DriveLock Release Notes

Release Notes 2021.1

DriveLock SE 2021

Table of Contents

1 Release Notes 2021.1

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 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:

DriveLock Installation Guide

This new document will walk you through the process of installing the different DriveLock components. It also provides a first overview of the DriveLock architecture.

DriveLock Administration Guide

The Administration Guide explains the DriveLock components and features in detail. It contains instructions for configuring DriveLock using the DriveLock Management Console (DMC).

DriveLock Control Center User Guide

This manual describes how to configure and use the DriveLock Control Center (DCC).

- 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. You will find the following topics documented in this manual:

- **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

This 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

You can accept the default options that are already configured in the Database Migration Wizard; we recommend that you only modify them in certain cases.

This 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 and version to 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 Migration 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. The events are displayed in the DCC in Forensics and in the DOC in 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.

> 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.
   - If you are using BitLocker Management, make sure to consider the following before you update:
     For details, see the BitLocker Management documentation at DriveLock Online Help.
     The **Do not decrypt** encryption setting prevents a possible change in the encryption status of the DriveLock Agents. Before updating, make sure to enable this option in the current encryption policy and save and publish the policy afterwards.

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 or higher to newer versions, 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.

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.

Disk Protection Update

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

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` msiexec or `DLSetup.exe`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 4.6.2 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	2021.1	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	2021.1	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	2021.1	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	Sup-port license requir-ed	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	2021.1	2020.2	2020.1	2019.2
SUSE 15.1	+	+	+	+
Ubuntu 18.04	+	+	+	+

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 and the limitations of its functionality, please refer to the separate Linux 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 approved to run on XP if it is used in certain ATMs.
- Windows XP Embedded: Do not install the DriveLock Virtual Channel and the DriveLock Agent on the same client!
- BitLocker Management is supported on Windows 7 systems only 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.
- Disk Protection is available for Windows 10 as of version 1703 for the Windows versions listed above (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. This will be the case after DriveLock version 2021.1 at the earliest.

Note: If you are running Windows 7, we recommend that you use the most current version. DriveLock does not distinguish between standard Windows license or ESU (Extended Security Update key). (Reference EI-1349)

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 and Control Center

Note: Please install both management components on the same computer, as the DCC uses 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 4.6.2 or higher
- Internet Explorer 11 or newer is required for remote control connections via the DCC.

Supported platforms:

Both DriveLock 2021.1 consoles have been tested and approved on the latest Windows versions officially available at the time of release and not yet at 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 4.6.2 or higher

> 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: We no longer ship a 32-bit version of the DES as of DriveLock version 2020.1.

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)

The DOC is available as a web application and as a Windows application (DOC.exe). The DOC.exe must be installed additionally and is required for extended agent remote control functions. Before installing the application on a computer, please make sure that the computer meets the following requirements to ensure full functionality.

Note: The web version of the DOC is automatically installed during the installation of the DES and can also be started via a browser. It is not necessary to install the DOC application (DOC.exe) for this purpose.

Main memory:

- at least 4 GB RAM

Free disk space:

- approx. 250 MB

Additional Windows components:

- .NET Framework 4.6.2 or higher

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. In this case, note the following aspects, among others:

- 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.
- It is common to have environments without a DES server in this context (only a 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 2020.2.

4.1 Version 2021.1

DriveLock 2021.1 is a feature release.

4.1.1 New features and improvements

This version includes the following new features and enhancements.

Licensing

As of version 2021.1, DriveLock provides a modified module structure. This affects the following modules:

- BitLocker To Go, Application Behavior Control and EDR are now standalone modules that can be activated independently.
  If your previous license already includes these features, you can continue using them without any restrictions.
- The EDR module contains part of the Application Behavior Control feature.
  If you do not need this functionality, simply disable the EDR module in the license dialog.

Microsoft Defender Firewall Management

DriveLock's ruleset is now also available for Microsoft Defender's firewall rules. You can now manage the firewall from DriveLock and use flexible configuration filters.

Security rules for local users and groups

DriveLock’s new version comes with extra protective features, allowing you to rename these accounts and providing them with changing and random passwords. This makes privilege escalation much more difficult and keeps hackers from taking over systems so easily.

Same as firewall management, this feature is part of the new "Native Security" license option.

Automatic reports in DriveLock Operations Center

Enables a regular overview of the status of your security measures with the new automatic reports in the DOC.

Restrict Bluetooth connections

With this feature you can specify detailed settings for connecting devices via Bluetooth. It either prevents pairings with new devices completely or restricts them to the Bluetooth services you are using.

Updating the configuration

You can now have a DriveLock Agent update the configuration only after all protective measures (e.g. drive and application control) have been enabled.

Other enhancements

Among other benefits, the new version includes the following enhancements:

- Free configuration of roles and permissions in DOC
- Improved general DOC usability
- Installation of backend components in larger environments
- Possibility of connection to SIEM system via Syslog
- Using AD groups in the DriveLock PBA

4.1.2 Bug fixes 2021.1

This chapter contains information about errors that are fixed with DriveLock version 2021.1. Our External Issue numbers (EI) serve as references, where applicable.

Reference	BitLocker Management
	The configuration of BitLocker password complexity was not saved correctly if you first applied a complexity setting and then disabled password complexity.
	The password for data partitions was changed twice if the password for the system partition was changed at the same time. Thus, when taking over existing BitLocker environments, an error could occur whereby individual data partitions were only taken over after a reboot.
EI-1312	An existing configuration for backing up BitLocker recovery keys in Active Directory was overwritten after installing DriveLock in such a way that backing up was no longer possible afterwards.
EI-1388	Taking over existing BitLocker environments failed in some cases for partitions where only one protector was present.
	Taking over BitLocker-encrypted systems failed if no protectors were present. Under certain conditions, system and data partitions are pre-encrypted with BitLocker after Windows 10 is installed without any protectors being created.
EI-1342	With certain settings in Windows Group Policy, the BitLocker password of data partitions could not be set by BitLocker Management.
EI-1337	Fixed an issue that prevented BitLocker from changing the pre-boot authentication type. This only affected systems that did not require re-encryption.
	Terminating the agent service was significantly delayed by the BitLocker Management component. In some cases, this could also lead to the DriveLock service crashing.

Reference	BitLocker Management
	When the options to pause BitLocker encryption were set in the policy, encryption continued even if the event occurred.
	When taking over existing BitLocker environments with at least one locked data partition, you could click the unlock button again even after the unlock operation had already been completed. Thus, you could not terminate the wizard any more.
EI-1395, EI-1396, EI-1416	When taking over BitLocker-encrypted drives, the password dialog appeared twice if both the system protector and the encryption algorithm had to be changed.
EI-1418	If the control panel was restricted to certain items via a system policy, this setting was overwritten as soon as DriveLock BitLocker Management was enabled.
EI-1464	If the license for BitLocker Management was missing, it was possible that a previously encrypted system was decrypted even though the 'Do not decrypt on configuration changes' setting had been specified.

Reference	Defender Management
	Once the dialog for delaying the start of the Defender scan had been displayed, the DriveLock service could no longer be terminated.
	The dialog for delaying the start of the Defender scan appeared even though a delay was not configured.
	The display of files in quarantine on the Defender tab of the Agent remote control dialog contained incorrect and truncated entries. Also, only part of the text was visible because the tooltip text was missing.

Reference	Device Control
EI-1323, EI-1336, EI-1341	File definitions for multiple file types were processed incorrectly by the file filter.
EI-1220	Fixed an issue that occurred when processing custom messages when locking iPhone and Android devices.
EI-1294	Drive rules have a priority order now.

Reference	DriveLock Agent
EI-1321	Sometimes it was not possible to run an action on the agent when the MMC and the DOC were started at the same time and used for agent remote control. If a user was logged on to Windows who did not have permissions for agent remote control, it was not possible to use agent remote control from the DOC, even if the user logged on to the DOC had permissions to do so.

Reference	DriveLock Enterprise Service (DES)
EI-1302	The DriveLock Enterprise Service Setup allows users to be selected from a different trusted forest model.
EI-1355	Fixed an issue that caused the DES to crash when a computer was deleted.

Reference	DriveLock Pre-Boot Authentication
	Emergency logon data was not uploaded if the system partition was not encrypted but the DriveLock PBA was supposed to be

Reference	DriveLock Pre-Boot Authentication
	installed.
	In the case where only data partitions were encrypted and not the system partition with DriveLock PBA enabled, the password for the data partitions was not requested. However, this password is needed because in this case data partitions are not unlocked automatically and manual unlocking with a user password is required.
	For drives pre-encrypted with BitLocker, the DriveLock PBA installation started and finished with an error.
EI-1243	After activating the network PBA, the system drive was decrypted and then re-encrypted even though the DriveLock PBA was already set up.
EI-1287	When using Windows Quick Start, data partitions were no longer automatically unlocked after startup. In environments where the DriveLock PBA was configured, the BitLocker recovery key was required for unlocking.

Reference	EDR/Events
	In the text for event 635, the error code to isolate the error was missing. The event provides information that the BitLocker password setting failed.
	Fixed an issue where saving a new alert category to a centrally stored policy failed.

Reference	Encryption-2-Go
EI-1212	Handling incomplete recovery information was corrected.

	File Protection
EI-1259	Fixed an issue with a BSOD in the Terminal Server environment.
EI-1163	Fixed an issue where copying XML files to SMB 3.0 cluster shares corrupted the XML file.

Reference	Configuration (policies)
EI-376	Users were not informed that they had selected the insecure HTTP protocol in the server configuration.
EI-1346	Improved AD information caching. Even if no AD information is available, DriveLock groups and assignments of centrally stored policies can be used as long as they do not depend on AD information.

Reference	Licensing
EI-1150	License activation in the MMC now also works when using a proxy server.

Reference	System Management
EI-1307	When available, the network name of the computer is now returned by the agent as FQDN and the NetBIOS name is only used if there is no FQDN. This makes agent remote control more stable, since it can also find computers in other domains.

4.2 Version 2020.2

4.2.1 Bug fixes 2020.2

This chapter contains information about errors that are fixed with DriveLock version 2020.2. 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 rule created in the policy.
	Fixed a bug in the DriveLock file system filter driver that caused a BSOD when inserting a USB stick.
EI-1188	It is now possible to access the memory card in a digital camera connected to the Fat Client or Thin Client with a USB cable if the `MtpRestartTimeout(REG_DWORD)` (REG_DWORD) value in the registry key `HKEY_LOCAL_MACHINE\SOFTWARE\CenterTools\DLSettings\Devices` is set to 3000 (ms). Note: Since Windows 10 Update 2020, the camera may only be accessed if the Generic virtual channel is set in the Citrix Workspace.
EI-1230	A blue screen sometimes occurred after connecting a USB stick. This bug is fixed now.

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 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,	A number of improvements have been made to the update mech-

Reference	DriveLock Agent
1080, 1090, 1116, 1156	anism.
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 Control Center (DCC)
EI-1068, EI-1069, EI-1091, EI-1076	In DCC, the ConfigID column now displays the policy name and version instead of the GUID.

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.

Reference	DriveLock Enterprise Service (DES)
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	File Protection
EI-1216	Fixed an issue where a service (DLFfeGui) would crash when decrypting encrypted folders. This issue is fixed now.
EI-1143, EI-1163	While mounting an encrypted folder, the service for re-encrypting unencrypted files no longer starts.

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 caller 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 for 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 issue 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.

4.3 Version 2020.1

4.3.1 Bug fixes 2020.1

This chapter contains information about errors that are fixed in DriveLock version 2020.1. 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	The first time you reached the dialog page where you set the time for policy settings to be deactivated, the current time used to be specified. 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.

4.3.2 Bug fixes 2020.1 HF1

This chapter contains information about errors that are fixed with DriveLock version 2020.1 HF1.

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

4.3.3 Bug fixes 2020.1 HF2

This chapter contains information about errors that are fixed with DriveLock version 2020.1 HF2.

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

4.3.4 Bug fixes 2020.1 HF3

This chapter contains information about errors that are fixed with 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 when detailed information is not required.
EI-1123	Fixed an error related to using Agent remote control which occurred with Novell eDirectory.
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

Reference	BitLocker Management
	enabled in Windows 10.
	The system drive password change failed for BitLocker-encrypted computers without 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.

Reference	DriveLock Enterprise Service (DES)
EI-1136	Fixed an issue that occurred when starting the DriveLock Enterprise Service when a large number of unprocessed events existed in the database.
	An incorrect log file was written during DES setup.

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.

4.4 Version 2019.2

4.4.1 Bug fixes 2019.2

This chapter contains information about errors that are fixed with DriveLock version 2019.2. Our External Issue numbers (EI) serve as references, where applicable.

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

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

Reference	BitLocker Management
EI-666	The error when encrypting a system drive [0x8031002c] was fixed by adjusting the Group Policy registry values.
EI-740	Existing BitLocker Managed Environments (e.g. MBAM) can be used torgether with DriveLock now. To do this, the following

Reference	BitLocker Management
	DWORD value must be added in the registry key: `HKEY_LOCAL_MACHINE \SOFTWARE \CenterTools \DLStatus \RegProtectionLevel` (Note: without spaces!). Set the value to 1. Note that you can only change this setting after shutting down the Agent. Restart the system afterwards.

Reference	DriveLock Control Center (DCC)
EI-734	The login screen for the DriveLock Control Center has been extended so that the German text for the user name is no longer truncated.

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

Reference	Disk Protection
EI-277	Switching domains after a WOL no longer results in a domain change.
EI-231	You can now set the entry for encryption certificates to **Not con-**

Reference	Disk Protection
	figured in the policy.
EI-579	You can now delete disk protection certificates from the file repository in the policy.

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

Reference	File Protection
EI-646	CSV files can be encrypted now
EI-640	The **User name and password** radio button is active now and selected by default.
EI-737	DLFldEnc no longer crashes during file copy.
EI-426	When encrypting an external hard drive with DriveLock FFE and performing a defragmentation with Windows, all files are now correctly encrypted and the NTFS file system is no longer damaged.
EI-112	File protection users with read permissions can mount encrypted folders now.
EI-626	When File Protection is licensed and Encryption-2-Go is not

Reference	File Protection
	required, you no longer get a warning or error message when configuring the whitelist rules for the drive.
EI-653	A user with DriveLock certificate will no longer receive an error when attempting to mount an encrypted folder.

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

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

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

Reference	Self-Service
EI-718	It is no longer possible to enter a time in the past in the Self-Service wizard.
EI-717	When exporting a Self-Service group to a CSV file, the umlauts (like äöü) are now saved correctly.

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

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

4.4.2 Bug fixes 2019.2 HF1

This chapter contains information about errors that are fixed with DriveLock version 2019.2 HF1.

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

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

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

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

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

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

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

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

4.4.3 Bug fixes 2019.2 SP1

Important bug fixes in this version

This chapter contains information about errors that are fixed with DriveLock version 2019.2 SP1.

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

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

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

Reference	Disk Protection
EI-756	Hardware compatibility issues related to Disk Protection have been fixed.

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

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

Reference	Encryption-2-Go
EI-639	DriveLock Mobile for MAC OS no longer encrypts the DriveLock.app folder.
EI-643	When using an encrypted USB device, the CPU is now no longer overloaded.

Reference	File Protection
EI-825; EI-884; EI-876	Several bugs that caused the File Protection driver to crash are fixed.
EI-868	You can rename network drives now when File Protection is active.
EI-537	Now only administrators can completely decrypt centrally managed directories.

Reference	File Protection
EI-628	When FP is the method used for USB encryption, the automatic decryption dialog now appears every time when connecting a USB drive.

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

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

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

Reference	Self-Service
EI-844	The Self-service wizard no longer accepts entering times in the past.
EI-538	Self-service is stopped (after you select the respective checkbox)

Reference	Self-Service
	when the user is connected via RDP with the client computer.

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

4.4.4 Bug fixes 2019.2 HF3

Important bug fixes in this version

This chapter contains information about errors that are fixed with DriveLock version 2019.2 HF3.

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

Reference	Device Control
EI-540	Improved detection of burning devices and setting correct access rights on volume.
EI-1028	Network drive is not locked any longer with the applied whitelist rule: 00000000-C0D0-C0D0-0001-00000000000A on Terminal Servers
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	File Protection
EI-1053	The "[DriveLock File Protection]" menu item could not be disabled via the DriveLock Agent's system tray icon. This bug is fixed now.

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.

5 Known Issues

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

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 Known limitations on the agent

Updating/installing/uninstalling the agent on Windows 7 x64

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

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 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.

5.5 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 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).

Using a local policy

Some settings are not applied correctly when you save or export a local policy, and therefore may not lead to the intended results when you test these settings on the individual computer. For this reason, please use one of the other configuration options (configuration file, group policy or centrally stored policy) for your tests as they are not affected by this restriction.

Taskpad view

The Devices node may be missing the scroll bar in the Taskpad view of the Management Console. As a workaround, simply resize the window, e.g. increase or decrease the width of the tree view, then the scroll bar is available again.

5.7 DriveLock Disk Protection

Windows Inplace Upgrade

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

Antivirus software

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

Application Control

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

Hibernation

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

UEFI mode

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

- The PBA provided by version 2019.2 is only available for Windows 10 systems, because the driver signatures from Microsoft required for the hard disk encryption components are only valid for this operating system.
- The PBA for UEFI mode may cause issues with PS/2 input devices (e.g. built-in keyboards).
- With VMWare Workstation 15 and also with a few hardware manufacturers, our test results revealed conflicts with mouse and keyboard drivers of the UEFI firmware, so that keyboard input in the PBA is not possible. By pressing the "k" key, you can prevent the Drivelock PBA drivers from loading once when starting the computer. After logging in to Windows on the client, you can then run the `dlsetpb /disablekbddrivers` command in an administrator command line to permanently disable the Drivelock PBA keyboard drivers. Be aware that the standard keyboard layout of the firmware is loaded in the PBA login mask, which usually is an EN-US layout, so special characters may differ.
  Introducing the combined driver as of version 2020.1 solves the issue on some systems (including VM Ware Workstation 15).
  For more information on hotkeys and function keys, see the corresponding chapter in the BitLocker Management documentation at DriveLock Online Help.

Note the following information:

- DriveLock 7.6.6 and higher supports UEFI Secure Boot.
- If you update the firmware, the NVRAM variables on the mainboard that DriveLock requires may be deleted. We strongly recommend that you install the firmware updates for the mainboard /UEFI before installing DriveLock PBA / FDE (this also applies to recently purchased devices or to bug fixes).
- A 32 bit Windows operating system or 32 bit DriveLock cannot be installed on 64 bit capable hardware. Please use a 64 bit version of a Windows operating system and DriveLock instead.
- There is still a limitation to disks up to a maximum of 2 TB disk size.

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

BIOS mode

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

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

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

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

Reference: EI-686)

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

Requirements for Disk Protection:

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

Restart after installation of PBA on Toshiba PORTEGE Z930:

Reference: EI-751)

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

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.

5.8 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.

Accessing a folder from a computer without DriveLock

- When accessing a mounted encrypted folder on a computer with DriveLock from a computer without DriveLock, a blue screen occurs on the computer with DriveLock.

5.9 DriveLock Pre-Boot Authentication

Hardware must support the TCP4 UEFI protocol for the DriveLock PBA network functionality to work. For this reason, some systems may run into trouble if the UEFI BIOS does not support the required network connections.

Currently, this is the case with the following system: Fujitsu LifeBook E459. (EI-1303)

5.10 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.

5.11 DriveLock Mobile Encryption

DriveLock Mobile Encryption: NTFS/EXFAT

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

5.12 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.

5.13 DriveLock Operations Center (DOC)

Multiple selection of computers in the Computers view

If you select several computers in the Computers view and then select the **Run actions on computer** command in the upper right menu to enable the trace for these computers, tracing is only started for the first selected computer. The others neither start the tracing nor report an error. 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 run the installation of DOC.exe while disk encryption is in progress with Disk Protection

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

View settings in DOC

Since DOC views have been optimized in version 2020.2, custom view settings may need to be reconfigured when updating from version 2020.1.

Export lists to Excel

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

5.14 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: Note that the Dutch content will be automatically deleted from the DES when you update to a version higher than 2019.1.

5.15 DriveLock and Thin Clients

Please note the following restrictions when using DriveLock and Thin 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.
- The “Fill any remaining space on drives” option does not work correctly when used for encrypting a DriveLock container via a Thin Client.

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
2021.1	November 2022

Support cycles:

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

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

Upgrades:

Customers who have previous product versions and a valid maintenance contract can upgrade the environment to the latest product version.

7 DriveLock Test Installation

If you want to have a detailed look at DriveLock and test the product, you can request a trial through the DriveLock website. Just follow the links on our website https://www.drive-lock.de/.

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

Once you have registered for a test, we will send you several emails with information to support your testing. See https://www.drivelock.de/cloud-testversion-information for a summary.

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

Copyright