



# DriveLock 5 – Release Notes

Version 5.5 R2



**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.

© 2009 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	New Features in Version 5.5 R2 .....	4
2	System Requirements.....	5
3	Updating an Earlier Version of DriveLock.....	7
4	Additional Information .....	10
5	Known Issues.....	11
6	Version History.....	13

# 1 New Features in Version 5.5 R2

## 1.1 DriveLock Application Launch Filter

You can now quickly and easily create a computer template containing all applications that are currently installed on a computer. Apply this template to allow the use of only these applications to protect against malicious software and unwanted applications. Application templates are most useful in organizations with standardized computer configurations.

When configuring application rules you now have access to an online database containing millions of signatures of both popular and less known programs. This database is constantly being expanded and updated. This database also vastly simplifies enforcing rules after applying updates or patches to your applications.

## 1.2 DriveLock Terminal Server Edition

DriveLock 5.5 introduced the ability to block the use of local drives on thin clients that are mapped in a terminal server session. Now you also get the same file filtering and auditing functionality for these drives that are available on other client computers. This lets you block access to specific file types, such as MP3 files or videos, and fully audit the transfer of files from and to USB drives attached to a thin client.

## 1.3 DriveLock Full Disk Encryption

Preboot authentication has been completely revised to improve support for token authentication. Also the user interface has been redesigned to be more appealing. A new rapid recovery mechanism allows much quicker access to data on an encrypted disk that has become inaccessible because of technical defects.

The Security Reporting Center displays additional information about the current encryption state and provides support for recovery operations.

## 1.4 DriveLock Removable Media Encryption

Password recovery for encrypted removable media, such as USB flash drives, and encrypted containers has been made easier and more flexible in DriveLock 5.5 R2. Helpdesk staff can now better help a user who forgot an encryption password, either online or offline, using a challenge/response mechanism. This password recovery doesn't require the transmission or sharing of an administrative password.

## 2 System Requirements

CenterTools DriveLock works in the background and therefore only uses minimal hardware resources. DriveLock runs under all common Windows operating systems and requires no additional infrastructure. Configuration and Agent deployment are done primarily by using Active Directory.

	Agent	DriveLock Management Console	Security Reporting Center (Requirements may differ depending on your system environment and your database installation)
Minimum CPU speed	400 MHz	400 MHz	500 MHz
Minimum Memory	128 MB RAM	128 MB RAM	128 MB RAM
Minimum Hard Disk	25 MB	85 MB	95-300 MB for database (~275 MB for standard installation)
Supported operating systems	Windows XP Professional SP2 or later  Windows Server 2003 SP1 or later  Windows Vista	Windows XP Professional SP2 or later  Windows Server 2003 SP1 or later  Windows Vista	Windows Server 2003  Windows Server 2003 SP1  Windows Server 2003 R2
Additional Software	Microsoft XML Core Services 6.0  Microsoft Native WLAN API for Windows XP (required for feature: „Disable WiFi connections when connect to a LAN“)  Microsoft IMAPI 2.0 (for CD/DVD Encryption)	Microsoft XML Core Services 6.0  Microsoft Management Console 3.0  .NET Framework 3.0  Microsoft IMAPI 2.0 (for CD/DVD Encryption)	Internet Information Services 6.0 (IIS) with ASP.NET 2.0  Microsoft SQL Server 2000 or newer  .NET Framework 2.0

CenterTools recommends that you always install the most current Service Pack and all security patches that are available for the version of the operating system you are using.

DriveLock supports 64-bit operating systems, except for DriveLock Full Disk Encryption, which is available for 32-bit systems only. To install DriveLock in a 64-bit edition of Windows, use the available 64-bit setup files.



The document “*DriveLock 5.5 R2 Full Disk Encryption*” contains additional information about supported operating systems and system requirements for DriveLock Full Disk Encryption.

# 3 Updating an Earlier Version of DriveLock

## 3.1 Updating from DriveLock 3.x

There are no known issues when updating to the new Agent version. It is recommended to update the DriveLock Management Console first, so you can adjust your configuration prior rolling out the new Agent to client computers.

DriveLock makes no changes to any Group Policy Object or configuration file when updating or installing the DriveLock Agent. When you open a Group Policy Object that was configured with version 3.x, DriveLock only informs you that you must re-activate the license. You can find more information about how to activate a license in Chapter 7.2.1 of the *“DriveLock 5.5 Administration Guide”*.

To allow recovery from any unintended changes to existing configuration settings, export all local or Group Policy-based DriveLock policies to a file. For more information about exporting policies, see Chapter 4.1 of the document *“DriveLock 5.5 Planning – Installation – Deployment”*.

Before installing the new Agent by using Group Policy, select the existing GPO used for deployment and add the new installation file (\*.MSI). After adding the installation file, select the option *“Update existing packages”* under *“Updates”* on the Properties page of the software deployment policy. Then click Add and select the old installation file. Ensure that the option *“Uninstall the existing package, then install the new package”* is selected (this is the default setting).

## 3.2 Updating from DriveLock 4.x

There are no known issues when updating to the new Agent version. It is recommended to update the DriveLock Management Console first, so you can adjust your configuration prior rolling out the new Agent to client computers.

DriveLock makes no changes to any Group Policy Object or configuration file when updating or installing the DriveLock Agent. When you open a Group Policy Object that was configured with version 4.x, DriveLock only informs you that you must re-activate the license. You can find more information about how to activate a license in Chapter 7.2.1 of the *“DriveLock 5.5 Administration Guide”*.

To allow recovery from any unintended changes to existing configuration settings, export all local or Group Policy-based DriveLock policies to a file. For more information about exporting policies, see Chapter 4.1 of the document *“DriveLock 5.5 Planning – Installation – Deployment”*.

Before installing the new Agent by using Group Policy, select the existing GPO used for deployment and add the new installation file (\*.MSI). After adding the installation file, select the option *“Update existing packages”* under *“Updates”* on the Properties page of the software deployment policy. Then click Add and select the old installation file. Ensure that the option *“Uninstall the existing package, then install the new package”* is selected (this is the default setting).

## 3.3 Updating from DriveLock 5.x

There are no known issues when updating to the new Agent version. It is recommended to update the DriveLock Management Console first, so you can adjust your configuration prior rolling out the new Agent to client computers. DriveLock makes no changes to any Group Policy Object or configuration file when updating or installing the DriveLock Agent.

To allow recovery from any unintended changes to existing configuration settings, export all local or Group Policy-based DriveLock policies to a file. For more information about exporting policies, see Chapter 4.1 of the document *“DriveLock 5.5 Planning – Installation – Deployment”*.

Before installing the new Agent by using Group Policy, select the existing GPO used for deployment and add the new installation file (\*.MSI). After adding the installation file, select the option *“Update existing packages”* under *“Updates”* on the Properties page of the software deployment policy. Then click Add and select the old installation file. Ensure that the option *“Uninstall the existing package, then install the new package”* is selected (this is the default setting).

The processing of permissions to nodes in the DriveLock Management console has changed in DriveLock 5.5. Permissions are now applied similarly to NTFS permissions, and Deny permissions take precedence over Allow permissions. As a result, if you set the permissions to a node to Invisible for the group Everyone, no user can see the node, even though other permissions may apply to this user.

Before upgrading from a previous version of DriveLock Full Disk Encryption, run the `“chkdsk /f”` command and perform a full defragmentation of the computer’s hard disk.

## 3.4 Updating from the Security Reporting Center 4.x

Security Reporting Center Version 5.5 uses completely new software architecture and a new user interface. The SRC Management Console is now tightly integrated into the DriveLock Management Console, but you can also still use it as a separate MMC snap-in. The DriveLock Web console is no longer needed. When updating the SRC, the installation program replaces the existing Web application with the new DriveLock Web service, updates the existing Consolidator to the new version and transfers the data from the existing database to a new database.

To allow recovery from any unintended changes to existing settings and data, back up the old SRC database prior to an update.

## 3.5 Updating from the Security Reporting Center 5.x

When updating the SRC, the installation program replaces the existing Web service with the new DriveLock Web services, updates the existing Consolidator to the new version and modifies the existing database. You don't need to uninstall any previously installed components.

To allow recovery from any unintended changes to existing settings and data, before upgrading the SRC perform a full backup of the SRC database prior to an update. In addition back up all contents of the *SRFileCache* directory, which is located in the SRC installation directory. (This directory does not exist with older installations of DriveLock.)

## 4 Additional Information

This chapter contains so additional comments you might want to consider when implementing DriveLock.

- Information about how to install DriveLock and how to deploy your configuration settings is covered in the document “DriveLock Planning – Installation – Deployment”. It is recommended that you read this planning document prior to the others.
- The DriveLock Full Disk Encryption disk recovery keys are mandatory for any emergency recovery or data recovery procedure. Please make sure you backup these important files regardless whether you store them on a central network location or on the Security Reporting Server.
- Backing up your DriveLock Group Policy regularly by using DriveLock export capability will be helpful in case your Group Policy gets damaged due to Active Directory communication problems while you adjust some configuration settings.

## 5 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.

### 5.1 DriveLock and Windows Vista

On Windows Vista 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.
- On rare occasions empty files may be created when content filtering blocks file operations:  
If the file filtering component detects invalid content a file, the Agent stops the operation and reports an “Access denied” error to the operating system. Versions of Windows prior Vista handle this error correctly. Windows Vista prompts the user to retry the operation and displays the incorrect error message “The file does already exist on the target media.” If a user then cancels the operation, Windows Vista creates an empty file on the target media.

### 5.2 Automatic updates and Application Launch Filter

If the Application Launch Filter is configured in 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.

### 5.3 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.

It has been observed that BIOS legacy USB support for USB keyboards and mice on some computers interferes with the DriveLock Full Disk Encryption USB stack, and can prevent two-factor authentication from completing successfully. If this occurs, disable the legacy support for USB keyboards and mice in the BIOS.

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 ([http://www.drivelock.de/s\\_kb.aspx?ID=110](http://www.drivelock.de/s_kb.aspx?ID=110)). 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.

For pre-boot authentication the NetBIOS domain name must not contain a period. (Windows 2000 and newer don't allow the creation of such domains. However, the name of a domain that was migrated from Windows NT may contain a period.)

# 6 Version History

## 6.1 DriveLock Version 5.6.0.400

The following issues have been changed or fixed since DriveLock Version 5.5.0.393:

- This release contains an updated version of DriveLock Full Disk Encryption.
- The password needed to uninstall DriveLock manually (if configured) can now be used either in plain text or encrypted (see our knowledge base for more details on how to uninstall DriveLock manually).
- An incompatibility between DriveLock FDE's pre-boot authentication and NetBIOS names containing a "." has been fixed.
- DriveLock FDE will be only installed on those computers added to the FDE licensed computer list previously.
- An error when creating an encrypted container manually and directly on a mobile device has been fixed.
- When using the DriveLock FDE on multiple partitions you can view the correct state of the encryption process within the DriveLock Management Console.
- In some cases a very fast Windows Authentication might prevent an encrypted mobile device to mount automatically.
- Correct event log information is logged when editing a DriveLock policy directly on a Terminal Server.
- Complete recovery information is send to the Security Reporting Center also when enforced encryption has been used.
- In some very rare cases the installation of DriveLock FDE might fail on high performance computers for the first time.
- When special configuration is used within whitelist rules for Terminal Server drives, a wrong filter template might have been used by the DriveLock Agent.
- Encryption of a complete partition failed (encryption of mobile devices) when offline recovery had been switched on.
- Recovery information of container files larger than 2 GB is now correctly transmitted to the Security Reporting Center.

## 6.2 DriveLock Version 5.6.0.393

The following issues have been changed or fixed since DriveLock Version 5.5.0.387:

- This release contains an updated version of DriveLock Full Disk Encryption.
- After the installation of Full Disk Encryption is complete, DriveLock pauses for 30 seconds instead of 5 seconds before restarting the computer.
- Manually created pre-boot authentication accounts can only contain letters, numbers and the characters “-“ and “\_”.
- An error that could occur when attempting to install DriveLock FDE without a valid license was fixed.
- An incompatibility of command-line tools for manually configuring FDE was fixed.
- Under certain circumstances user information was not listed for some events in the SRC.

## 6.3 DriveLock Version 5.5.0.387

The following issues have been added since DriveLock Version 5.5.0.366:

- A lost or forgotten removable media encryption password can now be reset using a challenge/response mechanism.
- Drive locking rules for Citrix and Terminal Server drive mappings can now include file filters for controlling and monitoring the flow of data.
- New functionality in file filter templates enables the processing of files without an extension.
- The Application Launch Filter (ALF) can now generate audit events when allowed programs are started in Blacklist mode.
- You can now create an application template based on a scan of all programs installed on a computer. Such a template can be used to easily allow all of these programs to be started.
- You can now create Application Launch Filter rules from an online database containing millions of application. This database is constantly updated and can be easily accessed while creating an application rule.
- The Operating section in the Security Reporting Center has been expanded to include additional information and details about Full Disk Encryption and status and available recovery options.
- You can now add Organizational Units from trusted domains to the list of licensed computers.
- A new *Fast Recovery* mechanism for Full Disk Encryption allows the targeted recovery of business critical files from a hard disk that has become inaccessible within just a few minutes.

The following issues have been fixed since DriveLock Version 5.5.0.366:

- The SRC doesn't display all user accounts in the format *domain\user*.
- In some cases the Application Launch Filter blocked the execution of the program *TrustedInstaller*, even though a whitelist rule for it exists.
- Agent remote control sometimes incorrectly reported that the system partition C: was encrypted even though a different partition was encrypted.
- The Unlock computer wizard stops responding after you changed the global Agent unlock settings in the DriveLock Management Console.
- DriveLock Full Disk Encryption certificates cannot be created when running the DriveLock Management Console on a 64-bit operating system.
- Vendor and Product ID information is not available on SD cards connected using the Secure Digital Host-Controller.
- Vulnerability of Agent Remote Control wizard, which could theoretically be manipulated to accept prepared response codes.

## 6.4 DriveLock Version 5.5.0.366

The following issues have been added since DriveLock Version 5.5.0.361:

- 64-bit support for DriveLock Agent and DriveLock Management Console.

The following issues have been fixed since DriveLock Version 5.5.0.361:

- WAN Miniport devices are sometimes not reactivated after reboot if they were previously disabled by using a network profile location.
- On rare occasions, when using very large external drives, existing unencrypted files may be deleted or not copied to a new encrypted container.
- If the service account used to access a UNC path to download configuration information has write access to that location, the file "*DLFileStore.zip*" may be deleted.
- The content of the file storage is not transferred correctly if the configuration file is loaded from an FTP location.
- The list of configured clients from the SRC cannot be automatically loaded into the DriveLock Management Console to activate client awareness.
- When opening the Properties dialog box of a DriveLock Management Console node, a previously added Novell user account may appear twice.
- When using the command line tool *DLCrypt* to generate an encrypted container file, the administrator password may not be set correctly.

- An encrypted container file cannot be mounted, when the command line tool *DLCrypt* is used and the password contains a diacritical character (Umlaut).
- It is not possible to add an entire domain to a license as an organizational unit.
- User notification messages are not displayed correctly when authorized media is inserted.
- A configuration file cannot be re-loaded from an FTP or HTTP location if a previous file transfer failed.

## 6.5 DriveLock Version 5.5.0.361

- It is now easier to deny access to the DriveLock Agent for everyone. This extends the existing functionality of denying access to specific users and groups.

The following issues have been fixed since DriveLock Version 5.5.0.349:

- Incorrect FDE licensing information is sent to the SRC when computers are licensed individually.
- Access permissions to MMC functions may be incomplete after exporting and re-importing configuration information.
- DriveLock Policy File Storage cannot be accessed when configuration files are used to store DriveLock configuration information.
- Updating a DriveLock GPO will force the Agent to check current networks and re-assign the current network profile. This could result in a Group policy refresh, if configured in the policy.
- You can't select any device in the Record Encrypted Media wizard after DriveLock receives an error from any recording device.
- GPO information is not collected completely by the DriveLock Support Tool in Windows Vista.
- User messages that are configured in whitelists are truncated if they contain more than 255 characters.
- The file filter may block some file types even if only auditing is configured in a template.
- You cannot import a configuration from a file (\*.dlc) that contains an empty Policy File Storage.
- On rare occasions Windows shell operations (for example, displaying the Open File dialog box) may take slightly longer if encryption is not licensed correctly.

## 6.6 DriveLock Version 5.5.0.349

The following issues have been added since DriveLock Version 5.5.0.345:

- Dutch and French were added as available languages.

The following issues have been fixed since DriveLock Version 5.5.0.345:

- Memory consumption could be high when you configured a SRC connection and the computer is in offline mode.
- The SRC installation failed if you use SQL 2000 Server.

## 6.7 DriveLock Version 5.5.0.345

The following issues have been fixed since DriveLock Version 5.0.1.324:

- Enforced encryption does not use all available disk space for encryption when the removable drive is empty.
- Incorrect number of licensed computers calculated when computer can't be deleted because of connection problems.
- Under certain circumstances, the configuration wizard locks CD-ROM drives when you select to lock only USB-connected drives.
- User accounts are sometimes not correctly displayed in event messages when you run the DriveLock Management Console in a Remote Desktop Connection session.
- Duplicate event entries are generated under certain circumstances even though you configured DriveLock to suppress them.
- When you attempt to change the password for an encrypted container and don't enter the existing password, DriveLock indicates that the password was changed even though it was not changed.
- Novell users are recognized only after a CD-ROM is locked.
- In rare occasions a user notification message is displayed even though you have configured a whitelist rule not to display any messages.
- You cannot use carriage return characters in the comment field of whitelist rules.
- Enforced encryption may stop and fail in some situations when you connect a second unencrypted removable drive.
- Time restrictions are not recognized within drive size whitelist rules under certain circumstances.
- Application whitelist rules don't recognize folders for locking or unlocking applications.
- On very rare occasions user notification messages fail to respond when enforced encryption is used in conjunction with a whitelist rule for encrypted containers.
- A DriveLock Group Policy doesn't display the DriveLock configuration node when you edit the policy on a computer running Windows Server 2008.
- Sometimes CD-ROM media are not authorized correctly as media information could not be completely scanned.

## 6.8 DriveLock Version 5.0.1.324 (SP1)

The following issues have been fixed since DriveLock Version 5.0.0.314:

### 6.8.1 General

- Incorrect or no error message is displayed when a user attempts to change a GPO without having the permissions required to save changes.
- DriveLock device drivers are not correctly signed for Windows Vista driver signing.
- The DriveLock Agent service generates “Service did not start within 30 seconds” messages in the Windows Event Log when licensed computers are specified in the DriveLock policy.
- Serial numbers are copied in entirely in capital letters from Device Scanner to new rules even though serial numbers are case-sensitive.
- “Set to unconfigured” is missing or does not reset all options for some configuration elements (Event message transfer settings, Network profiles, Administrative password).
- Incorrect error messages are created when shadow copies cannot be copied to the configured network location.
- “Invisible” permissions for the MMC node “Configuration files” do not work.
- Permissions for MMC nodes do not work correctly when a user changes settings by using the toolbar.
- When running commands at drive insertion / removal, the parameter %SIZE% does not work.
- Settings under “Drives | Settings | Shadow copy settings | Exception processes” do not work in some cases.
- In some cases empty files are created on removable drives when file filtering is active, a user tries to create new files and access is denied.
- Detection of VMware files (VMDK) does not handle all types of VMDK files.
- Detection of CAB files does not handle InstallShield CAB files.
- The DriveLock Agent service terminates unexpectedly when trying to load a configuration file using FTP or HTTP and the configured user name or password is incorrect.
- Nested groups do not work correctly in whitelist rules and for specifying licensed computers.
- In some cases network drive permissions are changed by DriveLock when these permissions contain an “Everyone – Full control” entry.
- MMC terminates unexpectedly when creating computer templates and the remote computer is not available.
- Device scanner: The columns “drives” and “devices” are reversed.

- In some cases file filtering is not active when DriveLock is configured to change drive letters of removable drives.
- In some cases the DriveLock Agent is not started on very fast computers and when a user immediately logs on.
- Windows Vista: The DriveLock control panel program displays an incompatibility warning.
- Windows Vista: Cosmetic problems with some icons and bitmaps.
- Windows Vista: In some cases user notifications for blocked applications do not work.
- Dutch version: Start menu items are displayed in English.

## 6.8.2 DriveLock Encryption

- In some cases when enforced encryption is enabled, the Agent can't mount volumes. This problem occurred primarily on fast computers and was caused by a race condition when starting the encryption device driver.
- Secure deletion does not work if file filtering is active on the target drive.
- Some context menu items for encryption are displayed even though DriveLock Encryption is not licensed.
- Password cannot be changed when a container is mounted using enforced encryption.
- Start menu items are disabled by policy but can be run using undocumented command line functions.
- Unmounting encrypted drives does not work when file filtering is configured for encrypted drives.
- Windows Vista: Mounting a container file using enforced encryption does not work if the administrative password is used for mounting.
- The Mobile Encryption Application terminates unexpectedly when importing the first file into an empty encrypted container.

## 6.8.3 Network Profiles

- After reboot and user login the wrong network profile icon is displayed in user notification area.
- Users can view and change existing personal profiles when the option "Enable creation of personal profiles" is changed after users created profiles.

## 6.8.4 Security Reporting Center

- The SRC is not running properly after installation on systems with missing or miss-configured prerequisites.

## 6.9 DriveLock Version 5.0.0.314

The following issues have been fixed since DriveLock Version 5.0.0.313:

- Vulnerability of Agent Remote Control (Possible Buffer Overflow Vulnerability, Secunia Advisory SA26951), which could theoretically be used to crash the Agent.
- In some rare cases, Agent Remote Control permissions are not applied in Novell environments.

## 6.10 DriveLock Version 5.0.0.313

The following issues have been fixed since DriveLock Version 5.0.0.311:

- Improvements related to the DriveLock startup process when groups containing licensed computers are specified.

## 6.11 DriveLock Version 5.0.0.311

The following issues have been fixed since DriveLock Version 5.0.0.308:

- If a Group Policy Object contains a version 4.1 license file, the activation wizard may fail during the re-activation process.
- The license information is not displayed completely.
- The header information contained in MP3-files is evaluated incorrectly.
- User access rights for features in a Group Policy Object are only valid for this GPO but not for other GPOs.
- Proxy settings defined in network profiles are sometimes applied only after they are confirmed by using the Internet Explorer settings dialog box.
- The Management Console may display an error message when importing a .DRL-file that contains a specific configuration setting.
- Windows Vista displays an error message about an incorrect desktop path when selecting the location for a new encrypted container file.

## 6.12 DriveLock Version 5.0.0.308

The following issues have been fixed since DriveLock Version 5.0.0.307:

- Under certain conditions users selected from Novell eDirectory are not correctly assigned to drives and devices.
- An error may occur when connecting an encrypted partition.