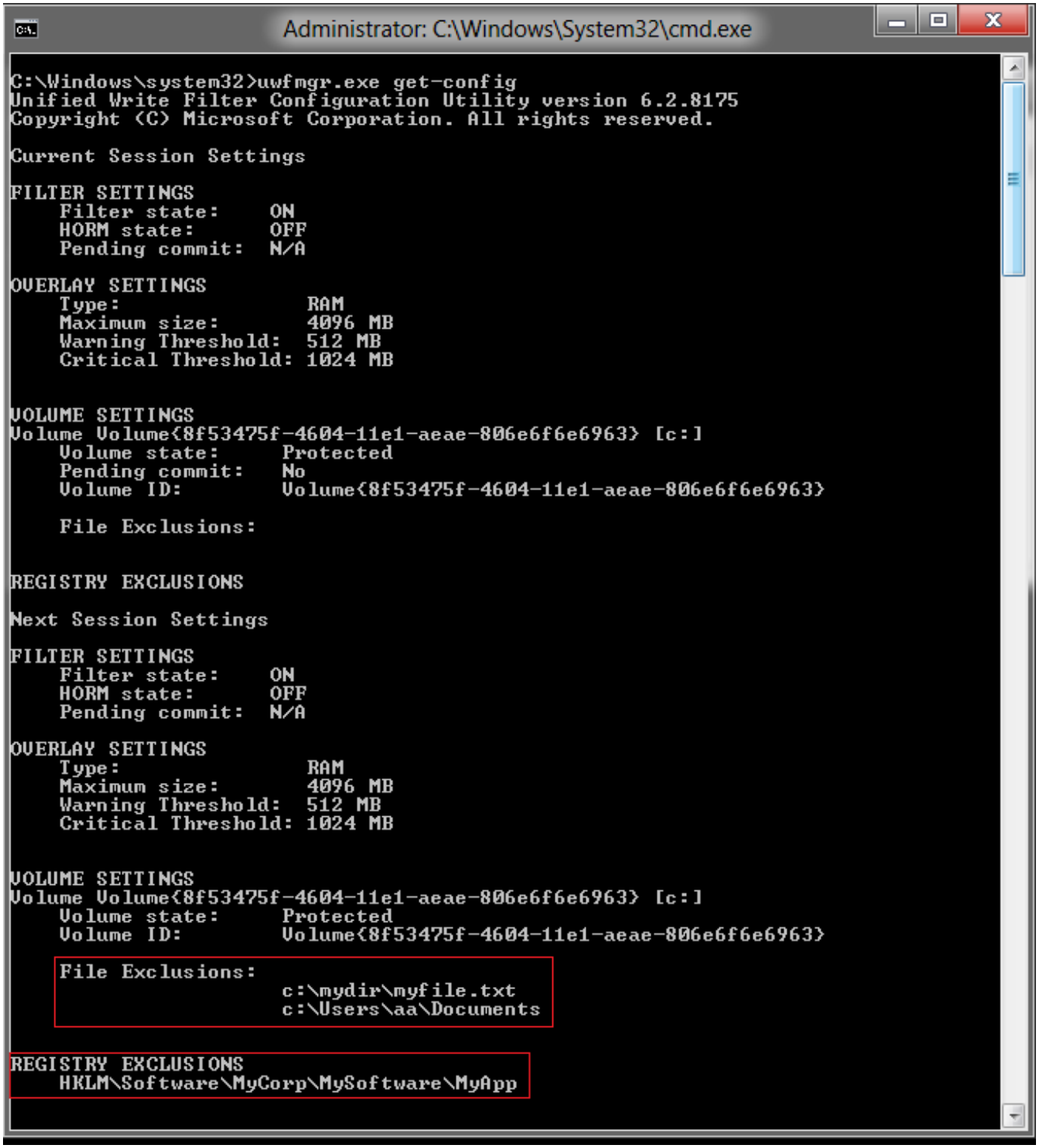


   b. To check the registry exclusion status, type `uwfmgr.exe registry get-exclusions`.

EMEA CONTACT
support@10zig.eu
+44(0) 116.214.8650
AMERICAS CONTACT
support@10zig.com
866.865.5250



c. To check UWF status, type `uwfmgr.exe get-config`.



5. Restart the system.

Step 4: To configure a UWF overlay for a protected Standard 8 system

In this step, you will configure a *UWF overlay* or a cache for a protected Standard 8 system.

1. On the embedded device, open a command prompt as an administrator. For Windows Shell, to open a command prompt, do the following:

    a. In Windows Explorer, navigate to \Windows\System32,right-click cmd.exe, and then click **Run as Administrator**.

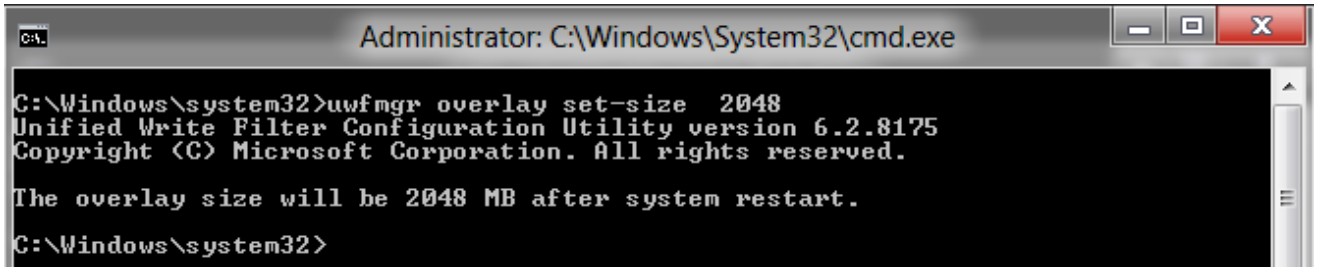
    b. Accept the UAC prompt.

2. To configure the UWF maximum overlay size, do the following:

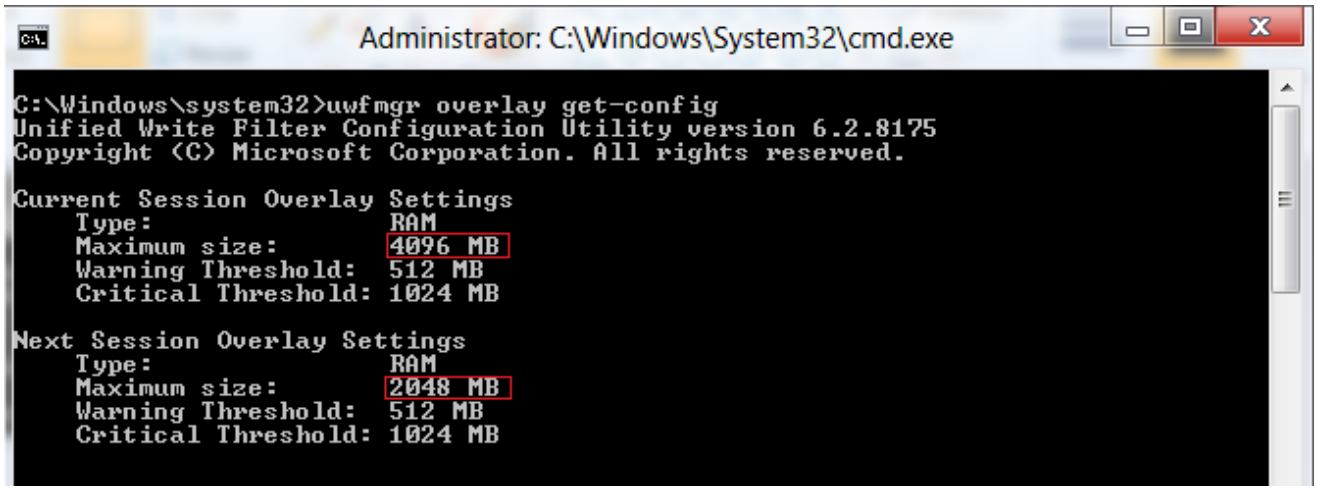
    Note To change maximum overlay size, you must first disable UWF in the current session.

    a. At the command prompt, type `uwfmgr.exe overlay set-size 2048`.

    After you restart, the maximum size is set to 2048 MB in the next session, as shown in the following figure.

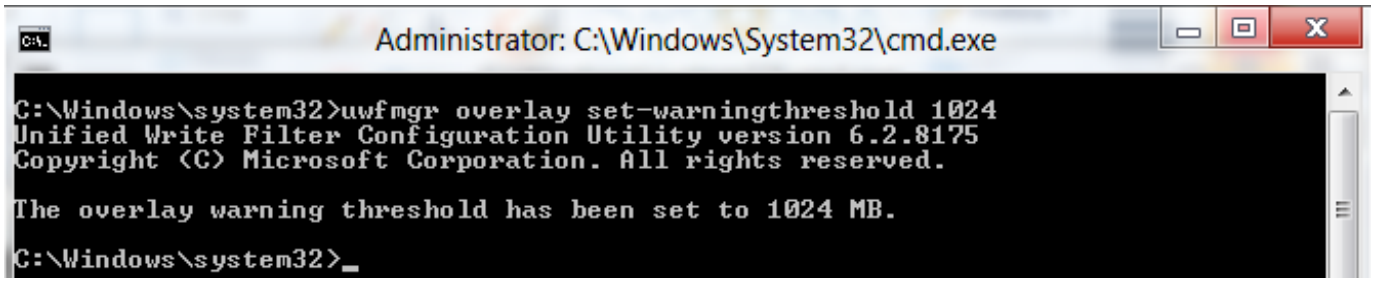


    b. To check the overlay settings status, type `uwfmgr.exe overlay get-config`.



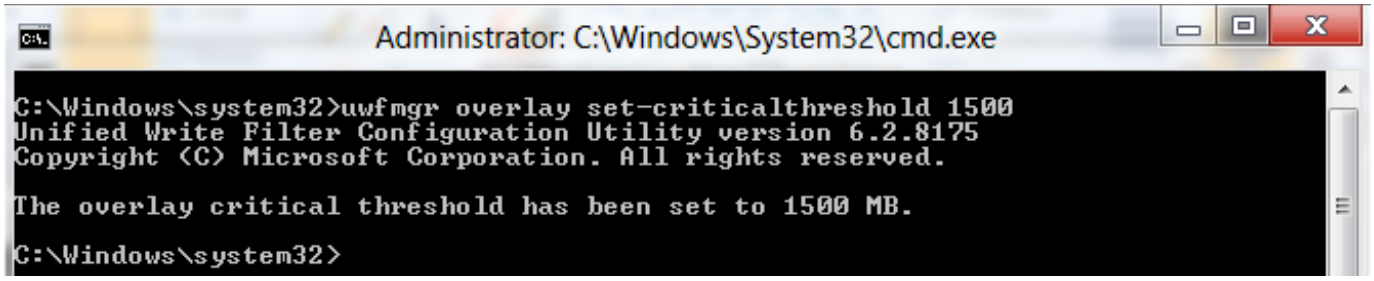
3. To configure the UWF overlay warning threshold, type `uwfmgr.exe overlay set-warningthreshold 1024`.

After you restart, the threshold is set to 1024 MB in the next session, as shown in the following figure.



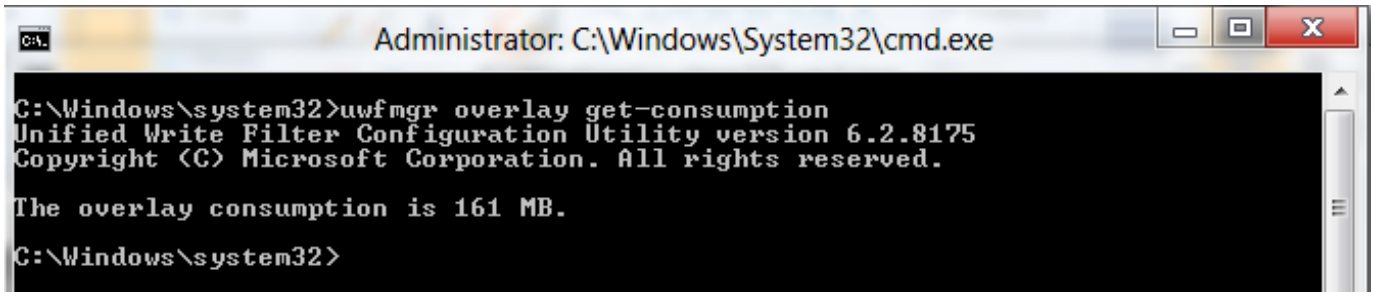
4. To configure the UWF overlay critical threshold, type `uwfmgr.exe overlay set-criticalthreshold 1500`.

   After you restart, the threshold is set to 1500 MB in the next session, as shown in the following figure.



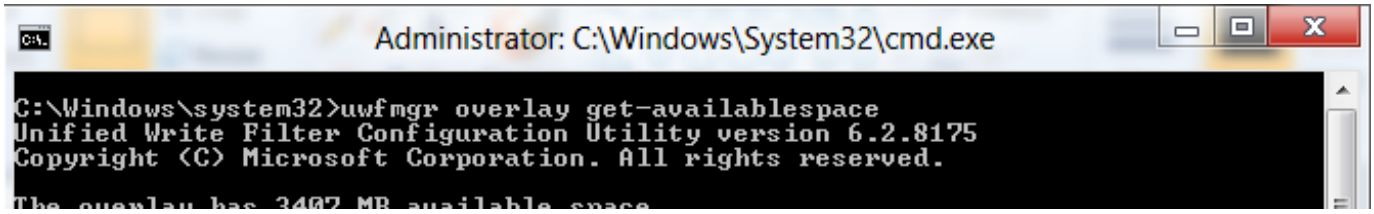
5. To display the UWF overlay consumption, type `uwfmgr.exe overlay get-consumption`.

   The current overlay consumption displays, as shown in the following figure.



6. To display the UWF overlay available space, type `uwfmgr.exe overlay get-consumption`.

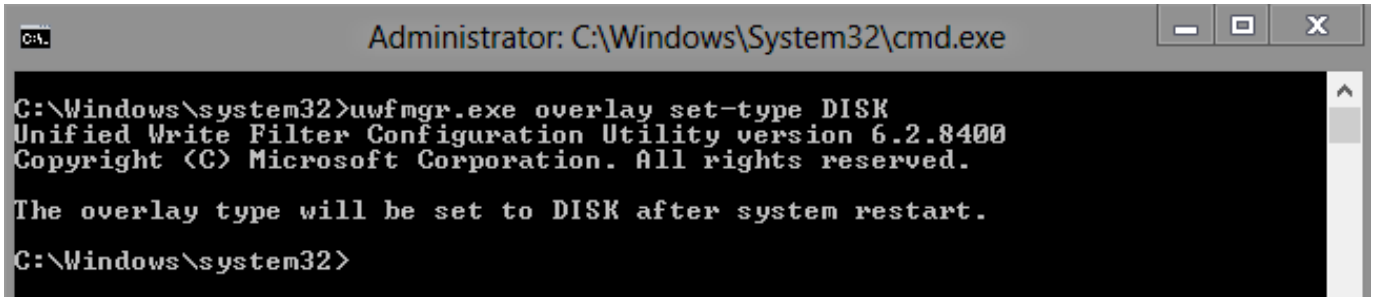
   The current overlay consumption displays, as shown in the following figure.



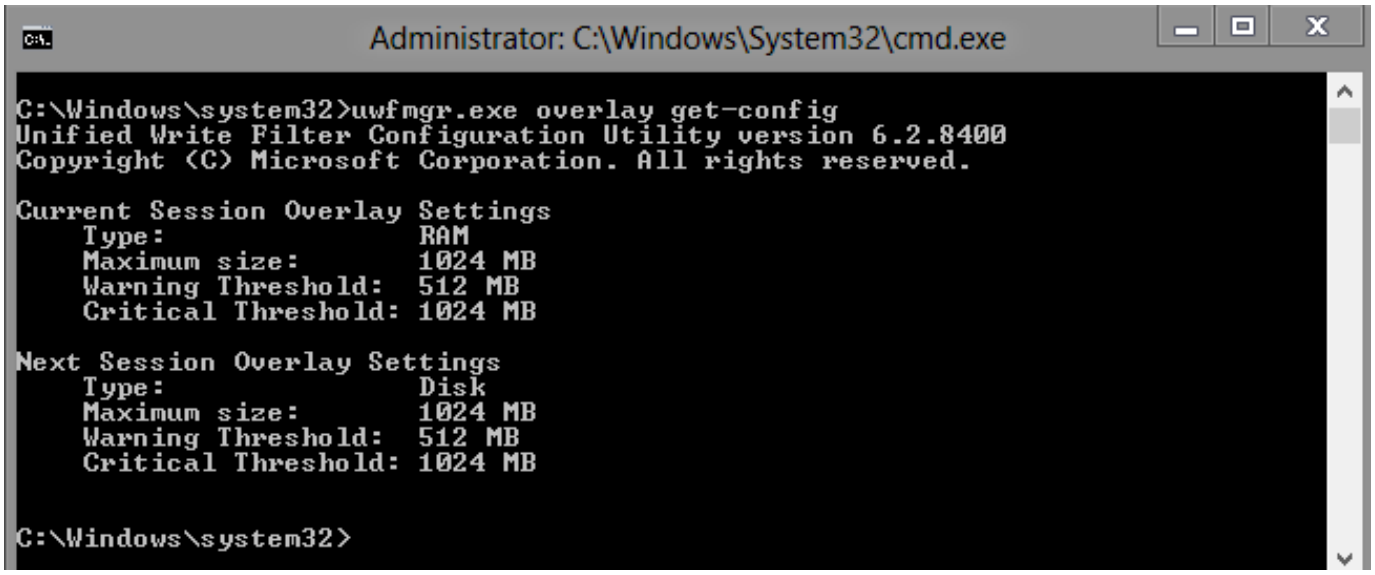
7. To change the overlay type, do the following:

   Note To change the overlay type, you must first disable UWF in the current session. To change overlay type to DISK mode, the overlay maximum size must be at least 1024M.

   a. To change overlay type from RAM to DISK, type `uwfmgr.exe overlay set-type DISK`.



   b. To verify that the overlay type will be DISK in the next session after you restart, type `uwfmgr.exe overlay get-config`.



Step 5: To configure HORM for a Standard 8 system

In this step, you will configure Hibernate Once/Resume Many (HORM) for a Standard 8 system.

1. On the embedded device, open a command prompt as an administrator. For Windows Shell, to open a command prompt, do the following:

   - In Windows Explorer, navigate to \Windows\System32,right-click cmd.exe, and then click **Run as Administrator**.
   - Accept the UAC prompt.

2. To enable hibernation on your device, type `powercfg /h on`.

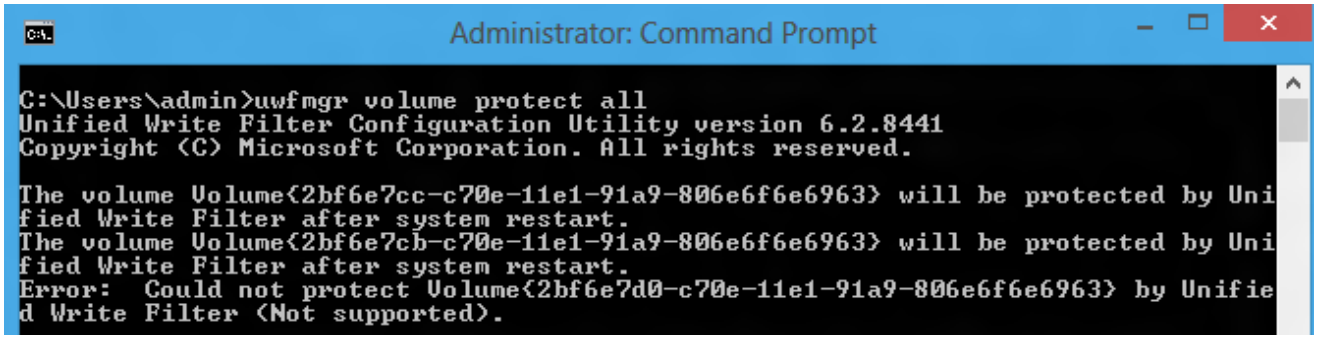
```
C:\Windows\system32>powercfg /h on

C:\Windows\system32>
```

3. To enable Unified Write Filter (UWF) on your device, type `uwfmgr filter enable`.

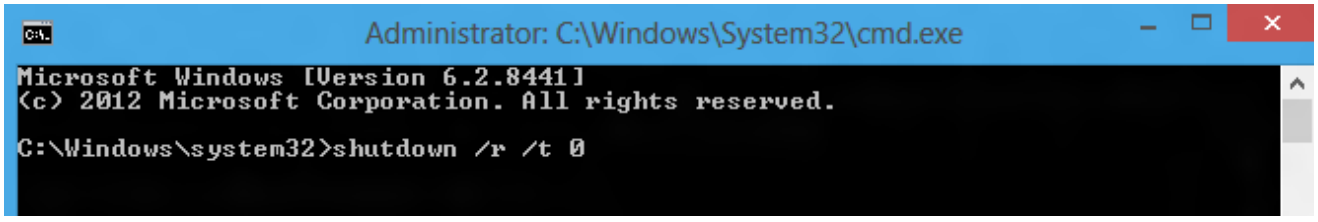
```
C:\Users\admin>uwfmgr filter enable
Unified Write Filter Configuration Utility version 6.2.8441
Copyright (C) Microsoft Corporation. All rights reserved.

Unified Write Filter is enabled after system restart.
```

4. To protect all volumes on your device, type `uwfmgr volume protect all`.

   Note DVD RW Drive and Floppy Drive throws an expected error that can be safely ignored.



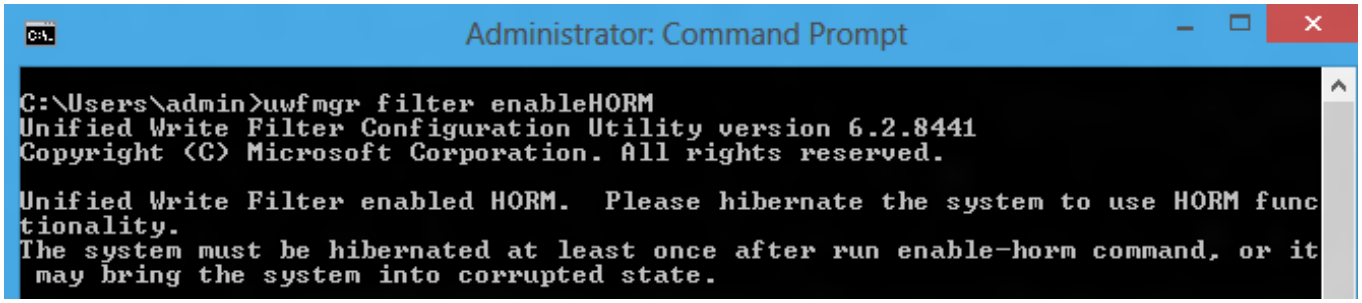
5. To restart your device to enable UWF, type `shutdown /r/t 0`.



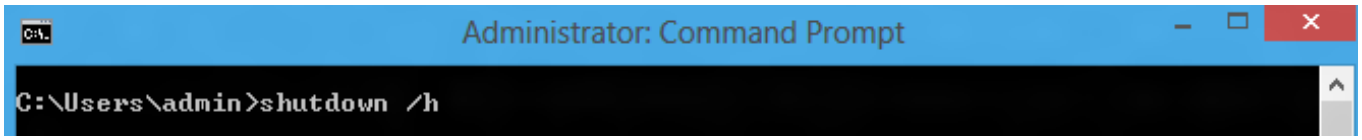
6. After your system restarts, to verify the UWF changes that you have made on your device, type `uwfmgr get-config`.


Administrator: Command Prompt
C:\Users\admin>uwfmgr get-config
Unified Write Filter Configuration Utility version 6.2.8441
Copyright (C) Microsoft Corporation. All rights reserved.
Current Session Settings
FILTER SETTINGS
Filter state: ON
HORM state: OFF
Pending commit: N/A
OVERLAY SETTINGS
Type: RAM
Maximum size: 1024 MB
Warning Threshold: 512 MB
Critical Threshold: 1024 MB
VOLUME SETTINGS
Volume Volume{2bf6e7cc-c70e-11e1-91a9-806e6f6e6963} [X:]
Volume state: Protected
Pending commit: No
Volume ID: Volume{2bf6e7cc-c70e-11e1-91a9-806e6f6e6963}
File Exclusions:
*** No exclusions
Volume Volume{2bf6e7cb-c70e-11e1-91a9-806e6f6e6963} [C:]
Volume state: Protected
Pending commit: No
Volume ID: Volume{2bf6e7cb-c70e-11e1-91a9-806e6f6e6963}
File Exclusions:
*** No exclusions
REGISTRY EXCLUSIONS
*** No exclusions
Next Session Settings
FILTER SETTINGS
Filter state: ON
HORM state: OFF
Pending commit: N/A
OVERLAY SETTINGS
Type: RAM
Maximum size: 1024 MB
Warning Threshold: 512 MB
Critical Threshold: 1024 MB
VOLUME SETTINGS
Volume Volume{2bf6e7cc-c70e-11e1-91a9-806e6f6e6963} [X:]
Volume state: Protected
Volume ID: Volume{2bf6e7cc-c70e-11e1-91a9-806e6f6e6963}
File Exclusions:
*** No exclusions
Volume Volume{2bf6e7cb-c70e-11e1-91a9-806e6f6e6963} [C:]
Volume state: Protected
Volume ID: Volume{2bf6e7cb-c70e-11e1-91a9-806e6f6e6963}
File Exclusions:
*** No exclusions
REGISTRY EXCLUSIONS
*** No exclusions

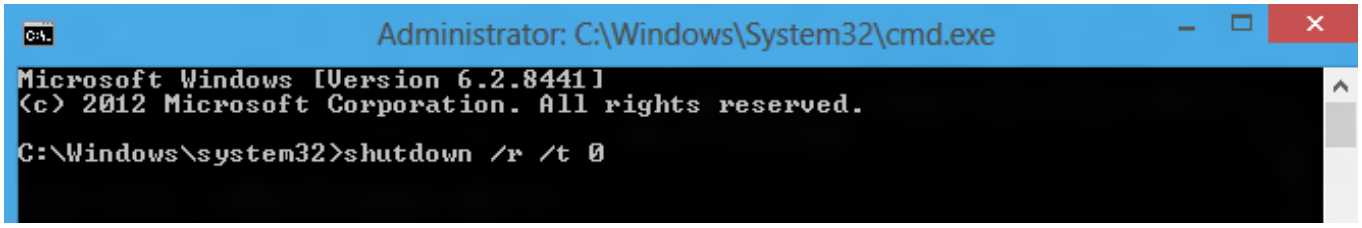
7. To enable HORM on your system, type `uwfmgr filter enablehorm`.
   Note Remove all file and registry exclusions before you enable HORM.



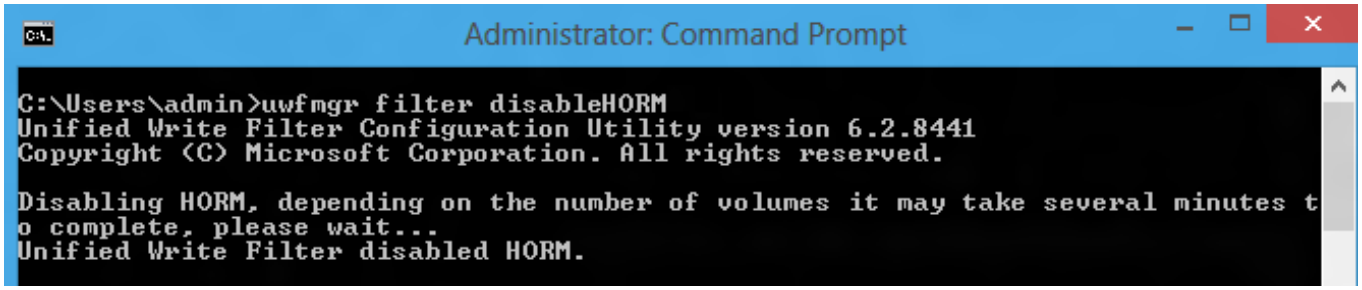
8. (Optional) In Control Panel, set the Power Option "When I press the power button" to avoid displaying the Command Prompt when resuming from hibernation, or use a script to close the command prompt on startup.
9. To hibernate the system one time to create an initial hibernation file at the command prompt, type `shutdown /h`.



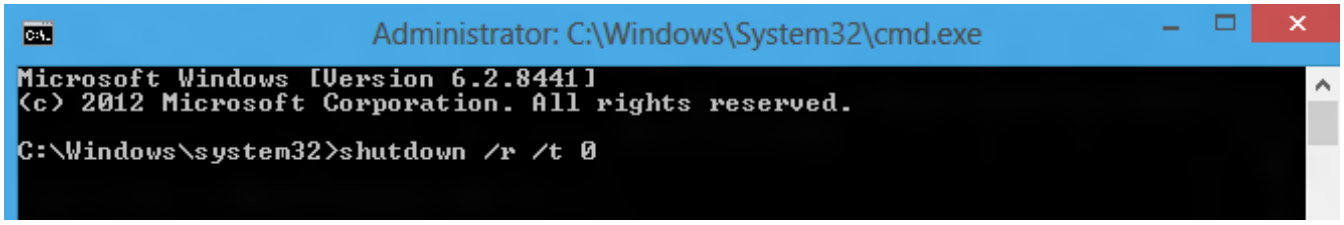
10. Press the power button to wake the system from hibernation.
11. After the system starts from hibernation to create an initial hibernation file, to shut down and restart the system, type `shutdown /r /t 0`.



12. When HORM is enabled, you cannot change the UWF configuration. To make changes, you must first disable HORM. To disable HORM, type `uwfmgr filter disablehorm`.



13. To restart the system to finish disabling HORM, type `shutdown /r /t 0`.



The system will restart normally with HORM disabled.

Conclusion

After completing this lab exercise, you will be able to do the following:

- Enable or disable a UWF filter.
- Add or remove volume protection.
- Add or remove a file and folder exclusion.
- Add or remove a registry key exclusion.
- Display overlay usage status and adjust its configuration.
- Configure and enable HORM on your device.