



# DriveLock

## Release Notes 2022.2 SP1

---

DriveLock SE 2023



# Table of Contents

<b>1 DOCUMENT CONVENTIONS</b>	<b>4</b>
<b>2 INFORMATION FOR 2022.2 SP1</b>	<b>5</b>
<b>3 RELEASE NOTES 2022.2</b>	<b>6</b>
3.1 Service pack version SP1 (Build 22.2.5)	6
3.1.1 Improvements and changes	6
3.1.2 Bug fixes 2022.2 SP1	6
3.2 Hotfix version HF1	9
3.2.1 Improvements and changes	9
3.2.2 Bug fixes 2022.2 HF1	10
3.3 Major version	12
3.3.1 Improvements and changes	12
3.3.2 Bug fixes 2022.2	18
<b>4 SYSTEM REQUIREMENTS</b>	<b>27</b>
4.1 DriveLock Agent	27
4.2 DriveLock Management Console	35
4.3 DriveLock Enterprise Service	35
4.4 DriveLock Operations Center (DOC)	37
<b>5 UPDATING DRIVELOCK</b>	<b>38</b>
5.1 Updating the DriveLock Agent	38
5.2 Updating the DriveLock Enterprise Service (DES)	39
5.3 Updating DriveLock Components	39
5.4 Manual Updates	40
<b>6 KNOWN ISSUES</b>	<b>42</b>
6.1 BitLocker Management	42
6.2 Defender Management	43
6.3 Disk Protection	43

6.4	Known limitations on the agent .....	46
6.5	DriveLock Device Control .....	46
6.6	DriveLock Enterprise Service (DES) .....	47
6.7	DriveLock File Protection .....	47
6.8	DriveLock, iOS and iTunes .....	49
6.9	DriveLock Management Console .....	49
6.10	DriveLock Mobile Encryption .....	50
6.11	DriveLock Operations Center (DOC) .....	50
6.12	DriveLock Pre-Boot Authentication .....	51
6.13	DriveLock in different environments .....	52
6.14	Self Service Unlock .....	52
6.15	DriveLock and Thin Clients .....	52
6.16	Encryption .....	52
<b>7</b>	<b>END OF LIFE ANNOUNCEMENT .....</b>	<b>54</b>
<b>8</b>	<b>DRIVELOCK DOCUMENTATION .....</b>	<b>56</b>
<b>9</b>	<b>DRIVELOCK TEST INSTALLATION .....</b>	<b>59</b>
	<b>COPYRIGHT .....</b>	<b>60</b>

# 1 Document Conventions

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



Warning: Red text points towards risks which may lead to data loss.



Note: Notes and tips contain important additional information.

**Menu items** or names of **buttons use bold formatting**.

*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 for 2022.2 SP1

In the release notes you will find important information about [new features](#) and bug [fixes](#) in the current service pack (SP1), as well as [new](#) features and [bug fixes](#) in the latest hotfix (HF1) and [new features](#) and [bug fixes](#) in the major release. Also included are known issues plus as well as additions to the documentation.

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 Managed Security Service has standalone documentation and release notes that are automatically provided if you are a Managed Service user.

## 3 Release Notes 2022.2

Here you can find all changes and improvements plus bug fixes in the latest DriveLock version.

### 3.1 Service pack version SP1 (Build 22.2.5)

#### 3.1.1 Improvements and changes

The DriveLock version 2022.2 Service Pack 1 (SP1) includes the following new features:

##### BitLocker Management

- As a way to prevent the use of weak passwords, you can add a text file with a list of terms to be excluded to the BitLocker management policy. Once a term from the list is used, the password will be denied.
- An extra command line parameter `blunlockdatadrives` has been added to the DriveLock Agent which allows BitLocker-encrypted data partitions to be unlocked even if they belong to a volume that was originally mounted in another client computer. For this parameter, you need to provide a user who is authorized to log on to the DES.

##### BitLocker To Go

- It is now possible for DriveLock to take over and manage external media (such as USB flash drives) that were not originally encrypted with DriveLock, without having to re-encrypt them.

##### DriveLock Operations Center (DOC): Events

- You can now configure notifications in the Events menu in DOC. To do so, you create notification rules to specify the action that is associated with an event. At present, the only possible action is to send an email to one or more recipients.

##### Inventory

- Collecting AD inventory data has been accelerated. (Reference EI-2364)

#### 3.1.2 Bug fixes 2022.2 SP1

Here you can find information about bugs that are fixed with DriveLock version 2022.2 SP1. Our External Issue numbers (EI) serve as references, where applicable.

	BitLocker Management
EI-2336	When taking over a computer already encrypted with BitLocker, more protectors than intended were created in individual cases. This caused the password dialog to be displayed over and over without being able to set the BitLocker password.
	If auto unlock had been set up for at least one data partition using BitLocker management in Windows, the system drive failed to decrypt after the DriveLock Agent took over with error number 0x80310029.
	BitLocker recovery information was backed up only if the data partition in question was not locked. Exchanging the recovery key of locked partitions was performed successfully, but the key could only be uploaded if the partition was unlocked.
	While using the BitLocker PBA, the recovery key was not exchanged until restarting the DriveLock Agent, if requested before.

	DriveLock Operations Center
EI-2368	In older DriveLock Agent versions, policy names were not resolved correctly.

	Encryption-2-Go
	The File Encryption functionality included in the Encryption 2-Go license did not work if a full File Encryption license was present but wasn't assigned to the DriveLock Agent.

	<b>Risk &amp; Compliance (EDR)</b>
EI-2435	Importing MITRE Attack rules only worked when both Risk & Compliance (EDR) and Application Control licenses were available. The Application Control license was in fact not required.

	<b>System Management (Firewall)</b>
EI-2394	Fixed an error that occurred when loading and applying policies with firewall rules if they were created in DriveLock versions older than 22.2 and had 'All' as the log type.



## **3.2 Hotfix version HF1**

### **3.2.1 Improvements and changes**

#### **DriveLock Agent**

- Now, maintenance tasks (reinstallation or repair of the agent MSI) are not carried out while the DriveLock service is running.  
Background: When performing maintenance tasks, the DriveLock service is not allowed to run. So far, the service was always suspended. Now, however, maintenance is stopped if the DriveLock service is already running. (Reference: EI-2308)

#### **DriveLock macOS Agent / DriveLock Operations Center**

- You can now download the DriveLock macOS Agent installation package directly from the Deployment section in the DriveLock Operations Center (DOC).

### 3.2.2 Bug fixes 2022.2 HF1

DriveLock 2022.2 HF1 is a hotfix release.

This chapter contains information about errors that are fixed with DriveLock version 2022.2 HF1. Our External Issue numbers (EI) serve as references, where applicable.

	BitLocker Management
EI-2356	Fixed a bug with the display of Bitlocker recovery keys in the DOC.

	Device Control
EI-1589	Fixed an error that occurred when checking the wds-scan-report.xml file.

Reference	Disk Protection
	When third-party file filter drivers are installed with the DriveLock PBA or Disk Protection, the DriveLock EFS (embedded file system) was not checked and repaired in some cases (EFS Sanity).

Reference	DriveLock Agent
EI-2310	After connecting Linux and macOS agents to the DES, the DOC now displays the status of the agents correctly and no longer as outdated.

Reference	File Protection
	New encryption format: The path to an encrypted folder may now contain diacritical characters (e.g. the dots for umlauts or the French or Spanish cedilla).

Reference	Infrastructure
EI-2328	Fixed an error that occurred when applying the proxy settings defined in the configuration profile for the user. The settings will now be reset correctly.

Reference	Licenses
EI-2335	Fixed an error related to the calculation of user licenses.

## 3.3 Major version

### 3.3.1 Improvements and changes

#### New features

- **USB drive control for Mac operating systems**

DriveLock has added the macOS platform to its supported operating systems. This also allows externally connected USB drives to be locked or unlocked under macOS Catalina, Big Sur, Monterey and Ventura. The DriveLock Agent is available for computers equipped with Intel chips and also for Apple's ARM architecture.



Note: The macOS agent is available on request. Please contact your DriveLock sales partner.

- **Application Control in DOC**

It is now much easier to unlock applications from within the DOC by using application rules. The inventory view has also been enhanced, making it easier to see when certain applications were last used, for example, and on how many computers they are installed.

- **File Protection**

DriveLock introduces a new File & Folder Encryption format for operating systems Windows 10 and later. Please note the [information](#) in the Updating DriveLock components chapter. For new customers, this new encryption is the standard. However, customers who have already set up encrypted directories can continue to use the previous encryption with this version.

- **Masking of personal and computer-related data (data masking/pseudonymization)**

In the DOC, you can now pseudonymize/mask computer and user names as key personal data records so that it is no longer possible to draw direct conclusions about a specific person or their behavior.

The key functions are:

- Enabling and disabling data masking for a tenant's environment
- Configuring permissions allowing to change data masking settings
- Configuring authorized persons who are allowed to see data in plain text
- Configuring the authorized persons who are allowed to approve a request for plain text display

- Plain text display is possible on the basis of an assigned permission, after the request has been approved by another DOC user, or after any other person has entered a special approval code
- Selecting specific events where data will be masked in all occasions or never.

- **Audit events**

Special audit events now indicate changes that affect or could affect the security of the environment. The DOC provides an additional filter for audit events, allowing all changes to safety-related settings to be fully tracked.

## Improvements

### Agent remote control

- Agent remote control now only uses HTTPS as default.

### Anonymous data

- Anonymous data / data masking: In previous versions, computer and user names as a key attribute of personal data were masked by encrypting event information before it was transferred to the DriveLock Enterprise Service. These encrypted records were then available for decryption in the DriveLock Control Center after being loaded from the DES, provided the correct certificates were available. Going forward, DriveLock will no longer provide this encryption of events, but instead will integrate data masking completely into the DOC.

### Database

- In the database installation wizard, you are now able to optionally activate a data conversion after an update.

### DriveLock Enterprise Service (DES)

- Several stored procedures for deleting old data have been added to the database maintenance. Please adjust the database maintenance steps you configured manually. For information on this topic, please refer to our "Database Guide" among the technical articles on [DriveLock Online Help](#). (Reference EI-2222)

### DriveLock Operations Center (DOC)

- Certificates can now be stored and used in the DOC to generate offline unlock response codes.
- A new standard dashboard with agent rollout information is available
- The DriveLock DOC Companion can now be deployed and installed as a separate installation package. This facilitates rollout in larger system environments and release processes.
- Logging on to the DOC is now also possible via the integrated Windows logon (Active Directory user) - eliminating the need for an additional user login process.
- The DOC now displays the current online status in the computer views. This gives the administrator additional information on whether a computer can currently be contacted for online unlocking or remote agent connection.
- This version also includes further usability improvements in the DOC and has incorporated customer feedback:

- List column widths are now maintained in most grid views when manually adjusted
- Users can now specify their preferred view when calling a menu item for the first time
- When deleting computers from the DOC, existing recovery information is now still stored in the database unless explicitly deleted
- In addition to the existing installation methods, a download link is now also available for cloud environments, which can be distributed within the company via e-mail, for example.

### DriveLock PBA

- BIOS Pre-Boot Authentication: As of version 2022.2, BIOS PBA is no longer supported and removed from the product scope. This makes DriveLock 2021.2 the last version with an update to DriveLock legacy BIOS pre-boot authentication.



Note: When you install a version 2022.2 agent, the system checks whether there is an active legacy BIOS PBA on the system. If this is the case, the agent will no longer be updated or installed.

- The DriveLock PBA can now be deactivated until the first Windows login by a user, who will then be synchronized into the PBA accounts (auto-logon mode).

### DriveLock Policy Editor

- Stringlist properties within DriveLock policies can now also be created in additive mode, meaning that a stringlist from an assigned policy does not overwrite the values of the same property from another assigned property, but only adds to them. It is possible to import/export multiple lines via copy & paste.

### Events

- An administrator can now configure which events are to be ignored when forwarding events centrally from the DES to a syslog service or via SMTP. This allows unwanted events to be filtered out in the target system. In addition, individual events from the DES can now be forwarded to any SYSLOG destination.
- The stored procedures for deleting old events have been modified. For details, see the DriveLock Database Guide in the Technical Articles section of [DriveLock Online Help](#).
- The agent now reports third party events that occurred while the agent was not run-

ning.

- In the Policy Editor, the EDR node has been renamed to Events and Alerts.

### **Firewall management**

- Firewall rules may now be easily read from an existing system via agent remote control and applied to a policy. (Reference EI-1765)
- Firewall rules may now include any setting options that can also be modified via Powershell commands.
- The Firewall Management component can now be completely disabled even if a license is present on a DriveLock Agent.

### **Group management**

- The Groups node has been completely removed from the DriveLock Management Console (DMC). Groups can now be fully managed or created in the DOC. (Reference EI-2178)
- When you add group members, you can now also add a comment, like the number of an internal support ticket. This allows administrators to document the reason for making the change.
- Now, you can create dynamic groups based on additional information, such as hardware product ID or computer vendor and other AD properties.

### **Installation**

- This version reduces the size of the DriveLock Agent installation file by more than 20%, allowing for faster and more efficient software distribution.
- In addition to the existing installation methods, a download link is now also available for cloud environments, which can be distributed within the company via e-mail, for example.

### **Licenses**

- Trial licenses are now only available through your DriveLock sales partner and are no longer automatically shipped with the product. (Reference EI-2123)
- EDR or Risk & Compliance functionality no longer needs to be licensed separately as of 2022.2.
- Application Control licenses are now listed as one single combined entry rather than listed separately.
- User licenses have been added to the license display in the DOC.



## **Network**

- The option to select custom network connections in the DriveLock Agent UI and in the network connection tray icon has been removed.

## **Security Awareness**

- Security Awareness packages with version 22.2 are only delivered to current agents with version 22.2 and newer to ensure compatibility.
- There is a new version of Security Awareness campaigns.

### 3.3.2 Bug fixes 2022.2

This chapter contains information about bugs fixed with DriveLock version 2022.2. Our External Issue numbers (EI) serve as references, where applicable.

Reference	Application Control
	Certificate checking for predictive whitelisting has been improved.
	Temporary unlocking is now terminated correctly.

Reference	BitLocker Management / BitLocker To Go
	Fixed an error when importing BitLocker management certificates into a policy.
EI-2203	When taking over existing BitLocker environments, it was possible that each time a policy update occurred, the BitLocker password was re-requested and re-set. This behavior was associated with the number of recovery keys that were entered for the system drive that was being taken over.
	The recovery key upload could fail if the policy update was not performed correctly or incompletely before.

Reference	Defender Management
	When merging policies, string lists in the Defender configuration sometimes did not correctly overwrite string lists from other policies. If this behavior was desired, you must now

Reference	Defender Management
	set the "Append values" option in the string list.
EI-2137	Fixed a bug that prevents Windows Defender from registering under certain circumstances


Reference	Device Control
EI-2028	Some external drives experienced a timing issue that resulted in a Blue Screen of Death (BSOD) error.
EI-2038	Fixed an error that caused device collections to stop working under certain circumstances in conjunction with old db3 CSP policies.
EI-1846	Bluetooth devices were not available with the Marvell AVASTAR wireless chip if the WiFi device was disabled during boot. The error is fixed after reboot.

Reference	Disk Protection
EI-2098	Fixed an error that the datAshur stick triggered at system start-up.
EI-2179	Fixed a BSOD (Blue Screen of Death) error that occurred when connecting an HP OfficeJet 200 printer.

Reference	DriveLock Agent
	The status of the hard disk self-monitoring (S.M.A.R.T.) is now read out correctly again.
EI-2201	Fixed an error where the agent crashed when an extremely long serial number was present in a drive collection.
EI-1995	During an update, the Windows Installer may not have replaced all DriveLock files, resulting in an inconsistent installation.
EI-2188	For file access events, the process was truncated at 128 characters.
EI-2029	Fixed an error where the agent crashed when there were multiple remote connections.
	The character combination "\n" (e.g. C:\windows\system32\notepad.exe) is now displayed correctly in message texts instead of replacing it with a line break.
	For some remote control events, the agent now sends error information.
EI-2159	The agent no longer crashes when the registration of the agent fails.
EI-2122	In some cases, the DriveLock service took a long time to start when no user was logged in.
EI-2020	Changes to ports in the Windows Firewall policy are now transmitted to the agent computer.

Reference	DriveLock Agent
EI-2190	Fixed an error that occurred in the DES certificate validation process that prevented certificate revocation list information from being retrieved.

Reference	DriveLock Enterprise Service (DES)
EI-2083	The DotNetZip library has been updated to version 1.16.0 (CVE-2018-1002205).

Reference	DriveLock Management Console (DMC)
	<p>The Device Scanner Database tab is now only displayed if there is matching content.</p> <div>  Note: Note: For new installations of DriveLock, this tab no longer exists.         </div>
EI-2048	When creating a new SB group, an endless progress bar came up, if there were no DriveLock groups in the environment at all.
EI-2126	In the RSOP, in "Policies applied", the DMC tried to open the Centrally Stored Policies in the GPO Editor instead of the Policy Editor, resulting in an error message.
EI-2111	The definition of dynamic groups can no longer be edited in the DMC starting with version 22.1. In spite of this, the definitions were deleted when you viewed the group properties, which made the group unusable.

Reference	DriveLock Management Console (DMC)
EI-2084	The number of conditional setting nodes per node was limited to 15. However, it was still possible to add as many as you wanted per node in the DMC, but after that the policy could not be opened in the DMC anymore - it crashed. The limit has now been increased to 50, you cannot add more than 50, and if you open a policy (unlikely) that contains more anyway, it will no longer crash.
EI-2054	After updating to 21.2 or newer, it was not possible to customize the agent configuration via DMC for agents older than 21.2.

Reference	DriveLock Operations Center (DOC)
EI-1980	Requesting the agent's local whitelist in the DMC now also works if the process takes up to 2 minutes. Previously, an error was displayed after 15 seconds.
	If you modify a widget after creating it or create a custom widget, some properties that are no longer supported will be displayed as obsolete when you refresh them.
EI-2073	Entering an incorrect password in the DOC login screen no longer results in multiple incorrect login attempts being registered in the AD. This could lead to a temporary account suspension.
EI-2030	Fixed an error when displaying the application control license

Reference	DriveLock Operations Center (DOC)
	for agents older than 21.2.
	When creating a filter for the Windows/DriveLock version for dynamic groups in the DOC, you are now also given a drop-down list with predefined values.
	When grouping by text or event ID, the ID or text displayed for third-party events sometimes did not match that of the event.
	The drive list did not show any drives when the policy was opened with DOC Companion.
EI-1525	A temporary unlocking by means of challenge/response via the DOC with weak codes did not show any error messages if the password or response code was incorrect.

Reference	DriveLock pre-boot authentication
EI-2118	Information about the fact that a PBA that had previously been deactivated was active again was displayed repeatedly.
	Fixed the issue of not getting a Single Sign On the first time after updating the DriveLock PBA.

Reference	DriveLock tools
EI-1985	DriveLock Support Companion no longer crashes when col-

Reference	DriveLock tools
	lecting system information on Windows XP.
EI-1975	DOC Companion now supports wildcards for proxy bypass lists.

Reference	Encryption-2-Go
EI-2074	Drive rules in the DMC: If the forced encryption was activated and the dialog was closed without switching to the access rights tab, invalid values were stored for the rule.

Reference	Events
	The user is now displayed in third-party events.
EI-2093	Some remote control events were missing parameters.
EI-1986	Event 443 now shows both the ID and the name of the components.

Reference	File Protection
	File Protection decryption did not always work on network shares when the folder was mounted and the encrypted folder was directly in the share.
EI-2086	In the DMC, you could not import an AD user from another trus-



Reference	File Protection
	ted domain (in DriveLock File Protection / Users and Groups).

	Licensing
EI-2018	An incorrect subscription end date was displayed when no Device Control license was present.
EI-2046	If you opened an old policy after an update and cancelled the License Activation Wizard, the license was removed from the policy. This sometimes resulted in unexpected system behavior. Now, a warning message is displayed when the wizard is canceled.

Reference	Logging
EI-2078	The settings for very detailed logging were not removed correctly.
EI-2049	Logging in the DMC is now enabled during installation.

Reference	System Management
EI-2021	After setting the remote ports of a firewall rule, they were correctly saved in the policy. However, after reopening the rule's properties dialog, it looked as if the ports had not been saved.

Reference	System Management
EI-1986	The components "Power Management" and "Local Users and Groups" can now be loaded under Windows XP and do not produce events with ID 443.



Reference	Terminal Services
EI-1497	Portable media devices (e.g. cameras, media players) are now managed in terminal service environments when connected via a terminal session (in ICA or RDP protocol).
EI-1915	It was not possible to mount encrypted containers under the same drive letter in two different Citrix terminal sessions when USB sticks were connected to the generic channel.

## 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	<p>Windows 7 SP1 Enterprise / Ultimate with Extended Support.</p> <p> Note: At some point after the release of version 2022.2, an additional Legacy Support license will be required for Windows 7 systems when you renew your maintenance or purchase a new version.</p>
Windows XP	<p>Windows XP SP3, additional legacy support license of DriveLock required.</p> <p> Note: Version 2022.2 is the last DriveLock version that supports the Windows XP operating system.</p>
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

Operating system	Versions
macOS	Catalina, Big Sur, Monterey, and Ventura - both Intel and ARM architecture.

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: Note that .NET Framework 4.7.2 is required for the DriveLock Agent on all Windows operating systems.

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

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

Feature	Operating system / functions					
	Win- dows 10 / 11	Win- dows Server	Win- dows 7	Win- dows XP	Linux	Mac OS
Device Con- trol	✓	✓	⓪	⓪	⓪	⓪
Application Control	✓	✓	✓	⓪	⓪	☒
Encryption 2-Go	✓	✓	✓	✓	⓪	⓪
BitLocker To Go	✓	✓	⓪	☒	☒	☒
BitLocker Man- agement	✓	✓	⓪	☒	☒	☒
Security Awareness Multimedia campaigns	✓	✓	✓	☒	☒	☒

Feature	Operating system / functions					
Defender Management	✓	✓	☒	☒	☒	☒
Vulnerability Management	✓	✓	✓	☒	☒	☒
Security Configuration Management	✓	✓	✓	☒	☒	☒
Disk Protection	✓(*)	☒	☒	☒	☒	☒
File Protection	✓	✓	①	☒	☒	☒

(\*): 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 Windows XP



Note: DriveLock 2022.2 is the last agent version that supports Windows XP. Future DriveLock versions cannot be installed on Windows XP.

- Device Control:  
Only digital cameras work (UMDF and WPD frameworks are available under XP), Bluetooth functionality is not available
- Application Control:



Application Behavior Control: The registry check does not work, rules with this configuration are ignored

#### 4. **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 decrypt 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.

#### 5. **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.

## **6. 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.

### 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 2022.2 SP1 has been tested and approved on the latest versions of Windows that were officially available at the time of release and that have not yet reached the end of the service period provided by Microsoft. Please check the [DriveLock Agent](#) chapter for a list of Windows versions that DriveLock supports.



Warning: DriveLock Management Console is only available as a 64-bit application.

## 4.3 DriveLock Enterprise Service

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 2012 R2 64-bit (minimum requirement for the DriveLock Operations Center)



Note: Please make sure you have installed SQL Express 2017 under Windows Server 2012 R2 before you can successfully install DriveLock version 2020.1.



Note: This version 2022.2 is the last version that supports installation on Windows Server 2012 R2 operating system.

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


On Windows 10 client operating systems, use a DES as a test installation only.




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

### Supported databases:

- SQL Server 2014 (minimum requirement for DriveLock Operations Center) or newer. This version 2022.2 is the last version that supports SQL Server 2014.
- SQL Server Express 2017 or newer (for installations with up to 200 clients and test installations)


 Warning: 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)

As of version 2021.2, we no longer include an MSI installer for installing the DriveLock Operations Center (DOC.exe) locally. We integrated all of the functions provided in the DOC.exe in other ways into our DOC platform (DOC Companion). That way, there is no need for an additional application.

 Note: 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.

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:

- Check whether the DriveLock Update Service **dlupdate** is running on your system; if it is, make sure to remove it.
- If you update the agent with DriveLock's auto update functionality, specify the **Automatic update setting** in the DriveLock policy:
  - Check the **Perform reboot to update the agent** checkbox and set the value for a user-deferred installation to **0**, to keep the time to restart the computer as short as possible.
- Please also specify the following **settings**:
  - **Run DriveLock Agent in unstopable mode**: Disabled
  - **Password to uninstall DriveLock**: Not configured
- 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:

- You must reboot the client computers after the DriveLock Agent has been updated so that the driver components are updated, too. If you are using a software deployment tool for the update, add this step to the update procedure or restart the updated computers manually.

## 5.2 Updating the DriveLock Enterprise Service (DES)

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 2022.2

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 2022.2.

- 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.

## 5.4 Manual Updates

Manually updating the agent fails if `DriveLock Agent.msi` is started from Windows Explorer (e.g. by double-clicking) and without local administrator permissions. In this case, start the MSI package from an administrative command window via `msiexec` or use `DLSetup.exe`.

### Update from older to newer DriveLock versions

If you update manually by starting `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`

## 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

#### Native BitLocker environment



Note: Starting with version 2019.1, you don't have to use the native BitLocker administration or group policies to decrypt computers that were previously encrypted with native BitLocker; these system environments can be managed directly now. 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

A USB flash drive was not mounted after encrypting it with an administrative password. To solve the issue, remove the USB flash drive first and then plug it back in.

## 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 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 chapter in the BitLocker Management 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.

### BIOS mode

On a small number of computer models the default DriveLock Disk Protection pre-boot environment configuration may not work correctly and cause the computer to become unresponsive. If this occurs turn off the computer and restart it while pressing the **SHIFT-Taste** key. When prompted select the option to use the 16-bit pre-boot operating environment.

Due to an issue in Windows 10 Version 1709 and newer, DriveLock Disk Protection for BIOS cannot identify the correct disk if more than one hard disk is connected to the system. Therefore Disk Protection for BIOS is not yet released for Windows 10 1709 systems with more than one hard disk attached until Microsoft provides a fix for this issue.



Note: An additional technical whitepaper with information on updating to a newer Windows version with DriveLock Disk Protection installed is available for customers in our Support Portal.

### 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.

## **6.4 Known limitations on the agent**

### **Updating/ installing/ uninstalling the agent on Windows 7 x64**

The Explorer (explorer.exe) crashes after updating, installing or uninstalling the DriveLock Agent on Windows 7 x64. This only happens in specific scenarios where the Windows command prompt is opened with admin privileges and the system has not been rebooted since the agent was updated/ installed/ uninstalled.

## **6.5 DriveLock Device Control**

### **Universal Camera Devices**

In Windows 10, there's a new device class: Universal Cameras; it is used for connected or integrated web cameras that do not have specific device drivers.

Currently, you cannot manage this device class with DriveLock.



Note: To control these devices, please install the vendor's driver that comes with the product. Then DriveLock automatically recognizes the correct device class.

### **Windows Portable Devices (WPD)**

Locking "Windows Portable devices" prevented that some Windows Mobile Devices could be synchronized via "Windows Mobile Device Center", although the special device was included in a whitelist.

Windows starting from Windows Vista and later uses a new "User-mode Driver Framework" for this kind of devices. DriveLock now includes this type of driver.

The driver is deactivated on the following systems because of a malfunction in the Microsoft operating system:

- Windows 8
- Windows 8.1 without Hotfix KB3082808
- Windows 10 older than version 1607

### Long serial numbers

Drives with serial numbers longer than 63 characters cannot be locked or unlocked by a whitelist rule with a required serial number or a permanent unlock 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.

### Windows Portable Devices on Citrix Generic Channel

The Windows Portable Device API does not return VID, PID and S/N in this configuration. Since the driver can retrieve the correct information, there are two workarounds for this problem:

- Connect the device to any agent and create a whitelist rule. The driver is able to obtain VID, PID and S/N, therefore the locking will be working as expected.
- Create a device collection and insert the device based on the Hardware ID. This is possible even for devices connected to the Citrix Generic Channel. Then create a whitelist rule for the collection (Reference: EI-1705)

### 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).

## 6.6 DriveLock Enterprise Service (DES)

DES setup may fail when using certificates created with OpenSSL.

## 6.7 DriveLock 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.

### 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 (DLFIdEnc.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 2022.2.

## 6.8 DriveLock, iOS and iTunes

DriveLock recognizes and controls current generation Apple devices (iPod Touch, iPhone, iPad etc.). For older Apple devices that are only recognized as USB drives no granular control of data transfers is available (for example, iPod Nano).

DriveLock and iTunes use similar multicast DNS responders for automatic device discovery in networks. When installing both DriveLock and iTunes the installation order is important:

- If DriveLock has not been installed yet you can install iTunes at any time. DriveLock can be installed at any later time without any special considerations.
- If DriveLock is already installed on a computer and you later install iTunes you have to run the following command on the computer before you start the iTunes installation: `drivelock -stopdnssd`. Without this step the iTunes installation will fail.

After an update of the iOS operating system on a device, iTunes will automatically start a full synchronization between the computer and the device. This synchronization will fail if DriveLock is configured to block any of the data being synchronized (photos, music, etc.).

## 6.9 DriveLock Management Console

In some cases, the Console crashed when you added a second user after having added a user beforehand. This issue is caused by the Microsoft dialog (AD Picker).

According to our information, this issue is known in Windows 10; please find details [here](#).

As soon as Microsoft has fixed the issue, we will reopen it on our side.

### Version differences between DMC and DES:

If you use the DriveLock Enterprise Service (DES) version 2022.1 or newer with a lower DMC version, the system crashes or displays a large number of error messages, making it impossible to work.

## 6.10 DriveLock Mobile Encryption

### DriveLock Mobile Encryption: NTFS/EXFAT

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

### Default enforced encryption settings

If you select the option "Fill any remaining empty space on drives", a small amount of storage space (very few MB) may remain free for technical reasons when calculating the available space. (Reference: EI-1784)

### Compatibility issue between NTFS and Mac operating systems

Due to an incompatibility with macOS and NTFS, drives formatted as NTFS drives on Windows cannot be used on Mac computers.

## 6.11 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.

### Version conflict when calling the RSOP

If a DriveLock Agent has version 2021.2 or later installed, then at least version 2021.2 or later is also required for the DriveLock Management Console (DMC) to display the RSOP correctly.

### Multiple selection of computers in the Computers view

If you select several computers in the Computers view and then select the **Run actions on computer** command in the upper right menu to enable the trace for these computers, tracing is only started for the first selected computer. The others neither start the tracing nor report an error. Our team is working on a solution.

### 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. Our team is working on a solution.

## Export lists to Excel

It depends on the available resources how many lists you can export. We recommend that you set the filters so that no more than 20,000 entries are exported. A higher number of entries may cause the action to be aborted or the exported list to remain empty. (EI-1379)

## 6.12 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 Inspiron 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.

### 6.13 DriveLock in different environments

Basically, DriveLock is designed to operate in Active Directory, but it can also be used without Active Directory. For more information, see the documentation (DriveLock Administration).

### 6.14 Self Service Unlock

If you use the Self Service wizard to unlock connected iPhone devices, it will still be possible to copy pictures manually from the connected iPhone after the unlock period ended.

### 6.15 DriveLock and 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.

### 6.16 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. Our team is working on a solution.

## 7 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.



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

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

Version	Continued Customer Care Support
All versions before 2021.2	EoL - not supported any more
2021.2	May 2024
2022.1	September 2023
2022.2	June 2025

### Support cycles:

Support periods for new product versions are adjusted to match the support period for Windows 10 Enterprise Edition, released during the same period of the year (release spring: approx. 18 months, release fall: approx. 30 months). When a new version is released, we also publish the support end of this version.

Maintenance updates and code fixes for bugs and critical issues will be released during this period. We also respond to inquiries via phone, email and Self-Service, provided by DriveLock's Product Support Team and related technical assistance websites.

### 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:

- As of version 2023.1, the option to change or configure the settings for event encryption is no longer available. Events are basically no longer encrypted. The data masking functions added in version 2022.2 completely replace the previous pseudonymization

by encryption.

- 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.
- Version 2022.2 is the last DriveLock version that supports the Windows XP operating system. You will not be able to install any future versions of the DriveLock Agent on this legacy Microsoft operating system. Also, it is not possible to update to newer versions on Windows XP anymore. Customers can run this DriveLock Agent on Windows XP until support for version 2022.2 ends. Please note that you will need the DriveLock legacy OS license as before.
- Starting with the 2023.1 release, the DriveLock legacy OS license will be required when running DriveLock on Windows 7. From this point on, this license must be purchased for all DriveLock versions still running on Windows 7.
- The following server operating systems and database versions are supported for the last time with this release:
  - SQL Server 2014, SP3
  - Windows Server 2012 R2
  - Windows 10 20H2 Enterprise
  - Windows 10 21H1 Pro/Enterprise


## 8 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 get information how to install the different DriveLock components.

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

### DriveLock Administration

 Note: We are currently revising the documentation related to the DriveLock administration. For this reason, we will temporarily provide two versions with different content. In addition, some content is currently only available and up to date in German, the English version will be added as soon as possible.

- The new **DriveLock Administration** documentation provides a brief introduction to the DriveLock Operations Center (DOC), and information on using the DriveLock Management Console (DMC) and the DriveLock Policy Editor.
- In the old **DriveLock Administration Guide**, you can still find chapters on drive and device control in this version.

### Application Control

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

### Defender Integration

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

### DOC Companion

This is a quick introduction to the DOC Companion tool which acts as an interface between the DriveLock Operations Center (DOC) and the DriveLock Management Console (DMC).

### DriveLock Encryption

The following features are included in this documentation:



- **DriveLock BitLocker Management**

This chapter details the required configuration settings and functionality DriveLock provides for hard disk encryption with Microsoft BitLocker.

- **DriveLock Disk Protection**

This chapter explains the configuration settings required for DriveLock Disk Protection (formerly known as FDE).

- **DriveLock Pre-Boot Authentication**

This chapter explains the procedure for setting up and using DriveLock PBA to authenticate users, and provides solutions for recovery or emergency logon.

- **DriveLock Network Pre-Boot Authentication**

This chapter describes the configuration for pre-boot authentication for use within a network.

- **DriveLock BitLocker To Go**

In this chapter you will find all the necessary configuration settings to integrate BitLocker To Go into DriveLock.

- **DriveLock Encryption 2-Go**

This chapter provides information on how Encryption 2-Go handles the encryption of external data media (such as USB flash drives or SD cards).

- **DriveLock File Protection**

This chapter contains information on how to configure DriveLock file and folder encryption, including 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.

## **Self-Service Portal**

This document explains how users can access the computers protected by DriveLock Disk Protection or BitLocker Management when they forget their passwords.

## **User Guide**

The DriveLock User Guide contains the documentation of all features available to the end user (temporary unlock, encryption and private network profiles). This PDF is intended to help end users navigate the options available to them.

## **Vulnerability Management**

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


## 9 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. Just follow the links on our website <https://www.drivelock.de/>.

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. See <https://www.drivelock.de/cloud-testversion-information> for a summary.

Please contact [info@drivelock.com](mailto:info@drivelock.com) / [sales@drivelock.com](mailto:sales@drivelock.com) for more information and assistance with your testing.



## Copyright

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

© 2023 DriveLock SE. All rights reserved.

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

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

