



# Windows XP mit Schreibschutz

Ein flexibler Schreibschutz macht Ihr System unverwundbar. Viren und Trojaner haben keine Chance. Programme lassen sich gefahrlos ausprobieren, ohne Spuren zu hinterlassen.

**W**enn Sie spezielle Treiber unter Windows XP installieren, erhalten Sie einen Schreibschutz für Ihr System, der sich beliebig ein- und ausschalten lässt. Bei aktivem Schreibschutz ist das Betriebssystem nach einem Neustart im gleichen Zustand wie zu dem Zeitpunkt, an dem der Schreibschutz aktiviert wurde. Somit sind auch Viren, Trojaner oder andere Schadprogramme beseitigt.

## Kompakt

- *Der Artikel zeigt, wie Sie für XP einen Schreibschutz einrichten, der sich beliebig ein- und ausschalten lässt.*
- *Der Schreibschutz lenkt alle Aktivitäten in den Arbeitsspeicher um.*
- *Sie benötigen nur spezielle Treiber aus der kostenlosen Testversion von Windows XP Embedded.*

Auch wenn Sie häufig Programme testen, sicher surfen oder einfach keine Spuren hinterlassen wollen, bietet sich ein Schreibschutz an.

**So geht's:** Technisch basiert der Schreibschutz auf den EWF-Filtern von Windows XP Embedded. EWF steht für Enhanced Write Filter, also erweiterter Schreibschutz. Windows XP Embedded kommt zum Beispiel in Systemen für Registrierkassen oder Telefonzellen zum

**Inhalt**

**Windows XP mit Schreibschutz**

- **Vorbereitung**
  - Windows Embedded herunterladen 5.23
  - EFW-Treiber extrahieren 5.23
  - Windows vorbereiten 5.24
- **Installation**
  - EFW-Treiber installieren 5.25
  - Registry anpassen 5.25
- **Konfiguration**
  - Schreibschutz testen 5.26
  - Schreibschutz per Knopfdruck 5.26
- **Alternative**
  - Schreibschutz mit FBWF 5.31
- XP mit Schreibschutz: So geht's 5.23
- Software-Übersicht 5.24

Einsatz, in denen keine Festplatte vorhanden ist. Die EFW-Treiber sorgen dafür, dass bei aktivem Schreibschutz Windows sämtliche Daten statt auf die Festplatte in den Arbeitsspeicher schreibt. Schreibvorgänge erfolgen außerdem sehr schnell, da sie im RAM ablaufen.

Um an die EFW-Treiber zu gelangen, laden Sie zunächst die kostenlose Testversion von Windows XP Embedded herunter. Daraus extrahieren Sie dann die EFW-Treiber. Ein spezielles Tool schaltet den Schutz nach Belieben ein oder aus. Wenn Sie etwa ein verdächtiges Programm testen oder auf verdächtigen Seiten surfen wollen, dann schalten Sie den Schreibschutz an. Anschließend schalten Sie ihn wieder aus. Auf Wunsch lassen sich alle Änderungen seit dem letzten Systemstart per Knopfdruck auf die Festplatte übernehmen.

Alles, was Sie benötigen, ist eine Internetverbindung und etwas Zeit.

**Vorbereitung**

Der Schreibschutz basiert auf den EFW-Treibern von Windows XP Embedded. Der Weg zu den benötigten Dateien ist etwas mühsam. Obwohl Sie nur wenige Dateien benötigen, die zusammen nicht einmal 400 KByte groß sind, müssen Sie dafür ein komplettes Betriebssystem herunterladen.

**Windows Embedded herunterladen**

EFW ist ein Bestandteil des Betriebssystems Windows XP Embedded (kostenlose Testversion, <http://microsoft.com/windows/embedded/en-us/download/default.aspx>).

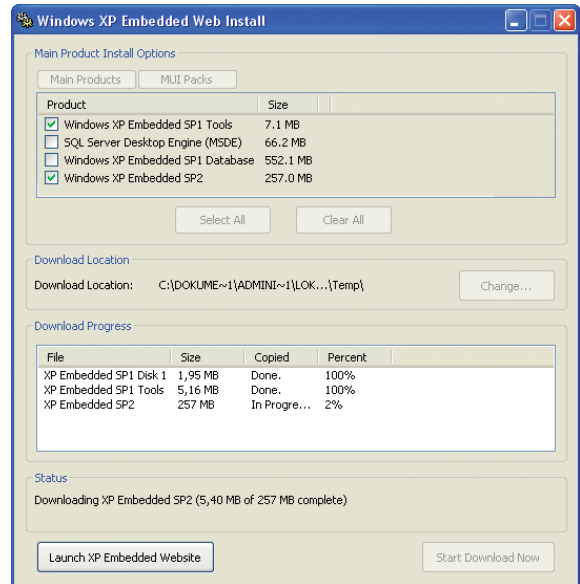
Um an die EFW-Treiber zu gelangen, laden Sie die kostenlose 120-Tage-Testversion herunter. Dazu müssen Sie sich zunächst bei Microsoft registrieren.

Klicken Sie danach auf der Download-Seite auf „Windows XP Embedded“ und im folgenden Fenster auf „Windows XP Embedded SP2 Evaluation Edition“. Sie erhalten eine kleine Datei namens „XPEFFI.exe“. Rufen Sie diese auf.

Ein Download-Manager startet. Hier wählen Sie die Pakete „Windows XP Embedded SP1 Tools“ und „Windows XP Embedded SP2“ aus. Ein Mausklick auf den Button „Start Download Now“

lädt die ausgewählten Dateien herunter. Sie sind zusammen rund 265 MByte groß (Bild A).

Nach dem Download der Pakete erscheint eventuell ein Fenster mit einem Warnhinweis, den Sie mit „OK“ quittieren. Danach lädt automatisch ein weiteres Programm, das Sie mit „Exit“ sogleich wieder beenden. Nun haben Sie alles, was Sie brauchen.



**Windows XP Embedded:** Laden Sie eine kostenlose Testversion dieses Betriebssystems herunter, um an die EFW-Treiber zu gelangen (Bild A)

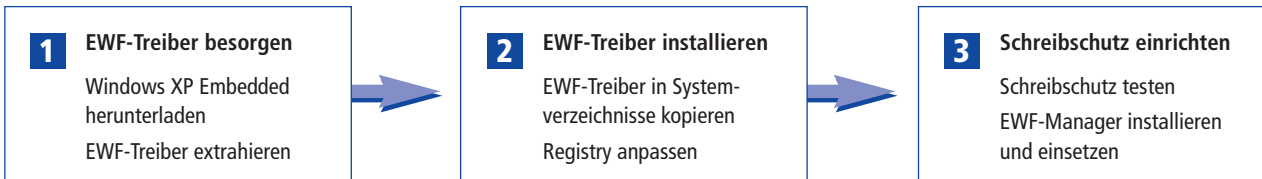
**EFW-Treiber extrahieren**

In diesem Abschnitt destillieren Sie die EFW-Treiber aus Windows XP Embedded heraus. Eine Installation des Betriebssystems ist dazu nicht notwendig.

Sie finden die im vorherigen Abschnitt heruntergeladenen Dateien standardmäßig im Verzeichnis ▶

**XP mit Schreibschutz: So geht's**

Für den Schreibschutz benötigen Sie spezielle Treiber aus Windows XP Embedded. Diese EFW-Treiber sorgen dafür, dass Windows alle Daten statt auf die Festplatte in den Arbeitsspeicher schreibt. Der Schreibschutz lässt sich nach Bedarf ein- und ausschalten.



„C:\Dokumente und Einstellungen\  
<benutzername>\Lokale Einstellungen  
\Temp“. Die Dateien heißen „Disk1.  
cab“, „Tools.cab“ und „WINDOWS\_XP  
\_EMBEDDED\_SP2E.EXE“. Wenn Sie  
das Verzeichnis nicht sehen, ändern Sie  
die Ordneroptionen im Windows-Ex-  
plorer entsprechend ab.

Entpacken Sie die CAB-Dateien mit  
Ihrem Packprogramm. Wenn dieses das  
CAB-Format nicht erkennt, verwenden  
Sie 7-Zip 4.65 (kostenlos, [www.7-zip.org](http://www.7-zip.org)  
und auf ).

Sie erhalten ein neues Verzeichnis  
namens „DISK1“. Gehen Sie dort in  
den Unterordner „Tools“ und rufen Sie  
die Datei „WINDOWS XP EMBEDDED  
TOOLS SP1.MSI“ auf. Sie benötigen  
nun eine Seriennummer. Diese befindet  
sich in der Datei „productkey.txt“ im  
Ordner „DISK1“. Wählen Sie als Instal-  
lationsart „Typical“ und als Installa-  
tionsort „This computer“.

Anschließend finden Sie unter  
„C:\Programme\Windows Embedded“  
eine weitere benötigte Datei namens  
„xpesp2.exe“. Sie befindet sich im Un-  
terordner „Installer\disk3“.

Diese Datei ist ebenfalls gepackt.  
Klicken Sie sie doppelt an und merken  
Sie sich, in welches Verzeichnis sie die  
darin enthaltenen Dateien extrahiert.  
Nach dem Entpacken erscheint ein

### Software-Übersicht

Programm	Quelle	Seite
7-Zip 4.65 (Open-Source-Packprogramm)	<a href="http://www.7-zip.org">www.7-zip.org</a>	24
EWF-Installer (Batch-Datei)	<a href="http://www.com-magazin.de/ergaenzungen">www.com-magazin.de/ergaenzungen</a>	25
„ewf.reg“ (Registry-Einträge)	<a href="http://www.com-magazin.de/ergaenzungen">www.com-magazin.de/ergaenzungen</a>	25
FBWF-Installer (Batch-Datei)	<a href="http://www.com-magazin.de/ergaenzungen">www.com-magazin.de/ergaenzungen</a>	31
„fbwf.reg“ (Registry-Einträge)	<a href="http://www.com-magazin.de/ergaenzungen">www.com-magazin.de/ergaenzungen</a>	31
Simple EWF-Manager 1.0.0.66 (EWF-Manager)	<a href="http://www.com-magazin.de/ergaenzungen">www.com-magazin.de/ergaenzungen</a>	26
Windows XP Embedded SP 2 (Betriebssystem)	<a href="http://www.microsoft.com/windowseembedded/en-us/downloads/default.mspx">www.microsoft.com/windowseembedded/en-us/downloads/default.mspx</a>	23
Windows XP Embedded SP 2 Feature Pack 2007 (Zusatzpakete)	<a href="http://www.microsoft.com/windowseembedded/en-us/products/wexpe/getting-started.mspx">www.microsoft.com/windowseembedded/en-us/products/wexpe/getting-started.mspx</a>	31

Alle -Programme finden Sie auf Heft-CD und -DVD in der Rubrik „Computer, XP mit Schreibschutz“.

Fenster „Database Backup“. Schließen  
Sie dieses Fenster nicht. Wechseln Sie  
stattdessen in das Verzeichnis, dessen  
Namen Sie sich soeben gemerkt haben.  
Hier liegen endlich die benötigten  
EWF-Dateien. Suchen Sie über die  
Suchfunktion des Windows-Explorers  
nach allen Dateien, die mit „ewf“ be-  
ginnen. Sie erhalten sechs Treffer (**Bild B**).

Kopieren Sie diese sechs Dateien in  
ein beliebiges Verzeichnis, in dem Sie  
sie später leicht wiederfinden.

Beenden Sie dann das noch geöffne-  
te Fenster „Database Backup“ mit  
„OK“. Brechen Sie den Wizard zur In-  
stallation von Windows XP Embedded  
mit „Cancel“ und „Ja“ ab.

Zum Schluss räumen Sie das ganze  
Durcheinander wieder auf. Starten Sie  
dazu die Datei „WINDOWS XP EMBED  
DED TOOLS SP1.MSI“ aus dem Ver-  
zeichnis „DISK1\TOOLS“ und entfer-  
nen Sie die Windows XP Embedded  
Tools. Löschen Sie alle in diesem Ab-  
schnitt erzeugten Verzeichnisse und Da-  
teien, natürlich mit Ausnahme der müh-  
sam gewonnenen EWF-Dateien.

### Windows vorbereiten

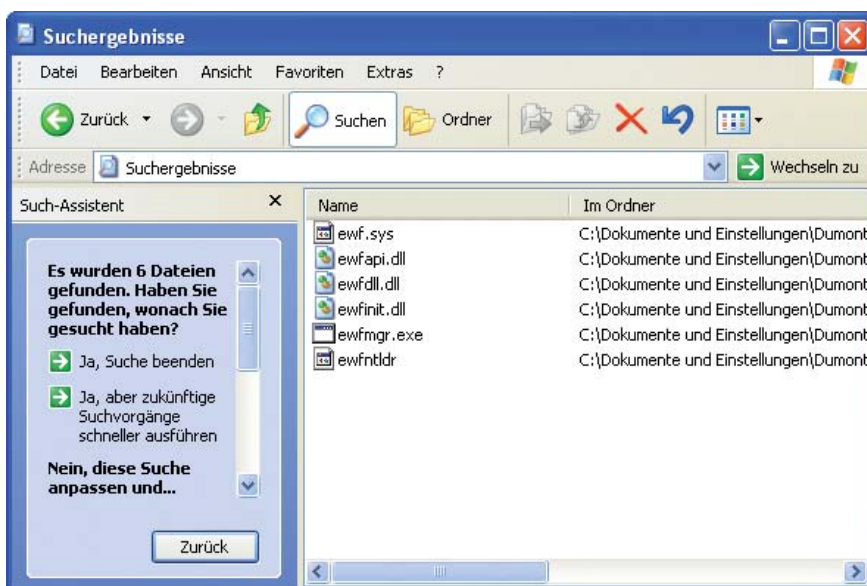
In diesem Abschnitt erledigen Sie op-  
tional einige Handgriffe, mit denen das  
schreibgeschützte Windows später flot-  
ter arbeitet.

Falls Ihre Festplatte mehrere Partitio-  
nen hat, empfiehlt es sich, die Auslage-  
rungsdatei „pagefile.sys“ auf eine Part-  
ition zu verlagern, die nicht schreibge-  
schützt werden soll. Ansonsten versucht  
Windows im Extremfall, den Arbeits-  
speicher in sich selbst auszulagern.

Rufen Sie dazu die Systemsteuerung  
auf und wechseln Sie zum Unterpunkt  
„Leistung und Wartung, System“. Dort  
klicken Sie im Reiter „Erweitert“ im Be-  
reich „Systemleistung“ auf den Button  
„Einstellungen“. Das Fenster „Leis-  
tungsoptionen“ erscheint.

Hier finden Sie im Reiter „Erweitert“  
den Bereich „Virtueller Arbeitsspei-  
cher“. Ein Klick auf „Ändern“ führt Sie  
zu Einstellungen wie Größe und Parti-  
tion der Auslagerungsdatei.

Um auf Nummer sicher zu gehen,  
lässt sich die Auslagerungsdatei auch



EWF-Treiber: Diese sechs Dateien sorgen für einen Schreibschutz von Windows XP (**Bild B**)


komplett deaktivieren (Bild C). Gegebenenfalls deaktivieren Sie auch die Systemwiederherstellung. Zu der entsprechenden Option gelangen Sie in der Systemsteuerung über „Leistung und Wartung, System, Systemwiederherstellung“.

Leistungsfördernd ist es ebenfalls, die temporären Dateien des Browsers auf eine nicht geschützte Partition auszulagern.

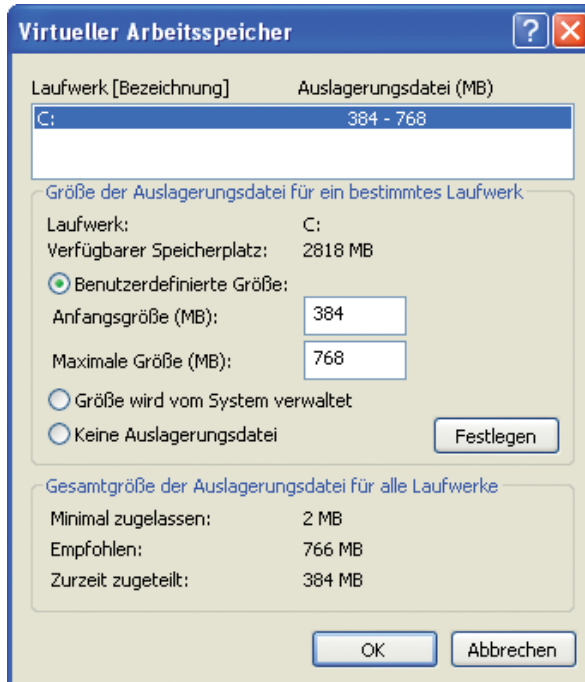
## Installation

In diesem Abschnitt installieren Sie die EWF-Dateien und passen anschließend die Registry entsprechend an.

### EWF-Treiber installieren

Um die EWF-Treiber zu installieren, kopieren Sie einfach die EWF-Dateien an die richtige Stelle im Betriebssystem. Sie können das von Hand erledigen oder Sie verwenden den EWF-Installer der com!-Redaktion (kostenlos, [www.com-magazin.de/ergaenzungen](http://www.com-magazin.de/ergaenzungen) und auf ).

Um den Installer zu verwenden, kopieren Sie die Datei „EWF-Installer.cmd“ zunächst in das Verzeichnis, in dem die EWF-Dateien liegen. Dort rufen Sie die Datei auf. Sie kopiert die sechs EWF-Dateien an die richtige Stelle, legt eine Sicherheitskopie der Datei „ntldr“ namens „ntldr.alt“ an und be-

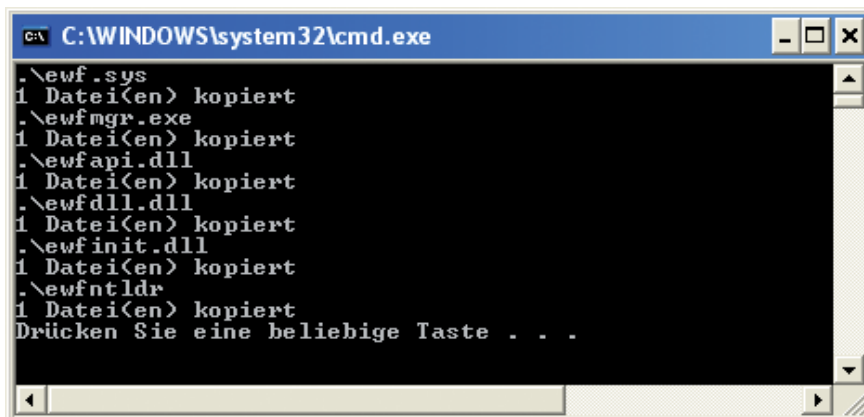


**Virtueller Arbeitsspeicher:** Hier verschieben oder deaktivieren Sie die Auslagerungsdatei von Windows XP (Bild C)

nennt die Datei „ewfntldr“ in „ntldr“ um (Bild D).

Wenn Sie dies lieber manuell erledigen wollen, dann kopieren Sie die Datei „ewf.sys“ in das Verzeichnis „C:\WINDOWS\system32\drivers“ und die übrigen Dateien mit Ausnahme von „ewfntldr“ in das Verzeichnis „C:\WINDOWS\system32“.

Benennen Sie in „C:\“ die Datei „ntldr“ zum Beispiel in `ntldr.alt` um und kopieren Sie die Datei „ewfntldr“ in dieses Verzeichnis. Schließlich benennen Sie „ewfntldr“ in `ntldr` um.



**EWF-Installer:** Das Tool kopiert die EWF-Dateien in die richtigen Verzeichnisse (Bild D)

### Registry anpassen

In diesem Abschnitt machen Sie Windows XP mit den EWF-Treibern bekannt. Dies geschieht über die Registry.

Da beim Abtippen der langen Registryschlüssel leicht ein Fehler passiert, verwenden Sie dazu die Datei „ewf.reg“ (kostenlos, [www.com-magazin.de/ergaenzungen](http://www.com-magazin.de/ergaenzungen) und auf ). Dennoch ist zunächst ein wenig Handarbeit nötig: Öffnen Sie den Registrierungs-Editor mit [Windows R], dem Kommando `regedit` und einem Klick auf „OK“.

Für den Fall, dass etwas schiefgeht, erstellen Sie erst einmal über den Menüpunkt „Datei, Exportieren...“ eine Sicherheitskopie der Registry.

Navigieren Sie dann zum Schlüssel „HKEY\_LOCAL\_MA-

CHINE\SYSTEM\CurrentControlSet\Enum\Root“ und klicken Sie den Eintrag mit der rechten Maustaste an. Wählen Sie im Kontextmenü den Punkt „Berechtigungen...“. Klicken Sie oben auf „Jeder“ und setzen Sie bei „Vollzugriff“ ein Häkchen in der Spalte „Zulassen“ (Bild E). Anschließend öffnen Sie die Datei „ewf.reg“ mit einem beliebigen Texteditor.

**Wichtig:** Der Eintrag in der letzten Zeile muss identisch sein mit dem Windows-Boot-Eintrag in der Datei „boot.ini“, die im Normalfall unter „C:\“ zu finden ist. In den meisten Fällen lautet der korrekte Eintrag

```
1 "ArcName" = "multi(0)disk(0)
rdisk(0)partition(1) "
```

Ändern Sie dies gegebenenfalls ab und speichern Sie die Datei. Dabei sind `multi` und `disk` die Nummern des Controllers und des Busses und deren Werte fast immer 0; `rdisk` bezeichnet die Nummer der Festplatte (0 und 1 für die primären Platten am Master/Slave-Port, 2 und 3 für die sekundären Platten am Master/Slave-Port). Schließlich ▶

gibt `partition` die Nummer der Partition an, auf der sich das Betriebssystem befindet. Hier beginnt die Zählung bei 1.

Klicken Sie nun die Datei „`ewf.reg`“ doppelt an, um die darin enthaltenen Registry-Einträge einzutragen.

Heben Sie die Berechtigung für „Jeder“ wieder auf: Entfernen Sie das Häkchen bei „Vollzugriff“ in der Spalte „Zulassen“.

Nach einem Neustart ist der Schreibschutz aktiv. Statt auf die Festplatte schreibt Windows dann alle Dateien und Änderungen in den Arbeitsspeicher.

Keine Sorge, wenn Sie beim Start eine Meldung erhalten, dass Windows nicht korrekt starten konnte: Das liegt an der gesperrten Auslagerungsdatei. Wählen Sie dann die Option „Start Windows Normally“.

## Konfiguration

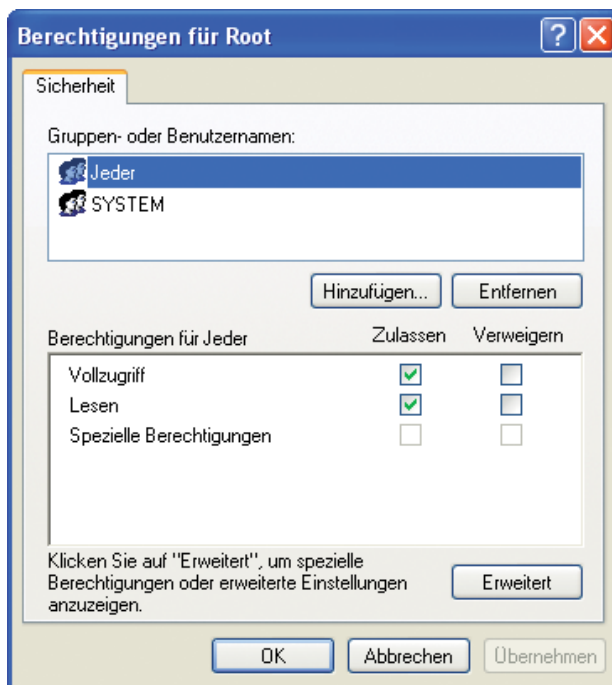
Die Installation der EWF-Treiber ist damit abgeschlossen. Nun richten Sie den Schreibschutz so ein, dass Sie ihn bequem bedienen und nach Belieben ein- und ausschalten können.

### Schreibschutz testen

Prüfen Sie zunächst, ob der Schreibschutz überhaupt funktioniert. Dazu ändern Sie den Bildschirmhintergrund oder löschen eine unwichtige Datei. Starten Sie Ihren PC neu. Wenn das Bild auf dem Desktop wieder das alte ist oder die im Schreibschutzmodus gelöschte Datei wieder da ist, dann funktioniert der Schreibschutz.

### Schreibschutz per Knopfdruck

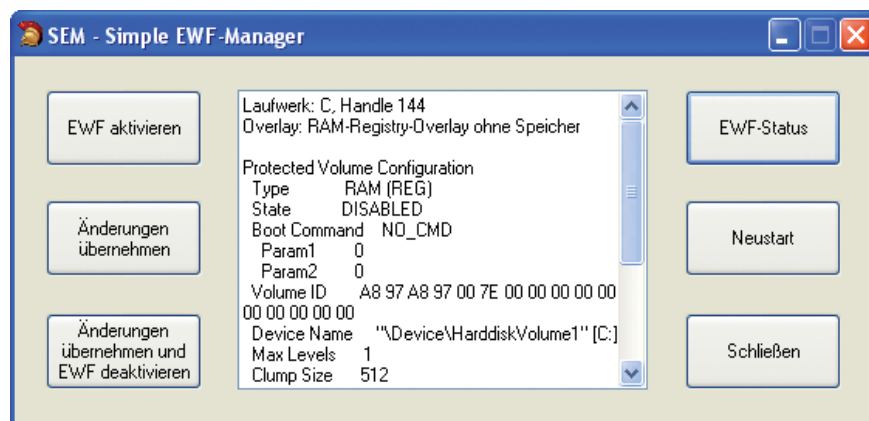
Um den Schreibschutz an- oder auszuschalten oder um Änderungen auf die Festplatte zu übernehmen, verwenden Sie entweder die Kommandozeile oder ein Programm mit grafischer Bedienoberfläche wie den Simple EWF-Manager



**Windows-Registry:** Setzen Sie die Berechtigungen für die Benutzergruppe „Jeder“ in der Spalte „Zulassen“ auf „Vollzugriff“ (Bild E)

ger 1.0.0.66 der com!-Redaktion (kostenlos, [www.com-magazin.de/ergaen](http://www.com-magazin.de/ergaen) zungen und auf ).

Der Simple EWF-Manager erfordert keine Installation und lässt sich einfach per Knopfdruck bedienen. Der Button „EWF aktivieren“ schaltet den Schreibschutz ein. „Änderungen übernehmen und EWF deaktivieren“ schaltet ihn aus und schreibt die Änderungen auf die Festplatte. In beiden Fällen ist die Einstellung erst nach einem Neustart wirksam. Dieser lässt sich auch über den Button „Neustart“ ausführen.



**EWF-Manager 1.0.0.66:** Das Tool schaltet den Schreibschutz für Windows an oder aus (Bild F)

Um bei aktivem Schreibschutz Daten auf die Festplatte zu schreiben, ohne den Schreibschutz auszuschalten, klicken Sie auf „Änderungen übernehmen“. „EWF-Status“ zeigt den aktuellen Status des Schreibschutzes (Bild F).

**Alternative:** Sie können den Schreibschutz auch über die Kommandozeile steuern. Rufen Sie dazu die Kommandozeile mit [Windows R], dem Befehl `cmd` und „OK“ auf.

Geben Sie den Befehl `ewfmgr.c:` ein, um den aktuellen Status dieser Partition zu erhalten. Ob der Schreibschutz aktiv ist, sehen Sie in der Zeile, die mit „State“ beginnt. „ENABLED“ bedeutet aktiv, „DISABLED“ bedeutet inaktiv (Bild G).

Um den Schreibschutz einzuschalten, verwenden Sie `ewfmgr.c: -enable`, und um ihn wieder auszuschalten `ewfmgr.c: -disable`. Die Änderung ist jeweils erst nach einem Neustart wirksam.

Der Befehl `ewfmgr.c: -commit` schreibt die Änderungen der aktuellen Sitzung vom Arbeitsspeicher auf die Festplatte, und `ewfmgr.c: -commit anddisable -live` übernimmt die Änderungen sofort und deaktiviert den Treiber. Das dauert etwas. In diesem Fall ist ein Neustart nicht notwendig.

**Lesen Sie weiter auf Seite 31** ▶

## Alternative

Neben EWF gibt es noch eine andere Technik namens FBWF, die Windows oder Teile davon mit einem Schreibschutz versieht. Diese ermöglicht es, einzelne Verzeichnisse vom Schreibschutz auszunehmen.

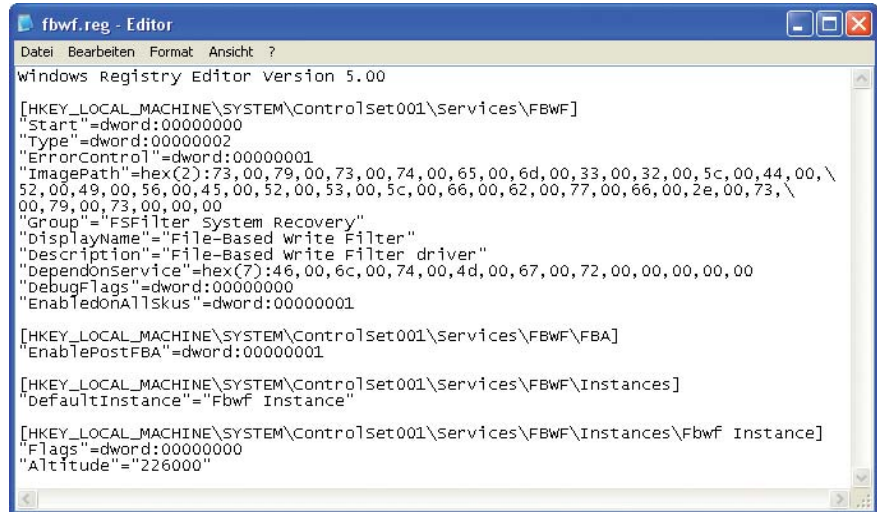
### Schreibschutz mit FBWF

FBWF steht für File Based Write Filter, also dateibasierter Schreibschutz, und ist eine Variante von EWF. FBWF benötigt weniger RAM und ermöglicht es zudem, einzelne Verzeichnisse so einzurichten, dass sie vom Schreibschutz ausgenommen sind.


Wie EWF ist auch FBWF Teil von Windows XP Embedded, genauer gesagt von einem Zusatzpaket für das Betriebssystem.


Um FBWF zu installieren, benötigen Sie einige kleine Dateien aus dem Windows XP Embedded SP 2 Feature Pack 2007 (kostenlos, [www.microsoft.com/windowembedded/en-us/products/com/windowembedded/en-us/products/wexpe/getting-started.mspx](http://www.microsoft.com/windowembedded/en-us/products/com/windowembedded/en-us/products/wexpe/getting-started.mspx)).

Zunächst laden Sie das Feature Pack herunter, es ist rund 130 MByte groß. Anschließend entpacken Sie die ISO-Datei, zum Beispiel mit 7-Zip 4.65. Sie erhalten unter anderem die Datei „XPEFP2007.exe“. Diese entpacken Sie ebenfalls. Kopieren Sie aus dem Unterordner „rep“ die Dateien „fbwf.sys“, „fbwfdll.dll“, „fbwflib.dll“ und „fbwfmgr.exe“. Löschen Sie schließlich die übrigen Dateien des Feature Packs wieder.



**Fbwf.reg:** Diese Registry-Einträge machen Windows XP mit dem Schreibschutz FBWF bekannt (Bild H)

Kopieren Sie nun die Datei „fbwf.sys“ in das Verzeichnis „C:\WINDOWS\system32\drivers“ und die anderen drei FBWF-Dateien in das Verzeichnis „C:\WINDOWS\system32“. Alternativ kopieren Sie die Datei „FBWF-Installer.cmd“ (kostenlos, [www.com-magazin.de/ergaenzungen](http://www.com-magazin.de/ergaenzungen) und auf ) in den Ordner mit den FBWF-Dateien und rufen diese dort auf. Sie kopiert die FBWF-Dateien automatisch an die richtige Stelle.

Auch bei FBWF müssen Sie den Treiber zunächst in der Registry bekannt machen. Dies erledigt die Datei „fbwf.reg“ (kostenlos, [www.com-magazin.de/ergaenzungen](http://www.com-magazin.de/ergaenzungen) und auf ) . Kopieren Sie sie auf die Festplatte und rufen Sie die Datei auf. Starten Sie den PC neu. Beachten Sie: EWF und FBWF sollten nie gleichzeitig aktiv sein.

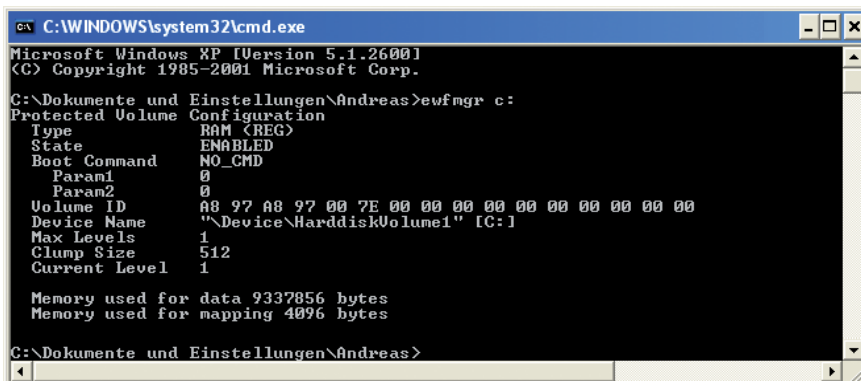
Die Bedienung von FBWF über die Kommandozeile ist etwas komplizierter als bei EWF: Zum Einschalten des Schreibschutzes verwenden Sie den Befehl `fbwfmgr /enable`. Anschließend legt `fbwfmgr /addvolume c:` das Laufwerk fest, das Sie schützen wollen. Schließlich bestimmen Sie über `fbwfmgr /setthreshold 256` die Größe des Puffers.

Wenn Sie einzelne Verzeichnisse vom Schreibschutz ausnehmen wollen, dann definieren Sie diese in der Art `fbwfmgr /addexclusion c:*\Pfad` zum Ordner.

Nach einem Neustart ist der Schutz aktiv. Beachten Sie: Bei aktivem FBWF lassen sich auch keine neuen Ordner anlegen, das ist Teil des Schutzes. Um den Schreibschutz später wieder auszuschaalten, verwenden Sie den Befehl `fbwfmgr /disable`.

Falls sich FBWF einmal aufhängen sollte, dann starten Sie Ihren PC von einer Live-CD und löschen die Datei „fbwf.sys“.

Andreas Dumont  
computer@com-magazin.de



**Ewfmgr:** Das Programm zeigt den aktuellen Schreibschutz-Status an (Bild G)

### Weitere Infos

- <http://msdn.microsoft.com/en-us/library/ms912906.aspx>  
Englischsprachiger Hintergrundartikel zu EWF