Whitepaper

DriveLock Disk Protection (FDE)

Troubleshooting

DriveLock SE 2017

DON'T GAMBLE WITH YOUR DATA

Inhalt

1 Einleitung

Im heutigen Computerzeitalter sind Festplatten ein Massenspeicher für vertrauliche Informationen geworden. Das weit verbreitete Windows Betriebssystem stellt keinen ausreichenden Datenschutz zur Verfügung, entweder auf einen Einzelplatz PC oder einem Netzwerk Computer (in den meisten Umgebungen). Wie auch immer, die Datensicherheit kann nicht gewährleistet werden, z.B. im Fall von System- (oder Festplatten-) Verlust. Wenn keine Maßnahmen zur Sicherung der betreffenden Daten getroffen wurden, kann jede Festplatte von einem System entfernt und die Daten darauf gelesen werden.

Um diese Sicherheitslücken zu schließen, ist eine Sicherheits- und Datenverschlüsselungs-Lösung für Festplatten in DriveLock integriert.

DriveLock Disk Protection (FDE) stellt die folgenden Funktionen zur Verfügung.

1.1 DriveLock Disk Protection (FDE) Funktionen

DriveLock Disk Protection stellt die folgenden Funktionen zur Verfügung:

- Festplattenverschlüsselung

  DriveLock FDE bietet eine sichere Datenverschlüsselung, die für den Benutzer vollkommen transparent ist.

- Pre-Boot Benutzer Authentifizierung (PBA)

  Diese dient der Anmeldung des Benutzers bevor das Betriebssystem gestartet wird, um die Entschlüsselungs-Schlüssel zu erlangen, damit die Betriebssystemdateien und der Rest der verschlüsselten Festplatte(n) entschlüsselt werden kann.

- Single Sign-On oder manuelle Windows Authentifizierung

  DriveLock FDE stellt eine automatische Windows (Domänen) Benutzer Anmeldung (SSO) zur Verfügung, die auf eine erfolgreichen Pre-Boot Authentifizierung folgt. Als Alternative ist auch eine manuelle Authentifizierung möglich.

- Notfall Wiederherstellung von Pre-Boot Benutzern und Token Anmeldungen

  DriveLock FDE stellt Notfall Anmeldeverfahren zur Verfügung, damit sich Smartcard/Token oder Windows Domänen Benutzer einmalig an der Pre-Boot Anmeldung authentifizieren können, wenn z.B. das Passwort oder die PIN vergessen wurde.

- Notfall Wiederherstellungstools

  DriveLock FDE stellt Tools zur Verfügung, um im Falle einer defekten Festplatte Daten auf dieser Festplatte wieder zu entschlüsseln.

1.2 Notwendige Schritte vor der Installation

Überprüfen Sie die folgenden Punkte und stellen Sie sicher, dass Sie die notwendigen Schritte vor der Installation von DriveLock FDE ausgeführt haben.

- Defragmentieren Sie alle Laufwerke, die von DriveLock FDE verschlüsselt werden sollen.
- Stellen Sie sicher, dass das Speichersystem gut geplant ist und keine weiteren Änderungen irgendwelcher Partitionen nötig wird. Falls nötig, nutzen Sie die Windows Datenträgerverwaltung, um Laufwerks- Spiegelungen, Partitionsgrößen etc. einzurichten.
- Verwenden Sie CHKDSK /f und die Festplatten-Hersteller-Diagnosetools, um die Integrität des Dateisystems aller Laufwerke sicherzustellen, die Sie zu verschlüsseln beabsichtigen. Reparieren Sie alle fehlerhafter Sektoren, falls welche existieren, da DriveLock FDE diese sonst nicht verschlüsseln kann. Bitte stellen Sie sicher, dass es keine unformatierten Partitionen mit zugeordneten Laufwerksbuchstaben gibt.
- Sichern Sie alle wichtigen Daten vor der Laufwerks-Verschlüsselung.
- Bitte beachten Sie, dass Windows 7 mit UEFI, sowie NVME unter BIOS nicht unterstützt wird.
- Windows 10 Upgrades - DriveLock 7.6.14 ist für Upgrades von Windows 10 auf Windows 10 Version 1607 (Anniversary Update) oder neuer (Creators Update) auf verschlüsselten Systemplatten vorbereitet. Dazu muss ein angepasstes Windows 10 Setup erstellt werden, das den DriveLock Verschlüsselungstreiber enthält. Ein Programm zum Erstellen des angepassten Windows 10 Setups kann über den DriveLock Support bezogen werden.

Hinweis: DriveLock 7.6.14 und älter:

Die DriveLock Disk Encryption für UEFI basierte Systeme funktioniert noch nicht mit Windows 10 Version 1703.

DriveLock 7.6.14: Die DriveLock Disk Encryption für BIOS basierte Systeme und alle anderen DriveLock Module sind mit Windows 10 Version 1703 kompatibel.

1.3 Dauer der Festplattenverschlüsselung

Die Verschlüsselung einer Festplatte hängt stark von der eingesetzten Hardware ab. Neue Geräte verschlüsseln die Festplatte meist schneller.

Beispielsweise dauert die Verschlüsselung bei einem neuen Laptop mit einer 500GB großen Festplatte ca. 3 Stunden, für eine 250GB Festplatte dauert es ca. 1,5 Stunden.

1.4 Einstellungen für die Anti-Virus Software

Damit es nach der Verschlüsselung von Rechnern keine Probleme gibt, ist es unbedingt notwendig, dass man dafür sorgt, dass z.B. Anti-Virus Programme die FDE nicht beeinflussen.

Dafür sollte man den Ordner C:\securdsk, in welchem unter anderem das verschlüsselte Dateisystem der PBA gespeichert ist, in allen Hintergrundprozessen mit Festplattenaktivität ausnehmen, so dass der Ordner nicht verändert wird.

Unter diese Hintergrundprozesse fallen z.B.: Anti-Virus Programme und Defragmentierungsprogramme.

1.5 Festplattenverschlüsselung bleibt stehen

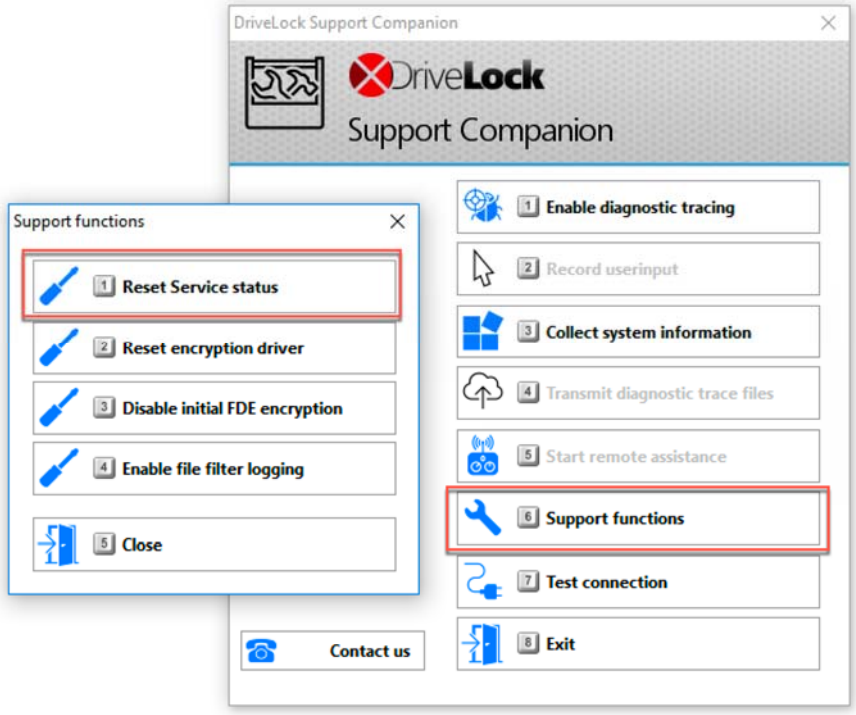
Bleibt der Verschlüsselungsvorgang während der Verschlüsselung stehen, so liegt dies meist an defekten Sektoren auf der Festplatte bzw. an Applikationen, die bestimmte Sektoren auf der Festplatte auf tieferer Systemebene sperren.

Folgende Schritte sind dann auszuführen:

1. Anti-Virus Programm abschalten
2. DriveLock Dienste stoppen
3. Rechner neu starten (ohne die Dienste vorher zu starten)

Sollte die Verschlüsselung danach nicht weiterlaufen, versuchen Sie den Status der FDE mithilfe des DriveLock Support-Tools zurücksetzen.

Dazu starten Sie das DriveLock Supporttool unter „C:\Program Files\CenterTools\DriveLock\DLSupportAgent.exe“ starten und den Punkt „Support functions“ auswählen. Es öffnet sich ein neues Fenster in dem Punkt 1 "Reset Service Status" auszuwählen ist.



Sollte dies jedoch auch nicht zum gewünschten Ziel führen muss der Rechner entschlüsselt werden, um wieder auf den Ausgangszustand zurück zu kommen. Dafür reicht es, dem Computer in der Richtlinie die Lizenz für die FDE zu entziehen und die Richtlinie auf dem Client zu aktualisieren. Dann beginnt der Rechner mit der Entschlüsselung.

Nachdem die Entschlüsselung vollständig durchlaufen wurde:

1. ist die Festplatte zunächst auf fehlerhafte Sektoren zu überprüfen. Dafür führt man den Befehl chkdsk /F /X /R in einer Kommandozeile mit Administratorrechten aus. Dadurch werden fehlerhafte Sektoren auf der Festplatte gefunden, markiert, und repariert.

2. Jetzt kann erneut versucht werden, die Festplatte zu verschlüsseln.

Sollte es immer noch nicht funktionieren, ist es notwendig das Betriebssystem neu installieren und erneut zu versuchen. Als letzter Schritt ist die Festplatte austauschen.

1.6 Pre-Boot Environment (PBA)

1.6.1 BIOS / UEFI Unterstützung

UEFI wird ab der Version 2.3.1 und ab der DriveLock Version 7.6.4 unterstützt.

Ab der DriveLock Version 7.6.6 wird UEFI auch in Verbindung mit Secure Boot unterstützt.

Bitte beachten Sie, dass die Festplattenverschlüsselung in Verbindung mit UEFI und Windows 7 nicht unterstütz wird. Dies ist erst ab Windows 8 möglich.

1.6.2 Übersicht der DriveLock Pre-Boot Authentifizierungsmethoden

Die DriveLock Pre-Boot Authentifizierung (PBA) ist fester Bestandteil der DriveLock Festplattenverschlüsselung und zwingend notwendig.
Sie ersetzt den MBR (bei BIOS) oder ist Bestandteil des UEFI Bootsystems. Hier gibt es Konfliktpotential mit anderen 3rd Party Tools, die ebenfalls den MBR ersetzen. Die PBA startet vor dem Betriebssystem. Sie authentifiziert alle Benutzer anhand einer eigenen, immer lokal vorliegenden Datenbank. Sie entschlüsselt den Disk Schlüssel. Nach der Authentifizierung des Nutzers werden die Windows Boot Dateien geladen.
Mit aktivem Single-Sign-On erfolgt die automatische Anmeldung am Windows Betriebssystem mit den in der PBA angegebenen Anmeldedaten.
Die PBA User Datenbank wird bei jedem Anmeldevorgang und bei Kennwortänderung aktualisiert. Ein Abgleich mit AD-Usern ist möglich.

BIOS:

Standardmäßig ist die 32-bit Version aktiv. Sie bietet Unterstützung für die Anmeldung mit Smartcards bzw. Token, hat einen hochauflösenden Hintergrund und kann sowohl vordefinierte als auch unternehmenseigene Bilder darstellen.

Durch inkompatible Hardware kann es zu Problemen mit der 32-bit Version kommen. Deshalb steht auch eine 16-bit Version zur Verfügung. Diese kann temporär beim Booten eingeschaltet (Shift-Taste drücken) oder fest für alle oder einzelne Clients zentral vorgegeben werden. Die 16-bit PBA startet schneller und funktioniert auch bei außergewöhnlicher Hardware. Die Verwendung von einigen Tokens oder Smartcards ist nicht möglich. Die Hintergrundbildänderung ist kostenpflichtig.

UEFI:

Seit der DL-Version 7.6.4 ist eine PBA auch für dieses Bootsystem verfügbar. Im Vergleich zur BIOS-Version der PBA gibt es einige Funktionen, die noch nicht unterstützt werden. An einer Angleichung des Funktionsumfangs wird gearbeitet.

Beschreibung		Bis Version 7.5.x		Version 7.6.x und höher zusätzlich
		16bit	32bit	UEFI
Installationszeitpunkt	Erstinstallation	Ja	Ja	Ja
	Versionsupdate	Ja	Ja	Ja
Hintergrundbild	Auflösung	640x480	1024x768	nativ
	Bildformat	.gif	.png	.png
	Farbtiefe	4 bit	32 bit	32 bit
	Austauschbar	Nein	Ja	Ja
Geräte	Tastatur	Ja	Ja	Ja
	Tastaturlayout	analog WindowsOS setup	konfigurierbar	konfigurierbar
	Maus	Nein	Ja	Nein
	Token/Smartcard	Nein	Ja	Ja (1)
	Fingerprint Reader	Nein	Nein	Nein
Software Interface	BIOS	Ja	Ja	Nein

	UEFI	Nein	Nein	Ja
Anmeldungsarten	Notfall – Anmeldung mit Benutzer	Ja	Ja	Ja
	Notfall – Anmeldung ohne Benutzer	Ja	Ja	Ja
	Verwendbarer Zeichensatz	UTF-8 / **Unicode**	UTF-8 / Unicode	UTF-8 / Unicode
Sprache	Multi-Language Support	Nein	Ja	Nein
Generelle Informationen	Vorteile	Performanter Bootvorgang (ca. 2 Sekunden – 30 Sekunden bei 32bit)	Hintergrundbild anpassbar Maus Funktionalität Tokens / SmartCard Unterstützung	Hintergrundbild anpassbar Performanter Bootvorgang (ca. 2 Sekunden)
	Nachteile	Hintergrundbild ändern ist kostenpflichtig Aufwand: 1 Tag Consulting	Langsamer, geringere Kompatibilität	Keine Maus Eingeschränkte Tokens / SmartCard Unterstützung

(1) Smartcard / Token-Support ab DriveLock 7.7 für folgende Token:

- DPrime MD 830 / 831 / 3810
- Gemalto (Aladdin) eToken 72K (Java)
- Gemalto (Aladdin) eToken NG-OTP 72K (Java)
- Gemalto (Aladdin) eToken NG-OTP (CardOS)
- Gemalto (Aladdin) eToken 32K (CardOS)
- Gemalto (SafeNet) 5110

1.6.3 Speicherbedarf der PBA (BIOS-basierte Systeme)

Damit die DriveLock 32bit PBA korrekt geladen werden kann, oder nach der Authentifizierung Windows startet, werden mindestens 604KB konventioneller Speicher von DriveLock benötigt.

Sollte die 32bit PBA oder Windows nicht starten kann als Workaround die 16bit PBA genutzt werden.

Alternativ können auch unnötige Funktionen des BIOS deaktiviert werden um mehr Speicher frei zu geben, dies ist aber nicht immer erfolgreich.

Ein Beispiel hierzu ist das PXE o.ä. - Ein BIOS das durch UEFI simuliert wird, belegt schon sehr viel Speicher. Das Verhalten hängt immer von den zusätzlich geladenen Funktionen des BIOS ab.

1.6.4 16bit PBA aktivieren

In seltenen Fällen kann es nach der Aktivierung der Pre-Boot-Authentifizierung (PBA) vorkommen, dass der PC beim Booten nicht mehr reagiert.

Der Grund hierfür ist in der Regel, dass die verwendete Hardware entweder von der 32bit PBA nicht unterstützt wird oder Windows-Treiber für diese Hardware nicht mit der PBA kompatibel sind. In diesen Fällen kann die 16bit PBA verwendet werden.

Hierzu gibt es drei Möglichkeiten:

1. Der Benutzer hält beim Starten des Rechners die **"Shift"-Taste** gedrückt. Dies aktiviert **einmalig** die 16bit PBA.

2. An dem Client, an dem die 16bit PBA aktiviert werden soll, wird in einer Kommandozeile der Befehl "**setpb /16**" eingegeben. Die 16bit PBA ist dann für einen **Reboot lang** aktiv.

3. Über die **Management Konsole** unter dem Punkt "Betrieb > Agenten-Fernkontrolle" kann die 16bit PBA **dauerhaft** aktiviert werden. Hierzu verbindet man sich mit dem entsprechenden Rechner.

4. Im Kontextmenü (Rechtsklick auf den Rechnernamen) über den Punkt "FDE-Eigenschaften" > "Agent umkonfigurieren" öffnet man ein weiteres Fenster zur Konfiguration der PBA und setzt den Haken "Richtlinie überschreiben". Nun kann man den Punkt "32bit Pre-Boot-Authentifizierung abschalten" setzen. Dadurch wird die 16bit PBA dauerhaft auf diesem Client aktiviert.

1.7 Disk Protection Recovery Video

https://dlweb.blob.core.windows.net/videos/Module%2015%20Disk%20Protection%20Recovery.mp4

1.8 Disaster Recovery Tools

1.8.1 DLFDEBACKUP.EXE - Creating Recovery Files

In preparation for disaster recovery, the command prompt utility, **dlfdeackup.exe**, must be used following each disk encryption status change. A folder, labeled with the computer name, will be created with the EFS recovery files inside, which are necessary for disk recovery. Note that you can also run this utility as a scheduled administrative task.

Usage: **DLFDEBACKUP.EXE [options]**

Options	Description	Default
/? | -usage	Displays usage help	
/v | -ver	Displays utility version	
/t | -tgt	Specifies target directory for backed up **Recovery Files**	Current directory. Note that it may be good practice to store the Recovery Files off the client system. This will ensure their availability in the rare case when the client system is rendered inoperable.

/n | -noverchk	No DriveLock version compatibility check is performed. For example, an 8.1 version of backup.exe can be run on an 8.2 (or higher) version of DriveLock. If /n is not used, a message will display to notify the user that there is a version mismatch between the backup.exe and the DriveLock version.

If, for some reason, the DriveLock secured system becomes inaccessible (due to data corruption, for example) the System Administrator can use the following disaster recovery tools to perform system diagnosis, decrypt the hard disk(s), manipulate the MBR, and administer the Pre-boot User database.

1.8.2 DLDISPEFS.EXE - FDE Diagnostic Utility

This diagnostic tool displays contents of the DriveLock system files. DriveLock stores system data in a number of files contained in the Embedded File System (EFS).

Usage: **DLDISPEFS.EXE [options] [>output_text_file]**

Options	Description
/? | -usage	Displays usage help
/a | -all	Displays contents of all DriveLock system files
/d | -dtes	Displays drive table entries
/c | -cfg	Displays configuration data
/k | -dky	Displays key data
/x | -ex	Displays exchange data
/u | -user	Displays the Pre-boot User database.
/r | -rec	Displays data from *Recovery Files*
/rp | -recpath	Specifies the path to the *Recovery Files*
No Arguments	Displays all system files

1.8.3 DECDISK.EXE - Disk Decryption Utility

This 16-bit, MS-DOS command prompt disk decryption utility is only used to decrypt a *non-bootable Windows installation* (i.e., when access to the GUI-based decryption mechanism is not available).

After a successful decryption using **decdisk**, and a successful Windows boot occurs, the disk is re-encrypted.

Usage: **DECDISK.EXE [options]**

Options	Description	Default
/? | -usage	Displays usage information	
/v | -ver	Displays utility version information	
/d | -display	Displays encryption information only	
/a | -all	Decrypts all encrypted partitions; not recommended for third-party disk recovery, as this option may decrypt the wrong disk	User specified
/e | -est	Estimates the region intended for decryption and forces the /r option	
/r | -rec	Uses *Recovery Files* for the decryption operation	
/rp | -recpath	Specifies the path to the *Recovery File* (points to the backup file set created with backup.exe)	Current directory
/dk | -diskkeyfile	This option must always be used. It specifies the encrypted diskkey file used for disk key recovery. Can be used in conjunction with the /r option. Allows the user to read the diskkey from the encrypted *.dke file.	

Decdisk will initially display a Partition Information section for all known hard disks. The output will be similar to the example shown on the next page.

If you notice an incorrect disk number in the Encryption Information section in the decdisk output, exit decdisk and re-run it with the /e option to enter the correct information manually.

```
Partition Information

Disk    Start Sector   End Sector     Megabytes      Type...
1       63             16771859       8189           Primary (Boot)
1       16771923       78140159       29964          Logical
2       63             417689         203            Primary
2       417690         10217339       4784           Primary
2       10217403       12498569       1113           Logical

Area  Disk  Start Sector      End Sector     Algorithm      Megabytes      %     Enc'ed
        Type
1.    1     63                16771859       3DES CBC       8189           100.00
        Primary
2.    2     6771923           78140159       3DES CBC       29964          100.00
        Logical
3.    2     63                417689         3DES CBC       203            100.00
        Primary
4.    2     417690            10217339       3DES CBC       4784           100.00
        Primary
5     2     10217403          12498569       3DES CBC       1113           100.00
        Logical

Select encrypted area to decrypt. (Ctrl-C to exit) _
```

In the above example, decdisk displays information regarding all known hard disk partitions. Disk is the physical disk number. Start Sector and End Sector are relative to the start of the physical disk. Decdisk also displays information regarding the encryption status of the above partitions. The Start Sector and End Sector columns show the extent of the encryption. The value in the Area section is used to select which area to decrypt.

The information above portrays two physical disks. The first disk has primary and extended partitions containing one logical drive. The second disk contains two primary partitions and an extended partition containing one logical drive. All partitions on these disks are fully encrypted with triple DES.

The user is required to select one of the encrypted areas to decrypt. As the decryption progresses, the user is informed of the percentage of the encrypted area still to be decrypted, and approximately how long the decryption will take as follows:

75.10% 3hrs:15mins remaining (Press Ctrl-C to stop)

Once the decryption is complete, the list of encrypted areas will be refreshed. When there are no more encrypted areas the following will message will display: No encrypted areas found.

1.8.4 Using Recovery Files

If serious system corruption occurs, the DriveLock system files may not be accessible. In this case, **decdisk.exe** requires the backed-up **Recovery Files**. These files are produced using **backup.exe** during normal DriveLock operation or obtained from Active Directory at the same time as disk key creation.

The following command line syntax example allows the user to select partitions for decryption:

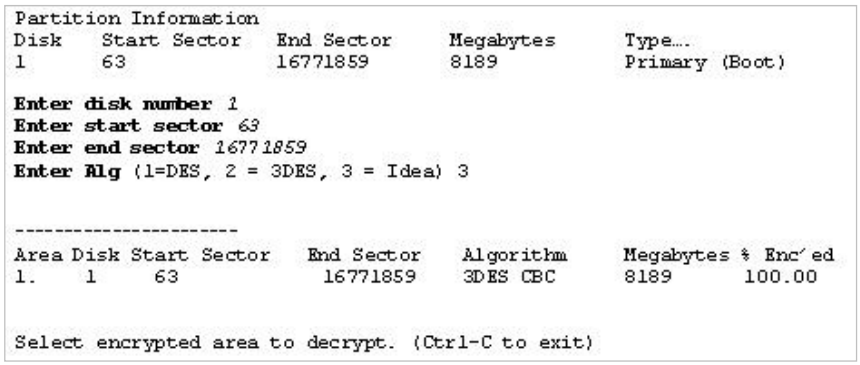
decdisk –dk l:\pd\diskkeys\computer.dke –r –rp l:\pd\backups\computer

where **l:\pd\diskkeys** is the path and **computer.dke** is the disk key file, and **l:\pd\backups\computer** is the path to the backup file set (i.e., the recovery file set).

After **decdisk** is run with the use of recovery files, it is necessary to run the **fdisk /mbr** command.

1.8.5 Manually Specifying the Decryption Area

Decdisk decrypts disk areas selectable by sector number (using the **/e | -est** option). The user manually provides the **Start** and **End Sectors** and the **Algorithm** as follows:



1.8.6 RMBR.EXE – MBR Recovery Utility

The DriveLock Boot Manager/Master Boot Loader is the very first utility that runs after the system BIOS is loaded. DriveLock modifies part of the MBR during installation. This is done to enable DriveLock to locate its embedded file system upon system boot and prior to all other disk access. If the MBR is altered, replaced, or corrupted after the DriveLock install, the **rmbr.exe** utility is used to recover it.

Restoring the DriveLock MBR requires a sector-by-sector search of the embedded file system located on the boot partition. Once the embedded file system is located, the DriveLock MBR can be restored. Reverting to the original system MBR in existence prior to the DriveLock install is done using the **fdisk /mbr** command.

Usage: **RMBR.EXE [options]**

Options	Description
/? | -usage	Displays usage help.
/v | -ver	Displays utility version.
/p | -pd	Recover the DriveLock MBR.
/o | -original	Recover the original system MBR. This is same as fdisk /mbr.
/r | -recovery	Use the DriveLock Recovery Files to perform any of the above operations.
/rp | -recpath	Specifies the path to the *Recovery File* (points to the backup file set created with backup.exe or obtained from Active Directory).

Note: If the backup file set was provided during disk decryption (using **decdisk**) by invoking the "/r [/rp ..]" argument, then the same argument ("/r [/rp ..]") should be invoked with **rmbr** when restoring MBR.

1.8.7 RMBR Initial Status Check

Prior to performing any MBR recovery, **rmbr** will display the current MBR status. If the DriveLock MBR has been unaltered since the install, the following message displays:

Current MBR is the DriveLock MBR

However, if **rmbr** detects any alteration to the DriveLock MBR, the following message displays:

Current MBR is not the DriveLock MBR

1.8.8 RMBR Version Compatibility Check

Rmbr will attempt to verify that it is working with the correct version of the DriveLock system.

If the version is incorrect, the following message displays:

Incompatible versions

DriveLock Version: 8.1 (example)

RMBR.EXE Version: X.X.X (example)

Note: Depending on the level of system data corruption, it is not always possible to determine the version of the currently installed DriveLock system.

1.8.9 Restoring the DriveLock MBR (RMBR /p)

RMBR will initially display the list of all DriveLock partitions. Select the partition you wish to recover the DriveLock MBR for.

```
Disk    Start Sector   End Sector     Megabytes      Type….
1       63             16771859       8189           Primary (Boot)
(ProtectDrive)

Select partition to recovery. (Ctrl-C to exit) _
Current MBR is not the ProtectDrive MBR
Searching for super block from sector 63 to sector 20487599
99.99% and 3hrs 20mins remaining. (Press Ctrl C to stop)
```

Rmbr.exe will search the disk sector by sector looking for the DriveLock super-block corresponding to the start of the DriveLock embedded file system. It is possible that remnants of previously installed DriveLock systems may exist on the disk. If a super-block is found, but it does not correspond to the current DriveLock installation, the following message displays:

Found super block at sector 1893443

Incorrect super block. Continuing search ..

If a valid super block is located, RMBR will display the version and ask the user for verification, as shown below.

Found super block at sector 1893443

DriveLock v8.1

Is this the correct version of DriveLock? [Y/N]

If the version is not correct, enter N and rmbr will continue. If the version is correct, enter Y and the following displays:

DriveLock MBR restored.

Current MBR is the DriveLock MBR.

1.8.10 Restoring the Original MBR (RMBR /o)

This option replaces the current MBR with the original system MBR that DriveLock saved during installation. This is only supported if there are no currently encrypted drives present on the system. Otherwise, decrypt before proceeding.

1.8.11 DLFDEUSERDB.EXE – Pre-boot User Database Administration Utility

This command line MS_DOS tool manipulates the DriveLock pre-boot user database, allowing the DriveLock Administrator to:

- List the names of users authorized to perform DriveLock pre-boot authentication.
- Remove Local and Domain (including Token/PIN user account) user accounts from the DriveLock pre-boot user database.
- Add Local and Domain user accounts (including Token/PIN user accounts) to the DriveLock user database.

Usage: DLFDEUSERDB.EXE [options]

Options	Description
/? | -usage	Displays usage help
/a | -add	Adds a user to the pre-boot database
/d | -domain	Specifies the Windows Domain that the newly added user is a member of (defaults to the *Local System Name*)
/f | -file	Specifies the filename of a file containing a user certificate
/l | -list	Displays a list of all existing pre-boot users
/n | -name	Specifies a username to add to the pre-boot database
/p | -password	Specifies the password of the newly added user
/r | -remove	Removes a user from pre-boot database
/v | -version	Displays version information

Note: To change a password, remove the user account (/r) first, and then add a new account (/a) with the new password.

2 Troubleshooting DriveLock FDE

2.1 System Debug and ACS Error Messages

Before proceeding, familiarize yourself with DriveLock Disk Protection Recovery.

2.1.1 System Debug

Password type account user cannot be authenticated by the PBA.	Run *dldispefs.exe /u*. This will display a list of all users and their account types. Password type account users are clearly indicated. If the user is shown to have a Password account type, then it is possible they are entering an invalid password. Passwords are case sensitive. Finally, if the user is positive they are entering the correct password, and no other user is able to log on, then the DriveLock files have become corrupt. See below for *FDE appears to be corrupt.*
Smart Card/Token type account user cannot be authenticated by the PBA.	Run *dldispefs.exe /u*. to list of all existing users and their account types. Smart Card/Token type account users are clearly designated. Although a user may have one or more token accounts, it is possible that the Certificate contained by the token does not match the Certificate originally used for this user's record creation in the DriveLock Pre-boot User database. Note that users may have multiple records in the pre-boot user database. The **Hash** field displayed by *Dispefs.exe* /u is the same as the **Thumbprint** field displayed when certificate details are viewed in Windows. Finally, if the user is positive they are using a valid token, and no other user is able to log on, then the DriveLock files have become corrupt. See below for *DriveLock appears to be corrupt*.
User successfully authenticates at Pre-boot but Windows does not boot.	It's possible that one of the Windows system files is corrupt. If Drive **C** is not encrypted, proceed with normal Windows recovery. If Drive **C** is encrypted, run **decdisk.exe** to decrypt the system drive and enable Windows Recovery tools access the system drive.
Pre-boot Authentication Program does not run.	If **fdisk /mbr** or another utility has replaced the DriveLock MBR, the Pre-boot Authentication program will not be run. If the system drive is encrypted the operating system will also fail to load. If the system drive is not encrypted, but other drives are, the operating system will load but access to the encrypted drives will be prevented by the DriveLock driver. To recover from this situation run **rmbr /p**.

DriveLock appears to be corrupt.

If DriveLock is corrupt; then one of the following is possible:

- Pre-boot Authentication Program will not run or behaves strangely
- Valid users can not be authenticated at pre-boot
- Operating system fails to load

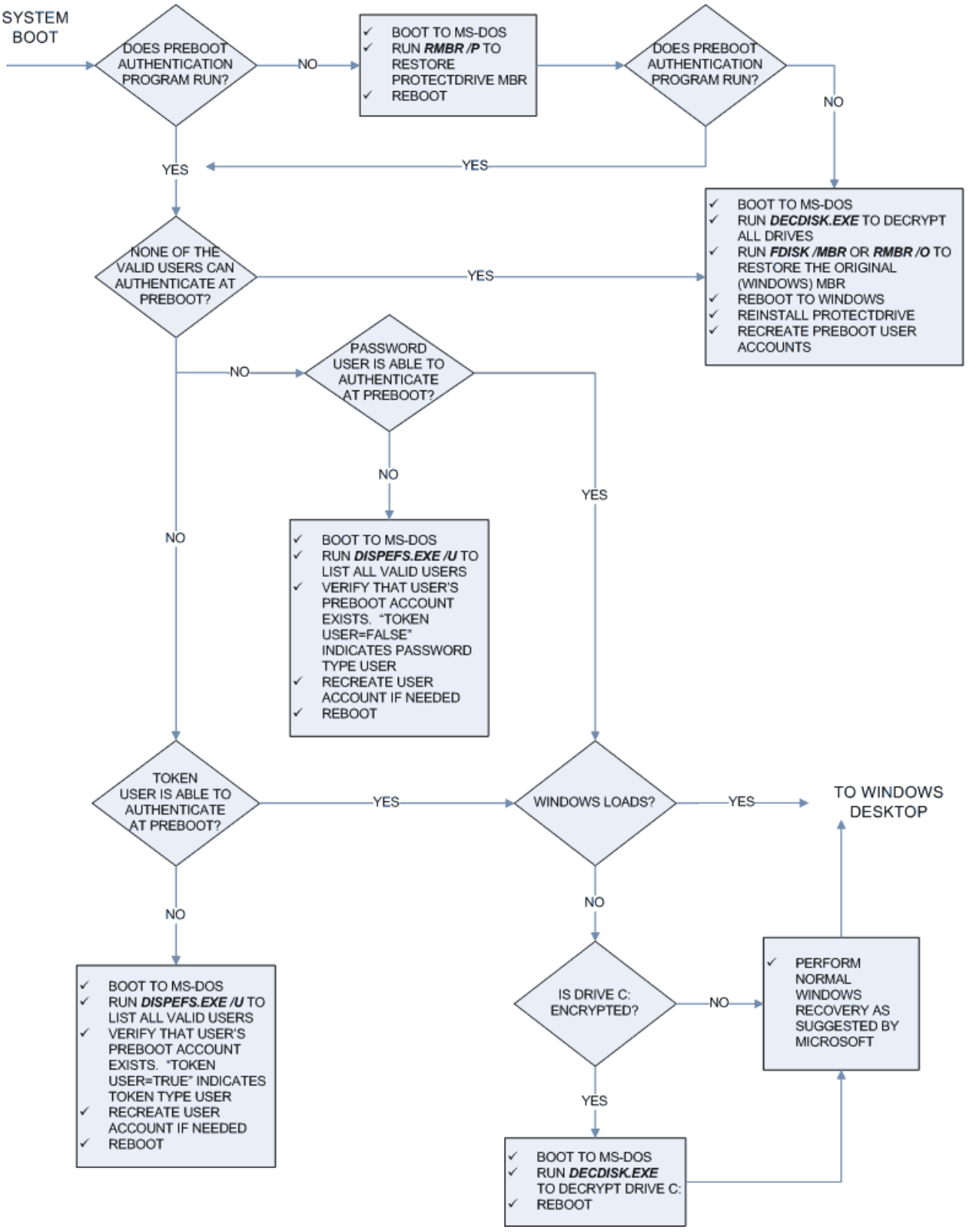
If none of the above sections apply or you failed to restore DriveLock to normal working order; then all the encrypted drives will need to be decrypted using **decdisk.exe**.

If **decdisk.exe** is unable to access the DriveLock Embedded File System (EFS); then use the Recovery Files originally created by **dlfdebackup.exe**.

Once all the drives have been decrypted, run **fdisk /mbr** or **rmbr /o** to restore the DriveLock MBR.

It is possible to boot the operating system once the system drive has been decrypted. It is not possible to uninstall DriveLock until all drives are decrypted.

The following flowchart represents the system debug information listed above. It is included for additional information.



2.1.2 ACS Error Messages (BIOS-based systems)

The DriveLock Disk Protection Access Control System (ACS) becomes active when a computer with DriveLock installed boots up. If an error occurs during its initialization, the system will display an error message composed of an error number and a brief description.

Error numbers are composed of three components:

CTXX where:

C is the module the error occurred in

T identifies the type of error and

XX is the actual error number

Module identifiers are:

0 Master Boot Loader (MBL)

1 VXBIOS

2 Not used

3 VROM

Type identifiers are:

0 Not used

1 Warning

2 Error

3 Fatal

The table on the next page lists all ACS errors, possible causes, and recommended recovery actions.

ACS Error	Component	Description	Possible Cause	Recovery Action
0301	MBL	Invalid master boot code checksum	MBR corruption MBR Trojan attack	Run rmbr.exe to recover the DriveLock MBR.
0305	MBL	Invalid VXBIOS -OR- Cannot boot from encrypted Removable Media (USB)	Signature, checksum or size verification of the VXBIOS failed possibly caused by disk corruption -OR- Removable Media does not have an OS	Contact DriveLock Support. -OR- Unplug Removable Media and reboot again. -OR- Modify the Boot Order in the BIOS configuration, and move the USB further down the device list.
0306	MBL	Invalid master boot record signature	MBR corruption MBR Trojan attack	Run rmbr.exe to recover the DriveLock MBR.
0307	MBL	No DriveLock partition info	Partition table corruption or change. Addition of fixed disk after DriveLock installation	Run rmbr.exe to recover the DriveLock MBR.

ACS Error	Component	Description	Possible Cause	Recovery Action
0313	MBL	Disk i/o error reading sector stack	Disk IO error (Hard disk failure) or partition table corruption	Run rmbr.exe to recover the DriveLock MBR.
0314	MBL	Disk i/o error reading VXBIOS	Disk IO error (Hard disk failure) or partition table corruption	Run rmbr.exe to recover the DriveLock MBR.
1100	VXBIOS	System Not Initialized	System could not load the disk encryption key or the DTE EFS is missing or corrupted.	Standard Recovery Procedure
1204	VXBIOS	VROM load Error	VROM file is missing, has an incorrect size, or a read error occurred	Standard Recovery Procedure
1205	VXBIOS	VROM Status Error	VROM signature verification failed or the program loader reported an error.	Standard Recovery Procedure
1300	VXBIOS	Insufficient memory	Failed to allocate memory for the VROM Insufficient memory available	Try to free up resources.
1301	VXBIOS	GDA file load error	GDA file is missing or a read error occurred when tying to initialize encryption information	Standard Recovery Procedure

ACS Error	Component	Description	Possible Cause	Recovery Action
1310	VXBIOS	Cannot Init EFS	EFS corruption	Standard Recovery Procedure
1311	VXBIOS	VROM load Error	VROM file is missing, has an incorrect size or a read error occurred (Displayed after a ACS1204 error)	- - -
1312	VXBIOS	VXVECT save fail	Failed to store original disk interrupt service routine (ISR) address in the EFS super block EFS corruption	Standard Recovery Procedure
1313	VXBIOS	SBLK get fail	Failed to locate the EFS Super Block	Run rmbr.exe to attempt to restore the DriveLock MBR.
1314	VXBIOS	Info open fail	Missing VDX EFS file EFS corruption	Standard Recovery Procedure
1315	VXBIOS	Info write fail	EFS corruption	Standard Recovery Procedure
1316	VXBIOS	VROM EXEC fail	Failed to execute the VROM (Displayed after a ACS1205 error)	- - -
1317	VXBIOS	Info read fail	EFS corruption	Standard Recovery Procedure

ACS Error	Component	Description	Possible Cause	Recovery Action
1318	VXBIOS	Diskette boot fail	Master Boot Loader signature verification failed; Missing operating system on floppy disk	Use bootable floppy diskette; Eject floppy diskette from drive and boot from hard disk
1319	VXBIOS	GDA open fail	GDA file is missing when trying to load (and execute) the original MBL.	Standard Recovery Procedure
1320	VXBIOS	GDA read fail	A read error occurred on the GDA file when trying to load (and execute) the original MBL.	Standard Recovery Procedure
1321	VXBIOS	Boot fail	Master Boot Loader signature verification failed.	Standard Recovery Procedure
3301	VROM	Too many logon attempts	Forgotten password Corrupted user database	Log on as other user; Exercise user key recovery; Run dispefs.exe.
3302	VROM	I/O error reading disk	Corrupted EFS Hard disk failure	Standard Recovery Procedure
3304	VROM	An unknown error has occurred	Internal program error	Standard Recovery Procedure

ACS Error	Component	Description	Possible Cause	Recovery Action
3305	VROM	Configuration file has been corrupted	MAC check of configuration file failed Corrupted EFS	Standard Recovery Procedure
3306	VROM	User information has been corrupted	MAC check of user database entry failed Corrupted EFS	Log on as different user at pre-boot and let failed user log on to Windows. User database entry will be regenerated. Alternatively, exercise user key recovery mechanism.
3308	VROM	DriveLock Administrator information has been corrupted	MAC check of DriveLock Administrator failed; Corrupted EFS	Log on as different user at pre-boot and let failed user log on to Windows User database entry will be regenerated. Alternatively, exercise user key recovery mechanism.

ACS Error	Component	Description	Possible Cause	Recovery Action
3309	VROM	Configuration file has been fatally corrupted	EFS corruption Hard disk failure	Standard Recovery Procedure
3310	VROM	Error occurred initializing the token	The token module could not be initialized and password logons are not allowed.	To diagnose this error further, contact DriveLock. To get access to the system, exercise the password fallback function.

2.2 Error Codes

2.2.1 EventID: 160 - DriveLock Disk Protection Installationsfehler

Nicht genügend freier Festplattenspeicher verfügbar, um die DiskProtection zu installieren.
Eventname: EVMSG_FS_NOTENOUGHDISKSPACE

2.2.2 EventID: 161 - Kontofehler

Das Benutzerkonto kann nicht angemeldet werden, um die DriveLock Disk Protection zu konfigurieren.
Eventname: EVMSG_FS_CANNOTLOGONUSER

2.2.3 EventID: 162 - DriveLock Disk Protection Paket-Download fehlgeschlagen

Das Installationspaket der DriveLock Disk Protection kann nicht von heruntergeladen werden.
Eventname: EVMSG_FS_DOWNLOADPKGERROR

2.2.4 EventID: 163 - DriveLock Disk Protection Installationsfehler

Das Installationspaket der DriveLock Disk Protection ist nicht lokal verfügbar.
Eventname: EVMSG_FS_LOCALINSTALLERROR

2.2.5 EventID: 164 - DriveLock Disk Protection Download erfolgreich

Das Installationspaket der DriveLock Disk Protection wurde erfolgreich heruntergeladen.
Eventname: EVMSG_FS_DOWNLOADSUCCESS

2.2.6 EventID: 165 - DriveLock Disk Protection Installationsfehler

Das Installationspaket der DriveLock Disk Protection kann nicht entpackt werden.
Die Datei fehlt oder ist defekt.
Eventname: EVMSG_FS_PKGEXTRACTERROR

2.2.7 EventID: 166 - DriveLock Disk Protection Installationsfehler

Die DriveLock Disk Protection-Datei ist im Richtliniendateispeicher nicht vorhanden.
Eventname: EVMSG_FS_SCRIPTMISSING

2.2.8 EventID: 167 - DriveLock Disk Protection Installationsfehler

Der Befehl "" kann nicht ausgeführt werden.
Eventname: EVMSG_FS_EXECUTEERROR

2.2.9 EventID: 168 - DriveLock Disk Protection Installation erfolgreich

DriveLock Disk Protection wurde erfolgreich installiert.
Eventname: EVMSG_FS_INSTALLSUCCESS

2.2.10 EventID: 169 - DriveLock Disk Protection Installationsfehler

Die Installation der DriveLock Disk Protection ist fehlgeschlagen
Eventname: EVMSG_FS_INSTALLFAILURE

2.2.11 EventID: 170 - DriveLock Disk Protection Installationsfehler

DriveLock Disk Protection ist auf diesem Computer konfiguriert, aber die Installation ist fehlgeschlagen.
Eventname: EVMSG_FS_INSTALLFAILEDBEFORE

2.2.12 EventID: 171 - DriveLock Disk Protection Installationsfehler

Die Status-Informationsdatei kann nicht erzeugt werden.
Eventname: EVMSG_FS_LOGZIPCREATEERROR

2.2.13 EventID: 172 - DriveLock Disk Protection Installationsfehler

Die DriveLock Disk Protection-Datei kann nicht an ihren Zielort kopiert werden.
Eventname: EVMSG_FS_SCRIPTCOPYERROR

2.2.14 EventID: 174 - DriveLock Disk Protection Installation verhindert

Die Installation der DriveLock Disk Protection soll ausgeführt werden, wird aber durch einen Administratoreingriff verhindert.
Eventname: EVMSG_FS_DELAYEDINSTALLATION

2.2.15 EventID: 175 - DriveLock Disk Protection Installationsfehler

Die Installation der DriveLock Disk Protection kann den Installationsordner nicht bereinigen.
Eventname: EVMSG_FS_CLEANUPFAILED

2.2.16 EventID: 176 - Fehler Pre-Boot Authentifizierung

Pre-Boot-Authentifizierung ist auf diesem Computer konfiguriert, aber die Initialisierung ist fehlgeschlagen.
Eventname: EVMSG_FS_PBAINITFAILEDBEFORE

2.2.17 EventID: 179 - DriveLock Disk Protection Verschlüsselung gestartet

DriveLock Disk Protection hat mit der Verschlüsselung der lokalen Festplatten begonnen.
Eventname: EVMSG_FS_ENCRYPTIONSTARTED

2.2.18 EventID: 181 - DriveLock Disk Protection Verschlüsselung erfolgreich

DriveLock Disk Protection hat die lokalen Festplatten erfolgreich verschlüsselt.
Eventname: EVMSG_FS_ENCRYPTIONSUCCEEDED

2.2.19 EventID: 183 - DriveLock Disk Protection Entschlüsselung gestartet

DriveLock Disk Protection hat mit der Entschlüsselung der lokalen Festplatten begonnen.
Eventname: EVMSG_FS_DECRYPTIONSTARTED

2.2.20 EventID: 184 - DriveLock Disk Protection Entschlüsselung erfolgreich

DriveLock Disk Protection hat die lokalen Festplatten erfolgreich entschlüsselt.
Eventname: EVMSG_FS_DECRYPTIONSUCCEEDED

2.2.21 EventID: 185 - DriveLock Disk Protection-Upload-Fehler

Die DriveLock Disk Protection-Daten konnten nicht zum {PrefixEnterpriseService} hochgeladen werden.
Eventname: EVMSG_SRVWSFDEUPLOADFAILED

2.2.22 EventID: 186 - DriveLock Disk Protection Systemfehler

Die Log-Datei konnte nicht zum Log-Archiv hinzugefügt werden.
Eventname: EVMSG_FS_EVMSG_FS_LOGZIPADDERROR

2.2.23 EventID: 187 - DriveLock Disk Protection Systemfehler

Wiederherstellungsinformationen können nicht unter abgelegt werden.
Eventname: EVMSG_FS_ERIMOVEERROR

2.2.24 EventID: 188 - DriveLock Disk Protection Deinstallation erfolgreich

DriveLock Disk Protection wurde erfolgreich deinstalliert.
Eventname: EVMSG_FS_UNINSTALLSUCCESS

2.2.25 EventID: 189 - DriveLock Disk Protection-Installation - falsche Paketversion

Installation oder Update der DriveLock Disk Protection wurde abgebrochen, weil eine falsche Version des Installationspaketes erkannt wurde.
Eventname: EVMSG_FS_INSTALLERWRONGVERSION

2.2.26 EventID: 206 - DriveLock Disk Protection Deinstallation fehlgeschlagen

Die Deinstallation der DriveLock Disk Protection ist fehlgeschlagen.
Eventname: EVMSG_FS_UNINSTALLFAILURE

2.2.27 EventID: 207 - DriveLock Disk Protection Fehler bei Konfiguration

Die Konfiguration der DriveLock Disk Protection kann nicht angewendet werden.
Eventname: EVMSG_FS_CONFIGAPPLYERROR

2.2.28 EventID: 208 - DriveLock Disk Protection Schlüsselsicherung fehlgeschlagen

Das Erstellen einer DriveLock Disk Protection-Schlüsselsicherung ist fehlgeschlagen.
Eventname: EVMSG_FS_KEYBACKUPERROR

2.2.29 EventID: 209 - DriveLock Disk Protection nicht lizenziert

DriveLock Disk Protection soll lokale Festplatten auf diesem Computer verschlüsseln, ist aber nicht lizenziert.
Eventname: EVMSG_FS_NOFDELICENSE

2.2.30 EventID: 210 - Kann PBA-Benutzer nicht lesen

DriveLock Disk Protection kann die Benutzer der Pre-Boot-Authentifizierung nicht lesen.
Eventname: EVMSG_FS_PBAUSERLISTERROR

2.2.31 EventID: 211 - Kann PBA-Benutzer nicht erstellen

DriveLock Disk Protection kann den Benutzer (Domäne) nicht zur Benutzerdatenbank der Pre-Boot-Authentifizierung hinzufügen.
Eventname: EVMSG_FS_PBAUSERADDERROR

2.2.32 EventID: 212 - Kann PBA-Benutzer nicht löschen

DriveLock Disk Protection kann den Benutzer (Domäne) nicht aus der Benutzerdatenbank der Pre-Boot-Authentifizierung löschen.
Eventname: EVMSG_FS_PBAUSERDELETEERROR

2.2.33 EventID: 213 - Kann PBA nicht deaktivieren

Die Pre-Boot-Authentifizierung kann nicht deaktiviert werden, wenn Festplatten verschlüsselt sind. Die {Product}-Konfiguration ist inkonsistent und sollte geändert werden, so dass Pre-Boot-Authentifizierung aktiviert ist, wenn Festplatten verschlüsselt sind.
Eventname: EVMSG_FS_PBADEACTIVEBUTENCRYPTED

2.2.34 EventID: 356 - DriveLock Disk Protection Installation fehlgeschlagen

Die Installation der DriveLock Disk Protection ist fehlgeschlagen.
Eventname: EVMSG_FS_MSIINSTALLFAILURE

2.2.35 EventID: 357 - DriveLock Disk Protection Deinstallation fehlgeschlagen

Die Deinstallation der DriveLock Disk Protection ist fehlgeschlagen.
Eventname: EVMSG_FS_MSIUNINSTALLFAILURE

2.2.36 EventID: 358 - Keine Installation oder Deinstallation wegen manueller Umkonfiguration

Die DriveLock Disk Protection wird nicht installiert oder deinstalliert, da sie nicht lizensiert oder manuell umkonfiguriert ist.
Eventname: EVMSG_FS_NOINSTALLORUNINSTALL

2.2.37 EventID: 359 - FDE: Manuell umkonfiguriert

Die DriveLock Disk Protection ist manuell umkonfiguriert.
Eventname: EVMSG_FS_SPECIALCONFIGACTIVE

2.2.38 EventID: 360 - DriveLock Disk Protection Integrationsmodul fehlerhaft

Das Integrationsmodul der DriveLock Disk Protection kann nicht geladen werden.
Eventname: EVMSG_FS_INTEGRATIONWRONG

2.2.39 EventID: 366 - DriveLock Disk Protection-Löschbefehl fehlgeschlagen

Ein DriveLock Disk Protection-Löschbefehlt wurde empfangen, konnte aber nicht ausgeführt werden
Eventname: EVMSG_FS_INVALIDWIPEREQUEST

2.2.40 EventID: 367 - DriveLock Disk Protection-Löschbefehl ausgeführt

Ein DriveLock Disk Protection-Löschbefehlt wurde ausgeführt. Das System wird neu gestartet.
Eventname: EVMSG_FS_FDEWIPEDSUCCESS

2.2.41 EventID: 475 - PBA aktiviert

Die Pre-Boot-Authentifizierung wurde erfolgreich aktiviert.
Eventname: EVMSG_FDE_PBAACTIVATED

2.2.42 EventID: 476 - PBA deaktiviert

Die Pre-Boot-Authentifizierung wurde erfolgreich deaktiviert.
Eventname: EVMSG_FDE_PBADEINSTALLED

2.2.43 EventID: 477 - EFS erzeugt

Das Embedded file system (EFS) wurde erfolgreich im SECURDSK-Ordner erzeugt.
Eventname: EVMSG_FDE_EFSCREATED

2.2.44 EventID: 478 - PBA Aktivierungsfehler

Die Pre-Boot-Authentifizierung konnte nicht aktiviert werden.
Eventname: EVMSG_FDE_PBAACTIVATIONFAILED

2.2.45 EventID: 479 - PBA Deaktivierungsfehler

Die Pre-Boot-Authentifizierung konnte nicht deaktiviert werden.
Eventname: EVMSG_FDE_PBADEINSTALLATIONFAILED

2.2.46 EventID: 480 - EFS-Erzeugung fehlgeschlagen

Das Embedded file system (EFS) konnte nicht erzeugt werden.
Eventname: EVMSG_FDE_EFSCREATEFAILED

2.2.47 EventID: 481 - Ausnahme aufgetreten

In einer DriveLock Disk Protection-Komponente ist eine Ausnahme aufgetreten.
Eventname: EVMSG_FDE_GENERALEXCEPTION

2.2.48 EventID: 482 - Ausnahme aufgetreten

Die Verschlüsselungskonfiguration wurde geändert.
Eventname: EVMSG_FDE_CRYPTCONFIGCHANGE

2.2.49 EventID: 483 - Ungültige XML-Konfiguration

Eine ungültige XML-Konfiguration wurde erkannt.
Eventname: EVMSG_FDE_INVALIDXMLCONFIG

2.2.50 EventID: 484 - XML-Konfiguration importiert

Eine XML-Konfiguration wurde importiert.
Eventname: EVMSG_FDE_XMLIMPORTEDDATA

2.2.51 EventID: 485 - BitLocker-verschlüsseltes Laufwerk erkannt

Das Laufwerk ist mit BitLocker Drive Encryption verschlüsselt. Es kann nicht mit DriveLock Disk Protection verschlüsselt werden.
Eventname: EVMSG_FDE_CANNOTENCRYPTBITLOCKER

2.2.52 EventID: 486 - Fehler beim Erzeugen des Schlüssels

Der zufällige Schlüssel für die Verschlüsselung des lokalen Systems konnte nicht erzeugt werden.
Eventname: EVMSG_FDE_FAILEDCREATEDISKKEY

2.2.53 EventID: 487 - Allgemeiner Fehler

Im DriveLock Disk Protection Verschlüsselungsdienst ist ein allgemeiner Fehler aufgetreten.
Eventname: EVMSG_FDE_STGENC_GENERALERROR

2.2.54 EventID: 488 - Allgemeiner Fehler

Im DriveLock Disk Protection Managementdienst ist ein allgemeiner Fehler aufgetreten.
Eventname: EVMSG_FDE_CDM_GENERALERROR

2.2.55 EventID: 495 - DiskProtection-Information

Eventname: EVMSG_FDE_GENERALINFORMATION

2.2.56 EventID: 496 - Wechseldatenträger entschlüsselt

Der Wechseldatenträger wurde erfolgreich freigegeben / entschlüsselt.
Eventname: EVMSG_FDE_UNLOCKRMBVL

2.2.57 EventID: 497 - Verschlüsselung abgeschlossen

Das Laufwerk wurde vollständig verschlüsselt.
Eventname: EVMSG_FDE_COMPLETEENCRYPTION

2.2.58 EventID: 498 - Entschlüsselung abgeschlossen

Das Laufwerk wurde vollständig entschlüsselt.
Eventname: EVMSG_FDE_COMPLETEDECRYPTION

2.2.59 EventID: 499 - Verschlüsselung gestartet

Die Verschlüsselung von Laufwerk wurde gestartet mit dem Algorithmus.
des Laufwerks sind bereits verschlüsselt.
Eventname: EVMSG_FDE_STARTENCRYPTION

2.2.60 EventID: 500 - Entschlüsselung gestartet

Die Entschlüsselung von Laufwerk wurde gestartet.
des Laufwerks sind bereits verschlüsselt.
Eventname: EVMSG_FDE_STARTDECRYPTION

2.2.61 EventID: 501 - Entschlüsselung gestartet

Ein Festplattenfehler ist bei der Ver-/Entschlüsselung von Sektor auf Laufwerk aufgetreten.
Die Festplatte ist möglicherweise defekt.
Eventname: EVMSG_FDE_CRYPTERRORSECTOR

2.2.62 EventID: 502 - Erfolgreiche Pre-Boot-Anmeldung

Erfolgreiche Pre-Boot-Anmeldung.
Eventname: EVMSG_FDE_PBA_LOGON

2.2.63 EventID: 503 - Erfolgreiche Notfall-Pre-Boot-Anmeldung

Erfolgreiche Notfall-Pre-Boot-Anmeldung.
Eventname: EVMSG_FDE_PBA_LOGONEMERGENCY

2.2.64 EventID: 504 - Fehlgeschlagene Pre-Boot-Anmeldung

Fehlgeschlagene Pre-Boot-Anmeldung.
Eventname: EVMSG_FDE_PBA_LOGONFAILED

2.2.65 EventID: 505 - Leere Pre-Boot-Benutzerdatenbank

Die Pre-Boot-Benutzerdatenbank konnte nicht gespeichert werden, da sie nach dem Speichern leer wäre.
Eventname: EVMSG_FDE_FAILED_US_NOUSER

2.2.66 EventID: 506 - DriveLock Disk Protection Verschlüsselungsdienst gestartet

Der DriveLock Disk Protection Verschlüsselungsdienst wurde gestartet.
Eventname: EVMSG_FDE_STGENC_SERVICESTARTED

2.2.67 EventID: 507 - DriveLock Disk Protection Verschlüsselungsdienst beendet

Der DriveLock Disk Protection Verschlüsselungsdienst wurde beendet.
Eventname: EVMSG_FDE_STGENC_SERVICESTOPPED

2.2.68 EventID: 508 - DriveLock Disk Protection Managementdienst gestartet

Der DriveLock Disk Protection Managementdienst wurde gestartet.
Eventname: EVMSG_FDE_CDM_SERVICESTARTED

2.2.69 EventID: 509 - DriveLock Disk Protection Managementdienst beendet

Der DriveLock Disk Protection Managementdienst wurde beendet.
Eventname: EVMSG_FDE_CDM_SERVICESTOPPED

2.2.70 EventID: 510 - DriveLock Disk Protection-Installation fehlgeschlagen

Beim Installieren von DriveLock Disk Protection ist ein Fehler aufgetreten.
Eventname: EVMSG_FS_INSTALLFAILED

2.2.71 EventID: 511 - DriveLock Disk Protection-Deinstallation fehlgeschlagen

Beim Deinstallieren von DriveLock Disk Protection ist ein Fehler aufgetreten.
Eventname: EVMSG_FS_UNINSTALLFAILED

2.2.72 EventID: 512 - DriveLock Disk Protection-Upgrade fehlgeschlagen

Beim Upgrade von DriveLock Disk Protection ist ein Fehler aufgetreten.
Eventname: EVMSG_FS_UPGRADEFAILED

2.2.73 EventID: 513 - DriveLock Disk Protection-Richtline fehlgeschlagen

Beim Anwenden der DriveLock Disk Protection-Richtlinie ist ein Fehler aufgetreten.
Eventname: EVMSG_FS_CANNOTAPPLYFDEPOLICY

2.2.74 EventID: 514 - Festplattenprüfung durchgeführt

Festplattenprüfung (ChkDsk) auf Laufwerk () erfolgreich durchgeführt.
Eventname: EVMSG_FS_CHKDSKSUCCEEDED

2.2.75 EventID: 515 - Festplattenprüfung fehlgeschlagen

Festplattenprüfung (ChkDsk) auf Laufwerk () fehlgeschlagen.
Eventname: EVMSG_FS_CHKDSKFAILED

2.2.76 EventID: 516 - DriveLock Disk Protection-Selbstzerstörung

Dieser Computer ist seit längerer Zeit offline. Die Disk Encryption-Selbstzerstörung wird in Tagen gestartet, wenn dieser Computer offline bleibt.
Eventname: EVMSG_FS_FDESELFWIPEWARNING

2.2.77 EventID: 517 - Entschlüsselung geplant

Die Unternehmensrichtlinie oder Lizensierung auf diesem Computer sind so konfiguriert, dass alle Festplatten entschlüsselt werden sollen. Die Entschlüsselung wird beginnen am...
Eventname: EVMSG_FS_DECRYPTIONSCHEDULED

2.2.78 EventID: 518 - EFS-Dateiupdate fehlgeschlagen

Die EFS-Datei kann nicht geändert werden (als Teil der Unternehmensrichtlinie).
Eventname: EVMSG_FS_CANNOTUPDATEEFSFILE

2.2.79 EventID: 519 - Ungültige Festplatten-Konfiguration

Die Installation der DriveLock Disk Protection ist auf diesem Computer nicht möglich. Die Festplatten-/Partitions-Einstellungen lassen die Installation nicht zu ().
Eventname: EVMSG_FS_INVALIDDISKCONFIG

2.2.80 EventID: 550 - PBA-Kennwortänderung

Benutzer (Domäne) hat sein Kennwort in der Pre-Boot-Anmeldung geändert.
Eventname: EVMSG_FS_PBAUSERPWDCHANGE

2.2.81 EventID: 926 - DriveLock Disk Protection-Notfallanmeldung erfolgreich

Eine Full Disc Encryption-Notfallanmeldung wurde erfolgreich durchgeführt.
Eventname: EVMSG_FDEREC_EML_DES_OK

2.2.82 EventID: 927 - DriveLock Disk Protection-Notfallanmeldung erfolgreich

Eventname: EVMSG_FDEREC_EML_FILE_OK

2.2.83 EventID: 928 - DriveLock Disk Protection-Wiederherstellungsschlüssel erzeugt

Ein Full Disc Encryption-Wiederherstellungsschlüssel wurde erzeugt.
Eventname: EVMSG_FDEREC_RDK_DES_OK

2.2.84 EventID: 929 - DriveLock Disk Protection-Wiederherstellungsschlüssel erzeugt

Ein Full Disc Encryption-Wiederherstellungsschlüssel wurde erzeugt.
Eventname: EVMSG_FDEREC_RDK_FILE_OK

2.2.85 EventID: 930 - {PrefixEnterpriseService} ausgewählt

Der {PrefixEnterpriseService} wurde von der {PrefixMMC} ausgewählt.
Eventname: EVMSG_MMC_SRVCHOOSENCONNECTION

2.2.86 EventID: 932 - DriveLock Disk Protection-Wiederherstellung fehlgeschlagen

Eine Full Disc Encryption-Wiederherstellung ist fehlgeschlagen.
Eventname: EVMSG_FDEREC_DES_ERROR

2.2.87 EventID: 933 - DriveLock Disk Protection-Wiederherstellung fehlgeschlagen

Eine Full Disc Encryption-Wiederherstellung ist fehlgeschlagen.
Eventname: EVMSG_FDEREC_FILE_ERROR

2.2.88 EventID: 934 - DriveLock Disk Protection-Installationspaket hochgeladen

Ein Full Disc Encryption-Installationspaket wurde zum Server hochgeladen.
Eventname: EVMSG_FDE_PKGUPLOAD_OK

2.2.89 EventID: 935 - DriveLock Disk Protection-Installationspaket-Upload fehlgeschlagen

Ein Full Disc Encryption-Installationspaket konnte nicht zum Server hochgeladen werden.
Eventname: EVMSG_FDE_PKGUPLOAD_FAIL

2.3 Notwendige Informationen für den Support

Damit der DriveLock Support die Probleme genauer analysieren kann sind die folgenden Informationen notwendig:

Hardware Hersteller?	
Hardware Modell?	
Betriebssystem?	
Betriebssystem 32bit o. 64bit?	
Betriebssystem Sprache?	
Betriebssystem Build Nummer?	
DriveLock Version?	
BIOS oder UEFI?	
BIOS oder UEFI Version aktuell?	
Boot über 16bit PBA möglich?	
SATA / RAID / NVME?	