DriveLock

Release Notes 2020.1 HF3

DriveLock SE 2020

Table of Contents

1 Release Notes 2020.1 HF3

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). It is intended for administrators and users who will be using the DriveLock Control Center.
  The manual also contains a brief introduction to the **DriveLock Operations Center**.
- **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 Clients**
  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 Management**
  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. It will be available soon.

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 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.

2.2 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.

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	2020.1	2019.2	2019.1	7.9.6
Windows 10 Pro				
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 10-2004	+	+	-	-
Windows 10-1909	+	+	+	-
Windows 10-1903	+	+	+	-

OS version	2020.1	2019.2	2019.1	7.9.6
Windows 10-1809	+	+	+	+
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	2020.1	2019.2	2019.1	7.9.6
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	Support license required
Linux Derivate (own DriveLock license)				
CentOS Linux 8	+	+	-	-
Debian 7	+	+	-	-
Fedora 31	+	+	-	-
IGEL OS starting with version 10	+	+	-	-

OS version	2020.1	2019.2	2019.1	7.9.6
Red Hat Enterprise Linux 5	+	+	-	-
SUSE 15.1	+	+	-	-
Ubuntu 19.10	+	+	-	-

Please note the important note in the Supported Platforms section.

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

Note: For more information about the Linux client, refer to the Linux documentation that is available separately.

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 Terminal Server 2012 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):

- 18082 and 18083: These two ports should not be used by other server services, but they don't have to be accessible from the 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.

4 Version History

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

4.1 Version 2020.1 HF3

DriveLock 2020.1 HF3 is a Maintenance Release.

4.1.1 Bug fixes

Important corrections in this version

This chapter provides information about bugs fixed in this DriveLock version 2020.1 HF3.

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

Reference	DriveLock Agent
EI-1147	Improved access time to network shares if detailed information is not needed.
EI-1123	Fixed an issue that occurred with Novell eDirectory when using agent remote control.
EI-1084	After retrieving the recovery key, it was not replaced in some cases after the reboot. If you had to enter a password after rebooting, the password dialog was not displayed either.
EI-1117, EI-1145	The file system filter blocked too much.

Reference	Application Control
EI-1124	The **Trusted process (allow this executable as well as all child processes)** option was grayed out. It is now available again in the standard application control without predictive whitelisting.

Reference	BitLocker Management
EI-1100	BitLocker Management could not automatically unlock data partitions after rebooting a computer with the Fast Startup option enabled in Windows 10.
	Changing the system drive password at a later time failed for BitLocker-encrypted computers without a TPM.

Reference	Device Control
EI-1118	The file system filter driver was changed to prevent blocking of devices.
EI-1155	Improved detection of CD/DVD burners.
EI-1121	The policy's tenant name is now sent with the policy so that no error occurs when reading device information from the remote client.

Reference	Encryption-2-Go
EI-1107	The file system filter driver was changed to prevent blocking of devices.

Reference	DriveLock Enterprise Service (DES)
EI-1095	The password for the DES user can now contain a semicolon. Formerly passwords like this terminated the DES setup.
EI-1136	Fixed an issue that occurred when starting the DriveLock Enterprise Service when a large number of unprocessed events existed in the database.
	Fixed an issue where the DES setup wrote an incorrect log file.

Reference	File Protection
EI-1051, EI-1064	Whenever DriveLock detects a change in the loading order of the file system filters that affects the DriveLock File Encryption driver, this change is now corrected and File Encryption will request a reboot.

Reference	DriveLock Management Console
EI-1139	Fixed an issue with whitelist rules, where DriveLock did not properly store the comments for the allowed serial numbers in the policy, so they were not displayed after reopening the policy.

Reference	Microsoft Defender
EI-1114	It was not possible to configure the settings for Microsoft Defender, they always remained at " Not configured ".

Reference	Network Pre-Boot Authentication
EI-1134	A network PBA login was not possible in the time between 18:12h and 24:00h (UTC). The required timestamp was calculated incorrectly.

Reference	Self-Service
	Non-standard ASCII characters can be used again when specifying a reason for self-service.

4.2 Version 2020.1 HF2

DriveLock 2020.1 HF2 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 2020.1 HF2.

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

Reference	DriveLock Pre-Boot Authentication
	Fixed an issue where the user was prompted to enter a BitLocker recovery key in certain situations after logging in to DriveLock PBA.

4.3 Version 2020.1 HF1

DriveLock 2020.1 HF1 is a Maintenance Release.

4.3.1 Important update information:

Inventory

As of version 2020.1 HF1, the inventory is available in the product regardless of the license type and can be enabled via the **Inventory and vulnerability scan** policy setting. Since this feature may increase data traffic, you can limit the time period for collecting inventory data.

Vulnerability scan

- The vulnerability scan requires an installation of version 2020.1 HF1 to be fully operational. The same version has to be installed on DriveLock Agents as well.
- Windows version 8.1 or higher is required for vulnerability scanning.

4.3.2 Bug fixes

Important corrections in this version

This chapter provides information about bugs fixed in this DriveLock version 2020.1 HF1.

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

Reference	Application Control
	If you selected the **Set to configured list** option in the **Directories learned for the local whitelist** dialog and excluded a folder, a blank entry appeared (blank entries or first characters missing).
	Folders for application rules were only visible at the top level after restarting the MMC - subfolders at a lower level were still there but no longer visible.

	Device Control
EI-1070	In some configurations, a script was able to access a drive within milliseconds after it was mounted. This bug is fixed now.

Reference	DriveLock Control Center (DCC)
EI-1055	OU filters configured for users now also work for event reports.

Reference	DriveLock Enterprise Service (DES)
	The DriveLock Service account no longer requires administrator rights on the Linked DES.

Reference	DriveLock Management Console
	The policy's tenant name is now submitted to prevent errors when reading drive information from the remote client.

	DriveLock Operations Center (DOC)
	Displaying a computer in the Computer Details view of the DOC did not work correctly (server error) if the OU name or path contained a single inverted comma.

Reference	DriveLock Pre-Boot Authentication
	Error handling has been improved when installing DriveLock PBA.

Reference	DriveLock Pre-Boot Authentication
	When changing the logon methods for pre-boot authentication, the PBA was sometimes not installed correctly.
EI-1071	Some MMC settings for the DriveLock PBA were not saved correctly. This affects the " User Synchronization" and "Users" tabs.
	The bluescreen after PBA logon to the encrypted computer (Windows 10 2004 BIOS) no longer appears.

Reference	File Protection
EI-1053	The "[DriveLock File Protection]" menu item can now be disabled via the DriveLock Agent's system tray icon.
EI-1064	File & Folder Encryption in combination with Full Disk Encryption may produce a bluescreen BugCheck 7F, {8, ...} after a Windows Inplace Upgrade. The Windows Inplace Upgrade changes the FFE driver load order. This is corrected during the first boot after the Upgrade, but the bluescreen may occur once.

Reference	Microsoft Defender
	When you set a specific day of the week for the Defender Scan, the next day of the week appeared (e.g. Friday instead of Thursday). However, the actual weekday was saved and evaluated.

4.4 Version 2020.1

DriveLock 2020.1 is a Feature Release.

4.4.1 New features and improvements

Version 2020.1 comes with many new features and improvements.

- New: DriveLock Vulnerability Scan (starting with version 2020.1 HF1)
- New: Network capabilities of the DriveLock pre-boot authentication with direct login to Active Directory
- New: Self Service Portal for end-users who forgot their access data for logging on to the PBA
- New: Full management of Microsoft Defender Antivirus is integrated into DriveLock
- DriveLock Operations Center includes many new views, reporting and management features
- Additional security features and automatic configuration options in DriveLock's Application Control including automated learning of application behavior

Please find below a brief overview of the new features.

Microsoft Defender Management

Microsoft Defender Antivirus lets you configure various settings to protect against malware, including some advanced options for running programs. By integrating it into DriveLock, you only need the DriveLock Management Console to configure this feature. This not only makes it easier to implement, but also to combine it with the powerful security features of DriveLock Application Control. When combined with the DriveLock interface control, unlocking external drives for users is linked to the outcome of a detailed scan: If Microsoft Defender Antivirus detects malicious software, the drive is not unlocked. And you can increase automation with DriveLock Endpoint Detection and Response. For example, when Microsoft Defender Antivirus detects a threat, you can use a script to shut down the computer or display a DriveLock security awareness campaign showing the next steps.

One of the new views in the DOC also includes Microsoft Defender Antivirus status reports on the latest threats and the status of the clients. A redesigned user interface, new filter functions, a graphical representation of the security status and enhanced navigation in the DOC provide administrators with a better overview of existing threats in their company. Any threats detected are more accurately analyzed and, if necessary, false or irrelevant noti-

fications can be suppressed altogether. This ensures that administrators are not distracted by irrelevant messages and can concentrate on other tasks.

Vulnerability Scan

> Warning: In order to run the vulnerability scan, you must have version 2020.1 HF1 installed (also for the DriveLock Agent).

The new vulnerability scan automatically scans a computer system on a regular basis for known Windows vulnerabilities. Here we have access to a database that is updated several times a day. DriveLock Operations Center (DOC) then displays the findings in a separate new view with a risk and impact assessment, including missing patches, outdated software or libraries of known vulnerabilities. This will allow security teams to evaluate the security level in the company more accurately and set automatic notifications based on the evaluations.

DriveLock Operations Center

When you launch the DriveLock Operations Center, you will notice the redesigned interface and expanded navigation area. It is now more intuitive and easier to use, allowing you to complete your tasks quickly and easily.

Information about individual computers is now clearly arranged on one large page. You can also customize the individual views for each user. At the same time, the charts also provide intuitive filtering and drill-down to the important data.

A role-based permissions model allows for an advanced security design tailored to the organizational structure. What's unique: You can also configure the type of data a user may see within the DOC. Users holding different roles only see the computers and related data associated with their responsibilities.

Pre-boot authentication (PBA) with network capabilities

DriveLock's network pre-boot authentication offers customers entirely new application scenarios. Provided the computer is directly connected to the company network, users can now log on to the Active Directory directly and without prior synchronization. This eliminates the need for provisioning, especially for multi-user laptops. And in an emergency, a different user can log on to an encrypted computer. In combination with DriveLock hard disk encryption, "Wake-On-LAN" with automatic software distribution in a company can be easily implemented and even provides easy and efficient theft protection for stationary systems.

Web-based Self-Service Portal

Another new feature is the DriveLock Self-Service Portal for end users. Users can access the Self-Service Portal 24/7 from a standard browser, which is also available on all smartphones. Provided they answer three predefined questions correctly and enter an additional TAN, they can identify themselves here even without a password.

Application Control

With its improved application control, DriveLock is designed to facilitate the daily work of administrators. The configuration does not require extensive knowledge about the behavior of individual applications, for example, knowledge about the libraries these applications call or the directories they write data to. DriveLock manages all of these tasks by learning the behavior of the application by means of temporary monitoring. During this process, the application or folder that has been previously specified, is automatically monitored over a period of time to see which actions the application is executing. From this data, the administrator can generate corresponding application permissions. This prevents unusual behavior immediately and ensures that users cannot bypass existing security measures. In addition, users can be alerted precisely at the point when an application tries to execute something unexpected. It is possible to send out simple messages or even start a security awareness campaign. Apart from increasing transparency, it also helps to ensure that users behave in a more security-conscious manner and keep learning as they do so.

Additional improvements in this DriveLock version

- Assigning security awareness campaigns to users is now easier, and campaigns that have already been run will not be repeated even if the user changes computers.
- In the DOC, users can check the current status reports for Disk Protection and start the emergency login for individual computers directly from the computer view.
- In the DriveLock Management Console, we have merged the two views of the currently available DriveLock MSI packages into one.
- You can now disable a policy assignment to a group of computers; it is no longer necessary to delete the assignment.
- The same applies to drive whitelist rules, which can now be easily enabled or disabled.
- BitLocker To Go also provides additional options that determine the visibility of BitLocker To Go start menu, context menu, or tray icon menu items for users.
- For troubleshooting, you can temporarily disable or adjust BitLocker's encryption settings for individual computers.

- The Management Console and Control Center can use DriveLock user accounts from the DOC for permissions.
- We have optimized the layout and startup behavior of the DriveLock PBA and implemented an improved driver for keyboard and mouse support.

4.4.2 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	BitLocker Management / DriveLock Pre-Boot Authentication
EI-891	In the overview for hard disk encryption, you found that Pre-Boot Authentication was shown as disabled even though the BitLocker PBA option was selected.
EI-872 , EI-989	Whenever possible, the firmware keyboard driver is now replaced by a newer driver that supports layouts.
EI-946	The credential provider for the NetIQ Client Login Extension did not work correctly with DriveLock on Windows 10. Users were not added to the Pre-Boot Authentication.

Reference	Device Control
EI-453	When adding a new file type definition, a false warning appeared that a file type definition already existed for this type.
EI-819	Drive and device collections were no longer stored in the policy and thus could not be used any more.
EI-540	Burning devices are now more easily identified and burning is enabled for users with write access to CD/DVD-ROM.
EI-776	The MTP driver dependencies that prevented the MTP driver from loading have been removed.

Reference	Device Control
EI-859	A misleading message regarding the release status of an iPhone is no longer displayed.

Reference	Disk Protection
EI-915	A new PS2 combined keyboard/mouse driver replaces keyboard drivers. The splash screen has been adjusted. Keyboard layout list shortened and re-sorted. ESC key now not only closes open menus, but activates the F1 key function (password login).
EI-756	Corrected the SSO data transfer behavior (BSOD) on several Dell notebooks.
EI-995	SSO for token logon is defined in DriveLock Credential Provider.
EI-914	If a license was removed from a Disk Protection or BitLocker management policy that requires separate installation steps and these steps have already been performed, DriveLock Agent displayed incorrect behavior. This bug is fixed now.

Reference	DriveLock Control Center (DCC)
EI-721	Fixed an error in the display of the license information.
EI-997	Fixed an error when loading the DCC helpdesk, that occurred with a large number of computers with FDE recovery data.

Reference	DriveLock Control Center (DCC)
EI-749	In the DCC Helpdesk, it was not possible to connect to an agent in a filtered list if the agent did not appear in the list.

Reference	DriveLock Enterprise Service (DES)
EI-896	The ChangeDesCert utility now also works correctly if a certificate was selected several times in a row with the menu command "Select".
EI-931	The DES (MQTT) will no longer attempt to listen to port 8083 and 8084. To reduce conflicts, port 18082 is now used instead of port 8080. This port is only used locally.
EI-977	Caching improves the performance when the agent on the DES requests configuration settings for agent remote control (MQTT).
EI-773, EI-998, EI-754	Improved performance of DES (alive and event processing)
EI-1024, EI-977	Fixed the error in the DES or MQTT configuration that caused increased load on the DES computer.
EI-874	Fixed the error in the DES that resulted in significantly increased memory consumption when listing many policies.
EI-937	Fixed an error when processing file access events with long path names.

Reference	DriveLock Operations Center (DOC)
EI-907	The DOC now allows login of users from child domains and domains linked via Forest Trust.
EI-922	The menu command to start the DOC from the DCC now works even if the DES server has a very long FQDN (fully qualified domain name).
EI-1000	You can solve the issue by using Microsoft Edge version 81.0.416.64 (official build) (64-bit).
EI-1006	It is now possible to group DriveLock agents by means of the Disk Encryption Status property.

Reference	Encryption-2-Go
EI-506	DriveLock Mobile Encryption (Encryption-2-Go and File Protection) can now be used on Apple OS X and Mac OS X without restrictions.
EI-761	Version 2020.1 includes a workaround for FAT 32 which solves the described issue.

Reference	File Protection
EI-763, EI-767	The driver was revised to solve potential synchronization problems.

Reference	File Protection
EI-941	Fixed the issue related to downloading Office 365 files to encrypted folders with pathnames > 128 characters.
EI-825	Replaced limiting static memory allocation by dynamic memory allocation in the driver to avoid problems with long file names.
EI-952	The unmount required to delete an encrypted folder was completely unsynchronized. This is fixed now.
EI-953	The unmount required to rename an encrypted folder was completely unsynchronized. This is fixed now.
EI-954	The unmount required for decrypting was missing and is now performed.
EI-955	The unmount required for copying and moving was missing and is now performed.
EI-956	The settings for the shell extensions are now evaluated correctly.
EI-537	Improved detection of centrally managed encrypted folders.
EI-940	The event variable CloudId, which was not initialized, is now initialized.

Reference	Configuration
EI-752	The DriveLock Agent is now able to successfully work with policy configuration files (.cfg) on UNC paths.

Reference	Configuration
EI-803	It did not work to configure the system using the configuration file.
EI-398	Policies without license information could affect the license information.

Reference	Management Console
EI-999, EI-990	Loading the policy assignments in the Management Console was too slow.
EI-827	When adding new licenses in the Management Console, newly added modules were automatically activated for all computers.
EI-719	Text in the Management Console that was too long was simply cut off when previewing contact information for the Offline Unlock Wizard.
EI-864	The Management Console now uses the proxy configured in the Internet Explorer settings for accessing the Internet.

Reference	Mobile Encryption
EI-643	Improvements for the encryption driver were already implemented in version 2019.2.
EI-639	DriveLock MAC applications are no longer encrypted on Windows computers.

Reference	Self-Service
EI-538	Self-service on the agent is now terminated as configured when a user logs off in an RDP session.
EI-762	The icons for the wizard banners must have a size of 49x49 pixels - since they were only 48x48 pixels before, white lines were added to the images.
EI-724	When using the Offline Unlock Wizard, you could jump to the next page even if you had not yet selected any modules to be unlocked.
EI-867	Beim erstmaligen Erreichen der Dialogseite, auf der die Dauer der Deaktivierung von Richtlinieneinstellungen gesetzt wird, wurde bisher die aktuelle Uhrzeit eingetragen. When moving back and forth one page, a time from the past would appear on the dialog page. Now, each time you access the page, the current time is entered, incremented by the maximum allowed unlock period.
EI-759	In some cases, the temporary unlock of the agent failed with "Access to DriveLock agent denied".
EI-991	The self-service unlock does not work on computers that have been identified by the OU.

Reference	Security Awareness
EI-810	Built-in pictures of Security Awareness were only available in English.

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.

5.1 Licensing

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

Wenn zur Verteilung der Richtlinien nicht GPO verwendet wird, schlägt ein manueller Update des Agent unter Windows 8.1 und höher fehl, sofern `DriveLock Agent.msi` aus dem Windows Explorer (z.B. per Doppelklick) und ohne Berechtigungen eines lokalen Admin-

istrators gestartet wurde. Starten sie das MSI-Paket aus einem administrativen Command Fenster per `msiexec` oder nutzen Sie `DLSetup.exe`.

Updating from DriveLock version 2019.1 to 2019.2

Wird ein Client-Update manuell über das Starten von `msiexec` oder `DLSetup.exe` durchgeführt, kann es vorkommen, dass sich der Windows Explorer nicht korrekt beendet. 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.

5.9 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

5.10 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).

5.11 DriveLock Disk Protection

Different encryption products

- Do not deploy DriveLock Disk Protection alongside other (third-party) disk encryption products. If a third-party product is already installed on a DriveLock Agent, do not assign a policy with Disk Protection settings or license to it.

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.

eMMC Flash Memory

- DriveLock Disk Protection (Full Disk Encryption) does not support eMMC flash memory storage devices. (Reference: EI-828)

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

1. Decrypt drive C:
2. Update Windows 10 from 1709 to 1903
3. Encrypt drive C:
   (Reference: EI-686))

Requirements for Disk Protection:

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

Restart after installation of PBA on Toshiba PORTEGE Z930:

- 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. (Reference: EI-751))

Workaround for DriveLock update from 7.7.x with Disk Protection with enabled PBA to the most current version of 2019.2

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

5.12 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.

eMMC Flash Memory

- DriveLock File Protection does not support eMMC flash memory storage devices. (EI-828)

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.

Create a new file in a folder that was previously deleted

- Continued access to a folder after an unsuccessful unmount can lead to unpredictable behavior. We recommend closing open files and retrying the unmount.
- Unmounting an empty encrypted folder fails

Decrypting an encrypted folder

- Once the decryption of an encrypted folder failed due to open files, it will not be possible to decrypt the folder at all, even after the open files are closed. To get around this, unmount the folder manually before running the decryption wizard again.

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)

- In general, DriveLock File Protection also supports storing encrypted directories on network drives with Distributed File System (DFS). However, since DFS and the underlying

storage system may have customer-specific characteristics, we recommend that you thoroughly test encrypted directories before using them.

5.13 DriveLock Pre-Boot Authentication

The DriveLock PBA does not accept and handle the EURO-sign "€" that a German keyboard provides when pressing the combination "Alt Gr" and "e".

5.14 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.

5.15 DriveLock Mobile Encryption

DriveLock Mobile Encryption: NTFS/EXFAT

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

5.16 BitLocker Management

Different encryption products

- Do not deploy DriveLock BitLocker Management alongside other (third-party) disk encryption products. If a third-party product is already installed on a DriveLock Agent, do not assign a policy with BitLocker Management settings or license to it.

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

- 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.

BitLocker To Go with Windows 7

- Encrypting a USB flash drive with BitLocker To Go in Windows 7 can take over an hour, compared to only a few minutes in Windows 10.

5.17 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 com-

puters, tracing is only started for the first selected computer. The others neither start the tracing nor report an error. Our team is working on a solution.

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

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

5.18 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.

5.19 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.

5.20 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.

5.21 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	Continued Customer Care Support
7.9	December 2020
2019.1	December 2020
2019.2	May 2022
2020.1	December 2021

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 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