

DriveLock Release Notes

Release Notes 2026.2

DriveLock SE 2026



Table of Contents

1 DRIVELOCK RELEASE NOTES 2026.2 4

1.1 New features, improvements and changes 5

1.2 Bug fixes 12

1.3 Known issues and notes 18

1.3.1 BitLocker Management 18

1.3.2 BitLocker To Go 20

1.3.3 Container encryption (Encryption 2-Go) 20

1.3.4 Device Control 20

1.3.5 Disk encryption (Disk Protection) 23

1.3.6 DriveLock Enterprise Service (DES) 26

1.3.7 DriveLock inventory 26

1.3.8 DriveLock Operations Center (DOC) 26

1.3.9 DriveLock Pre-Boot Authentication 28

1.3.10 File encryption (File Protection) 30

1.3.11 macOS Agent 31

1.3.12 Notes on antivirus software 31

1.3.13 Self-service 33

1.3.14 Thin Clients 33

1.4 Recommended configuration 34

1.4.1 Security settings for the DriveLock Agent 34

1.4.2 Preferred centrally stored policies 34

1.4.3 Using trusted certificates 35

1.4.4 License management in the DOC 35

1.5 End-of-life information 35

1.5.1 Version-specific deprecations 38

2 SYSTEM REQUIREMENTS FOR OPERATING DRIVELOCK 39

2.1 DriveLock Agent 39
2.2 DriveLock Management Console 47
2.3 DriveLock Enterprise Service (DES) 47
2.4 DriveLock Operations Center (DOC) 49
3 SECURITY BULLETINS 50
COPYRIGHT 51

1 DriveLock Release Notes 2026.2

Build: 26.2.2.19872

Date: 2026-11-18

The DriveLock Release Notes contain important information about new features, changes and bug fixes in the main version 2026.2, as well as known limitations. They also contain an overview of the system requirements for using DriveLock, plus end-of-life announcements.

Please find a detailed description of the new features, improvements and changes in 2026.2 in the **What's new?** chapter in the DriveLock documentation at DriveLock Online Help.

> Note: This version includes internal improvements for enhanced stability and security. We recommend updating to the latest version.

Find the release notes of previous and still supported versions in the **Archives** menu at DriveLock Online Help.

Please note the general information on updating to new versions in the the DriveLock documentation.in the chapter **Updating DriveLock** in the DriveLock documentation at DriveLock Online Help.

1.1 New features, improvements and changes

The following sections provide an overview of the new features, improvements, and changes in DriveLock version 2026.2.

This version includes security enhancements, stability improvements, and refinements to existing functionality.

A detailed description can be found in the **What's new?** chapter in the DriveLock documentation at DriveLock Online Help.

> Warning: With every release, additional functionality is migrated from the DriveLock Management Console (DMC) to the DriveLock Operations Center (DOC). Some features may behave slightly differently in the DOC due to technical differences in implementation. Please ensure that all agents have been updated to the latest version before using the new DOC features in production.

> Warning: Installing the update may lead to changes in product behavior in certain areas. Before proceeding with the update, review your configuration to determine whether your current environment is affected. Relevant topics are marked with the following warning icon: ⚠

Application Control (AC)

- Block outgoing network connections: Application Control now supports blocking outgoing network connections through application behavior rules.
- ⚠ Changed reporting of script execution: Script execution is no longer reported through the previous file access events 650 and 651, but through the new events 795 and 796, which provide additional information.
- ⚠ SHA-224 support discontinued: The SHA-224 hash algorithm is no longer supported for hash calculations in Application Control and Device Control.

Awareness with DriveLock Aware

- DriveLock Aware provides cloud customers with a new awareness solution based on the AwareGo platform. It combines behavior-based risk assessments (Human Risk Assessment) with targeted security awareness training.

BitLocker Management

- Additional storage of BitLocker recovery keys in Active Directory Domain Services (AD DS) or Microsoft Entra ID can now be enabled through a setting in the DriveLock Oper-

ations Center (DOC). Recovery keys continue to be stored on the DriveLock Enterprise Service (DES) as well.

Defender Management

- Configure Microsoft Defender Antivirus in the DOC: Microsoft Defender Antivirus and its settings can now be configured directly in the DriveLock Operations Center (DOC) using the policy editor. All previously supported Group Policy settings (GPOs) are available. In addition, the current Microsoft Defender Antivirus status on DriveLock Agents can be viewed in the DOC.
- Start signature updates for Microsoft Defender in the DOC: Signature updates for Microsoft Defender can now also be started directly from the DriveLock Operations Center (DOC).

Device Control (DC)

- ⚠ If no device rules exist for a device, the setting "**Report events for devices of this type**" of the respective device class now also controls event generation. (Reference EI-3225) (Reference EI-3225)
- When using hash lists in volume identification files, files that are not included in the hash list can now be deleted or renamed.

DOC Companion

- Update the DOC Companion: After updating to DriveLock 26.2, the DOC Companion must also be updated to continue working.
  Important: If you installed the DOC Companion using the offline installer, make sure the new version is installed.

DriveLock Agent

- Automatic reactivation of Wi-Fi adapters: Wi-Fi adapters are now automatically re-enabled when the "**Block WiFi connections when the computer is connected to a LAN**" setting is disabled. (Reference EI-3351)
- ⚠ Changed permissions for Agent remote control: Permissions for Agent remote control must now be configured explicitly. If no permissions are configured, local administrators and domain administrators no longer automatically have access to Agent remote control.
  Important: Review your existing permission settings and configure the required access permissions if necessary.
- Choose the notification type: Users can now choose whether notifications are displayed as DriveLock pop-ups or Windows toast notifications from the DriveLock tray

menu.

- Improved Agent update: Handling of corrupted MSI product registrations has been improved when updating the DriveLock Agent. (Reference EI-3288)
- Remote control of the Agent through the DES using HTTP is no longer supported. Communication through the DES using MQTT/HTTPS remains available.
- The Security Awareness button has been removed from the DriveLock Mobile Encryption Application (MEA).

DriveLock Enterprise Service (DES)

- DES now supports certificates with high key derivation iteration counts, for example, client certificates used to send data to Syslog. The maximum allowed value can be adjusted using a configuration parameter. (Reference EI-3287)
- Extended database connection configuration: Additional parameters for the database connection can now be configured in the DriveLock Server Setup Wizard.
- ⚠ Increased security requirements for sending email: For email sent through the DES, the mail server certificate must be trusted by Windows. Self-signed certificates that Windows does not trust are no longer accepted.
- In the Syslog configuration, the "**Optional host name used for TLS handshake**" field can now be left empty. In this case, the host name specified under "**Server**" is used automatically. If an IP address is specified there, the host name for the TLS handshake must still be entered explicitly.
- Policy processing in On-Premise installations has been improved to further enhance security. Managed Cloud environments are not affected.
- The DES now supports SQL logins for database connections. This allows DES to connect to SQL Server instances that are outside the Active Directory domain.
- The protection of security-relevant information in logs has been further improved for On-Premise installations.
- The username and password for DES proxy authentication can now be configured directly in the DOC server settings. (Reference EI-3385)
- ⚠ Trusted certificates for the DES and linked DES servers: Certificate trust is now strictly validated during communication between the central DES and linked DES servers.
- Validation of permissions for administrative functions has been improved.

- When configuring the mail server, you can now specify whether TLS encryption uses STARTTLS or starts immediately when the connection is established. Alternatively, the TLS method can be selected automatically based on the port used.

DriveLock groups

- New filter criterion for Windows services: The new "**Service status**" filter criterion lets you check the status of a Windows service by its internal service name, for example when defining dynamic computer groups.

DriveLock Operations Center (DOC)

- Configuration filters in the DOC: Configuration filters previously available in the DriveLock Management Console (DMC) can now also be created and used in the DriveLock Operations Center (DOC). They allow different settings within a policy to be applied depending on specific computers, users, or time periods.
- Data export for reports: Report data can now also be exported in JSON or CSV format. Data export is available for pie charts, bar charts, horizontal bar charts, and lists. You can choose whether to export only the data or also include the report as a PDF.
- Edit comments for group members: In the DriveLock Operations Center (DOC), comments for group members can now also be edited after they have been added. Previously, comments could only be entered when adding a group member.
- Extended data masking: Personal data in file paths, selected properties, and individual event parameters can now be masked selectively. Regular expressions (RegEx) can also be used to mask individual parts of a value.
- Improved dashboard functionality: The dashboards in the DriveLock Operations Center (DOC) have been further optimized to improve usability and the user experience.
- ⚠ Import and export configurations without checksum validation: Checksums are no longer validated when importing and exporting configurations, such as dashboards, widgets, and external links. This allows exported configurations to be edited manually and then imported again.
  Important: Incorrect changes to exported configurations can lead to inconsistent data in the database when the configurations are imported again. (Reference EI-3387)
- LISA – the new DriveLock AI Assistant: LISA is now available as an AI-powered assistant in the DriveLock Operations Center (DOC). Users can ask questions directly in the DOC and receive AI-generated answers to help them work with DriveLock.

- List and card views in the DOC: Most views in the DriveLock Operations Center (DOC) can now be displayed as either a list or cards. Sorting and filtering options have also been expanded.
- ⚠ Package management is now performed in the DriveLock Operations Center (DOC). There you can manage DriveLock installation packages and specify which package versions are used for installing and automatically updating DriveLock components.
  Important: After updating the DES, package management must be reconfigured in the DOC.
- The new template library in the DriveLock Operations Center (DOC) provides preconfigured rules, policies, filters, dashboards, and bundles. The templates are based on typical use cases and proven configurations. They can be imported as independent copies and then adapted to the respective environment.
  Please note that the template library is available exclusively in DriveLock Managed Services.
- Time-based rule validity in the DOC: Rules can now also be limited to specific times or date ranges in the DriveLock Operations Center (DOC). Previously, this feature was only available in the DriveLock Management Console (DMC).

DriveLock policies

- Extended management of content types in policies: Allowed content types can now also be added to or removed from existing policies. Content types can also be selected individually when importing, exporting, and cloning policies.

DriveLock unlock functionality

- Offline unlock available only when configured: The offline unlock option is now displayed in the user interface only if offline unlocks are configured for the respective drive type or device class.

File encryption (File Protection)

- A custom Readme file can now be used for encrypted File Protection folders. To do so, store the FfeReadMe.pdf file in the file store. It replaces the default Readme file.

Linux Agent

- FIPS-compliant encryption is now also supported on Linux.
- In addition to Samba Winbind, Linux Agents now support SSSD for integration with Active Directory. AD computer objects can now also be used alongside AD users and groups.
  The following features are now available:

- Assign policies and licenses based on the computer's AD or OU membership
- Use of AD users and groups in Device Control rules
- Create dynamic computer groups based on AD properties
- Transmission of Active Directory inventory data to the DES
- Support for AD users on IGEL OS: AD users can log in and be used in Device Control rules without the computer having to be joined to an AD domain.

- Linux Agents now also support Application Control and file filtering on NTFS3 file systems.
- Linux Agents now support offline unlocks, allowing blocked drives and devices to be unlocked temporarily.

macOS Agent

- macOS Agents now support offline unlocks, allowing blocked drives to be unlocked temporarily.
- Temporary online unlock of USB drives on macOS: The DriveLock Operations Center (DOC) can now temporarily unlock all or individual USB drives on macOS computers, provided the computer is online.

Operating systems

- Extended support for Windows on Arm: On Windows 11 Arm64-based systems, DriveLock now also supports Application Control, Device Control, Drive Control, Application Behavior Control, Microsoft Defender Management, and Firewall Management, as well as inventory and local users and groups. See System requirements.

System Management

- The new System Management feature lets you automate administrative tasks on managed computers and enforce defined compliance requirements.
  - Configure actions in the DOC: You can now create and manage PowerShell and batch scripts as actions in the DriveLock Operations Center (DOC). Actions can have parameters and can be used in remote tasks and compliance enforcement rules, as well as in response to events. You specify parameter values when using the action.
  - ⚠ Action execution time: A maximum execution time now applies to PowerShell and batch scripts. The default is 60 seconds. Once this time has elapsed, the script can be terminated automatically if the corresponding option is enabled. Review the settings of existing actions and adjust them if necessary.

- Remote tasks: Remote tasks let you trigger actions on managed computers directly from the DOC as needed. Tasks are distributed through policies and become available in a computer's context menu once the DriveLock Agent has reported them to the DES.
- Compliance enforcement rules: Compliance enforcement rules let you automatically check defined states on managed computers and execute actions if deviations are detected. For example, a script can create a missing file.

1.2 Bug fixes

DriveLock 2026.2 is a major version.

This chapter contains information on errors that have been fixed with DriveLock version 2026.2. Our External Issues (EI) numbers, if available, serve as a reference.

Reference	Application Control (AC)
EI-3284	Fixed an issue where Application Control was unable to calculate executable file hashes on network shares with certain permission configurations.
	Fixed an issue where signature verification did not work for certain file types (such as PS1 and MSI files) if the signature used a SHA-256 digest.

Reference	BitLocker Management (BLM)
	Fixed an issue where the "Always use down-level logon names during single sign-on" option could no longer be enabled.
	Fixed an issue where the BitLocker PBA was incorrectly shown as "Active" in the DOC even though protection of the system drive was disabled.
EI-3298	Fixed an issue where BitLocker key recovery could not be performed through the DOC.

Reference	BitLocker To Go
	Selecting "<Local Computer>" on the "Automatic Unlock Com-

Reference	BitLocker To Go
	puters" tab of enforced BitLocker To Go encryption did not result in automatic unlocking.
EI-3118	Fixed an issue where BitLocker To Go encryption could fail if a Windows policy required the use of an extended XTS encryption algorithm.
EI-3402	Fixed an issue where the DriveLock Agent could transmit incomplete recovery information after encrypting a drive with BitLocker To Go.

Reference	Device Control (DC)
	Fixed an issue where users without the required permissions were presented with the option to add drives or devices from the inventory when creating temporary unlocks.
EI-3366	Fixed an issue where the notification that a temporary unlock was about to end displayed the configured duration instead of the actual remaining time.

Reference	Disk Protection
	Fixed an issue where volumes encrypted with Disk Protection were incorrectly displayed as "Unencrypted" after a restart.

Reference	DriveLock Agent
EI-3248	Fixed an issue where certain third-party events were not transmitted to the DES even though they were selected in the policy.
	Parameters of some third-party events were sometimes displayed incorrectly or in the wrong order.
EI-3288	Fixed an issue during DriveLock Agent updates where installation could fail with error 1603 under certain circumstances. The previous Agent version could be removed without the new version being installed.
	Fixed an issue where the DriveLock service process was displayed with an incorrect icon in Windows Task Manager on some Windows 11 systems.
	Fixed an issue where the DriveLock Agent could crash while processing an MQTT event.

Reference	DriveLock Enterprise Service (DES)
EI-3381	Fixed an issue when selecting organizational units (OUs) for role assignments.
	Fixed an issue affecting rules for event processing and forwarding.

Reference	DriveLock group management
EI-3405	Fixed an issue where references to Active Directory groups in static DriveLock user groups could contain invalid data.

Reference	DriveLock Management Console
	Fixed an issue where user behavior rules from DOC-managed policies were not displayed in the RSOP view of an Agent. The rules were already visible when opening these policies in the DMC.
	Fixed an issue where the DMC could crash under certain circumstances when searching for a user in Microsoft Entra ID.

Reference	DriveLock Operations Center (DOC)
	Fixed an issue where the "Configure Agent" task was not displayed in the context menu of a computer.
	Fixed an issue where the "Temporary unlocks" tab was displayed to users without the required permissions. When the tab was opened, an error message was displayed.
EI-3332	Fixed an issue where special characters in passwords were not displayed by the "Show local user password" function.
	Fixed an issue where incorrect permissions were required to query groups in the DOC Object Picker. The GroupManagement Read permission is now required to query groups.

Reference	DriveLock Operations Center (DOC)
EI-3280	Custom notification messages for drive rules and application collection rules are now displayed correctly on the agent.
EI-3370	Fixed an issue where complex reports were empty when sent by email.
EI-3372	Fixed an issue where sending email through SMTP servers without user authentication failed.

Reference	DriveLock Pre-Boot Authentication (PBA)
	Fixed an issue where, in rare cases, the network logon configuration for Pre-Boot Authentication (PBA) was re-registered on the server during system shutdown. As a result, network logon in the PBA no longer worked.

Reference	Encryption 2-Go
	Fixed an issue affecting administrator passwords in Container Encryption policies.

Reference	File Protection (FFE)
	Fixed an issue where an error occurred under certain circumstances when creating an encrypted folder on the DriveLock Agent.

Reference	File Protection (FFE)
EI-3375	Fixed an issue where managed folders in File Protection could no longer be managed after user certificates were renewed.
EI-3321	Fixed an issue where the Mobile Encryption Agent could produce corrupted files when reading encrypted files.
	Fixed an issue where the configured folder name for enforced encryption was duplicated in the destination path when a user selection rule was used, for example D:\secure\secure instead of D:\secure.

Reference	Unlocks / Self-Service
EI-3222	Fixed an issue where user authentication through Self-Service failed under certain circumstances with an "Access denied" error.

Reference	Linux Agents
	Fixed an issue where the Linux Agent could crash under certain circumstances when a configuration filter was configured.

1.3 Known issues and notes

1.3.1 BitLocker Management

Windows Inplace Upgrade

> Warning: Please note that BitLocker encryption is temporarily deactivated by Microsoft during an inplace upgrade and automatically reactivated after completion. However, if a bootable medium (e.g. CD-ROM) is still connected after the upgrade has been completed, the temporary deactivation remains in place and the encryption must be reactivated manually.

Supported versions and editions:

- DriveLock BitLocker Management supports the following operating systems:
  - Windows 7 SP1 Enterprise and Ultimate, 64 bit, TPM chip required
  - Windows 10 Pro and Enterprise, 32/64 bit
  - Windows 11 Pro and Enterprise, 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 chapter in the current documentation at DriveLock Online Help.
  - 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.

Encryption of external hard 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.

1.3.2 BitLocker To Go

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.

Enforced encryption with BitLocker To Go

- With enforced encryption (BitLocker To Go), unencrypted access is only possible until the next configuration update.

1.3.3 Container encryption (Encryption 2-Go)

Incorrect calculation of memory requirements with enforced encryption under macOS

- When using a rule for enforced encryption with configured free space on the target medium, the size of a new container may not be calculated correctly.

Reduced performance when encrypting exFAT drives on macOS

- Encryption 2 Go may encrypt exFAT-formatted drives significantly slower on macOS than FAT32-formatted drives.
  As a workaround, encrypted containers created on exFAT-formatted drives under macOS must first be attached to a Windows Agent 26.1 with an Encryption 2 Go license. After that, they can be used on Windows without restrictions. (Reference: EI-3138)

1.3.4 Device Control

License settings

- If you have not made any changes to the license settings since version 2020.2, you may encounter issues when migrating the license settings. To avoid this, either make a change before **updating** (for example, by adding and then removing a computer), or reconfigure drive and device activation correctly after the update. (Reference EI-3123)

Blocked devices when using Citrix Workspace

- When used with Citrix Workspace, devices may fail to start on some computers because Windows cannot load the DriveLock driver `DLDevFlt.sys`. The Citrix USB Monitor Driver `ctxusbmon.sys` may cause problems when unloading `DLDevFlt.sys`.

> Note: There are indications that this issue has been resolved in a newer version of Citrix Workspace. We therefore recommend updating Citrix Workspace to the latest version. If the issue persists, open a support ticket with Citrix.

Possible workarounds if updating does not resolve the issue:
Because the issue is likely related to unloading `DLDevFlt.sys`, you can try delaying or preventing the driver from being unloaded.
If the issue occurs only when devices are blocked by DriveLock, enable the setting **Disable blocked devices in Device Manager**.
If DriveLock does not block any devices or this setting does not resolve the issue, you can alternatively use the **Report device removal** setting. This keeps the driver loaded until the device is removed again. Refer to the description of this feature for more information. (Reference EI-2825)

Quotas / File filters

- Write filters should be configured more restrictively than read filters. On Windows, write operations may require read permissions depending on the use case, which could allow read restrictions to be bypassed under certain circumstances. (Reference: EI-3130)
- 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.
- 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 a simple read or write request from a user. A file may be temporarily saved, opened several times, duplicated or renamed before the actual read/write processing takes place. Interfering processes acting on behalf of the user (AV) may further falsify the planned behavior. In version 2025.1, only the first in a series of identical creations of a file is counted towards the "Number of files". (Identical means: same user, same process and same access type - read or write.) This should allow a more reasonable usage of the quota "number of files" count than in older versions.

File filtering for archive files (container files)

- Due to technical limitations, nested embedded files within PDF documents cannot be detected.

- If a file excluded in the file filter is copied to an archive file, the entire archive file is deleted. We recommend that you do not edit archive files directly on the controlled volumes, but on the local hard disk, where no file filter is usually set. (Reference EI-2650)
- Detection of password protection for OpenOffice documents within container files is currently not supported.
- Please note the following information:
  - Non-standard application and file handling behavior may lead to unexpected results. For example, 7-Zip opens ZIP archives and may display portions of a blocked executable file while operating in analysis mode. (Reference EI-2651)
  - WebDAV drives are still not supported
  - Hash exclusions are not applied within archives
  - Simulation mode does not include content scanning
  - If an archive is blocked and initial action was a move from an unfiltered location, the source in the unfiltered location is currently deleted as well.

  Please also note that
  - archives can be scanned up to a nesting level of 2, i.e. zip1/zip2 is scanned, but zip1/zip2/zip3 is blocked,
  - size/number of contained files are not limited; therefore, in spite of a variable timeout adapted to compressed size, a timeout may occur during the scan
  - timeouts and other failures, e.g. failure to open the archive for scanning for whatever reason, will not lead to blocking access.

Content scan

- In certain cases, it's technically not possible to block the deletion of a file. In previous versions, an event for blocking the deletion was still generated in these cases, even though the file had already been deleted.
  Solution: Since the deletion of a file that is classified as unwanted by the content check due to its content is not always an error, the content check and thus also the generation of the event is now omitted.
- Content scan is not possible in folders that have been encrypted with File Protection. It is currently disabled for these folders.

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.

Samsung Shield T7

- The serial numbers for Samsung Shield T7 running Windows are reversed. This may apply to all USB SCSI mass storage devices (UAS).

Cumulative Windows Server 2022 Security Updates on Terminal Server

- Please take the following manual steps if you continue to encounter errors on the affected Windows servers after installing or updating the DriveLock Agent: (Reference EI-2639)
  - **If MTP control is activated:**

    Stop the DriveLock Agent Services and the DriveLock Health Monitor (e.g. net stop drivelock & net stop dlhm) before installing the Windows update. They will be restarted automatically after the reboot.
    If necessary, restart DriveLock manually if it does not restart automatically.

  - **If MTP control is not activated:**

    After updating from an older DriveLock Agent version, please execute the following commands once in the command line: `drivelock -regmtpfltinf` and `drivelock -unregmtpfltinf`.

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).

1.3.5 Disk encryption (Disk Protection)

Important information

- Disk Protection is no longer supported for Windows 7 or older.

Windows Inplace Upgrade

- If you have activated a certain number of automatic logins for the PBA before updating to a current Windows 10 version (dlfdecmd ENABLEAUTOLOGON <n>), the automatic login 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 deactivate Application Control, if 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.

- DriveLock PBA is designed for Windows 10 and 11 because the driver signatures required for the full disk encryption components are only valid for these operating systems.
- 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 in the DriveLock documentation at DriveLock Online Help.

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 recommend that you install the firmware updates for the mainboard / UEFI before installing the DriveLock PBA / FDE (also for newly purchased devices or 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.

1.3.6 DriveLock Enterprise Service (DES)

Registration of linked DES

- A linked DES can only be registered if the user has not activated multi-factor authentication (MFA).

Windows Server 2016: Certificate is not created during DES installation

- When using the legacy DES Setup Wizard on Windows Server 2016, no certificate is created even if the corresponding option is selected. If no certificate is available, the DES cannot be used.
  Workaround: Run the Setup Wizard again and select the option to change or renew the certificate. A new certificate will be generated during this process.

1.3.7 DriveLock inventory

Duplicate entries in CSV exports (DOC) (Reference EI-3131)

When exporting large amounts of data from the DOC (e.g. computers, drives, devices), the CSV export may contain duplicate entries if the underlying list changes during the export (e.g. due to newly added objects).

Workaround:

- Duplicates can simply be deleted from the CSV file.
- To avoid duplicates as far as possible, we recommend:
  - sort the view/query by a column that rarely changes (e.g. name or ID), and
  - limit the export scope so that fewer data records are exported (e.g. by filtering or smaller subsets).

1.3.8 DriveLock Operations Center (DOC)

⚠ Adjusted role permission checks on groups and policy collections

- Role permissions for groups are now checked within the context of the specific group or OU. Previously, it was possible to add or remove computers in any group, even if the user only had permissions for a specific group or OU. In version 2024.2, the permission checks have been adjusted to respect restrictions to the assigned group or OU. To grant permissions across all groups or OUs, use the global "Manage Groups" permission.
  The same applies to policy collections, where the "Manage Policy Collection" permission is now checked accordingly.

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

- Logging on to the DOC continues to work even if the user has already been removed from an AD group and therefore no longer has authorization to log on to the DOC. This is because group memberships for a user are read from the group token. This information is only updated at certain intervals.

Logging in with Windows authentication for users in the 'Protected Users' group

- It is not possible to log in to the DOC using Windows authentication if a user belongs to the "Protected Users" security group. However, logging in via a password works here.
- It is also not possible to log in to the DOC via Windows authentication if users have logged in to Windows with a smartcard. At present, this is not supported. (Reference EI-2597)

1.3.9 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.

1.3.10 File encryption (File Protection)

ISO files cannot be mounted from encrypted folders

- ISO files stored in encrypted folders cannot currently be mounted on Windows.

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.

FireEye

- The FireEye product may trigger a blue screen error (BSOD).

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.

Accessing encrypted folders

- Access to encrypted folders on drives that are not mounted with drive letters but as volume mountpoints is not supported.
- File Protection cannot be used if the encrypted folder is located in an encrypted container.

Locking file regions on network shares

- To resolve potential compatibility issues with certain programs, starting from version 2024.2, the setting 'Files on network shares for which file region locks are not modified' can be used as a workaround.

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 this type of workflow is wanted, we recommend either disconnecting the folder before removing it or removing the device "safely" (e.g. by ejecting it) and allowing for possible rejection, i.e. 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 in this second run.

Distributed File System (DFS)

- DriveLock File Protection supports storing encrypted directories in the new format on network drives 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.

1.3.11 macOS Agent

Data masking on macOS

- Please note that data masking is not yet implemented for the macOS Agent.

DriveLock Mobile App

- On macOS, moving a folder within the Mobile Encryption Application (MEA) to a subfolder within this folder deletes the moved folder completely.

1.3.12 Notes on antivirus software

Depending on the antivirus software in use, it may be necessary to configure exclusions.

The installation of DriveLock Disk Protection may fail if antivirus software quarantines the hidden directory C:\SECURDSK. In this case, you should temporarily disable antivirus protection for the duration of the installation. We recommend defining this directory as a permanent exclusion in the antivirus software.

Note: The same applies if a system contains multiple partitions encrypted with Disk Protection, regardless of whether they are logical partitions on the same storage medium or separate hard disks or SSDs.

If you encounter additional unexpected issues with antivirus software, the following list contains the executable files, directories, and services used by DriveLock:

Files and directories used by DriveLock:

- "C:\SECURDSK" (EFS)
- "C:\Program Files\CenterTools\DriveLock" (application directory)
- "C:\ProgramData\CenterTools DriveLock" (cache/working directory)

Processes/services used by DriveLock:

- **DriveLock**

  Display name: DriveLock
  Executable path: "C:\Program Files\CenterTools\DriveLock\DriveLock.exe"

- **dlhm**

  Display name: DriveLock Health Monitor
  Executable path: "C:\Program Files\CenterTools\DriveLock\DLHM.exe"

- **StorageEncryptionService**

  Display name: DriveLock Full Disk Encryption Encryptor
  Executable path: "C:\Program Files\CenterTools\DriveLock\DlFdeEncSvc.exe"

- **ClientDataManager**

  Display name: DriveLock Full Disk Encryption Manager
  Executable path: "C:\Program Files\CenterTools\DriveLock\DlFdeMgr.exe"

- **dlupdate**

  Display Name: DriveLock Update and Installation
  Executable path: "C:\Windows\DLUpdSvc.exe"

- **dessvc**

  Display name: DriveLock Enterprise Service
  Executable path: "C:\Program Files\CenterTools\DriveLock Enterprise Service\DES.exe"

- **DESTray**

  Function: Displays the DES icon in the taskbar

Executable path: "C:\Program Files\CenterTools\DriveLock Enterprise Service\DESTray.exe"

- **DesRestarter**

  Function: Restarts the DES service
  Executable path: "C:\Program Files\CenterTools\DriveLock Enterprise Service\DesRestarter.exe"

- **FESFDS**

  Function: OSR service
  Executable path: "C:\Program Files\CenterTools\DriveLock\FESF\FesfDs.exe"

- **FESFPolicy**

  Function: OSR service
  Executable path: "C:\Program Files\CenterTools\DriveLock\FESF\FESFPolicy.exe"

Microsoft Defender for Endpoint and encrypted network folders

- On clients with **Microsoft Defender for Endpoint** installed, copying data to an encrypted network folder (File Protection: New Format, Automatic Mode) may, under certain circumstances, trigger the blue screen error (BSOD) **MUP_BUGCHECK_NO_FILECONTEXT** caused by **MsSense.exe**.
  To prevent a BSOD, appropriate **EDR exclusions** should be configured in Microsoft Defender for Endpoint for encrypted network folders so that the MsSense.exe process does not scan these folders. The configuration can be found under **Settings > Endpoints > Rules > EDR Exclusions** in Microsoft Defender for Endpoint. (References EI-2684, EI-3167)

Windows 10 clients with Kaspersky Endpoint Security 10.3.0.6294

- Using File Protection in the New Format (PFE) together with Kaspersky Endpoint Security on the same system may, depending on the antivirus software configuration, result in a blue screen error (BSOD). (Reference EI-2524)

1.3.13 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 unlocking, for as long as the device is connected

1.3.14 Thin Clients

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

- Security Awareness cannot be used on IGEL clients.

1.4 Recommended configuration

1.4.1 Security settings for the DriveLock Agent

For additional security when operating DriveLock Agents, we recommend enabling both of the following options together.

Configuration: DOC -> Settings -> Installation -> Security settings

- **Join token:**

  Only agents with a valid, tenant-specific join token are allowed to register. This prevents unauthorized installations.

- **Verify agent identity:**

  The DriveLock Enterprise Service validates the identity of each agent to ensure that reported data originates from the correct system.

Further information can be found in the **Security settings for agent installations** chapter in the DriveLock documentation at DriveLock Online Help.

1.4.2 Preferred centrally stored policies

When using DriveLock - especially for distributing configuration settings to secure the DriveLock Agent on client systems - we recommend deploying centrally stored policies.

In contrast to Group Policy Objects (GPOs), these provide enhanced security, greater flexibility in assignment, and do not rely on Active Directory. They can also be applied over the internet.

For further details see the chapter **Distribution of DriveLock configuration settings** in the DriveLock Online Help at DriveLock Online Help.

1.4.3 Using trusted certificates

For existing installations, verify that the certificates used for communication between the central DriveLock Enterprise Service (DES) and linked DES servers meet the trust requirements. Starting with version 26.2, certificate trust is enforced for this communication. This requirement also applies to DriveLock Enterprise Service Status.

Self-signed certificates are not recommended. However, you can continue to use them if they meet the required certificate specifications and are trusted on the systems involved.

For more information about certificate requirements and using self-signed certificates, see Certificate validation for communication between DES servers.

Communication between DriveLock Agents and the DES is not affected by this change.

1.4.4 License management in the DOC

We recommend managing DriveLock licenses in the DriveLock Operations Center (DOC) rather than through DMC-managed policies.

When importing a license key through the DMC, the license may appear in the DOC but may not be fully included in DOC-managed policies. If the DriveLock Enterprise Service (DES) is offline, the agents will not receive a license through the policy in this case.

1.5 End-of-life information

DriveLock will notify you by newsletter well in advance of the end of support and maintenance for a specific DriveLock version. For more information, see also version-specific deprecations.

The following DriveLock versions are subject to the corresponding End-of-Life (EoL) dates:

Version	On-Premise support available through:	Cloud customer support:
All versions prior to 2024.2	EoL - not supported any more	-
2024.2	Development support [*1]: June 2026	-

Version	On-Premise support available through:	Cloud customer support:
	Product support *2: December 2026	
2025.1	Development support *1: December 2026 Product support *2: June 2027	-
2025.2	Development support *1: June 2027 Product support *2: December 2027	
2026.1	Development support *1: December 2027 Product support *2: June 2028	Support available
2026.2	current version	Support available

Note: We recommend that all customers upgrade to the latest DriveLock version.

Support lifecycle

Starting with version 2023.1, the support lifecycle for new DriveLock product releases is as follows: When a new product version is released, the End-of-Life (EoL) date for the **previous version** is announced.

*1 From the date the EoL is announced, DriveLock provides full support for that version for an additional 12 months. This includes critical maintenance updates, bug fixes, and fixes for critical issues.

After the full support period (12 months) ends, no further updates will be released for that version.

*2 DriveLock Product Support remains available for an additional six months to respond to phone, email, and self-service support requests.

This policy applies to all On-Premise versions starting with version 2023.1.

Upgrades:

Customers using earlier product versions with a valid maintenance agreement can upgrade their environment to the latest product version.

1.5.1 Version-specific deprecations

In addition to our current DriveLock End-Of-Life information, we would like to draw your attention to version-specific deprecations.

Feature deprecations:

- Due to the upcoming end of life (EoL) of Windows Server 2016 in January 2027, the operating system will no longer be supported starting with version 2026.2.
- The fixed assignment of centrally stored policies (CSPs) to DriveLock agents is deprecated.
- The use of application templates in the DMC is deprecated.
- Support for the legacy encryption format used by File Protection will be removed in one of the upcoming releases.
- The Security Awareness content currently provided by DriveLock will be discontinued on December 31, 2026. For future awareness training, Human Risk & Training with AwareGo-based training content can be used.

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

The 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 11 LTSC	All LTSC versions until the end of their respective extended support period
Windows 10	As of 20H2, only Pro / Enterprise editions
Windows 10 LTSC	all LTSC versions until the end of their respective extended support period
Windows Server	2016/2019/2022/2025 (Standard or Datacenter) with Desktop Experience
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	Debian 13, Fedora 44, IGEL OS 12.8, AlmaLinux/Red Hat Enterprise Linux 10, SUSE 16, Ubuntu 26.04 LTS, or later versions.
macOS	Starting with macOS 14 Sonoma with Intel (x86_64) or Apple Silicon (arm64) architectures

- The Windows DriveLock Agent supports x86-based systems (32-bit and 64-bit) as well as Windows 11 on Arm64-based systems. A 64-bit architecture is recommended for x86-based systems. Windows Server is supported on 64-bit systems only. The available functionality depends on the operating system and architecture.
- The Agent Installer requires Microsoft .NET Framework 4 (Client Profile), which is already included with current Windows operating systems. On Windows 7, it must be installed manually. (Reference: EI-2869)

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 of functions: ✓

Reduced range of functions: ◒

No support:✕

Feature	Operating system / functions				
	Windows 10 / 11	Windows Server	Windows 11 Arm64 (*1)	Linux	macOS
Drive Control	✓	✓	✓	◒	◒
Device Control	✓	✓	✓	◒	✕
Application Control	✓	✓	✓	◒	✕
Application Behavior Control	✓	✓	✓	✕	✕
Container encryption (Encryption 2-Go)	✓	✓	✕	◒	◒
BitLocker To Go	✓	✓	✕	✕	✕
BitLocker	✓	✓	✕	✕	✕

Feature	Operating system / functions				
Management					
Security Awareness Multimedia campaigns	✓	✓	✕	✕	✕
Defender Management	✓	✓	✓	✕	✕
Vulnerability Management	✓	✓	✕	✕	✕
Security Configuration Management	✓	✓	✕	✕	✕
Disk encryption (Disk Protection)	✓(*)	✕	✕	✕	✕
File encryption (File Protection)	✓	✓	✕	✕	✕

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

(*1): On Windows 11 running on Arm64-based systems, inventory management, firewall management, and local users and groups are also supported.

Further information on system requirements for different DriveLock modules:

- **Security Awareness:** Please note that as of version 2022.1, 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.
- **File Protection:** Starting with version 2024.1, the latest Microsoft Visual C++ Redistributable v14 is required. Please follow this .link.
- **DriveLock Pre-Boot Authentication (PBA)**: 40 MB of free disk space in the EFI system partition (ESP) is required for installation.

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
       Further information can be found under 'Update process' and 'Update catalog'.
       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**
   - Drive control:
     - File filters with restrictions
     - No unlocking for drives already encrypted with Encryption 2-Go
     - Self-service with restrictions
   - Device control is not supported
   - Encryption 2-Go:
     - For macOS, the Mobile Encryption Application (MEA) is available as before for decrypting external USB drives.
     - The macOS agent can automatically encrypt drives with an Encryption 2-Go container, but the full functionality for Windows is not yet available.

   For more information about the macOS agent, please refer to the "macOS" section in the DriveLock Online Documentation.

4. **Restrictions for Linux**
   - Drive control:
     - Starting with version 2025.2, file filters are supported in drive rules. However, not all options available on Windows are supported yet.
   - 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.

   For more information on the Linux client and the limitations of its functionality, please refer to the Linux topics in the DriveLock online documentation.

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 2026.2 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 (DES)

> 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 10.0 Runtime (Microsoft Download Link)
- ASP.NET 10.0 Core Runtime (Microsoft Download Link)
- .NET Desktop Runtime 10.0 (Microsoft Download Link)

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.

Warning: If you are updating from version 2021.2 (or earlier), please update to version 2024.2 first, and then update to a newer version.

Required DriveLock Services ports:

Port	Usage
1883; 3004; 4370; 5370; 6369; 3003; 4567; 4766; 18083; 18084	These local ports must not be used by other server services. They are only used internally and do not have to be open externally.
8883	The agents connect to the DES on this port so that they can be accessed via remote agent control. The DES installation program automatically enables the clearance in the local firewall of the computer.
4568	This port is mainly used for the DriveLock Operations Center (DOC).
6066; 6067	These ports are used to transfer management and status information from the agents.

Supported platforms:

- Windows Server 2016/2019/2022/2025 (Standard or Datacenter) with Desktop Experience

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

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

Supported databases:

- Microsoft SQL Server 2017 or later is required to run DriveLock. The database must have a compatibility level of 140 or higher. References: EI-3074; EI-3204; EI-3188
- 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.

3 Security Bulletins

You can now find a comprehensive list of our current Security Bulletins at DriveLock Online Help.



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.

© 2026 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.

