DriveLock Release Notes

Release Notes 2023.2

DriveLock SE 2023

Table of Contents

1 DriveLock Release Notes 2023.2

Build: 2023.2.2

Date: 2023-12-04

The DriveLock Release Notes contain important information on bug fixes and known issues in this version. They also contain an overview of the system requirements for using DriveLock, as well as our End-of-Life announcements.

Please find a summary of the new features in this version here, for a detailed description please refer to the What's new? topic in the DriveLock documentation.

Links to the release notes of past and still supported versions can be found in the Archive menu at DriveLock Online Help.

1.1 New features and improvements in version 2023.2

- Multi-factor authentication at the DOC
- New Security Awareness functions in the DOC
- Improved accessibility
- Option to delete computers via API
- Improved display of reports in the DOC
- File Protection: the old and new encryption formats work at the same time
- Firewall: Improved logging
- Improved inventory
- More extensive options for the drive list rules
- Improved priority setting for drive, device and application rules

1.2 Bug fixes

DriveLock 2023.2 is a major version.

This chapter contains information on errors that have been fixed with DriveLock version 2023.2. Our External Issue numbers (EI) serve as references, where applicable.

	Application Control
	The installed DOC Companion is now included in the special application control rule using the "Installed Drivelock modules" option.
EI-2529	Checking the file owner in application control rules failed for some files on network shares.

	Operating system management
EI-2522	The firewall settings and firewall rules defined in the policy were not created immediately after a new user logged on, but only when the policy was reloaded or the DriveLock service was restarted.

	BitLocker Management (BLM)
	If BitLocker was configured improperly, BLM repeatedly tried to initiate a repair. If BitLocker was configured improperly, BLM repeatedly tried to initiate a repair. If this occurred, the DriveLock agent would no longer shut down properly.
EI-2523	After initial encryption with a BitLocker password and then restarting, the password dialog sometimes reappeared.

	Defender Management
	The interval for sending the current Defender status to the DES has been shortened from 24 to 6 hours.
EI-2472	Under certain circumstances, the Microsoft Defender status in the DOC was incorrectly displayed as not up-to-date, although the Windows Defender on the affected agents was actually up-to-date.

	Device Control
	File filter templates/quotas: Reading quotas for larger files now works regardless of the file type.
	The file size limit is now checked correctly.
EI-2546	In earlier versions of the file size limit function and other quota settings, creating new files via a copy operation was not monitored. This bug is fixed now.
EI-1657	Fixed a bug where the file size limit for shadow copies was ignored.

Reference	Disk Protection
EI-2146	Due to a timing problem, the events 506 "The Disk Protection encryption service was started" and 508 (for Disk Protection / DriveLock PBA) "The Disk Protection management service was started" were not written when booting the client.

Reference	DriveLock Management Console (DMC)
EI-2548	The DMC crashed when a DLC file was imported into a centrally stored policy in the old format, into a configuration file or into a GPO.

Reference	DriveLock Operations Center (DOC)
	If a drive rule only contained drives without a serial number, changes to the rule were ignored when saving.
EI-2489	In the DOC, the functions "BitLocker - Show recovery key" and "Advanced - Show local user password" are only available on computers for which the corresponding recovery data is stored in the database.
EI-2163	Grouped lists now show all the contents of the groups.
EI-2545	The list of drives contained in a drive rule always displayed all drives on all pages, even if only a certain number of drives were to be displayed.

Reference	Encryption-2-Go
EI-2067	When mounting a USB stick encrypted with Encryption 2-Go, the admin password was always used if defined. Two options were in conflict, one of which has now been removed. The admin password is now only used if the 'Attempt to mount using administrative password first' option is selected.

Reference	File Protection (FFE)
EI-2560	The PCloud software caused an error in the DriveLock file filter due to device naming. Now the file filter no longer attempts to connect to the PCloud device.
	In previous versions, quota settings were applied to ignored processes, which reduced the user quota in a non-transparent way. This has now been fixed. However, read/write accesses from third-party applications (e.g. AVs) in connection with non-ignored processes still lead to the quota for non-user accesses being counted.
	If a folder on a network share was decrypted by a DriveLock agent, it could happen that other agents could not access this folder afterwards.
	Decryption of a Folder encrypted with "New Format" executed on an agent running in "Old format" left the folder unusable, therefore this kind of decryption is now prevented.
	In some cases, access to the simple folder was still denied after decryption, as if it were still encrypted. This is fixed.

Reference	Groups / Permissions
	Drivelock user groups can now be included in the list of users who are allowed to accept the usage policy.

Reference	Security Awareness
	Security awareness campaigns of the 'Training' type were always reported as 'canceled' by the agent, even if they had been fully completed. As a result, such a campaign was displayed over and over again.
	Usage policies were displayed for users who were not allowed to use the device (and if they accepted, the device was unlocked).
EI-2570	Fixed a bug where the reported memberships in user groups were not updated correctly on some occasions.

Reference	Self-service
EI-2256	If self-service is started after the usage policy, the user can now select the required self-service rule (if more than one rule applies to the current computer).

Reference	Vulnerability Management
	The DOC option "Hide vulnerability" for a single computer did not work.

1.3 Known issues

1.3.1 BitLocker Management

Supported versions and editions:

DriveLock BitLocker Management supports the following operating systems:

- Windows 7 SP1 Enterprise and Ultimate, 64 bit, TPM chip required
- Windows 8.1 Pro and Enterprise, 32/64 bit
- Windows 10 Pro and Enterprise, 32/64 bit
- Windows 11 Pro and Enterprise, 32/64-bit

Native BitLocker environment

Since version 2019.1, if you want to manage an existing system environment that already contains computers encrypted with BitLocker, they no longer need to be decrypted beforehand via the existing BitLocker management or group policies. DriveLock detects native BitLocker encryption automatically and creates new recovery information. The drives are only decrypted and encrypted automatically if the encryption algorithm configured in the DriveLock policy differs from the current algorithm.

After that, you can use DriveLock BitLocker Management to manage your computers and securely store and utilize the recovery information.

Using passwords

With DriveLock BitLocker Management, the misleading distinction between PINs, passphrases and passwords is simplified by simply using the term "password". Also, this password is automatically used in the correct BitLocker format, either as a PIN or as a passphrase.

Since Microsoft has different requirements for the complexity of PIN and passphrase, the following restrictions apply to the password:

- Minimum: 8 characters In some cases, you can also enter 6 characters (numbers); for more information, see the Password options in the current documentation.
- Maximum: 20 characters

Warning: Note that BitLocker's own PBA only provides English keyboard layouts, which means that using special characters as part of the password may cause login issues.

Encrypting extended disks

Microsoft BitLocker limitations prevent external hard disks (data disks) from being encrypted if you have selected the "TPM only (no password)" mode, since BitLocker expects you to enter a password (BitLocker terminology: passphrase) for these extended drives.

Encryption on Windows 7 agents

On Windows 7 agents, the following error may occur when you use the new execution options added in DriveLock 2020.2: BitLocker does not encrypt on Windows 7 if the "when the screen saver is configured and active" and "when no application is running in full screen mode" options are enabled.

Moving from Disk Protection to BitLocker Management

You must remove Disk Protection with the appropriate policy setting before you can use BitLocker Management.

Encryption with BitLocker To Go

After encrypting a USB stick with an administrative password, it would not connect. To solve the issue, remove the USB flash drive first and then plug it back in.

Misleading message when updating from version 2022.2 to 2023.1

If the policy is set to allow end users to delay encryption, when upgrading from version 2022.2 to 2023.1, the "BitLocker Encryption" dialog box is incorrectly displayed even though the volumes are already encrypted. As soon as the "Encrypt" button is clicked, the dialog box disappears and neither encryption nor decryption takes place.

1.3.2 Defender Management

The quick scan can only work if a user is logged in to the system locally. It will not do just to log in via a remote desktop connection (RDP session), because Defender management tasks cannot be performed from the DOC in RDP or Terminal Server / Citrix sessions. (Reference EI-2092)

1.3.3 Device Control

Quota / File filter templates

- On the Quota tab, the bytes written or read per time unit are counted, not the actual files. Therefore, the creation of new files with 0 bytes is not blocked.
- Each opened file counts towards the number, even for the same file, and sizes are accumulated.
- The read quota has priority over the write quota, as a read operation is required before the write operation and is blocked if the read quota has already been exceeded.
- The behavior of quotas is application-specific and depends on how an application opens a file for what appears to be just a read or write request from the user.
- A file can be cached or opened multiple times or duplicated or renamed before the actual read/write processing, e.g. Wordpad consumes the number of files by 3 each time it is opened.
- Interfering processes that act on behalf of the user (AV) can further distort the planned behavior.

Long serial numbers

Drives with serial numbers longer than 63 characters cannot be blocked or allowed by a whitelist rule with a required serial number or a default policy.

Files blocked for a short time

Files may be blocked on a USB flash drive for short time during a configuration update when a file filter is configured and access is permitted for specific users or groups.

CD-ROM drives

DriveLock only shows a usage policy once when a CD is inserted. When ejecting the CD and inserting a new one, the usage policy does not appear any more but the new CD is blocked nonetheless. When you restart DriveLock, the usage policy appears again.

Note: This is because DriveLock only recognizes the actual device in the policy (CD-ROM drive), not the content (CD-ROM).

1.3.4 Disk Protection

Windows Inplace Upgrade

If you have enabled a certain number of automatic logins for the PBA (dlfdecmd ENABLEAUTOLOGON <n>) before updating to a current Windows 10 version, the automatic logon is active throughout the upgrade process. However, since the <n> counter cannot be updated during the process, we recommend that you just set it to 1 so that after upgrading, after another reboot, there is only one automatic login followed by another user login to the PBA.

Antivirus software

Antivirus protection software may cause the DriveLock Disk Protection installation to fail if the antivirus software quarantines files in the hidden `C:\SECURDSK` folder. If this occurs, please disable your antivirus protection for the duration of the Disk Protection installation. We recommend that you configure your virus scanner with an exception for the folder.

Application Control

We strongly recommend that you disable Application Control as long as it is active in whitelist mode for the duration of the Disk Protection installation to prevent programs required for the installation from being blocked.

Hibernation

Hibernation will not work while a disk is encrypted or decrypted. After complete encryption or decryption windows has to be restarted once to make hibernate work again.

UEFI mode

> Note: Not all hardware vendors implement the complete UEFI functionality. You should not use the UEFI mode with UEFI versions lower than 2.3.1.

- The PBA provided by version 2019.2 is only available for Windows 10 systems, because the driver signatures from Microsoft required for the hard disk encryption components are only valid for this operating system.
- The PBA for UEFI mode may cause issues with PS/2 input devices (e.g. built-in keyboards).
- With VMWare Workstation 15 and also with a few hardware manufacturers, our test results revealed conflicts with mouse and keyboard drivers of the UEFI firmware, so that keyboard input in the PBA is not possible. In this case, you can use the "k" key to prevent the DriveLock PBA drivers from loading once when you start the computer.

After Windows logon to the client, you can then run the `dlsetpb /disablekbddrivers` command in an administrator command line to permanently disable the DriveLock PBA keyboard drivers. Be aware that the standard keyboard layout of the firmware is loaded in the PBA login mask, which usually is an EN-US layout, so special characters may differ.
Introducing the combined driver as of version 2020.1 solves the issue on some systems (including VM Ware Workstation 15).
For more information, please refer to the Shortcut and function keys chapter in the current documentation.

Note the following information:

- DriveLock 7.6.6 and higher supports UEFI Secure Boot.
- If you update the firmware, the NVRAM variables on the mainboard that DriveLock requires may be deleted. We strongly recommend that you install the firmware updates for the mainboard /UEFI before installing DriveLock PBA / FDE (this also applies to recently purchased devices or to bug fixes).
- A 32 bit Windows operating system or 32 bit DriveLock cannot be installed on 64 bit capable hardware. Please use a 64 bit version of a Windows operating system and DriveLock instead.
- There is still a limitation to disks up to a maximum of 2 TB disk size.
- Some HP computers always have Windows in position 1 of the UEFI boot order and the DriveLock PBA has to be selected manually in the UEFI boot menu. In this case fast boot has to be switched off in UEFI to keep the DriveLock PBA at position one.

Workaround for Windows Update from 1709 to 1903 while encrypting drive C: with Disk Protection:

Reference: EI-686

1. Decrypt drive C:
2. Update Windows 10 from 1709 to 1903
3. Encrypt drive C:

Requirements for Disk Protection:

Disk Protection is not supported for Windows 7 on UEFI systems.

Restart after installation of PBA on Toshiba PORTEGE Z930:

Reference: EI-751

After activating Disk Protection with PBA and restarting the above-mentioned notebooks, Windows cannot be started and so the notebook cannot be encrypted. Our team is working on a solution.

1.3.5 DriveLock Mobile Encryption

DriveLock Mobile Encryption: NTFS/EXFAT

DriveLock Mobile Encryption (Encryption 2-Go) can mount NTFS/EXFAT containers as read-only.

1.3.6 DriveLock Operations Center (DOC)

Old versions of DOC.exe are no longer supported

You will need to manually uninstall old DOC.exe versions starting with version 2021.2. Note that these old versions will no longer work with an updated DES and are therefore discontinued.

Login to the DOC for users who have been removed from an AD group

Users can still log in to the DOC even if they have already been removed from an AD group and therefore no longer have authorization for logging in. This is because group memberships for a user are read from the group token. This information is only updated at certain intervals.

1.3.7 DriveLock Pre-Boot Authentication

- Hardware must support the TCP4 UEFI protocol for the DriveLock PBA network functionality to work. For this reason, some systems may run into trouble if the UEFI BIOS does not support the required network connections. This is specifically the case with the following systems:
  - Fujitsu LifeBook E459. (Reference: EI-1303)
  - Fujitsu LifeBook U772
  - Acer Spin SP11-33
  - Acer Spin SP513-53N
  - Dell Inspirion 7347
- The UEFI firmware of guest systems in Hyper-V environments does not supply the Microsoft Corporation UEFI CA 2011 certificate, which is mandatory for using DriveLock PBA on Hyper-V clients with SecureBoot enabled. Therefore, the DriveLock PBA is presently not supported on Microsoft Hyper-V clients. (Reference EI-2194)
- The EURO character "€", that a German keyboard provides when entering the 'Alt Gr' and 'e' combination, is not recognized when logging into the DriveLock PBA.
- On some DELL devices, the implementation of time counting differs from the standard and may result in a longer time span than expected. Unfortunately, we cannot solve this hardware-related issue through programming. (Reference: EI-1668)
- DriveLock uses its own UEFI driver for keyboards by default (either a simple one or a combination driver with mouse support) to offer international keyboard layouts within the PBA as well. It is loaded with the help of a UEFI standard interface. On some models, this interface specified in the UEFI standard is not implemented correctly or not at all. In such cases, it is possible to disable loading the DriveLock driver, either using the command line command "dlsetpb /KD-" or via a setting within the policy available in DriveLock version 2021.2.
  Note that the default driver implemented by the manufacturer is used here, which usually only supports an English keyboard layout.
- If you add additional unencrypted disks to an already encrypted system, always make sure to access the new disks after the existing disks to avoid any access issues to the EFS or failure to synchronize users. (Reference: EI-1762)
- When the PBA is installed, the Windows logon screen provides logon for other users, but does not show the user who was logged on last time. This occurs because of the

"Fast User Switching" feature used for that purpose in Windows and its implementation by Microsoft. (Referenz: EI-1731)

- Warning: In the event of a time change (for example, winter time to daylight saving time), you run into a mismatch between server and system time if your DriveLock Agents were shut down prior to the change (thus using the 'old' time), but the time on your server has already been changed. In this case, the login to the network PBA is blocked. End users must select a different logon method once (user name / password entry) or you need to adjust the system time manually. Once both times are synchronized, logging into the network PBA will work again. (Reference EI-1817)
- The DriveLock PBA requires smart card readers to have a CCID V1.1 compliant interface.

1.3.8 Settings for enforced encryption

Setting the encryption method for forced encryption of an external storage device

If the administrator did not specify the encryption method, a dialog for selecting the encryption method (Encryption-2-Go, Disk Protection, BitLocker To Go) appears on the DriveLock agent when connecting the external storage device. In some cases, however, this dialog appears incorrectly even for SD card readers without media.

1.3.9 File Protection

Microsoft OneDrive

- With Microsoft OneDrive, Microsoft Office may synchronize directly with OneDrive instead of writing the file to the local folder first. Then the DriveLock encryption driver is not involved and the Office files will not be encrypted in the Cloud. To stop this behavior, deselect **"Use Office 2016 to sync files I open"** or similar settings in OneDrive. Make sure that Office files as other files always are stored locally.
- Deleting encrypted folders in the local OneDrive directory can, under certain circumstances, result in an empty folder remaining.

NetApp

- Currently, some incompatibility persists between DriveLock's encryption driver and certain NetApp SAN drivers or systems that cannot yet be more precisely defined. Please check the functionality you require before using File Protection in this system environment. We are happy to help you here to analyze the issue in detail if necessary.

Windows 10 clients with Kaspersky Endpoint Security 10.3.0.6294

- The blue screen error persists after activating DriveLock File Protection (DLFldEnc.sys).

Accessing encrypted folders

- Access to encrypted folders on drives that are not mounted with drive letters but as volume mountpoints is not supported.

Cancel folder encryption

- We do not recommend canceling the encryption/decryption of folders. If this happens (has happened) nevertheless, do not delete the database file, as the status of the running files will be lost.

File Protection and USB drives

- You cannot use DriveLock File Protection to fully encrypt a connected USB drive if the drive already contains an encrypted folder. In this case the following message appears “Cannot read management information from the encrypted folder".
- In case a removable storage device (USB stick) is encrypted, removing the device may make it impossible to open the folder that was just encrypted. If the device is formatted and reconnected externally when this happens, a new initial encryption that follows may be stuck due to the previous deactivation error.

If you prefer this type of workflow, we recommend either disconnecting the folder before removing it or removing the device "safely" (e.g. by ejecting it) and allowing for closing open files.

Check for unencrypted files

- If the 'CheckForUnencryptedFiles' function finds unencrypted files in network folders after a successful mount, the subsequent initial encryption of these files fails.
  We recommend canceling the process, then unmounting and remounting the folder.
  The check and initial encryption is successful the second time.

Distributed File System (DFS)

- DriveLock File Protection basically also supports storing encrypted directories on a network drive with Distributed File System (DFS). DriveLock File Protection basically also supports storing encrypted directories on a network drive with Distributed File System (DFS). Since DFS and the associated storage system can contain customer-specific characteristics, however, we recommend that you test encrypted directories in detail before using them. Please note the information in the Updating the DriveLock components chapter.

> Warning: If you have previously used a version older than 2021.2, make sure that there are no encrypted folders on DFS network drives before updating to version 2023.1.

1.3.10 Self-service

If you are using the self-service wizard to unlock Apple iPhone devices, it is still possible to manually copy images from the iPhone device after the unlock is complete, as long as the device is connected.

1.3.11 Thin Clients

Please note the following restrictions when using DriveLock and Thin Clients:

- Security Awareness cannot be used on IGEL clients.

1.4 End-of-Life announcement

DriveLock sends out a newsletter in time to inform you about the end of support and maintenance for a specific DriveLock version.

For the following versions, the corresponding End-of-Life (EoL) data apply:

Version	On-premise customer support exists until:	Cloud customer support exists until:
All versions before 2021.2	EoL - not supported any more	EoL - not supported any more
2021.2	May 2024	EoL - not supported any more
2022.1	EoL - not supported any more	EoL - not supported any more
2022.2	June 2025	EoL - not supported any more
2023.1	Development support *1: December 2024 Product support *2: June 2025	Until the release of a version following 2023.2
2023.2	current version	current version

Note: We recommend that all our customers install the latest DriveLock version.

Support lifecycle:

Starting with this release, we are adjusting the support lifecycle for new DriveLock product versions for all operating systems.

As soon as a new product version is released, we announce the End of Life (EoL) of the **previous version**.

*1 DriveLock will continue to provide full support for this version for 12 months from the date of the EoL announcement. This includes critical maintenance updates, code fixes for bugs and critical issues.

After the expiration of full support (12 months), DriveLock will no longer release new updates for this version.

*2 However, DriveLock product support is available for a further 6 months to answer telephone, e-mail and self-service inquiries.

This applies to all on-premise versions from version 2023.1.

Upgrades:

Customers who have previous product versions and a valid maintenance contract can upgrade the environment to the latest product version.

End of life of features:

- Version 2023.2 is the last version that supports Novell Directory Services (NDS).
- We have stopped developing the DCC and it will no longer be part of our product. DriveLock 2021.2 is the last version that officially supports the DCC until May 2024.

Note: **TLS 1.2**: Please ensure that all operating systems running DriveLock support TLS1.2 by October 31, 2024.

2 System requirements for operating DriveLock

The values listed in this document are recommended and represent minimum requirements. The requirements may vary depending on your configuration of DriveLock, its components and features, and your system environment.

2.1 DriveLock Agent

DriveLock Agent can be installed on different versions of Windows, Linux and macOS.

Operating system	Versions
Windows 11	As of 21H2, only Pro / Enterprise editions
Windows 10	As of 20H2, only Pro / Enterprise editions
Windows 10 LTSC	all LTSC versions until expiry of the respective Extended Support
Windows Server	2016, 2019, 2022
Windows 7	Windows 7 SP1 Enterprise / Ultimate with Extended Support. Note: An additional Legacy Support license is required when running on Windows 7 systems.
Linux	CentOS 8, Debian 11, Fedora 34, IGEL OS 11.05, Red Hat Enterprise Linux 5, Suse 15.3, Ubuntu 20.04 or newer versions
macOS	starting with version Catalina (10.15) with Intel (x86_64) and Apple Silicon (arm64) architectures

The Windows DriveLock Agent is basically available for AMD-/Intel X86-based systems (32-bit and 64-bit architecture). We recommend using a 64 bit system for the DriveLock Agent.

Server operating systems are only supported under 64-bit. You will find the restrictions of the individual functionalities described below.

Warning: .NET Framework 4.7.2 is required to display security awareness campaigns on DriveLock Agents.

See the following table for an overview of the functionality available on a particular operating system.

- Complete range:(✓)
- Reduced scope:(⓪)
- No support:(☒)

Feature	Operating system / functions				
	Windows 10 / 11	Windows Server	Windows 7	Linux	Mac OS
Device Control	✓	✓	⓪	⓪	⓪
Application Control	✓	✓	✓	⓪	☒
Encryption-2-Go	✓	✓	✓	⓪	⓪
BitLocker To Go	✓	✓	⓪	☒	☒
BitLocker Management	✓	✓	⓪	☒	☒
Security Awareness Multimedia campaigns	✓	✓	✓	☒	☒
Defender Management	✓	✓	☒	☒	☒

Feature	Operating system / functions				
Vulnerability Management	✓	✓	✓	☒	☒
Security Configuration Management	✓	✓	✓	☒	☒
Disk Protection	✓(*)	☒	☒	☒	☒
File Protection	✓	✓	⓪	☒	☒

(*): On Windows 10 and newer, Disk Protection is available only for UEFI systems, BIOS support has been discontinued.

Note: Security Awareness: Please note that as of version 22.1, Content AddOn packages can only be displayed correctly if Microsoft Edge WebView2 is installed on the agents . Please follow the download link: https://developer.microsoft.com/en-us/-microsoft-edge/webview2/#download-section. Windows 11 already has Microsoft Edge WebView2 installed automatically.

Details on the restrictions for operating systems that can only use some of the DriveLock features:

1. **Restrictions for Windows Server**
   - DriveLock pre-boot authentication is not available for server operating systems.
   - Microsoft Defender settings are only available for Windows Server 2016 and later.
2. **Restrictions for Windows 7**

   Make sure that the latest available patch level is installed on a Windows 7 client.
   - In general:
     - After updating, installing or uninstalling DriveLock Agent on Windows 7 x64, the Explorer (explorer.exe) may crash. This only occurs if the Windows

command prompt is opened with admin privileges and the system has not been rebooted since the agent was updated/ installed/uninstalled.

- KB3140245 must be installed on Windows 7
  Please find further information here and here.
  Without this update, WinHTTP cannot change any TLS settings and the error 12175 appears in the dlwsconsumer.log und DLUpdSvx.log log files.
- KB3033929 (SHA-2 code signing support) must be installed on Windows 7 64 bit.
- DriveLock Service adds missing registry values for TLS 1.2 connections on computers running Windows 7.
  The following registry values are the prerequisite for communication with the DES in addition to KB3140245:
  - `[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\SecurityProviders\SCHANNEL\Protocols\TLS 1.2\Client]"Enabled"=dword:00000001`
  - `[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\SecurityProviders\SCHANNEL\Protocols\TLS 1.2\Server]"Enabled"=dword:00000001`
  - `[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\InternetSettings\WinHttp] "DefaultSecureProtocols"=dword:00000800`

    Note: If the `DefaultSecureProtocols` value already exists, add the value `0x00000800` for TLS 1.2.

- BitLocker Management:
  - Only available for Windows 7 SP1 Enterprise and Ultimate, 64-bit - TPM chip is required
  - BitLocker does not encrypt on Windows 7 if the options "When the screen saver is configured and active" and "When no application is running in full screen mode" are enabled.
- BitLocker To Go:

- Only available for Windows 7 SP1 Enterprise and Ultimate

- Device Control:
  - In Windows 7, you cannot use the Bluetooth options for devices in the Device class locking section.

- File Protection:
  - Under Windows 7, only the limited functionality is available for the new encryption format and only the previous legacy driver is available for the old encryption format. The appropriate encryption format is selected automatically.

- Security Awareness Multimedia Campaigns:
  - To be able to display Security Awareness multimedia campaigns you need a local installation of WebView2 for Windows 7. For more information, click here: https://docs.microsoft.com/en-us/microsoft-edge/webview2/

3. **Restrictions for macOS**

- Device Control:
  In this version, only USB-attached drives identified by their hardware ID can be blocked or allowed.
  In addition, please note the following restrictions:
  - You need to configure your own rule types for whitelisting (Hardware ID instead of Product ID/Vendor)
  - No unlocking for specific users or user groups
  - No file filter and auditing
  - No forced encryption
  - No unlocking for drives already encrypted with Encryption 2-Go
  - No self-service functionality

- Encryption 2-Go:
  - For macOS, the Mobile Encryption Application (MEA) is available as before for decrypting external USB drives.
  - The macOS Agent is not yet able to automatically encrypt drives with an Encryption 2-Go container.

  For more information about the macOS Agent, please refer to the separately available macOS documentation on DriveLock Online Help.

4. **Restrictions for Linux**
    - Device Control:
        - You need to configure your own rule types for whitelisting (Hardware ID instead of Product ID/Vendor)
        - No unlocking for specific users or user groups
        - No file filter and auditing
        - No forced encryption
    - Application Control:
        - DriveLock Application Control requires Linux kernel version > 5 for use on Linux agents.
        - Application Control cannot be used together with IGEL OS.
        - None of the Application Behavior Control functions are available on Linux.
    - Encryption 2-Go:
        - Containers or encrypted USB drives cannot be created, only connected.

    For more information about the Linux client and the limitations of its functionality, please refer to the separately available Linux documentation on DriveLock Online Help.
5. **Restrictions for terminal server environments and thin clients**
    - The DriveLock Agent requires the following system requirements in order to use the DriveLock Device Control functionality:
        - XenApp 7.15 or newer (ICA).
        - Windows Server 2016 or newer (RDP).
    - Security awareness campaigns for users at login and ICA drive connections are not available when using thin clients without DriveLock Agent installed.

2.2 DriveLock Management Console

Before you install the DriveLock Management Console, please make sure that the computer meets all of these requirements to ensure full functionality.

> Warning: Always use the DriveLock Management Console (DMC) that matches the DriveLock Enterprise Server (DES) version.

Main memory:

- at least 4 GB RAM

Free disk space:

- approx.350 MB

Additional Windows components:

- .NET Framework 4.8 or higher

Supported platforms:

The Management Console 2023.2 has been tested and released on the current levels of 64-bit Windows versions that were officially available at the time of release and that have not yet reached the end of the service period at Microsoft. Please check the DriveLock Agent chapter for a list of Windows versions that DriveLock supports.

2.3 DriveLock Enterprise Service

> Note: This information applies only to DriveLock On-Premise installations.

Before distributing or installing the DriveLock Enterprise Service (DES) on your corporate network, please ensure that the computers meet the following requirements and are configured properly to provide full functionality.

Main memory / CPU:

- at least 8 GB RAM, CPU x64 with 2,0GHz and EM64T (Extended Memory Support)

Free disk space:

- at least 4 GB, with policies that do include Security Awareness campaigns with video sequences (Security Awareness Content AddOn), approx. 15 GB is recommended
- if the server is also running the SQL-Server database, additional 10 GB are recommended for storing DriveLock data

Additional Windows components:

- .NET Framework 4.8 or higher is required for installation!

Note: Depending on the number and duration of the DriveLock events that are stored, the size of the DriveLock database can vary greatly from one system environment to another. It is therefore difficult to provide an exact specification here. We recommend setting up a test environment with the planned settings over a period of at least a few days to determine the exact values. These values can be used to calculate the required memory capacity.

Required DriveLock API Services Ports (DOC/MQTT):

- 5370, 6369 and 4369: These three ports should not be occupied by other server services, but they do not have to be accessible from outside (internal only)
- 8883: The agents connect to the DES on this port so that they can be accessed by agent remote control. The DES installation program automatically enables the clearance in the local firewall of the computer.

Supported platforms:

- Windows Server 2016 64-bit
- Windows Server 2019 64-bit
- Windows Server 2022 64-bit

On a Windows 10/11 client operating system, a DES should only be run as a test installation.

Warning: The DES is only available as a 64-bit application.

Supported databases:

- DriveLock requires SQL Server 2016 as of version 2023.1. The database must have a compatibility level of 130 or higher.
- SQL Server Express 2016 or newer for installations with up to 200 clients and test installations
- The DES requires the **Microsoft SQL Server 2012 Native Client version 11.4.7001.0**. In case this component is not yet installed, this happens automatically before the DES is actually installed. If an older version is already installed, it will be updated automatically.

Note: Please refer to the applicable Microsoft documentation regarding the system requirements for installing the SQL database or SQL Express.

Warning: The database connection between the DriveLock Operations Center and the database requires a TCP/IP connection.

2.4 DriveLock Operations Center (DOC)

Note: This information applies only to DriveLock On Premise installations.

The web-based DriveLock Operations Center is included in the DES installation and is not a stand-alone component. It is accessed via a browser. The DriveLock Policy Editor can be accessed via DOC Companion.

SQL Server 2016 or newer is the minimum requirement for DriveLock Operations Center.

DriveLock Operations Center is only available for AMD / Intel X86 based 64-bit systems.

Please also note the following information.

Copyright

Information in this document, including URL and other Internet Web site references, is subject to change without notice. Unless otherwise noted, the example companies, organizations, products, domain names, e-mail addresses, logos, people, places, and events depicted herein are fictitious, and no association with any real company, organization, product, domain name, e-mail address, logo, person, place, or event is intended or should be inferred. Complying with all applicable copyright laws is the responsibility of the user.

© 2023 DriveLock SE. All rights reserved.

DriveLock and others are either registered trademarks or trademarks of or its subsidiaries in the United States and/or other countries.

The names of actual companies and products mentioned herein may be the trademarks of their respective owners.