DriveLock Release Notes

Release Notes 2025.2

DriveLock SE 2025

Table of Contents

1 DriveLock Release Notes 2025.2

Build: 25.2.2.61370

Date: 2025-12-12

Warning: This release will initially be delivered for DriveLock Managed Services (Cloud). The on-premises version will follow at a later date.
Information in the release notes and accompanying documentation will therefore only apply to on-premises environments once the on-premises version has been released.

The DriveLock Release Notes contain important information about new features, changes and bug fixes in the main version 2025.2, 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 2025.2 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

Below you will find a list of the new features, improvements and changes contained in version 2025.2.

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 **What's new?** chapter 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)

- Added two new optional columns in the rule overview in the DOC: 'Date created' and 'Date modified'. These enable better traceability of the rule history and facilitate the maintenance of complex sets of rules.
- AC now uses the access rights of the evaluated process, e.g. when calculating hashes for network paths. (Reference: EI-2991)
- The option "Upload local whitelist to DriveLock Enterprise Service" is only displayed if it is activated in an existing policy.
- Extended process evaluation: The check now also applies to non-service-based processes and their child processes.
- ⚠ There is a new setting to control when signatures are accepted.
- AC rules now support multiple filters within a single rule. This allows more complex scenarios to be implemented more efficiently without the need for multiple rules.

- The command line support in the Application Behavior Control (ABC) has been extended:
  - Command line checks can also be carried out for rules with several target objects.
  - There is a new comparison type "matches" for the use of wildcards in addition to "contains".

BitLocker Management

- A new policy option allows the automatic suspension of BitLocker or DriveLock PBA logon during Windows system updates.
- New event when suspending and resuming BitLocker encryption.
- The dialog after encryption can now be suppressed for BitLocker/Disk Protection.
- Remote wipe now also supports system partitions encrypted with BitLocker PBA or BitLocker TPM only.
- You can now specify which TPM registers are set for BitLocker encryption. The only exception is PCR 11, which is always enabled.
- BitLocker recovery with key ID: When recovering BitLocker-encrypted drives via the key ID in the DOC, a password can now be entered for certificate access. (EI-3048)

Defender Management

- New option in the Defender dialog in the DMC: A Defender offline scan is now possible and can be triggered manually.
- The following rules have been added to the list of predefined rules: (Reference EI-2940)
  - Block rebooting machine in Safe Mode (block rebooting of the computer in Safe Mode)
  - Block use of copied or impersonated system tools (Block use of copied or impersonated system tools)

Device Control (DC)

- Extended functionality: Temporary unlock now supports custom device classes, targeted unlocks for individual devices, and multiple simultaneous unlocks. Unlock Request Wizard now supports temporary unlocks.
- Event 787 is now generated instead of event 111 when a drive is completely blocked.

- Drive and device control can now be activated separately in the DOC. Important: As long as not all agents have been updated to version 25.2, both activation settings must remain identical.

Disk Protection

- The automatic suspension of the DriveLock PBA logon during Windows system updates is now also available for Disk Protection.

DriveLock Agent

- The DriveLock Agent has been improved with regard to the handling of permissions.
- Several enhancements have been made to improve overall product security.
- Support for LDAPS on DriveLock Agent and DMC DriveLock Agent and the MMC now support LDAPS by default and use port 636 if the system requirements are met. Otherwise, LDAP queries will continue to use port 389, with SSL encryption applied where possible. System requirements: A valid certificate must be installed on the domain controller, and port 636 must be open.

DriveLock Enterprise Service (DES)

- Server Setup Wizard: If the database compatibility level cannot be checked, there is now an option to continue the installation anyway.
- A new option is now available in the Server Setup Wizard to automatically perform database maintenance after a database update. This option is activated by default and helps to avoid potential performance problems that can arise due to a lack of maintenance.
- Improved event data validation with agent identity verification enabled: Incoming event data is now more reliably validated and filtered when agent identity verification is active.
- New output of the syslog in JSON format: The forwarding of events via syslog is now also possible in JSON format. This structured format facilitates processing by SIEM systems.
- The protection of agent identity has been further improved to reliably prevent unauthorized access - e.g. through man-in-the-middle attacks.
- Improved security when uploading trace data: Only ZIP archives can now be uploaded via the upload interface for trace data.
- The DES now prefers Secure LDAP via port 389 for LDAP access.

- Security improvements have been implemented in the areas of tenant name validation and system information access control.
- Deprecated or unused methods have been removed from the DES SOAP interfaces.

DriveLock Operations Center (DOC)

- Various improvements to the DriveLock Operations Center (DOC) user interface:
  - The view settings of individual or all workspaces can now be exported and imported.
  - All view-related settings have been consolidated under a new menu item (Configure views). The associated dialogs have been simplified for improved usability.
  - The header of the DOC now always shows the logged-in user and the current tenant.
  - Assignments can now be added directly from the policy view via the toolbar or context menu.
  - Improved object selection in the DOC: Improved handling of large lists in the object selection dialog by adding paging and enhanced filtering options.
  - Context menus for linked objects: Right-clicking on linked objects in list views now displays the appropriate context menu (e.g., computer menu).
  - Context menus for grouped items: Items representing a specific object (e.g., computer or user name) now show the full context menu for that object.
  - The column selection dialog has been redesigned to offer a clearer structure, with categories and improved search and filtering options.
  - External links can now be executed via an object's context menu and can also be imported and exported.
  - Reports now also support the A3 paper format and printing in landscape format.
  - In the views for policies, policy versions and policy assignments, a column can now optionally be displayed that shows the number of computers from which a policy has been reported.
  - Added a widget to the policy detail view that displays which computers received the selected policy.
  - Groups can now be created and filled directly from the computer or user view.

    - Temporary unlocks can now be performed directly in the DriveLock Operations Center (DOC), eliminating the need to use the DMC interface. This also applies when responding to unlock requests.
- Improvements to widgets and dashboards:
    - Added new widgets for custom Awareness Campaigns to the user dashboard.
    - Introduced a redesigned widget selection dialog with categories, filters, search, and preview.
    - Regular dashboard widgets can now also be used in detail views.
    - Widgets can now be created based on additional, shared schemas.
    - Drilldown widgets and expert mode queries have been reworked and are now easier to configure.
    - The detail view configuration has been simplified and now supports context-aware widgets such as computer, user, or device widgets.
    - Improved "Arrange my dashboards" dialog: Drag-and-drop is now clearly left-to-right, and a text search has been added.

DriveLock Environment

- Schema extensions using custom properties: Added support for creating, reading, updating, and deleting custom properties (CRUD) for users, computers, drives, devices, and software via the DOC and the scripting API.
- Schema extensions can also be imported and exported
- Newly defined properties can now also be used as filter criteria in dynamic computer groups.

Encryption

- Configuration of all three encryption types – container-based encryption, File Protection, and BitLocker To Go – is now fully supported in the DOC. This includes all available options for settings, recovery rules, and enforced encryption.
- The behavior of the general encryption settings in the DOC has been revised. Configuration now differs slightly from the DMC. Note: If older agent versions are still in use, care must be taken, as not all settings may be fully supported.

Linux Agent

- IgelOS: The agent now reports the correct user name, even if the user is not logged on to the domain.

- If a temporary unlock request is denied by an administrator, Linux endpoints can now display a custom message explaining the reason for the denial. This provides immediate feedback to users about their request.
- Linux clients now support configuring access permissions with the “Block with exceptions” option. This allows blocking access to drives or devices while granting access to specific users or groups – including AD users if AD integration is enabled.
- DriveLock Agents on Linux now correctly recognize AD users when the system is joined using Samba Winbind, enabling accurate user-based access control for AD environments.
- The DriveLock Agent now supports file filter configuration within drive rules on Linux. This enables more detailed control over access to individual files without blocking the entire device.

Licensing

- Selected modules can now be activated directly in the DriveLock Operations Center (DOC), eliminating the need to switch to the DriveLock Management Console (DMC).

macOS Agent

- Drive control now supports user- and group-based rules — including Active Directory users and groups.

Self-service

- Self-service rules: Default unlock duration can now be configured: In addition to defining a maximum unlock duration, administrators can now configure a default duration that is preselected in the self-service dialog. Users can still adjust this value as needed.

1.2 Bug fixes

DriveLock 2025.2 is a major version.

This chapter contains information on errors that have been fixed with DriveLock version 2025.2. Our External Issues (EI) numbers, if available, serve as a reference.

Warning: Please note that some issues may cause a change in product behavior when you install the update. Before updating, make sure to check your settings to see if your existing environment is affected. The issues are labeled with the following icon ⚠

Reference	Application Control (AC)
EI-3065	Application Behavior Control (ABC): Fixed a bug that caused certain ABC rules to trigger unexpected behavior in some programs.

	BitLocker Management (BLM)
	The 'Export certificate' task created incorrect file names when exporting encryption certificates from a BitLocker management policy.
	Fixed a bug where encryption was not paused for logged-on users, even though the corresponding option was enabled in the policy.
EI-2880	After temporarily deactivating a data partition encrypted with BitLocker, the PBA status was displayed as 'suspended' although the BitLocker PBA was still active.
	In some cases, the password input field for setting a new BitLocker password was automatically pre-assigned without

	BitLocker Management (BLM)
	prompting.
EI-3025	In rare cases, BitLocker encryption was canceled with the error "The system could not find the specified file".
EI-2969	Fixed a bug that occurred when accessing BitLocker recovery data on computers when the DOC account had the 'Encryption Officer' role but it was restricted to a DriveLock group.
	During the decryption of BitLocker-encrypted partitions, event 658 (BitLocker encryption suspended) was reported in some cases.
EI-3037	Fixed a bug that made it impossible to reset the BitLocker password via the DOC.
	During BitLocker To Go encryption of external drives, a Windows dialog with a progress bar was displayed in some cases, which could be used to perform further actions. The display of this dialog is now prevented.

	Device Control (DC)
	When creating device rules for some events (e.g. Event ID 120), it happened that the information from the event parameters (e.g. hardware ID) was not correctly transferred to the rule.
	In the DOC under Security Controls -> Drives -> Events, the display for event 120: Serial interface locked was missing.

	Device Control (DC)
	Fixed a blue screen when renaming to controlled USB data carriers (in the event of a name conflict with an existing file).
EI-2996	Fixed an issue that caused a system crash (Blue Screen) when moving files into or out of subfolders if a file with the same name already existed in the target directory.
	Renaming a permitted non-archive file to an archive file is now blocked as this is a content conflict.
EI-2954	The content check for NTFS Alternate Data Streams (ADS) has been corrected. Known ADS can now be checked via user-defined file type definitions in the format ':ADS name'. Without such a definition, ADS will not be blocked. Only the file name of the main data stream is relevant for extension blocking.
	Fixed a bug that caused certain .MP4 files to be incorrectly blocked even though this file type was allowed according to the configured file type definitions. The recognition of .MP4 files has been extended accordingly.
	Fixed a bug where Windows/AD groups used in DriveLock groups were not applied correctly in drive permissions.
EI-2998	For drive and device rules, the timestamp of the last event in the device list was sometimes displayed incorrectly or not at all - especially for rules with many entries.

	Disk Protection
	In some cases, the title bar of some encryption dialogs was not displayed correctly.
EI-3030	The status of partitions encrypted with Disk Protection was displayed as 'suspended' in the DOC, although encryption was active.

	DriveLock Agent
EI-2994	A blue screen could occur when files on drives controlled by DriveLock were renamed without a file extension and has been fixed.
EI-3057	Fixed an issue where the license check could occasionally cause a crash when starting the DriveLock Agent.
EI-2980	Fixed a bug that caused agents to display license warnings even though a valid license was available.

Reference	DriveLock Enterprise Service (DES)
	Fixed listing of recovery data when the option "only last entry per computer" was selected (MMC, FDE Recovery Wizard).
	Fixed a cross-site scripting (XSS) vulnerability that occurred during data export.
	The EntraID functionality in the server now uses the proxy con-

Reference	DriveLock Enterprise Service (DES)
	figured in the server settings (backend).
	When querying events via the API, not all properties were returned if the query parameter 'select' was empty.
	Fixed an issue that caused problems when renaming cloned computers with an active Join or Identity Token. In addition, the behavior when renaming master images has been optimized.

Reference	DriveLock Management Console
EI-2977	In the taskpad view for the global settings in the DMC, some tasks opened an incorrect configuration dialog.
EI-3028	Adding the serial number of a connected Android smartphone to a whitelist rule no longer worked - the serial number was not transferred.
	When resetting a policy version, the publication comment is now reliably removed and no longer incorrectly saved.

Reference	DriveLock Operations Center (DOC)
EI-2982	When exporting from rules, all contained drives or devices are now taken into account - not just the selected ones.
	Some events (524-529) were incorrectly moved from Drives ->

Reference	DriveLock Operations Center (DOC)
	Polling/Shadow Copies to Devices -> Polling/Shadow Copies.
	Various events were missing in the DOC under Encryption -> Events, which should have been visible there.
	After suspending BitLocker encryption for a certain period of time, the DOC no longer displayed when encryption would be reactivated.
EI-2998	Fixed a bug where the timestamp of the last use of drive rules was not displayed correctly in the DOC.
EI-3062	Fixed an issue that occurred when setting role properties.
EI-3024	Operating several linked DES servers no longer leads to MQTT connection problems.

Reference	DriveLock Pre-Boot Authentication
	After completing the re-encryption with the DriveLock PBA, the message that all drives were encrypted was not displayed.
	If a manual restart was specified in the policy, the installation of the DriveLock PBA could be faulty.

Reference	Encryption 2-Go
	When using a rule for forced encryption with configured free space on the target medium, the size of a new container was not calculated correctly.
EI-1966	Fixed a bug where the password recovery wizard for Encryption 2-Go containers was not started from the mount dialog of the Mobile Encryption Application (MEA).

Reference	File Protection (FFE)
	Fixed a bug that prevented the creation of a centrally managed encrypted folder via the agent user interface.
	In DOC, it was not possible to replace a certificate with another one for File Protection users if it had expired, for example. In addition, expired validity is now indicated by red lettering.

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 Device Control

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).

Quota / File filter templates

- On the Quota tab, the bytes written or read per time unit are counted, not the actual files. Therefore, the creation of new files with 0 bytes is not blocked.
- 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 filter for archive files

- 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-2651)
- Please note the following information:
  - Nonstandard application behavior may lead to unexpected results, e.g. 7zip opens the zip and shows sections of a forbidden exe in analysis mode
  - 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. (Reference DL-7643)

  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 earlier versions, an event indicating a deletion block was still generated, even though the file had already been deleted.
  Update: Since deleting a file classified as unwanted based on content inspection is not necessarily an error, content scanning and the related event generation are now skipped in such cases.

- 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).

1.3.4 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.

1.3.5 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).

1.3.6 DriveLock Operations Center (DOC)

Temporary unlock in the DOC currently requires additional permission

In version 25.2, the ability to temporarily unlock computers directly in the DOC was introduced. Currently, executing this action also requires the **Show tenant settings** permission to ensure the wizard functions properly.

This applies exclusively to the new temporary unlock feature available in the DOC as of version 25.2.

⚠ 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.

Widgets in the detail view

The new detail view functionality in version 2025.2 includes many new widgets that currently display incorrect information due to a lack of filtering. This will be fixed in the next version. This error does not occur with the built-in widgets.

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)

1.3.7 DriveLock Pre-Boot Authentication

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

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

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

1.3.8 File Protection

Microsoft OneDrive

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

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.

Windows 10 clients with Kaspersky Endpoint Security 10.3.0.6294

- Using File Protection in new format (PFE) and Kaspersky on the same system can lead to a blue screen error (BSOD), depending on which settings are used in the AV software. (Reference EI-2524)

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.

Copying data to a network folder encrypted with a new format

- The blue screen error (BSOD) MUP_BUGCHECK_NO_FILECONTEXT may occur when copying 20-40 MB to an encrypted network folder. (New format, automatic mode) (Reference EI-2684)

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.

1.3.9 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.

1.3.10 Self-service

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

1.3.11 Thin Clients

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

- Security Awareness cannot be used on IGEL clients.

1.4 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.

1.5 End Of Life Announcement

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

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

Version	On-premise customer support exists until:	Cloud customer support exists until:
All versions before 2024.1	EoL - not supported any more	EoL - not supported any more
2024.1	Development support *1: December 2025 Product support *2: June 2026	EoL - not supported any more
2024.2	Development support *1: June 2026 Product support *2: December 2026	Until the release of a version following 2025.1
2025.1	Development support *1: December 2026	Until the release of a version following 2025.2

	Product support *2: June 2027	
2025.2	current version	current version

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

Support lifecycle:

Since version 2023.1, the support lifecycle for new DriveLock product versions is as follows: once a new product version is released, we announce the End-Of-Life (EOL) of the **previous version**.

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

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

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

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

Upgrades:

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

End of life of features:

- With version 2025.2, the DLSetup.exe can no longer be started on 32-bit systems.
- With version 2025.2, the power management available in the DriveLock Management Console (DMC) is no longer supported.

Note: **TLS 1.2**: Please make sure that all operating systems running DriveLock support TLS 1.2. as of now.

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 10	As of 20H2, only Pro / Enterprise editions
Windows 10 LTSC	all LTSC versions until expiry of the respective Extended Support
Windows Server	2016, 2019, 2022, 2025
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 12, Fedora 40, IGEL OS 11.05, Red Hat Enterprise Linux 5, SUSE 15.4, Ubuntu 24.04, AlmaLinux OS 9.4 or newer versions The IgelOS 12.5 base system is required for the DriveLock IgelOS App 25.1 to function properly.
macOS	From version Ventura (version 13) with Intel (x86_64) and Apple Silicon (arm64) architectures

The Windows DriveLock Agent is basically available for AMD-/Intel X86-based systems (32-bit and 64-bit architecture). We recommend using a 64 bit system for the DriveLock Agent. Server operating systems are only supported under 64-bit. You will find the restrictions of the individual functionalities described below.

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

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

Complete range of functions: ✓

Reduced range of functions: ◒

No support:✕

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

Feature	Operating system / functions				
Vulnerability Management	✓	✓	✓	✕	✕
Security Configuration Management	✓	✓	✓	✕	✕
Disk Protection	✓(*)	✕	✕	✕	✕
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:** As of version 2024.1, the current Microsoft Visual C++ Redistributable 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**

- Device Control:
  - No unlocking for specific users or user groups
  - No file filter and auditing
  - No unlocking for drives already encrypted with Encryption 2-Go
  - No self-service functionality
- Encryption 2-Go:
  - For macOS, the Mobile Encryption Application (MEA) is available as before for decrypting external USB drives.
  - The macOS agent 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 topics in the DriveLock online documentation.

4. **Restrictions for Linux**
    - Device Control:
        - No unlocking for specific users or user groups
        - No file filter and auditing
        - No forced encryption
    - Application Control:
        - DriveLock Application Control requires Linux kernel version > 5 for use on Linux agents.
        - Application Control cannot be used together with IGEL OS.
        - None of the Application Behavior Control functions are available on Linux.
    - Encryption 2-Go:
        - Containers or encrypted USB drives cannot be created, only connected.

    For more information 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 2025.2 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 Framework 4.8 or higher is required for installation!
- .NET 8.0 Runtime(Microsoft Download Link)
- ASP.NET 8.0 Core Runtime(Microsoft Download Link)
- .NET Desktop Runtime 8.0(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 inform-

Port	Usage
	ation from the agents.

Supported platforms:

- Windows Server 2016 64-bit
- Windows Server 2019 64-bit
- Windows Server 2022 64-bit
- Windows Server 2025 64-bit

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

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

Supported databases:

- DriveLock version 2024.1 or higher requires at least SQL Server 2016 SP1 or newer. The database must have a compatibility level of 130 or higher.
- SQL Server Express 2016 or newer for installations with up to 200 clients and test installations
- The DES requires the **Microsoft SQL Server 2012 Native Client version 11.4.7001.0**. In case this component is not yet installed, this happens automatically before the DES is actually installed. If an older version is already installed, it will be updated automatically.

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

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

2.4 DriveLock Operations Center (DOC)

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

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

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

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

3 Security Bulletins

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

Copyright