DriveLock Release Notes

Release Notes 2020.2

DriveLock SE 2021

Table of Contents

1 Release Notes 2020.2

The release notes contain important information about new features and bug fixes in the latest version of DriveLock. 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 formatting**. *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 set up DriveLock with 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. It is the first document after the Release Notes that you should read during a new installation.
- **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). It is intended for administrators and users who will be using the DriveLock Control Center.
  The chapter **DriveLock Operations Center (DOC)** contains an overview of the views and functionalities of the browser-based user interface.
- **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 Events**
  This documentation contains a list of all current DriveLock events with descriptions.
- **DriveLock Security Awareness**
  This manual describes the new security awareness features, which are also included in DriveLock Smart SecurityEducation.
- **DriveLock Linux Agent**
  This manual explains how to install and configure the DriveLock Agent on Linux clients.
- **DriveLock BitLocker Management**

  This manual provides a description of all necessary configuration settings and the functionality provided by DriveLock for disk encryption with Microsoft BitLocker.
  - **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 Application Control**

  As of version 2020.1, this manual replaces the Application Control chapter contained in the Administration Guide. This chapter remains available there as a reference for older versions until further notice, but is not updated anymore.

- **Microsoft Defender Integration**
  This document describes how to integrate and configure Microsoft Defender in DriveLock.

- **Vulnerability Scan**

  This document describes the new vulnerability scanning functionality, its configuration settings, and its use in the DriveLock Operations Center (DOC) and DriveLock Management Console.

2 Updating DriveLock

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

2.1 Migrating the databases

When updating from DriveLock 2020.1 (or older) to 2020.2, the two DriveLock databases are merged. The data from the DriveLock-DATA database will be migrated to the DriveLock database.

As of version 2020.2, the DriveLock-DATA database is no longer used and can be archived or deleted after migration. This applies both to the main "root" databases and to the tenant databases, if used.

If necessary, custom SQL jobs created for maintenance and backup need to be adjusted. This also applies to any queries and tools you may have created that use the DriveLock DATA.

Database Migration Wizard

The wizard is automatically started by the Database Installation Wizard after a successful update.

Warning: Make sure to back up all DriveLock databases before database migration.

- The Database Migration Wizard analyzes all DriveLock databases and checks whether data should be migrated and how much data needs to be migrated. Based on the data found, it proposes how to configure the migration.

  Note: It is possible to interrupt and resume the migration process at any time. No data is lost.

- The following data is migrated from the DriveLock-DATA database to the DriveLock database:
  - EDR categories
  - EDR alerts
  - Event data
  - Security Awareness Sessions

    Note: Any EDR categories you have created will need to be migrated to ensure EDR functionality after the update. Events, EDR alerts and Security

> Awareness Sessions can also be migrated later. We recommend that you migrate only the important data first and schedule the migration of bulk data at a time when activity is low.

2.1.1 Requirements for successful migration

Start the Database Migration Wizard as administrator so that it can access the registry area of the DES configuration and start the DES service if necessary.

Note the following for remote SQL servers:

- Database Migration Wizard uses Microsoft Distributed Transaction Coordinator (MSDTC) to ensure data integrity across databases during migration.
- For remote SQL servers, MSDTC configuration may be required.

> Note: An error message will be displayed if this step is necessary.

- MSDTC Configuration: https://docs.microsoft.com/en-us/troubleshoot/windows-server-/application-management/enable-network-dtc-access
- MSDTC Firewall Configuration: https://docs.microsoft.com/en-us/troubleshoot/windows-server/application-management/configure-dtc-to-work-through-firewalls

2.1.2 How to migrate the databases

You can keep the default options that are pre-set in the Database Migration Wizard. Changing them is recommended only in special cases.

The migration process goes through the following steps:

1. Connect to the main database
   The first step is to perform a connection test to the main DriveLock database, reading the connection data from the registry.

   > Note: In case you want to change the default settings, click the **Advanced Mode** button (see 3.).

2. Analyze the databases
   After testing the connection, the wizard analyzes the data in the databases.
   Then, it determines the connection parameters to the event databases and, if available, the tenant databases from the main DriveLock database.

The wizard checks the connection to and version of each database. The databases must be up to date to support migration.

> Note: If the version of a database is not up to date, please use the Database Installation Wizard to update the database and start the migration again.

3. Configure data migration settings
   This step is only displayed in **Advanced Mode**. Migration is configured on a per-client basis and provides the following customization options:
   - Prepare databases
     This option runs the database maintenance (index maintenance) on both databases and automatically prepares the event data to ensure a more efficient migration.
   - Migrate event data
     This option migrates the events as they can be evaluated in the reports in DCC / DOC.
     - Reprocess events after migration
       This option is necessary to create the links from the events to the other data such as computers, users, drives, devices, etc. These are displayed in DCC Forensics and DOC related entities.
       The processing of this data may take some time for larger amounts of data. When the DriveLock Enterprise Server is running, this will happen in the background.
     - Check for existing events
       Use this setting to check whether the data in the target database has already existed before the migration. This may be the case if you migrate the data at a later point in time. This option can be turned off to speed up the migration. If errors occur, we recommend repeating the migration and checking the data. In case an error occurs, no data will be lost.
   - Migrate security awareness session data
   - Migrate EDR categories
   - Migrate EDR alerts data
   - Processing batch sizes
4. Database migration processing

- The databases are migrated one after the other, depending on the tenant. You can stop the migration and start it again. The output shows the progress of the migration.
- Migrated data is deleted from the source database (here the event database).
- After successful migration, the DriveLock Enterprise Service is started again.

> Note: When the migration is finished, the event databases are no longer needed and can be archived or deleted.

2.2 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 afterwards.
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.

2.3 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 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 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.

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.

2.3.1 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.

2.3.2 Updating DriveLock Disk Protection

After updating the DriveLock Agent, any existing FDE installation will be automatically updated to the latest version without re-encryption. After updating the FDE, a restart 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.

2.4 Manual Updates

If you do not use GPO to distribute the policies, a manual update of the agent on Windows 8.1 and later fails if `DriveLock Agent.msi` was launched from Windows Explorer (e.g., by double-clicking) and without permissions of a local administrator. Start the MSI package from an administrative command window via `msiexec` or use `DLSetup.exe`.

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.

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.

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	2020.2	2020.1	2019.2
Windows 10 Pro			
Windows 10 20H2	+	+	+
Windows 10-2004	+	+	+
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 20H2	+	+	+
Windows 10-2004	+	+	+

OS version	2020.2	2020.1	2019.2
Windows 10-1909	+	+	+
Windows 10-1903	-	+	+
Windows 10-1809	+	+	+
Windows 10-1803	+	+	+
Windows 10-1709	-	+	+
Windows 10-1703	-	-	-
Windows 10-1607	-	-	-
Windows 10 Enterprise LTSB/LTSC			
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	+(*)	+(*)	+

OS version	2020.2	2020.1	2019.2
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
The following Linux derivatives and newer versions (own DriveLock license)			
CentOS Linux 8	+	+	+
Debian 7	+	+	+
Fedora 31	+	+	+
IGEL OS starting with version 10	+	+	+
Red Hat Enterprise Linux 5	+	+	+

OS version	2020.2	2020.1	2019.2
SUSE 15.1	+	+	+
Ubuntu 18.04	+	+	+

(*): Please see the important note in the Supported Platforms section.

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

Note: For more information about the Linux client and the limitations of its functionality, please refer to the separate Linux Agent documentation.

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.

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!
- BitLocker Management is only supported on Windows 7 systems with TPM and only for 64 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.
- DriveLock Disk Protection is available for Windows 10 Version 1703 and higher (see Known Issues).
- 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 7.15 or newer (ICA).
- Windows Server 2012 R2 or 2016 (RDP).
- Creating DriveLock File Protection encrypted folders on Terminal Service is not supported.

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 2020.1 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 / 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 4.5.2 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.

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)

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

- 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:

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

- SQL Server 2012 (minimum requirement for the DriveLock Operations Center) or newer
- SQL Server Express 2014 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 only works 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.

3.4 DriveLock Operations Center (DOC) Application

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

Note: The DriveLock Operations Center can also be started as a Web application via a browser. It is not necessary to install the DOC application (DOC.exe).

Main memory:

- at least 4 GB RAM

Free disk space:

- approx. 250 MB

Additional Windows components:

- .NET Framework 4.5.2 or newer

Supported platforms:

The DriveLock Operations Center application has 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 DriveLock Operations Center is only available for Intel X86-based 64-bit systems.

3.5 DriveLock in workgroup environments (without AD)

DriveLock can also be used without Active Directory. Please note the following:

- The rights and roles concept for the administrators / helpdesk staff can only be established from local users
- It is not possible to assign policies and whitelist rules to AD groups, AD users, AD OUs, but only to local objects (computer names and users).
- The name resolution must be working because DriveLock Control Center (DCC) accesses the clients via the NETBIOS/FQDN name (which is important for helpdesk activities).
- If DNSSD is disabled, you have to know your clients in detail as there is no AD inventory.
- In workgroup environments, logging in to DriveLock Operations Center (DOC) is not possible (this only works with an AD account)
- Agent remote control can be used to access clients (incl. Push Install) only if all clients are installed with a default administrative user
- In this context, it is common to have environments without a DES Server (only DriveLock Agent with local configuration) or DES Servers that distribute a configuration file via HTTP web server

4 Version History

The version history contains all changes and innovations since the last major release, DriveLock Version 2020.1.

4.1 Version 2020.2

DriveLock 2020.2 is a Feature Release.

4.1.1 New features and improvements

Version 2020.2 comes with many new features and improvements.

DriveLock Management Console

- Configuration filters: You can create configuration filters based on the computers, users or times parameters. These parameters were previously only configured once per policy and can now be used multiple times in different settings of a single policy.

DriveLock Enterprise Service (DES)

- The ChangeDesCert.exe tool checks whether the certificate used so far by the DES exists in the system; it displays a warning when selecting the option to generate a new certificate.
  By default, the DriveLock Enterprise Service Setup offers to continue using the previously used certificate if it exists in the system.

DriveLock databases

- The two separate DriveLock databases are merged into a single database with the help of the Database Migration Wizard.

DriveLock Application Control

- Configuring application rules has been simplified, individual rule types (path, owner, hash) are now combined with each other by means of a new rule type (file properties rule).

> Note: If you have been using one or more of these individual rules in a policy in an older DriveLock version (before 2020.2), they are automatically converted to a file properties rule, taking over the properties set in each rule. However, the file properties rules are only compatible with pre-2020.2 DriveLock Agents, if the property combinations in the new rule exactly match the corresponding property options from the old rule types.

Microsoft Defender Integration

- Users can delay the execution of a Defender scan.
- Microsoft Defender can be disabled for a limited time via temporary unlock.

DriveLock BitLocker Management

- Now only numbers can be used for the BitLocker PBA. On systems with TPM, it is also possible to enter 6 digits instead of the usual 8.
- Users can delay the encryption with BitLocker.

DriveLock Pre-Boot Authentication (PBA)

- DriveLock PBA now also supports CardOS 5.0 / 5.3 smartcards with the standard DriveLock middleware profile PKCS#15.

DriveLock Operations Center (DOC)

- The DOC user interface has been optimized and list views and temporal displays now have new functionalities that allow more flexibility in selecting data.

DriveLock Endpoint Detection & Response (EDR)

- The agent can send the events of other event providers (e.g. Windows Eventlog or third-party products) to the central DES. These can also be used with alerts (EDR) and consolidated with other events.
- You can also add predefined application rules based on MITRE ATT&CK®.

Vulnerability Scan

- The vulnerability scan can be started via the agent remote control.

4.1.2 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	Device Control
EI-1228, EI-1235, EI-1236	The definition of Office file formats has been extended based on the respective specification.
EI-1220	The custom message is now displayed instead of the default message when an Apple device has been blocked by a base rule.
	Fixed a bug in the DriveLock file system filter driver that caused a BSOD when inserting a USB stick.

Reference	Disk Protection
	The uninstallation of the DriveLock Agent will abort if DriveLock Disk Protection is installed on the system. The user will see a corresponding message that DriveLock Disk Protection must be uninstalled before the DriveLock Agent can be uninstalled. Up to now, the DriveLock Agent uninstallation failed without any error messages in this case.

Reference	DriveLock Agent
EI-1137	Fixed an issue where DriveLock blocked Google drives.
EI-815	In the Application Whitelist display, a column has been added to

Reference	DriveLock Agent
	show the hash of each file to get a better overview.
EI-769	Fixed a bug where Japanese could be selected as the language for the agent user interface. Japanese is no longer supported.
EI-1179	Changing the network location did not immediately reconfigure MQTT. As a result, at times the agent could not be reached via agent remote control.
EI-1179	When switching between different DES servers, agents could temporarily not be reached via MQTT because they received the wrong server certificate for MQTT communication from the DES.
EI-1065	Filters on AD groups and AD OUs sometimes only worked correctly if there was a connection to the AD.
EIs: 1066, 1075, 1080, 1090, 1116, 1156	A number of improvements have been made to the update mechanism.
EI-1182	Agent remote control via the DES sometimes failed if the agent was connected to a Linked DES and remote control was only possible via MQTT. This happened when the user running the Linked DES did not have rights on the central DES.
EI-932	Fixed a bug where a Drivelock Agent installed with unstoppable mode sometimes ended up in an inconsistent state.

Reference	DriveLock Enterprise Service (DES)
	Up to now, it was possible to run DriveLock Enterprise Setup without providing a certificate. This bug is fixed now. You must either select a certificate or explicitly specify to generate a new one.
EI-1095	The password for the DES user can now contain a semicolon. Formerly passwords like this terminated the DES setup.
EI-1122	Fixed an issue when adding licensed computers to the server.
EI-1097	The description (AD) of the computer is now saved correctly in the inventory.
EI-1197	Fixed a bug when configuring policy assignments to very long OU names.
EI-1171	The Database Installation Wizard now detects the configured Client SecurityProtocol settings (TLS).
EI-1246	The database installation wizard now recognizes settings from linked DES and makes the appropriate preselection.
EI-1164	Fixed an issue regarding the evaluation of the certificate revocation list.
EI-1202	Improved performance when processing AgentAlives (agent status message) and when saving events.

Reference	DriveLock Management Console
EI-1049	The DMC sometimes displayed computers with the name of the previous entry in the Agent remote control node.
EI-1150	Fixed a bug with license activation via proxy in the DMC. The DMC uses proxy settings that are set via Internet Explorer. The proxy entered via the DriveLock command `setproxy` is not taken into account.
EI-1133	While saving a GPO, an error sometimes occurred that a path could not be found.
EI-1135	When saving a GPO, an error sometimes occurred that the user did not have sufficient rights.
EI-1151	While working in the DriveLock File Protection node, the root tenant was always preselected in some dialogs instead of the tenant that was actually being used.

Reference	DriveLock Operations Center (DOC)
	You can reset filters set via a context menu command only in the main view. In other views you need to click 'Refresh' to reset the filters.

Reference	DriveLock Pre-Boot Authentication
EIs: 1103, 1106, 1110, 1138,	A workaround has been implemented for some issues with internal keyboards in the PBA.

Reference	DriveLock Pre-Boot Authentication
1160, 1170, 1178	
EI-1218	Single sign-on via DriveLock PBA failed when a user's password was changed outside DriveLock and SafeGuard file encryption (credential provider) was also present on a system.

Reference	EDR
EI-1241	The events, which were generated when no connection to the DES was possible, were not sent to the DES afterwards in all cases.
EI-1240	Event 257 (file deleted) was not generated in all cases.
EI-1154	Fixed an issue in the wording of event 474.

Refer-ence	Encryption-2-Go
EI-1204	Since Windows 10, Windows notifies a user unlock as a new logon and not as an unlock. In conjunction with the DriveLock PBA and Enc2Go, for example, this cancels a backup that is currently running. In order to identify an unlock as a user unlock again, you have to set the following GPO: Windows Registry Editor Version 5.00 • ; Computer Configuration -> Windows Settings -> Security Settings ->

Refer-ence	Encryption-2-Go
	• ; Local Policies -> Security Options "Interactive logon: Do not display last user name" • ; Set to "Enabled": asks to unlock the machine only to currently logged user • ; https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/interactive-logon-do-not-display-last-user-name • [HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System] • "dontdisplaylastusername"=dword:00000001

	File Protection
EI-1146	The memory loss has been fixed.
	The code has been extended to allow copy/move to root share.
EI-1111; EI-1279	Sophos SAVSERVICE.EXE is handled as a backup app.
EI-1159	When shutting down the computer, the FFE driver could not always be removed because Windows terminated the DriveLock service prematurely.
EI-1143	Fixed an issue with copying Outlook messages to the network.

Reference	Configuration (policies)
EI-1005	Now, the agent no longer evaluates Group Policy Objects if there are centrally stored policies or configuration files available.

Reference	Licensing
EI-1192	In the File Protection trial license provided, the number of File Protection licenses was 0 instead of 10.
EI-1099	Even with a valid license, a warning was briefly displayed when you opened a policy in the DMC indicating that you were "only" working with a test license.

Reference	Security Awareness
EI-1057	The Security Awareness view in DriveLock Operations Center (DOC) is now always displayed, regardless of the license check.

5 Known Issues

This chapter contains known issues for this version of DriveLock. Please read this information thoroughly as it will help you avoid unnecessary trial and support efforts.

License activation

At present, it is not possible to activate a license via a proxy server that requires an explicit login. In this type of environment, you can use our activation by telephone.

5.1 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.

5.2 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.

5.3 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.

5.4 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

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).

Applying a local policy

Some settings are not applied correctly when you save or export a local policy, and therefore may not provide the expected results when you test these settings on individual computers. Therefore, please use one of the other configuration options (configuration file, group policy, or centrally stored policy) that are not affected by this limitation for your testing.

5.5 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.).

5.6 DriveLock Disk Protection

Disk Protection and DriveLock Operations Center (DOC)

The information about the status of encrypted hard disks in the DOC does not show the proper values if the hard disks have been encrypted with DriveLock Disk Protection rather than BitLocker. Up to and including DriveLock 2019.2, we recommend that Disk Protection customers use DriveLock Control Center functionality to monitor their system environment.

Up to and including DriveLock 2019.2, we recommend that Disk Protection customers use 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 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. 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.

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.

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

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.

5.7 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 (DLFldEnc.sys).

Accessing encrypted folders

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

Cancel folder encryption

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

File Protection and USB drives

- You cannot use DriveLock File Protection to fully encrypt a connected USB drive if the drive already contains an encrypted folder. In this case the following message appears “Cannot read management information from the encrypted folder".

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. . Access to the folder mapped as a drive is denied if the DFS reference member is not selected for the mapping.

5.8 DriveLock Pre-Boot Authentication

In order to use the network functionality of the DriveLock PBA, hardware should support the TCP4 UEFI protocol. For this reason, some systems may cause issues if the UEFI BIOS does not support the required network connections.

This is the case for the following system: Fujitsu LifeBook E459. (EI-1303)

5.9 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.

5.10 DriveLock Mobile Encryption

DriveLock Mobile Encryption: NTFS/EXFAT

The DriveLock Mobile Encryption (Encryption-2-Go) cannot be used for NTFS/EXFAT containers.

5.11 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 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 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.

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.

5.12 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 other computers 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.

Do not start installation of DOC.exe while performing disk encryption with File Protection

Be sure to avoid installing DOC.exe on a hard disk that is being encrypted with File Protection at the same time. (Reference: EI-1025)

View settings in the DOC

Due to optimized DOC views in the new version 2020.2, user-defined view settings may need to be reconfigured when updating from version 2020.1.

5.13 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.

5.14 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.

5.15 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.

5.16 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.

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

Version	Continued Customer Care Support
7.9 and 2019.1	EoL December 2020
2019.2	May 2022
2020.1	December 2021
2020.2	May 2023

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.

During this period, we will release maintenance updates and code fixes for bugs and critical issues. 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.

7 DriveLock Test Installation

You can install DriveLock - the Agent, Management Console, Control Center, Enterprise Service and Microsoft SQL Express - 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