

DriveLock Release Notes

Release Notes 2026.1 Patch 1

DriveLock SE 2026



Table of Contents

1 DRIVELOCK RELEASE NOTES 2026.1 PATCH 1 4

1.1 Patch version 2026.1 Patch 1 5

1.1.1 Improvements and changes 5

1.1.2 Bug fixes 5

1.2 Major version 2026.1 9

1.2.1 New features, improvements and changes 9

1.2.2 Bug fixes 16

1.3 Known issues and notes 24

1.3.1 BitLocker Management 24

1.3.2 BitLocker To Go 26

1.3.3 Container encryption (Encryption 2-Go) 26

1.3.4 Device Control 26

1.3.5 Disk encryption (Disk Protection) 29

1.3.6 DriveLock Enterprise Service (DES) 32

1.3.7 DriveLock inventory 32

1.3.8 DriveLock Operations Center (DOC) 32

1.3.9 DriveLock Pre-Boot Authentication 34

1.3.10 File encryption (File Protection) 36

1.3.11 macOS Agent 37

1.3.12 Self-service 37

1.3.13 Thin Clients 37

1.4 Notes on antivirus software 38

1.5 Recommended configuration 39

1.5.1 Security settings for the DriveLock Agent 40

1.5.2 Preferred centrally stored policies 40

1.5.3 Use of Trusted Certificates 41

1.6 End-of-Life (EoL) information 41
1.6.1 Version-specific deprecations 43
2 SYSTEM REQUIREMENTS FOR OPERATING DRIVELOCK 44
2.1 DriveLock Agent 44
2.2 DriveLock Management Console 51
2.3 DriveLock Enterprise Service (DES) 51
2.4 DriveLock Operations Center (DOC) 53
3 SECURITY BULLETINS 54
COPYRIGHT 55

1 DriveLock Release Notes 2026.1 Patch 1

Build: 26.1.3.16176

Date: 2026-08-17

The DriveLock Release Notes contain important information about changes and bug fixes in this patch version: 2026.1 Patch 1. Here you will also find information about new features, changes, and bug fixes in the major release, as well as an overview of the system requirements for using DriveLock and our end-of-life announcements.

Please find a detailed description of the new features, improvements and changes in 2026.1 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 Patch version 2026.1 Patch 1

1.1.1 Improvements and changes

Below is a list of improvements and changes included in this version 2026.1 Patch 1.

DriveLock Enterprise Service (DES)

- Self-signed certificates are no longer supported for email delivery. The mail server certificate must be trusted by Windows.
- DES now supports SQL logins for the database connection. This allows DES to connect to SQL Server instances that are outside the Active Directory domain.
- 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-3294)

Linux Agents

- Linux Agents now also support Application Control and file filtering on NTFS3 file systems.

macOS Agents

- Container Encryption (Encryption 2-Go) on macOS now supports the Logged-on Users feature.

1.1.2 Bug fixes

DriveLock 2026.1 Patch 1 is a patch version.

This chapter contains information about bugs that have been fixed in DriveLock Patch version 2026.1 Patch 1. Our External Issues (EI) numbers, if available, serve as a reference.

Reference	Application Control (AC)
EI-3299	Fixed an issue where Application Control was unable to calculate executable file hashes on network shares with certain permission configurations.

	BitLocker Management
	Fixed an issue where the "Always use down-level logon names during Single Sign-On" option could not be enabled.
EI-3300	Fixed an issue where BitLocker key recovery could not be performed through the DOC.

Reference	DriveLock Container Encryption (Encryption 2-Go)
	Fixed an issue with FIPS-compliant container encryption. Creating new containers and re-encrypting USB drives now works correctly with the "FIPS encryption only (compatible with 25.2, Linux/macOS)" setting.
	Fixed an issue affecting administrator passwords in Container Encryption policies.

	DriveLock File Encryption (File Protection)
	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	DriveLock Management Console
	Fixed an issue where User Behavior Rules were not displayed in the RSOP view for agents using DOC-managed policies.

	DriveLock Operations Center (DOC)
	Fixed an issue where incorrect permissions were required to query groups in the DOC Object Picker. Group Management read permissions are now required to query groups.
	Fixed an issue where the "Temporary unlocks" tab was displayed to users without the required permissions.
	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-3302	Custom notification messages for drive rules and application collection rules are now displayed correctly on the agent.
EI-3310	Fixed an issue where the "Temporary unlocks" and "Unlock requests" tabs in the DOC were displayed only when both an Application Control and a Device Control license were active.

	macOS Agent
	Fixed an issue where the agent status was displayed incorrectly on macOS clients in domain environments.
	Fixed an issue where an incorrect domain name was stored and displayed for local macOS users.
	Fixed an issue where the Operating System Language property was not displayed in the computer inventory of the DriveLock Oper-

	macOS Agent
	ations Center (DOC).

1.2 Major version 2026.1

1.2.1 New features, improvements and changes

Below you will find a list of the new features, improvements and changes contained in version 2026.1.

This release introduces improvements that further enhance the security and stability of the application. Through targeted optimizations and refinements of existing security mechanisms, the new version provides even stronger protection against potential risks. In addition, measures have been implemented to make the product more robust and performant, ensuring a smoother and more reliable user experience overall.

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

- The creation of Application Control rules in advanced mode has been optimized in the DOC. Instead of creating multiple separate rules, the DOC now creates a single rule with nested filters.
- Unlock requests can now also be used for executable files. This allows users to request temporary access to executable files blocked by Application Control.
- Application collections can now be created and edited in the DriveLock Operations Center (DOC).
- User behavior rules are now available in the DriveLock Operations Center (DOC). These rules allow you to define which actions users are permitted to perform with applications or scripts.

- Application Control now supports ignoring process behavior. For selected applications, DLL loads, file access, or registry access can be excluded from monitoring, evaluation, and learning. This feature cannot be used in combination with Trust/Learn mode. (Reference EI-3094)
- Application Control now includes the new setting 'Avoid file access conflicts'. When enabled, Application Control delays competing file access requests from other processes to help prevent file access conflicts. (Reference EI-3115)

Awareness

- Two new dashboard widgets are now available for Awareness campaigns. These widgets provide an overview of the status and results of your own campaigns. (Reference EI-2953)
- Human Risk & Training now provides integration with the AwareGo platform for security assessments and security awareness training.

Container encryption

- The return codes of DLCrypt.exe have been revised to provide a clearer distinction between successful and failed operations.
- User selection rules for enforced encryption can now be configured directly in policies managed through the DOC.
- ⚠ FIPS-compliant encryption has been revised. AES-XTS-256 is now supported as an additional encryption method. Please refer to the related Known Issue for additional information.

File encryption (File Protection)

- ⚠ The default behavior for password complexity in encrypted folders has changed. By default, the settings configured under Password Requirements are now applied. This change also affects container encryption.

Defender Management

- The DOC and the API now support starting Microsoft Defender Offline scans. User notifications and postponement options can be configured when triggering a scan.

Device Control (DC)

- ⚠ Behavior change: COM and LPT ports are now managed only if corresponding settings are configured in the MMC. (Reference EI-3129)
- Container file inspection now supports Microsoft Office and PDF documents. As part of this enhancement, the previous term Archives has been renamed to Container Files.

- ⚠ Behavior change: MTP devices and media players are now assigned to the Smartphones device class in both the DOC and MMC. As a result, unlocking such devices now requires permission to unlock smartphones. Permission to unlock devices alone is no longer sufficient.
- Access attempts to MTP devices blocked by Windows services or other processes running in Session 0 are no longer reported when the required permissions are missing. This change affects reporting only. (Reference: EI-3097)
- A drive type can now be defined for individual drive entries in drive rules within the DOC. This allows rules that apply to multiple drives from the same manufacturer to be restricted to specific drive types, such as CD/DVD drives or USB drives.
- Settings that determine whether drive rules apply to removable media, hard drives, and CD/DVD drives can now also be configured in the DOC. These settings can be configured separately for each drive type within a rule.
- Drive rules in the DOC can now be configured to apply only to specific logged-on users or user groups.
  Please note that on systems with multiple users logged on simultaneously, such as terminal servers, behavior may differ from the expected rule application.
- Device handling for allowed and blocked devices on Windows has been improved. Device states are now detected more reliably, reducing unnecessary device restarts.
- Blocking events caused by file filters and quota restrictions are now logged as dedicated events.
- To prevent data loss, blocked archives are now first copied to the user's temporary folder (subfolder DLDeleted) and analyzed there before being moved to the target drive where file filtering is active.
- Archives copied or moved to monitored locations are now inspected before being written to the destination. This prevents unchecked archives from being left behind on removable media.

DriveLock Agent

- Starting with version 26.1, a custom banner (DLUserDlgBanner.png) can be displayed in the unlock request dialog.
- Administrators can now provide an additional menu item in the DriveLock Agent context menu that allows users to temporarily disable notifications.

DriveLock Enterprise Service (DES)

- The Visual C++ runtime libraries have been updated. A server restart is required after upgrading to version 26.1 for the changes to take full effect. (Reference EI-3071)
- Sending events to a syslog service has been optimized for improved performance. In addition, it is now possible to configure how events are separated within the data stream. (Reference EI-3232)
- Security mechanisms for cloud connectivity tests in On-Premises environments have been improved.
- Policy processing in On-Premises installations has been improved to further enhance security. Managed Cloud environments are not affected.
- The protection of security-relevant information in logs has been further improved for On-Premises installations.
- Validation of permissions for administrative functions has been improved.
- Custom fields can now be defined for the 'CVE List' schema extension.
- Custom fields can now be defined for executable files through schema extensions.
- The handling of cloned computer renaming has been improved when join tokens or identity tokens are in use. In addition, master image processing has been revised to reduce renaming-related issues.
- A separate event is now available for deleting computers, making it easier to track these processes. (Reference EI-3100)
- In the Server Setup Wizard, you can now continue with the installation even if the required database compatibility level cannot be verified.

DriveLock Unlocks

- ⚠ The transmission format for offline unlocks has been revised and improved. In particular, the time window for entering response codes has been limited to 60 minutes.
- Offline unlocks can now also be configured in policies managed through the DOC. No additional password or certificate settings are required for this configuration.
- The Unlocks view in the DOC has been enhanced. Administrators can now centrally view all unlocks as well as the associated events and objects for a selected unlock.
- ⚠ The configuration of unlock requests has been extended. Unlock requests are now configured at the drive type and device class level and are disabled by default. Users can only create unlock requests for drive types and device classes that have been

explicitly configured to allow unlock requests. In addition, the user experience for unlocks and unlock requests has been improved.

- Temporary unlocks can now be tracked and analyzed in detail within the DOC.

DriveLock Management Console (DMC)

- The DriveLock Management Console has been enhanced to allow Microsoft Entra ID users to be selected directly. (Reference EI-3161)

DriveLock Operations Center (DOC)

- User notifications can now be configured and customized directly in the DriveLock Operations Center in multiple languages. In addition to standard messages, custom notification texts can be created and managed. Custom notifications are enabled by default.
- The User Principal Name (UPN) is now displayed for members of Microsoft Entra ID groups.
- Custom computer properties can now be populated using agent properties.
- When adding a drive or device to a rule (for example, from an event or an unlock request), multiple rules can now be selected at the same time.
- For security reasons, the agent identity is no longer displayed in plain text. Instead, the 'Agent Identity' column indicates whether an identity has been reported to the server.
- File type definitions can now also be created, edited, and imported in the DriveLock Operations Center (DOC). In addition, creating custom file type definitions has been simplified by allowing file contents to be analyzed and compared directly.
- The dialog for adding widgets has been redesigned. A new navigation system and additional filters make it easier to find and add widgets. Widgets can now also be added by double-clicking without closing the dialog.
- In the Inventory menu, an overview of all agent actions is now available in addition to the computer list, allowing you to monitor their status in one place.
- When creating rules, you can now select an existing or new folder directly as the storage location. This makes it easier to organize rules from the moment they are created.
- Additional agent settings previously available only in the policy editor of the DriveLock Management Console are now also available in the DOC.
- Encryption features in the DriveLock Operations Center have been consolidated into a central Encryption area. Administrators can now manage BitLocker Management,

BitLocker To Go, Full Disk Encryption, Container Encryption, and File Protection through a unified navigation structure.

DriveLock Pre-Boot Authentication (PBA)

- Drivelock now supports Microsoft UEFI CA 2023 signed bootloaders. If the Microsoft UEFI CA certificate is updated, DriveLock will automatically update the PBA accordingly. (Reference EI-2983)

DriveLock policies

- Policies and policy content can now be imported and exported in the DOC. Planned changes are displayed before import. In addition, the DOC detects missing DriveLock groups and can create them automatically if required.

Linux Agent

- IGEL OS clients now report the correct user name after an Active Directory login.
- Self-service rules are now also supported for Linux agents. Users with the appropriate permissions can initiate self-service unlocks directly through the Linux agent's unlock interface.
- Support for temporary unlocks on Linux agents has been expanded. Individual drives, individual devices, and custom device classes can now be unlocked. In addition, multiple active unlocks are now supported simultaneously.
- When a drive is completely blocked on Linux, the new event 787 is now generated instead of the previously used event 111.
- Local Linux users are now created as objects on the server. They are displayed in the DOC and can be used in rules. (Reference EI-3228)
- The Linux agent now notifies users when a temporary unlock starts, is about to expire, and has expired.

macOS Agent

- The DOC now includes instructions for deploying the macOS agent via MDM systems such as Microsoft Intune or JAMF.
- Starting with version 26.1, Container Encryption on macOS supports user selection rules for enforced encryption.
- File filters in Drive Control are now supported on macOS. User/process exclusions, hash-based file exclusions, and shadow copies are not currently supported on macOS.
- The 'Logged-On Users' feature for drive rules is now supported on macOS.

- Drive Control on macOS now supports user- and group-based rules, including the use of Active Directory users and groups.
- The agent status dialog has been standardized across macOS and Linux.
- Drive Control on macOS now supports self-service unlocks. Note that he option "End unlock when the current user logs off" for self-service drive unlocks is currently not supported on macOS.
- The user interface for drive unlock requests on macOS has been aligned with the cross-platform user experience. Offline unlocks are currently not supported on macOS.
- The startup time of the macOS agent has been optimized. (Reference EI-3255)

Roles and permissions

- Permissions assigned to the Administrator role for infrastructure and server settings have been revised.

1.2.2 Bug fixes

DriveLock 2026.1 is a major version.

This chapter contains information on errors that have been fixed with DriveLock version 2026.1. Our External Issues (EI) numbers, if available, serve as a reference.

Reference	Application Control (AC)
EI-3155	Fixed an issue where subsequent changes to nested filters in AC rules were lost when saving the parent rule.

	Awareness
EI-3181	Fixed an issue affecting the display of awareness content packages.

	BitLocker Management (BLM)
EI-3112	Fixed an issue where encryption did not start or the password was not changed after entering the BitLocker password.
EI-3043	Fixed an issue affecting BitLocker recovery via the key ID in the DOC, where it was not possible to enter a password for certificate access.
	In some cases, event 658 (BitLocker encryption suspended) was reported while decrypting BitLocker-encrypted partitions.
EI-3035	Fixed an issue that prevented BitLocker passwords from being reset through the DOC.

	BitLocker Management (BLM)
EI-3201	Fixed an issue that prevented BitLocker recovery certificate files from being used in the DOC.
	A warning message is now displayed when a password change fails because installation media is present.
	Fixed an issue where the option to use a dictionary remained enabled even when password requirements were disabled.

	Device Control (DC)
	Fixed an issue where quotas did not work on network shares.
	Fixed an issue introduced with the driver caching implementation in version 25.1, where content inspection events were generated only for the first process accessing a file. Event generation is now process-specific, ensuring that blocked and allowed access is reported correctly while preserving the existing content inspection caching behavior.
EI-3122	When using a Defender scan in a drive rule, a blocked drive was incorrectly unlocked after a successful scan. This issue has been fixed.
	If the option to display the usage policy is not enabled for a temporary unlock, the usage policy of the associated drive rule is now correctly disabled.
	Fixed an issue where self-service unlock of a remote computer did not work when an explicit user account was used.

	DriveLock Agent
EI-3072; EI-3071	The Visual C++ runtime libraries included in the DriveLock Agent Installer have been updated. This resolves an intermittent agent installation issue that could result in error code 1603.
	Fixed an issue where temporary unlocks did not work correctly when the option "End unlock when the user logs off" was enabled.
EI-3051	Fixed an issue where license validation could, in rare cases, cause the DriveLock Agent to crash during startup.

	DriveLock Database
EI-3073	Fixed an issue that could occur during the installation of a new database when querying existing database user roles.

Reference	DriveLock Enterprise Service (DES)
EI-3119	Fixed an issue where event 787 (Drive blocked) was not displayed in the drive activity history.
	Improved validation of event data when agent identity verification is enabled, ensuring that unauthorized events are correctly rejected.
EI-3085	Fixed an issue where offline unlocks did not work correctly when weak challenge/response codes were used.

Reference	DriveLock Enterprise Service (DES)
	Corrected agent identity verification to prevent unauthorized access under certain circumstances.
EI-3135	An error in the DLSetup.exe has been fixed, which caused the DES installation to abort under certain circumstances.
	DriveLock On-Premises: Fixed a security issue that could allow unauthorized users to access DES configuration data through URL manipulation.
	A vulnerability has been fixed that allowed SQL code to be injected under certain circumstances.
	Added additional validation checks when accessing local resources on the DES to prevent unauthorized file access.
	Fixed a potential DES crash that could occur during log file initialization.
	Fixed an issue that could occur when updating API tokens.
EI-3157	Fixed an issue where forwarding certain Application Control events to a syslog service could fail.
	Fixed an issue affecting rules for event processing and forwarding.
EI-3274	Fixed an issue where the path to the DriveLock Enterprise Service executable was not correctly enclosed in quotation marks during installation.

Reference	DriveLock Management Console
EI-3070	Fixed an issue where an error message was displayed when accessing the Policy Assignments node while logged on to a tenant other than the root tenant.

Reference	DriveLock Operations Center (DOC)
EI-3086	Fixed an issue where offline unlocks of computers in the DOC were always granted for 135 minutes, regardless of the selected duration.
EI-3068	Fixed an issue where the recursive rule view in the DOC did not indicate the subfolder to which a rule belonged. An optional column displaying folder information is now available.
EI-3069	Fixed an issue where the Add to Rule action did not work correctly when rules were stored in policy subfolders. In such cases, only rules outside subfolders—or no rules at all—were displayed. The selection dialog now correctly reflects the folder hierarchy.
EI-3061	Fixed an issue that occurred when setting role properties.
	Fixed an issue where users without the role permission “Manage policy settings” were unable to add devices or drives to rules in the DOC.
	Fixed an issue where the “Date created” and “Date modified” columns remained empty when a large number of rules were

Reference	DriveLock Operations Center (DOC)
	displayed.
EI-3133	Fixed an issue where unlock requests could only be viewed by users with the Edit Additional Event Data permission.
	Fixed an issue where creating an application rule for Linux in the DOC did not perform any action.
EI-3143	Fixed an issue where filtering by the Name column was not possible in the group membership definitions list.
EI-3156	Fixed an issue where the serial number was not retained for certain events when adding a device to a rule or creating a new rule.
	Fixed an issue where deleting old policy versions was not always possible for policies with a very large number of versions.
EI-3110	Fixed an issue where the Last Event Timestamp column could appear empty.
EI-3095	Fixed an issue in the DOC object picker where domains were not displayed correctly.
EI-3093	Fixed an issue in the DOC object picker that could occur for users with limited permissions.
EI-3226	Fixed a display issue in the DOC syslog configuration where the status toggle was not displayed correctly.

Reference	DriveLock Pre-Boot Authentication
EI-3087	Fixed an issue where automatic logon to the network PBA could fail because the required users were no longer configured.
	Fixed an issue where the DriveLock PBA installation could fail when a manual restart was configured in the policy.
EI-3096	Fixed an issue where the number of restarts without PBA logon was incorrectly interpreted by the DriveLock Agent and displayed incorrectly in the DOC.
EI-3162	Fixed an issue where, after automatic logon to the network PBA and subsequent logon to Windows, automatic logon using the machine account could still occur.

Reference	Encryption 2-Go
EI-3125	Fixed an issue where creating a container on an exFAT-formatted USB drive took longer than expected.

Reference	File Protection (FFE)
	Fixed an issue where files copied from an encrypted network folder to an unencrypted network folder in Legacy Format mode were not decrypted.

Reference	File Protection (FFE)
	Fixed an issue where it was no longer possible to add users to centrally managed folders in the DOC.

	Inventory
EI-3121	Fixed an issue where users in the DOC were not assigned to the correct Active Directory structure and an incorrect value was displayed in the Domain column.

	Vulnerability Scan
EI-3145	Fixed an issue that occurred while synchronizing CVE entries.

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 to version 2025.2** (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

- If you're using Citrix Workspace, some computers might not start because Windows can't load the Drivelock driver`DLDevFlt.sys`. Apparently the "Citrix USB Monitor Driver" ctxusbmon.sys causes problems when unloading the `DLDevFlt.sys`.
  Recommended procedure: Open a support ticket with Citrix.
  Possible workarounds until Citrix has fixed the problem:

1. Uninstall Citrix Workspace.
2. Since the problem is caused by the fact that `DLDevFlt.sys` cannot be unloaded, you can try to work around it by only allowing `DLDevFlt.sys` to be unloaded with a delay or not at all. If the problem only exists in cases where devices are blocked by DriveLock, you can achieve this by switching on the "Disable blocked devices in Device Manager" setting. If DriveLock does not block any devices or this setting is not successful, you can use the "Report device removal" setting, as the driver remains loaded until the device is removed again (please refer to the notes in the description of this new feature). (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 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

1.3.13 Thin Clients

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

- Security Awareness cannot be used on IGEL clients.

1.4 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)

1.5 Recommended configuration

1.5.1 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.

1.5.2 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.

1.5.3 Use of Trusted Certificates

Starting with version 26.2, trusted certificates are required for communication between linked DES servers and the central DES. Self-signed certificates are no longer supported for this purpose. This change does not affect agent connections to the central DES.

1.6 End-of-Life (EoL) 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 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	Support available

Version	On-Premise support available through:	Cloud customer support:
2026.1	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.

1.6.1 Version-specific deprecations

In addition to our general End-of-Life information, this section highlights deprecations that are specific to this version.

Feature deprecations:

- 2026.1 is the last version that supports File Protection on 32-bit systems and on Windows 7.
- 2026.1 is the last version that supports the DriveLock Mobile Encryption Application (MEA) on 32-bit systems.
- 2026.1 is the latest version that supports SHA-224 as a hash algorithm.
- 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 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.
- 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	Linux	Mac OS
Drive Control	✓	✓	◒	◒
Device Control	✓	✓	◒	✕
Application Control	✓	✓	◒	✕
Application Behavior Control	✓	✓	◒	✕
Container encryption (Encryption 2-Go)	✓	✓	◒	◒
BitLocker To Go	✓	✓	✕	✕
BitLocker Management	✓	✓	✕	✕
Security Aware-	✓	✓	✕	✕

Feature	Operating system / functions			
ness 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.

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 2026.1 Patch 1 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.

