DriveLock

Release Notes 2019.2 SP1

DriveLock SE 2020

Table of Contents

1 Release Notes 2019.2 SP1

This document contains important information about the new version of DriveLock and changes from previous DriveLock versions. The DriveLock Release Notes also describe changes and additions to DriveLock that were made after the documentation was completed.

Please find the complete DriveLock documentation at www.drivelock.help.

1.1 Document Conventions

Throughout this document the following conventions and symbols are used to emphasize important points that you should read carefully, or menus, items or buttons that you need to click or select.

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 forma**tting. *Italics* represent fields, menu commands, and cross-references.

`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.

1.2 Available 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 visit our documentation portal drivelock.help to find our most current versions.

At present, DriveLock provides the following documentation for your information:

- **DriveLock QuickStart Guide**
  The QuickStart Guide describes the required steps to setup DriveLock using the DriveLock QuickStart setup wizard. The DriveLock QuickStart setup wizard can be used to simplify the installation and configuration of a basic DriveLock environment.

- **DriveLock Installation Guide**
  The Installation Guide describes the available installation packages and the steps for installing each DriveLock component. After you have read the Release Notes, this is the first document we recommend reading when you install DriveLock first.
- **DriveLock Administration Guide**
  The Administration Guide describes the DriveLock architecture and components. It contains detailed instructions for configuring DriveLock using the DriveLock Management Console (DMC). This document is intended for DriveLock administrators who need to become familiar with all available DriveLock functionality.
- **DriveLock Control Center User Guide**
  This manual describes how to configure and use the DriveLock Control Center (DCC). This document is intended for administrators and users who will be using the DriveLock Control Center.

> Note: The DriveLock Operations Center (DOC) will replace the DriveLock Control Center (DCC) later this year.

- **DriveLock Manual Supplement for Certification Compliant Operation**
  This manual describes the steps and settings required if DriveLock 2019.2 is to be installed, configured, and operated according to the Common Criteria Certification. The certification applies to a subset of the functionality (Device and Application Control) of the DriveLock Agent, configured by signed centrally stored policies. The remaining functions of the Agent can be used alongside the evaluated functions.
- **DriveLock User Guide**
  The DriveLock User Guide contains the documentation of all features available to the end user (temporary unlock, encryption and private network profiles). The user guide is intended to help end users find their way around the options available to them.
- **DriveLock Security Awareness**
  This manual describes the new security awareness features, which are also included in DriveLock Smart SecurityEducation.
- **DriveLock Linux Agents**
  This manual explains how to install and configure the DriveLock Agent on Linux clients.
- **DriveLock BitLocker Management**
  This manual describes how to use DriveLock BitLocker Management. It also explains the configuration settings available for hard disk encryption with native BitLocker in a

DriveLock environment.

The **DriveLock Pre-Boot Authentication** chapter explains how you set up and use the DriveLock PBA to authenticate users, and provides solutions for recovery or emergency logon.

The **BitLocker To Go** chapter describes the configuration settings required to manage drives encrypted with BitLocker To Go with DriveLock.

2 Updating DriveLock

When you update to higher versions of DriveLock, please note the following information.

2.1 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 unstoppable 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.
   - With BitLocker Management, note the following before updating (for more details see the Bitlocker Management documentation on DriveLock Online Help) : The new encryption setting **Do not decrypt** prevents a potential change of 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 afterward.
2. During the update:
   - Run the update 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.

2.2 Updating DriveLock Components

General information on updating to the current version

- The DriveLock Installation Guide explains all the steps you need to take to update to the latest version.
- The DriveLock Management Console and the DriveLock Control Center are installed in individual directories. This ensures that there is no interaction when these components are updated automatically.

> Note: The DriveLock Control Center uses some components of the DriveLock Management Console to access the client computers remotely. Both components must have the same version number, matching the version of the installed DES.

Important information regarding certificates

With DriveLock version 2019.2 you can find the new tool **ChangeDesCert.exe** in the DES program directory at C:\Program Files\CenterTools\DriveLock Enterprise Service\ChangeDesCert.exe. Note that if you want to exchange an existing DES server certificate using ChangeDesCert.exe, you must import the new certificate into the computer's Certificate Store and configure the private key as exportable.

> Warning: The existing self-signed DES certificate can no longer be used when updating from version 7.x to 2019.1 and will be replaced by a newly created 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 to 2019.2, however, you can continue to use the self-signed DES certificate.

Updating DriveLock Disk Protection

After the DriveLock Agent has been updated, an existing DriveLock Disk Protection installation will be updated automatically and without re-encryption to the most current version. After updating the Disk Protection components, a reboot may be required.

For further information on updating DriveLock Disk Protection or updating the operating system where DriveLock Disk Protection is already installed, see our separate document available for download from our website www.drivelock.help.

3 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.

Note: Microsoft regularly publishes software patches for its software products on the so-called Microsoft Patchday, Patch or Update Tuesday. DriveLock fully supports these Microsoft updates with the Microsoft operating system versions described in the supported platforms section in the DriveLock Agent chapter.

3.1 DriveLock Agent

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

Main memory:

- at least 4 GB RAM

Free disk space:

- approx. 1 GB with average policies that do not include your own video files
- at least 2 GB if Security Awareness campaigns are used with video sequences (Security Awareness Content AddOn)

Note: How much disk space you need largely depends on how DriveLock agents are configured via policies and on the settings and features they contain. It is therefore difficult to provide an exact specification here. We recommend that you verify and determine the exact value in a test setup with a limited number of systems before performing a company-wide roll-out.

Additional Windows components:

- .NET Framework 4.5.2 or newer (for Security Awareness Campaigns in general)
- 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.

Supported platforms:

DriveLock supports the following Windows versions for the listed agent versions:

OS version	2019.2	2019.1	7.9.6
Windows 10 Pro			
Windows 10-1909	+	+	-
Windows 10-1903	+	+	-
Windows 10-1809	+	+	+
Windows 10-1803	+	+	+
Windows 10-1709	-	+	+
Windows 10-1703	-	+	+
Windows 10-1607	-	+	+
Windows 10 Enterprise			
Windows 10 Enterprise-1909	+	-	-
Windows 10 Enterprise-1903	+	+	-
Windows 10 Enterprise-1809	+	+	+
Windows 10 Enterprise-1709	+	+	+
Windows 10 Enterprise-1703	-	+	+
Windows 10 Enterprise-1607	-	+	+
Windows 10 Enterprise LTSB/LTSC			

OS version	2019.2	2019.1	7.9.6
Windows 10 Enterprise 2019 LTSC	+	+	+
Windows 10 Enterprise 2016 LTSB	+	+	+
Windows 10 Enterprise 2015 LTSB	+	+	+
Windows Server			
Windows Server 2019	+	+	+
Windows Server 2016	+	+	+
Windows Server 2012 R2	+	+	+
Windows Server 2012	+	+	+
Windows Server 2008 R2 SP1	+	+	+
Windows Server 2008 SP2	+	+	+
Older Windows versions			
Windows 8.1	+	+	+
Windows 7 SP1	+	+	+
Windows XP	Support license required	Support license required	Support license required

Warning: We recommend that all our customers install our latest version.

The DriveLock Agent is available for systems based on Intel X86 (32 bit and 64 bit architecture). We recommend using a 64 bit system for the DriveLock Agent. Server operating systems are being tested on 64 bit only.

Note: Please also read the notes on the DriveLock agent update.

Restrictions

- DriveLock Disk Protection is only allowed for use with XP employed in certain ATMs.
- Windows XP Embedded: Do not install the DriveLock Virtual Channel and the DriveLock Agent on the same client!
- On Windows 7 systems with TPM, DriveLock BitLocker Management supports 64 bit systems and not 32 bit.
- Disk Protection UEFI and GPT partitioning are supported for drives up to max. 2 TB for Windows 8.1 64 bit or newer and UEFI version V2.3.1 or newer.
- Starting with version 2019.2, the agent status is a separate option and should be explicitly configured. The default setting is not to display a status.

Note: Microsoft discontinues support for its Windows 7 operating system as of January 2020. However, DriveLock will continue to support Windows 7 with a regular client license. We will notify our customers in time when Windows 7 is eligible for extended legacy support. At the earliest, this will occur after DriveLock version 2020.2.

Citrix environments

The DriveLock Agent requires the following systems to be able to make full use of the DriveLock Device Control feature:

- XenApp 6.5 Hotfix Roll Up 4 or newer (ICA).
- Windows Terminal Server 2012 or 2016 (RDP).
- DriveLock File Protection is not supported with Citrix Terminal Server.

Warning: Please note that Citrix product names have changed. Please refer to https://-docs.citrix.com/en-us/citrix-virtual-apps-desktops/1808/whats-new.html for more information(Our reference for the Citrix name change: EI-768 (INC04120))

3.2 DriveLock Management Console (DMC) and Control Center (DCC)

> Note: Make sure to install the two management components on the same computer because the DCC will access some of the dialogs provided by the DriveLock Management Console.

Before distributing or installing the DriveLock management components DMC and DCC on your corporate network, please ensure that the computers meet these requirements and are configured properly to provide full functionality.

Main memory:

- at least 4 GB RAM

Free disk space:

- approx. 350 MB

Additional Windows components:

- .NET Framework 4.5.2 or newer
- Internet Explorer 11 or newer is required for remote control connections via the DCC.

Supported platforms:

The two DriveLock 2019.2 Management Consoles have been tested and are released on the latest versions of those Windows versions which were officially available at the time of the release and which 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.

The two DriveLock Management Consoles are available for systems based on Intel X86 (32 bit and 64 bit architecture). We recommend using a 64 bit system. Server operating systems are being tested on 64 bit only.

3.3 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:

- at least 8 GB RAM

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 4.5.2 or newer

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.

Supported platforms:

- Windows Server 2012 R2 64-bit (minimum requirement for the DriveLock Operations Center)
- Windows Server 2016 64-bit
- Windows Server 2019 64-bit

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

Warning: Starting with DriveLock version 2020.1, we no longer deliver a 32-bit version of the DES.

Supported databases:

- SQL Server 2012 (minimum requirement for the DriveLock Operations Center)
- SQL Server 2014

- SQL Server 2016
- SQL Server 2017
- SQL Server 2019
- SQL Server Express 2012 or newer (for installations with up to 200 clients and test installations)

Warning: Oracle Support EOL -Starting with version 2019.1, Oracle is no longer supported as database solution. The new DOC and DriveLock 2019.2 work only with Microsoft SQL Server. All upcoming DriveLock versions will only support Microsoft SQL Server.

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

Additional restrictions in version 2019.2:

- The service account the linked DES is running with must have access to the private key of the DES certificate in the computer account.

4 Version History

The version history provides an overview of all new features, changes and bug fixes since the last DriveLock release.

4.1 Version 2019.2 SP1

DriveLock 2019.2 SP1 is a Service Pack Release.

4.1.1 New features

DriveLock Linux Agent

With release 2019.2 SP1, DriveLock supports assignment of centrally stored policies to DriveLock Agents running on Linux.

Linux support in this version is limited to blocking/allowing external devices and drives connected to the Linux clients via a USB interface. This gives DriveLock administrators the means to control the use of external devices and drives, even on DriveLock Linux Agents, so that these client computers are protected against malware attacks as well.

For more information and instructions on installation and configuration, see the DriveLock Linux Agent documentation on DriveLock Online Help.

BitLocker Management

In addition to setting a delay for decryption, you can now also disable decryption completely. The advantage of this option is that the encryption status remains the same after an update, and no decryption is required at all. This ensures that DriveLock Agents are not left in a vulnerable state for any length of time.

4.1.2 Bug fixes

Important corrections in this version

This chapter provides information about bugs fixed in this DriveLock version 2019.2 SP1.

Our External Issue numbers (EI) serve as references, where applicable.

Reference	Agent remote control
EI-749	Now you can establish a remote agent connection via the DCC independently of the applied filter.

Reference	Device Control
	The popup that was incorrectly displayed no longer appears when a new document is saved.
EI-776	The error that occurred when loading smartphones after installing DriveLock is fixed.
EI-489	The issue with Terminal Servers, which sometimes blocked unconfigured network drives, is now fixed.

Reference	Disk Protection
EI-756	Hardware compatibility issues with DELL 7400 2in1 models related to Disk Protection have been fixed.

Reference	DriveLock Agent
	Now, the request code is verified as soon as it is entered.

Reference	DriveLock Control Center (DCC)
EI-760	Reporting/Forensics: The DCC displays the ADSPath value correctly now.

Reference	Encryption-2-Go
EI-639	DriveLock Mobile for MAC OS no longer encrypts the DriveLock.app folder.
EI-643	When an encrypted USB device is used, the CPU is no longer subjected to excessive load.

Reference	File Protection
EI-825; EI-884; EI-876	Several bugs that caused the File Protection driver to crash are fixed.
EI-868	You can rename network drives now when File Protection is active.
EI-537	Now only administrators can completely decrypt centrally managed directories.
EI-628	When File Protection is the method used for USB encryption, the automatic decryption dialog now appears every time when connecting a USB drive.

Reference	Groups and Permissions
EI-791	To evaluate the group membership, the Global Catalog server is now also queried correctly.

Reference	Management Console (DMC)
	The MMC is now capable of importing very large CSV files (> 100 kB).

Reference	Licensing
	When you update a license, it is no longer assigned to all computers.

Reference	Self-Service
EI-844	The Self-service wizard no longer accepts entering times in the past.
EI-538	Self-service is stopped (after you select the respective checkbox) when the user is connected via RDP with the client computer.

Reference	Thin Clients
EI-794	The Explorer no longer crashes when used with Terminal Servers.

4.2 Version 2019.2 HF1

DriveLock 2019.2 HF1 is a Maintenance Release.

4.2.1 Bug fixes

Important corrections in this version

This chapter provides information about bugs fixed in this DriveLock version 2019.2 HF1.

Our External Issue numbers (EI) serve as references, where applicable.

Reference	BitLocker Management
	Due to a registry key that was blocked by the agent, local group policies were no longer updated properly. As a result, individual group policies were deleted and some applications may have stopped working.

Reference	Device Control
	Drive and device collection functionality was not available because the devices or drives that were collected were not correctly detected when evaluating the policies.
EI-820	The volumeID functionality for Device Control did not work correctly.

Reference	DriveLock Agent
EI-812	It is possible to reconnect to the "System Event Notification Service" on Windows 7. The Explorer error message no longer appears.

Reference	DriveLock Control Center
EI-765, EI-749	The Use FQDN for agent connection setting is available in the DCC.

Reference	Events
	You can create event filter definitions for events without parameters now.

Reference	File Protection
EI-825	Paths or file names exceeding 384 characters caused a blue screen (BSOD) in the File Encryption driver. This bug will be fixed in the next release.

Reference	Policies
EI-752	The DriveLock configuration files were loaded correctly, but the corresponding path was ignored when evaluating their policies.

4.3 Version 2019.2

DriveLock 2019.2 is a Feature Release.

4.3.1 New features and improvements

Version 2019.2 contains a large number of new functionalities and improvements. Below you will find a summary of the new features.

Application Control

With this release, we' ve added improved anti-malware capabilities by extending our white-list technology to all assets:

- Better protection against attacks without files (file-less attacks) - Ability to block specific child processes
- Application Control is now also able to control other executable files (e.g. .APPX - MSI, MST, MSP - PS1, BAT, CMD, VBS, JS, OCX, OCX)

This allows you to restrict legitimate programs (which are whitelisted) to actions and permissions that are really needed so that attacks become even more difficult. In this way you can ensure that only authorized software and scripts will be executed. In addition, you can now also control access to scripting tools (such as MS PowerShell, VBS, Python, and command line).

New application permissions offer the following benefits:

- Prevent an application (or process or script) from being started from within a permitted application which could potentially harm the system.
- Determine how a particular application should gain access (e.g. read or write access to files or the registry).

New DriveLock Pre-Boot Authentication (PBA) with BitLocker Support

Version 2019.2 introduces a new DriveLock PBA that replaces the previous DriveLock UEFI PBA. This advanced PBA works with both BitLocker and DriveLock Disk Protection encrypted drives. The new DriveLock PBA is currently only available for Windows 10 64-bit systems running on UEFI platform. A separate license is required for the new PBA for BitLocker (BitLocker PBA Add-On). This license is based on a BitLocker Management license. The following functionality is also available in this new PBA for BitLocker encryption:

- Login with user name / password
- Emergency logon with a lost password via Challenge-Response method
- Single sign-on (SSO) for Windows logon

- Login with Smartcard and eToken
- Support for other keyboard layouts and virtual keyboard
- Exchangeable PBA background images

BitLocker To Go

Another new feature is enforced encryption of external USB storage media with BitLocker To Go. You can now select BitLocker To Go as an additional encrypting option for enforced encryption.

Similar to our container encryption Encryption 2-Go, you can choose between a user password or a central administrative password for authentication. By using a central administrative password, you can ensure that data can only be accessed within the company. If a USB drive is already encrypted with BitLocker To Go, DriveLock recognizes it as already encrypted and does not re-encrypt it.

As usual, the recovery information is uploaded to the DES where it is stored centrally and securely encrypted.

Security Awareness

Security Awareness includes the following new features:

- Users are now able to select and view security awareness campaigns on demand
- Administrators can enforce a full-screen mode for displaying campaigns
- mp4 video files can be selected as content
- Administrators can monitor campaigns more effectively

Endpoint Detection & Response (EDR)

Endpoint Detection & Response technology provides full transparency and better control over endpoints. EDR automatically detects security-critical operations due to improved analytics and automation features.

Automated response capabilities are available and can be configured to respond effectively to incidents. Endpoint errors can be responded to automatically, depending on the application. We have redesigned the overall display and configuration of the DriveLock events. It is now also possible to combine several events into rules and generate security alerts from them. In addition, suitable on-the-spot response measures can be initiated on the agent to resolve the security issue.

Security alerts can be triggered based on how often events occur or when they occur - that is, they can be triggered by combining different event filters within a specific period of time.

New features in the DriveLock Operations Center (DOC)

The DOC now allows you to create additional 'out of the box' dashboards for Security Awareness, Application Control and BitLocker. All the widgets you need are already included on each dashboard, but you can arrange them as you like.

The DOC offers several new views:

- Groups: Check group memberships, add computers to groups, or control policies assigned to specific groups in this view.
- SecAware: Here you can get an overview of all campaigns and their states. In this view you also take a tour that provides a quick introduction; you can restart this tour at any time.
- EDR: You can view the various alerts and sort them by severity and category. You can monitor your endpoints continuously from the EDR view.

In addition, it is now possible to start other administrative tasks from the DOC, such as enabling or disabling agent tracing. Quick filters allow you to easily filter by specific properties.

The DOC has been completely revamped with new evaluation and display options added.

Now you can also open the DOC as follows:

- From your browser, by manually entering the URL **https://server:port** in the browser (for example: https://dlserver.dlse.local:4568)
- Select the file `DOC X64.msi` zur Installation aus. Im Startmenü wird Ihnen anschließend unter **DriveLock** der Eintrag **Operations Center** angezeigt. Alternativ dazu können Sie die `DriveLock.OperationsCenter.exe` from the DriveLock installation directory and start it manually. The DOC is opened in DriveLock's own browser-based interface.

Additional improvements in this DriveLock version

- Immediate support of data locks, such as the Koramis data lock
- Filtering of drive and device class rules is now also supported
- Increased Self-Service processing options, for example Offline Unlock even without network connection

4.3.2 Bug fixes

Important corrections in this version

This chapter provides information about bugs fixed in this DriveLock version. Our External Issue numbers (EI) serve as references, where applicable.

Reference	Agent remote control
EI-613	Agent remote control will only use secure ports for the connection.
EI-729	If SSL is enforced (or even disabled) when a policy is updated, the agent automatically disables port 6064 once the policy is updated.
EI-517	Use the new **Connect As** menu item in the DriveLock Agent context menu to set the port and usage of HTTPS. The port can also be specified in the DriveLock Control Center settings.

Reference	Application Control
EI-731	Local whitelist tray icon is displayed in Remote Desktop Session (RDP) now.

Reference	BitLocker Management
EI-666	The error when encrypting a system drive [0x8031002c] was fixed by adjusting the Group Policy registry values.
EI-740	Existing BitLocker Managed Environments (e.g. MBAM) can be used torgether with DriveLock now. To do this, the following DWORD value must be added in the registry key: `HKEY_LOCAL_MACHINE \SOFTWARE \CenterTools \DLStatus \RegProtectionLevel` (Note: without spaces!). Set the value to 1. Note that you can only change this setting after shutting down the Agent. Restart the system afterwards.

Reference	DriveLock Control Center (DCC)
EI-734	The login screen for the DriveLock Control Center has been extended

Reference	DriveLock Control Center (DCC)
	so that the German text for the user name is no longer truncated.

Reference	Device Control
EI-735	The registry key "IsAppTermServ" is no longer lost when upgrading the agent.
EI-461	File filter settings (content scanners) are now allowed for portable media devices and are no longer ignored.

Reference	Disk Protection
EI-277	Switching domains after a WOL no longer results in a domain change.
EI-231	You can now set the entry for encryption certificates to **Not configured** in the policy.
EI-579	You can now delete disk protection certificates from the file repository in the policy.

Reference	Encryption-2-Go
EI-137	You can now set the size limit for encrypted drives.

Reference	File Protection
EI-646	CSV files can be encrypted now
EI-640	The **User name and password** radio button is active now and selected by default.
EI-737	DLFldEnc no longer crashes during file copy.
EI-426	When encrypting an external hard drive with DriveLock FFE and performing a defragmentation with Windows, all files are now correctly

Reference	File Protection
	encrypted and the NTFS file system is no longer damaged.
EI-112	File protection users with read permissions can mount encrypted folders now.
EI-626	When File Protection is licensed and Encryption-2-Go is not required, you no longer get a warning or error message when configuring the whitelist rules for the drive.
EI-653	A user with DriveLock certificate will no longer receive an error when attempting to mount an encrypted folder.

Reference	Groups and Permissions
EI-570	Central File Protection group permissions no longer overwrite individual user permissions if an individual user is included in the added group.
EI-633	You can now remove AD groups from static DriveLock groups.

Reference	Management Console (DMC)
EI-96	The correct security protocol is now displayed in the GUI for the transfer between server and agent.
EI-738	A LocalHashes.dhb with 0 bytes is no longer created on the client side within the DMC (agent remote control), which led to an event error 222.
EI-321	The warning "No DriveLock Enterprise Service is available because no valid server connection is configured." no longer pops up while using the DMC.
EI-726	The device scanner now lists all scanned computers.

Reference	Policies
EI-660	The Event Log was 'flooded' with events with Event ID 362 after selecting the automatic DriveLock Agent update. We fixed this bug and improved the processing of events.
	The option **Push centrally stored policies to Agents when publishing** in the server settings now works without any errors.
EI-617	When assigning a large number of policies and checking the status using the `-showstatus` command line command, the display text was truncated. This bug is fixed now.
EI-676	If a policy is based on computer group mapping, the AD group name is now displayed in the agent user interface rather than the AD identifier.

Reference	Self-Service
EI-718	It is no longer possible to enter a time in the past in the Self-Service wizard.
EI-717	When exporting a Self-Service group to a CSV file, the special characters (umlauts such as ä,ö,ü) are now saved correctly.

Reference	Security Awareness
	Campaigns are now displayed only to users defined in the policy and not to all users.

Reference	System Management
EI-516	You can no longer enter the same port for agent remote control and HTTPS in the Remote control settings and permissions dialog.

5 Known Issues

This chapter contains known issues for this version of DriveLock. Please read this chapter carefully to avoid any unnecessary time and effort for testing and support.

5.1 License activation

At present, it is not possible to activate a license via a proxy server that requires an explicit login.

5.2 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.

Important update information:

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.

5.3 Installing Management Components with Group Policies

Note that you cannot install the DriveLock Management Console, the DriveLock Control Center or the DriveLock Enterprise Service using Microsoft Group Policies. Instead, use the DriveLock Installer to install these components as described in the Installation Guide.

5.4 DriveLock Device Scanner

You can use the Device Scanner integrated in the product in all environments where only the default tenant "Root" has been set up. This applies to most customer installations.

If you have several tenants in your environment, you will get an error message when displaying or storing the scan results.

5.5 Manual Updates

If you do not use GPO to distribute the policies, a manual update of the Agent under Windows 8.1 and higher will fail if the DriveLock Agent.msi file was started from Windows Explorer (e.g. by double-clicking) and without permissions of a local administrator. Start the MSI package in a command window via msiexec or use the DLSetup.exe file.

Updating from DriveLock version 2019.1 to 2019.2

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.

5.6 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.

5.7 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.).

5.8 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.

5.8.1 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

5.8.2 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).

5.9 DriveLock Disk Protection

Disk Protection and DriveLock Operations Center (DOC)

The DOC now correctly displays status information of hard disks encrypted with DriveLock Disk Protection version 2019.2 SP1 or higher. The inventory component displays the encryption status and the encryption method of the hard disks in the DOC.

Note: Disk Protection customers running versions up to 2019.2 are encouraged to use the DriveLock Control Center functionality to monitor their system environment.

Inplace Update to Windows 10 1903

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 counter <n> cannot be updated during the process, we recommend that you only set it to 1, so that the user logons in the PBA are required again immediately after the Windows Inplace Upgrade.

If you want to disable user logins to the PBA during the update process, reset the counter to 1, so that the automatic login only takes place once after the update and after a restart and the users must login to the PBA after that.

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 white-list 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. The UEFI mode must not be used with UEFI versions lower than 2.3.1.

The new PBA available with 2019.2 is currently only available for Windows 10 systems, because the Microsoft driver signatures required for the hard disk encryption components are only valid for this operating system.

Pre-boot authentication (PBA) for UEFI mode does not yet generically support all PS/2 devices.

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. By pressing the "k" key, you can prevent the Drivelock PBA drivers from loading once when starting the computer. After you log on to Windows on the client, you can then run the `dlsetpb /disablekbddrivers` command from an administrator command line to permanently disable the Drivelock PBA drivers. Please note that the standard keyboard layout of the firmware is loaded in the PBA login screen, which generally has an EN-US layout, meaning that special characters may differ.

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.
- On some HP PCs Windows always will be set to position one again in the UEFI boot order and the DriveLock PBA has to be selected manually from the UEFI boot menu. In this case fast boot has to be switched off in UEFI to keep the DriveLock PBA at position one.
- Windows 10 Version 1703 (Creators Update) can remove the DriveLock boot entry from the UEFI boot menu while shutting down or when hibernating. Therefore the DriveLock PBA will no longer boot at the next startup and Windows cannot boot from the encrypted system hard disk. In August 2017 Microsoft released Update KB4032188 which resolves this issue. Update KB4032188 will be installed automatically by Windows or can be downloaded manually: download link.
  Check if update KB4032188 or any later update that replaces KB4032188 is installed before you install DriveLock Disk Protection for UEFI.
  When upgrading to Windows 10 Version 1703 where DriveLock Disk Protection for UEFI is already installed, add update KB4032188 to the Creators Update before you upgrade.

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.

Workaround for DriveLock update from 7.7.x with Disk Protection with enabled PBA to version 2019.2 SP1

First, update from 7.7.x to version 7.9.x. Only then do you update to version 2019.2. Please contact our support for further questions.

5.10 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 switch off the Office synchronization, uncheck **Use Office 2016 to sync Office files that 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 (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.
- You can prevent performance drops during extensive backups to encrypted folders or large encrypted drives by disabling the check for unencrypted files on these drives. (Reference: EI-763, EI-767)

Office 365 files

If the path to the encrypted folder exceeds 128 characters, opening downloaded Office 365 files may fail. (EI-641)

eMMC Flash Memory

DriveLock does not support eMMC Flash Memory for use with File Protection. (EI-828)

Distributed File System (DFS)

DriveLock File Protection currently does not support storing encrypted folders on network drives with Distributed File System (DFS).

5.11 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.

5.12 DriveLock Mobile Encryption

DriveLock Mobile Encryption: NTFS/EXFAT

At present, container files formatted with NTFS or exFAT can only be read with the Mobile Encryption Application. We recommend using BitLocker To Go or formatting with the FAT file system.

5.13 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.

Password requirements

In Drivelock BitLocker Managment, the difference between PIN, passphrase and password is confusing for the user, we have simplified it by only using the word "password". In addition, this password is automatically applied in the correct BitLocker format, either as a PIN or as a passphrase.

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

- Minimum: 8 characters
- Maximum: 20 characters

> Warning: Note that BitLocker's own PBA only provides English keyboard layouts when using BitLocker, so the use of special characters as part of the password can lead to login problems.

Encrypting extended disks

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

Group policy configuration

If you distributed the DriveLock BitLocker configuration to the agents via group policies, you cannot set computer-specific passwords via the DriveLock Control Center because of a technical issue.

In this case, the DriveLock Agent ignores the required machine-specific policies.

5.14 DriveLock Operations Center (DOC)

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.

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. The system only updates this information at certain intervals.

5.15 DriveLock Security Awareness

Changed content for the Security Awareness Content AddOn

Starting with version 2019.1, DriveLock no longer supports Dutch campaign contents. Instead, we support French now.

> Warning: Please note that the Dutch content will be automatically deleted from the DES when updating to DriveLock 2019.1 and 2019.2.

Security Awareness on IGEL clients

Security Awareness version 2019.2 cannot be used on IGEL clients. We are working on a solution and will provide it with one of our next releases.

5.16 Antivirus

General information on Antivirus

Since DriveLock 7.8, the on-demand scanner (Cyren) will not be included any more. Customers with a valid Avira license/subscription can use the Avira scanner to scan external drives, until the subscription terminates.

Avira Antivirus

Starting with DriveLock Version 7.9, Avira Antivirus is no longer supported.

5.17 DriveLock and Thin Clients

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

- Security Awareness Campaigns cannot run within a Thin Client Session.
- The “Fill any remaining space on drives” option does not work correctly when used for encrypting a DriveLock container via a Thin Client.

5.18 DriveLock WebSecurity

DriveLock WebSecurity is no longer part of the product since version 2019.1. Customers with a valid WebSecurity license can continue using DriveLock version 7.9 until the license runs out.

6 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.

The following versions are currently subject to end-of-life:

Version	Full Support / Code Correction	Continued Customer Care Support
7.8	December 2019	June 2020
7.7	July 2019	January 2020

Full Support / Code Correction:

Shortly after a new product version is released plus 12 months. Full DriveLock product support for the previous release will continue for one full year from the release of a new product version. Critical maintenance updates will continue to be released during this time.

Continued Customer Care Support:

Continued product support will continue for 18 months from the release of a new product version. All current maintenance updates will be available. However, no new updates will be released after the Full Support has ended (12 months). Respond to inquiries via phone, email and Self-Service. Provided by DriveLock's Product Support Team and related technical assistance websites.

7 DriveLock Test Installation

You can install the DriveLock components - Agent, Management Console, Control Center, Enterprise Service and Microsoft SQL Express - all together on one computer. This allows you to test DriveLock for an initial trial with minimal hardware requirements.

Note: Please refer to our Quick Start Guide which guides you through the initial installation; you can download it from www.drivelock.help. Here you will also find information on creating a test installation and setting up an initial configuration with the Quick Start Wizard.

When you download DriveLock software from www.drivelock.de, a 30 day test license is already included. If you install DriveLock on one computer only with a local policy, you do not have to enter a license in the configuration. You can use the 30 day test license that is installed with the DriveLock Management Console (default path C:\Program Files\CenterTools\DriveLock MMC\Tools\AgentTrial.lic) if you want to test disk encryption or if you plan to install the Agent individually on different client computers and configure it using a group policy, a centrally stored policy and/or a configuration file. The test license is automatically imported to the policy you create with the help of the Quick Start Wizard.

Copyright