



DriveLock 6

Release Notes

Copyright

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

© 2010 CenterTools Software GmbH. All rights reserved.

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

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

Table of Contents

1	INTRODUCTION	5
1.1	DOCUMENT CONVENTIONS	6
2	NEW FEATURES IN VERSION 6.....	7
2.1	ARCHITECTURAL CHANGES.....	7
2.2	UPDATED USER INTERFACE.....	8
2.3	QUICK AND EASY IMPLEMENTATION	8
2.4	DATA ANONYMIZING	9
2.5	NEW DRIVE CONTROL FUNCTIONALITY.....	9
2.6	CD AND DVD SHADOW COPIES	9
2.7	ENCRYPTION 2-GO	10
2.8	A NEW LEVEL OF APPLICATION CONTROL.....	10
2.9	REPORTING AND ANALYSIS	11
3	DRIVELOCK DOCUMENTATION	12
4	TEST INSTALLATION AND UPGRADE.....	12
4.1	DRIVELOCK EVALUATION	12
4.2	UPGRADING AN OLDER VERSION OF DRIVELOCK.....	13
4.3	UPDATE DES 6.0.0.480 TO DES 6.0.0.488.....	13
5	ADDITIONAL INFORMATION	14
6	KNOWN ISSUES.....	14
6.1	DRIVELOCK UND XENAPP.....	14
6.2	DRIVELOCK AND WINDOWS VISTA / WINDOWS7	14
6.3	AUTOMATIC UPDATES AND APPLICATION LAUNCH FILTER.....	14
6.4	DRIVELOCK FULL DISK ENCRYPTION.....	15
7	VERSION HISTORY.....	15
7.1	DRIVELOCK VERSION 6.0.0.480	15
7.2	DRIVELOCK VERSION 6.0.0.488	15




1 Introduction

This document contains important information about new features in DriveLock 6 and changes since DriveLock 5.5 R2. Also, it describes the product documentation and the intended audience for each documentation component.

The DriveLock release notes also describes changes or additions to DriveLock that were made after the documentation was completed.

1.1 Document Conventions

Throughout this document the following conventions and symbols are used to emphasis important issues that you should read carefully or menus, items or buttons you have to click on or select.

	<p>Caution: This symbol means that you should be careful to avoid unwanted results, such as potential damage to operating system functionality or loss of data</p>
	<p>Hint: Useful additional information that might help you save time.</p>
	<p>Information: Additional information about the current topic</p>
<p><i>italic</i></p>	<p>Italics represent fields, menu commands, and cross-references.</p>
<pre>C:\> command</pre>	<p>A fixed-width typeface represents messages or commands typed at a command prompt.</p>
<p>Next</p>	<p>Bold type represents a button that you need to click.</p>
<p>ALT + R</p>	<p>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.</p>
<p>ALT, R, U</p>	<p>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.</p>

2 New Features in Version 6

DriveLock 6 is a major release that includes completely new functionality, additional configuration choices and important architectural changes in addition to many small improvements. This document describes the most important changes and provides a concise overview of DriveLock 6, illustrating the new possibilities for securing a client environment that this new version makes possible.

2.1 Architectural Changes

In DriveLock 6 the Security Reporting Center (SRC), including the SRC Server and the SRC Management Console, are being replaced with new components. Only the central SQL database remains in place and is being expanded. Instead of the SRC, DriveLock uses the new DriveLock Enterprise Service to combine the functionality of the following older components into a single central service:

- DriveLock Consolidator Service
- DriveLock File Cache Service
- SRC Web Services

As a result of the new architecture there is no longer a need to enable and run Microsoft Internet Information Services on the central server. The DriveLock Enterprise Service can run on a dedicated server or it can be co-located on any existing server that meets the hardware requirements. The DriveLock Enterprise Service can use an existing instance of Microsoft SQL Server on the server where it is installed or on a remote server. You can also use the free SQL Server Express version, which is sufficient for many smaller environments.

The new DriveLock Control Center (DCC) replaces the SRC Management Console. The DCC is a standalone application instead of an MMC snap-in, which means fewer limitations to appearance and functionality of the application. This results in faster performance and better usability in the current version and will enable additional functionality in future versions.

The architectural changes allow for an even easier installation experience because there are system and network prerequisites. As a result, daily use and administration are less complex and many tasks can be performed more efficiently. System stability is increased and if a problem occurs, troubleshooting is streamlined and gets easier.

2.2 Updated User Interface

The DriveLock Management Console has been updated to include a modern user interface that is visually appealing, consistent with current design standards and even easier to navigate. Many of the existing Task Views have been redesigned and display the current configuration settings without requiring an administrator to switch to the “Classic MMC View”. This can simplify and streamline both administration and troubleshooting.

The DriveLock Management Console contains a new Basic Configuration section(Starter Mode) to make it easier for you to configure most common aspects without being distracted by advanced settings. This process is aided by many wizards. Administrators who are new to DriveLock or don't frequently configure DriveLock policies will find administration tasks to be much easier to perform. At the same time they can be confident that they configured everything that's required to implement DriveLock without missing critical settings. Experienced DriveLock administrators can hide the Basic Configuration.

Administering whitelist rules is made easier by the addition of folders. To help you keep track of a large number of whitelist rules, you can now create folders and subfolders to organize these rules. For example, you can group whitelist rules by department or by device type (one folder for rules covering Kingston flash drives, another folder for rules covering SanDisk flash drives). Similarly, file filter templates can be grouped into folders, for example one folder for all Microsoft Office file types.

The goals for making the changes to the DriveLock Management Console are to make it even easier to get started implementing DriveLock and to enable you to quickly and easily integrate DriveLock into your current network and security infrastructure. The main benefits are improved data security and reduced administration costs.

2.3 Quick and Easy Implementation

The previous versions of DriveLock included a test mode for the Application Launch Filter that lets you test policy settings in a live environment without negatively impacting users. This test mode has been expanded and now covers all areas of DriveLock. You can now extensively test all policy settings, including whitelist rules, for as long as you need to be confident that everything works as expected. In test mode the DriveLock Agent analyzes policy settings but doesn't block drives, devices or applications. The Agent performs all event reporting and displays all configured user notifications and dialog boxes. Once you have confirmed that everything works as expected, you can change your policy to enforce the settings. It's hard to imagine how implementing DriveLock could be any easier.

2.4 Data Anonymizing

Some localities restrict which personally identifiable data about employees companies can monitor and record. System administrators have to incorporate these requirements into the design of their network infrastructure. DriveLock now includes the tools to implement such design requirements. Administrators can configure the reporting of events by DriveLock Agents to not send any user-specific information to the DriveLock Control Center or other destinations, such as an e-mail address. To ensure that any such restrictions remain enforced DriveLock can monitor and record all changes to configuration settings.

2.5 New Drive Control Functionality

In addition to the drive types that you could control using previous versions, DriveLock now lets you create rules that control the use of SD cards and internal drives. You can also use the category “internal drives” to control the increasingly popular external eSATA drives, which connect to computers using the same hardware bus as internal SATA drives.

Drive whitelist rules can now include multiple file filter templates, enabling you to use a combination of allowed and blocked file types in such rules. You can now also enforce all drive rule options on a per-user or per-group basis, including enforced encryption and automatic execution of scripts. For example, you can now require encryption for all flash drives but still allow helpdesk personnel to use unencrypted drives.

If you want to give your users autonomy over the use of removable drives instead of categorically blocking them, you can enable users to authorize the use of such drives themselves, for example by typing a password you gave them. Because user education is a critical component of network infrastructure security, you can also configure DriveLock to display a notification before a user can access a removable drive. Such a notification can contain tips for how to securely use removable media, an excerpt of your organization’s security policy, or a warning that the use of removable media is allowed but that all user activity is logged. You can even configure the notification to play a video file. The new notification capabilities can help you improve users’ security awareness without much effort.

2.6 CD and DVD Shadow Copies

Previous versions of DriveLock included the ability to create shadow copies of files that users accessed on removable drives or copied to such drives. DriveLock 6 extends this functionality to CDs and DVDs that users create. If you allow the use of CD/DVD burners, DriveLock can create a complete

copy of each disc a user creates and save it to a central location. The shadow copy is stored as an ISO file and is a complete image of the disc. You can use many common tools to view the data that is contained in an ISO image.

2.7 Encryption 2-Go

DriveLock's removable media encryption, which was previously called "Encryption License Classic", has been renamed to "Encryption 2-Go License". In addition to the name change, the functionality has also been improved. A new policy option for enforced encryption lets you configure whether all available space on a flash drive or other removable drive is encrypted, or whether a portion of the drive remains unencrypted.

DriveLock also incorporates new encryption libraries that are FIPS 140-2 certified. If your organization requires that encryption meets FIPS requirements you can now use DriveLock for removable media encryption.

2.8 A New Level of Application Control

The new release of DriveLock contains a completely re-designed and much improved version of the Application Launch Filters (ALF). If you previously used the ALF, you will still find all familiar features, including the test mode, the application hash database (which can be based on all applications on an entire hard drive) and rules that cover all programs that are part of the operating system or all .NET applications. You can also continue to use a combination of whitelist and blacklist rules for maximum flexibility. You can take advantage of a full spectrum of options for configuring which users can run which programs on which computers. The DriveLock Application Launch Filter takes care of implementing your policies. The functionality provided by DriveLock goes far beyond the basic application control included in Windows 7 and affords you unique flexibility.

DriveLock 6 also contains two new types of application rules that you can use to block or allow applications based on additional criteria: File Owner Rules and Certificate Publisher Rules. When evaluating a File Owner Rule, the DriveLock Agent checks whether the ownership of a program file, for example Administrator or System, matches the policy setting. Because Windows automatically sets the file ownership when a program is installed, you can use this type of rule to easily allow the use of all applications that were installed by an authorized administrator or a trusted service account. Applications that were installed by any other user, or that don't require installation to run, are automatically blocked. One advantage of using File Owner Rules is that DriveLock continues to

enforce the current policy even after a program is updated centrally or locally by an authorized administrator.

Certificate Publisher Rules can verify the origin and version of a program file. You can use this type of rule to allow or deny the use of applications based on a specific software certificate, the certificate's issuer, the software publisher or the program version. For example, you only need a single rule to easily allow the use of all internal applications that are signed with a specific software certificate or all applications published by a trusted software vendor.

Because it's easy to combine criteria for allowing or blocking applications, DriveLock can enforce your settings based on only a few rules you configure, unlike other solution that require you to configure a complicated set of rules that needs to be updated frequently. DriveLock's simplicity makes it an ideal tool for implementing effective application control in both small organizations and large enterprises without requiring a extensive administrative resources.

2.9 Reporting and Analysis

In DriveLock 6 you can view a report of all configuration settings and save the configuration as an XML file. This lets you easily document your current configuration settings and make it available for compliance reporting.

The biggest change in DriveLock 6 is how it re-defines the analysis of security data. The new DriveLock Control Center contains all tools you need to quickly generate a relevant overview of your entire DriveLock deployment and endpoint activity. In addition to comprehensive and flexible reporting features, the DriveLock Control Center contains tools to enable forensic analysis of events. It lets you easily pinpoint relevant monitoring data and investigate all aspects of client activity that are unusual or that represent security risks. The report types that were available in previous versions have been enhanced with more powerful filtering options and they are complemented by new report types.

You can use the DriveLock Control Center to drill down into your data to discover the background of event data and to discover hidden connections between events. Your starting point could be a specific user, a certain file or a flash drive you found in the parking lot. For example, you can start with a report that identifies all files that were copied to a specific flash drive during a certain time period. Taking this information you can then easily find out which other flash drives the same files were copied to and all computers where these devices were used. As you are adjusting your search criteria you can easily back-track, return to the original data and investigate other aspects that are hidden in your event data. The flexibility of this method allows you to gain insight into what's going on in your network and helps you assess the impact of security incidents.

3 DriveLock Documentation

The DriveLock Documentation consists of the following four manuals:

- [DriveLock Installation Guide](#)
The Installation Guide describes the available installation packages, the system requirements and the steps for installing each DriveLock component. This is the first document a DriveLock administrator should read.
- [DriveLock Administration Guide](#)
The Administration Guide describes the DriveLock architecture and components. It contains detailed instructions for configuring DriveLock using the DriveLock Management Console. 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. This document is intended for administrators and users who will use DriveLock Control Center for reporting and forensic analysis.
- [DriveLock User Guide](#)
The DriveLock User Guide is aimed at end users. It describes how to request the temporary unlocking of a computer, how to use DriveLock Encryption 2-Go and how to use Network Profiles.

4 Test Installation and Upgrade

4.1 DriveLock Evaluation

The DriveLock Installation Guide describes the necessary steps to install DriveLock on a single computer, for evaluation purposes. Before installing DriveLock, please ensure that all system requirements are met.

You can install the DriveLock Enterprise Service, the DriveLock Control Center and Microsoft SQL Express 2005 or 2008 on the same computer (not Windows XP operating systems). This topology makes it easy to evaluate DriveLock's central reporting features using minimal hardware.

If you downloaded the DriveLock software from the Web site (www.drivelock.com), a 30-day trial license is included. To evaluate DriveLock on a single computer, you don't need to perform any license configuration.



If you install the DriveLock Agent on multiple client computers and configure DriveLock settings using Microsoft Group Policy or a configuration file, you must add a license key to the configuration. You can use the evaluation license key (AgentTrial.lic) that is installed with DriveLock (by default, in "C:\Program Files\CenterTools\DriveLock").

4.2 Upgrading an older Version of DriveLock

When upgrading from DriveLock 5 to DriveLock 6, please first read the important information about this process in the DriveLock Installation Guide and ensure to upgrade the DriveLock Agents before upgrading the DriveLock Management Console.



It is not possible to update Agents Version 5.0 SP1 or older to DriveLock 6. Please update to DriveLock 5.5R2 before updating to DriveLock 6.

Detailed information about the update process is covered in a DriveLock whitepaper, which is available for download on the DriveLock website (www.drivelock.com).

4.3 Update DES 6.0.0.480 to DES 6.0.0.488

When upgrading from DES 6.0.0.480 to DES 6.0.0.488, please first uninstall the old DES version. Next install the new DES 6.0.0.488 version. An existing DES database can be used with the new DES version. Therefore you can select your existing database during installation. All data incl. FDE recovery files will be still available.

5 Additional Information



Starting with DriveLock 6, changes to a group policy configuration must be explicitly saved. To apply your configuration changes to the group policy, in the left pane of the Group Policy Object Editor, click **CenterTools DriveLock** and then in the task view in the right pane, click **Save**.

6 Known Issues

This chapter contains all known issues for this version of DriveLock. Familiarize yourself with the information in this chapter to avoid unnecessary effort during testing and deployment.

6.1 DriveLock und XenApp

Citrix XenApp 6 and XenApp 5 are not supported in the current version of DriveLock.

6.2 DriveLock and Windows Vista / Windows7

On Windows Vista and Windows 7 the following issues may occur:

Locking “Portable devices” does not work for some devices:

Windows Vista uses a new User-Mode Driver Framework for these types of devices. Some devices may not be locked or unlocked correctly because of malfunctioning driver components.

6.3 Automatic Updates and Application Launch Filter

If the Application Launch Filter is configured for whitelist mode and a rule with the setting “Allow automatic updates” exists, updates may not install properly under certain conditions. As a workaround, create application rules for each of these updates.

6.4 DriveLock Full Disk Encryption

Virus protection software may cause the DriveLock Full Disk Encryption installation to fail if the antivirus software quarantines files in the C:\SECURDSK folder. If this occurs, disable virus protection for the duration of the Full Disk Encryption installation and re-enable it after the installation is complete.

It is strongly recommended that you run “chkdsk /f” and the Windows disk defragmentation utility before upgrading from previous versions of DriveLock Full Disk Encryption.

On a small number of computer models, the default DriveLock Full Disk Encryption 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] key. When prompted, select the option to use the 16-bit pre-boot operating environment. To make this adjustment permanent, follow the steps described in the DriveLock [Knowledge Base](#) Technical Support maintains an extensive list of computer models that DriveLock Full Disk Encryption has been tested on and that have been validated to function without changes to the pre-boot environment.

7 Version History

7.1 DriveLock Version 6.0.0.480

DriveLock 6 is a major release that includes major changes to the DriveLock architecture and contains a large number of new features and configuration options. All new functions and the new architecture are described in detail in the DriveLock manuals and are not separately listed here.

7.2 DriveLock version 6.0.0.488

New functionality:

- 64 bit version available
- 64-bit version of FDE available
- The DriveLock Management Console now includes parent OUs when displaying licensed computers from Active Directory

- It is now possible to select and move multiple drive whitelist rules in a single step

The following issues in the previous version 6.0.0.480 have been fixed:

- When installing the DES, it is now possible to select a remote SQL database without using integrated authentication.
- Internet Explorer script errors occurred in some cases when opening the Management Console.
- Under certain conditions on computers running Windows Vista system some system functionality was disabled.
- Not all active DriveLock Agents were displayed when the list of Agents is retrieved from the DES server.
- Sometimes incorrect data was displayed when viewing the licensing status in the DES.
- In rare cases SOAP SSL errors were logged in the Event Viewer.
- In some cases the DES intermittent errors occurred when starting the DES service.
- Several additional small bug fixes.