Windows Embedded Standard I filtri sui dischi e sul registro: UWF – Unified Write Filter

#### di [Beppe Platania](http://mvp.microsoft.com/it-it/mvp/Beppe%20Platania-4029281) - Microsoft eMVP

Blog: <http://beppeplatania.com/it>

* 1. cid:image002.png@01CE4D59.40AA6520

#### Riveduto e corretto da: [Gianni Rosa Gallina](http://mvp.microsoft.com/it-it/mvp/Gianni%20Rosa%20Gallina-4034912) - Microsoft eMVP

Blog: <http://gianni.rosagallina.com/it>

1. *Dicembre 2014*

Negli articoli precedenti ci siamo interessati ai filtri di scrittura in generale, dell’Enhanced Write Filter (EWF) e del File Based Write Filter (FBWF); in questo ci occuperemo di quello che va sotto il nome di filtro di scrittura unificato ***filtro-UWF*** (Unified Write Filter).

Il filtro di scrittura unificato (***filtro-UWF***) prende il nome proprio per la sua caratteristica di offrire sia le funzionalità del ***filtro-EWF*** (indirizzato ad una protezione sui settori del volume) sia quelle del ***filtro-FBWF*** (indirizzato ad una protezione basata su file e cartelle di un volume). Il ***filtro-UWF,*** inoltre, integra anche le funzionalità del ***filtro sul registro*** e ne offre di nuove.

Con l’introduzione del ***filtro-UWF*** avvenuta con Windows Embedded 8 Standard, gli altri tre filtri menzionati in precedenza sono diventati “sconsigliati” (deprecated) anche se nel configuratore ***ICE*** sono ancora presenti in una sezione dedicata della parte di “lockdown” denominata “Compatibility Write Filters”. Il motivo per cui non sono stati eliminati del tutti è legato al fatto di non voler costringere, chi avesse sviluppato applicativi che utilizzano le chiamate a questi filtri, di doverle aggiornare per allinearsi a quelle nuove del ***filtro-UWF.***

Il ***filtro-UWF*** lavora a livello di settore del volume, ma prevede comunque funzionalità che operano a livello di file e di registro. Come per gli altri filtri sui dischi, ***filtro-UWF*** intercetta le scritture che andrebbero su un settore del volume protetto e le memorizza in un overlay, poi, quando l’applicativo richiede delle letture dallo stesso settore il ***filtro-UWF*** le recupera direttamente dall’overlay.

Per permettere la gestione a livello di file-system il ***filtro-UWF*** fornisce un servizio che tiene conto di quali sono le cartelle e/o i file che vanno scritti direttamente sul volume fisico e non sull’overlay.

L’overlay del ***filtro-UWF*** può essere di tipo ***RAM Overlay*** e ***DISK Overlay***. Il primo tipo, che è quello di default, prevede un overlay in RAM con un dimensionamento configurabile. Il ***DISK Overlay*** prevede un overlay su un file di dimensione configurabile posizionato sul volume di sistema. La prima configurazione è consigliata in presenza di dischi flash o allo stato solido per limitare il più possibile le scritture. La seconda configurazione è consigliata quando si ha bisogno di proteggere il sistema da interventi non voluti, ma il volume di sistema è un disco rotante senza problemi di limiti di scrittura. Bisogna ricordare, inoltre, che, anche se l’overlay viene memorizzato su un file del volume di sistema, questi viene perso al riavvio.

Il ***filtro-UWF*** prevede un singolo overlay anche se i volumi da proteggere sono più di uno. Le variabili che configurano l’overlay, oltre al tipo, sono quelle che determinano e controllano la sua dimensione:

***OverlayMaximumSize*** che è la dimensione massima dell’overlay in MB;

***OverlayWarningThreshold*** è la soglia di attenzione per cui si può ottenere un avvertimento;

***OverlayCriticalThreshold*** è la soglia critica per cui si può sapere che l’overlay è pieno.

Con il termine volume di solito si individua una delle partizioni in cui può essere diviso un disco, ma ricordiamo che un volume può essere formato addirittura da più dischi. Il volume, che va selezionato sempre con una lettera di sistema con la variabile ***DriveLetter***, può essere poi memorizzato in due modi in accordo con la variabile ***Binding***:

Con il **DeviceID** che il sistema gli assegna al momento dell’abilitazione quando la variabile ***Binding*** vale “***Tight Binding***” che è la configurazione di default;

Con la lettera che il sistema gli assegna al momento dell’abilitazione (es. C:) quando la variabile ***Binding*** viene messa a “***Loose Binding***”;

Per la parte che riguarda il **filtro sul registro** che è stato integrato nel ***filtro-UWF***, ci sono tre parametri che si occupano della configurazione di questa parte:

**RegistryExceptionsUserDefined** che è la lista delle chiavi da escludere dalla protezione;

**DomainSecretKeyPersisted** che è una variabile booleana per escludere o meno la chiave segreta del Dominio;

**TSCALPersisted** che è una variabile booleana per escludere o meno la chiave di accesso dei client via RDP (Remote Desktop Protocol).

**Nota:** Per la lista delle chiavi di registro escludibili dal **filtro sul registro** esistono alcune limitazioni:

Come radice della chiave è ammessa soltanto **HKLM**.

Il ramo “System” non può essere garantito alcune chiavi vengono aggiornate prima che il servizio di UWF sia attivo.

## Prerequisiti di sistema

Nel pianificare l’utilizzo di questa funzionalità è bene controllare le caratteristiche del disco che si vuole proteggere e tutta una serie di prerequisiti di sistema:

***Modalità RAM*** 🡪 durante l’attivazione del ***filtro-UWF*** esso stesso crea un nuovo overlay in memoria che verrà riempito via via dalle memorizzazioni dei settori che vengono aggiornati. Se dei dati che fanno parte dei settori all’interno dell’overlay vengono cancellati, l’overlay diminuisce di dimensioni;

***Modalità DISK*** 🡪 durante l’attivazione del ***filtro-UWF*** esso stesso crea un nuovo file di overlay sul disco di sistema di dimensioni definite dalla variabile ***OverlayMaximumSize***.

La funzionalità ***HORM*** (Hibernate Once/Resume Many) è prevista soltanto con un overlay di tipo RAM.

Per tutti e due i tipi di overlay è possibile, a livello programmatico, essere avvertiti quando le dimensioni dell’overlay hanno superato la soglia di attenzione (***OverlayWarningThreshold***) o quella critica (***OverlayCriticalThreshold***).

Per le sue segnalazioni operative, il ***filtro-UWF*** utilizza il repository degli eventi di sistema (**Event Logs**). Quindi, in caso di problemi legati al funzionamento del ***filtro-UWF***, vi consigliamo di riferirvi ai messaggi di sistema sia per indagare personalmente sia per coinvolgere un qualsiasi supporto tecnico esterno.

Poiché, come vedremo tra poco, il ***filtro-UWF*** ha un’architettura che coinvolge sia l’area di sistema che l’area utente i messaggi verranno memorizzati, a seconda dei casi, nell’area corrispondente all’applicativo che li ha generati: “system” se generati dal servizio che si occupa dell’overlay, “application” se generati dai configuratori.

## Gli elementi del filtro-UWF

La tecnologia del ***filtro-UWF*** utilizza un certo numero di elementi che si occupano, ognuno per il proprio compito, di eseguire tutte le funzionalità che il filtro prevede: dalla gestione dell’abilitazione e disabilitazione all’avvio fino alla possibilità di memorizzare stabilmente i cambiamenti avvenuti fino ad un certo momento con una chiamata a sistema.

Il Modulo che contiene tutti questi elementi si chiama: “***UnifiedWriteFilter***”, nel catalogo è posizionato nel ramo: Features\Lockdown\Unified Write Filter (UWF)\ e contiene gli elementi descritti nella seguente tabella:

|  |  |
| --- | --- |
| Elemento | Descrizione |
| Uwfreg.sys  Uwfrtl.sys  Uwfs.sys  Uwfvol.sys | Sono i driver di sistema del ***filtro-UWF***. Come si può notare, dovendo intervenire a più livelli, il numero dei driver è maggiore di quello degli altri filtri sui dischi. Questi driver si occupano di intercettare le richieste di scrittura e lettura dal disco che si sta proteggendo indirizzando la funzione al disco fisico o all’overlay a seconda dei casi. |
| UwfServiceingSvc.exe  UwfServiceingShell.exe | Sono gli eseguibili dei servizi che gestiscono i vari elementi che compongono il ***filtro-UWF.*** |
| Uwfresources.dll  Uwfwmi.dll | Sono le DLL di supporto agli eseguibili dei vari elementi che compongono il ***filtro-UWF.*** |
| Uwfmgr.exe | Uwfmgr.exe (UWF Manager Console Application) è l’applicazione a riga commando che permette di conoscere lo stato del ***filtro-UWF*** e la sua configurazione attuale. Inoltre, offre una serie di comandi per modificare lo stato del ***filtro-UWF*** e la sua configurazione. (Più avanti vedremo la lista dei comandi in dettaglio) |
| Uwfservicingscr.scr | E’ lo screen-saver utilizzato durante l’aggiornamento di sistema (vedi ***UWF Servicing***). |

Nei parametri di configurazione presentati dal configuratore ***ICE*** per questa funzionalità, alcuni sono generici di tutti i filtri sui dischi:

|  |  |
| --- | --- |
| Nome | Descrizione |
| BootStatusPolicy | Determina, in caso di errori che si dovessero presentare all’avvio o al riavvio del sistema, quali debbano essere visualizzati. Poiché stiamo operando proprio per poter spegnere il dispositivo direttamente interrompendo l’alimentazione, è meglio evitare che, alla ripartenza del sistema, venga visualizzato un qualsiasi messaggio d’errore. I possibili valori sono:  DisplayAllFailures – Visualizza tutti gli errori;  IgnoreAllFailures – Non visualizzare errori (**default**);  IgnoreBootFailures – Non visualizzare gli errori di avvio del sistema;  IgnoreShutdownFailures – Non visualizzare gli errori di chiusura del sistema. |
| DisableAutoDefrag | Determina se disabilitare o meno il servizio di deframmentazione disco.  Questo servizio, utile se si sta lavorando con un disco rigido, diventa inutile e dannoso se si sta lavorando con una flash che ha già internamente un sistema di organizzazione delle scritture ottimizzato per la propria natura. I valori possibili sono soltanto:  **True**; Disabilita il Servizio (**default**);  **False**; Abilita il Servizio. |
| DisableSR | Determina se disabilitare o meno la memorizzazione dei dati “di ripristino” del sistema.  Nel nostro caso specifico, spesso conviene evitare che il sistema scriva dei dati “di ripristino” sul disco che, protetto dal ***filtro-UWF***, li scriverebbe di fatto in memoria e al riavvio, se non salvati con un comando specifico, li perderebbe.  0; Abilita la memorizzazione dei dati “di ripristino”;  1; Disabilita la memorizzazione dei dati “di ripristino” (**default**). |
| EnablePrefetcher | La funzionalità di “Prefetch” fa in modo che il sistema cominci a caricare dei dati degli applicativi più utilizzati dall’utente nella sessione prima ancora che questi ne chieda nuovamente il caricamento. Tutto questo velocizza i tempi di risposta percepiti dall’utente nel momento in cui richiede i successivi caricamenti.  0; Disabilita la funzionalità (**default**);  1; Abilita la funzionalità. |
| EnableSuperfetch | La funzionalità di “Superfetch” è una miglioria alla funzionalità di “Prefetch” estendendola oltre la sessione: il sistema memorizza gli applicativi più utilizzati dall’utente e comincia a precaricarli nella prossima sessione prima ancora che l’utente ne chieda il caricamento. Tutto questo velocizza i tempi di risposta percepiti dall’utente nel momento in cui richiede applicativi che aveva utilizzato nelle sessioni precedenti. In caso specifico di utilizzo del ***filtro-UWF***, questa memorizzazione verrebbe persa al riavvio e quindi in generale la funzionalità è meglio lasciarla disabilitata in modo da non affaticare il sistema con azioni inutili.  0; Disabilita la funzionalità (**default**);  1; Abilita la funzionalità. |
| PagingFiles | Determina il nome ed il posizionamento del file di ***paging*** del sistema. Il file di ***paging*** è il luogo dove il sistema si appoggia quando è in carenza di RAM. Nel nostro caso, dove stiamo utilizzando il ***filtro-UWF***, utilizzare un ***paging*** potrebbe portare ad un controsenso: il sistema è in carenza di RAM e tenta di scrivere su un ***paging*** file che è su un volume protetto e che quindi scriverebbe su un overlay che è esso stesso in RAM!!  Come **default** la funzionalità è disabilitata ed il valore di questo parametro è una stringa vuota. |

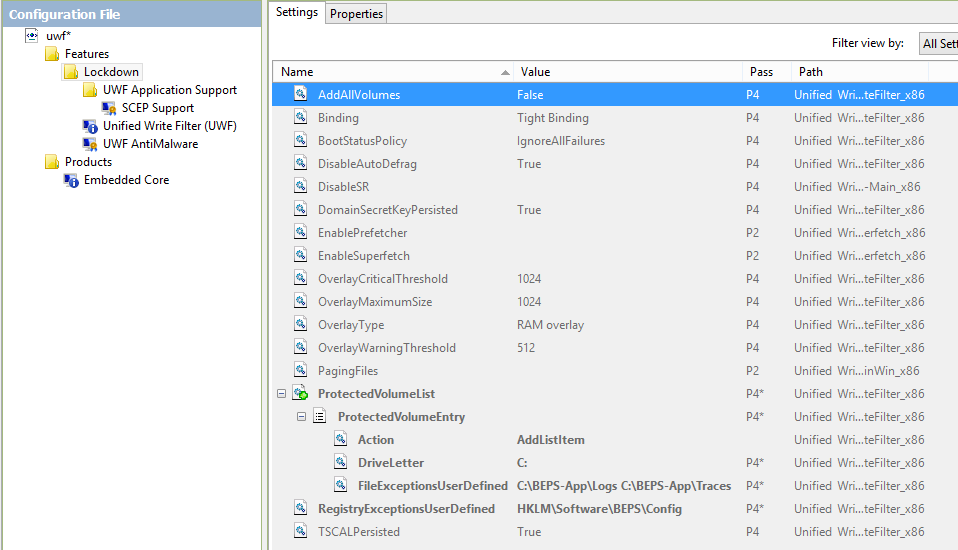
Altri parametri di configurazione sono specifici del ***filtro-UWF***:

|  |  |
| --- | --- |
| AddAllVolumes | Determinare se applicare il ***filtro-UWF*** a tutti i volumi del sistema.  **True**; Applica il filtro a tutti i volumi del sistema.  **False**; Non applica il filtro a tutti i volumi del sistema, ma si riferirà alle sezioni **ProtectedVolumeList** (**default**). |
| Binding | Seleziona il tipo di definizione del volume:   |  |  | | --- | --- | | Tipo | Descrizione | | Loose Binding | Il volume viene individuato tramite la sua lettera (es. **C:**). | | Tight Binding | Il volume viene individuato tramite il suo device-ID (**default**). | |
| DomainSecret  KeyPersisted | Determinare se escludere dal **filtro sul registro**, interno alla funzionalità di ***filtro-UWF***, la chiave di autenticazione del dominio (secret key).  **True**; Mantiene la memorizzazione della chiave (**default**);  **False**; Non esclude la chiave dal filtro e quindi questa verrà persa al prossimo riavvio. |
| OverlayCriticalThreshold | Determina il valore della soglia critica, in MB, per l’overlay del ***filtro-UWF***. Quando la dimensione dell’overlay raggiunge o supera questo valore di soglia critica, il servizio di controllo del ***filtro-UWF*** invia un evento di notifica. Il valore di default è 1024MB. |
| OverlayMaximumSize | Contiene il valore della massima dimensione del l’overlay del ***filtro-UWF***. Il valore è un numero intero espresso in MB. Il default è 1024MB. |
| OverlayType | Seleziona il tipo di overlay da utilizzare per il ***filtro-UWF***:   |  |  | | --- | --- | | Tipo | Descrizione | | RAM overlay | L’overlay è memorizzato in RAM (default). | | DISK overlay | L’overlay è memorizzato su un file (pre-allocato) del disco di sistema. |   NOTA: Anche se l’overlay è memorizzato su un file, con il riavvio tutti le modifiche verranno perse. |
| OverlayWarning  Threshold | Determina il valore della soglia di attenzione, in MB, per l’overlay del ***filtro-UWF***. Quando la dimensione dell’overlay raggiunge o supera questo valore di soglia, il servizio di controllo del ***filtro-UWF*** invia un evento di notifica. Il valore di default è 512MB |
| ProtectedVolumeList | Elenca la lista dei volumi (partizioni) che devono essere protette dal ***filtro-UWF***. Se il volume non è presente in questa lista, non potrà essere protetto a “run-time”.  Questo è un parametro “complesso” che prevede, per ogni volume inserito, un’ulteriore lista di parametri (vedi la prossima tabella). |
| RegistryExceptions  UserDefined | Contiene la lista delle chiavi di registro da escludere dal **filtro sul registro**, interno alla funzionalità di ***filtro-UWF***. Quando una chiave è inserita in questa lista, tutte le modifiche che subisce durante la sessione verranno “mantenute” anche dopo il riavvio. |
| TSCALPersisted | Determinare se escludere dal **filtro sul registro**, interno alla funzionalità di ***filtro-UWF***, la chiave di accesso dei client via RDP (Remote Desktop Protocol).  **True**; Mantiene la memorizzazione della chiave (**default**);  **False**; Non esclude la chiave dal filtro e quindi questa verrà persa al prossimo riavvio. |

Lista dei parametri per ogni volume configurato nel ***filtro-UWF***.

|  |  |
| --- | --- |
| Nome | Descrizione |
| Action | Determina come deve essere inizializzato il volume. I possibili valori sono:  **AddListItem** La configurazione del volume viene aggiunta all’immagine (**default**);  **Modify** La configurazione del volume viene aggiornata;  **RemoteListItem** La configurazione del volume viene rimossa. |
| DriveLetter | E’ la lettera del volume che si vuole proteggere. I valori permessi sono: da **C:** a **Z:** |
| FileExceptions  UserDefined | E’ la lista delle cartelle o dei file da escludere dalla protezione sul volume di questa sezione di configurazione.  Per inserire più cartelle e/o più file basterà elencarli uno sotto l’altro:  C:\BEPS-App\Logs  C:\BEPS-App\Traces |

Nella figura seguente vediamo come si presenta la configurazione dei parametri del ***filtro-UWF*** nel configuratore ICE.

* 1. 

## La configurazione del filtro-UWF a riga comando

***Uwfmgr.exe*** è l’applicativo a livello console che permette di interagire con i servizi e le configurazioni del ***filtro-UWF.*** L’applicazione può essere utilizzata da un utente senza privilegi di amministratore per ottenere informazioni sul filtro, ma per effettuare qualsiasi modifica si ha bisogno dei privilegi.

L’eseguibile si trova nelle cartelle di sistema (%windowsdir%\system32), quindi è accessibile da qualsiasi cartella. Molti comandi del ***filtro-UWF*** hanno bisogno di un riavvio per diventare operativi.

La sintassi:

* 1. Sintassi
  2. uwfmgr.exe
  3. Help | ?
  4. Get-Config
  5. Filter
  6. Help | ?
  7. Enable
  8. Disable
  9. Enable-HORM
  10. Disable-HORM
  11. Reset-Settings
  12. Volume
  13. Help | ?
  14. Get-Config {<volume> | all}
  15. Protect {<volume> | all}
  16. Unprotect {<volume> | all}
  17. File
  18. Help | ?
  19. Get-Exclusions {<volume> | all}
  20. Add-Exclusion <file>
  21. Remove-Exclusion <file>
  22. Commit <file>
  23. Registry
  24. Help | ?
  25. Get-Exclusions
  26. Add-Exclusion <key>
  27. Remove-Exclusion <key>
  28. Commit <key> [<value>]
  29. Overlay
  30. Help | ?
  31. Get-Config
  32. Get-AvailableSpace
  33. Get-Consumption
  34. Get-Files {<drive> | <volume>}
  35. Set-Size <size>
  36. Set-Type {RAM | DISK}
  37. Set-WarningThreshold <size>
  38. Set-CriticalThreshold <size>
  39. Servicing
  40. Enable
  41. Disable
  42. Update-Windows
  43. Get-Config
  44. Help

I parametri di questo comando, come si vede dall’elenco riportato nella sintassi sono divisi in sezioni che evidenzieremo con i titoli in grassetto e sottolineati, vediamoli in dettaglio:

|  |  |
| --- | --- |
| Nome | Descrizione |
| Help | ? | Visualizza l’help della sintassi generale. |
| Get-Config | Visualizza la configurazione del ***filtro-UWF*** e quella che avrà dopo il prossimo riavvio. |
| Filter | Questa è la sezione che configura i parametri dei filtri. |
| Help | ? | Visualizza l’help relativo ai comandi dei filtri. |
| Enable | Abilita il ***filtro-UWF*** al prossimo riavvio. I parametri utilizzati saranno quelli del momento del riavvio. |
| Disable | Richiede la disabilitazione del ***filtro-UWF*** al prossimo riavvio. |
| Enable-horm | Richiede l’attivazione della funzionalità di ***HORM*** senza aspettare il prossimo avvio. |
| Disable-horm | Richiede la disattivazione della funzionalità di ***HORM*** senza aspettare il prossimo avvio. |
| Reset-Settings | Ripristina la configurazione del ***filtro-UWF*** come era al momento dell’installazione. |
| Volume | Questa è la sezione che configura i parametri dei volumi. |
| Help | ? | Visualizza l’help relativo ai comandi sui volumi. |
| Get-Config  {<volume> | all} | Visualizza la configurazione del volume specificato (o di tutti i volumi se si è specificato ***all***) e quella che avrà (avranno) dopo il prossimo riavvio. |
| Protect  {<volume> | all} | Aggiunge il volume specificato (o tutti i volumi se si è specificato ***all***) dalla lista dei volumi che verranno protetti al prossimo riavvio con il ***filtro-UWF*** abilitato. |
| Unprotect  {<volume> | all} | Rimuove il volume specificato (o tutti i volumi se si è specificato ***all***) dalla lista dei volumi che verranno protetti al prossimo riavvio con il ***filtro-UWF*** abilitato. |
| File | Questa è la sezione che configura i parametri relativi alla lista di esclusione delle cartelle e/o dei file dal ***filtro-UWF***. |
| Help | ? | Visualizza l’help relativo ai comandi sui file. |
| Get-Exclusions  {<volume> | all} | Visualizza la lista di esclusione delle cartelle e/o dei file del volume specificato (o di tutti i volumi se si è specificato ***all***) e quella che avrà (avranno) dopo il prossimo riavvio. |
| Add-Exclusion <file> | Aggiunge la cartella (o il file) alla lista di esclusione del volume protetto dal ***filtro-UWF***. Questa esclusione sarà attiva al prossimo riavvio. |
| Remove-Exclusion <file> | Rimuove la cartella (o il file) dalla lista di esclusione del volume protetto dal ***filtro-UWF***. Questa esclusione sarà aggiornata al prossimo riavvio. |
| Commit <file> | Aggiorna il contenuto di un file NON protetto prendendo il suo valore dall’overlay e aggiornandolo sul volume fisico.  Il nome del file deve essere completo di volume e di percorso |
| Registry | Questa è la sezione che configura i parametri relativi alla parte di **filtro sul registro**. |
| Help | ? | Visualizza l’help relativo ai comandi sul registro. |
| Get-Exclusions | Visualizza la lista di esclusione delle chiavi di registro del ***filtro-UWF*** e quella che avrà (avranno) dopo il prossimo riavvio. |
| Add-Exclusion <key> | Aggiunge la chiave alla lista di esclusione delle chiavi. Questa esclusione sarà attiva al prossimo riavvio. |
| Remove-Exclusion <key> | Rimuove la chiave dalla lista di esclusione delle chiavi. Questa esclusione sarà aggiornata al prossimo riavvio. |
| Commit <key> [<Value>] | Aggiorna il contenuto di una chiave NON protetta con il valore scelto o, se la variabile <value> è omessa, aggiorna tutti i valori dalla radice della chiave specificata in avanti con il loro valore attuale. |
| Overlay | Questa è la sezione che configura i parametri relativi all’overlay. |
| Help | ? | Visualizza l’help relativo ai comandi sull’overlay. |
| Get-Config | Visualizza la configurazione attuale dell’overlay e quella che avrà dopo il prossimo riavvio. |
| Get-AvailableSpace | Visualizza la quantità di spazio disponibile per l’overlay del ***filtro-UWF.*** |
| Get-Consumption | Visualizza la quantità di spazio utilizzato dall’overlay del ***filtro-UWF.*** |
| Get-Files { <drive> | <Volume>} | Visualizza la lista dei file del volume contenuti nell’overlay. Il volume può essere indicato o con la sua lettera o con il suo Volume-ID. |
| Set-Size <size> | Assegna la dimensione dell’overlay in MB. Questa dimensione sarà effettiva al prossimo riavvio. |
| Set-Type {RAM | DISK} | Assegna il tipo di overlay da utilizzare: RAM oppure DISCO. Per selezionare il tipo DISCO (DISK) il ***filtro-UWF*** deve essere disabilitato. |
| Set-WarningThreshold <size> | Assegna la dimensione di soglia in MB che utilizzerà il servizio del ***filtro-UWF*** per notificare il suo superamento a livello di attenzione. |
| Set-CriticalThreshold <size> | Assegna la dimensione di soglia in MB che utilizzerà il servizio del ***filtro-UWF*** per notificare il suo superamento a livello di criticità. |
| Servicing | Questa è la sezione che configura i parametri relativi all’aggiornamento.  (vedi ***UWF Servicing*** più avanti) |
| Help | ? | Visualizza l’help relativo ai comandi all’aggiornamento. |
| Enable | Disabilita la modalità di aggiornamento per la prossima sessione di lavoro. |
| Disable | Abilita la modalità di aggiornamento per la prossima sessione di lavoro. |
| Update-Windows | Singolo comando per l’aggiornamento di Windows. Microsoft consiglia di utilizzare il comando Enable che, nel suo script, richiama questo singolo, ma lascia abilitato l’aggiornamento di Windows. |

Tutti questi parametri di configurazione e tutti i comandi che abbiamo scorso possono essere richiesti anche in forma programmatica interfacciandosi alla libreria WMI (Windows Management Instrumentation) oppure con dei comandi power-shell dall’interno di un’applicazione con tutti i vantaggi che questo comporta:

NON dover chiedere all’utente di effettuare operazioni da riga comando sul ***filtro-UWF***;

Effettuare le richieste nel momento opportuno (dal punto di vista programmatico) ad esempio per richiedere l’ibernazione quando tutti gli applicativi coinvolti hanno finito le loro inizializzazioni.

Poter “tracciare” su dei file di log le operazioni fatte in modo da poter controllare a posteriori ed evitare ogni contestazione.

## UWF Servicing

Con il termine **Servicing** si intende l’aggiornamento del sistema operativo quello, per intenderci, che in BIG Windows si effettua abilitando la funzionalità di ”Windows Update”. Generalmente per dei dispositivi Embedded si sconsiglia di effettuare aggiornamenti “senza uno stretto controllo” non tanto per una sfiducia nell’effetto che potrebbero avere degli aggiornamenti non preventivamente provati in laboratorio, ma soprattutto per non avere dispositivi nominalmente uguali, ma con livelli di aggiornamento diversi. Questa situazione, infatti, è uno dei fattori più problematici dell’assistenza sul campo.

Ci sono però dispositivi embedded esposti ad internet o soluzioni specifiche tipo i Thin-Client che possono aver bisogno di essere allineati con gli aggiornamenti di Windows. Per questo il ***filtro-UWF*** ha previsto tutta una serie di soluzioni per abilitare e disabilitare l’aggiornamento del sistema e, in particolare, delle cartelle contenenti i file di appoggio e i database degli anti-malware.

Gli elementi coinvolti in questa funzione sono:

***Uwfmgr.exe*** applicativo di configurazione e gestione del filtro-UWF a riga comando;

***UwfServicingScr.scr*** applicativo di screensaver che viene attivato durante l’aggiornamento;

***UwfServicingMasterScript.cmd*** comando di script che gestisce i singoli comandi di aggiornamento;

**E**mbedded **L**ockdown **M**anager (=***ELM***) applicativo di configurazione e gestione ad interfaccia grafica.

Quando si parla di aggiornamenti di sistema in ambiente embedded ci si riferisce sempre ad aggiornamenti **critici**, di **sicurezza** o di **driver**. Non si prevedono aggiornamenti legati a nuove versioni di applicativi o di pacchetti che non erano presenti al tempo della costruzione del sistema.

Per abilitare gli aggiornamenti di sistema si dovrà procedere in questo modo:

Attivare un prompt di comandi con privilegi di amministratore e spostarsi sulla cartella:

%windowsdir%\system32>

Abilitate il servizio di aggiornamento: > uwfmgr.exe servicing enable

Riavviate il sistema: >shutdown /r /t 0

Il sistema si riavvierà utilizzando un utente abilitato e creato al momento (**UWF-Servicing**) ed inizierà l’aggiornamento.

Durante l’aggiornamento verrà visualizzato lo screen-saver ***UwfServicingScr.scr*** che può essere personalizzato in modo da aiutare l’utente a capire cosa sta accadendo.

Il sistema verrà riavviato, se necessario e, se gli applicativi di aggiornamento incontreranno dei problemi, tutto verrà ripristinato come prima dell’inizio dell’aggiornamento ed il servizio verrà disabilitato.

Al termine senza problemi dell’aggiornamento il servizio verrà disabilitato e verranno riabilitate tutte le liste di esclusione sui file, sulle cartelle e sulle chiavi di registro.

## L’Antivirus in presenza di filtri di scrittura

In molte soluzioni Embedded c’è un uso di programmi di Antivirus, antimalware, ecc... questo perché con la parola Embedded si abbracciano numerose categorie di soluzioni: dai registratori di cassa alle macchine per il medicale, dalle macchine per l’industria ai chioschi informativi. Tutte le volte che bisogna lasciare il sistema “aperto”, senza filtri, senza la possibilità di limitare gli accessi al sistema dell’utente, senza la possibilità che l’utente non abbia privilegi da amministratore, allora l’uso di un antivirus è altamente consigliato. In molti altri casi, invece, quando si usano molti o tutti gli accorgimenti suggeriti in questo documento, l’uso di un antivirus può essere evitato, risparmiando così un notevole sforzo architetturale e organizzativo per tenerne aggiornate le definizioni.

L’utilizzo di un filtro di scrittura è uno di quegli accorgimenti che limita completamente la possibilità del virus di installarsi permanentemente nel sistema (ad ogni riavvio verrà perso con tutti i dati volatili della sessione). Se il dispositivo è sempre acceso (7/24), però, non soltanto i filtri di scrittura non aiutano (dal momento che la loro azione non avrebbe mai effetto, attendendo un riavvio che non arriverà), ma l’eventuale azione di un’applicazione malevola potrebbe continuare in memoria.

Per queste ragioni, nella versione Standard 8 sono stati introdotte delle funzionalità e degli accorgimenti che permettono di utilizzare agevolmente alcuni antivirus/antimalware anche in concomitanza con l’uso del ***filtro-UWF***.

Il primo passo per poter utilizzare queste funzionalità è quello di inserire i moduli opportuni nella costruzione del sistema:

UWF-Antimalware che fa parte del ramo lockdown;

SCEP-Support che fa parte del ramo lockdown\UWF Application Support

(SCEP è la sigla di “System Center EndPoint Protection”).

I due moduli aggiungono, nelle liste di esclusione del ***filtro-UWF***, le cartelle di lavoro e le chiavi di registro necessarie agli antivirus standard di Microsoft per lavorare correttamente.

UWF-Antimalware:

Cartelle

C:\Program Files\Windows Defender

C:\ProgramData\Microsoft\Windows Defender

C:\Windows\WindowsUpdate.log

C:\Windows\Temp\MpCmdRun.log

Chiavi di registro

HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows Defender

SCEP-Support:

Cartelle

C:\Microsoft\Security Client

C:\Windows\Windowsupdate.log

C:\Windows\Temp\Mpcmdrun.log

Chiavi di registro

HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Microsoft Antimalware

A questo punto potrebbe sorgere la domanda se altri antivirus possono essere utilizzati sui dispositivi embedded protetti da scrittura. La risposta è sì, conoscendo a sufficienza l’organizzazione delle cartelle e delle chiavi di registro si potrebbero aggiungere alle liste di esclusione, ma bisogna controllare se il produttore dell’antivirus che si vuole utilizzare ha dichiarato di conoscere e gestire questo sistema operativo embedded: Standard 8. Sul sito di Microsoft embedded: <http://www.microsoft.com/windowsembedded/en-us/catcatalog.aspx> potete trovare la lista degli applicativi dichiarati compatibili per un certa versione di Windows Embedded.

## Script e screen-saver per l’aggiornamento

***UwfServicingMasterScript.cmd*** è il comando di script che gestisce l’aggiornamento del sistema. Si trova nella cartella *%windowsdir%\system32* e può essere modificato perché possa eseguire, con le stesse modalità dell’aggiornamento di sistema, anche quello degli applicativi. Per far questo, intervenite sul paragrafo: :UPDATE\_SUCCESS del comando di script.

***UwfServicingScr.scr*** è l’applicativo di screensaver che viene attivato durante l’aggiornamento e, anche per lui, possiamo intervenire con una sua completa configurazione modificando queste chiavi di registro:

Windows Registry Editor Version 5.00

[HKEY\_LOCAL\_MACHINE\Software\Microsoft\Windows Embedded\ServicingScreenSaver]

"ColorBackground"=dword:000000ff

"ColorText"=dword:0000ff00

"ColorProgress"=dword:00ff0000

"ScreenSaverTitle"="Device"

"ScreenSaverSubTitle"="Servicing device…"

"HideScreenSaverText"=dword:00000000

"HideScreenSaverProgress"=dword:00000000

"Font"="Algerian";

## Il filtro-UWF e HORM (=Hibernate Once, Resume Many)

Come abbiamo discusso precedentemente introducendo la funzionalità di ibernare lo stato del sistema in un certo momento e memorizzando questo stato in un disco protetto da scrittura con il ***filtro-EWF***, questa tecnologia è presente anche con il ***filtro-EWF*** a patto che questi sia utilizzato in modo opportuno.

Per utilizzare la funzionalità di ***HORM***, infatti, il ***filtro-EWF*** deve essere abilitato per poter attivare a sua volta l’***HORM*** e la configurazione del ***filtro-EWF*** deve sottostare a queste raccomandazioni:

Tutti i volumi montati al momento dell’ibernazione devono essere protetti dal ***filtro-EWF***;

Non devono essere presenti liste di esclusione né di file o cartelle né di chiavi di registro;

L’overlay del ***filtro-EWF*** deve essere di tipo RAM.

Controllare la configurazione delle power option del sistema poiché il ***filtro-EWF*** NON protegge il file d’ibernazione dagli altri eventuali comandi di ibernazione del sistema. Quindi, se il sistema è configurato in modo che dopo un certo tempo va in “sleep” questo vuol dire che viene effettuata una sovrascrittura del file hiberfile.sys alterando le nostre aspettative del funzionamento dell’***HORM***.

Per abilitare l’***HORM*** sul disco di sistema C: si dovrà procedere in questo modo:

Attivare un prompt di comandi con privilegi di amministratore e spostarsi sulla cartella:

%windowsdir%\system32>

Abilitate il ***filtro-EWF***: >uwfmgr.exe filter enable

Proteggete tutti i volumi del sistema: >uwfmgr.exe volume protect all

Riavviate il sistema: >shutdown /r /t 0

Attivate le applicazioni ed i servizi che riterrete opportuni fino ad arrivare al momento in cui volete effettuare l’ibernazione del sistema (che diverrà lo stato di partenza da questo momento in avanti).

Attivare un prompt di comandi con privilegi di amministratore e spostarsi sulla cartella:

%windowsdir%\system32>

Per abilitate l’ibernazione sul sistema: >powercfg /h on

Per abilitare la funzionalità di ***HORM***: >uwfmgr.exe filter enable-horm

Per effettuare l’ibernazione: > shutdown /h

Premere il tasto di alimentazione per far ripartire il sistema dopo che ha memorizzato il file d’ibernazione;

Quando è attivata la funzionalità di ***HORM*** NON si possono effettuare modifiche alla configurazione del ***filtro-EWF***.

Per disabilitare l’***HORM*** si dovrà procedere in questo modo:

Attivare un prompt di comandi con privilegi di amministratore e spostarsi sulla cartella:

%windowsdir%\system32>

Disabilitate la funzionalità di ***HORM***: > uwfmgr.exe filter disable-horm

Riavviate il sistema: >shutdown /r /t 0

Il sistema ripartirà normalmente e NON dal hiberfile.sys.

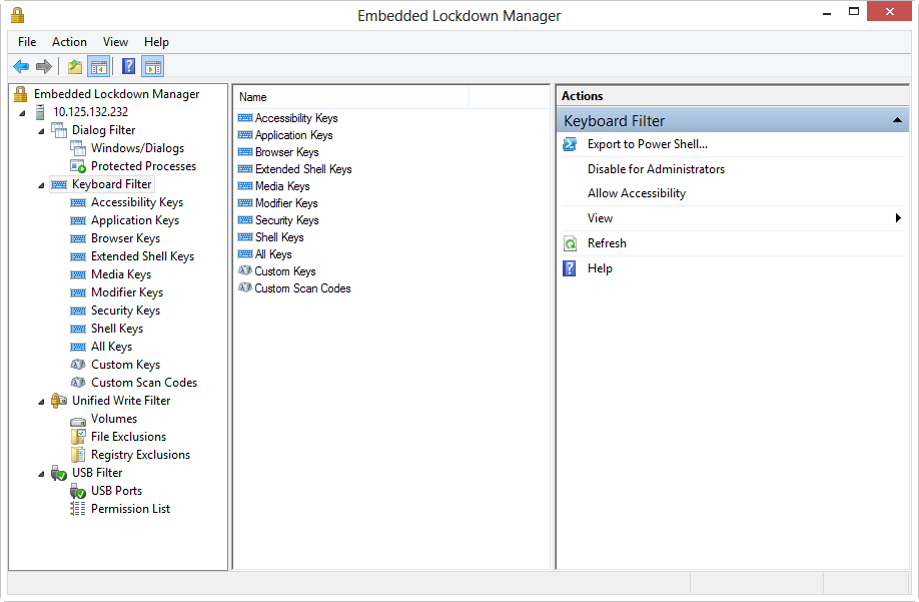
Come si evince da questo paragrafo la funzionalità di ***HORM*** anche se ha dei benefici sul tempo di disponibilità dell’applicazione (tempo di avvio del sistema più il tempo di lancio delle applicazioni), risulta una procedura abbastanza complessa. Prima di scegliere di utilizzarla, vi consigliamo di valutare bene se l’avvio normale di Windows Embedded 8 Standard non sia già soddisfacente per le vostre esigenze.

## Configurazione del filtro-UWF mediante ELM (Embedded Lockdown Manager)

Un altro modo di configurare i parametri del filtro è quello di utilizzare un nuovo snap-in della Console di manutenzione di Windows (**MMC** = **M**icrosoft **M**anagement **C**onsole) che si chiama **ELM** (**E**mbedded **L**ockdown **M**anager). Questo strumento, creato proprio per le esigenze di Windows Embedded, ha un’interfaccia utente grafica e permette di configurare, oltre al filtro sul disco, anche altre funzionalità che aiutano a proteggere il sistema operativo bloccando ogni tentativo di accesso al sistema: filtro sulla tastiera, filtro dei messaggi, scelta della Shell di avvio, ecc… da cui **lockdown.**

**ELM** è un nuovo tool di Windows Embedded 8 ed è così importante che merita di essere affrontato in un capitolo dedicato.

Riportiamo soltanto un esempio di come si presenta:



Riepilogando il ***filtro-UWF*** protegge uno o più volumi operando in memoria o su un file di un disco in cui crea un overlay che può essere controllato programmaticamente. Questo filtro, oltre a offrire allo stesso tempo le funzionalità del filtro-EWF e del filtro-FBWF, ci presenta nuove soluzioni per semplificare l’aggiornamento del sistema e per gestire al meglio la sua convivenza con gli antivirus.

#### di [Beppe Platania](http://mvp.microsoft.com/it-it/mvp/Beppe%20Platania-4029281) - Microsoft eMVP

Blog: <http://beppeplatania.com/it>

#### Riveduto e corretto da: [Gianni Rosa Gallina](http://mvp.microsoft.com/it-it/mvp/Gianni%20Rosa%20Gallina-4034912) - Microsoft eMVP

Blog: <http://gianni.rosagallina.com/it>