DriveLock Release Notes

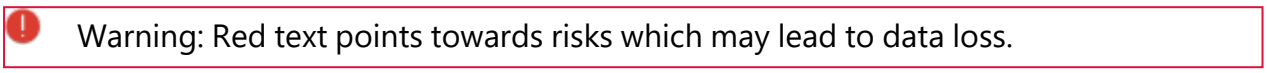
Release Notes 2023.1HF1

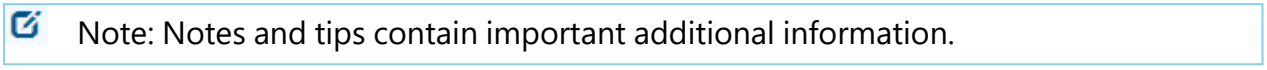
DriveLock SE 2023

Table of Contents

1 Document conventions

Throughout this documentation, the following conventions and symbols are used to highlight important aspects or visualize objects.





Menu items or names of **buttons use bold forma**tting.

Italic font represents fields or titles of referenced documents.

`System font` represents messages or commands typed at a command prompt.

A plus sign between two keyboard keys means that you must press those keys at the same time. For example, ALT+R means that you must hold down the ALT key while you press R. A comma between two or more keys means that you must press them consecutively. For example 'ALT, R, U' means that you must first press the Alt key, then the R key, and finally the U key.

2 Information on 2023.1 HF1

See the release notes for important information about bug fixes in the 2023.1 HF1 hotfix release and about new features, enhancements, and bug fixes in the 2023.1 major release. Also included are system requirements, known limitations and other important announcements.

The complete DriveLock documentation, as well as links to the release notes of past and still supported versions, can be found at DriveLock Online Help.

Note: Please note that some information in these release notes is only relevant for DriveLock On-Premise.

3 Version 2023.1

3.1 Hotfix version HF1 (Build 23.1.3)

3.1.1 Bug fixes 2023.1 HF1

DriveLock 2023.1 HF1 is a hotfix version.

This chapter contains information about issues that are fixed with DriveLock version 2023.1 HF1. Our External Issue numbers (EI) serve as references, where applicable.

Reference	Defender Management
EI-2514	If the "Save events with e-mail" option was enabled for DriveLock events 684 and 697, neither events were generated nor e-mails were sent for detected threats under some circumstances.

Reference	Device Control
EI-2513	If no connection to the AD controller was available, event processing could become very slow and cause timeouts when checking if files matched the file filter.

Reference	Disk Protection
EI-2491	Windows boot would hang when a Disk Protection decryption with network pre-boot enabled was interrupted by a reboot.

Reference	DriveLock Agent
EI-2506	After updating the agent, some composite devices were some-

Reference	DriveLock Agent
	times disabled depending on the device control configuration.

Reference	DriveLock Operations Center (DOC)
	The functionality to display the passwords of local users did not work if you did not enter a 'full name' in the policy for the users.
	When trying to create a drive rule from an event, the dialog boxes (Vendor ID, Product ID, Hardware ID, Serial Number) were not filled with the appropriate values from the given event.

Reference	DriveLock policies
	In some circumstances it was possible that the application/drive rules created in the DOC disappeared. This occurred when the default policy was published in the DMC and there was a | in the name or comment of a rule, for example.

Reference	Self-service groups
	During self-service unlock, the wizard for enforced encryption was displayed. This issue is now fixed.

3.2 Major version

3.2.1 What's new?

Improved DOC design and user interface

- The DriveLock Operations Center features a new structure and look & feel as well. Based on the DriveLock modules, the menu structure allows quick entry and reflects the Critical Security Controls (CSC), providing measures targeted at better protection against attacks. Tabs along the top provide a clear overview and forward-looking expandability.

Improved management of Security Awareness Campaigns

- It is now much easier to create, manage, and evaluate security awareness campaigns featuring clear objectives, content, start and end dates, and targeted recipients. An audit trail feature helps track campaign results and historical trends during security audits. With the appropriate role assigned, staff departments can manage campaigns independently from within the DOC and can roll out focused content to other departments by means of the new user groups.

Advanced features for BitLocker and BitLocker To Go

- DriveLock has made it even easier to take over and replace managed BitLocker environments. During re-provisioning, DriveLock takes over any existing data partitions. External media (e.g. USB flash drives) that are already encrypted with BitLocker To Go can now be taken over and managed by DriveLock without having to be re-encrypted. In addition, DriveLock is capable of reading blocked storage media and data partitions that are connected externally, even if there is no DriveLock Agent on them or the original assignment to an endpoint is unknown. All use cases meet the highest security standards.

Universal drive rules across all operating systems

- The DOC is now able to support all operating systems with just a single drive rule. DriveLock Agents on Windows, Linux and macOS now support the hardware ID as a drive criterion. It can now also be combined with serial number in drive collections. This leads to a faster centralized management for heterogeneous endpoints with only one drive configuration.

Advanced Bluetooth device management

- Improved Bluetooth device management lets administrators control Bluetooth devices as easily as they control other technologies. They can create rules, like blocking keyboards but allowing mice, controlling devices based on device type or

manufacturer, and managing Bluetooth classes and services. This makes configuration easier and eliminates complexity. It all adds up to an optimized Bluetooth device management solution in just a few steps.

Mac agent with proxy support

- The DriveLock macOS Agent now provides proxy support essential for deployment in enterprise environments, whether through automatic configuration via PAC/WPAD or manual configuration options. In addition, protocol-specific proxy support ensures compatibility and secure communication for HTTP(S), SOAP, and MQTT protocols, meeting the unique requirements of each protocol.

Cross-domain endpoint management

- Dynamic groups can now filter based on the computer's distinguished name (DN) and the DN of the groups the computer is a member of. This makes it easier to manage complex directory infrastructures when computers are accessible across their directory service's scope.

Secure password management for temporary local administrator accounts

- The Configuration Management module features managing local user accounts, including temporary local admin accounts that have automatically generated and secure passwords available for change on a daily basis. Now helpdesk users can view and supply end users with the current (daily) local admin password in the DOC. Same applies to the password history. For example, this is useful when a virtual machine is restored to a previous snapshot and the password in effect at that time is needed. To perform this task, the help desk needs a corresponding role and permissions in the DOC, while existing customers must first store a certificate in the DOC. This takes the capabilities beyond those of Microsoft LAPS (Local Administrator Password Solution).

Enforce complex password requirements for DOC accounts

- Cloud customers can now configure a password policy that meets their security requirements. Complex password rules can be enforced for DOC accounts that do not use single sign-on (SSO), plus they can prevent reuse of recent passwords.

Working with user groups

- Similar to creating computer groups, it is now also possible to configure static user groups. They are especially convenient for assigning and controlling how security awareness campaigns are executed. In addition, you can use them in policies in all user lists where you could previously use Azure AD groups.

Optimized Azure AD synchronization

- This only applies to cloud customers. Synchronization between DriveLock and Azure AD has been streamlined to only those groups relevant to the DriveLock environment while also speeding up the process.
- After the update, Azure AD synchronization will be disabled. In order to reactivate synchronization, you will need to select the groups you want to synchronize. Groups that have already been synchronized will remain in the DriveLock database, but will no longer be updated unless they are selected again.

E-mail notification for specific events

- The DriveLock platform now features an email notification channel. Critical events, such as virus detection, will be communicated. This allows for more effective monitoring and response to security incidents, while avoiding email inbox overload. The ability to integrate additional communication channels in the future provides additional value and flexibility for notification of important events.

Windows 7 Legacy Support

- As of version 2023.1, DriveLock supports Windows 7 endpoints only with a paid Legacy/Extended Support license. Organizations will be notified of this in the DOC.

Windows XP

- Starting with version 2023.1, Windows XP is no longer supported.

3.2.2 Improvements and changes

In addition to the new features, this version offers further improvements in the following areas:

Application Control

- A new setting leads to a significant improvement in performance because rules are now evaluated much faster. (Reference EI-2429)

Device Control

- The content check for Unicode text files (<FORMFEED> allow; <NUL> don't allow) has been improved. (Reference EI-2397)

DriveLock Agent

- macOS Agent: In the DOC in the Installations section, the macOS Agent can be easily installed via the command line with the appropriate parameters (Reference: EI-2366)
- The installation of DriveLock Agent via DLSetup.exe is no longer possible. The agent can be installed and updated via the command line with appropriate parameters. (Reference EI-2351)
- The DriveLock Agent (x64).msi supports a new parameter: REMOVEDATA. This parameter can be specified during uninstallation (REMOVEDATA=1), so that not only the program files but also all configuration data of the agent are deleted during uninstallation.
- **Agent Remote Control:**
  - It is now possible to disable both HTTP and HTTPS for remote control. (Reference: EI-2121)
  - Remote access to agents can now be secured using role-based access rights. Two new roles or permissions have been added to the DOC that determine whether agents can be accessed read-only or whether changes are also allowed.

DriveLock Enterprise Service (DES)

- If a user is to be added in the DOC from a domain to which the DES has no authorization, a password dialog is now displayed. This only affects the on-premise version of DriveLock. (Reference EI-2280)

DriveLock Operations Center (DOC)

- Audit events are now displayed in their own tab.

DriveLock Pre-Boot Authentication (PBA)

- For better error analysis, an event is now reported (event number 757) that the PBA could not be installed because the requirements for SecureBoot are not met. The reason is the missing Microsoft Corporation UEFI CA 2011 certificate.

Event Encryption

- As of version 2023.1, the ability to change or configure settings for client-side event encryption is removed. Events are basically no longer encrypted. The data masking function in the DOC completely replaces the previous pseudonymization by encryption.

Inventory

- A new event (ID 2710) is now triggered when a computer is selected by the server to perform an AD inventory. This only affects DriveLock Managed Services. (Reference EI-2289)

Licensing

- The Risk&Compliance (EDR) module has been incorporated into the Zero Trust platform. The "Evaluate event filters" and "Evaluate 3rd party events" options can now be activated or explicitly deactivated.
- The Native OS Security license has been renamed to Security Configuration Management. The functional scope remains unaffected and still includes firewall management and administration of local users and groups.

3.2.3 Bug fixes 2023.1

DriveLock 2023.1 is a major version.

This chapter contains information about issues that are fixed with DriveLock version 2023.1. Our External Issue numbers (EI) serve as references, where applicable.

	Application Control
EI-2381	Application Behavior Control did not recognize or blocked renaming and moving of files

	Operating system management
	If the Local users management mode setting in the Operating system management node under Local users and groups was set to Authoritative, users on the agent were not removed correctly, even if they were previously deleted in the policy.
EI-2466	Outgoing firewall connections were previously always logged as incoming connections. This issue is now fixed. DriveLock events 747 and 748 are now generated for outgoing connections.
EI-2438	If you create or update multiple local users at the same time, they will no longer all receive the same password.

	BitLocker Management
	The "DlFdeCmd.exe cryptstatus" command did not show the correct status for unencrypted drives when the Drivelock PBA for Bitlocker was installed.

	BitLocker Management
	After upgrading BitLocker Management with DL-PBA, several exceptions were thrown and reported to the NT event log. This behavior is now fixed.
	BitLocker Management prevented blocking USB flash drives with unapproved or missing BitLocker company IDs by removing corresponding Windows policy settings.

	Defender Management
EI-2372	The day of the week set in the wizard for setting up scheduled scans was evaluated incorrectly and also displayed incorrectly in the DriveLock Management Console (DMC) outside the wizard (e.g. Wednesday set, but evaluated as Thursday).
EI-2343	If a file fails to be restored from the Defender quarantine and the reason is that the original directory where the file was moved to the quarantine no longer exists, the DMC now displays a corresponding error message.
EI-2333	If no media is inserted in the drive, no scan of the drive is triggered and thus no error message about a failed scan is displayed.

	Device Control
	It is now possible to disable the usage policy for drives that are not yet ready for use (e.g. SD card reader without SD card).

Reference	Disk Protection
	If third-party file filter drivers have been installed with DriveLock PBA or Disk Protection, in some cases the DriveLock EFS (Embedded File System) has not been checked and repaired (EFS Sanity).
	Not all partitions were encrypted immediately one after the other. This issue is now fixed.
	Occasionally, a DriveLock Agent update would deregister a service from the DriveLock PBA.

Reference	DriveLock Agent
EI-2121	If the agent remote control was configured to use HTTP only, the self-service did not work.
EI-2465	If the 'Allow remote access in Windows Firewall' setting was disabled, previously configured firewall rules for remote connections to the DriveLock Agent were no longer deleted.
EI-2006	When uninstalling DriveLock Agent, the data for accessing BitLocker-encrypted drives was mistakenly deleted.

Reference	DriveLock Enterprise Service (DES)
EI-2461	When installing a new linked DES, an existing configuration is

Reference	DriveLock Enterprise Service (DES)
	now correctly recognized.
EI-2402	Fixed an error where the agent status could not be processed by the server if GPOs were used for configuration.

Reference	DriveLock Management Console (DMC)
	No agent action was generated after requesting a recovery key for BitLocker Management in the DMC, so the user was not prompted for a new BitLocker password on the client.
EI-2305	You could start the wizard to create a new tenant, even if the wizard determined that you were not authorized to do so. Without this permission, the wizard cannot be started at all now.

Reference	DriveLock Operations Center (DOC)
EI-2475	When you enter the code to offline unlock a computer in DOC, it may be necessary to enter 25 characters, but depending on the configuration, 15 characters may be sufficient. The error message "invalid code" falsely appeared after manually entering the first 15 characters of the code that was actually 25 characters long. Now the message appears generally until the sufficient number of characters has been entered or if the 15 or 25 character long code is invalid.

Reference	File Protection (FFE)
EI-2392	Fixed a bug where access to the Barco Clickshare button was denied.
EI-2471	The BSOD error that occurred when the user's SID could not be retrieved for a request (e.g. due to virtualization and redirection) has been fixed.
EI-2386	Fixed the bug where encrypting Office 365 Cloud files caused a bluescreen error in the "old FFE format".
	Restoring from a system restore point did not work with FFE. This is fixed.
	ReFs is not supported by the "old FFE format".
	Access control for users with read access did not work in the previous version 22.2.x when using the new format. This issue is fixed now.

Reference	Groups / Permissions
EI-2462	If there were too many group memberships, a user was prevented from logging in via SAML. Now the effective group memberships are filtered by the group-based role assignments. This requires users to log in again when changing role assignments.

Reference	Licenses
EI-2157	Fixed the issue related to activating the license using a proxy server. It is no longer necessary to enter a user.

Reference	Security Awareness
EI-2439	Security awareness campaigns created in the policy with a specified language were not necessarily displayed on the agent with the same language.
EI-2403	In the case of a security awareness campaign of type Test, the parameters of the event 'Test failed' were filled with 0 for correct/wrong answers respectively.
	Sometimes the type of a security awareness campaign in the security awareness library was specified as "unknown".
EI-2313	.NET Framework 4.7.2 is no longer a requirement for the agent, only for Security Awareness.

Reference	Pre-boot authentication
EI-2245	When requesting recovery data for PBA emergency logon in the DOC, there was no alternative certificate to select, so recovery was not possible in some cases.

4 System requirements

This section contains recommendations and minimum requirements. The requirements may vary depending on your configuration of DriveLock, its components and features, and your system environment.

4.1 DriveLock Agent

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

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

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

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

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

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

- Complete range:(✓)
- Reduced scope:(Ⓞ)
- 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	✓	✓	⓪	☒	☒

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

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

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

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

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

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

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

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

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

- Only available for Windows 7 SP1 Enterprise and Ultimate

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

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

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

3. **Restrictions for macOS**

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

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

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

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

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

4.2 DriveLock Management Console

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

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

Main memory:

- at least 4 GB RAM

Free disk space:

- approx.350 MB

Additional Windows components:

- .NET Framework 4.8 or higher

Supported platforms:

The Management Console 2023.1HF1 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.

4.3 DriveLock Enterprise Service

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

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

Main memory / CPU:

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

Free disk space:

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

Additional Windows components:

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

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

Required DriveLock API Services Ports (DOC/MQTT):

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

Supported platforms:

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

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

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

Supported databases:

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

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

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

4.4 DriveLock Operations Center (DOC)

Note: This information applies only to DriveLock on-premise installations.

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

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

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

Please also note the following information.

5 Updating DriveLock

If you are upgrading to **newer** versions of DriveLock, please note the following information.

5.1 Updating the DriveLock Agent

Please note the following when you update the DriveLock Agent to a newer version:

1. Before starting the update:
   - If you don't use DriveLock's autoupdate feature to update the agent, specify the following **setting** in the DriveLock policy:
     - **Run DriveLock Agent in unstoppable mode**: Disabled
   - If you are working with one of DriveLock's encryption features, make sure to specify a minimum of 5 days as decryption delay in the encryption settings in case of uninstallation.
   - If you are using BitLocker Management, make sure to consider the following before you update:
     For details, see the BitLocker Management documentation at DriveLock Online Help.
     The **Do not decrypt** encryption setting prevents a possible change in the encryption status of the DriveLock Agents. Before updating, make sure to enable this option in the current encryption policy and save and publish the policy afterwards.
   - If you are using Disk Protection, please note the following before updating:
     When you update, agents with BIOS systems that already have Disk Protection installed will not be updated and will remain at that particular version until Disk Protection is uninstalled.
2. During the update:
   - Perform the upgrade with a privileged administrator account. This is automatically true for the auto update.
3. After the update:
   - If you are using File Protection or Disk Protection, a reboot after the DriveLock Agent update is required to update the driver components. This reboot is recommended once the components have been updated. If you are using a software deployment tool for the update, add this step to the update procedure or restart the updated computers manually.

5.1.1 Manual updates

- If you want to run `DriveLock Agent.msi`, it must be done from an administrative command window via `msiexec`. Double-click from Windows Explorer does not work.
- If you update manually by starting `msiexec` msiexec or DLSetup.exe, it may happen that Windows Explorer does not close correctly. As a result, the Windows user interface disappears (black screen) and does not restart even after the agent update. If this happens, you will have to start the Explorer manually via the Task Manager or initiate a reboot. This mainly affects customers who are using client management software that may be running the `msiexec` in a user session. The problem can be solved by adding the following parameters to the msiexec call:
  - `MSIRESTARTMANAGERCONTROL=Disable`
  - `MSIRMSHUTDOWN=2`

5.2 Updating the DriveLock Enterprise Service (DES)

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

When updating the DES from version 2021.1 to higher versions, please note the following:

To perform the update successfully, you need a valid license including maintenance. It must be stored in your currently running system in the database of the DES or renewed and uploaded via the DMC before starting the update.

5.3 Updating DriveLock components

The DriveLock Installation Guide explains all the steps you need to take to update to the latest version. The Release Notes include some additional information you should be aware of when updating your system.

Warning: The existing self-signed DES certificate can no longer be used when updating from version 7.x to 2019.1 or higher and will be replaced by a newly generated certificate. The new certificate can be created automatically as a self-signed certificate and stored in the certificate store of the computer. When updating from 2019.1 or higher to newer versions, however, you can continue to use the self-signed DES certificate.

Updating the DriveLock Management Console (DMC)

When updating from DriveLock version 7.7.x to higher versions, please use the following workaround to update the DMC: Rename the `DLFdeRecovery.dll` and then reinstall the

DMC.

Updating the DriveLock database

When upgrading from version 2020.1 or older to newer versions, the two DriveLock databases are merged. In this case, an additional migration step is necessary. For more information, see the Technical Article *TA-Database Migration* on DriveLock Online Help - Technical Articles.

Disk Protection Update

After updating the DriveLock Agent, any existing Disk Protection (also known as FDE) installation will be automatically updated to the latest version without re-encryption. After updating the FDE, a restart may be required.

We have compiled more information that is important for updating DriveLock Disk Protection or updating the operating system with DriveLock Disk Protection installed in the document *TA - Windows 10 Upgrade with Drivelock Disk Protection* , also on DriveLock Online Help - Technical Articles.

Updating File Protection to version 2023.1

File encryption features a new encryption format. This new format is now used on new DriveLock Agents as the default. Existing agents will keep using the old format. The format is set with the new File Protection setting **Applied encryption formats**. You can explicitly define a specific encryption format if needed.

> Note: New and old encryption formats are not compatible and must be handled in separate policies. For more information, see the File Protection chapter in the Encryption documentation at DriveLock Online Help.

- **DFS support**
  - The **Old Format** and **Old Format (old driver)** encryption formats do not support DFS.

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

  - DFS shares are supported with the **New Format** option, even if they do not use the primary server only. This was tested on Windows Server 2022 and Windows

Server 2019.

6 Known issues

This chapter contains known issues for this version of DriveLock. Please review this information carefully to reduce testing and support overhead.

6.1 BitLocker Management

Supported versions and editions:

DriveLock BitLocker Management supports the following operating systems:

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

Native BitLocker environment

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

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

Using passwords

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

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

- Minimum: 8 characters In some cases 6 characters (numbers) are also accepted. For more information see the current BitLocker Management documentation on 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.

Encrypting extended disks

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

Encryption on Windows 7 agents

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

Moving from Disk Protection to BitLocker Management

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

Encryption with BitLocker To Go

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

Misleading message when upgrading from version 2022.2 to 2023.1

If the setting in the policy allows end users to delay encryption, the BitLocker Encryption dialog box is falsely displayed when upgrading from version 2022.2 to 2023.1, even though the hard disks are already encrypted. As soon as you click the "Encrypt" button, the dialog box disappears and no encryption or decryption is performed.

6.2 Defender Management

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

6.3 Device Control

Long serial numbers

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

Files blocked for a short time

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

CD-ROM drives

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

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

6.4 Disk Protection

Windows Inplace Upgrade

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

Antivirus software

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

Application Control

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

Hibernation

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

UEFI mode

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

- The PBA provided by version 2019.2 is only available for Windows 10 systems, because the driver signatures from Microsoft required for the hard disk encryption components are only valid for this operating system.
- The PBA for UEFI mode may cause issues with PS/2 input devices (e.g. built-in keyboards).
- With VMWare Workstation 15 and also with a few hardware manufacturers, our test results revealed conflicts with mouse and keyboard drivers of the UEFI firmware, so that keyboard input in the PBA is not possible. In this case, you can use the "k" key to prevent the DriveLock PBA drivers from loading once when you start the computer. After Windows logon to the client, you can then run the `dlsetpb /disablekbddrivers` command in an administrator command line to permanently disable the DriveLock PBA keyboard drivers. Be aware that the standard keyboard layout of the firmware is loaded in the PBA login mask, which usually is an EN-US layout, so special characters may differ.
  Introducing the combined driver as of version 2020.1 solves the issue on some systems (including VM Ware Workstation 15).
  For more information on hotkeys and function keys, see the corresponding topic in the Encryption 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 strongly recommend that you install the firmware updates for the mainboard /UEFI before installing DriveLock PBA / FDE (this also applies to recently purchased devices or to bug fixes).
- A 32 bit Windows operating system or 32 bit DriveLock cannot be installed on 64 bit capable hardware. Please use a 64 bit version of a Windows operating system and DriveLock instead.
- There is still a limitation to disks up to a maximum of 2 TB disk size.

- Some HP computers always have Windows in position 1 of the UEFI boot order and the DriveLock PBA has to be selected manually in the UEFI boot menu. In this case fast boot has to be switched off in UEFI to keep the DriveLock PBA at position one.

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

Reference: EI-686)

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

Requirements for Disk Protection:

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

Restart after installation of PBA on Toshiba PORTEGE Z930:

Reference: EI-751)

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

6.5 DriveLock Mobile Encryption

DriveLock Mobile Encryption: NTFS/EXFAT

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

6.6 DriveLock Operations Center (DOC)

Old versions of DOC.exe are no longer supported

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

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

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

6.7 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.

6.8 Settings for enforced encryption

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

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

6.9 File Protection

Microsoft OneDrive

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

NetApp

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

Windows 10 clients with Kaspersky Endpoint Security 10.3.0.6294

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

Accessing encrypted folders

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

Cancel folder encryption

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

File Protection and USB drives

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

Distributed File System (DFS)

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

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

6.10 Self-service unlock

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

6.11 Thin Clients

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

- Security Awareness may not be able to be used on IGEL clients.
- The “Fill any remaining space on drives” option does not work correctly when used for encrypting a DriveLock container via a Thin Client.

7 DriveLock in different environments

DriveLock is basically designed to use Active Directory, as it follows the AD permissions concept and structure. For example, drives can be shared with specific user groups or policies can be assigned to OUs. However, it can also be used without Active Directory.

DriveLock without Active Directory

If you want to use DriveLock without Active Directory, you can still use DriveLock groups and Azure AD integration is also available. You can use DriveLock computer groups or Azure AD computer groups wherever you can use AD computer groups or OUs.

DriveLock and Azure AD user groups, on the other hand, cannot be used everywhere.

Please note the following:

- A DriveLock on-premises installation uses the local users of the computer where the DES is installed for managing the environment.
- If you are a DriveLock Managed Services user, you can use an Azure AD integration for logging in to the DOC or you can create your own users. Here, you can also assign permissions to Azure-AD groups.
- If the MQTT connection between the agent and DES is disabled, you need to have name resolution (NETBIOS/FQDN Name) working in order to access the clients for helpdesk activities.

8 End-of-Life announcement

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

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

Version	On-premise customer support exists until:	Cloud customer support exists until:
All versions before 2021.2	EoL - not supported any more	EoL - not supported any more
2021.2	May 2024	EoL - not supported any more
2022.1	September 2023	EoL - not supported any more
2022.2	June 2025	Until the release of a version following 2023.1
2023.1	current version	current version

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

Support lifecycle:

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

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

From the date of the EOL announcement, DriveLock will provide full support for this version for another 12 months. 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. However, DriveLock product support will be available for an additional 6 months to respond to phone, email 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:

- DriveLock 2023.1 is the last version to include DNS SD support for automatically locating the agent or server.
- We have stopped developing the DCC and it will no longer be part of our product. DriveLock 2021.2 is the last version that officially supports the DCC until May 2024.

9 DriveLock documentation

Note: We will update our documentation more frequently and independently of DriveLock releases in the future as a result of ongoing restructuring and maintenance. Please find our latest versions at DriveLock Online Help.

The DriveLock documentation consists of the following documents as of now:

DriveLock Installation

Here you will find information for the 'on-premise' installation of the individual DriveLock components.

Note: Note that customers of DriveLock Managed Security Services are provided with alternative installation information.

DriveLock Administration

Here you will find information on operating DriveLock, instructions on working with DriveLock Operations Center (DOC), DriveLock Management Console (DMC), DriveLock Policy Editor, as well as settings for DriveLock Enterprise Service (DES) and DriveLock Agent. You can also get help with configuring global and general settings for drive and device control or event and operating system management.

Application Control

This documentation contains all the information you need to employ DriveLock Application Control.

Defender Management

Here we describe the integration and configuration of Microsoft Defender in DriveLock.

DriveLock Encryption

The following features are included in this documentation:

- **DriveLock BitLocker Management**

  Contains all the necessary configuration settings and functionality that DriveLock provides for hard disk encryption with Microsoft BitLocker.

- **DriveLock Disk Protection**

  Contains all necessary configuration settings for DriveLock Disk Protection (formerly FDE).

- **DriveLock Pre-Boot Authentication**

  Contains the procedure for setting up and using the DriveLock PBA to authenticate users, as well as recovery/emergency login solutions.

- **DriveLock Network Pre-Boot Authentication**

  Contains the configuration for pre-boot authentication within a network.

- **DriveLock BitLocker To Go**

  Contains all the necessary configuration settings to integrate BitLocker To Go with DriveLock.

- **DriveLock Encryption 2-Go**

  Contains information on how the encryption of external data media (such as USB sticks or SD cards) works with Encryption 2-Go.

- **DriveLock File Protection**

  Provides information on configuring DriveLock File and Folder Encryption and the new encryption format that will be used starting with version 2022.2.

DriveLock Events

This document contains a list of all current DriveLock events with descriptions.

Linux Agents

This document describes how to install and configure the DriveLock Agent on Linux operating systems.

macOS Agents

This document describes how to install and configure the DriveLock Agent on macOS operating systems.

Security Awareness

This documentation describes the security awareness functions that also form the basis of the DriveLock Security Awareness Content product.

Vulnerability Management

This documentation describes DriveLock vulnerability scan functionality, configuration settings and usage in DOC and DMC.

10 DriveLock test installation

If you want to have a detailed look at DriveLock and test the product, you can request a trial through the DriveLock website. To do so, simply follow the links on our website https://www.drivelock.com/.

We will provide you with a cloud-based tenant. This way, you can fully focus on the DriveLock Agent and DriveLock's protection functionality.

Once you have registered for a test, we will send you several emails with information to support your testing.

Please contact info@drivelock.com / sales@drivelock.com for more information and assistance with your testing.

Copyright