



DriveLock 6

What's New?

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.

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.

» 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.

» USER INTERFACE FACELIFT

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.

» 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.

» 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.

» 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.

» 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.

» ENCRYPTION 2-GO

DriveLock's removable media encryption, which was previously called "Encryption License Classic", has been renamed to "Encryption 2-Go". 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.

» 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.

» REPORTING UND 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.