



Administration Guide 2021.1

5/20/2021

Table of Contents

Part I	Document Conventions	11
Part II	DriveLock Management Console	13
	1 Management Console Structure	14
	2 Changing the User Interface Language	15
	3 Checking for Updates	16
	4 Configuring Server Connections	17
	Connection Settings for Proxy Servers	19
	5 Selecting the DriveLock Configuration Mode	19
	6 Configuring User Permissions to Console Nodes	20
Part III	Deploying DriveLock Configuration Settings	23
	1 Centrally Stored Policies	25
	Policy Assignments	26
	Configuring the Agent	27
	2 Group Policy	28
	3 Configuration Files	29
	4 Local Computer Policy	31
	5 Computer-specific policy customizations	33
	6 Resultant Set of Policies (RSOP)	34
Part IV	Configuring the DriveLock Enterprise Service	35
	1 Creating Server Connections in the DriveLock Management Console	36
	2 Administering DES Servers	37
	3 DES Operating Modes	38
	Central Server	38
	Linked Server	39
	Linked DES to Connect to the DriveLock Cloud	40
	Registering a Linked DES as a Cloud Relay	41
	Changing the Operating Mode	42
	4 Assigning Permissions	43
	5 Configuring Maintenance Operations	44
	6 Configuring Update Synchronization	45
	7 Configuring Network Settings	46
	Using a Proxy Server	47
	Configuring E-Mail Settings for Scheduled Reports	48
	8 Using a Multi-Tenant Environment / SaaS	49
	Creating a Tenant	50
	Assigning Agents to a Tenant	50
	Deleting a Tenant	51
	Performing Active Directory Object Inventory Collection	51
	Tenant-Aware Certificate Management	53
	9 Viewing License Information	53

10	Customer Experience Improvement Program	54
11	Viewing the DriveLock Enterprise Service Status	54
Part V	DriveLock Groups	56
1	Creating DriveLock Groups	57
	Creating Static Computer Groups	58
	The Add Button	60
	The Import Button	60
	Creating Dynamic Computer Groups	61
	Using Groups in Policies	64
	Policy Assignments	65
Part VI	Configuring Global DriveLock Settings	69
1	Using Predefined Security Configurations	70
2	Creating Configuration Reports	71
3	Activating Your License	73
4	Agent Hardening and Global Security Settings	75
	Configuring Global Security Settings in Basic Configuration mode	76
	Configuring Global Security Settings in Extended Configuration mode	80
	Permissions for the DriveLock Agent Service	80
	Locking Down the DriveLock Agent	82
	Running DriveLock in Windows Safe Mode	82
	Password to Uninstall DriveLock	83
	Agent Remote Control Settings and Permissions	84
5	Configuring the Agent User Experience	84
	Configuring the Agent User Experience in Basic Configuration mode	85
	Configuring the Agent User Experience in Extended Configuration mode	89
	Taskbar notification area settings	89
	Offline Unlock Control Panel Settings	90
	User Interface Language on Agents	92
6	Connecting to the DriveLock Enterprise Service	92
	Configuring DriveLock Enterprise Service Connections	93
	Proxy Server	94
	Proxy Settings on the Agent	95
	Monitoring Agents by Using the DriveLock Enterprise Service	96
	Agent Monitoring Using the DriveLock Management Console	96
	Sending Licensed Computer Information to the DES	98
7	Configuring the DriveLock Simulation Mode	99
8	Trusted Certificates	100
	Checking trusted certificates in the Management Console	100
	Selecting trusted certificates	101
9	Using the DriveLock Policy File Storage	103
10	Using Multilingual Notification Messages	107
	Defining Languages and Standard Message Texts	108
	Defining Custom Message Texts for Multiple Languages	111
11	Configuration Filters and Conditional Settings	114
	Creating a configuration filter	115
	Use case	117
12	Configuring Additional Settings	119
	Configure the Internet Connection Firewall to Allow Remote Control	119
	Advanced DriveLock Agent Settings	120
13	Self-service groups	122

Configuring self-service groups	123	
Start the self-service wizard	125	
Part VII	Settings in Rules Across Modules	127
1	User Permissions	128
2	Time Limit Settings	128
3	Settings for Computers	130
4	Logged on Users	130
5	Network Settings	132
6	Additional Options	133
Part VIII	Endpoint Detection and Response (EDR)	134
1	Event Transfer	135
Configuring Event Message Transfers	135	
Configuring Event Transfer Destinations	136	
Configure the event log destination	137	
Configure SMTP server settings	137	
Configure SNMP server settings	137	
Configuring Enterprise Service connection settings	138	
Additional Event Transfer Options	138	
Anonymizing event data	138	
Transfer options	139	
Customizing the reported computer name	140	
2	Event Responses	140
3	Event Filters	140
4	Alerts	142
Part IX	Locking Drives and Devices	143
1	Locking Drives	144
Configuring Drive Locking In Basic Configuration Mode	146	
Enabling Drive Locking	146	
Configuring Basic Whitelist Rules	151	
Configuring Advanced Drive Locking Settings	155	
General Drive Locking Settings	155	
Global Security Settings for Controlling Drives	155	
Configuring End User Messages	157	
Configuring User Notification Messages for Locking Drives	157	
Configuring File Digest Generation	158	
Volume Identification Files	159	
Shadowing Configuration	161	
Drive Monitoring Using S.M.A.R.T.	161	
Advanced Global Settings for Controlling Drives	162	
Enabling Drive Locking	162	
Creating Drive Rules	165	
Organizing Drive Whitelist Rules	166	
Creating Whitelist Templates	168	
Vendor/Product ID Rule	170	
Drive Collection Rule	173	
Network Drives Rule	175	
WebDAV-Based Network Drives	176	
Drive Size Rule	178	
Base Rule	179	
Terminal Services Rule	180	

Creating a Rule Based on a Template	180
Hardware-ID Rule	181
Common Settings for Drive Whitelist Rules	182
Controlling and Auditing File Access	182
Assigning Drive Letters	183
Defining Custom Notification Messages	184
Additional Options	186
Specifying Commands	189
Locking and Controlling Recording to CDs/DVDs	191
Creating File Filters	194
Defining File Types	194
Defining File Type Groups	197
Creating a New File Filter Template	199
Using a File Filter Template	208
Using File Filter Templates with Encrypted Drives (Encryption 2-Go)	209
Creating Drive Collections	210
Using Media Authorization	213
Monitoring Data Transfers by Using Shadowing	216
Configuring Global Shadowing Settings	216
General Settings	217
Client Options for Shadowing	218
Shadowing Exceptions	219
Server Upload Settings for Shadowing	220
Shadowing Time Limitations	221
Network Limitations	222
Encryption	222
Configuring Shadow Copies in Drive Whitelist Rules	223
Viewing Shadow Copies	226
2 Locking Devices	230
Configuring Device Locking Using Basic Configuration Mode	231
Configuring Advanced Device Locking Settings	241
General Device Locking Settings	241
Configuring User Notification Messages for Locking Devices	241
Advanced Global Settings for Controlling Devices	243
Enabling Device Locking	243
Granular Control of iTunes-Synchronized Devices	247
Configuring Serial and Parallel Port Locking	252
Creating Device Rules	252
Creating Device Collections	256
Bluetooth Devices	259
Using Computer Templates	260
Creating a New Computer Template	261
Creating a Computer Template Based On the Local Computer	262
Creating a Computer Template Based On a Remote Computer	262
Creating a Pre-Defined Template from the Database	263
Creating an Empty Template	264
Working with Computer Templates	264
Editing a Computer Template Device List	265
Importing New Devices into a Computer Template	266
Exporting Devices from a Computer Template	266
Defining Computer Template Permissions	267
Activating a Computer Template	268
Displaying Devices Defined By a Computer Template	268
Part X Configuring Network Profiles	270
1 Configuring Global Network Profiles Settings	274
Defining Network Profile End-User Appearance	274

Disabling Simultaneous Wi-Fi and LAN Connections	275
Using Third-Party VPN Clients	276
2 Defining Network Locations	277
Active Directory Site	279
Network Location Based on IP Information	281
Network Adapters	282
Geographic Locations	282
Wireless Network SSID	284
Other Locations	284
Command Result	285
3 Creating Configuration Profiles	286
Internet Explorer Proxy Settings	287
Windows Live Messenger / MSN Messenger Settings	288
Default Printer and Group Policy Processing	289
4 Using Network Locations in Whitelist Rules	289
5 Defining User-Specific Network Profiles	290
Part XI DriveLock Application Control	292
1 Standard Application Control	293
Basic configuration	294
Configuring the Scanning and Blocking Mode	295
Auditing and simulation	296
Whitelist mode and Blacklist mode	296
Configuring basic application rules	297
Configuring Simple Application Rules	298
2 Extended Application Control	301
Extended Configuration	301
Configuring the Scanning and Blocking Mode	302
Auditing and simulation	303
Whitelist mode and Blacklist mode	304
Whitelist mode	305
Blacklist mode	305
Configuring a Hash Algorithm for Hash-Based Rules	305
Configuring User Notifications	306
Special Settings	307
Configuring Application Rules	308
Using Application Hash Databases	308
Using Publisher Certificate Rules	312
Using File Owner Rules	314
Using Hash Rules	316
Using Special Rules	318
Other Application Rules	320
Using file path rules	320
Using Application Templates	321
Adding a single application	323
Adding a set of applications	324
Scanning/Blocking DLLs	325
Predictive Whitelisting	325
Configuring Common Rule Settings	328
Configuring User Settings	328
Configuring time limits	328
Configuring Computer Settings	329
Configuring network limitations	330
3 Application Permissions	331
Defining Application Permissions	332

Options in the Dialog	333
Priority	333
Accessing Application	333
Access Mode	333
Target	334
Action	334
Activating and Inheriting	335
Computers, Networks, Time Limits	335
Use Cases	336
Use Case 1: Prevent PowerShell from Being Started	336
Use Case 1 with Application Collection	337
Use Case 2: Restrict Loading a DLL	338
Use Case 3: Run Scripts	339
Use Case 4: Read a Specific Directory	340
Use Case 5: Write to a Specific Directory	342
Use Case 6: Restrict Registry Access	343
Application Collections	345
Application Collection for Microsoft Office	346
Script Definition	347
Part XII DriveLock Disk Protection	349
1 Preparing to Deploy DriveLock Disk Protection	352
2 Basic Configuration of Disk Protection	354
Creating Recovery Keys	354
Exporting and Importing Encryption Certificates	359
License Settings	360
Disk Protection Settings	361
3 Configuring Disk Protection in Extended Configuration Mode	364
Installation Settings	365
Configuring Pre-Boot Authentication	369
Authentication Methods and Logon Settings	369
AD User Synchronization	371
Users	372
Emergency Logon	373
Wipe the PBA database	375
Network PBA	377
Encryption Settings	378
Configuring Encryption Settings	378
Configuring the Backup of Recovery Data	380
4 Recovery Procedures	381
Viewing Diagnostics Data	381
Emergency Logon Procedure	383
Recovering Encrypted Disks	388
Creating the Files Required for Decryption	388
Creating Recovery Media	391
Recovering Disks	399
5 Uninstalling DriveLock Disk Protection	401
Uninstalling DriveLock Disk Protection Completely	402
Decrypting Hard Disks	403
Uninstalling or Reconfiguring Disk Protection on a Single Computer	403
6 User Logon	406
UEFI Pre-Boot Authentication	406
Authentication with User Name and Password	408
Smartcard Authentifizierung	413
BIOS Pre-Boot Authentication	414
Authenticating With User Name, Password and Domain Name	414

Authenticating With Smartcard or Token and PIN	415
Windows Authentication	416
Part XIII BitLocker Management and BitLocker To Go	417
Part XIV DriveLock Encryption 2-Go	419
1 How DriveLock Encryption 2-Go Works	420
DriveLock Encryption Algorithms	420
DriveLock Encryption Modes	421
2 Configuring DriveLock Encryption	422
Configuring Encryption Using Basic Configuration Mode	422
Configuring General Encryption Settings	423
Configuring Enforced Encryption	425
Configuring Password Recovery	427
Configuring Encryption Using Extended Configuration Mode	430
Configuring Global Parameters	430
Encryption Strength Settings	431
Encryption End User Appearance	437
Encrypted Drive Settings	442
End user restrictions	445
Configuring Password Recovery	451
Configuring an Administrative Password	452
Creating an Offline Recovery Certificate	456
Configuring Enforced Encryption	463
Settings Available for All Automatic Encryption Rules	464
Creating Multiple Encryption Rules	469
Creating User Selection Rules	471
3 Recovering Encrypted Containers	475
User-Initiated Password Recovery	475
Recovering Encrypted Drives and Folders	475
Part XV DriveLock File Protection	477
1 How Does DriveLock File Protection Work?	478
2 Supported Encryption Mechanisms	479
3 Configuring DriveLock File Protection	480
Creating a Master Certificate for Key Management	480
Configuring Certificate Management	481
Configuring Encryption Rules for Clients	482
Configuring encryption settings	483
Configuring the encryption user interface	484
Configuring Settings for Encrypted Folders	485
Configuring Additional Settings	486
Configuring Enforced Encryption	486
Configuring Recovery Certificates	487
Company certificate	489
4 Managing User Accounts and Certificates	489
How User Administration Works	490
Managing User Accounts	490
Managing Groups	492
Managing Certificates	493
5 Centrally Managing Encrypted Folders	495
Creating an Encrypted Folder	495
Modifying Permissions	496
6 Recovering Encrypted Folders	497

7	Reporting and Analysis	498
Part XVI	Defender Management	499
Part XVII	Security Awareness	501
1	Usage Policies	502
Part XVIII	Inventory and Vulnerability Scan	506
1	Settings	507
	Client Compliance	507
	Configuring Hardware and Software Inventory	508
Part XIX	Operating System Management	511
1	Power Management	512
2	Local Users and Groups	513
	Settings	513
	User and group rules	514
3	Firewall	516
	Settings	516
	Inbound and outbound rules	517
Part XX	Using Agent Remote Control	518
1	Policy Settings for Agent Remote Control	519
2	Performing Agent Tasks	521
	Viewing Agents	521
	Connecting to a DriveLock Agent	523
	Connect as	524
	Viewing the Agent Configuration (RSOP)	524
	Viewing Currently Attached Devices	527
	Manually Updating the Policy	532
	Displaying Inventory Data	533
	Viewing the disk encryption status	534
	Manually Uploading Disk Protection Recovery Data	535
	Manually Uploading Encryption 2-Go Recovery Data	536
	Viewing Disk Health Information (S.M.A.R.T.)	536
	Activating Tracing	537
	Displaying and Deleting Locally Learned Applications	538
	Checking the Defender Status	540
	Disconnecting from an Agent	541
3	Unlocking Agents	541
	Configuring General Unlocking Settings	541
	Unlocking Drives, Devices and Smartphones	541
	Setting Time Limits and Suspending Restrictions	542
	Temporarily Unlocking a Single Online Agent	545
	Temporarily Unlocking an Offline Agent	546
	User Procedure to Unlock an Offline Agent	546
	Administrator Procedure to Unlock an Offline Agent	547
	Temporarily Unlocking Multiple Agents	550
	Configuring Default Settings for Agent Remote Control	552
Part XXI	Software Deployment and Update	554
1	Manually Updating DriveLock	555

2	Publishing Software Packages	556
3	Push Installation of DriveLock	559
	Per-Server Global Settings	560
	Automatic Push Groups / OUs	560
	Execute Push Installation	560
4	Configuring Automatic Updates	561
	Configuring Fully Automatic Updates	562
	Configuring Semi-Automatic Updates	562
	Disabling Automatic Package Downloading	563
Part XXII	Using DriveLock in Terminal Server Environments	565
1	Terminal Server Connections	566
	Fat Clients / Desktop Clients	566
	Windows Embedded Clients	567
	Virtual Clients	567
	Thin Clients	567
	Thin Clients by Wyse Running Linux V6	567
2	Configuring Drive Control	568
	Global Permissions	568
	Rules Based on Mapped Drive Letter	568
	Rules Based on Hardware Characteristics	570
	Using the File Filter	570
3	Using Application Control	571
Part XXIII	Troubleshooting and Tools	572
1	Viewing Information about Drives and Containers	573
2	Commands for Troubleshooting	574
3	Troubleshooting Network Adapters	574
4	Creating a Trace File	575
	Creating a DriveLock Driver Trace File by Using the Support Tool	575
	Creating a DriveLock Driver Trace File by Using the Command Line	576
	Creating a DriveLock Trace File by Using the Management Console	577
	Generating BitLocker-specific system information	578
5	Manually Refreshing the Policy	578



Part I

Document Conventions



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 you need to click or select.

Caution: This format means that you should be careful to avoid unwanted results, such as potential damage to operating system functionality or loss of data

Hint: Useful additional information that might help you save time.

Italics represent fields, menu commands, and cross-references. **Bold** type represents a button that you need to click.

A `fixed-width typeface` 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.



Part II

DriveLock Management Console



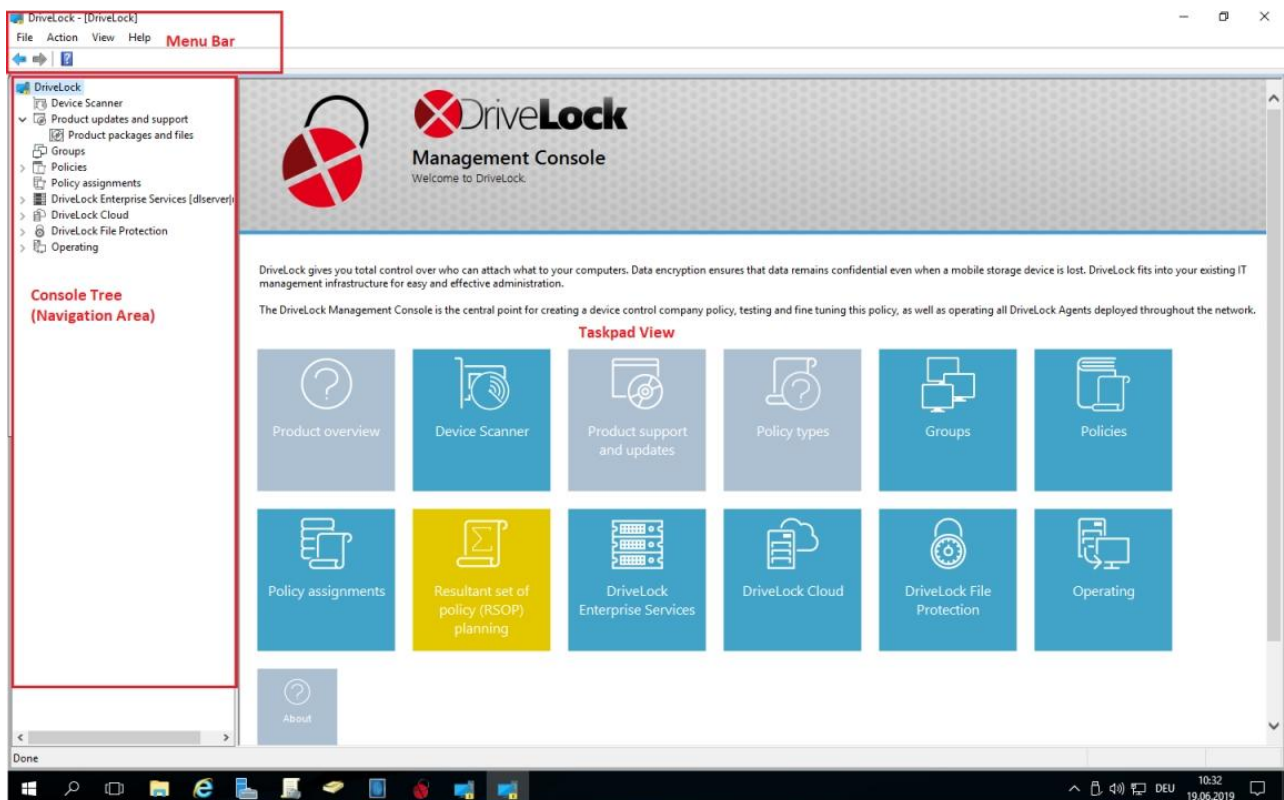
2 DriveLock Management Console

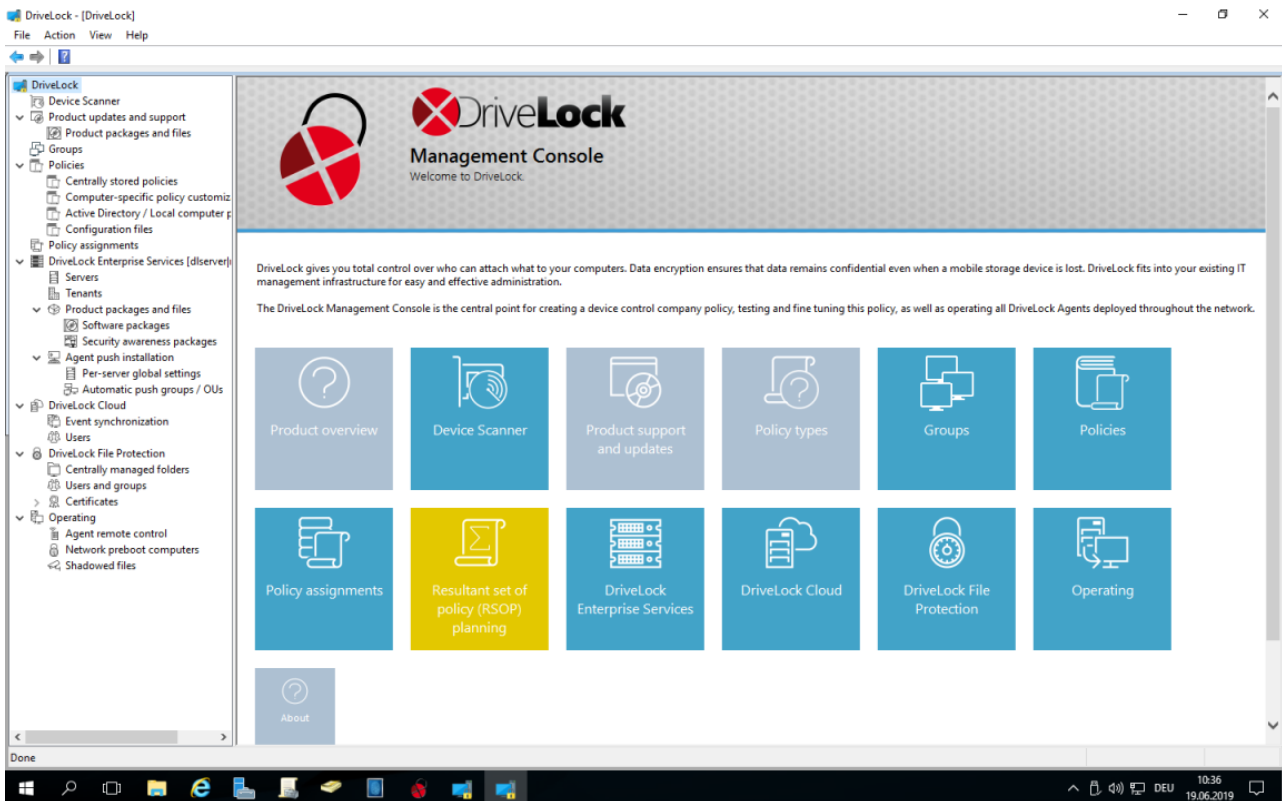
Use the DriveLock Management Console (MMC) to perform day-to-day management tasks and to configure DriveLock. This chapter covers how to use and configure the Management Console and how to restrict access to management functions so that only authorized administrators can use them.

2.1 Management Console Structure

The DriveLock Management Console (DMC) is a Microsoft Management Console (MMC) snap-in that can be used on its own or in conjunction with other MMC snap-ins.

After you have installed the DriveLock Management Console you can start it from the Windows Start menu under **All Programs / DriveLock / DriveLock Management Console**.





The menu bar at the top of the console contains the standard MMC menus and buttons that provide quick access to common functions. For example, clicking the question mark opens a Help window.

The console tree on the left is used to navigate through the various functional areas of the Management Console. Many nodes in the console tree contain subnodes that you can expand or collapse by double-clicking the node.

The right section of the Management Console displays taskpad views. Depending on the node you select in the console tree, taskpads contain links subnodes or configuration elements. You can navigate taskpad views by clicking the links in it.

You can right-click most nodes in the console tree and configuration areas in the classic MMC to display a context menu from where you can configure various settings.

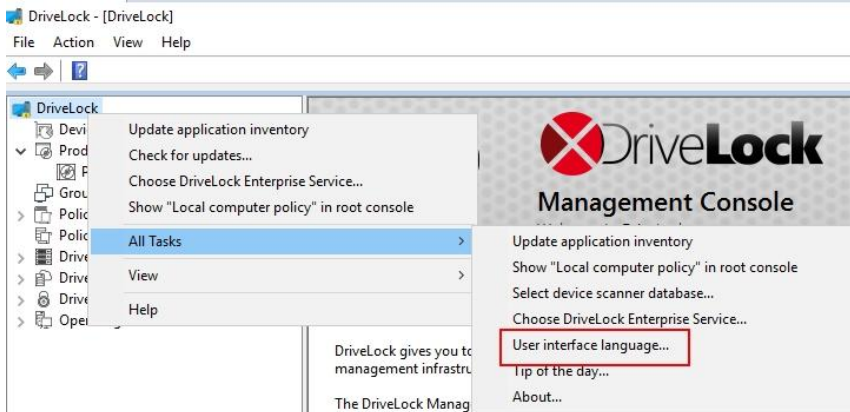
If you prefer the classic MMC view without taskpads you can optionally switch to that view (**Classic MMC view**) in several areas of the Management Console. Use **Context menu / View / Taskpad view** to switch back.

With DriveLock 7.5 the taskpad view has been optically structured more clearly using an Windows 8 like design (see the screen shots above). The functions are shown as tiles now. As far as there are no functional changes and no principal differences caused by the new design, this manual still uses the old screen shots.

2.2 Changing the User Interface Language

Right-click **DriveLock** then click **All tasks -> User interface language**.

Depending on which operating system language you use, some default buttons and menu items will be displayed in that language, not in the user interface language you select in DriveLock.



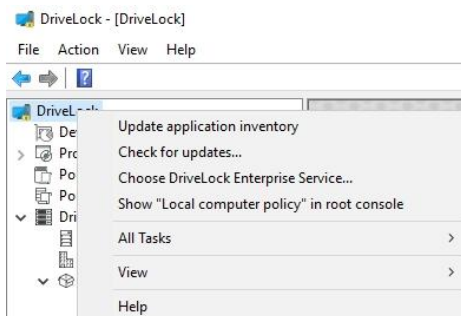
In the following dialog box, select the language.

A few Management Console elements, such as the menu bar and context menus are always displayed in the language for which you installed the Management Console or the operating system language and don't change when you select a different language.

Click **OK** to proceed. The Management Console switches to the selected language.

2.3 Checking for Updates

Right-click **DriveLock**, then click **Check for updates**.

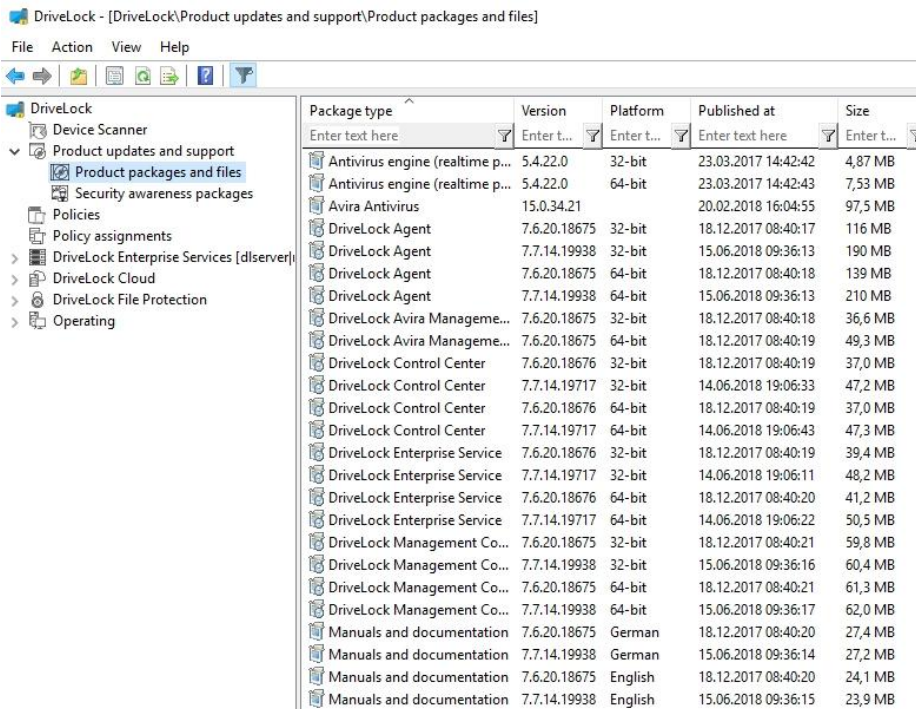


The program connects to the DriveLock Web site to check for available updates. If a newer version is available, a notification is displayed.

You can also view the current version of all DriveLock components under **Product updates and support -> Product packages and files**.

DriveLock - [DriveLock\Product updates and support\Product packages and files]

File Action View Help



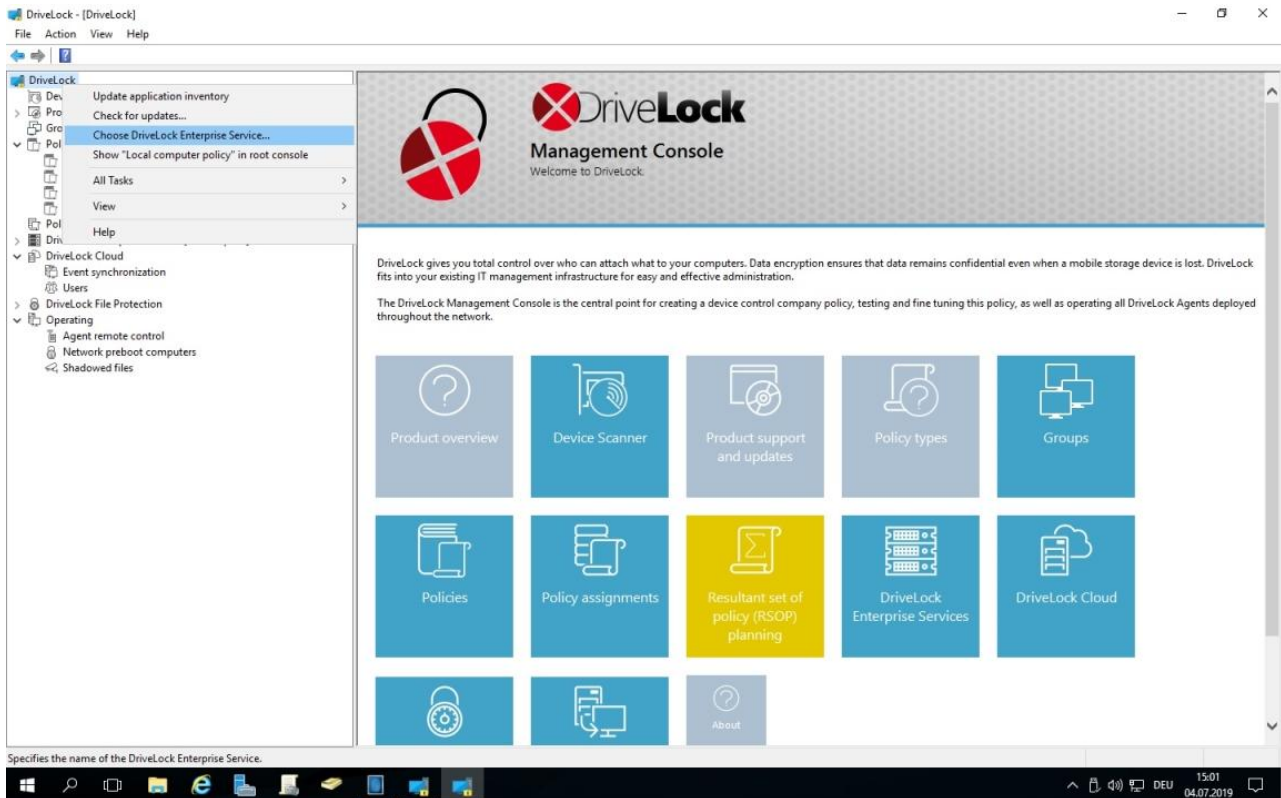
Package type	Version	Platform	Published at	Size
Antivirus engine (realtime p...	5.4.22.0	32-bit	23.03.2017 14:42:42	4,87 MB
Antivirus engine (realtime p...	5.4.22.0	64-bit	23.03.2017 14:42:43	7,53 MB
Avira Antivirus	15.0.34.21		20.02.2018 16:04:55	97,5 MB
DriveLock Agent	7.6.20.18675	32-bit	18.12.2017 08:40:17	116 MB
DriveLock Agent	7.7.14.19938	32-bit	15.06.2018 09:36:13	190 MB
DriveLock Agent	7.6.20.18675	64-bit	18.12.2017 08:40:18	139 MB
DriveLock Agent	7.7.14.19938	64-bit	15.06.2018 09:36:13	210 MB
DriveLock Avira Managem...	7.6.20.18675	32-bit	18.12.2017 08:40:18	36,6 MB
DriveLock Avira Managem...	7.6.20.18675	64-bit	18.12.2017 08:40:19	49,3 MB
DriveLock Control Center	7.6.20.18676	32-bit	18.12.2017 08:40:19	37,0 MB
DriveLock Control Center	7.7.14.19717	32-bit	14.06.2018 19:06:33	47,2 MB
DriveLock Control Center	7.6.20.18676	64-bit	18.12.2017 08:40:19	37,0 MB
DriveLock Control Center	7.7.14.19717	64-bit	14.06.2018 19:06:43	47,3 MB
DriveLock Enterprise Service	7.6.20.18676	32-bit	18.12.2017 08:40:19	39,4 MB
DriveLock Enterprise Service	7.7.14.19717	32-bit	14.06.2018 19:06:11	48,2 MB
DriveLock Enterprise Service	7.6.20.18676	64-bit	18.12.2017 08:40:20	41,2 MB
DriveLock Enterprise Service	7.7.14.19717	64-bit	14.06.2018 19:06:22	50,5 MB
DriveLock Management Co...	7.6.20.18675	32-bit	18.12.2017 08:40:21	59,8 MB
DriveLock Management Co...	7.7.14.19938	32-bit	15.06.2018 09:36:16	60,4 MB
DriveLock Management Co...	7.6.20.18675	64-bit	18.12.2017 08:40:21	61,3 MB
DriveLock Management Co...	7.7.14.19938	64-bit	15.06.2018 09:36:17	62,0 MB
Manuals and documentation	7.6.20.18675	German	18.12.2017 08:40:20	27,4 MB
Manuals and documentation	7.7.14.19938	German	15.06.2018 09:36:14	27,2 MB
Manuals and documentation	7.6.20.18675	English	18.12.2017 08:40:20	24,1 MB
Manuals and documentation	7.7.14.19938	English	15.06.2018 09:36:15	23,9 MB

The Management Console displays the newest version of all components. To download a component, right-click it and then click **Download**.

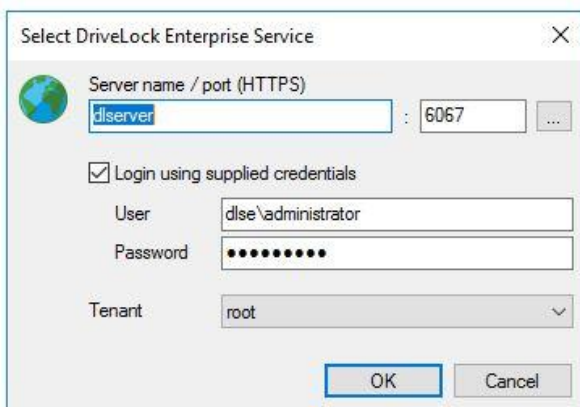
Click **Security awareness modules** to view the available modules which can be downloaded with the DriveLock Enterprise Service (DriveLock Enterprise Services -> Security awareness modules). If you have licensed the Security Awareness Content AddOn, all modules are listed; if not, you can see the modules that are available for demo purposes.

2.4 Configuring Server Connections

The DriveLock Management Console connects to the central DriveLock Enterprise Service to store information, such as license data or centrally stored policies, and to retrieve data. To ensure that the DriveLock Management Console can connect to the DriveLock Enterprise Service (DES) you need to configure a server connection.



To create a new server connection, right-click **DriveLock**, then click **Choose DriveLock Enterprise Service**.



Note: When the DriveLock Management Console connects with the DES the first time, DriveLock checks the DES certificate. Please refer to chapter [Certificates](#) for more information.

If the DriveLock Management Console was able to locate the DES using DNS-SD at startup, the server name appears in the dialog box. If the server does not appear, type the server name. If you configured the DriveLock Enterprise Service to use a non-standard port you must also type the port number.

To connect to the DriveLock Enterprise Service using a different user account than the one you are currently logged on with, provide the credentials of that account to use and then click **OK**.

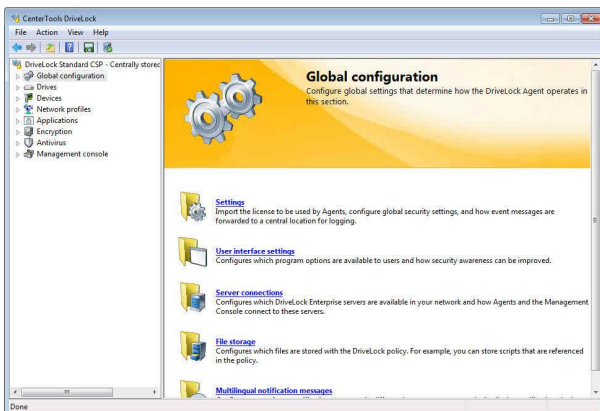
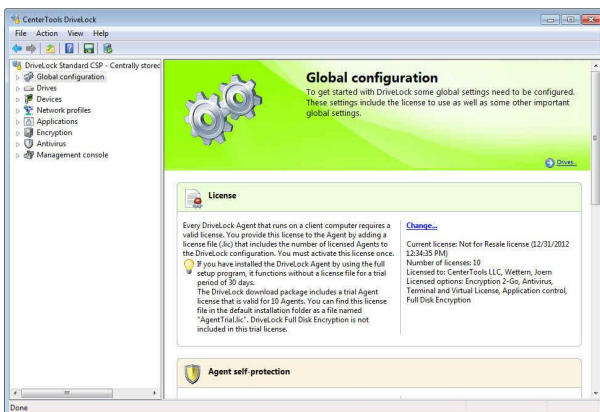
The account you use to connect to the DriveLock Enterprise Service must have been assigned access permissions in the DES. For more information about assigning permissions when installing the DriveLock Enterprise Service, refer to the *DriveLock Installation Manual*. For more information about configuring permissions after installation, refer to the chapter [Configuring the DriveLock Enterprise Service](#).

2.4.1 Connection Settings for Proxy Servers

The DriveLock Management Console and DOC.exe use the system proxy settings. For some actions, you can specify an explicit proxy.

2.5 Selecting the DriveLock Configuration Mode

The DriveLock configuration mode determines which taskpads are displayed when you create and edit DriveLock policies. You can select Basic Configuration or Extended Configuration. Basic Configuration mode is the recommended mode for administrators who are getting started with DriveLock. In this mode, rarely used configuration settings are not displayed and wizards are available that guide you through the all the steps that are required to perform most tasks.



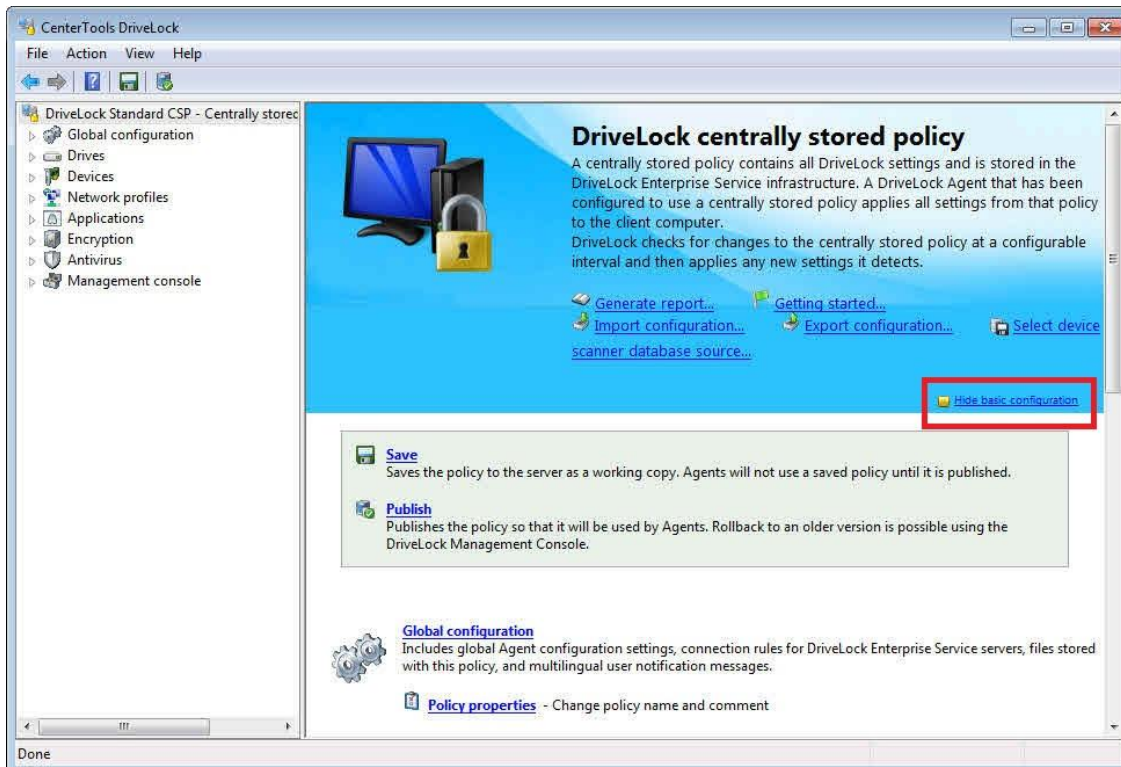
The left picture shows a configuration page in Basic Configuration. The picture on the right shows the same page in Extended Configuration mode.

In Basic Configuration mode, taskpad sections also display a colored header that indicates the state of the current configuration:

- **Red header:** Important settings have not been configured yet
- **Yellow header:** Some configuration settings may not be complete or as secure as they can be and should be reviewed
 - **Green header:** All settings are configured for secure operations

To disable or re-enable the Basic Configuration mode, in the policy window, in the console tree, click the top node and then click the Basic Configuration link in the taskbar.

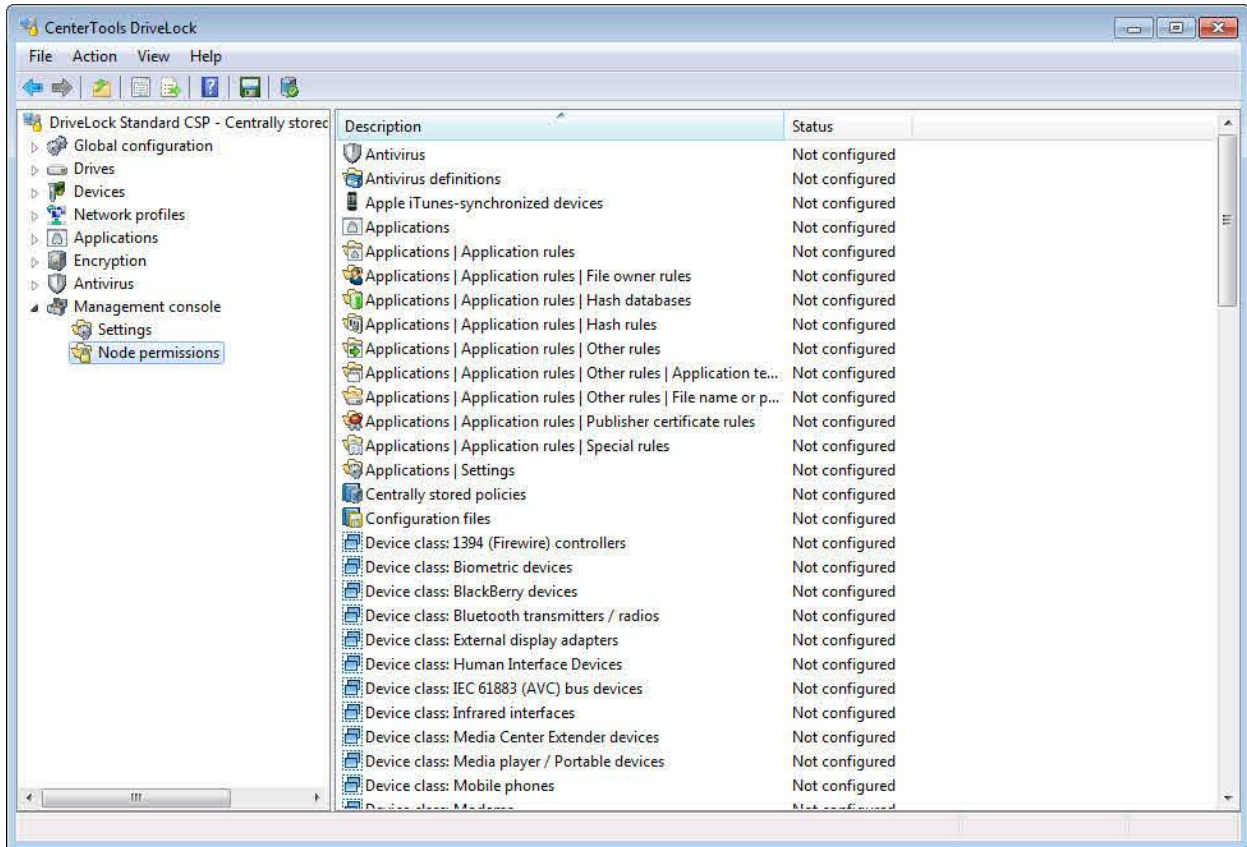
The first time you open a newly created policy, the *Getting started* window appears. Unless you are familiar with DriveLock, select **Assisted configuration** to create the initial policy settings.



To open this window at a later time, select the top node of the policy, and then in the right pane click **Getting started**.

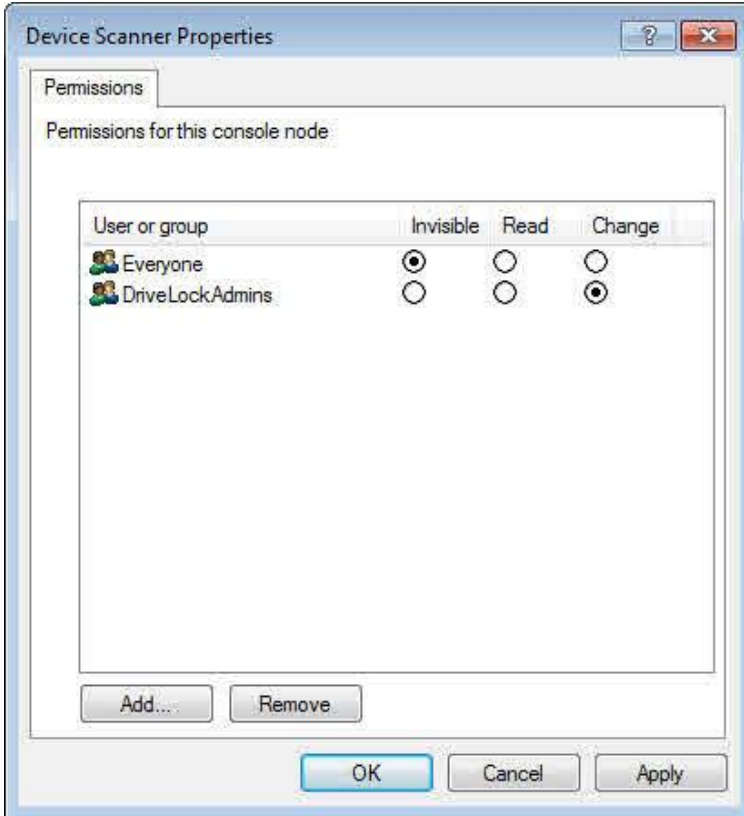
2.6 Configuring User Permissions to Console Nodes

You can configure the DriveLock Management Console to control which users and groups can access console functions. To control access, configure the permissions for nodes in the console tree. The permissions you configure in a policy are enforced by DriveLock Agents and can prevent users from installing and using the DriveLock Management Console on client computer without being authorized to do so. For more information about DriveLock policies, refer to the chapter [Deploying DriveLock Configuration Settings](#).



Click **Management console** -> **Node permissions** to view a list of all node permissions. The default setting for all nodes is *Not configured*. Until you change the permissions, the group “Everyone” has *Change* permissions to all nodes.

To view the detailed settings of an object, double-click it.



To assign node permissions to a user or a group, click **Add**, and then select a group or user. Click **Remove** to remove the selected account from the list.

You can assign the following access permissions:

- *Invisible*: The node is not displayed, and not accessible to the user.
- *Read*: The user can view the node and any configuration settings, but cannot change any settings.
- *Change*: The user can change all settings under the node.

If you assign permissions to more than one group and a user is a member of several of these groups, the permission setting with the highest priority that applies to the user or any of the groups is enforced. For example, when both the Invisible and the Change permissions apply to a user, the Change permission is enforced.

Each node must be configured with at least one user or group that has Change permissions. If you attempt to remove all Change permissions settings, DriveLock displays a warning message.



Part III

Deploying DriveLock Configuration Settings



3 Deploying DriveLock Configuration Settings

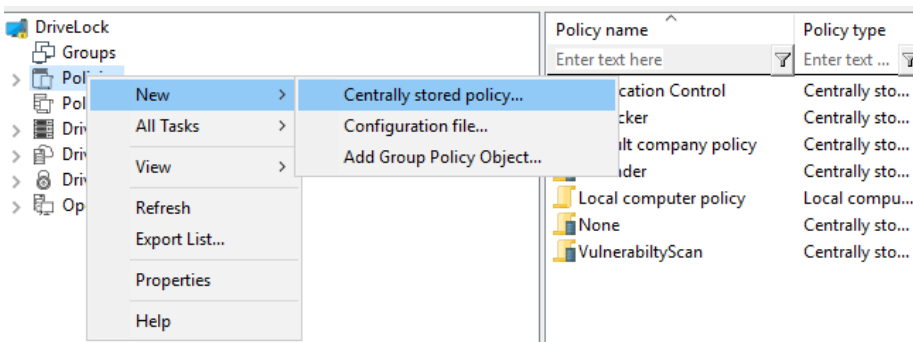
This section explains several methods for deploying configuration settings to client computers.

The following table provides an overview of the available deployment methods. You can use this information to help you determine which deployment method is most appropriate for your environment:

	Central Configuration	Requires DES	Uses Existing Infrastructure	History / Versioning	Scalability	Quick Configuration
Centrally Stored Policy	Yes	Yes	No	Yes	Good	Yes
Group Policy	Yes	No	Yes (AD)	No	Very good	No
Configuration File	Yes	No	Yes (UNC, http, ftp)	No	Acceptable	No
Local Policy	No	No	No	No	-	No

Before distributing settings to multiple clients on the network, we recommend that you first test them on one or more test clients.

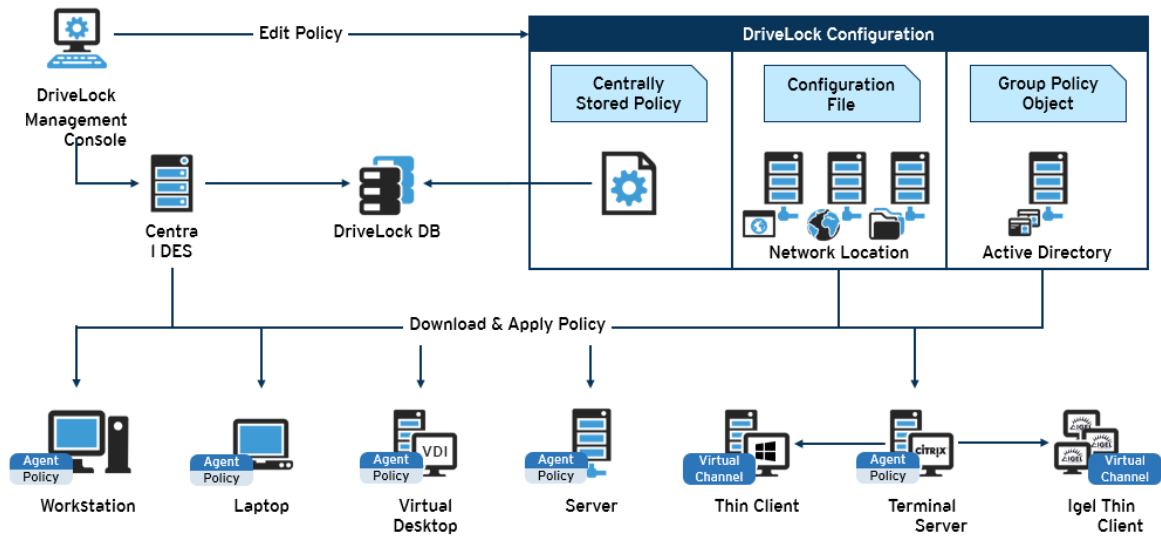
DriveLock policies are managed here:



Architecture

The following figure shows how DriveLock distributes the configuration settings:

DriveLock Policy Processing



3.1 Centrally Stored Policies

Centrally Stored Policies (CSP) are stored in the DriveLock database and are distributed to the agents via the DriveLock Enterprise Server (DES). CSPs are a good choice for most use cases because:

- CSPs support versioning and change tracking and can be edited or published separately by the administrator.
- Several CSPs can be assigned to one agent (which is not the case with configuration files, for example).
- CSPs can be used in almost any network environment, including Active Directory, Workgroups and Novell Directory Service.

For Managed Security Service Provider (MSSP), CSPs may also be the best choice to separate CSPs for different tenants.

To use CSPs, the DriveLock Enterprise Service (DES) is required.

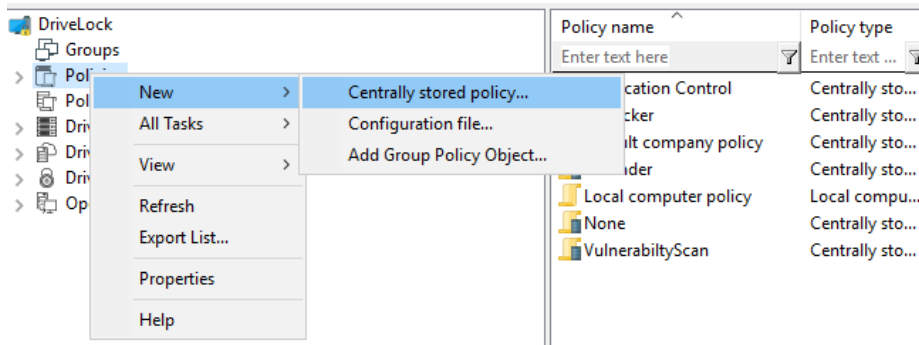
One or more CSPs can be assigned to computers, DriveLock groups, AD groups, OUs or even all computers. The CSPs can belong to the default tenant (root) or any other tenant. The agent knows the DES servers from where it can obtain CSPs. This way, CSPs with different settings can be combined, e.g. one CSP contains only basic settings that are then distributed to all clients and another contains special settings that are only assigned to clients in a specific department. For example, you might want to create a CSP that contains the USB sticks from Marketing, meaning that this CSP will only be used by the Marketing clients.

Example

Order, Policy	Assigned to	Description
1) License policy	All Computers	Contains license information for all computers
2) Default_All	All Computers	Default settings for all computers
3) USB sticks	Marketing clients	Unlocked USB sticks for marketing
4) Disk Protection Laptops	Laptops	Disk Protection
5) Application Control Servers	Servers	Allowed applications for servers

Create and configure CSPs

To create a new CSP for root or other tenants to cover your desired scenarios (e.g. FDE only for laptops) right-click **Policies / Centrally Stored Policies** and select **New / Centrally Stored Policy**.



Enter a name, select a tenant and enter a short description to explain the purpose of the new policy. If appropriate, check **use existing policy as template** and select a policy you want to copy. Click OK to store the new CSP. Then a new window will open, where you can configure the new policy.

To edit an existing CSP, right click on the CSP and select **Edit**.

Remember to enter your license information under Global settings (as described in the chapter "[Activating Your License](#)").

You can use the export and import functions to copy settings between different policy types, for example from a local policy to a CSP.

When you have finished editing the policy, close the policy window. DriveLock prompts you whether you want to save the changes you made.

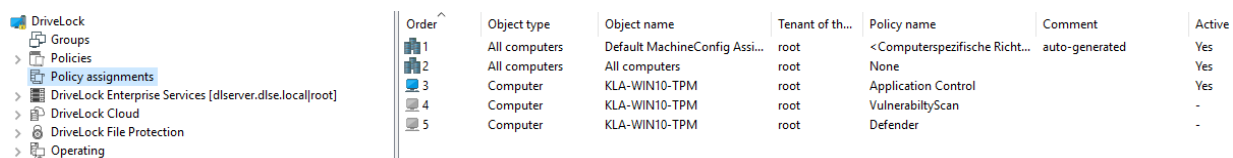
- **Save Only:** The policy is saved but not published. It is not available to DriveLock Agents until it gets published
- **Save and publish:** The policy is saved and then published. Once published, it becomes available to DriveLock Agents.
- **Cancel — Discard changes:** The policy is not saved and all changes are discarded. No new policy version is created or made available to DriveLock Agents.

You can also save a policy at any time during editing by clicking the **Save** or **Publish** buttons on the toolbar.

3.1.1 Policy Assignments

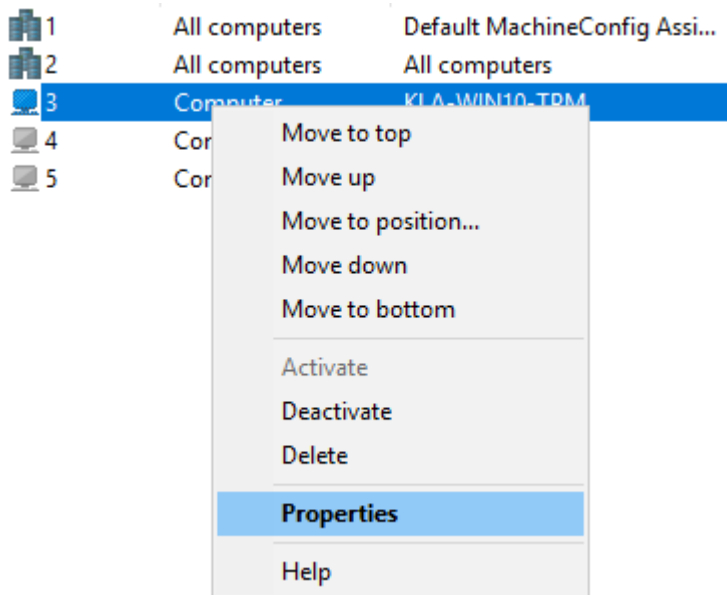
Policy Assignment

Now assign the policies to computers, groups, DriveLock groups, OUs or even All computers, where they should apply. Open **MMC / Policy assignments / RightClick / New / <type of assignment>**. In the next dialog, enter the appropriate computers, groups or OUs, select a tenant (or all tenants) and the policy, you want to assign. Policies stored for the root tenant can be selected for any tenant, while policies stored for any other tenant can only be selected for this tenant.



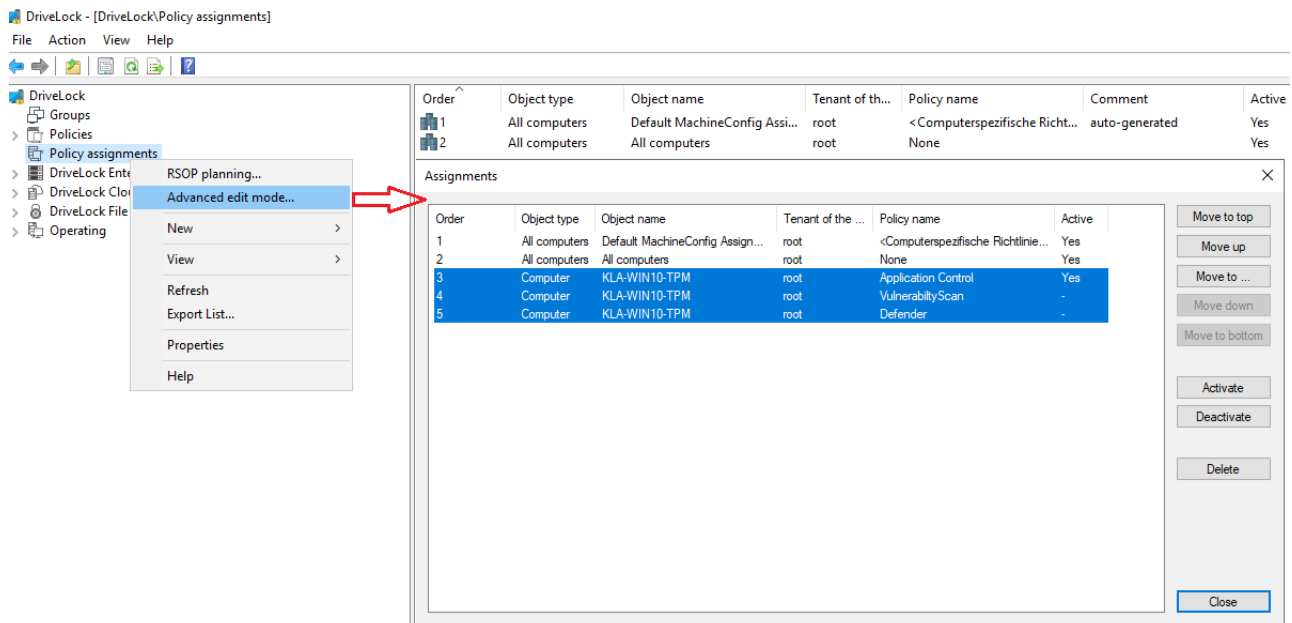
Order	Object type	Object name	Tenant of th...	Policy name	Comment	Active
1	All computers	Default MachineConfig Assi...	root	<Computerspezifische Richt...	auto-generated	Yes
2	All computers	All computers	root	None		Yes
3	Computer	KLA-WIN10-TPM	root	Application Control		Yes
4	Computer	KLA-WIN10-TPM	root	VulnerabilityScan		-
5	Computer	KLA-WIN10-TPM	root	Defender		-

To change the order, right click an entry.



You can move the entry to where you want to place it.

Open **MMC / Policy assignments**, right-click and select **Advanced edit mode ...** to open the **Assignments** dialog if you want to edit or move more than one policy at a time:



In this window you can select several policies and **move them up or down or delete them**.

3.1.2 Configuring the Agent

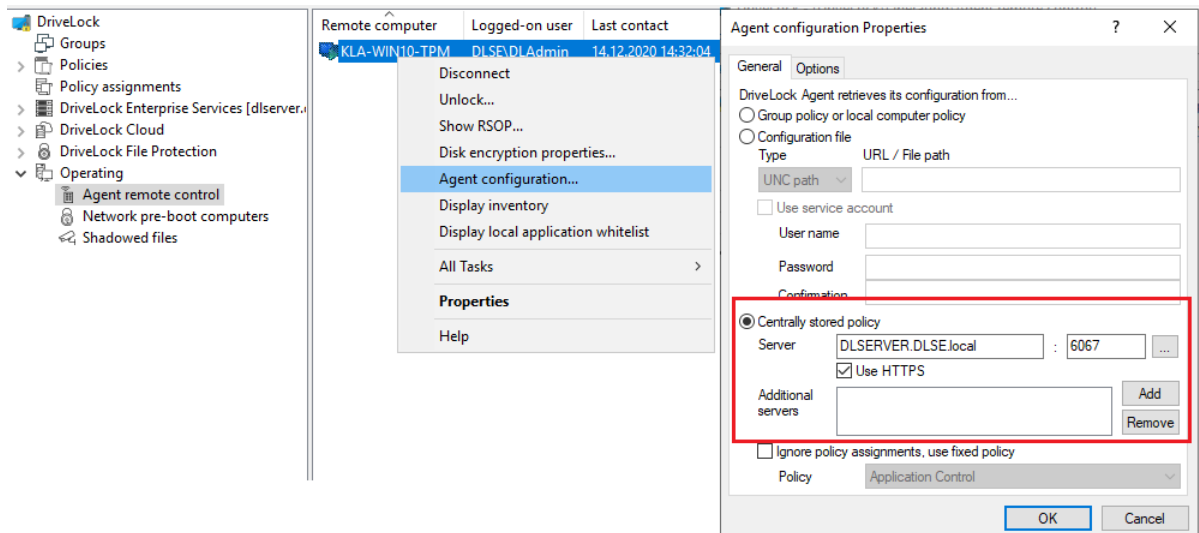
DES Assignment

The last step is to assign a list of DriveLock Enterprise Servers (DES and/or LDES) to the agents. There are several methods to assign CSPs / DES servers to agents depending on how you deploy the agents on the PCs.

- *Software Deployment* - use the deployment wizard to generate an adapted MSI package or MSI command line to install an agent with a server list already assigned. Open **MMC / Policies / RightClick / All Tasks / Deploy**

centrally stored policy... For more information about using the Deployment Wizard, refer to the DriveLock Installation Manual.

- *DriveLock Push Installation* - configure the [Per-Server Global Settings](#) - select Configuration type: **Centrally stored policy (assignment)** and enter the server list
- *Change an existing assignment* - [Using Agent Remote Control](#). Connect to the agent and select **Agent configuration / Centrally stored policy** and enter the server list



- Using the command line on an agent PC. Enter `C:> Drivelock -setserver <srvlst>#<tnt>` (see `Drivelock -help` for more information)

- *DNS-SD* - if the DriveLock agent detects a DES via DNS-SD, no DES assignment is necessary. The agent will ask this DES for policy assignments

When a DriveLock Agent uses a CSP, it checks for changes to the policy settings at startup and at a configurable interval after that (default: 30 minutes).

3.2 Group Policy

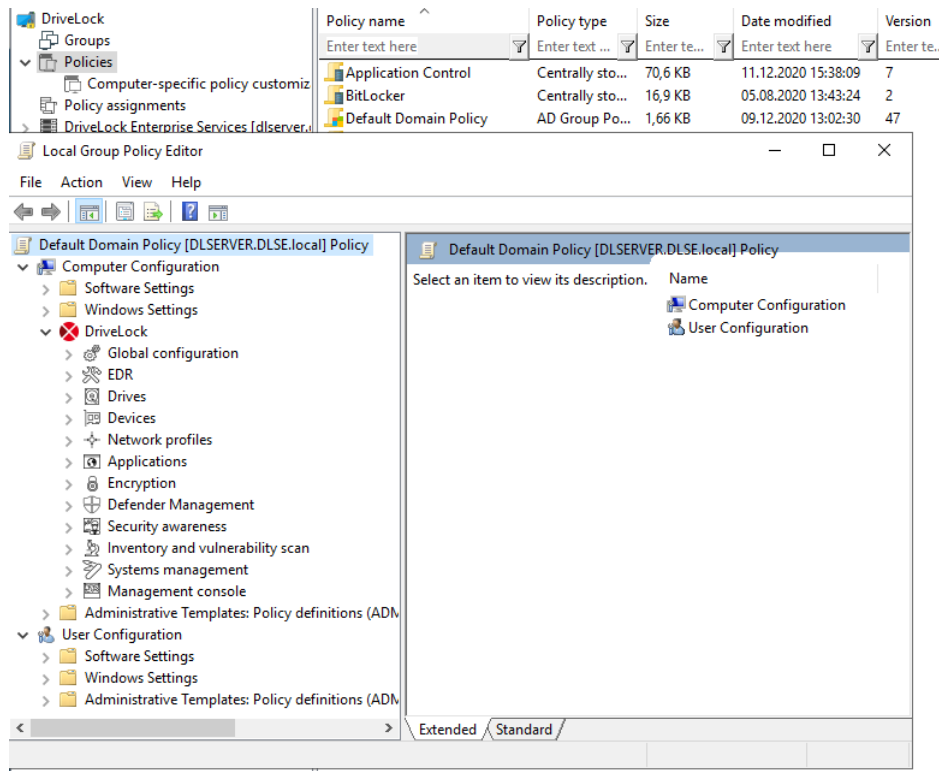
Another way of configuring the DriveLock Agent on multiple computers in a network is by using an Active Directory Group Policy. DriveLock can be configured by using the Group Policy Object Editor in conjunction with the DriveLock Management Console (MMC) snap-in. This snap-in is automatically installed as part of the DriveLock installation.

DriveLock can use Group Policy to deploy settings to computers that belong to an Active Directory domain. The DriveLock Agent running on these computers automatically applies all settings that are contained in the Group Policy Object.

In Active Directory computers are often arranged in Organizational Units (OUs) to apply common settings to multiple computers. For example, an OU may contain all computers in a department or business unit. A DriveLock policy can be easily applied to all these computers by linking a Group Policy Objects containing DriveLock settings to the OU. Another reason to use OUs is delegation of administration tasks. Assigning GPOs to an OU instead of an entire domain or Active Directory site is a recommended practice because it allows you to maintain the appropriate protection level for each department or business unit.

To add existing or new Group Policies containing DriveLock settings, right-click Policies -> New -> Add Group Policy Object... to add the Group Policy to the MMC.

Then select the appropriate GPO and click Edit. This opens a new window with the Microsoft GPO Editor where you can edit the settings.



The Group Policy Object Editor displays the same DriveLock configuration items in the console tree that are available when you use a local configuration.

The DriveLock Agent service applies configuration changes immediately after Windows receives updated Group Policy settings from a domain controller. Depending on the time until the next scheduled Group Policy update, it may take several minutes after you change the configuration until this update takes place. To apply changes to a GPO immediately, manually initiate a Group Policy update. To do this, on the client computer open a command prompt window and then type the following command:

```
gpupdate /force
```

You can find more information about how to use Group Policy to deploy a DriveLock configuration in the technical article *“DriveLock Interaction with Active Directory”*, which is available at DriveLock Online Help (<https://drivelock.help>). This article also contains replication traffic information and deployment tips.

3.3 Configuration Files

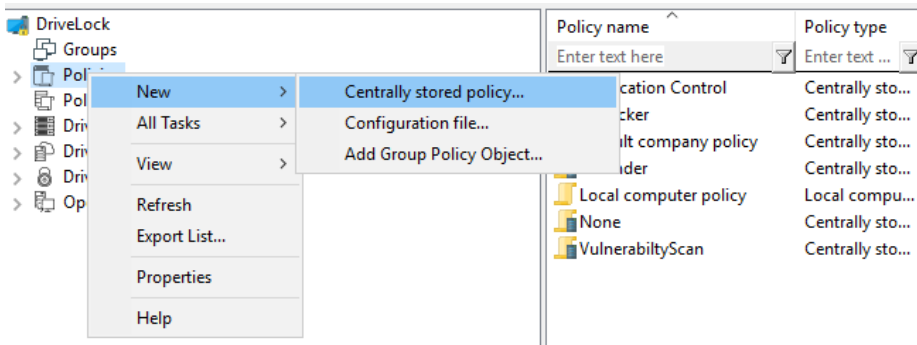
You can centrally install and configure DriveLock even in networks without Active Directory, such as networks using Novell NetWare. In network environments without Group Policy or a DriveLock Enterprise Service you can distribute central DriveLock configuration settings by using a configuration file. This file can be placed on a central network drive (using a UNC path) or it can be accessed by using HTTP or FTP.

Using configuration files is similar to using Group Policy. However, user-specific configuration options are limited when Active Directory is not available as the central user database. You can still use local users or groups in your configuration settings. Also, you can use Novell eDirectory, if available.

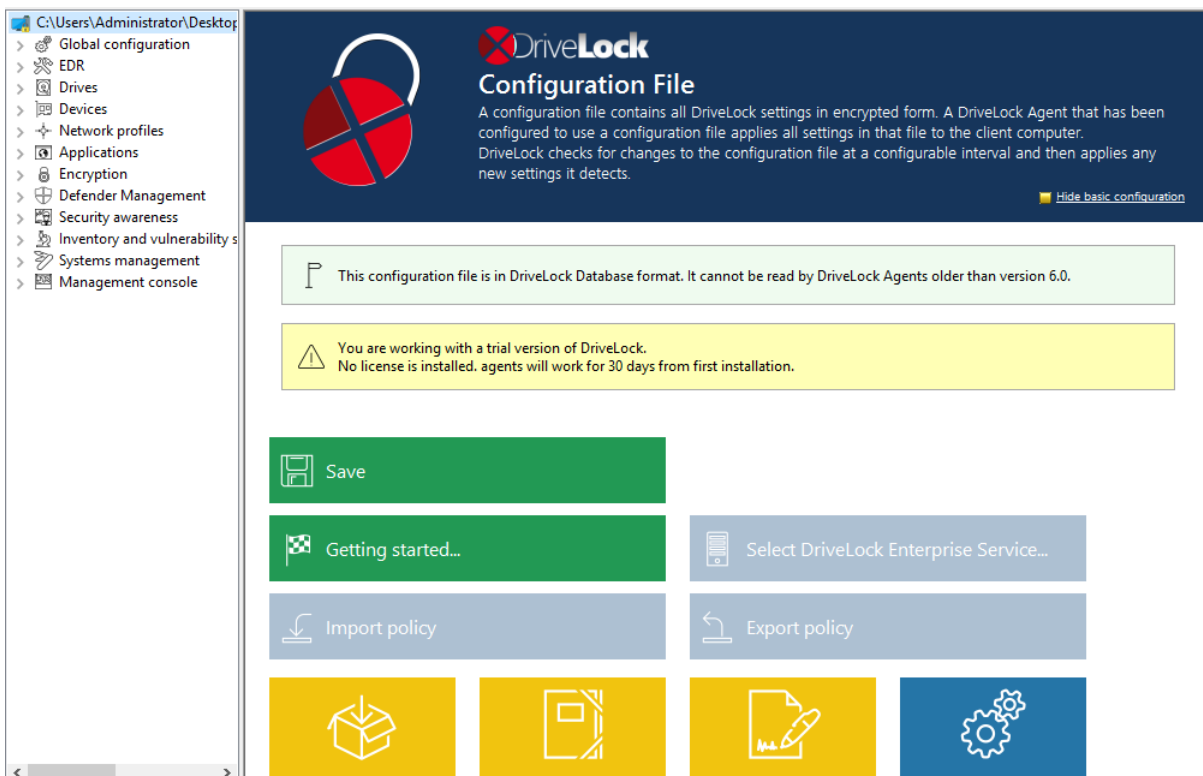
You can find additional information about using DriveLock in a Novell network in the whitepaper *“DriveLock – Interaction with Novell”*, which you can get from DriveLock by request.

Start the DriveLock Management Console (**Start -> Programs -> DriveLock -> DriveLock Management Console**) and then click **Policies**.

Right-click "**Policies -> Configuration files**" and then click **Create new Configuration file**.



DriveLock prompts you to provide the name and location of the new configuration file and then opens a new window, displaying the policy. You can configure policy settings in this window. You can also export or import settings.



Remember to enter your license information under Global settings (as described in the chapter "[Activating Your License](#)").

You can transfer settings between a configuration file and other policy types by using the **Import configuration** and **Export configuration** commands.

To edit an existing configuration file to the DriveLock Management Console, in the console tree, right-click Policies and then click **Open Configuration file**. In the dialog box, type the file name and location and then click **Open**. The configuration file will appear in the right pane.

Right-the file, and then click **Edit** to open a new DriveLock Management Console window where you can edit the settings in the configuration file.

The DriveLock Management Console automatically saves changes you make to a configuration file when you close the window.

When you have finished editing your configuration, close the window. To save the file using a different name, right-click the top node in the console tree, and then click **Save as**.

Once the changes are complete, apply the configuration to client computers by copying the configuration file to the network location from which clients retrieve their policy settings, replacing the old configuration file with the new one.

You must configure the DriveLock Agent that you distribute to client computers to obtain its configuration settings from the configuration file. To facilitate this process, DriveLock contains a software distribution assistant that can create a customized MSI or MST file. You can use the DriveLock Deployment Wizard, which is described in the document “**DriveLock Installation Guide**”, to deploy configuration settings.

The DriveLock Agent can retrieve configuration files using any of the following methods:

- **UNC:** For example “\\myserver\share\$\drivelock\dlconfig.cfg”
- **FTP:** For example “myserver/pub/drivelock/dlconfig.cfg”
- **HTTP:** For example “http://myserver/drivelock/dlconfig.cfg”

In environments without Active Directory (such as Novell NetWare) you must specify the location of the configuration file during the Agent installation (as described in the *DriveLock Installation Guide*).

You should create an initial configuration file prior to the Agent roll-out and then specify the location of the configuration file during setup by using the command line or a modified installation file.

The DriveLock Agent reads the configuration file during installation and then starts enforcing the policies in this file.

When you use configuration files, the Agent only checks for changes to the configuration file when the DriveLock Agent service starts or at an interval that you can configure.

When you are installing the DriveLock Agent that will use a configuration file, you need to provide the Agent with the location of this file. The easiest way to accomplish this is by using the Deployment wizard. To start the wizard, right-click *Policies -> All Tasks -> Deploy configuration file*. For more information about the deployment process, refer to the DriveLock Installation Manual.

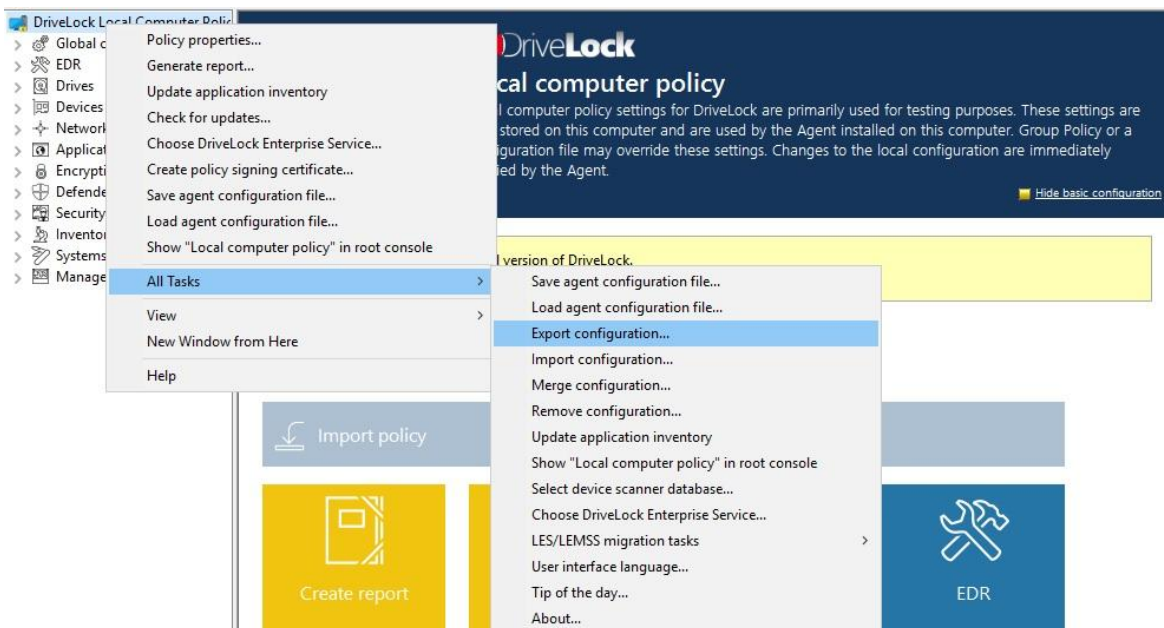
3.4 Local Computer Policy

To configure a standalone computer with the DriveLock Agent installed, use a local policy. This configuration is only applied to the computer on which you are running the DriveLock Management Console.

To edit the local policy, open **Start -> All Programs -> DriveLock -> DriveLock Local Policy**.



A local policy can be used to test a company-wide policy on a single computer before deploying it to the rest of the network. Once you are satisfied with your configuration, you can export the settings to a file and then import them into another policy using the following procedure.



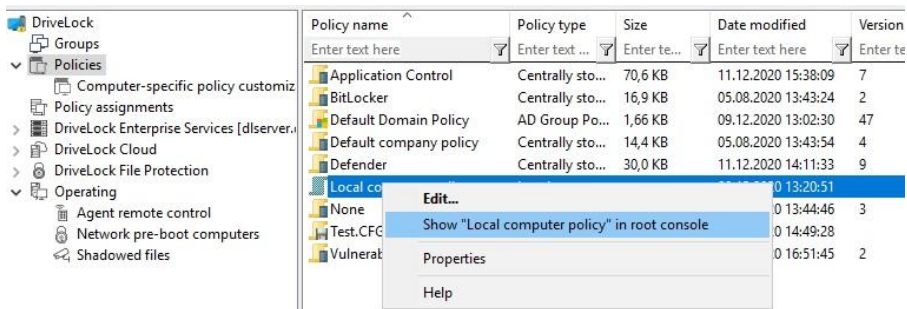
To export a configuration, right-click **DriveLock** in the Management Console, then select **All Tasks** from the context menu and then **Export configuration....** The configuration file has a **.dlr** extension.

To import the configuration settings into a policy, right-click **DriveLock** and then click **All Tasks -> Import configuration**. You can also export a policy from a GPO and import it into a local DriveLock policy. In addition, you can use the export procedure to back up your current configuration settings.

Selecting the option “*Save agent configuration file*” generates an Agent configuration file (**.cfg**). You can use the file to deploy a DriveLock configuration when you don’t want to use Group Policy or when you deploy DriveLock in a network without Active Directory.

To clear all configuration settings from an existing DriveLock policy, either local or GPO-based, right-click **DriveLock** and then select **All Tasks -> Remove configuration**.

You can display the settings in a local policy as a node in the console tree of the DriveLock Management Console.



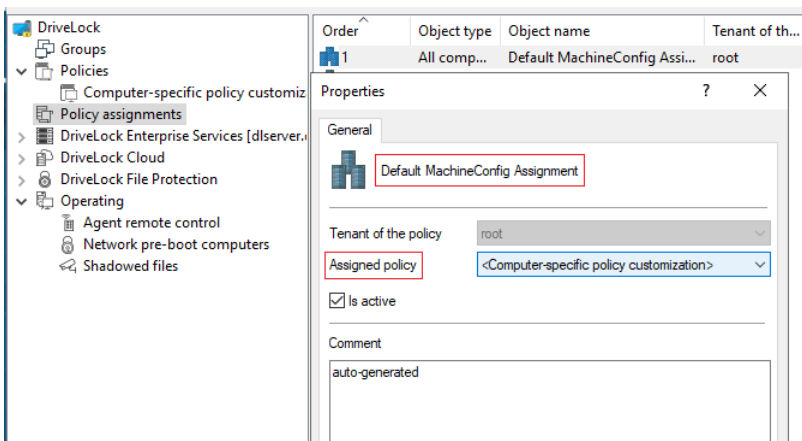
To display a local policy in the DriveLock Management Console, right-click the local policy, and then click **Show "Local policy" in root console**. The next time you start the Management Console, the new entry appears in the console tree:

To restore the initial settings, right-click **Local policy**, point to **All Tasks** and then click **Show "Local policy" in root console** to deselect this setting.

3.5 Computer-specific policy customizations

A Computer Specific Policy Adaptation (CPA) is technically a centrally stored policy that only contains settings for a single computer. However, unlike normal centrally stored policies, they are not assigned individually, but through a single **policy assignment**, the computer specific policy customization.

A CPA basically is a normal DriveLock policy, but with settings only applied to a single computer. CPAs are introduced with DriveLock 7.9 and used for a computer specific BitLocker password configuration. Such a CPA is generated automatically and usually there is no need to edit or change it. CPAs are listed separately, so they don't interfere with your normal policies. CPAs might become more important in future releases.

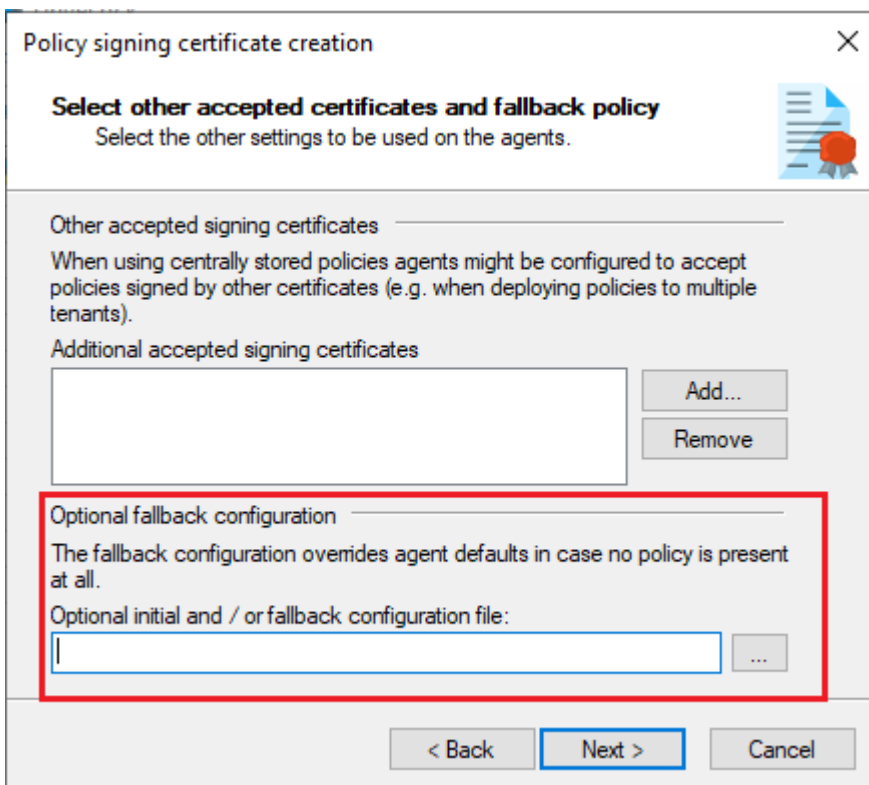


- By default, this type of assignment is called **Default MachineConfig Assignment**. It provides the CPA for each computer.
- CPAs are used, for example, for computer-specific BitLocker password settings. A CPA is generated automatically when required.
- CPAs are managed or displayed separately from the other policies in a separate node.
- CPAs work even if DriveLock Agent is not configured to use centrally stored policies. In this case, the agent requires a configured server connection.

3.6 Resultant Set of Policies (RSOP)

The agent merges all policies assigned to it into a final policy (Resulting Set of Policies, RSOP) in the specified order. Depending on the agent configuration, one of the following combinations is used for this (order of evaluation:)

1. Fixed policy (setting under Agent configuration, General tab, option **Ignore policy assignments, use fixed policy**) + computer specific policy assignment (CPA)
2. Policy assignments
3. Configuration file + computer specific policy assignment (CPA)
4. Local configuration + group policy object + computer specific policy assignment (CPA)
5. Fallback configuration file (special configuration file on an agent), setting during policy signing certificate creation, see figure:



Policy signing certificate creation

Select other accepted certificates and fallback policy
Select the other settings to be used on the agents.

Other accepted signing certificates

When using centrally stored policies agents might be configured to accept policies signed by other certificates (e.g. when deploying policies to multiple tenants).

Additional accepted signing certificates

Add...

Remove

Optional fallback configuration

The fallback configuration overrides agent defaults in case no policy is present at all.

Optional initial and / or fallback configuration file:

...

< Back Next > Cancel



Part IV

Configuring the DriveLock Enterprise Service



4 Configuring the DriveLock Enterprise Service

The DriveLock Enterprise Service (DES) is the central component of a DriveLock installation. It processes event messages from clients, stores the event data in a database and creates connections between the events. It also acts as an interface for all database queries by DriveLock Agents and the DriveLock Management Console and it stores important Agent data, such as data that is required to recover encrypted data.

When DriveLock is managed by a service provider offering “security as a service”, the DriveLock Enterprise Service acts as a conduit between the service provider and the customer, providing various proxy functions.

4.1 Creating Server Connections in the DriveLock Management Console

The DriveLock Management Console needs to connect to the DriveLock Enterprise Service for various tasks, such as retrieving licensing information and centrally stored policy settings. To enable this functionality you need to initially create a server connection in the DriveLock Management Console.

To configure DES settings, right-click the top node in the DriveLock Management Console (*DriveLock*) and then click **Choose DriveLock Enterprise Service**.



If the DriveLock Management Console detected a DES server during startup using DNS-SD, the detected server appears in the dialog box. If no server is displayed, type the name or address of the server. If you changed the ports on the DES server from their defaults you also need to type the port numbers.

To authenticate to DES using a different account than the one you are logged on with, you can provide the name and password of the account that will be used for the authentication.

The account that is used to authenticate to the DES server needs to have been assigned permissions the required to administer DES. You can assign these permissions users and groups during the installation of the DriveLock Enterprise Service or by configuring the DES settings after the installation. These tasks are described in the DriveLock Installation Manual and the section “Assigning Permissions” in this manual.

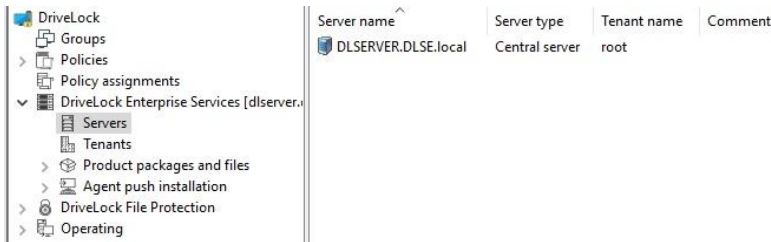
Click **OK** to save the server connection.

4.2 Administering DES Servers

To configure DES settings use the *DriveLock Enterprise Services* node in the DriveLock Management Console.

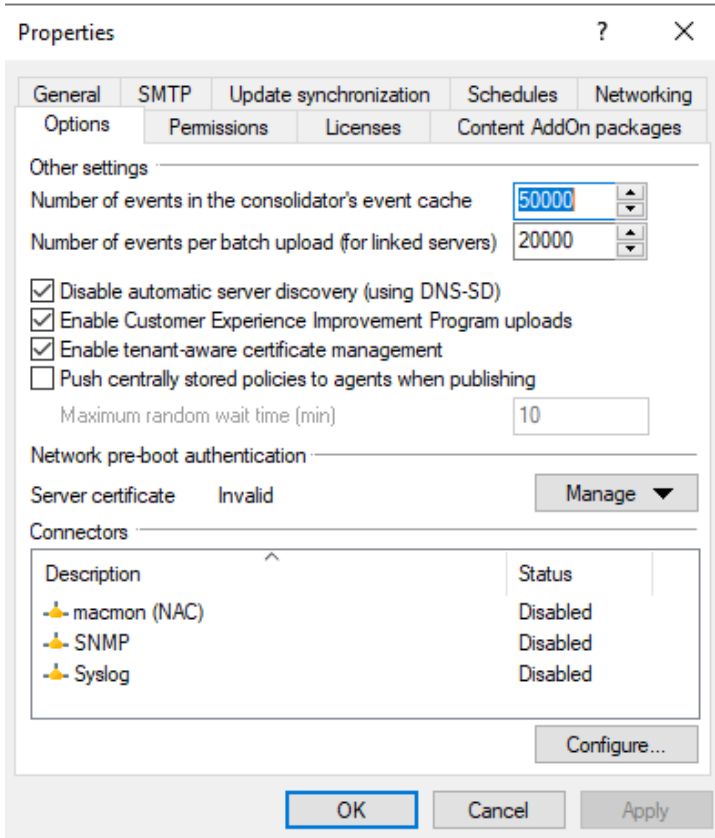


Click **Servers** to display a list of all DES servers that have been registered in the DriveLock database manually or by using DNS-SD.



DES servers are automatically added the first time the DES service starts and connects to the database. The column *Server type* displays each DES server’s operating mode (Central server or Linked server). You can configure settings separately for each server in the list after selecting it from the list. Most settings are configured only on the central server and are not available for linked servers.

Double-click the name of a server to view or change its settings. You can disable automatic server discovery using DNS-SD on the Options page.



To disable automatic discovery, select the checkbox **Disable automatic server discovery (DNS-SD)**. Once automatic discovery has been deactivated, the server will no longer announce itself on the network and all clients must be configured with the correct DES server connection.

Connectors

You may configure connections to various third-party software. E.g. if you configure the SNMP connector, the DES sends all events to an external monitoring system via SNMP V1. Ask your DriveLock consultant for more information.

4.3 DES Operating Modes

The DriveLock Enterprise service can run in one of two modes:

- *Central DriveLock Enterprise Service*
- *Linked DriveLock Enterprise Service:*

Most DriveLock environments use only the central DriveLock Enterprise Service. Linked DES servers are typically only used in very large, distributed environments or hosted services environments.

4.3.1 Central Server

The first DES server that belongs to the same infrastructure is always a central server with a connection to a database. Additional DES servers are always installed as linked servers. They don't access the database directly but rather interact with it via the Central server.

One of the main functions of a Central DES server is to process event data and store it in a database. Because processing of events can take some time, events are first stored in a local cache and processed in the background before they are written to the database. This ensures quick responses to clients even when a large number of events are received from clients or in environments with a very large number of clients (20,000 or more).

By default the cache holds up to 20,000 events. If the cache is full, new event messages from Agents are rejected. When an Agent is notified that an event message has been rejected, it will try to send it again at a later time. The DES processes events in the cache in the background and will receive new event messages once there is available space in the cache. You can change the cache size on the Options tab of each server.

When the DriveLock Enterprise Service is stopped, any event data remaining in the cache is by default saved to the file `%PROGRAMDATA%\CenterTools DriveLock\SavedCache.db3`. This event data is processed when the service is started again.

4.3.2 Linked Server

The Linked Server mode is designed for branch offices that are connected to a central location over a slow WAN link. A linked server can compress event data and send it to the central Server at configurable times. This reduces the amount of bandwidth used for event reporting and ensures that no bandwidth is consumed during peak usage times. Linked servers are also used in hosted “Security as a Service” installations.

A linked server can perform the following functions:

- Process all events and upload them to central server according to schedule
- Process Agent Alive status messages and upload them to the central server according to schedule
- Accept recovery data (Encryption 2-Go and FDE) and forward it to the central DriveLock Enterprise Service immediately
- Accept inventory data from DriveLock Agents and forward it to the central DriveLock Enterprise Service immediately
- Retrieve installation packages stored on the central DriveLock Enterprise Service and make them available to Agents
- Retrieve Centrally Stored Policies from the central DriveLock Enterprise Service and make them available to Agents
- Edit Centrally Stored Policies with the DriveLock Management Console (tenant specific)
- Upload Active Directory user and group data to the central DriveLock Enterprise Service. For more information about this process, refer to the section “Performing Active Directory Object Inventory Collection”.
- Accept Agent remote control requests from the central DriveLock Enterprise Service and route them to the correct Agent (Agent Remote Proxy).

The DriveLock Control Center cannot use a linked DriveLock Enterprise Service to access any DES data. Instead, it must connect to the central DriveLock Enterprise Service. Also, a linked server cannot process inventory data from DriveLock Agents older than version 7.0.

On the General tab, specify the interval at which the linked server uploads event data to the central server. The default is every hour.

On the Options tab you can configure the number of events per batch upload to the central server. This is the maximum number of events that are cached on the linked server before it starts uploading the events to the central server. If this number is too low, it may take a long time until events are uploaded and will be included in reports. For a small branch office where only few events are generated, this number may need to be reduced from the default of 20,000 to 10,000 or even less.

Once the cache holds the number of events you have configured, the event data is compressed and saved as a file in the folder `%PROGRAMDATA%\CenterTools DriveLock\Storage`.

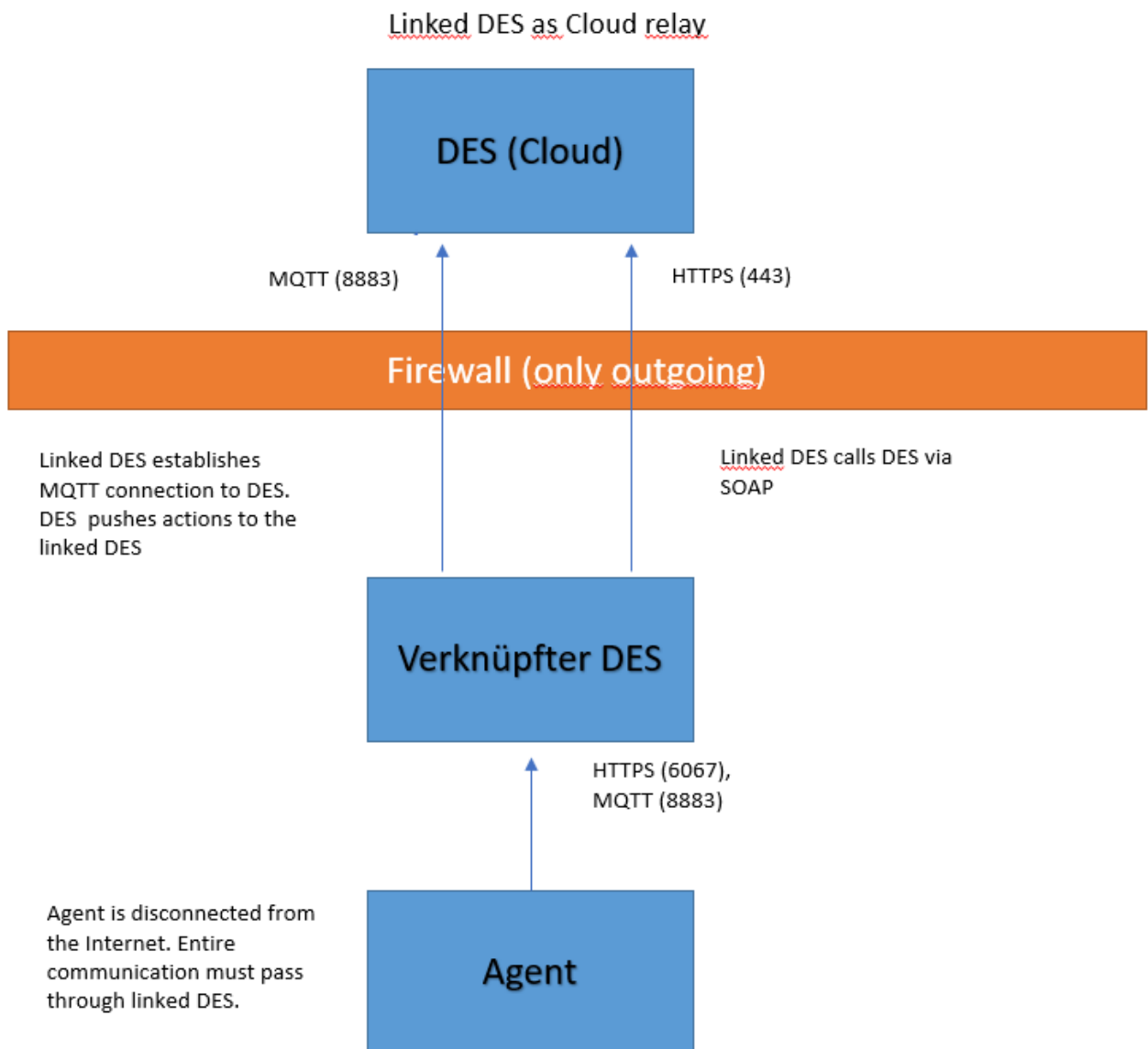
The central DES server stores event data it receives from other DES servers in the folder `%PROGRAMDATA%\CenterTools DriveLock\ReceivedStorage`. It then decompresses the data in the background and adds it to the database.

4.3.2.1 Linked DES to Connect to the DriveLock Cloud

The linked DES in cloud mode acts as an intermediary to connect agents to the DriveLock Cloud without an Internet connection. It accomplishes three tasks in the process:

- Route requests from the agents to the cloud
- Cache data from the central DES
- Provide an MQTT broker
 - > Allows agents to be controlled via agent remote control.
 - > Allows the central DES in the cloud to reach the linked DES.

Network diagram:

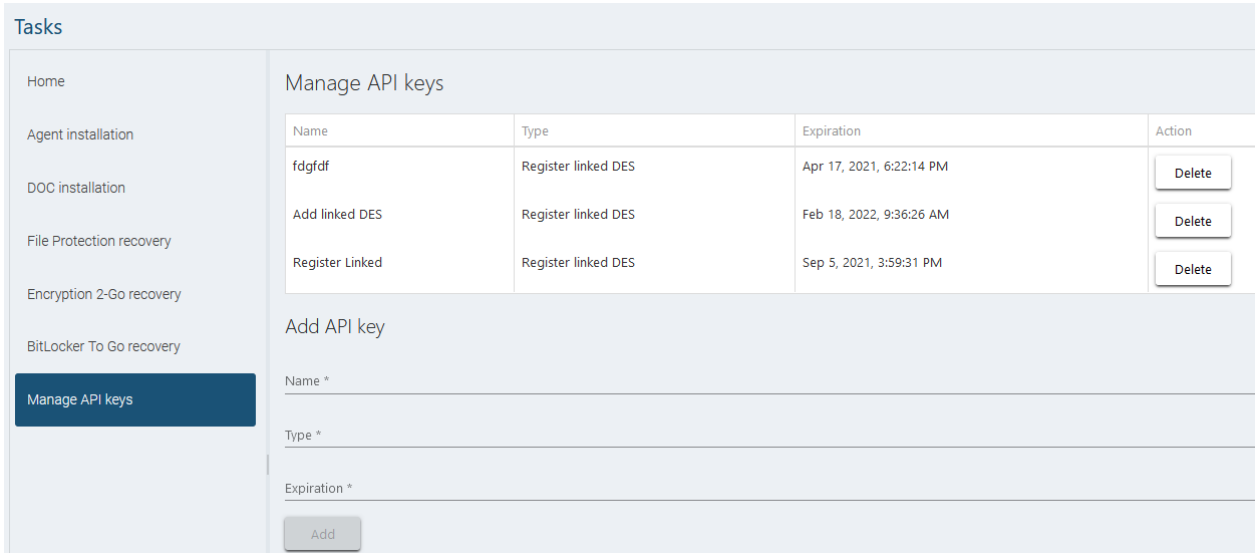


4.3.2.1.1 Registering a Linked DES as a Cloud Relay

To register a linked DES, follow these steps.

1. Create an API key that allows the linked DES to be registered in the cloud client

- In the DOC, open the **Tasks** view and then **Manage API Keys**, see figure:



The screenshot shows the 'Tasks' view with 'Manage API keys' selected. The main area displays a table of API keys and an 'Add API key' form.

Name	Type	Expiration	Action
fdgdfd	Register linked DES	Apr 17, 2021, 6:22:14 PM	Delete
Add linked DES	Register linked DES	Feb 18, 2022, 9:36:26 AM	Delete
Register Linked	Register linked DES	Sep 5, 2021, 3:59:31 PM	Delete

Below the table is the 'Add API key' form with the following fields:

- Name *
- Type *
- Expiration *
- Add button

- Create a new key of the type **Register linked DES**.
- This will produce a long string (API key) that will be used for authorization. Now the key must be transferred to the linked DES in a secure way. Which method you choose is up to you.

Note that the key has an expiration date. This only means that when the expiration date is reached, you can no longer use the key to register a linked DES with the cloud; it does not mean that the linked DES will no longer work. After use, keys can therefore also be deleted safely.

2. Register the linked DES in the cloud in the Database Installation Wizard

- Open the Database Installation Wizard and select the **Linked DriveLock Enterprise Service connected to the DriveLock Cloud** option.

Select DES role

Select the role for the DriveLock Enterprise Service on this computer.

- Central DriveLock Enterprise Service (default)
Select this mode if this is the only DriveLock Enterprise Service in your organization or if it is the central service in a distributed installation. A database server connection is required for this mode.
- Linked DriveLock Enterprise Service
Select this mode if the DriveLock Enterprise Service on this computer reports to the central DriveLock Enterprise Service. No database will be installed.
- Linked DriveLock Enterprise Service connected to the DriveLock Cloud
Select this mode if the DriveLock Enterprise Service on this computer is part of the managed DriveLock Cloud environment. No database will be installed.

- In the next dialog copy the API key into the text field.

Linked DriveLock Enterprise Service cloud registration
Register your server using an API key

Insert a registration API key.
You may obtain an API key using the DriveLock Operations Center. Navigate to "Tasks" and select "Manage API keys".

```
eyJ0b3N0IjojZGV2LmRyaXZibG9jay5jbG91ZCI6InRva2VudjoiWVdWekxUSTFOaTFqWW1NNmFMXVUMIZPVTBSWWJsWjZVMVJZVTNoaWQweFdkkejAST21NNWEzbGFUa1pWwkvJm01WdcE5ZMHAzV0dkdFNRZGJlRUZlWlZkUVRUWjVWUzgzYW1GeVNsTnRMMDfyTUhCaGlyMvPva0ptU2swMFJ6Rm1lRmh0VE4ek4xRk1TangxVFZvMGRWZGhZVWVY0VSbFRsVndXRk5EWTB4cWJhbFRPRWxpU1doUFZY3ZPVEJWUFE9PSJ9
```

Register server

< Back

Next >

Cancel

- Click **Register server**.

4.3.3 Changing the Operating Mode

The operating mode of a DES server is set after the DES installation by the Database Installation Wizard. To change the operating mode at a later point, you need to run the wizard again.

Select DES role

Select the role for the DriveLock Enterprise Service on this computer.

Central DriveLock Enterprise Service (default)

Select this mode if this is the only DriveLock Enterprise Service in your organization or if it is the central service in a distributed installation. A database server connection is required for this mode.

Linked DriveLock Enterprise Service

Select this mode if the DriveLock Enterprise Service on this computer reports to the central DriveLock Enterprise Service. No database will be installed.

Linked DriveLock Enterprise Service connected to the DriveLock Cloud

Select this mode if the DriveLock Enterprise Service on this computer is part of the managed DriveLock Cloud environment. No database will be installed.

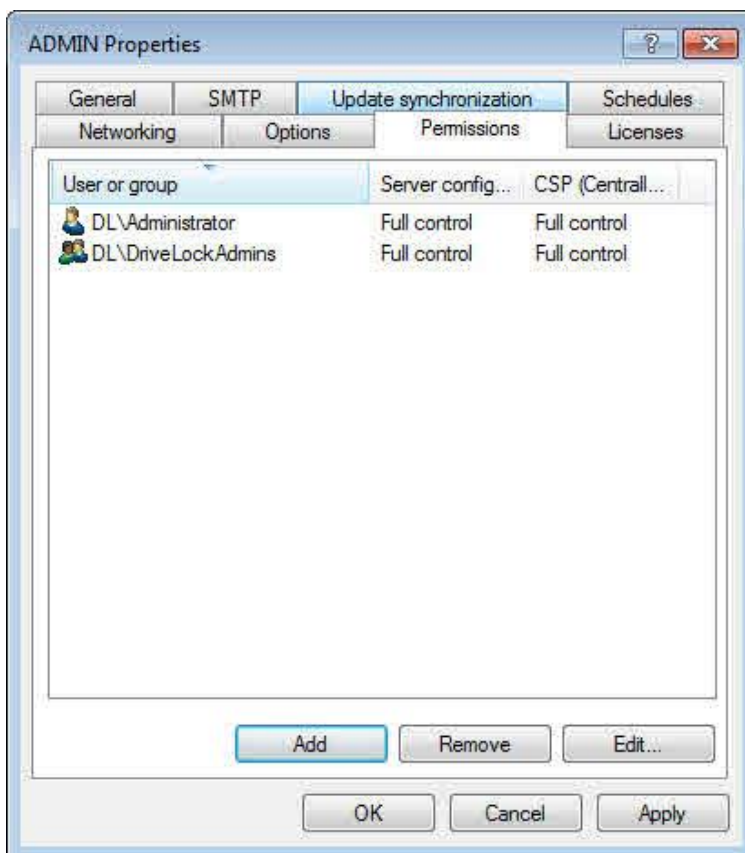
Select the option **Linked DriveLock Enterprise Service**. For more information about installing the DriveLock Enterprise Service, refer to the DriveLock Installation Manual.

4.4 Assigning Permissions

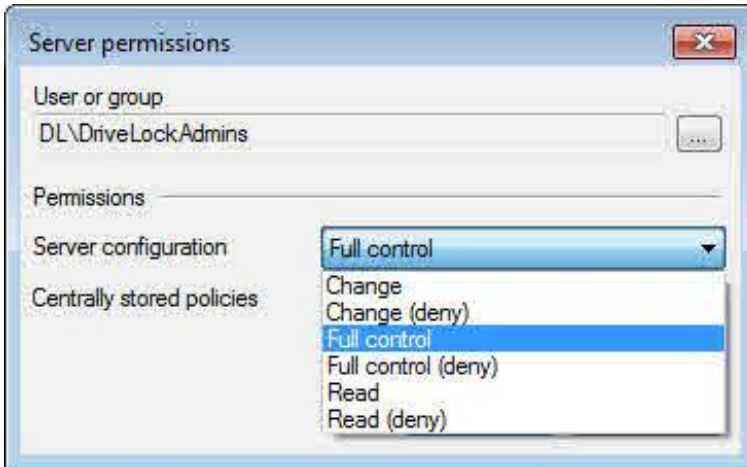
To ensure that only authorized persons can change DriveLock Enterprise Service settings or create Centrally Stored Policies, access control is enforced whenever the DriveLock Enterprise Service is accessed. Only authorized users can make any changes. Permissions are assigned separately for each server. In a typical configuration with only a central DriveLock Enterprise Service, permissions only need to be configured for that server.

The user who initially configures the DriveLock Enterprise Service needs to have the permissions to perform this task. The installation wizard prompts for a user or group that will be initially assigned the required when you install or upgrade the DriveLock Enterprise Service. For more information, refer to the *DriveLock Installation Manual*.

You can view or change access permissions in the DriveLock Management Console under *DriveLock Enterprise Services* -> *Servers* -> <server name> on the *Permissions* tab.



You can add new users and assign Allow or Deny permissions for configuring the server and centrally Stored Policies. Available permissions are Read, Change and Full Control.



Ensure that at least one user or group is assigned Full Control permissions in both categories. If you accidentally remove all permissions, contact DriveLock technical support.

4.5 Configuring Maintenance Operations

Database maintenance is important to reduce the growth of the database size and to optimize database indexes to provide optimal performance even when large amounts of data are being processed. You configure how these functions are performed in the *Properties* dialog box of the central DES server on the *Schedules* tab.

You should configure database maintenance settings for the DriveLock Enterprise Service only if you are using an Express version of Microsoft SQL Server. If you are using any other version of Microsoft SQL Server, DriveLock recommends that you configure database maintenance task manually by using stored procedures on the server. For information about the steps required to configure maintenance tasks to be performed by the database server, contact DriveLock technical support or refer to the technical article available on the DriveLock Web site www.drivelock.com.

Server name	Server type	Tenant name	Comment
DLSERVER.DLSE.local	Central server	root	

Properties ? X

Options Permissions Licenses Content AddOn packages

General SMTP Update synchronization Schedules Networking

SecaaS (Security as a Service)

Enable Active Directory object inventory

Database maintenance

Enable automatic database maintenance

Perform maintenance every days

Enable event grooming

Delete events older than days

Enable database backup (Microsoft SQL Server only)

Number of backups to keep

Shrink database after backup

Backup path

Statistics update

Update statistics data for reporting every days

To limit the growth of the DriveLock database, the DriveLock Enterprise Service server can automatically delete old event data. You should configure database cleanup to delete event data that is no longer needed to create reports or forensic analysis or after you have archived your data using third-party tools.

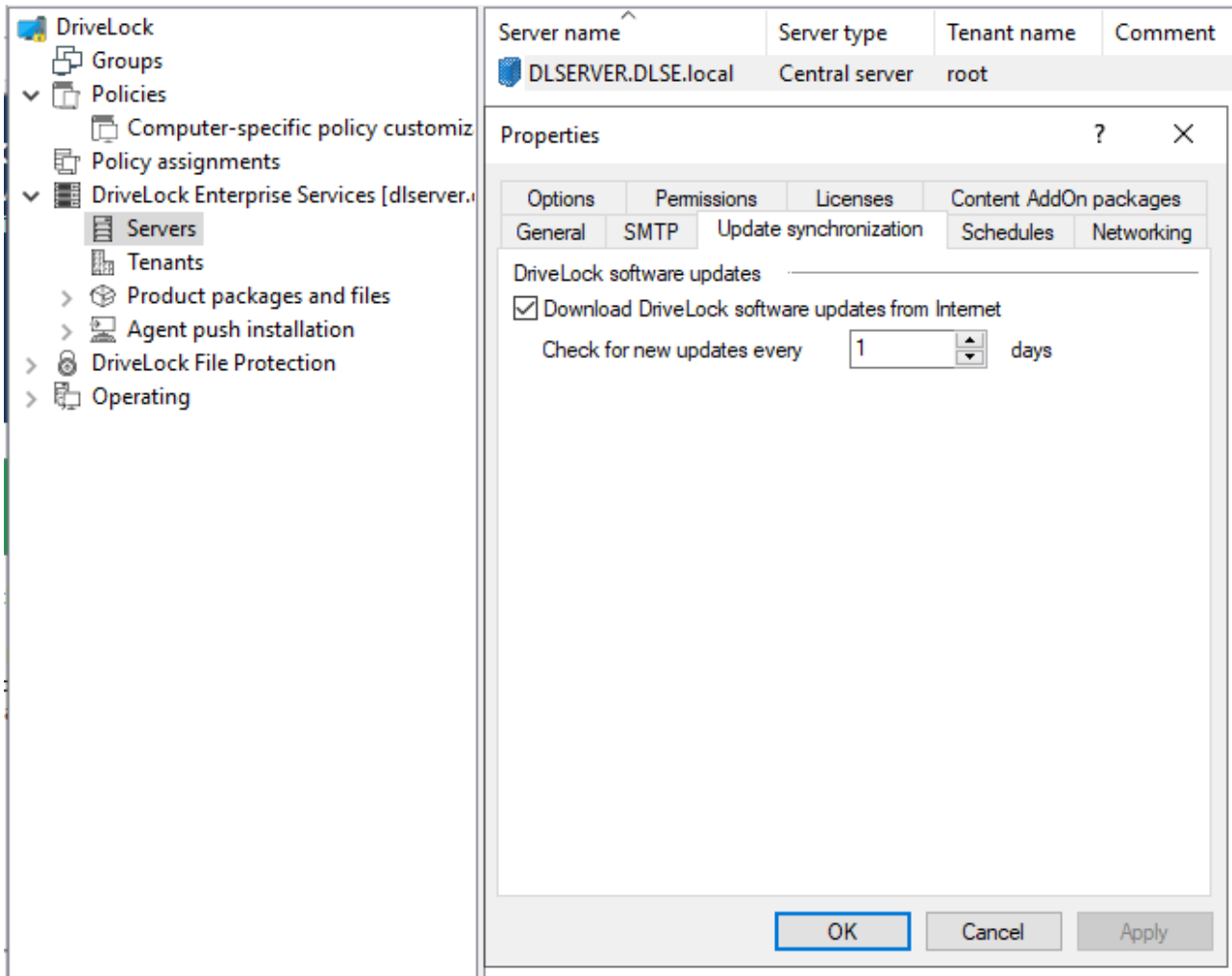
To enable database cleanup and automatically delete old event data, select the *Enable automatic database maintenance* checkbox. If maintenance tasks are performed by your database server, deselect this checkbox.

If you are configuring the DriveLock Enterprise Service to perform maintenance, specify how often this task will be performed and the length of time for which to retain data. By default, the DES deletes events that are older than 30 days every day at 5:00 A.M. To improve the performance when creating reports, database indexes need to be updated on a regular basis. By default, this operation is performed at 3:00 AM every day.

Modify the settings for database maintenance to change the frequency of maintenance tasks and the age after which events are deleted from the database.

4.6 Configuring Update Synchronization

You can configure the DriveLock Enterprise Service to periodically download newly available DriveLock software updates from the Internet. You can specify how often the DriveLock Enterprise Service will look for new updates.



Server name	Server type	Tenant name	Comment
DLSERVER.DLSE.local	Central server	root	

Properties

Options | Permissions | Licenses | Content AddOn packages

General | SMTP | Update synchronization | Schedules | Networking

DriveLock software updates

Download DriveLock software updates from Internet

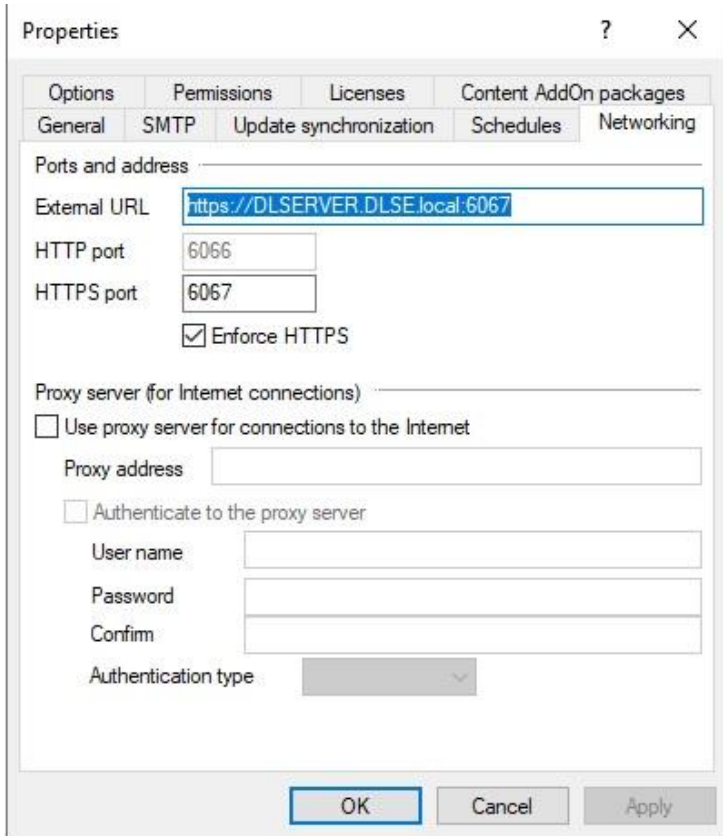
Check for new updates every days

OK Cancel Apply

4.7 Configuring Network Settings

Network settings are configured independently for the Central DriveLock Enterprise Service and any Linked DriveLock Enterprise Service. By default, communications between DriveLock Agents and the DES are encrypted. For this reason, the **Enforce HTTPS** option is set by default.

By default, a DES server listens on TCP port 6066 for unencrypted connections and port 6067 for SSL-encrypted connections. If required in your network, you can change these ports on the *Networking* tab.



The screenshot shows the 'Properties' dialog box with the 'Networking' tab selected. The 'Ports and address' section contains the following fields and options:

- External URL: `https://DLSERVER.DLSE.local:6067`
- HTTP port: `6066`
- HTTPS port: `6067`
- Enforce HTTPS

The 'Proxy server (for Internet connections)' section contains the following options and fields:

- Use proxy server for connections to the Internet
- Proxy address: [Empty text box]
- Authenticate to the proxy server
- User name: [Empty text box]
- Password: [Empty text box]
- Confirm: [Empty text box]
- Authentication type: [Dropdown menu]

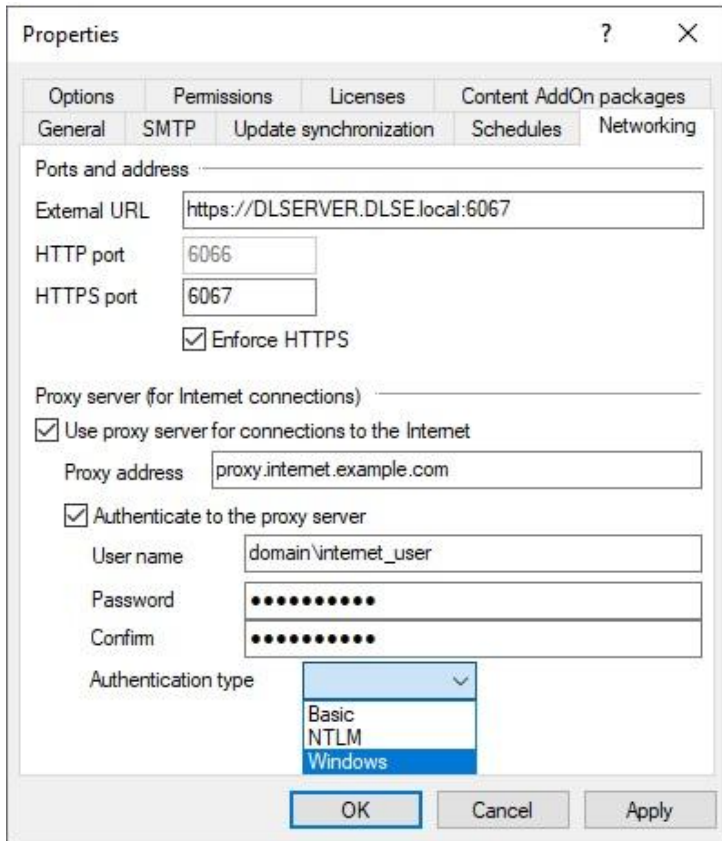
Buttons at the bottom: OK, Cancel, Apply.

To ensure consistent communications across your network, all DriveLock Enterprise Service servers should be configured to use the same ports.

If you change the port that the DES uses, this change must also be reflected in the Agent configuration under Extended configuration -> Global Configuration -> Server Connections.

4.7.1 Using a Proxy Server

To download product updates and virus definitions to a DES server, an Internet connection is required. If your network connects to the Internet using a proxy server you need to configure each DES server to use the appropriate proxy server on the *Networking* tab.



If required, configure the following settings:

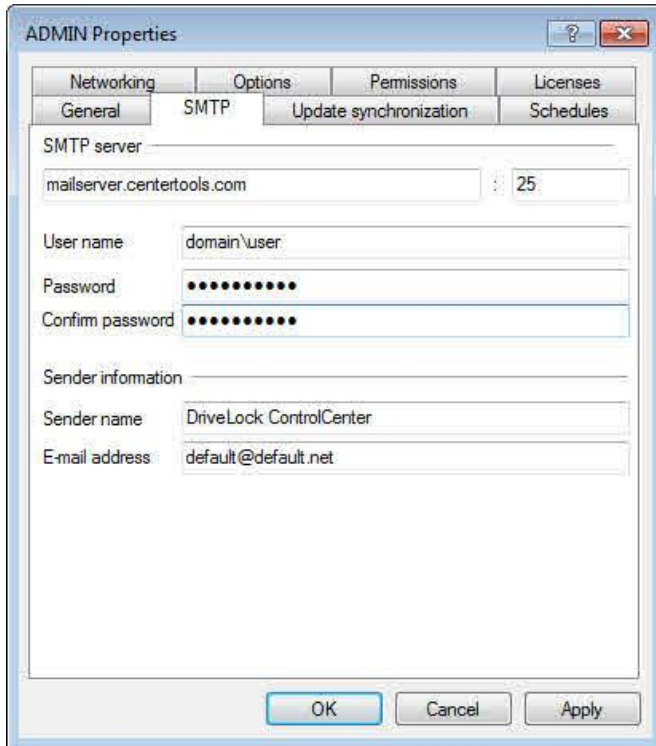
- *Proxy address*: Type the name or address of the proxy server. If the proxy server does not use port 80, you also need to add the port in the format *server:port*, for example *proxy.example.local:8080*.
- *Use proxy server for connections to the Internet*: Select this checkbox to connect via a proxy server.
- *Authenticate to the proxy server*: Select this checkbox if the proxy server requires authentication. Provide the user name and password that is used to connect to the proxy server and then select the authentication type. The proxy server must support the authentication type you select:
 - *Basic*: Authentication data is sent in clear text.
 - *NTLM*: Authentication data is encrypted.
 - *Windows*: Windows integrated authentication. Authentication data is encrypted. The service account under which the DES service is running is used to authenticate and the user name and password in the dialog box is ignored.

4.7.2 Configuring E-Mail Settings for Scheduled Reports

You can use the DriveLock Control Center to configure scheduled reports that are automatically generated and sent via e-mail. These reports are generated by the DES. To enable the sending of such reports you need to specify how the DES server connects to a mail server using the SMTP protocol. You configure these settings on the SMTP tab.

To specify the mail server, type its name in the SMTP server box. If the mail server does not use TCP port 25 for SMTP, also specify the appropriate port.

If the mail server requires authentication for sending SMTP e-mail, type the required credentials in the User name and Password boxes. Type the name and e-mail address that will be used as the sender for messages containing reports in the E-mail sender name and E-mail sender address boxes. Typically an internal e-mail address is used for this purpose.



For more information about creating scheduled reports, refer to the *DriveLock Control Center manual*.

4.8 Using a Multi-Tenant Environment / SaaS

DriveLock and the DriveLock Enterprise Service can be used in a Software as a Service (SaaS) environment where a single service provider administers DriveLock for multiple customers. This can be an external service provider or an internal IT organization that provides services to several independent departments. In a SaaS infrastructure, the customers or departments are referred to as *tenants*. When you configure DriveLock for a multi-tenant environment, a single DES receives event and recovery data from Agents belonging to several tenants and then stores the data from each tenant in a separate database.

Because data from multiple tenants is kept separate and access permissions can be configured separately for each tenant, a service provider can easily provide outsourced DriveLock services for multiple customers while maintaining the security of each customer's data. For example, you can make each customer's data available only to that customer and ensure that it cannot be viewed by other customers. To accomplish this, a linked DriveLock Enterprise Service must be installed at each customer site. Each linked server is connected to the central DriveLock Enterprise Service of the service provider. A separate tenant is created for each customer installation to logically keep the data from each customer separate and to ensure that customer can only view their own data.

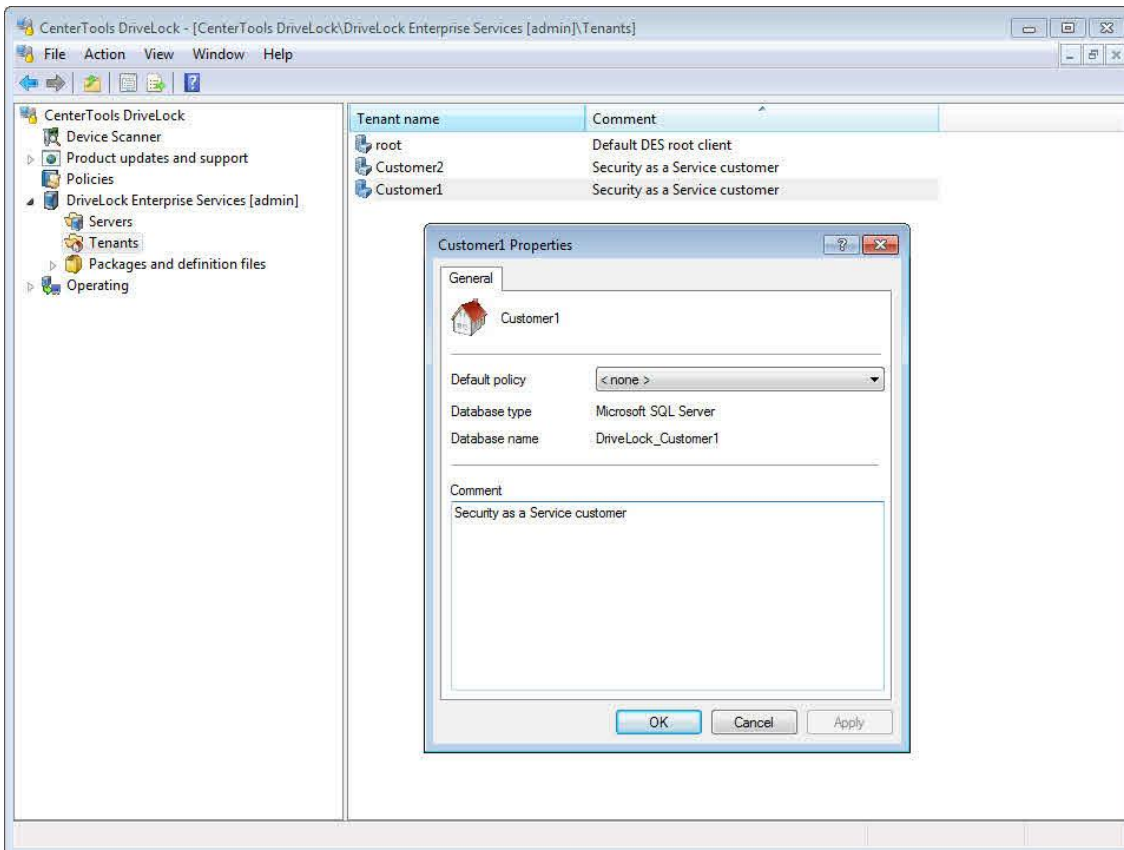
To enable the linking of events to the correct tenant, a dedicated linked DES server must be installed for each tenant. This can be a linked DES server that connects to a central DES server. A typical infrastructure might include the following:

- Server 1 (central DES, standard tenant "root")
- Server 2 (Linked DES, connecting to Server 1, standard tenant "Customer A"
 - DriveLock Agents of Customer A connect to Server 2 using tenant name "Customer A"
- Server 3 (Linked DES server connecting to Server 1, default tenant "Customer B"
 - DriveLock Agents of Customer B connect to Server 3 using tenant name "Customer B"

You configure the DES server's standard tenant name on the *General* tab of the DES server's Properties dialog box.

4.8.1 Creating a Tenant

If you finished creating a new tenant, a new database is created for the tenant with the tenant name appended to the name of the initial DriveLock database. For example, if you selected the default name *DRIVELOCK* for the database when you installed the DES, the databases for the tenant *CUSTOMER* will be named *DRIVELOCK_CUSTOMER* and *DRIVELOCK_CUSTOMER-DATA*.



The default client “root” exists in all DES installations. To create additional tenants, under *DriveLock Enterprise Services* right-click *Tenants* point to *New* and then click **Tenant**.

Type the name of the new tenant. This name cannot contain any special characters.

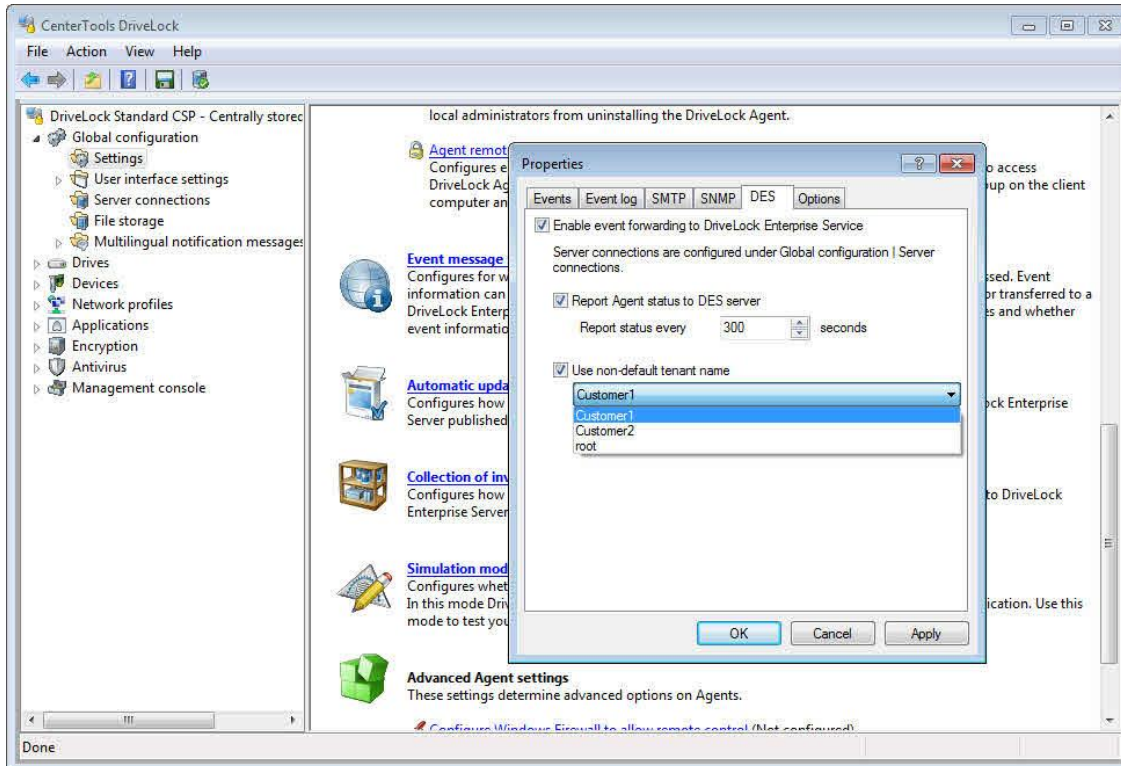
Provide the credentials of a user who has the permissions to create a new database on the database server that is used by DES.

4.8.2 Assigning Agents to a Tenant

To enable DES to assign data from DriveLock Agents to the correct tenant you also need to assign DriveLock Agents to a tenant.

If you don’t assign an Agent to a tenant, it is automatically assigned to the default tenant “root”.

To assign an Agent to a tenant, in your policy under *Global configuration* -> *Settings* -> *Event message transfer settings*. On the *DES* tab, select the *Use non-default tenant name* checkbox and then select the tenant that Agents will be associated with.



4.8.3 Deleting a Tenant

To delete a tenant and the associated database, under *DriveLock Enterprise Services -> Tenants*, right-click the tenant and then click **Delete tenant**.

When you delete a tenant, the associated database is also deleted. This database contains all event data associated with the tenant and recovery data for Encryption 2-Go and Disk Protection. Without this data, encryption recovery will no longer be possible for any clients associated with the tenant.

When you delete a tenant you also need to remove any existing Agent assignments for this tenant under *Extended configuration -> Global configuration -> Settings -> Event message transfer settings* on the DES tab.

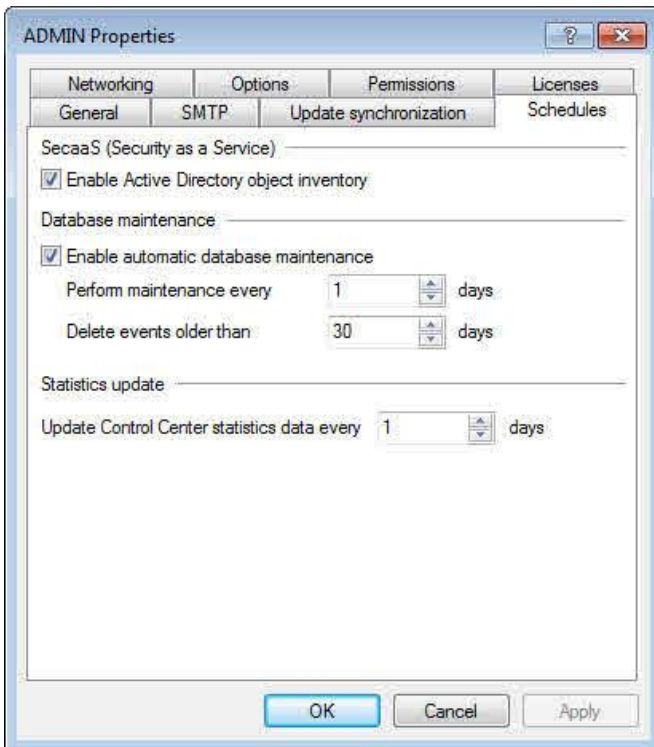
4.8.4 Performing Active Directory Object Inventory Collection

When you assign permissions to in a policy, you can normally only select from users and groups in your own domain or trusted domains. To assign permissions in policies that will be used in non-trusted domains additional steps are required to make the user and group information available. For example, this will allow a service provider without direct access to a tenant's Active Directory to edit permissions in a tenant's policies.

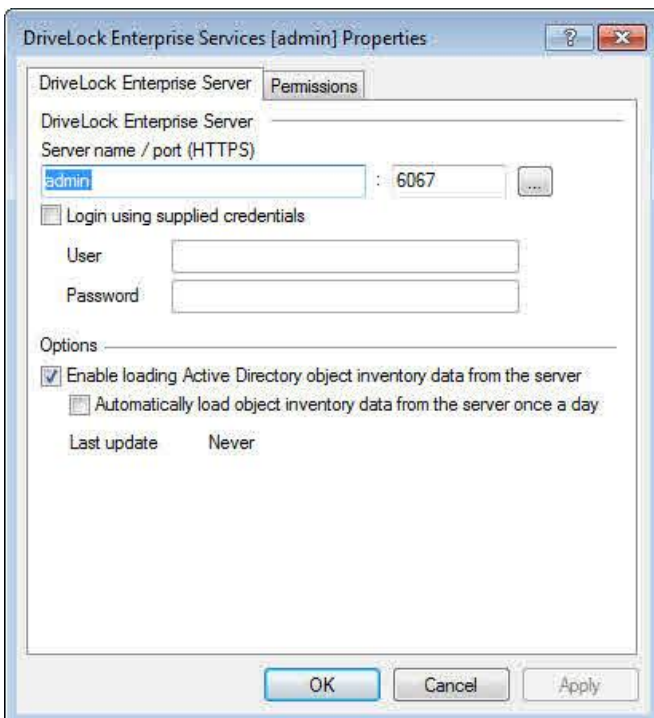
To make user and groups from non-trusted domains available, a DriveLock Enterprise Service can retrieve the required information about users and groups and store them in the DriveLock database for use within a configuration.

When you run the DriveLock Management Console on a computer in the same domain where the configuration will be used, there's no need to first retrieve Active Directory data because the DriveLock Management Console can directly access Active Directory. However, there may be some performance benefits to using inventoried data, especially in large Active Directory environments.

To enable Active Directory object inventory collection, you need to enable this option in the Properties of the central DriveLock Enterprise Service. Because inventory collection is a repeating task, this setting is displayed on the *Schedules* tab.



Once the *Enable Active Directory object inventory* option has been enabled, the DriveLock Enterprise Service starts a process every 24 hours to enumerate all users and groups in the current domain and synchronizes this data with the existing data in the DriveLock database. If you are using different tenants, data is separated by tenant.



After the first inventory collection has been performed you can use inventory data in the DriveLock Management Console. To do this, in the console tree right-click *DriveLock Enterprise Service [Servername]* and then click

Properties. Here you can enable the loading from Active Directory object inventory data from the server. You can also enable the loading of data once a day and view the last time the data was retrieved.

4.8.5 Tenant-Aware Certificate Management

In case your tenants use DriveLock File Protection and the *DriveLock Certificate Management* to manage the user certificates, you can use the master certificate assigned to tenant root to sign all user certificates of all your tenants.

If you want to separate the certificate management for your tenants, you have to enable the *tenant-aware certificate management* at the DriveLock Enterprise Server. Then the master certificates are stored in the tenants database.

At MMC / **Drivelock Enterprise Services** open the server **Properties**, tab **Options** and check **enable tenant aware certificate management**.

For all suitable tenants open the tenant **Properties**, tab **Certificate mgmt** and check **Enable key and certificate management**.

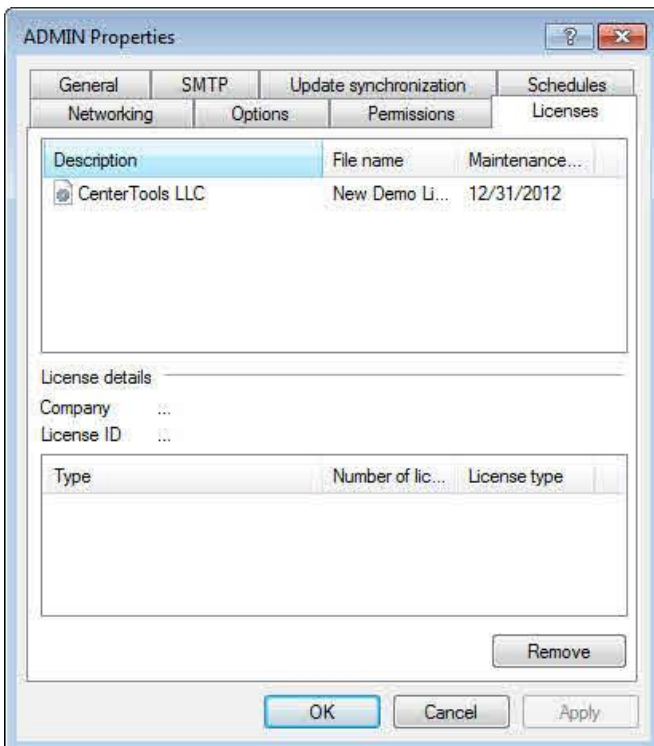
If you enable or disable *tenant-aware certificate management* while user certificates already exist, the exiting certificates are still valid, as long as the master certificate they are signed with, exists.

For more information about certificate management, see: [Configuring DriveLock File Protection](#)

4.9 Viewing License Information

When you create a new DriveLock policy and add license information to it you can also transfer this license data to the DriveLock Enterprise Service. This is required to activate some DriveLock Enterprise Service functionality for supporting certain features, such as management of Security Awareness Content AddOn.

You can maintain the current licensing information on the DES on the central DES's *Licenses* tab.

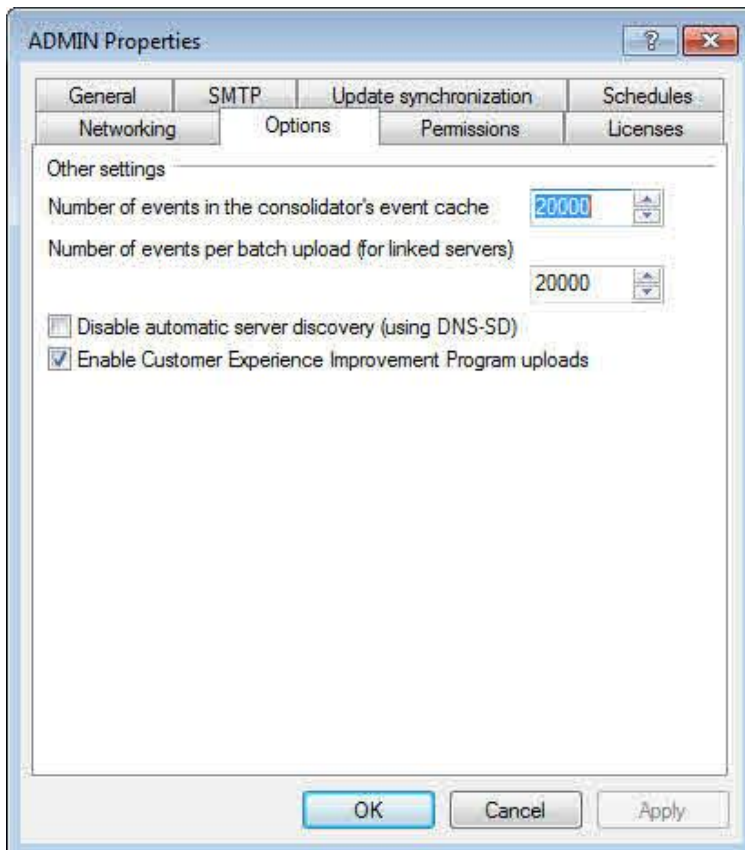


All licenses that are stored by the DriveLock Enterprise Service are displayed. Select a license to view details about it. Click **Remove** to delete the license data from the database.

4.10 Customer Experience Improvement Program

DriveLock maintains a *Customer Experience Improvement Program* that collects statistical data about the speed and frequency of commonly used DriveLock tasks. The data is collected anonymously, uploaded to DriveLock and used to improve DriveLock. No personal data is collected, transmitted or stored by DriveLock.

You are given the option to participate in this program during the installation of DES. To later opt out of the program, under *DriveLock Enterprise Services -> Servers*, in each server's *Properties* dialog box, on the *Options* tab, deselect the *Enable Customer Experience Improvement Program uploads* checkbox.

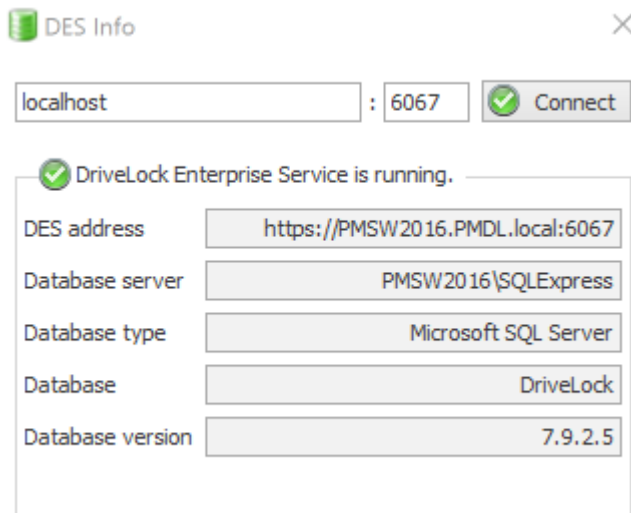


4.11 Viewing the DriveLock Enterprise Service Status

DES includes a status monitor application that can display the DES status in the Windows system tray. The color of the icon (green, yellow, red) indicates whether the service is running and can be contacted. While the service is starting it may take several minutes before the status changes to green.

To start the status monitor, click *Start -> All Programs -> DriveLock -> DriveLock Enterprise Service Status*.

Double-click the icon to open the DES Info window where you can view the current server, database settings or database version.



Right-click the icon in the system tray to display a menu from where you can perform additional tasks, such as starting or stopping the service.

Part V

DriveLock Groups

5 DriveLock Groups

Starting with DriveLock version 2019.1, you can define your own computer groups and use them for assigning DriveLock policies or within policies to configure policy settings.

5.1 Creating DriveLock Groups

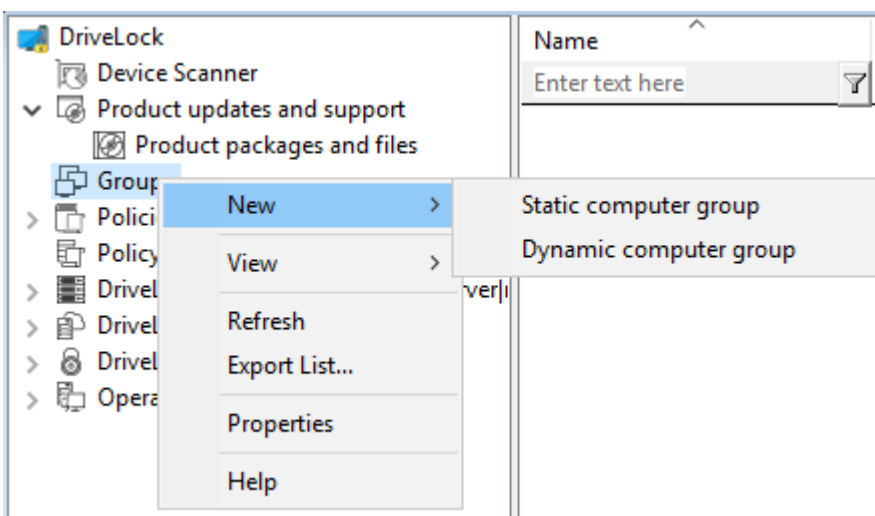
There are two different DriveLock groups:

- [Static computer groups](#) are defined by *manually* adding computers, groups, or organizational units from Active Directory (AD), from individual computers (which are added individually by name), or even from existing DriveLock groups.
- [Dynamic computer groups](#) are defined *from the results of queries (criteria)*, e.g. query for operating system version, IP range, Windows version and more.

DriveLock determines the membership of an Agent in a dynamic group as follows: First, the filter criteria you specify are stored in a database. Then, the criteria are transferred to the agent computers where they are evaluated. This is followed by the client reporting back on its respective group membership. After updating the configuration, the members are displayed in the dynamic group's properties (**Current Members** tab).

Note that DriveLock version 2019.1 or newer must be employed on the DriveLock Management Console, the DriveLock Enterprise Service (DES) and on all DriveLock Agents. Older DriveLock versions on the Agents prevent proper evaluation and feedback of the respective group membership.

You can create DriveLock groups centrally in the DriveLock Management Console in the **Groups** node (see figure):

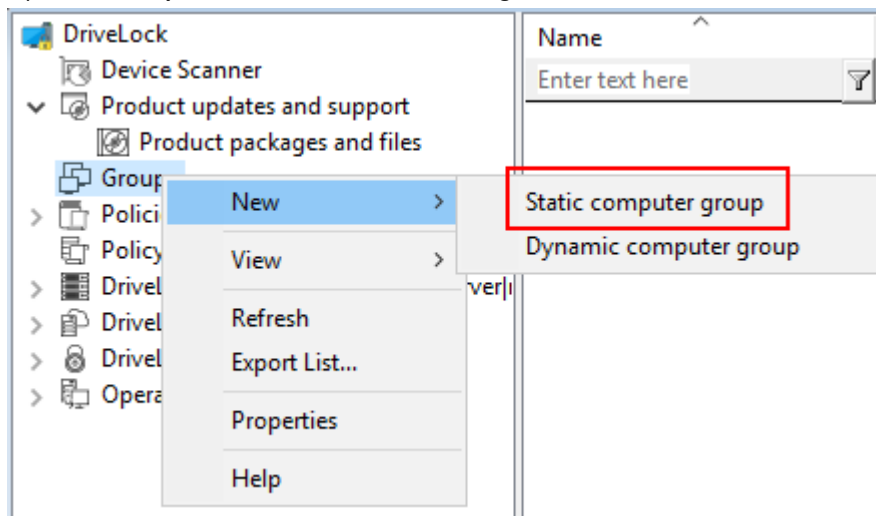


You can create new DriveLock groups, change existing ones or delete them at any time. Changes always affect the policies where the group is used. You can only delete a group if it is no longer used in a policy.

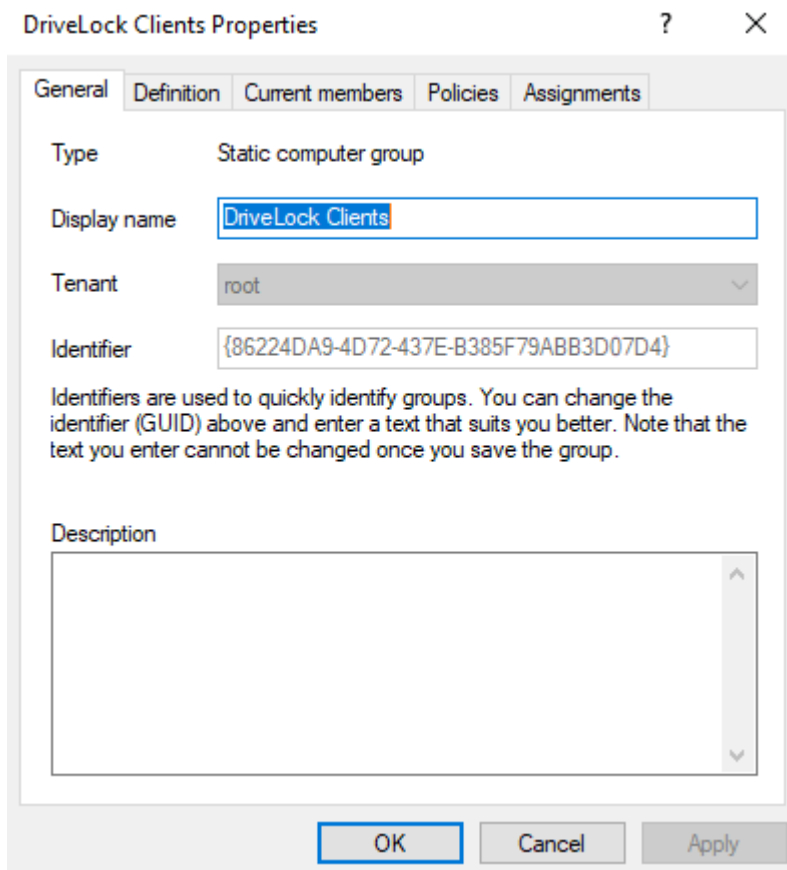
5.1.1 Creating Static Computer Groups

To create a static computer group, please follow these steps:

1. Open the **Groups** node in the DriveLock Management Console and select **Static computer group**.



2. Enter a name for the group on the **General** tab, select a corresponding tenant and enter a comment, if you want. In the example below the computer group is called **DriveLock Clients** because it consists of DriveLock clients.

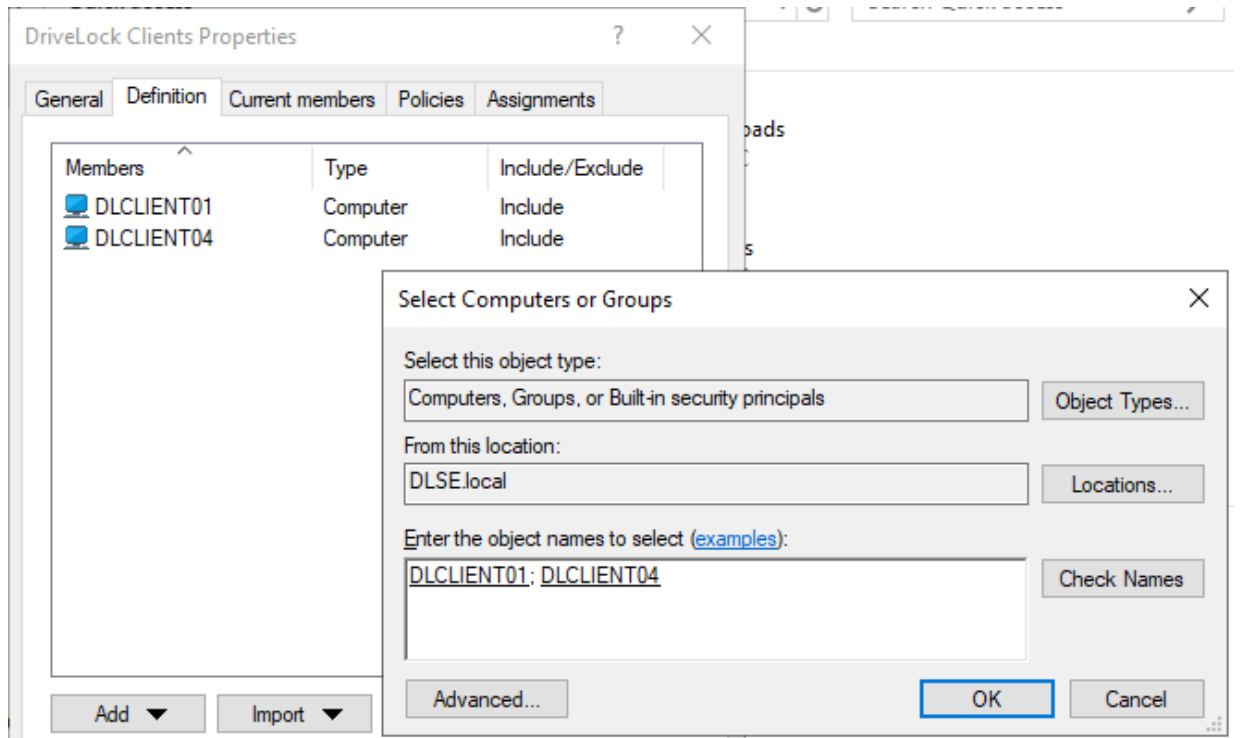


The **Identifier** is entered automatically as unique ID. When you create the group, you can change it which may be helpful for you to find the group easier later on (for example in log files).

Note that you once you've assigned an identifier you cannot change it later!

3. On the **Definition** tab you can [add](#) or [import](#) computers by clicking the buttons at the bottom of the dialog. In the example below, two computers named DLCLIENT01 and DLCLIENT04 were added to the static groups with

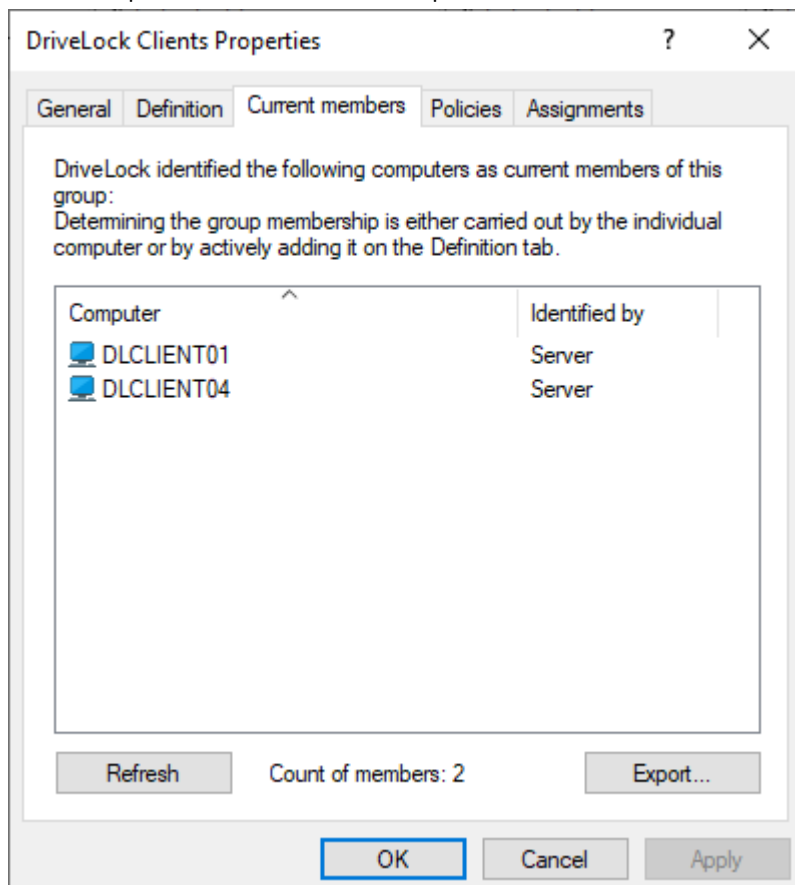
the option **Active Directory Computer or Group...**



You can also use the **Remove**, **Include** or **Exclude** buttons as needed.

- After updating the configuration, the **Current Members** tab provides you with a list of computers that belong to your static group.

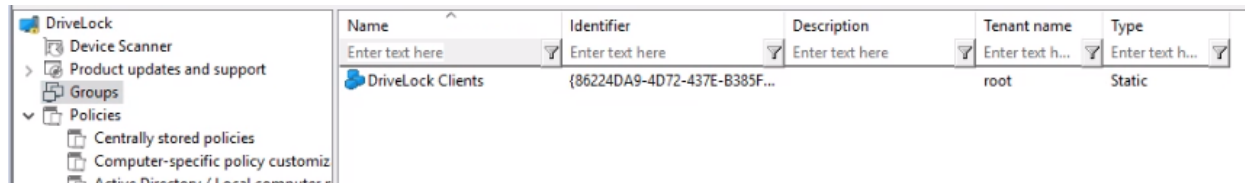
In the example below these are the computers DLCLIENT01 and DLCLIENT04.



In the **Identified by** column you can see how DriveLock determined the group membership. If the groups were added via the DriveLock Management Console, **Server** is entered in the column.

As soon as the client reports its group membership back to the DES, the column entry is **Client**.

5. Find more information on the other tabs **Policies** and **Assignments** in the [Using groups in policies](#) chapter.
6. If you check the **Group** node in the DriveLock Management Console now, you can see the name of the static group you created (see example below).

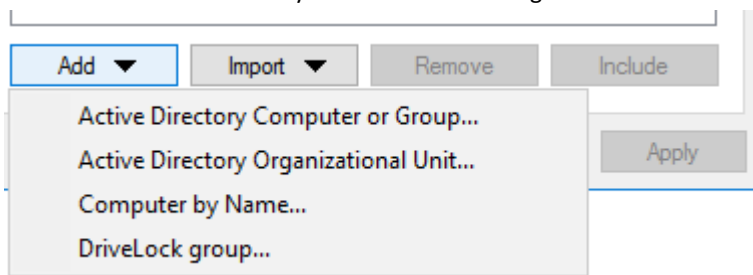


Name	Identifier	Description	Tenant name	Type
DriveLock Clients	{86224DA9-4D72-437E-B385F...}		root	Static

5.1.1.1 The Add Button

This is how you proceed on the **Definition** tab to add computers, organizational units, or groups to the static computer group.

Click the **Add** button. Here you have the following choices:



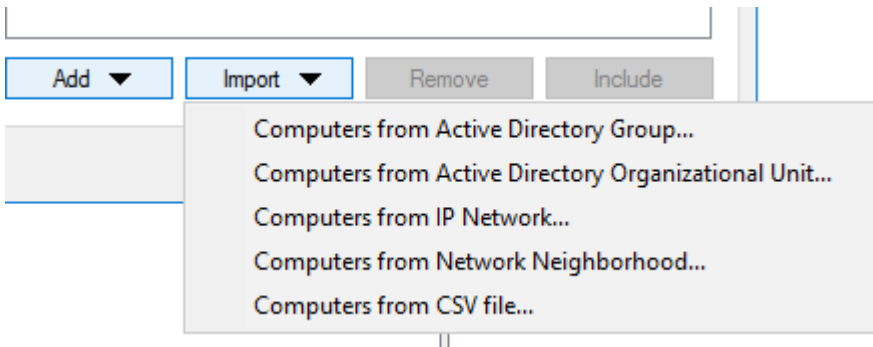
1. **Active Directory Computer or Group...**
Select individual computers or groups directly from the AD and add them to your static group.
2. **Active Directory Organizational Unit...**
Select the computers from an AD OU.
3. **Computer by Name...**
Add individual computers by name to your group.
4. **DriveLock-Group...**
You can also add a DriveLock group (dynamic or static) which you created earlier.

Please note that you cannot use wildcards for static group definitions.

5.1.1.2 The Import Button

This is how you proceed on the **Definition** tab to add *individual* computers from different sources to the static computer group.

Click the **Import** button. Here you have the following choices:

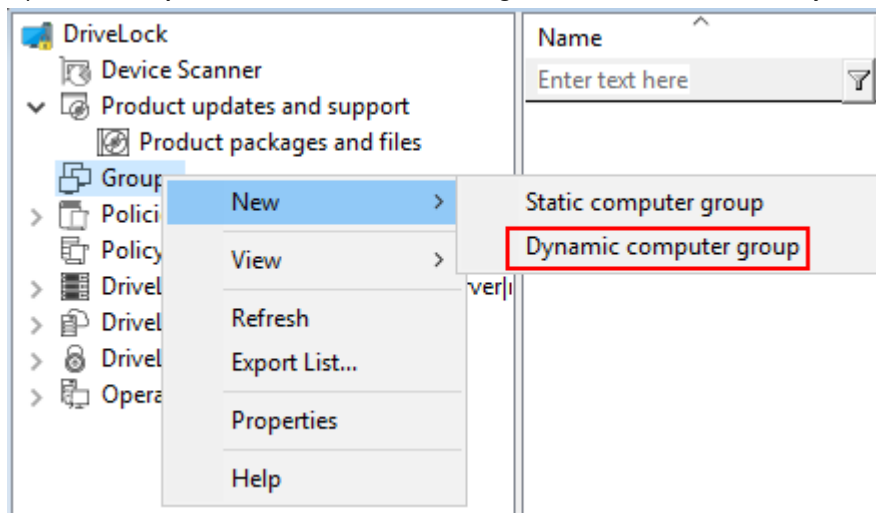


1. **Computer from Active Directory Group...**
Import computers from the selected AD group directly into your static group.
2. **Computer from Active Directory Organizational Unit...**
Select the relevant AD OU from where you want to import the computers.
3. **Computer from IP Network...**
Indicate a specific IP range where the computers you want to import are located.
4. **Computer from Network Neighborhood...**
Select the computers from the direct network locations as members.
5. **Computer from CSV file...**
Select the CSV file that lists the computers you want to add to the static group.

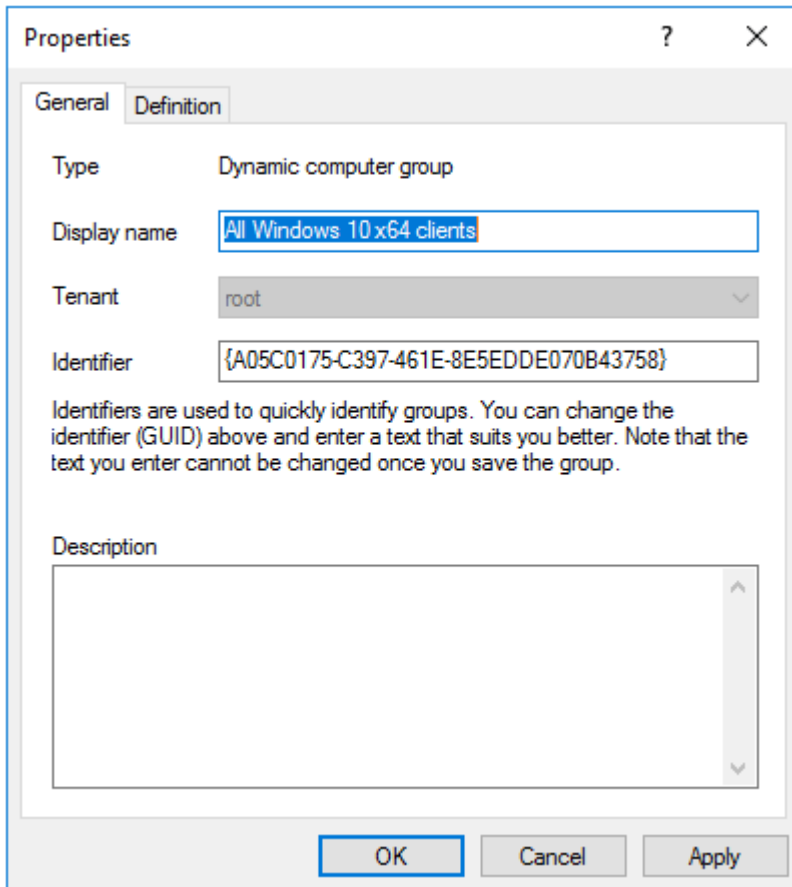
5.1.2 Creating Dynamic Computer Groups

To create a dynamic computer group, please follow these steps:

1. Open the **Groups** node in the DriveLock Management Console and select **Dynamic computer group**.



2. Enter a name for the group on the **General** tab, select a corresponding tenant and enter a comment, if you want. In the example below, the dynamic group will consist off members who are using *Windows Version 10* as operating system version and who have an *x64 Architecture*.



Properties

General Definition

Type Dynamic computer group

Display name All Windows 10 x64 clients

Tenant root

Identifier {A05C0175-C397-461E-8E5EDDE070B43758}

Identifiers are used to quickly identify groups. You can change the identifier (GUID) above and enter a text that suits you better. Note that the text you enter cannot be changed once you save the group.

Description

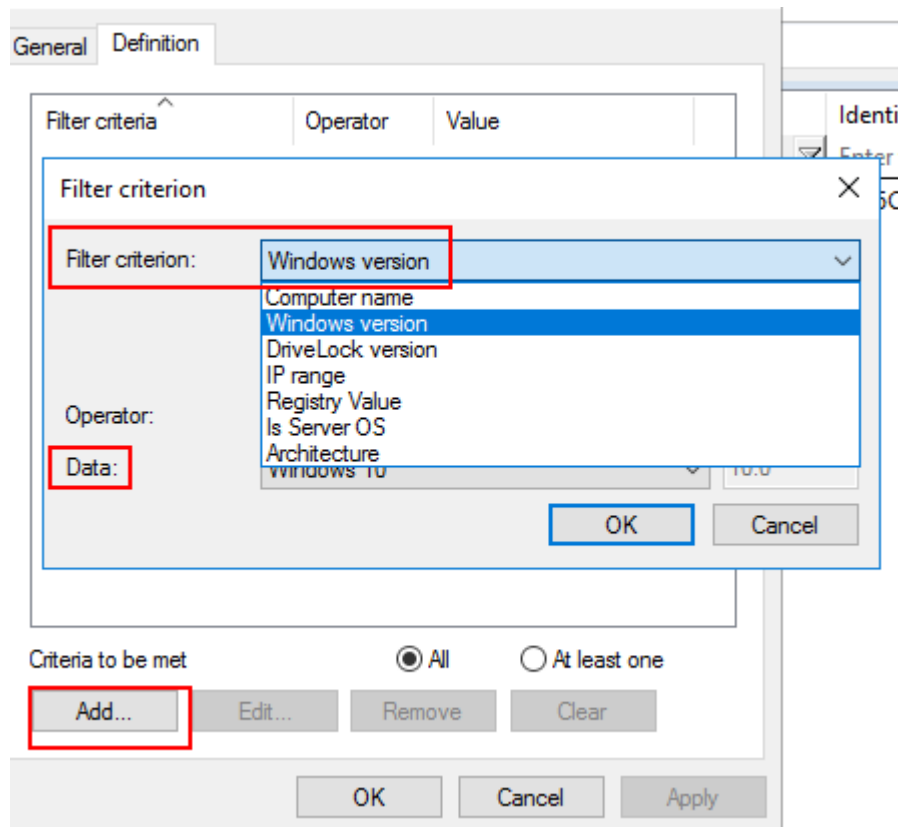
OK Cancel Apply

The **Identifier** is entered automatically as unique ID. When you create the group, you can change it which may be helpful for you to find the group easier later on (for example in log files).

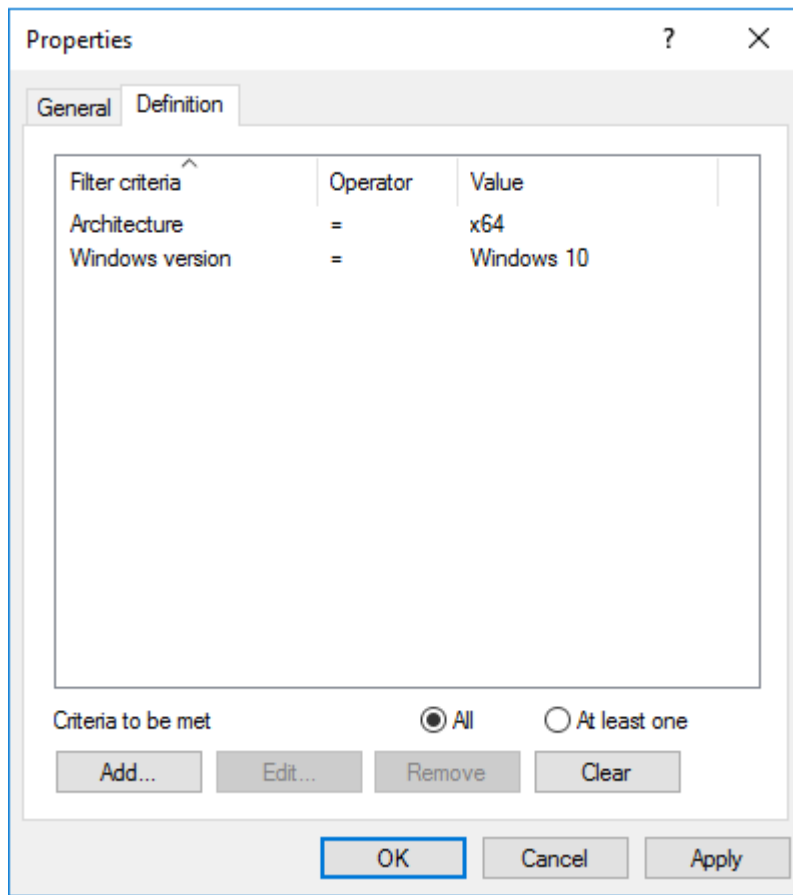
Note that you once you've assigned an identifier you cannot change it later!

- On the **Definition** tab you can select the filter criteria. You can also select whether **All** or **At least one** criteria must be met.

In the example below, the **Windows version** (here Windows 10 as **Data**) is selected first and after that the **Architecture** filter criterion. The selected **Operator** is a '=' here. In other cases you may also use different operators.



4. When you are done with adding the **criteria**, you can see which ones you selected in the list. See example below:



Click **Edit** if you want to edit the criteria later, click **Remove** if you want to delete them from the list.

5. Finally, click **OK** to create your dynamic group.
6. When you are finished, you can use your dynamic group for configuring and assigning policies.
7. In the **Dynamic Group Properties** you will also see the **Current Members**, **Policies** and **Assignments** tabs (see more information in chapter [Static Groups](#)).

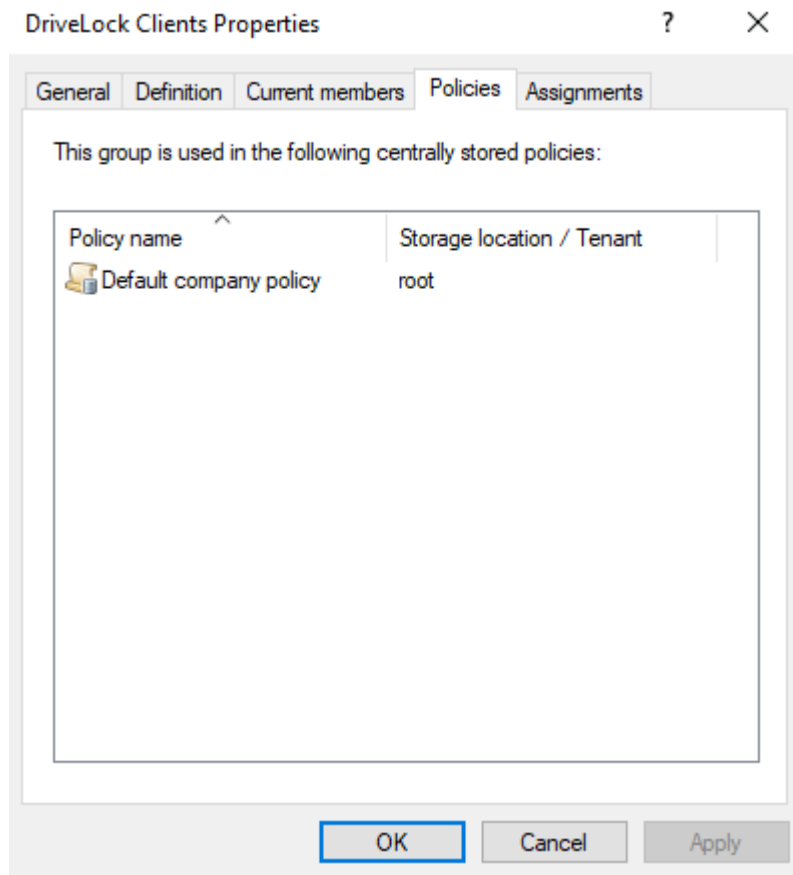
5.1.3 Using Groups in Policies

You can use static and dynamic groups in all whitelist rules (drive and device whitelist rules), in application rules and in file filter templates. Also, you can use groups to define rules for Security Awareness.

In order to use groups in policies, you have to define them first. We do not provide any default DriveLock groups which you can use out of the box.

After defining your DriveLock group, it will appear on the **Policies** tab to show you where it is being used.

In the example below, the properties dialog for the **DriveLock Clients** group (see example in [Creating Static Computer Groups](#)) shows the policy where the group is being used (here the **Default company policy**).

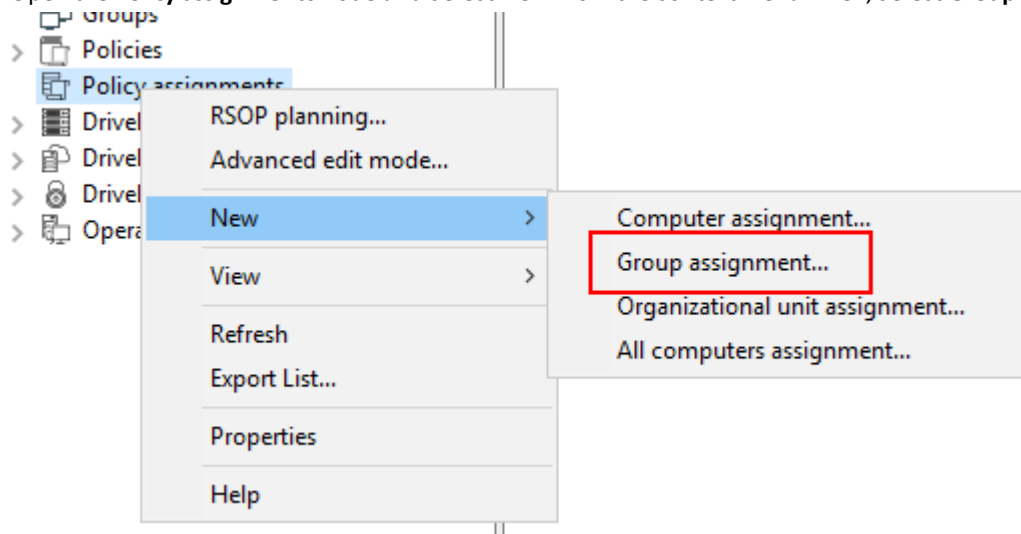


Please note that it is absolutely necessary to be connected to a DES to be able to implement DriveLock's group concept. Clients that are only temporarily disconnected (offline) from the DES will be updated with the current policies (and group settings) the next time they connect.

5.1.3.1 Policy Assignments

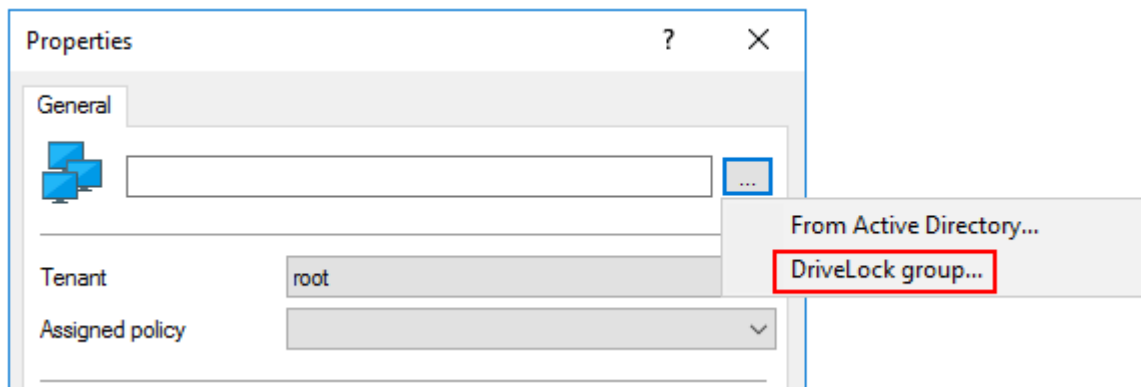
To [deploy policies](#) (group assignments) you can either select a group from the AD or a DriveLock group (static or dynamic).

1. Open the **Policy assignments** node and select **New** from the context menu. Then, select **Group assignments...**



Before you can use any DriveLock groups in policy assignments, you have to create them first.

2. Click ... and select **DriveLock group...**




3. As described in the example in chapter [Creating Static Computer Groups](#) you can select your DriveLock group (named **DriveLock Clients** in this example), the corresponding tenant (here **root**) and the respective policy (here

Default company policy).

Properties ? X

General

 DriveLock Clients ...

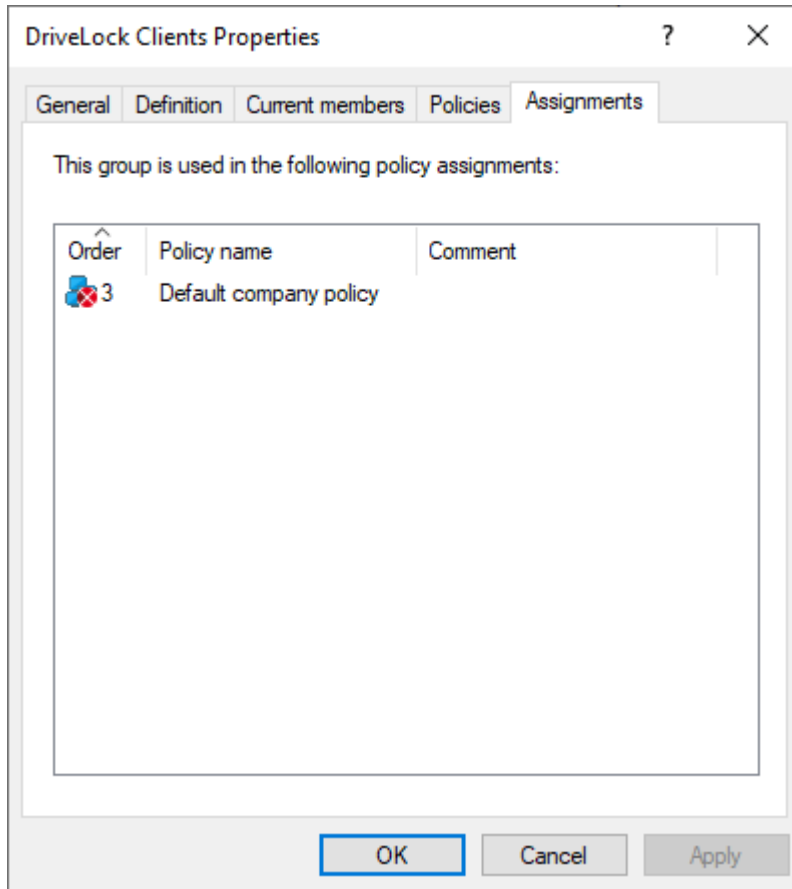
Tenant root

Assigned policy Default company policy

Comment

OK Cancel Apply

4. After having assigned the DriveLock group to a policy (in this example **Default company policy**), the policy appears on the **Assignments** tab of the group's properties dialog.





Part VI

Configuring Global DriveLock Settings



6 Configuring Global DriveLock Settings

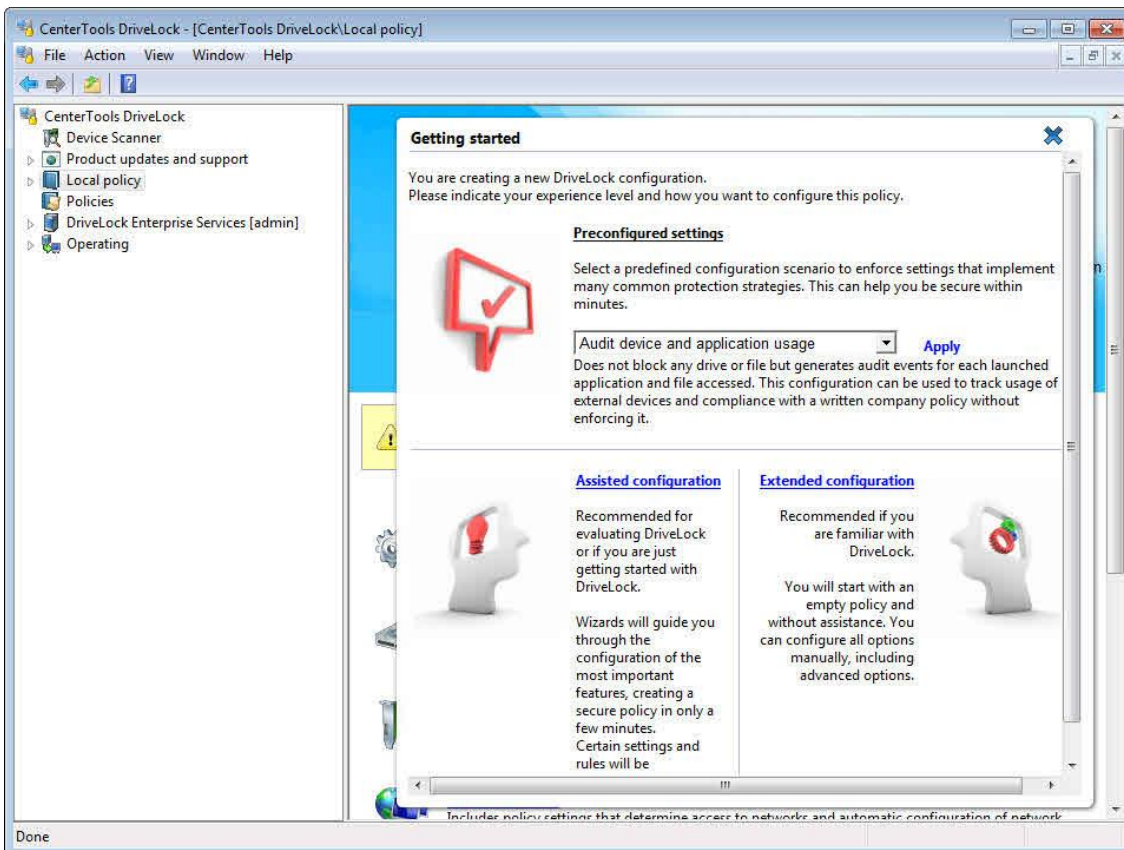
Global settings in a DriveLock policy apply to all Agents that use this policy, whether the policy settings are stored in a Group Policy Object (GPO), a centrally stored policy or a configuration file. When using a local configuration, the global settings apply to the local Agent only.

When using Group Policy to deploy DriveLock settings, it is recommended to use Group Policy permissions to ensure that only authorized administrators can view or modify the DriveLock policy. If you use a configuration file, use Windows file permissions to implement such controls. When using centrally stored policies, DriveLock Enterprise Service permissions enforce the security of your policy settings.

6.1 Using Predefined Security Configurations

When you create the first DriveLock configuration you can start with one of the predefined security configurations and skip configuring many individual settings. This can make it much easier and quicker to get started with DriveLock.

If you are using a local policy for testing, open this local policy. The *Getting started* window appears. This window also appears when you open a configuration file, centrally stored policy or Group Policy Object for the first time and then click **DriveLock** in the console tree.



In the *Getting started* dialog box, select one of the pre-configured policies. A short description of the policy settings appears below the selection. When you click **Apply**, DriveLock starts the Configuration Wizard, which guides you through the steps to configure additional required settings, such as license activation and connecting to the DriveLock Enterprise Service. Once you have completed the wizard, DriveLock applies all settings.

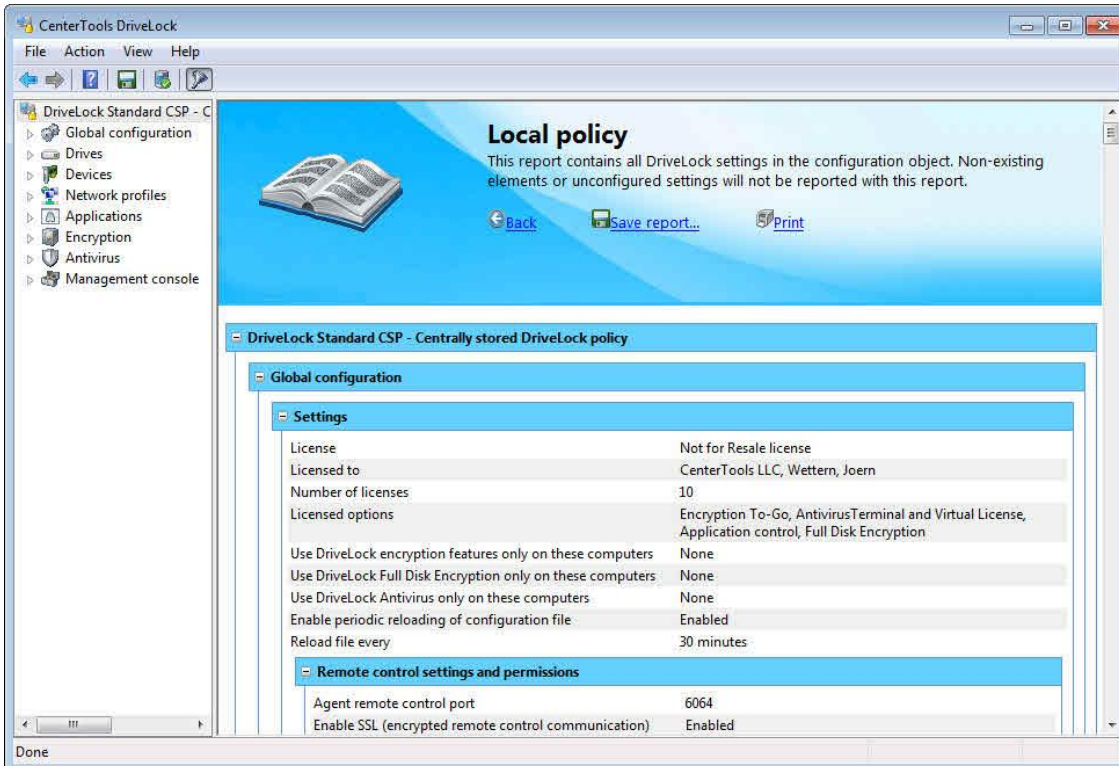
For more information about license activation and configuration of a DES connection, refer to the sections "[Licensing](#)" and "[Configuring DES connections](#)".

6.2 Creating Configuration Reports

DriveLock can generate a XML-based report of all configured settings that is similar to a Windows Group Policy report. Settings that are not configured are not included in the report. You can view, save or print a configuration report.

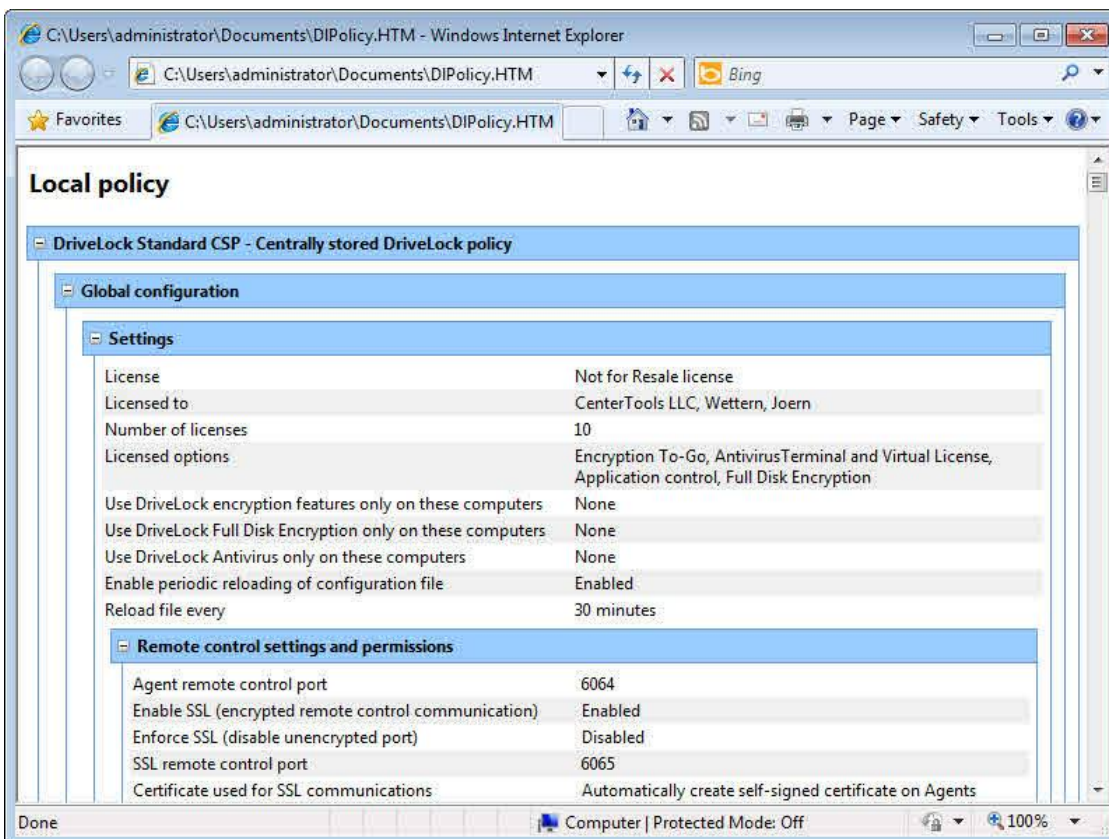


Click **Generate report** to generate a configuration report.

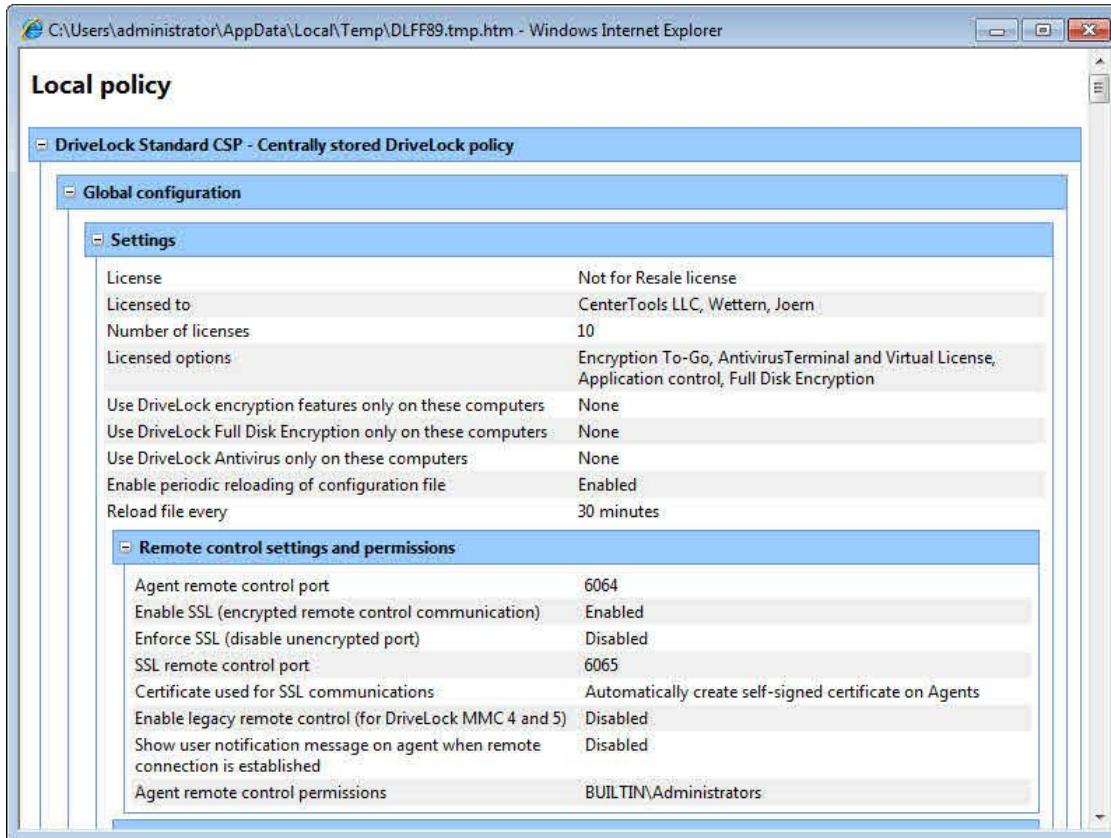


Scroll through the sections and settings and use "+" and "-" to expand and collapse sections.

Click **Save report** to save a configuration report as an "*.html" file. Use Internet Explorer to open and view the configuration report.



Click **Print** to print a configuration report. A new Internet Explorer window opens and displays the Print dialog box. Select a printer and then click **Print**.



6.3 Activating Your License

Each DriveLock Agent installed on a client computer must have a valid license. Depending on the licenses you have purchased and how many of them you have, a certain number of modules will be available for your agents after you add the license file (.lic) or license key.

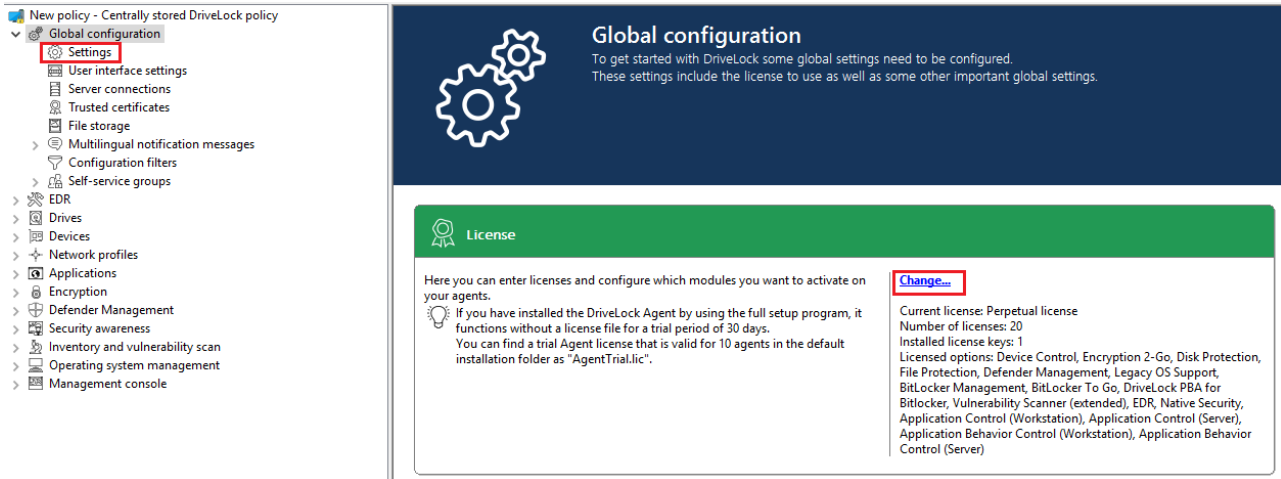
The license must be activated once in a policy.

If you have installed a DriveLock Enterprise Service (DES), please transfer the license information directly to it. You can only activate certain server features, such as downloading the Security Awareness Content AddOn, if a valid license is present on the DES.

If you are installing DriveLock for the first time and have not yet entered a license in the policy, the agent will initially receive a trial license for a period of 30 days.

The download package also includes a trial license that is valid for 10 agents. This license (AgentTrial.lic) is located in the default installation directory under C:\Program Files\CenterTools\DriveLock MMC\Tools.

Configure the license information in **Global configuration | Settings | License**.



Global configuration
To get started with DriveLock some global settings need to be configured. These settings include the license to use as well as some other important global settings.

License

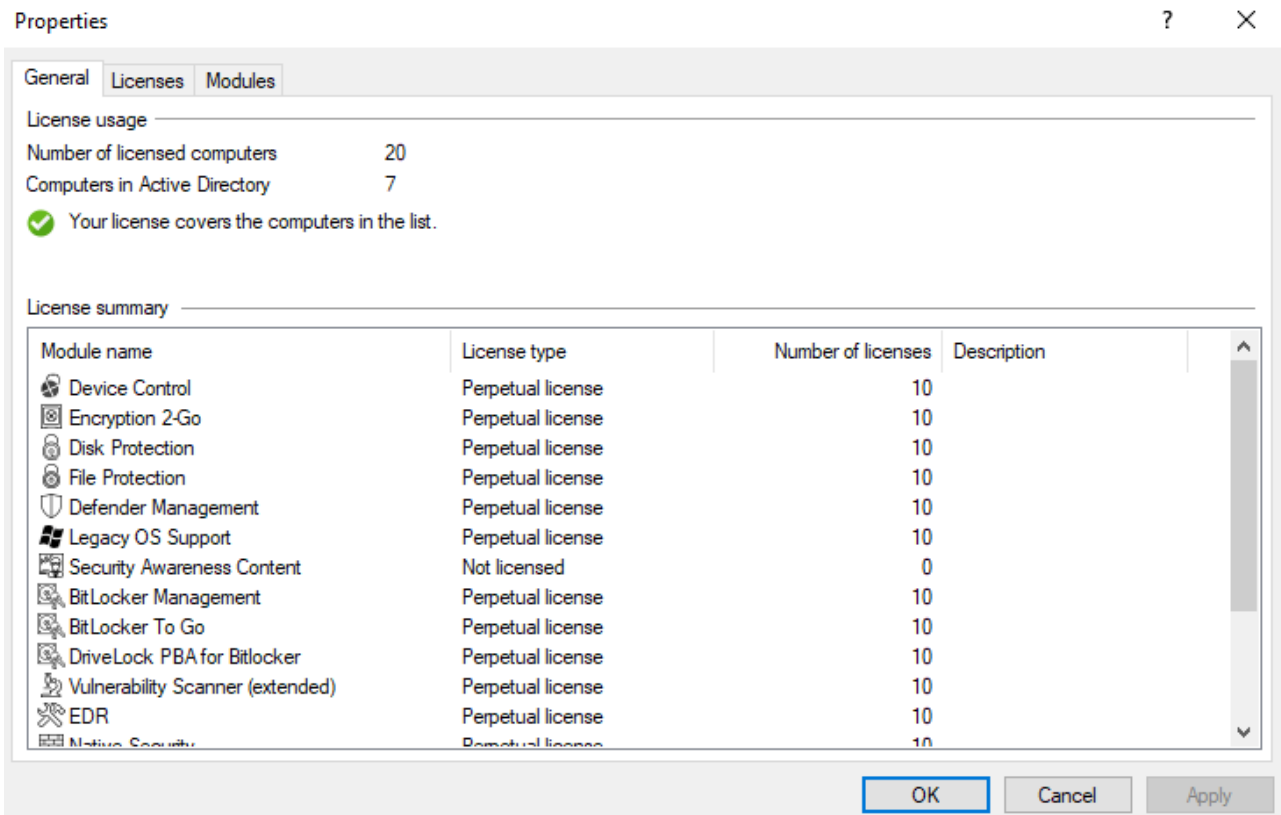
Here you can enter licenses and configure which modules you want to activate on your agents.

If you have installed the DriveLock Agent by using the full setup program, it functions without a license file for a trial period of 30 days. You can find a trial Agent license that is valid for 10 agents in the default installation folder as "AgentTrial.lic".

[Change...](#)

Current license: Perpetual license
Number of licenses: 20
Installed license keys: 1
Licensed options: Device Control, Encryption 2-Go, Disk Protection, File Protection, Defender Management, Legacy OS Support, BitLocker Management, BitLocker To Go, DriveLock PBA for BitLocker, Vulnerability Scanner (extended), EDR, Native Security, Application Control (Workstation), Application Control (Server), Application Behavior Control (Workstation), Application Behavior Control (Server)

Click **Change...** to open the license dialog.



Properties [?] [X]

General Licenses Modules

License usage

Number of licensed computers: 20
Computers in Active Directory: 7

Your license covers the computers in the list.

License summary

Module name	License type	Number of licenses	Description
Device Control	Perpetual license	10	
Encryption 2-Go	Perpetual license	10	
Disk Protection	Perpetual license	10	
File Protection	Perpetual license	10	
Defender Management	Perpetual license	10	
Legacy OS Support	Perpetual license	10	
Security Awareness Content	Not licensed	0	
BitLocker Management	Perpetual license	10	
BitLocker To Go	Perpetual license	10	
DriveLock PBA for Bitlocker	Perpetual license	10	
Vulnerability Scanner (extended)	Perpetual license	10	
EDR	Perpetual license	10	
Native Security	Perpetual license	10	

OK Cancel Apply

The **General** tab displays the license status of each module.

On the **Licenses** tab, you can **add your license file or license key**, or remove expired or trial licenses if necessary.

Follow the license activation steps in the wizard.

The DriveLock license can be activated either online or manually by calling the DriveLock Activation Center. For online activation, select **Online**. If it is necessary to specify a proxy server for your Internet connection, click **Proxy** and enter the server name, a user and the appropriate password.

The license will be activated by connecting to the DriveLock activation server. This usually takes only a few seconds.

Notes for telephone activation:

1. To avoid any inconsistencies, please make sure that the computer you are using for activation has a current time and the correct time zone.
2. The activation code is only valid for a certain period of time. You must enter the activation code within one hour, or you will have to request a new activation code. If this happens, click Cancel and start the Activation Wizard again.

After successful activation, we recommend that you transfer the licenses to DriveLock Enterprise Service. At this point, specify the server name where your DriveLock Enterprise Service is installed. If you do not specify a name, the transfer process will be skipped.

To view the contents of a license, highlight the license and click **Properties...**

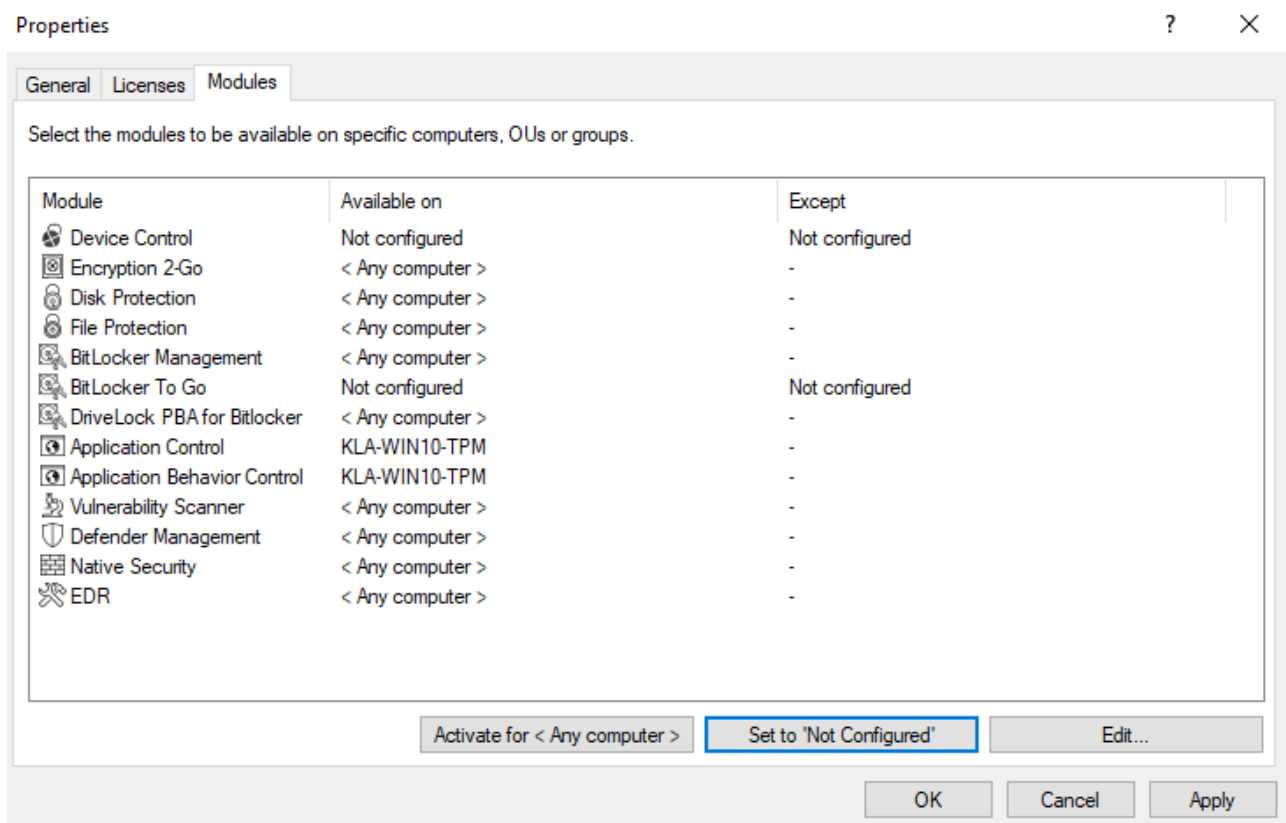
On the **Modules** tab you can configure which module will be active on each agent.

With this information you can...

- avoid that a certain module is used on too many DriveLock Agents (only active modules "use up" a license)
- avoid initializing modules on an agent that are not needed there.

If you set modules to the value '**Not configured**', the settings from another policy will be used. This means that you can configure different modules in different policies instead of only in the policy where you enter the license.

The total number of licenses required is determined based on agent feedback. You will be alerted if you do not have enough licenses.

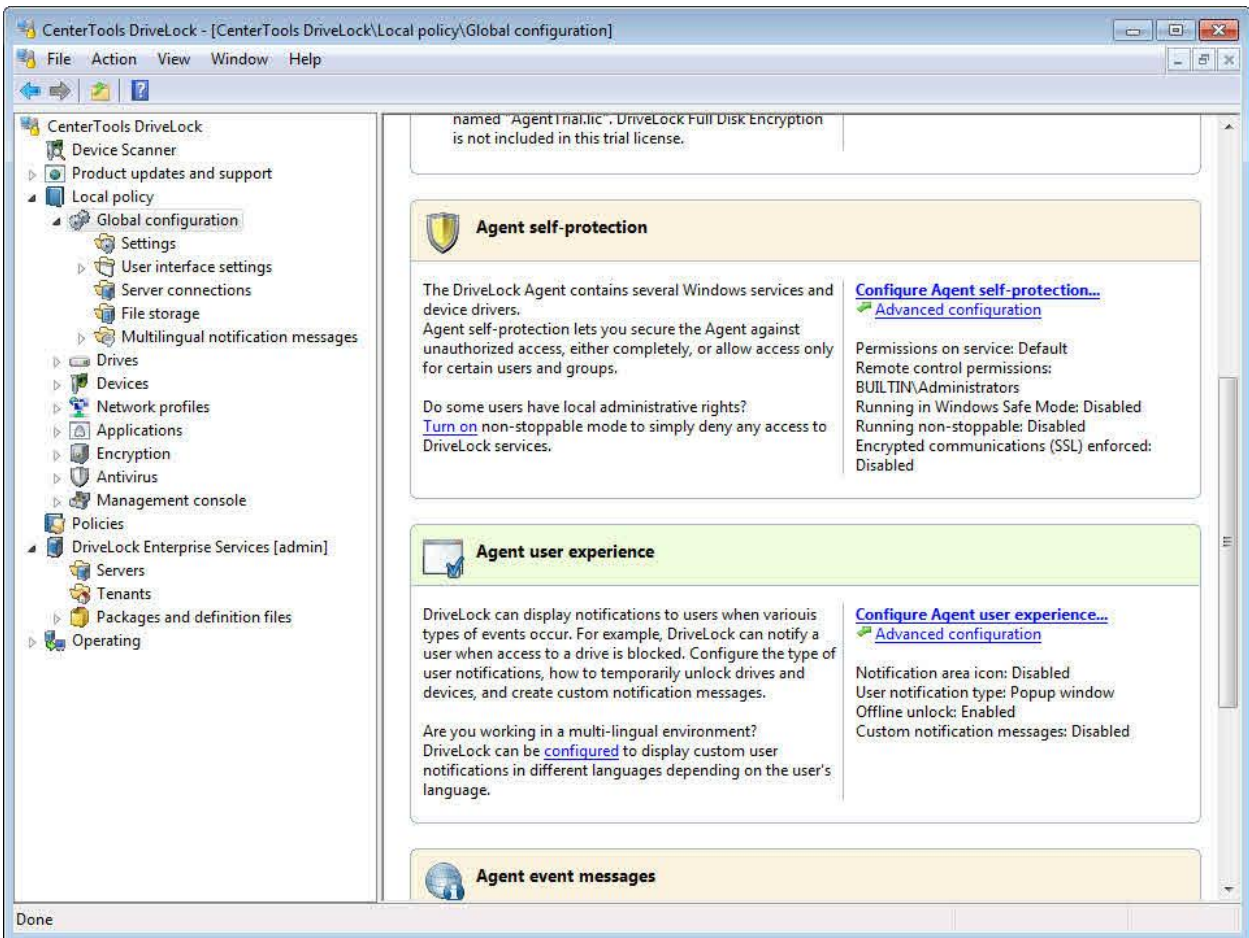


6.4 Agent Hardening and Global Security Settings

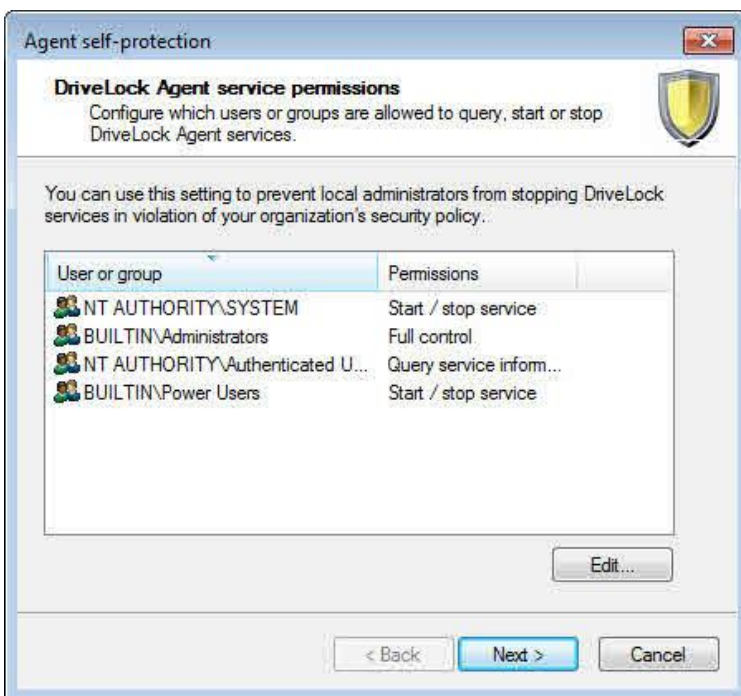
Agent hardening protects against users bypassing policy settings that are enforced by the DriveLock Agent.

Use Basic configuration mode to quickly configure basic security setting in a few short steps. Use extended settings to configure more details and additional settings not available in Basic configuration mode.

6.4.1 Configuring Global Security Settings in Basic Configuration mode

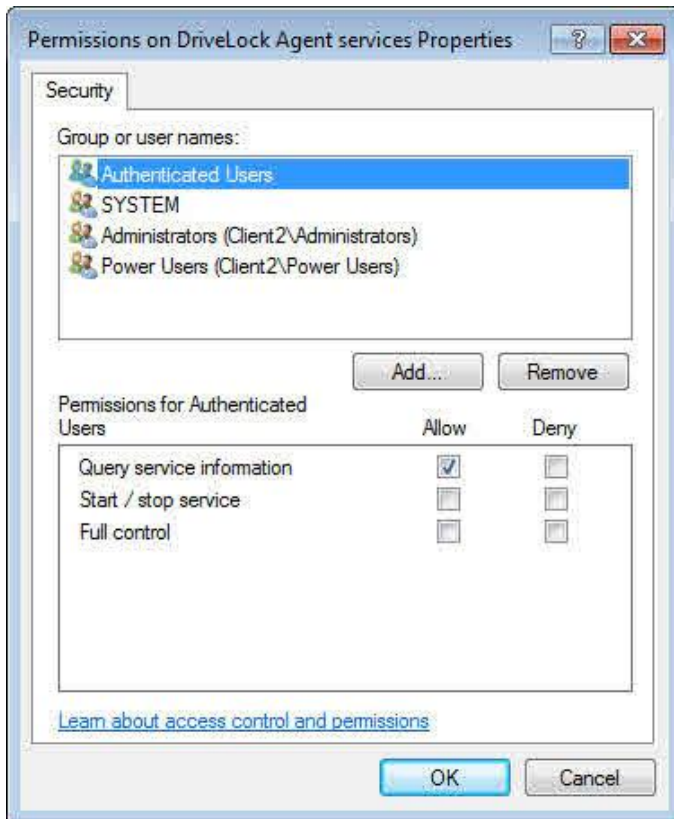


Click **Configure Agent self-protection**. The Agent self-protection wizard starts.



To control which users can access or stop the DriveLock service on client computers, configure permissions for the DriveLock Agent service. For example, you could deny "Power Users" the permission to stop the service.

To change permissions for users and groups, click **Edit**.



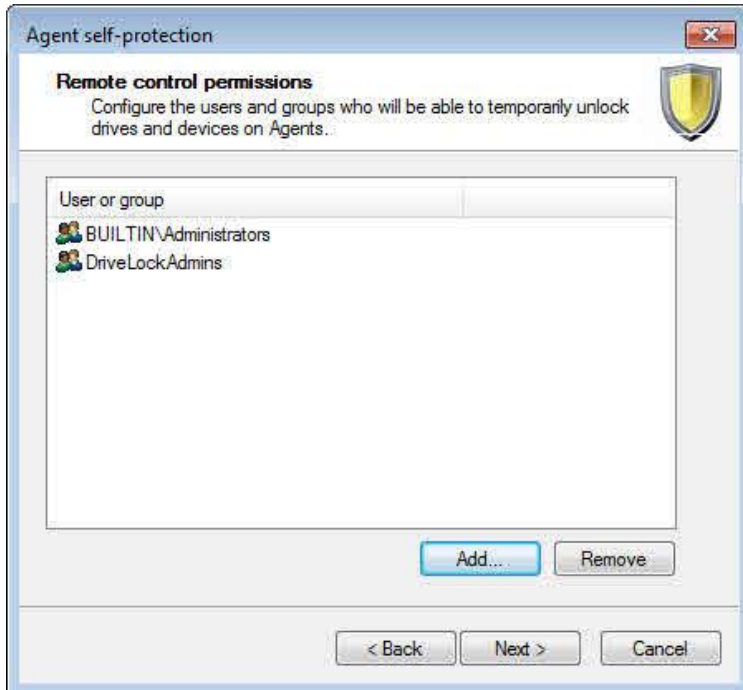
Click **Add** or **Remove** to add accounts to or remove accounts from the permissions list.

Select an account to configure the permissions assigned to it, and then select the Allow and Deny checkboxes to allow or deny the following permissions:

- Query service information (display the properties of the service)
- Start / stop service
- Full control

You cannot revoke the permissions of the local System account. If you attempt to do this, DriveLock automatically restores these permissions because they are required for DriveLock to function.

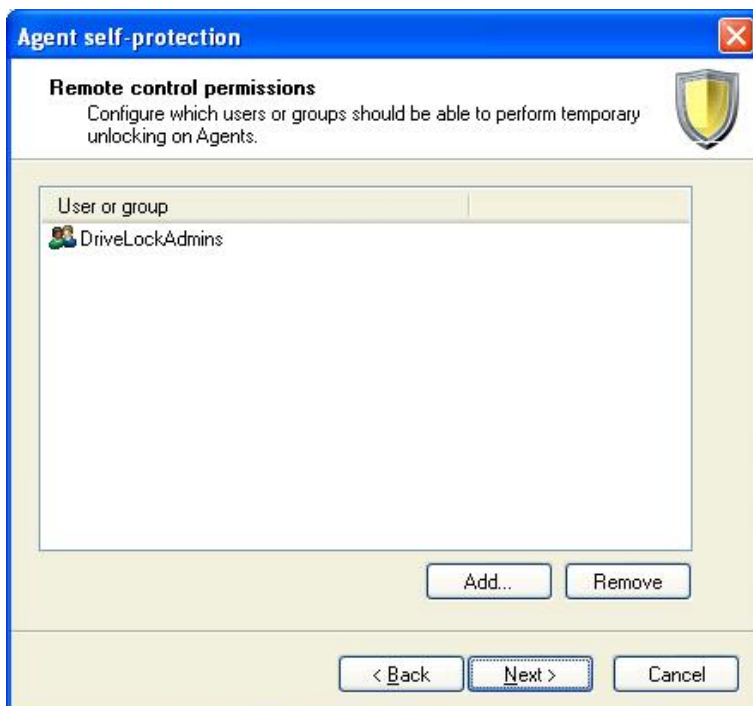
Click **OK** and then click **Next**.



Remote control permissions determine which users or groups are allowed to unlock Agent-controlled drives or devices by using the “Agent remote control” feature of DriveLock.

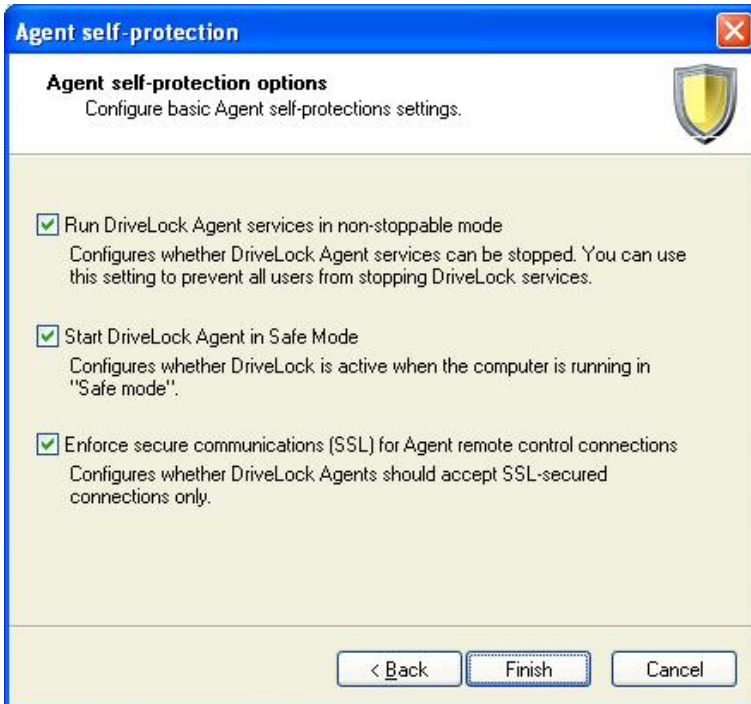
Click **Add** and then select users or groups that are allowed to connect to the DriveLock Agent.

Click **OK** after selecting the correct user or group.



By default, the built-in Administrators and Domain Admins groups have the permissions required to use Agent remote control. When you configure remote control permissions, only the users and groups you add to the list are authorized to use Agent remote control. To retain the permissions for the Administrators or Domain Admins groups, you must add them to the list.

Click **Next** to proceed.



To prevent all users from stopping the DriveLock Agent, activate “**Run DriveLock Agent services in non-stoppable mode**”.

When you enable non-stoppable mode, no user can stop the DriveLock Agent, regardless of any permissions you may have configured.

Select the option “**Start DriveLock Agent in Safe Mode**” to start the DriveLock Agent when the client computer is running in Safe-Mode. When you select this option, users can’t bypass the restrictions in your policy by starting the computer in Safe Mode.

When using DriveLock in Safe Mode, you can no longer revert to previous configuration settings by booting into Safe Mode. This can complicate the process of restoring access to a client computer if DriveLock blocks devices that are required to use the computer because of a configuration errors.

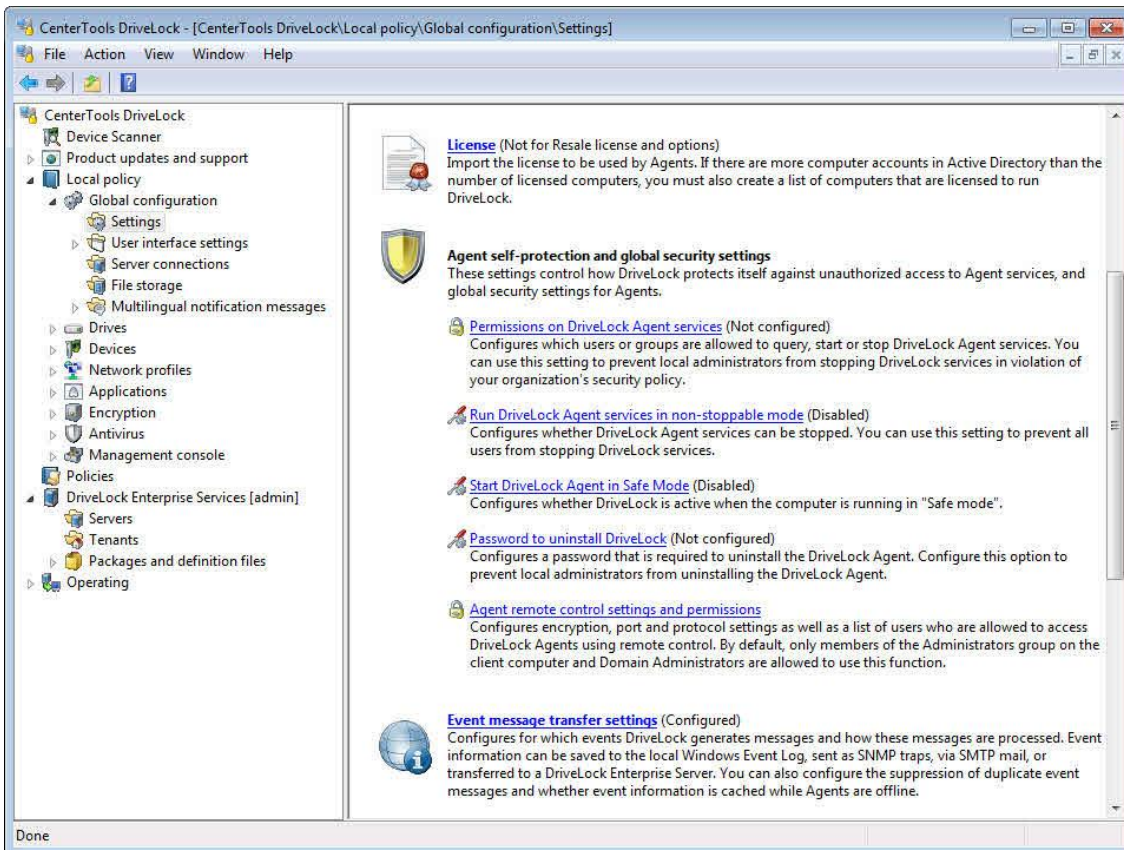
To enforce that communications are encrypted when you connect to an Agent by using Agent remote control, select “**Enforce secure communications (SSL)...**”.

Click **Finish** to save the settings.

The taskpad displays a summary of the settings you configured. Review the summary to confirm that all settings are configured as intended.

To quickly enable non-stoppable mode, in the task view, click **Turn on**. A confirmation that non-stoppable mode will be enforced is displayed.

6.4.2 Configuring Global Security Settings in Extended Configuration mode

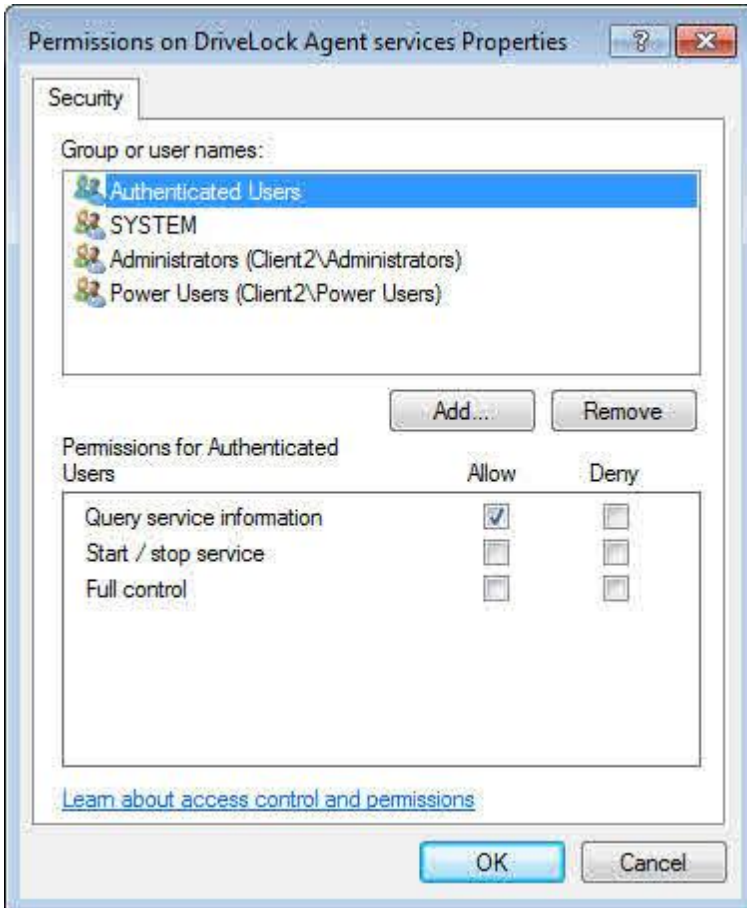


Click **Global configuration** and then **Settings**.

6.4.2.1 Permissions for the DriveLock Agent Service

Configure permissions for the DriveLock Agent service to control which users can access or stop the DriveLock service on client computers. For example, you could deny "Power Users" the permission to stop the service.

Click **Add** or **Remove** to add accounts to or remove accounts from the permissions list.



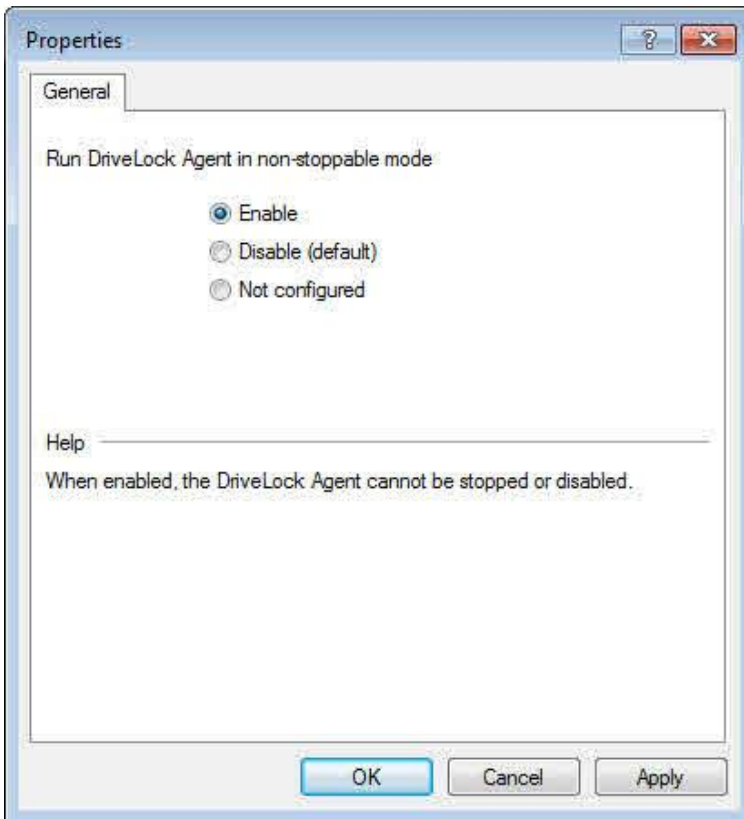
Select an account to configure the permissions assigned to it, and then select the Allow and Deny checkboxes to allow or deny the following permissions:

- Query service information (display the properties of the service)
- Start / stop service
- Full control

You cannot revoke the permissions of the local System account. If you attempt to do this, DriveLock automatically restores these permissions because they are required for DriveLock to function.

6.4.2.2 Locking Down the DriveLock Agent

To prevent all users from stopping the DriveLock Agent, click **Run DriveLock Agent services in non-stoppable mode**.

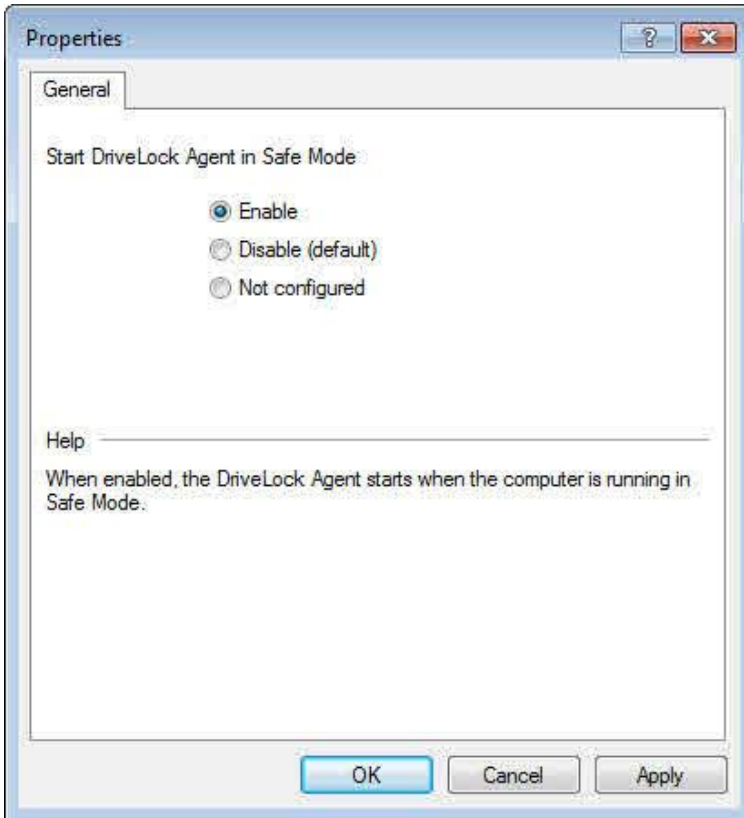


To activate the lockdown, select **Enable** and then click **Apply** or **OK**.

When you enable non-stoppable mode, no user can stop the DriveLock Agent, regardless of any permissions you may have configured. Also, uninstalling the DriveLock Agent is not possible while the non-stoppable mode is active.

6.4.2.3 Running DriveLock in Windows Safe Mode

Select the option **“Start DriveLock Agent in Safe Mode”** to start the DriveLock Agent when the client computer is running in Safe-Mode. When you select this option, users can’t bypass the restrictions in your policy by starting the computer in Safe Mode.

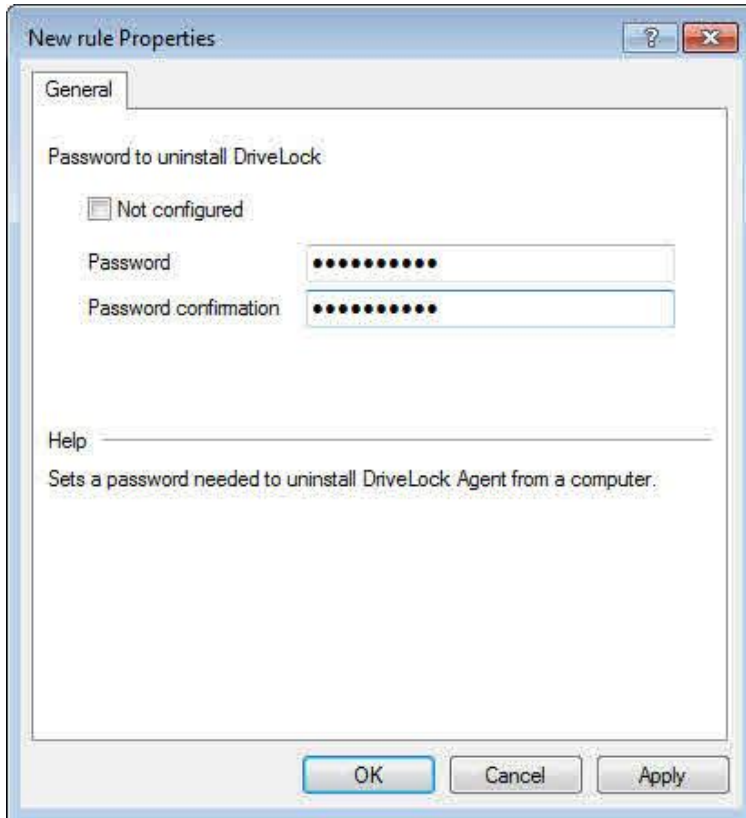


When using DriveLock in Safe Mode, you can no longer revert to previous configuration settings by booting into Safe Mode. This can complicate the process of restoring access to a client computer if DriveLock blocks devices that are required to use the computer because of a configuration errors.

6.4.2.4 Password to Uninstall DriveLock

To prevent users from uninstalling the DriveLock Agent when your company policy requires that DriveLock is installed and active, configure a password that must be provided when uninstalling DriveLock on a client computer.

To set the password, click **Password to uninstall DriveLock**.



When the password is set to **“Not configured”**, no password is required to uninstall the Agent.

To uninstall a DriveLock Agent when the password has been configured, use the following command at the Windows command prompt:

```
msiexec /x DriveLockAgent.msi UNINSTPWD= your password
```

The password for uninstalling only applies to the DriveLock Agent. You cannot prevent users from uninstalling of the Drivelock Management Console by requiring a password.

Before upgrading to a newer version of DriveLock, change the password for uninstalling to “Not configured” before updating DriveLock Agents in your network. Change the configuration again to require a password when the update has been completed.

6.4.2.5 Agent Remote Control Settings and Permissions

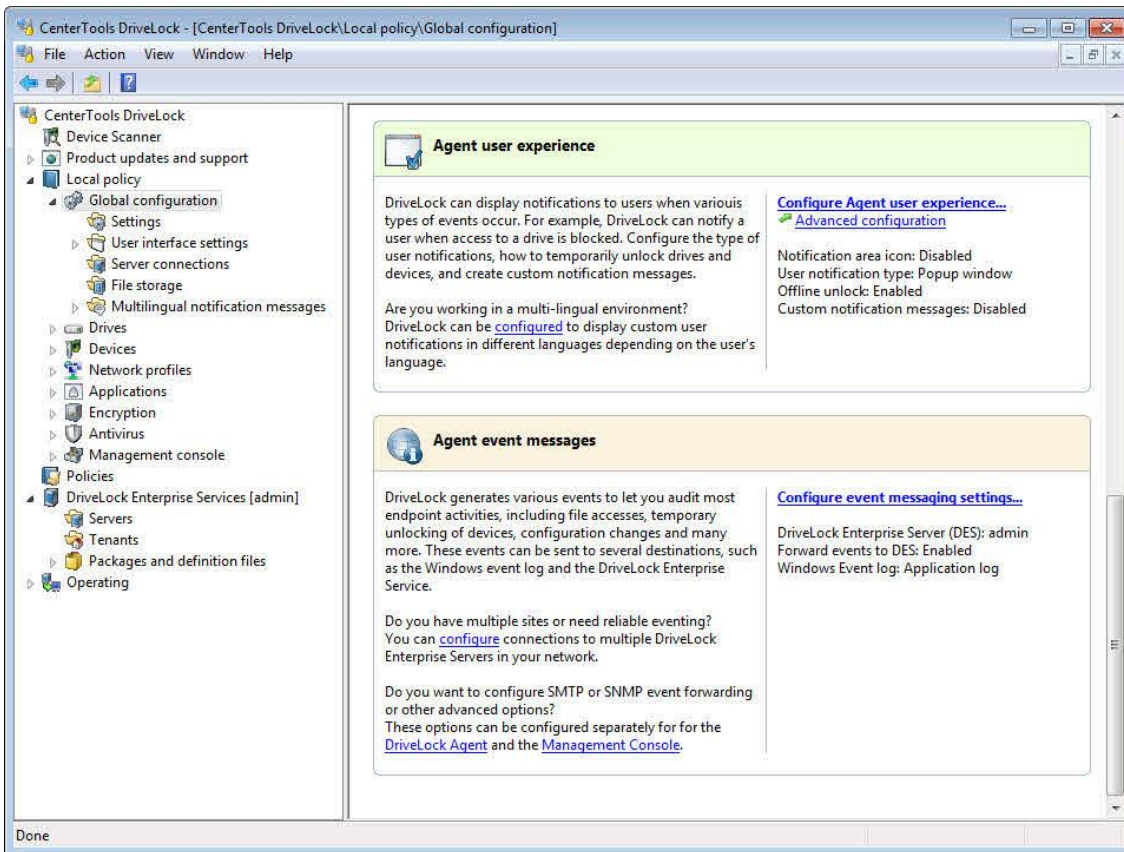
Please refer to chapter [Policy Settings for Agent Remote Control](#) for more information.

6.5 Configuring the Agent User Experience

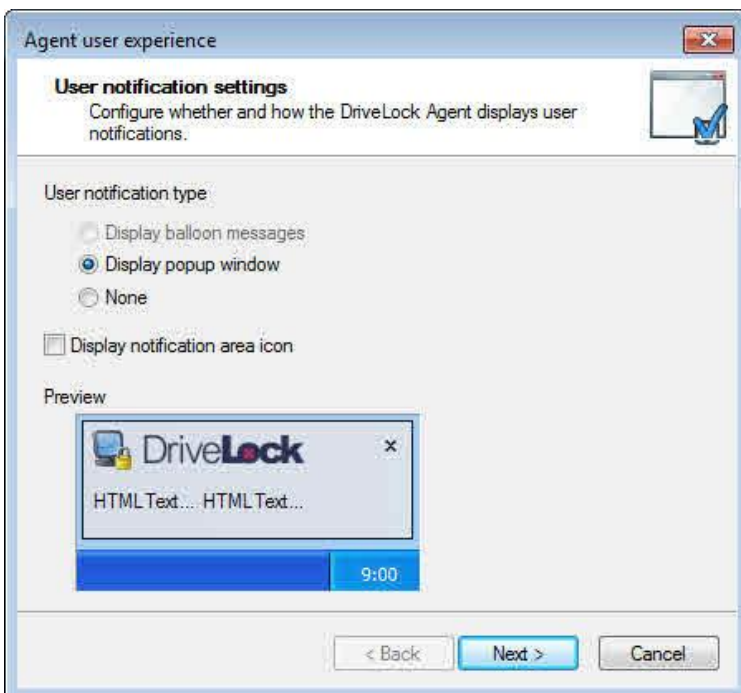
You can configure the appearance of DriveLock notification messages, whether DriveLock task bar icons and menu items are available to users and the language used for displaying notifications and menu items.

You can configure these settings easily in DriveLock Basic configuration mode. Some settings are not available in Basic configuration mode, but you can configure these settings or make more detailed configuration changes using the advanced settings.

6.5.1 Configuring the Agent User Experience in Basic Configuration mode



In the task view, click **Global configuration** and then click **Configure Agent user experience**.



You can configure DriveLock to display an icon in the taskbar notification area and to display notification messages to users when certain events occur. Global configuration settings control the style of these notification messages. Select how notification messages are displayed from the following two styles:

- Popup window:

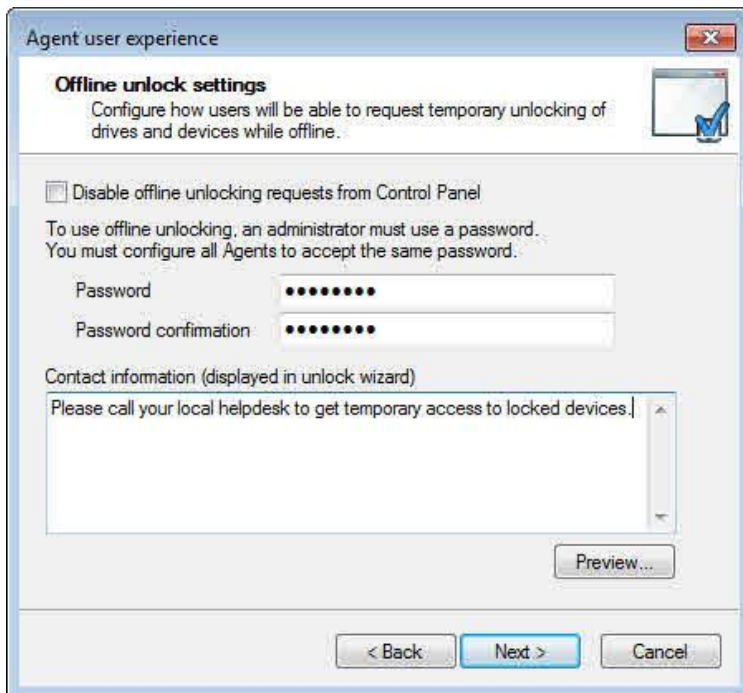


- Balloon message:



When using popup windows to display messages, you can use HTML tags in the message to format the text. When using balloon messages, the DriveLock icon is also displayed in the notification area. To display this icon even when no notification message is displayed, select the **“Display notification icon”** checkbox.

Click **Next** to continue.

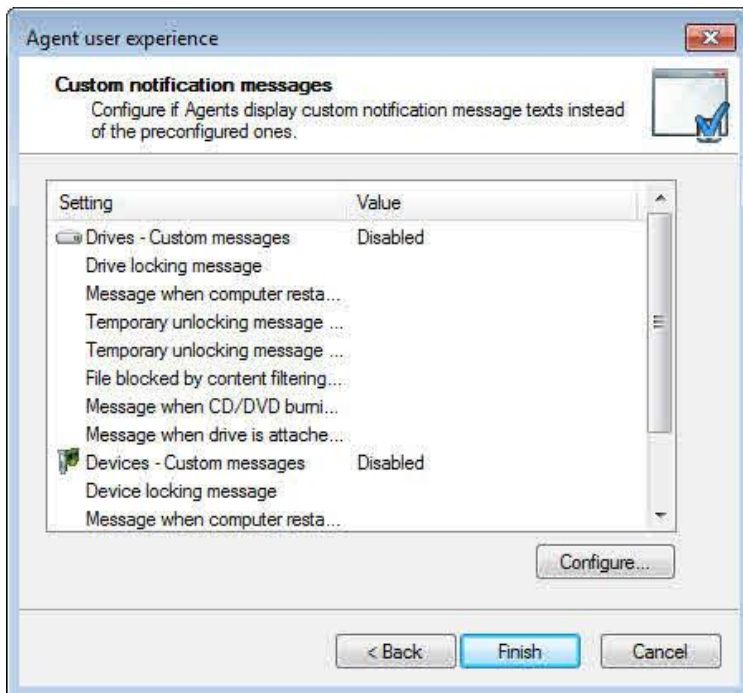


You can configure DriveLock to let administrators or helpdesk personnel temporarily unlock devices and removable drives even when the computer is not connected to a network (offline). To initiate offline unlocking, a user starts a wizard from the Windows Control Panel. Select the **“Disable offline unlocking requests from Control Panel”** checkbox to not display the offline unlocking applications in the Control Panel or the context menu of the DriveLock taskbar icon.

To prevent unauthorized unlocking of drives and devices, you should require administrators and helpdesk personnel to type a password before they can generate an unlock code. To set this password, type it twice.

To display contact information or other custom information in the wizard to help users obtain assistance with unlocking drives or devices, type this text.

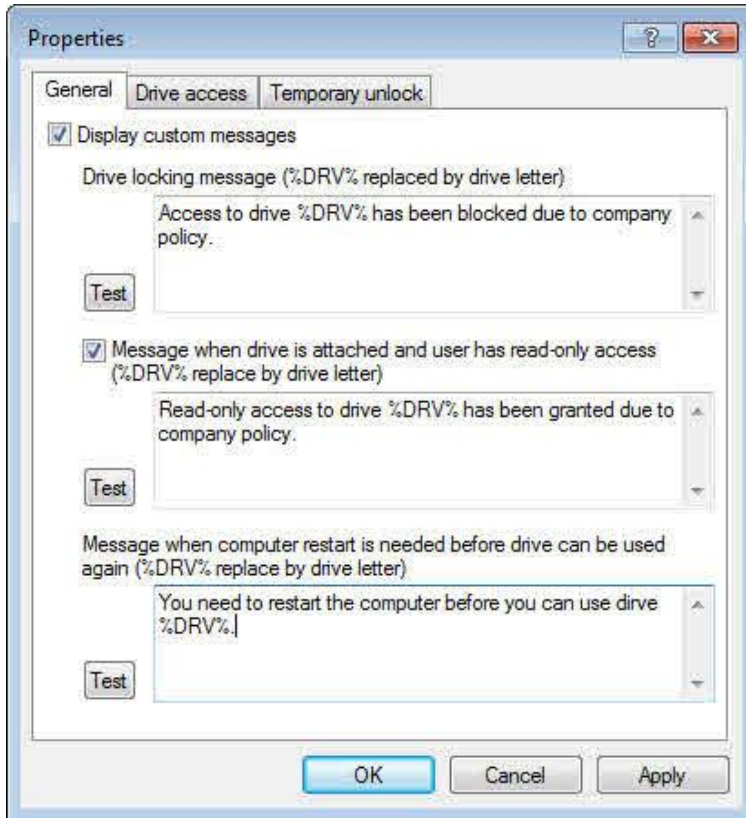
Click **Next** to proceed.



You can customize many of the user notification messages that DriveLock displays. When you configure a custom message, the DriveLock Agent displays it instead of the built-in message. There are three different types of messages:

1. Drive messages are displayed when DriveLock blocks drives, prevents CD/DVD burning, denies file access or unlocks access temporarily.
2. Device messages are displayed when DriveLock blocks devices.
3. Application messages are displayed when DriveLock prevents the start of an application.

To use custom drive messages, click **“Drives -> Custom messages”** and then click **Configure**.



To use custom messages when a user inserts a drive, select the **“Display custom messages”** checkbox. Type the text the DriveLock Agent displays when locking a drive. To refer to the drive letter, use the variable **“%DRV%”**, which will be replaced with the actual drive letter when the message is displayed.

Click **Test** to verify that the custom message appears correctly. DriveLock displays the message as it will appear to users.

Use the other sections of the General tab to configure custom messages that will be displayed to users when drive access is restricted to read-only and when Windows requires a computer restart before a newly inserted drive can be used.

Select the **Drive access** tab to configure custom messages for file access or locking of CD/DVD burners.

You can use the following variables in custom messages for drives:

- %DRV% is replaced with the drive letter.
- %PATH% is replaced with the file path.
- %NAME% is replaced with the file name.
- %EXT% is replaced with the file extension.
- %REASON% is replaced with the reason why a file was blocked.

Select the **Temporary unlock** tab to configure custom messages when a drive or device is temporarily unlocked by an administrator or helpdesk personnel, edit the default messages. To refer to the duration for which a drive or device has been unlocked, use the variable **“%TIME%”**, which will be replaced with the actual duration when the message is displayed.

Configure any other custom messages that you will use in your policy. After reviewing the settings, click **Finish** to close the wizard.

6.5.2 Configuring the Agent User Experience in Extended Configuration mode

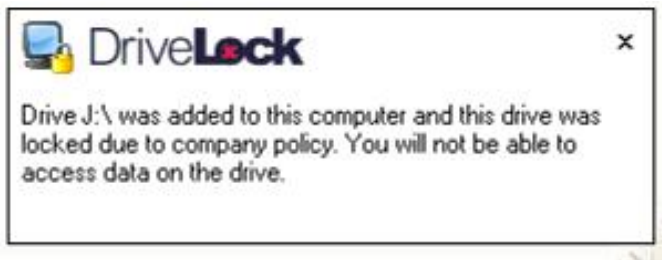
6.5.2.1 Taskbar notification area settings

You can configure DriveLock to display an icon in the taskbar notification area and to display notification messages to users when certain events occur. Global configuration settings control the style of these notification messages.

To open the Properties dialog box, under *Global settings* -> *User interface settings*, click **Taskbar notification area settings**

Select how notification messages are displayed from the following two styles:

- Popup window:



- Balloon message:



When using popup windows to display messages, you can use HTML tags in the message to format the text. When using balloon messages, the DriveLock icon is also displayed in the notification area. To display this icon even when no notification message is displayed, select the **“Display notification icon”** checkbox.

Use the **“Show messages for”** slider to configure the duration for which the message is displayed.

Select the **“Show balloon messages”** checkbox to display messages as balloon messages. To display balloon messages, you must also select the **“Show notification area icon”** checkbox.

To activate the DriveLock sound that it played when a DriveLock notification is displayed, select the **“Play sound when a message is displayed”** checkbox.

On the *Options* tab configure which items are displayed when you right-click the DriveLock taskbar icon and the order in which they appear.

To change the order of a menu item, select the item and then click **Up** or **Down**. To remove an element, click **Remove**. To add a divider, click **Add**. To restore the default settings, click **Restore**.

Setting tray icon context menu

Go to the *Options* tab to configure how the DriveLock features are displayed to the users in the tray icon context menu.

You can either show or disable the following elements:

- Temporarily unlock computers
- Stop temporary unlock
- (Change) user interface language

- (Start) self service unlock
- Submenu "DriveLock Encryption 2-Go"
- Submenu "DriveLock File Protection"
- About DriveLock

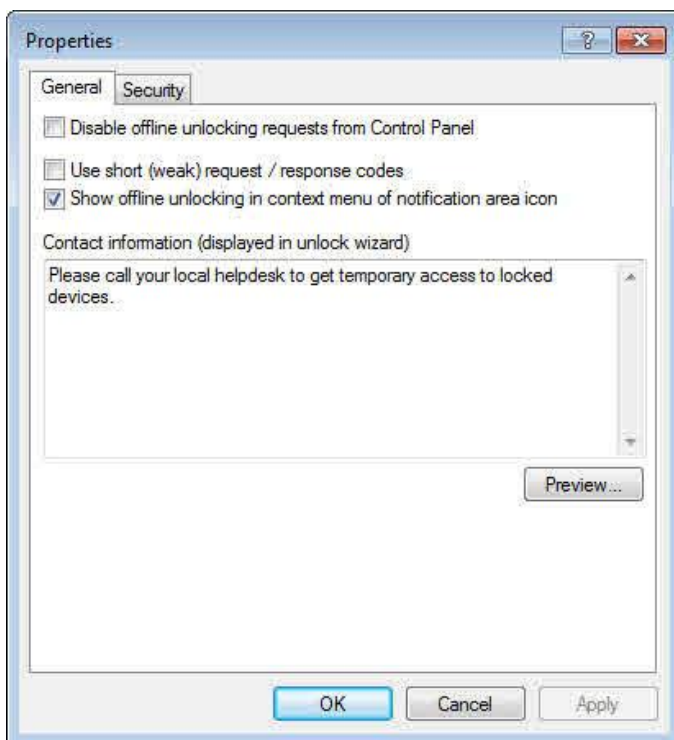
To change the order of the elements, select an element and click **Up** or **Down**. Click **Remove** to delete the selected element. If you want to add elements that are currently not visible, simply add a separator by clicking **Add** and then **---(Separator)**.

To reset the default settings, click **Reset**.

6.5.2.2 Offline Unlock Control Panel Settings

You can configure DriveLock to let administrators or helpdesk personnel temporarily unlock devices and removable drives even when the computer is not connected to a network (offline). To initiate offline unlocking, a user starts a wizard from the Windows Control Panel.

To configure offline unlock settings, under **Global settings -> User interface settings**, click **Offline unlock control panel settings**.



Select the **"Disable offline unlocking requests from Control Panel"** checkbox to not display the offline unlocking applications in the Control Panel or the context menu of the DriveLock taskbar icon. To display contact information or other custom information in the wizard to help users obtain assistance with unlocking drives or devices, type this text.

To simplify the unlocking process for users and helpdesk personnel you can select the **Use short (weak) request / response codes** checkbox.

Using shorter challenge / response codes makes the unlocking process less secure.

Click the **Security** tab to configure whether administrator or helpdesk personnel who create unlock codes that are authenticated using a password or a certificate. If you require a certificate, the certificate and private key must be in the local certificate store of the user who generates the unlock code.

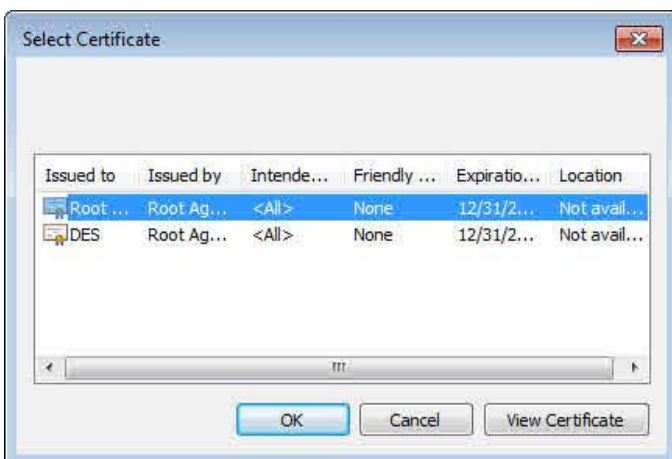


To use password authentication, select **Use password**, type the password twice and then click **OK**.

To use a certificate for authentication you must specify this certificate.

You can import the certificate from a file or use a certificate from the Windows certificate store on the local computer. To import a certificate from a file, click **Import from file** and then select the certificate file.

To use a certificate from the certificate store, click **Import from store**.



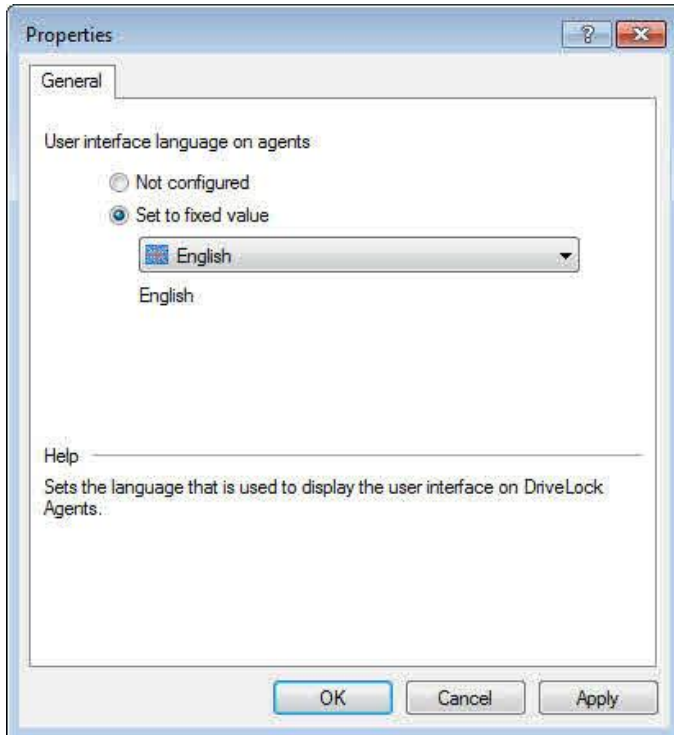
Select the certificate and then click **OK**.

If you use a certificate to authenticate the offline unlocking, you need to provide the certificate's private key each time you create an offline unlocking code.

6.5.2.3 User Interface Language on Agents

You can configure the language that the DriveLock Agent uses to display encryption related-menus and other user interface elements. This option only applies if you have activated DriveLock encryption on the Agent.

If you select **“Not configured”** the Agent uses the default language configured in Windows or the language configured for the current user.



6.6 Connecting to the DriveLock Enterprise Service

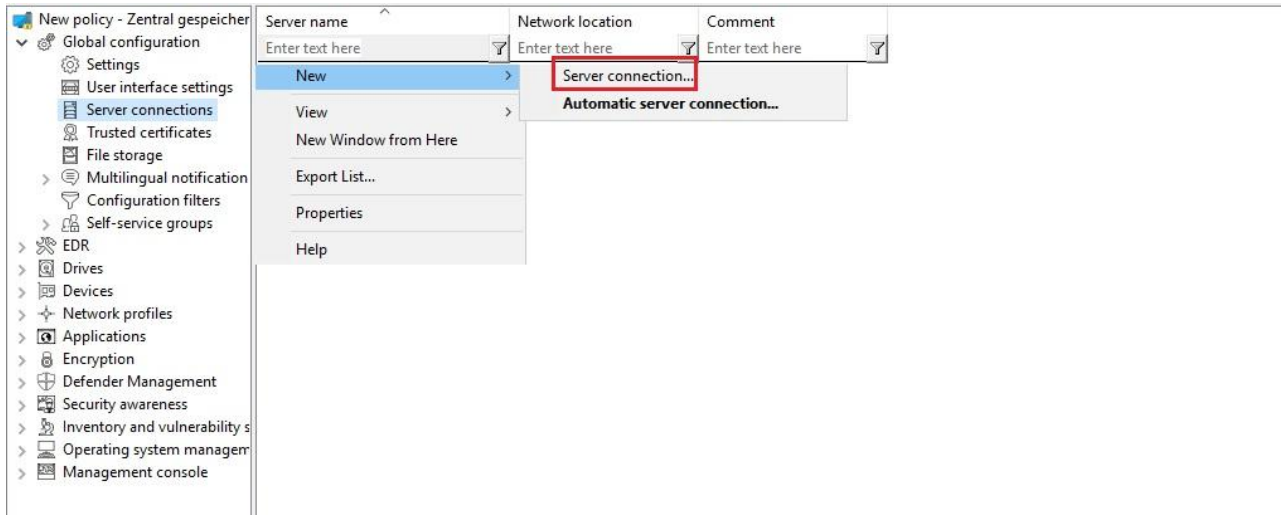
The DriveLock Enterprise Service (DES) is the DriveLock component that performs all centralized functions. It performs the following tasks:

- It receives event messages from the DriveLock Agents and adds them to the DriveLock database.
- It stores files in the DriveLock database, such as files that are required for password and disk recovery functions.
- It receives “Agent alive” messages from Agents and stores them in the DriveLock database. It also provides the status of Agents to the DriveLock Management Console to enable monitoring of DriveLock Agents.
- It can store information about licensed computers in the DriveLock database.
- It can automatically download software updates (optional).

You can install the DriveLock Enterprise Service on one or more servers in your network, but you can use only one central database. To enable the DriveLock Management Console and the DriveLock Agents to connect to the DES, you must configure at least one DES connection. You must also configure how data is sent and retrieved as described in this section.

6.6.1 Configuring DriveLock Enterprise Service Connections

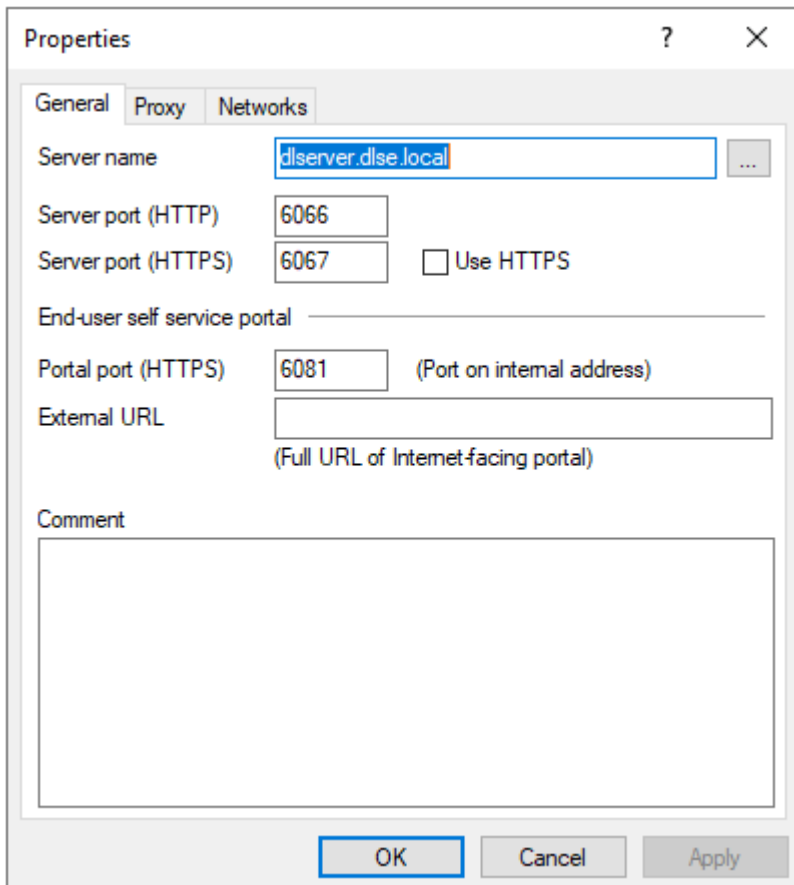
Large networks may contain more than one server running the DES, for example to ensure DES availability in branch offices or to manage network DES-related network traffic. To enable DriveLock Agents and the Management Console to connect to the DES in such an environment, you may need to define more than one DES connection.



To manage connections to DES servers, under *Global configuration*, click **Server connections**.

Quick Configuration: If no server connections are defined or an automatic server connection exists, DriveLock Agents discover a DES server automatically using mDNS/DNS-SD.

To create a server connection, right-click **Server connections** and then click **New -> Server connection**.



Type the name of the server where you installed the DES. If you changed the default ports used by the server, specify the port numbers. By default, the DES uses TCP port 6066 to receive event messages from Agents. The default ports for connections from the Management Console to retrieve data and display reports are TCP port 6066 for unencrypted connections and TCP port 6067 for encrypted connections. If clients need to connect to the DES server by using a proxy server, select the corresponding tab. See [Proxy Server](#) for more information.

To enforce the use of encrypted connections to the DES, select the “Use HTTPS” checkbox. DriveLock will automatically create an SSL certificate that will be used to encrypt communications with the DES.

Before you select the option “Use HTTPS” you must configure additional settings for the DriveLock Enterprise Service (DES) to ensure that the DriveLock Agent can communicate with the DES.

Select the **Networks** tab to configure the network locations where the DES connection will be used.

Select from the following options:

- To use this connection in any network location, select “*Used for any network connection*”. This is the default.
- To select a previously defined network connection, click “*Used in selected network location*” and then select an entry from the list.

You cannot select a specific network location for sending DriveLock Management Console events.

- To use this connection when a computer is located in an Active Directory site click “**Used in Active Directory site**” and then click the “...” button select an Active Directory site. This is the easiest method to configure separate connections for different AD sites.
- To use this connection when the computer is not in any defined network location, click “**Used in locations where no dedicated server is defined**”.

Click **OK** to apply all settings and close the dialog box.

6.6.2 Proxy Server

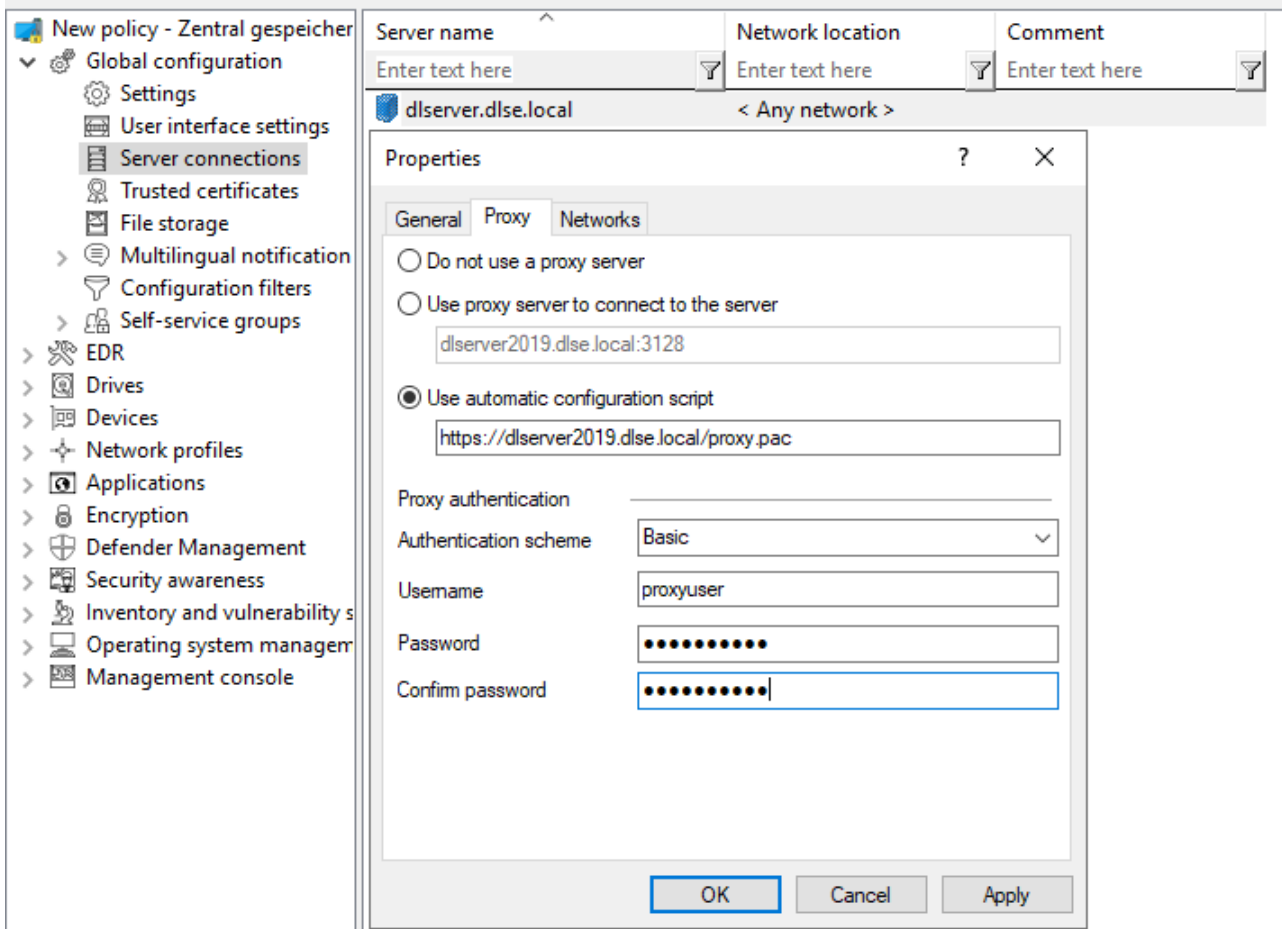
You can specify a proxy server in the DES connection settings. It is possible to specify a different proxy for each server.

To add a proxy, right-click **Server connections** and then select **New: Server connection**.

Then choose the **Use proxy server to connect to the server** option on the **Proxy** tab and specify the appropriate server.

Alternatively, you can also **use an automatic configuration script** (*.pac file). Specify the URL as required here.

If necessary, enter the **authentication scheme**, a **user name** and **password**.



Once you specify a proxy server in the policy, the settings set by the MSI are no longer used.

6.6.2.1 Proxy Settings on the Agent

You can also set the proxy server settings directly on the agent. The following two command line commands are used for this purpose

- `drivelock -setproxy <proxytype>;<proxy>` and
- `drivelock -setproxyaccount <authscheme>;<proxyuser>;>proxypassword>`

<proxytype> specifies the proxy type and can be named, pac, none or netsh

<proxy> contains either the proxy or the URL for the proxy auto configuration file.

Examples:

```
drivelock -setproxy name;myproxy:myport
```

```
drivelock -setproxy pac;//myhttpserver/myproxy.pac
```

```
drivelock -setproxy none
```

```
drivelock -setproxy netsh
```

If the proxy requires authentication, you can set the user and password with the `drivelock -setproxyaccount <authscheme>;<proxyuser>;>proxypassword>` command. Here, <authscheme> is used to specify the authentication scheme (basic, ntlm, passport, digest und negotiate).

These settings are stored in the registry in the registry key
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\DriveLock\Parameters.

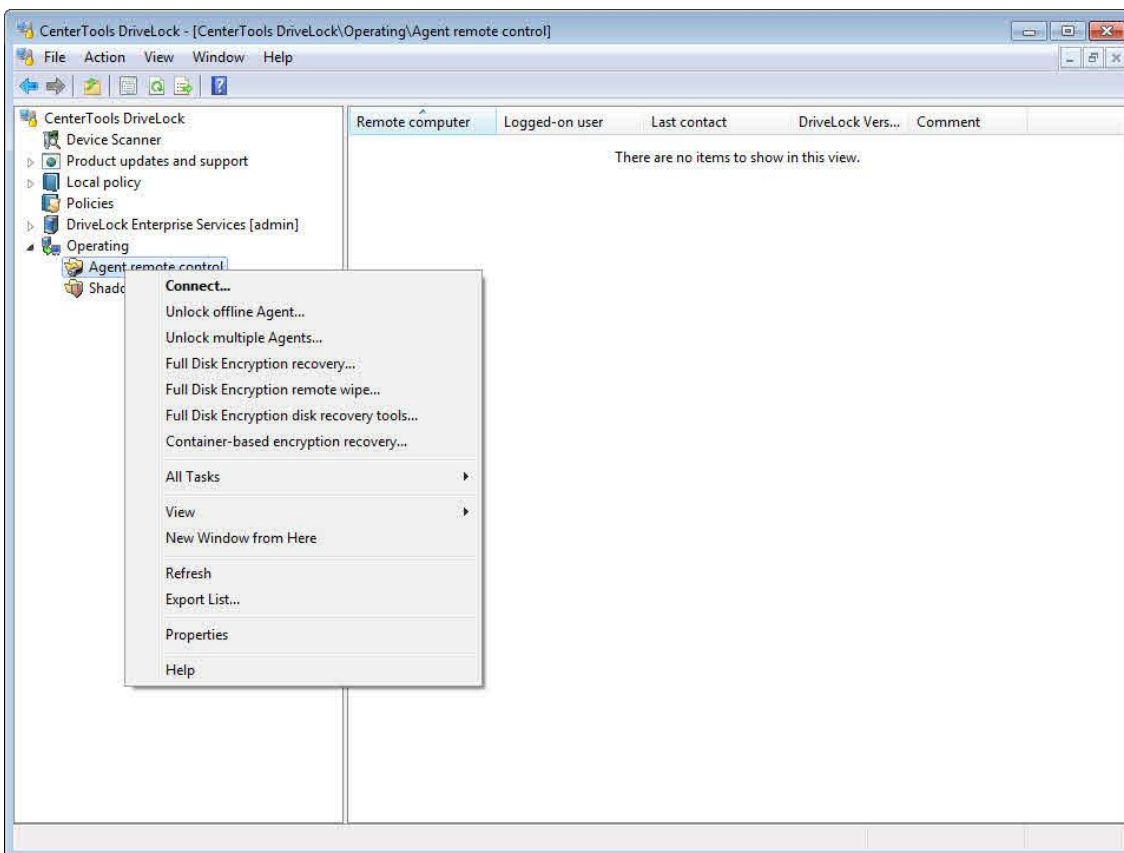
They are evaluated with priority, so if a proxy is set with the `drivelock -setproxy` command, all other settings are ignored.

You can delete proxy settings that were specified when running the MSI (please refer to the Installation Guide for details) or set with the `drivelock -setproxy` command with the `drivelock -removeproxy` command.

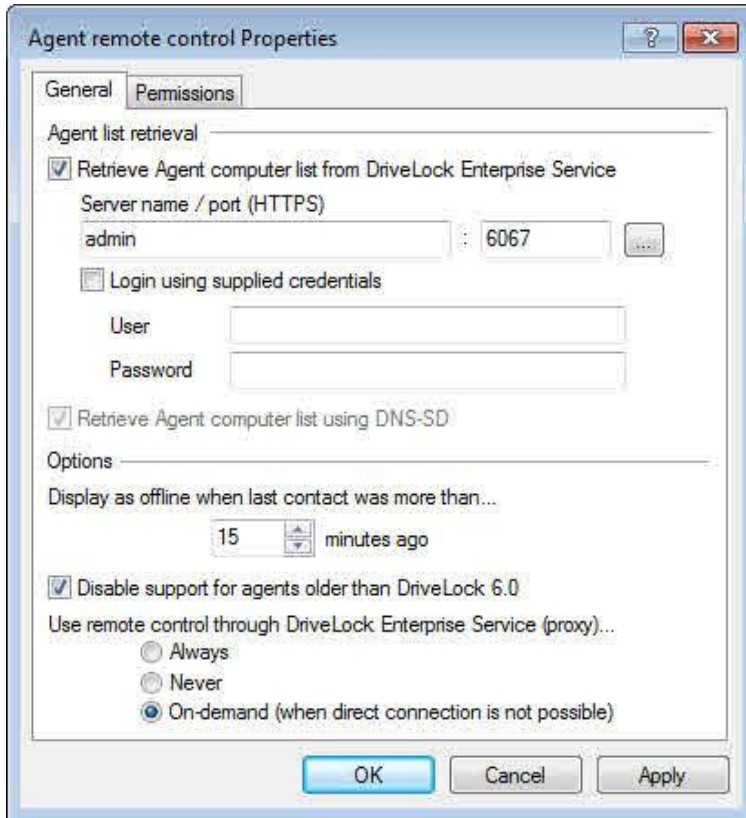
6.6.3 Monitoring Agents by Using the DriveLock Enterprise Service

6.6.3.1 Agent Monitoring Using the DriveLock Management Console

If you use the DriveLock Enterprise Service (DES), you can view the status of DriveLock Agents in the DriveLock Management Console.



To configure the Management Console to retrieve a list of Agents from the DES, right-click **Agent remote control** and then click **Properties**.



Select the **“Retrieve client computer list from DriveLock Enterprise Service”** checkbox and then select a server connection. To connect using a different user account than the one you are currently logged on with, provide the credentials of that account.

Configure the option **“Display as offline when last contact is more than... minutes ago”** to define an interval after which a DriveLock Agent is displayed as “offline” if it has not sent its status to the DES.

When viewing the Agent status in the Management Console, agents that are offline are identified by an icon containing red square.

If all DriveLock Agents in your network are running DriveLock 6.0 or newer, select the *Disable support for agents older than DriveLock 6.0* checkbox. This will deactivate the use of all ports that are no longer used in current versions of DriveLock.

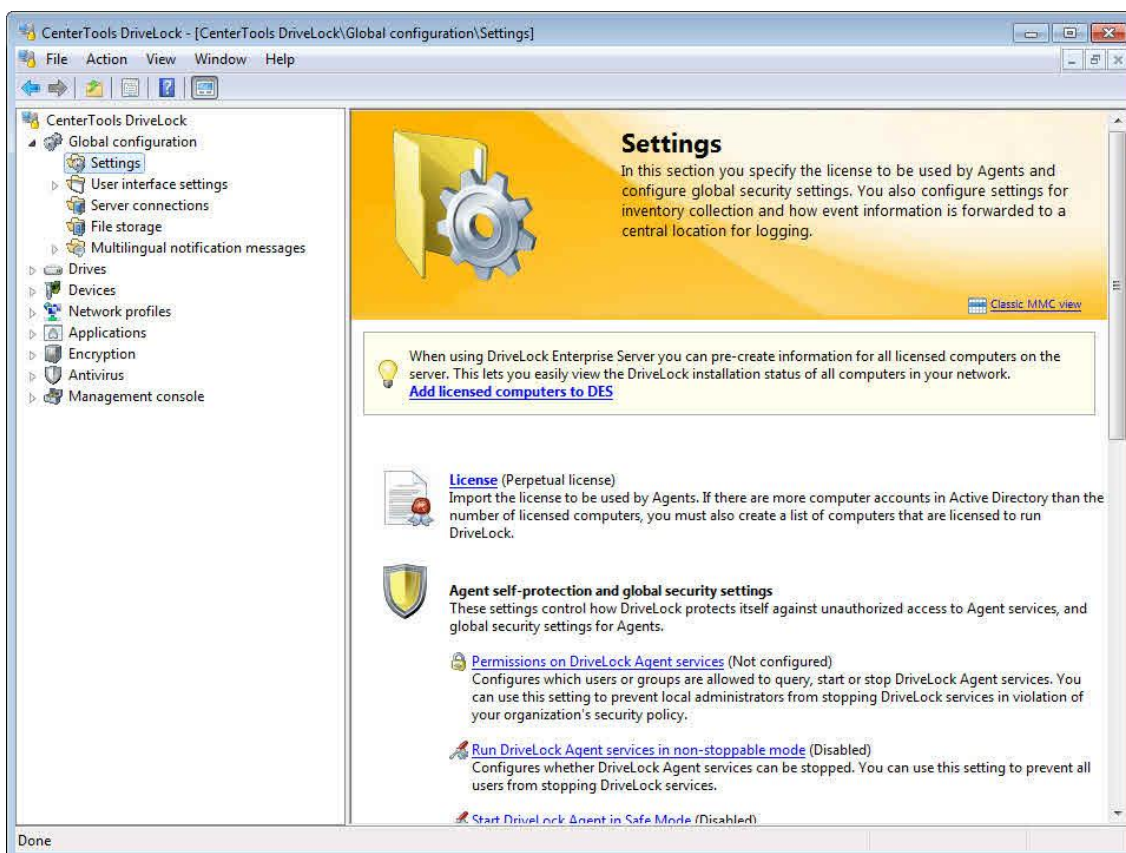
In environments where the DriveLock Management Console is run on a computer that is not in the same network as the Agent, the DriveLock Enterprise Service can proxy this connection. For example, this can be used by a Security-As-A-Service provider to connect to an Agent in a customer’s network. Change the setting *Use remote control through DriveLock Enterprise Service (proxy)* to configure how the DriveLock Management Console connects to the client for remote control:

- *Always*: The connection is always established via the DriveLock Enterprise Service.
- *Never*: The DriveLock Management Console always connects directly to the Agent without going through the DriveLock Enterprise Service.
- *On-demand*: The DriveLock Management Console attempts to connect directly to the Agent. If the connection attempt fails, a connection via the DriveLock Enterprise Service is attempted.

6.6.3.2 Sending Licensed Computer Information to the DES

You can view additional information about the status of DriveLock Agents by using the DriveLock Control Center. Status messages that Agents send to the DES contain information about which DriveLock components the computer is licensed to run. To include additional computers in your network that are licensed to run DriveLock but currently don't have the DriveLock Agent installed in reports, you must manually add these computers to the DriveLock database. Once the database contains all licensed computers, you can easily identify computers that are not protected by DriveLock because no Agent is installed. To add computers to the database, you use the DriveLock Management Console.

Before continuing, ensure that you have configured a valid DES connection for the DriveLock Management Console and that you have completed the steps for retrieving a list of clients from the DES that are described in the section “[Agent Monitoring using the DriveLock Management Console](#)”.



In the console tree, under **Global configuration**, click **Settings**. In the task pane, click **Add licensed computers to DES**. The DriveLock Management Console sends a list of all licensed computers to the DES using the currently active DES connection.

If you specified that only some of the computers in Active Directory are licensed to run DriveLock, the Management Console transmits the list of these computers to the DES. Otherwise, it sends a list of all computers in Active Directory to the DES.

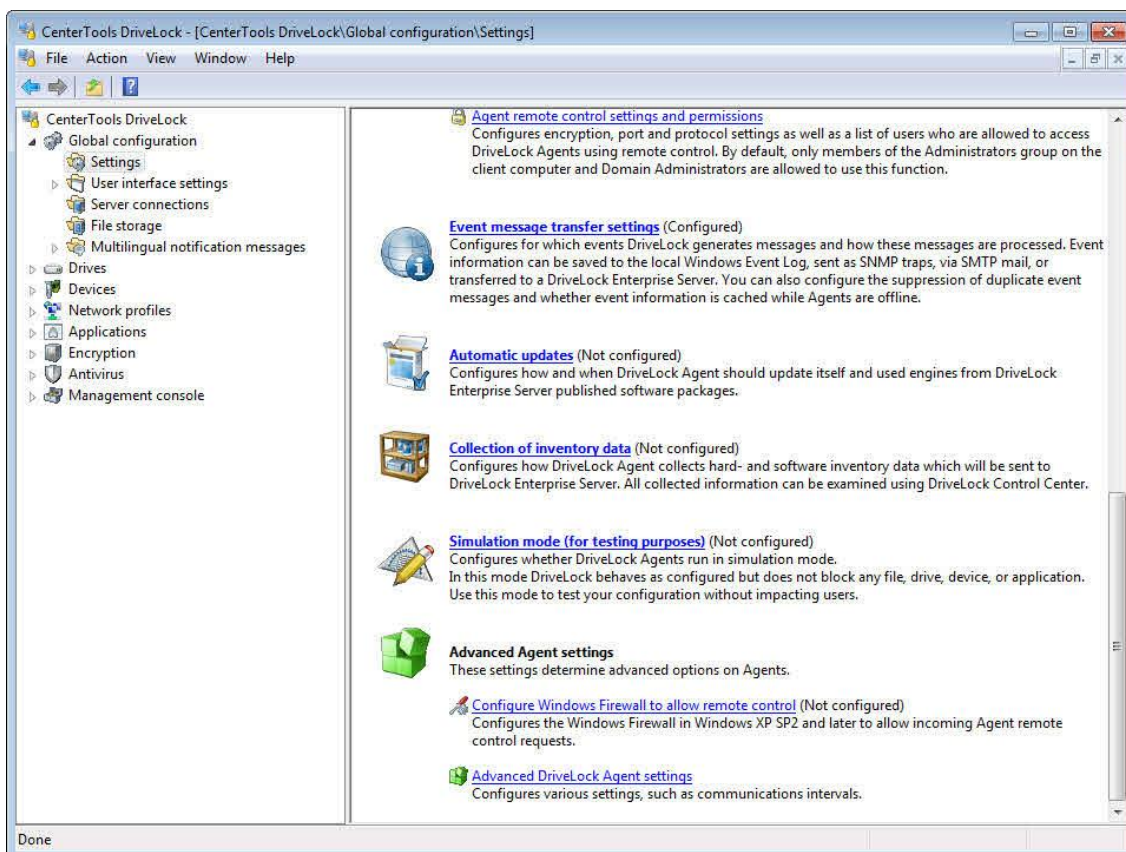
For more information about using the DriveLock Control Center to monitor clients, refer to the *DriveLock Control Center User Guide*.

6.7 Configuring the DriveLock Simulation Mode

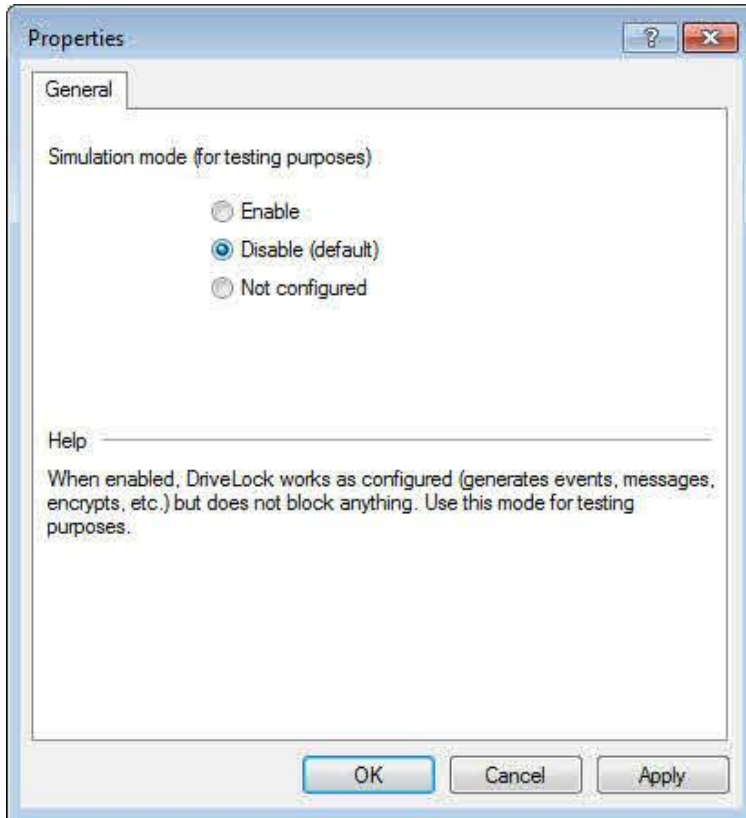
The DriveLock Simulation Mode allows you to configure and deploy a policy without impacting users. In Simulation Mode you can monitor all DriveLock operations but the Agent does not block drives, devices or applications. You typically use Simulation Mode after you have configured the initial DriveLock policy. After you apply this policy to computers in Simulation Mode you can review events and talk to users to identify instances where policy settings are not correctly applied. For example, you may find that the policy blocks access to a removable drive that a user needs to use. If you identify such problems, you can easily correct them before users are impacted. Once you determine that the policy works as intended, you can de-activate the Simulation Mode and DriveLock will enforce all policy settings.

When Simulation Mode is enabled, DriveLock functions as follows:

- DriveLock doesn't block removable drives, devices, applications and network connections.
- File filtering is disabled.
- Events are generated normally and are sent to the Windows event log and to external systems according to the policy settings.
- User notification messages are displayed as configured in the policy.
- Enforced encryption is enabled; unencrypted drives are encrypted as configured in the policy.
- All other functions work normally.



To configure DriveLock Simulation Mode, click **Settings**, scroll down and then click **Simulation mode (...)**.



By default, DriveLock Simulation Mode is disabled.

Select **Enable** to activate DriveLock Simulation Mode.

Click **OK** to apply the changes.

6.8 Trusted Certificates

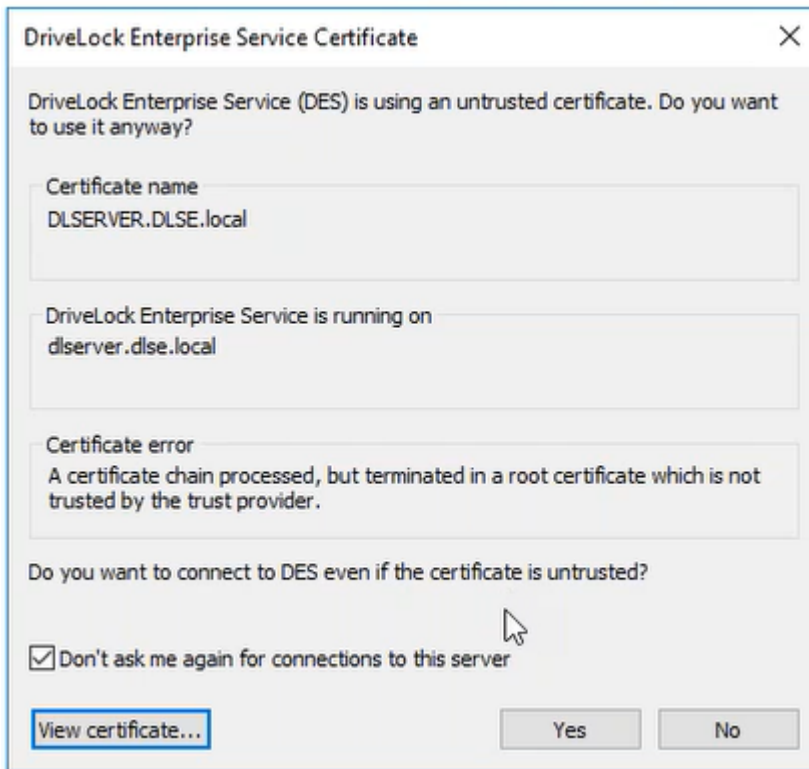
DriveLock Version 2019.1 introduces the use of trusted certificates to ensure secure communication between the DriveLock Management Console or DriveLock Agents and the DES. You can specify these certificates in the **Global configuration** of a policy.

6.8.1 Checking trusted certificates in the Management Console

The first time you open the DriveLock Management Console after updating to version 2019.1, DriveLock checks the SSL certificate that you created during the installation of the DriveLock Enterprise Service (DES).

If Windows categorizes the certificate as not trustworthy or if the certificate is invalid, the following message appears first (see figure).

Please note that Windows initially does not consider self-signed certificates trustworthy because it cannot verify the root certificate.



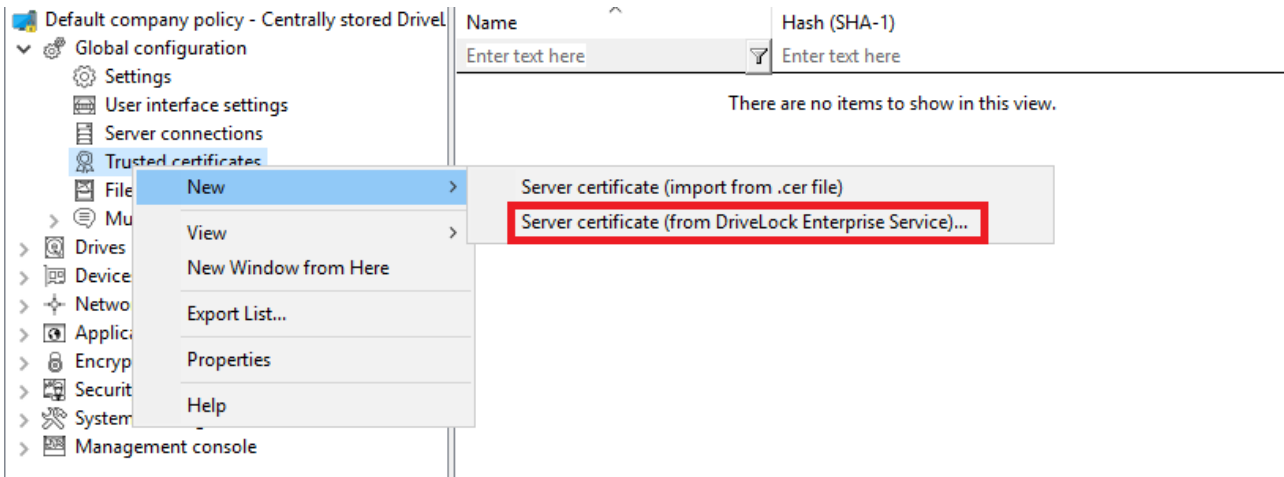
You can view the certificate and verify that it is actually the certificate the DES uses before you accept its use. In this case, DriveLock writes a corresponding entry in the registry under `HKEY_CURRENT_USER/SOFTWARE/CenterTools/DriveLock/MMC`. The message no longer appears because the certificate has been entered.

6.8.2 Selecting trusted certificates

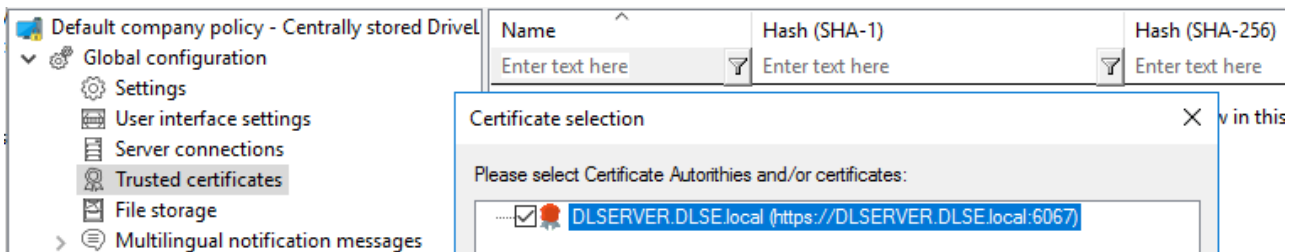
We recommend that you use this setting to increase the security requirements for communication between DriveLock Agent and DES. If you do not specify certificates, DriveLock cannot ensure that the Agent will communicate with the correct DES.

Option 1: Server certificate (from DriveLock Enterprise Service):

You can select the certificate the DES (or linked DES) uses (see figure below). This is the server certificate you created when setting up the DES with the *Create self-signed certificate* option.

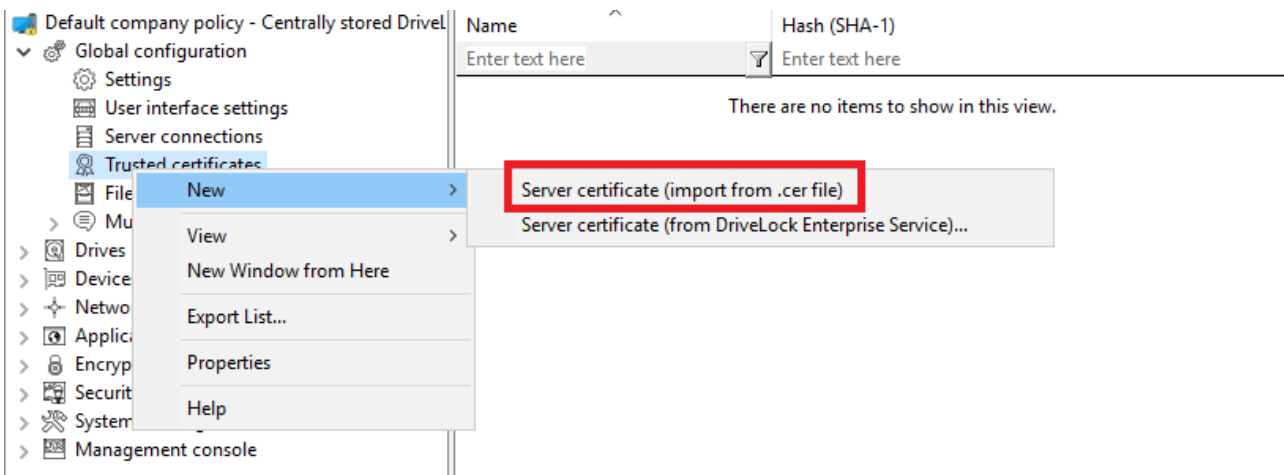


Next, select the DES (or linked DES) certificates the Agent(s) will communicate with (in the example below this is DLSERVER.DLSE.local...):



Option 2: Server certificate (import from .cer file):

If you want to import *an existing server certificate* for communication, you can select it here and use it in the policy:



Next, select the certificate in the Explorer.

With option 2 you can also import the Root CA certificate. In this case, the DriveLock Agents will trust all certificates with this Root CA. If your DES certificates all have the same Root CA, you don't have to list them individually.

The list of trusted certificates now displays the information about the certificate (SHA-1 and SHA-256). *Note: The hash SHA-1 is now only used for XP.*

The DriveLock Agents you assign your policy to will then trust this server certificate and only communicate with the trustworthy servers.

Starting with DriveLock version 2019.2 you can find the ChangeDesCert.exe tool in the DES program directory at C:\Program Files\CenterTools\DriveLock Enterprise Service\ChangeDesCert.exe. Note that if you want to exchange an existing DES server certificate using ChangeDesCert.exe, you must import the new certificate into the computer's Certificate Store and configure the private key as exportable.

Important notes:

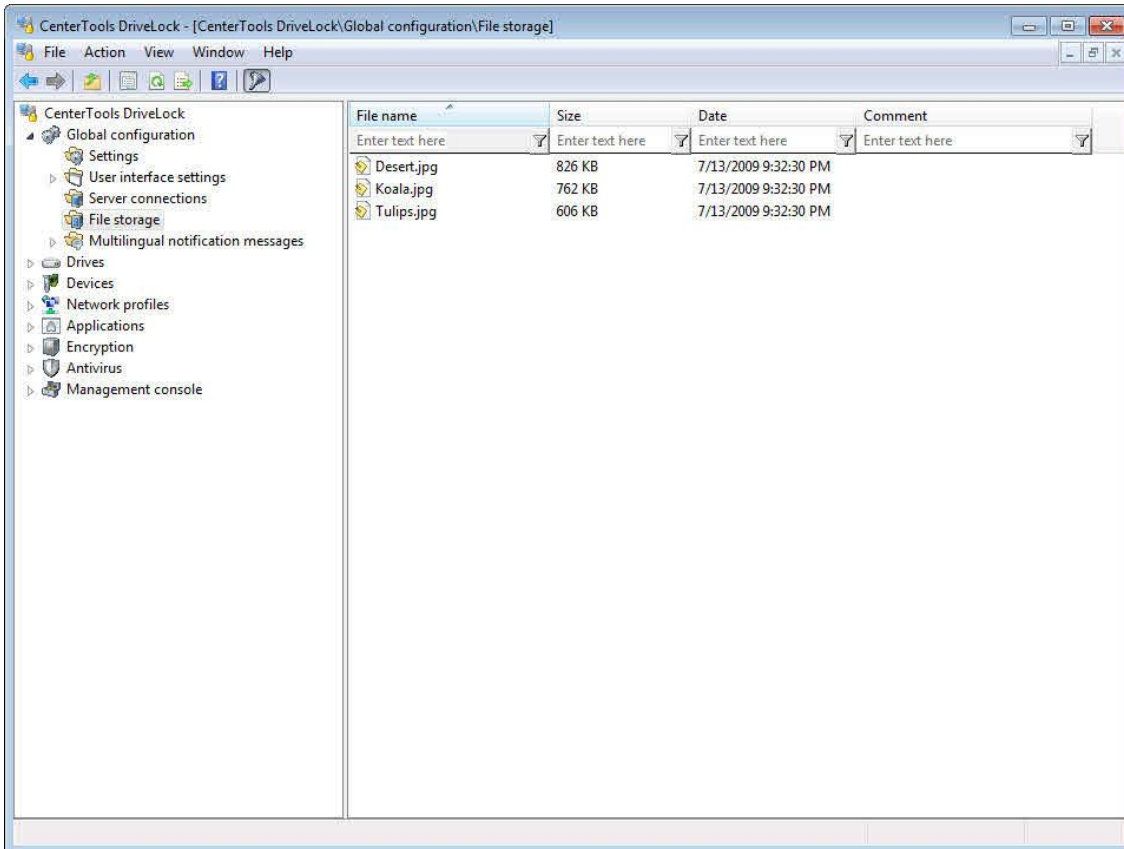
- Make sure to keep your certificates up to date at all times. If you need to replace the DES certificate or install additional linked DES, please add the new certificates to the list in time and make sure the DriveLock Agents are assigned this policy before communicating with the DES (or the new linked DES).
- As long as a DriveLock Agent has not yet succeeded in finding the DES certificate in the list of trusted certificates, it accepts connections to any DES. Once the certificate has been successfully verified, the Agent only communicates with the DES whose hash values match the list of trusted certificates.
- If you remove all certificates from this list, the Agents will communicate again with all DES.

An error message appears on the DriveLock Agent when it receives an invalid certificate and the communication between the DES and the Agent is no longer possible! In this case, the only solution is to edit the local registry of the Agent manually. Please contact DriveLock Support for further information.

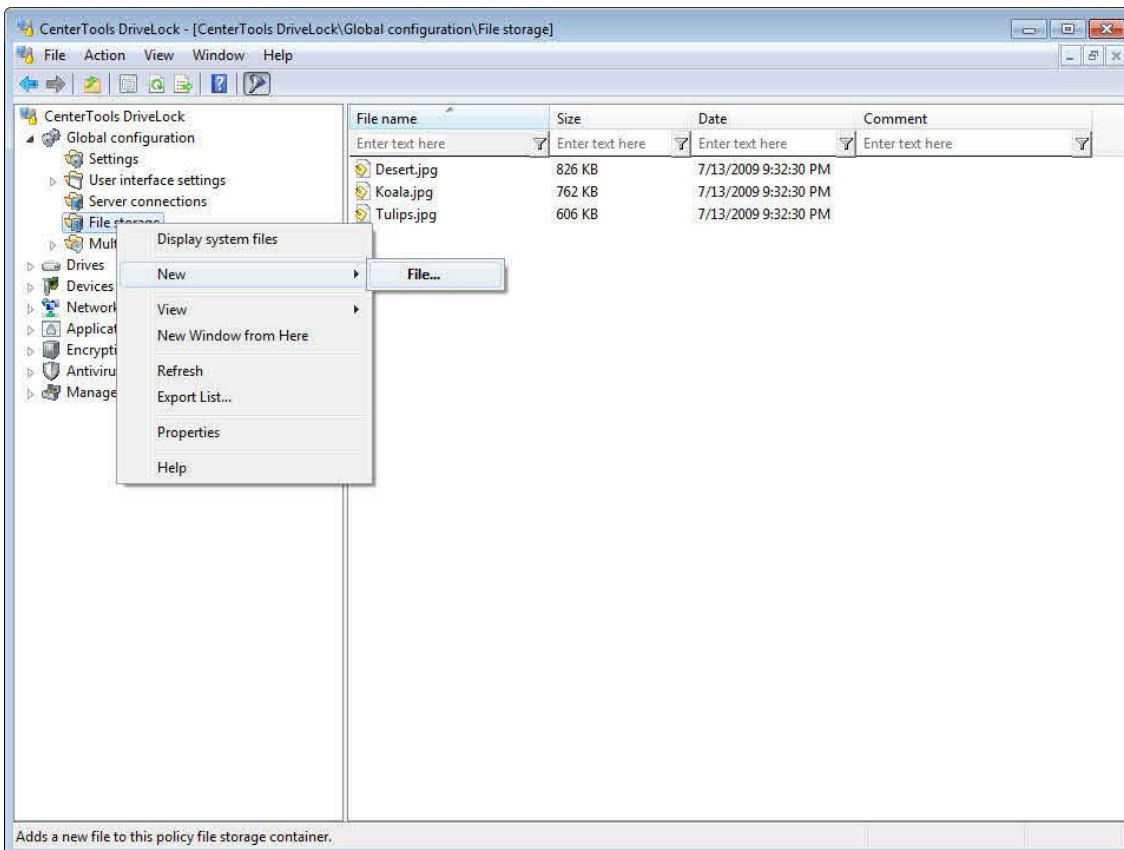
6.9 Using the DriveLock Policy File Storage

The DriveLock Policy File Storage is a protected storage area that is stored with a DriveLock configuration and distributed to Agents. The purpose of this storage is to store files that are needed to run programs that may be configured in various DriveLock rules, such as scripts and dictionary files. Using the Policy File Storage makes it easy to deploy scripts or programs that are used by the DriveLock Agent to client computers. After you import files into the storage they will be automatically delivered to the Agent together with the corresponding configuration settings. You can use the Policy File Storage in policies that are distributed using a configuration file or Group Policy.

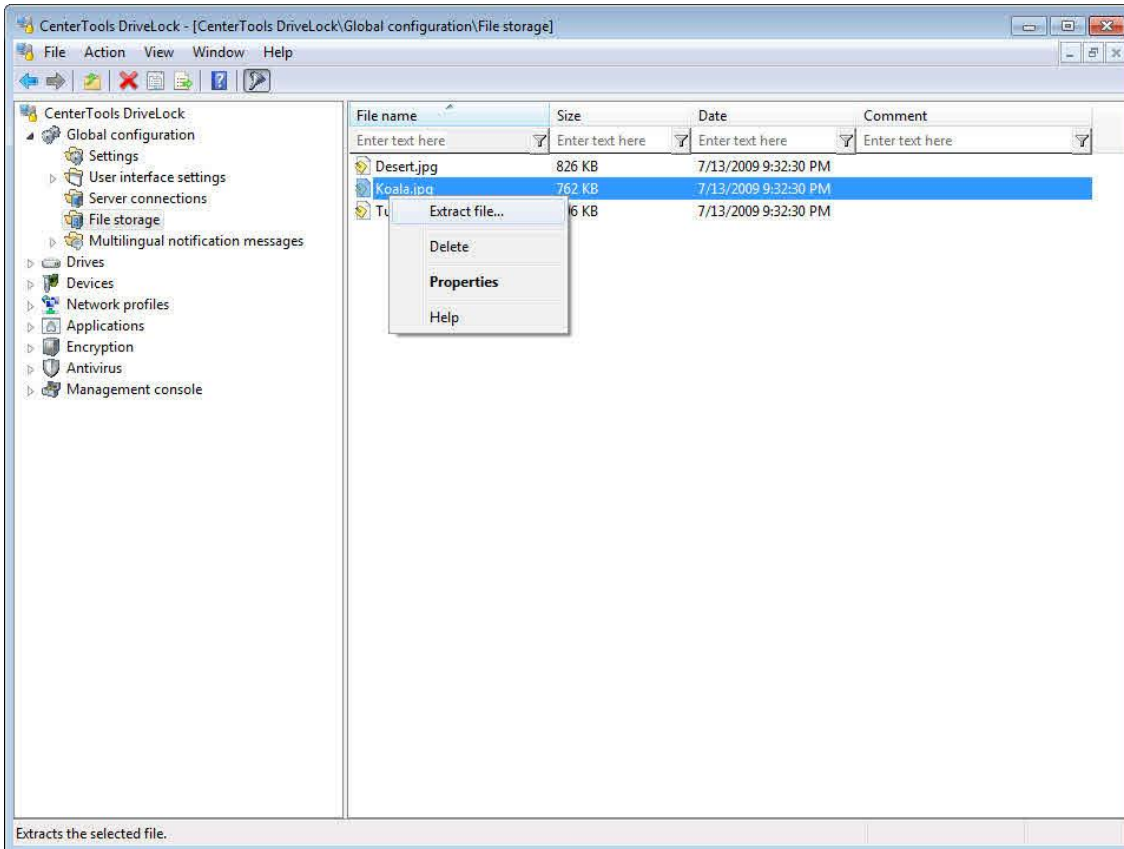
Importing large files into the Policy File Storage can increase network traffic and logon times as the client computer retrieves these files when Group Policy settings are applied to a client computer and the Policy File Storage has not been loaded previously or has changed.



Click **File storage** to see the list of all the files included in your Policy File Storage.

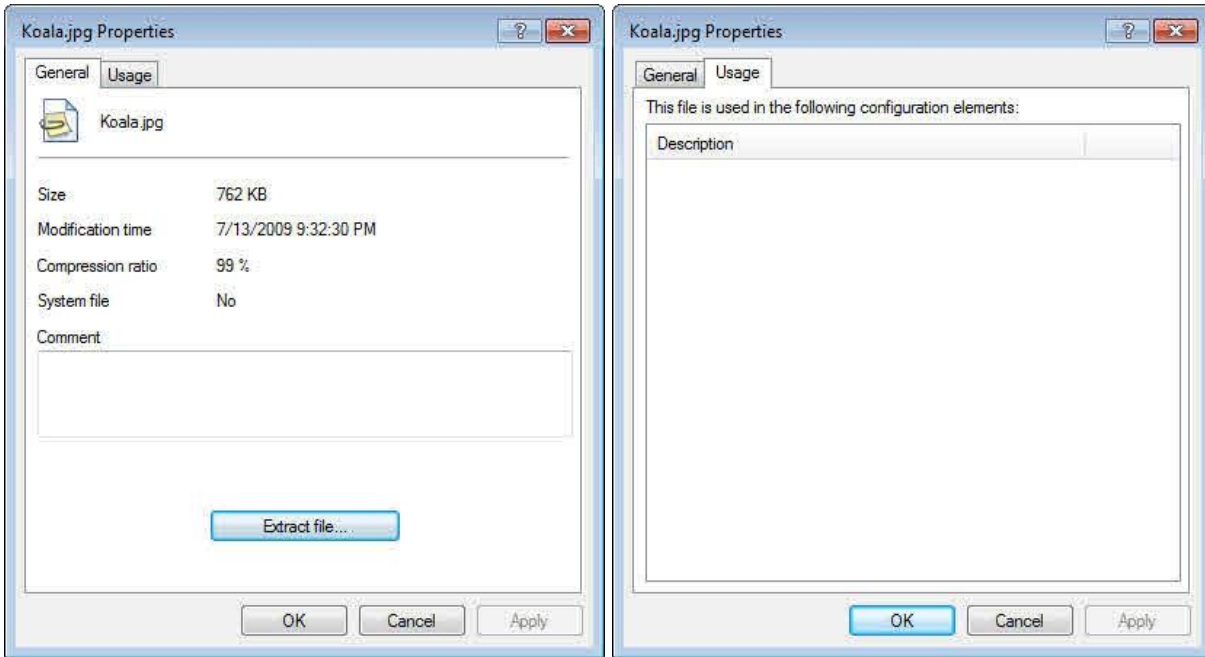


Right-click **File storage** and then click **New -> File** to import a file into the Policy file storage. Navigate to the directory containing the file to import and then select the file.



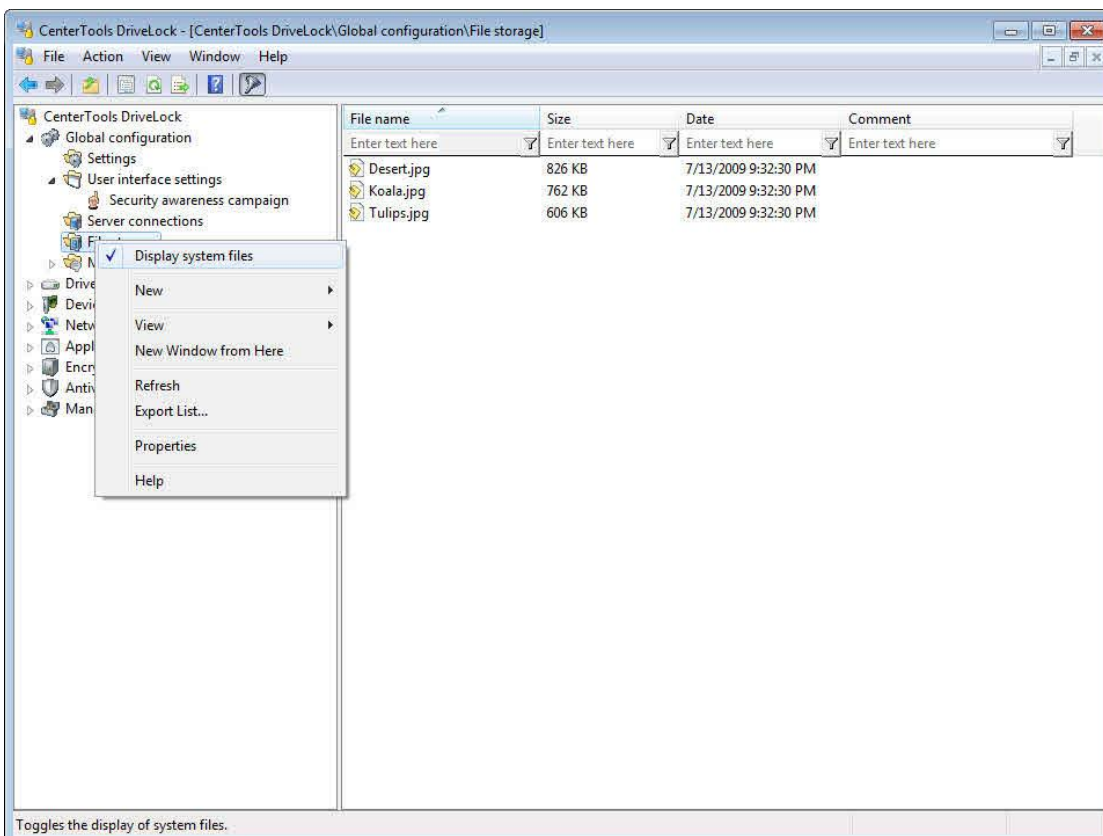
To view or modify a file in the file storage, right-click the file and then click one of the following:

- *Extract file* – Save a copy of the selected file to a destination you specify.
- *Delete* – Delete the selected file from the file storage.
- *Properties* – Display the properties of the selected file and where this file is used in your policy, for example in a whitelist command or when a network location is detected.



Click **Extract file** to extract the selected file.

Right-click **File storage** and click **Display system files** to view information about system files that DriveLock stores with the policy, such as encryption certificates.



System files cannot be deleted or extracted from the Policy File Storage.

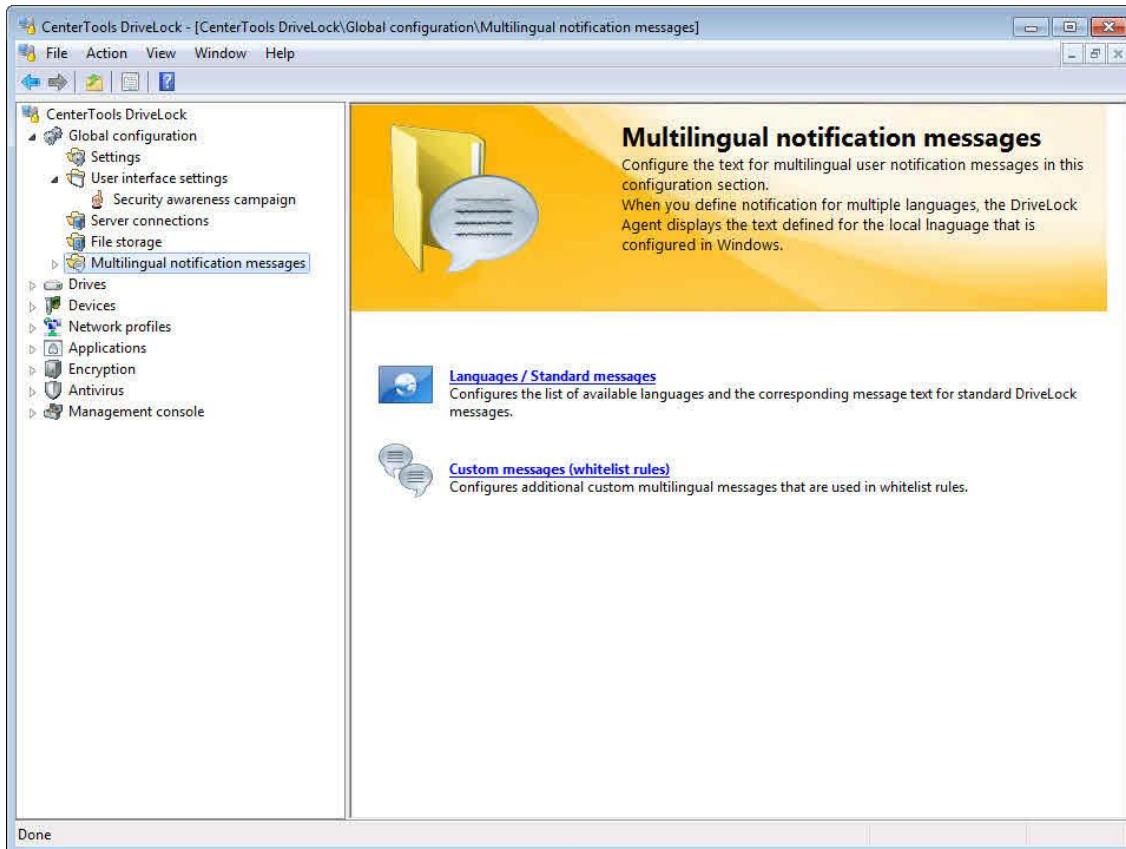
Right-click **File storage** and click **Properties** to view information about the Policy file storage.

Click **Reset storage** to delete the current storage and create a new Policy File Storage.

Resetting the current file storage deletes all files in the storage, including any system files. Ensure that you have a copy of these files before resetting the file storage. This is especially important if you use DriveLock Disk Protection because the Policy File Storage contains files that are required for disaster recovery operations.

6.10 Using Multilingual Notification Messages

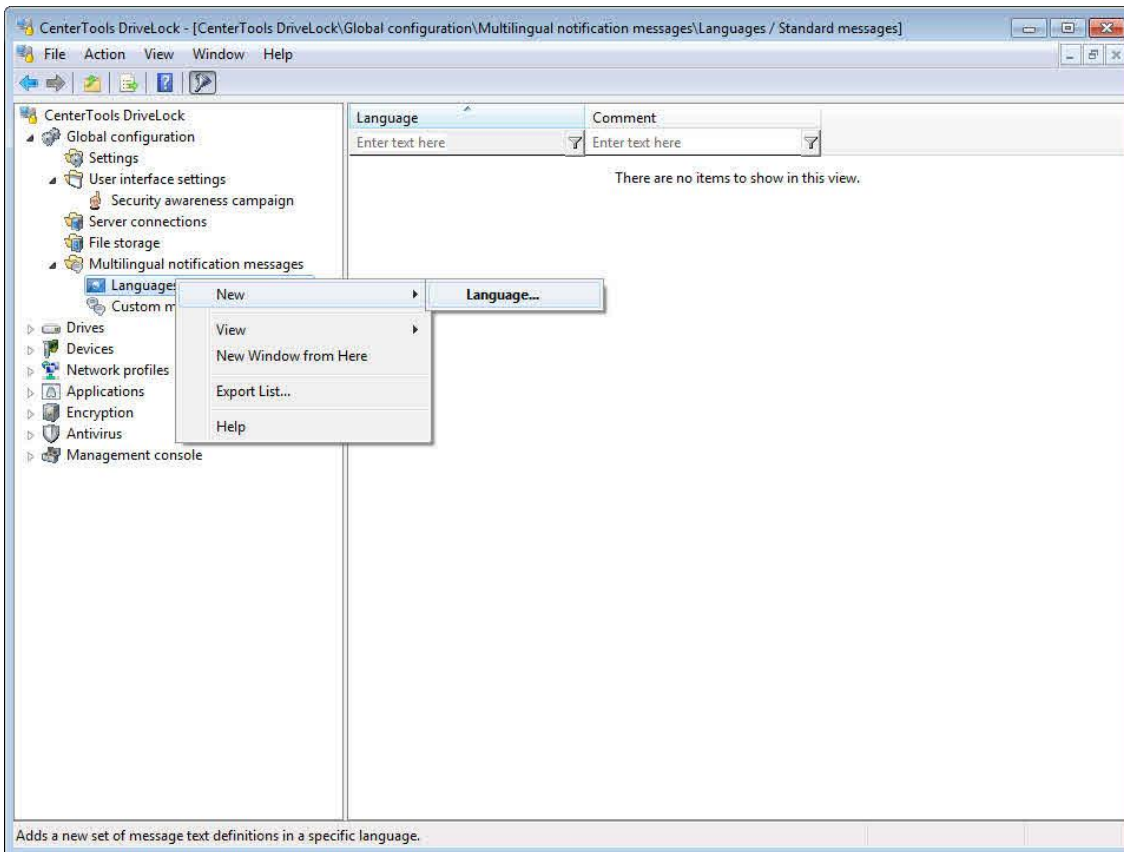
You can define separate text messages for different languages to be used in user notification messages.



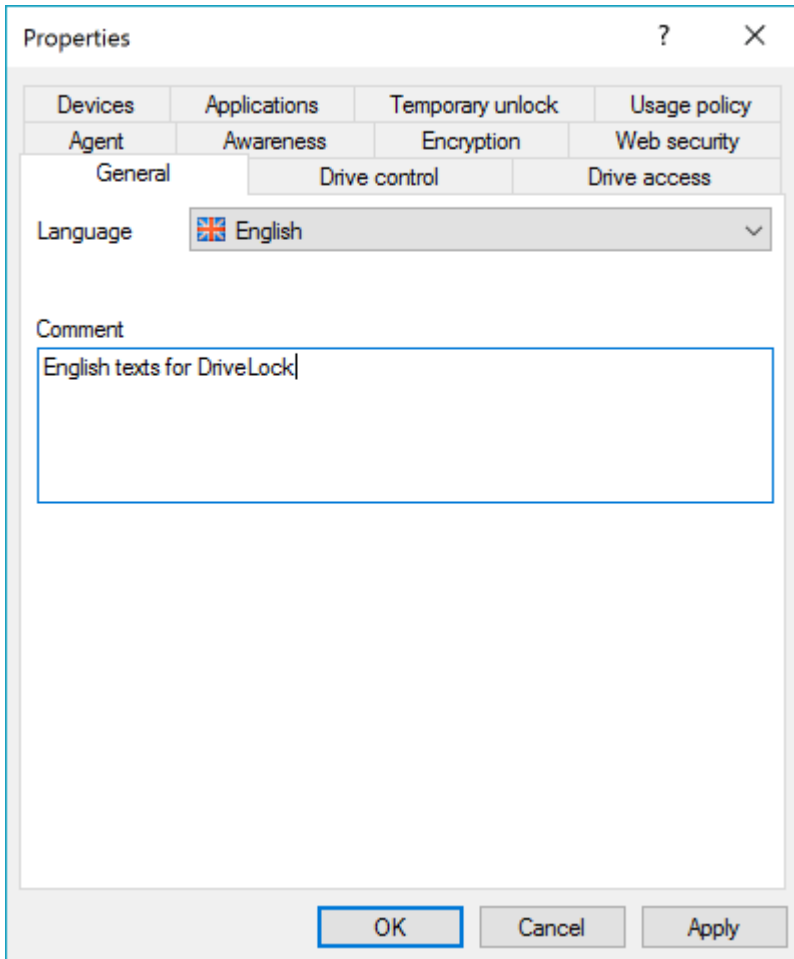
To configure languages and multilingual messages, click **Multilingual notification messages**.

Before you can define text for messages to be used in whitelist rules you must configure which languages are available.

6.10.1 Defining Languages and Standard Message Texts



Right click **Languages / Standard messages** and then click **New -> Language**.



Select a language from the list and type an optional description.

The list contains all currently available Windows languages.

On the **Drive control** tab, type the standard messages to be used when DriveLock locks drives.

The variable %DRV% will be replaced by the drive letter when the message is displayed.

Click **Test** to verify that your message appears correctly. DriveLock displays the message as it will appear to users.



On the **Drive access** tab, specify file filtering and CD/DVD burning message texts.

The variables will be replaced when the message is displayed as follows:

- %DRV% will be replaced by the drive letter.
- %PATH% will be replaced by the file path.
- %NAME% will be replaced by the file name (without extension).
- %EXT% will be replaced by the file extension.
- %REASON% will be replaced by an indication, why a file has been blocked (for example, "wrong content").

Click **Test** to verify that your message appears correctly. DriveLock displays the message as it will appear to users.

On the **Devices** tab, specify device messages. The variable %DEV% will be replaced by the device name when the message is displayed.

On the **Applications** tab, specify application control messages. The variable %EXE% will be replaced by the file name and path of the program when the message is displayed.

On the **Temporary unlock** tab, configure messages that DriveLock displays when drives or device are unlocked by an administrator. The variable %TIME% will be replaced by the duration for which drives or devices are unlocked. You can configure separate message to be displayed depending on whether the duration is specified in minutes or an expiration time applies. Enter the information that will be displayed on the first page of the offline unlock wizard.

On the **Usage policy** tab, configure usage policy settings.

You can configure DriveLock to allow access to one or more removable drives only after a user clicks the Accept button in a popup message explaining the drive usage policy, such as the following example:



The following settings determine the information displayed in this message:

- *Caption text*: Text displayed in the header (for example, “Company Drive Usage Policy”)
- *Usage policy text*: Text displayed in the message window (for example, “All access to external...”)
- *Accept button text*: Text used for the accept button
- *Decline button text*: Text used for the decline button

Optionally you can load the usage policy text from a file (either *.txt or *.rtf). You can select a file from the following locations:

- The local file system on the computer where the Agent applies the policy settings
- The DriveLock Policy File Storage. Files in the Policy File Storage are prefixed with an asterisk (*).

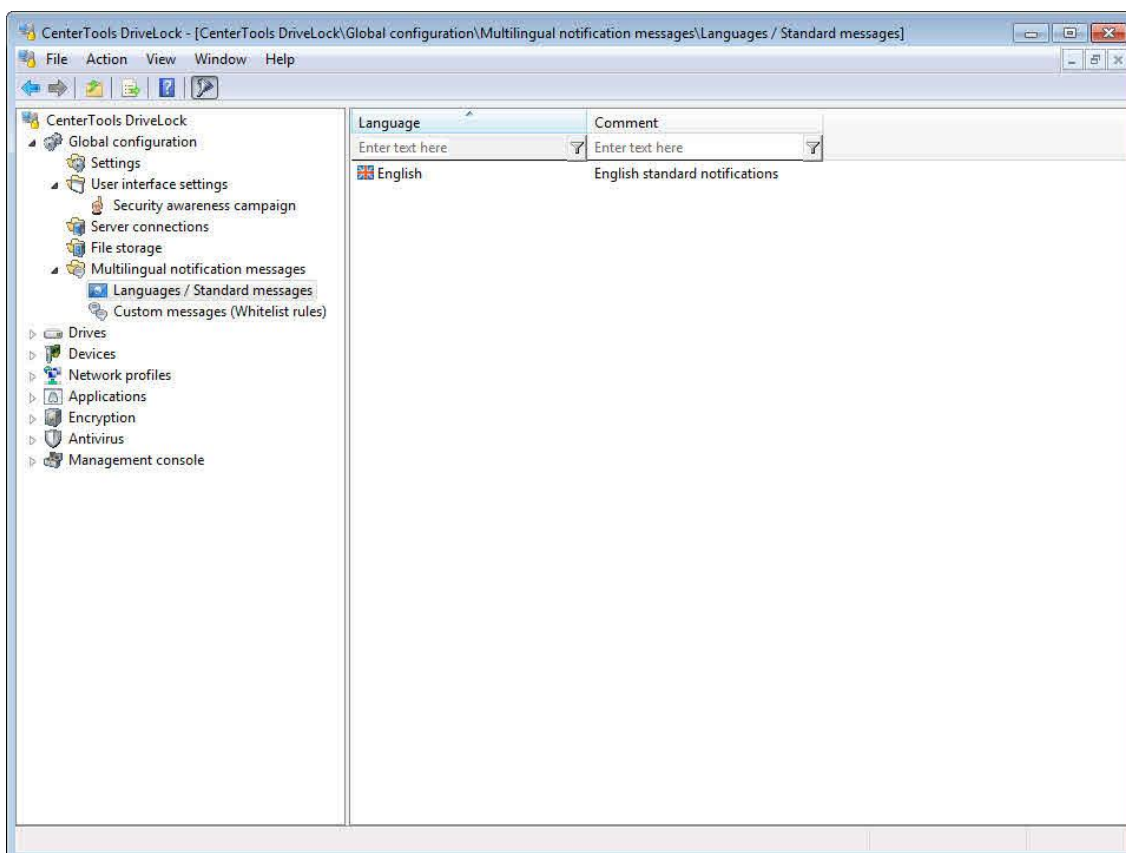
The DriveLock Policy File Storage is a protected storage area that is stored with a DriveLock configuration and distributed to Agents. For details on how to import files into the Policy File Storage and how to use these files, refer to the section [“Using the DriveLock Policy File Storage”](#).

To display a video file instead of text, select the “Play video” check box and specify a Windows video file (*.avi), that will be displayed in the usage policy message box. You can specify a file in the local file system on the computer where the Agent applies the policy settings or the DriveLock Policy file storage.

On the **Agent** tab, configure messages that DriveLock displays when an administrator establishes a remote connection to an Agent. The variable %USER% will be replaced by the name of the user who initiated the connection when the message is displayed.

On the **Awareness** tab, configure standard texts for the security awareness campaign window.

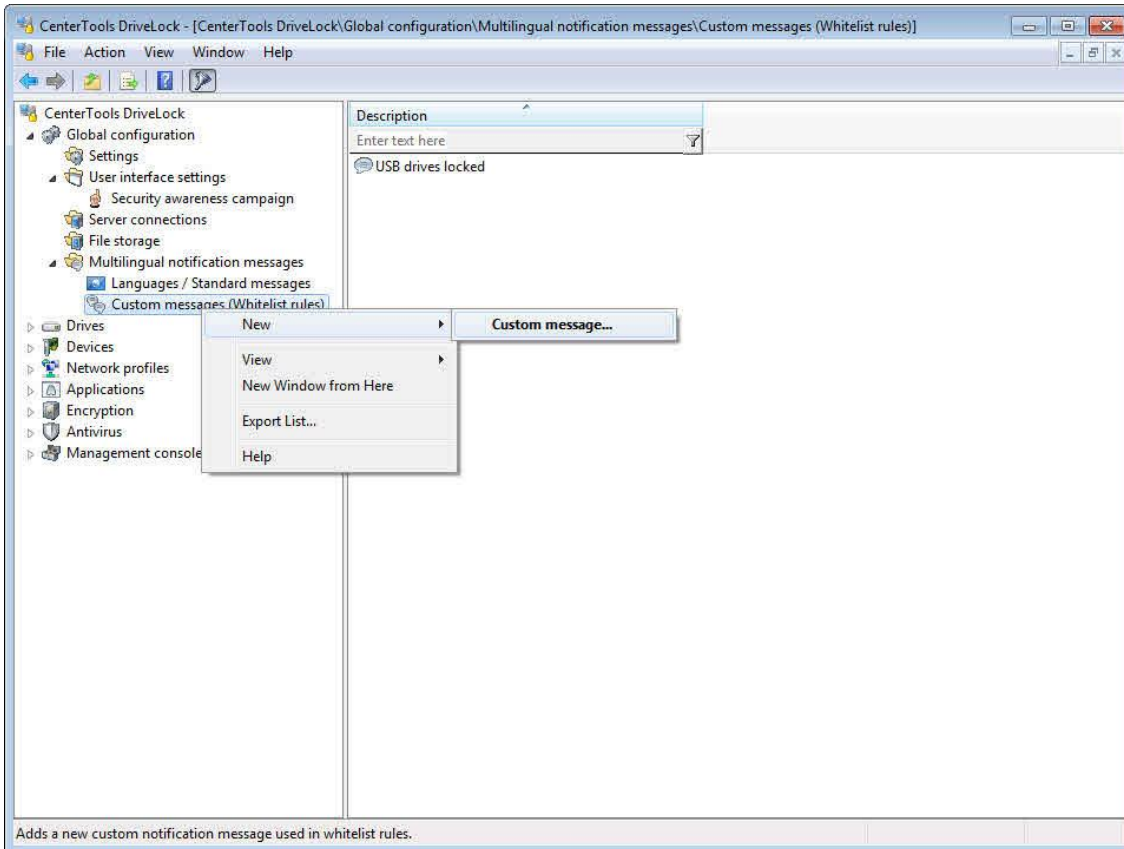
Click **OK** to apply the changes you made and to close the dialog box.



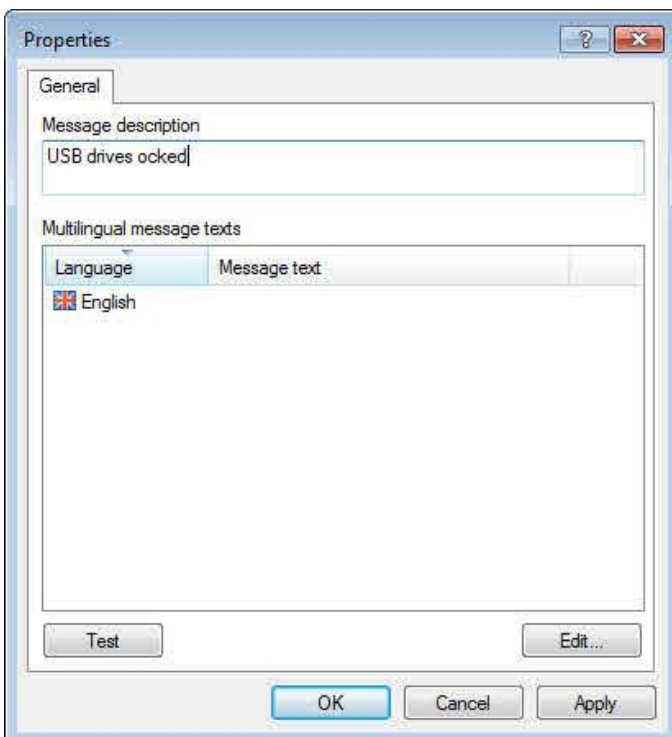
The right pane displays a list of all languages you defined.

6.10.2 Defining Custom Message Texts for Multiple Languages

In addition to standard messages you can define multilingual messages to be used in specific whitelist rules. Before you can define custom messages you must configure the available languages, as described in the previous chapter.



Right click **Custom messages (Whitelist rules)** and then click **New -> Custom message**.

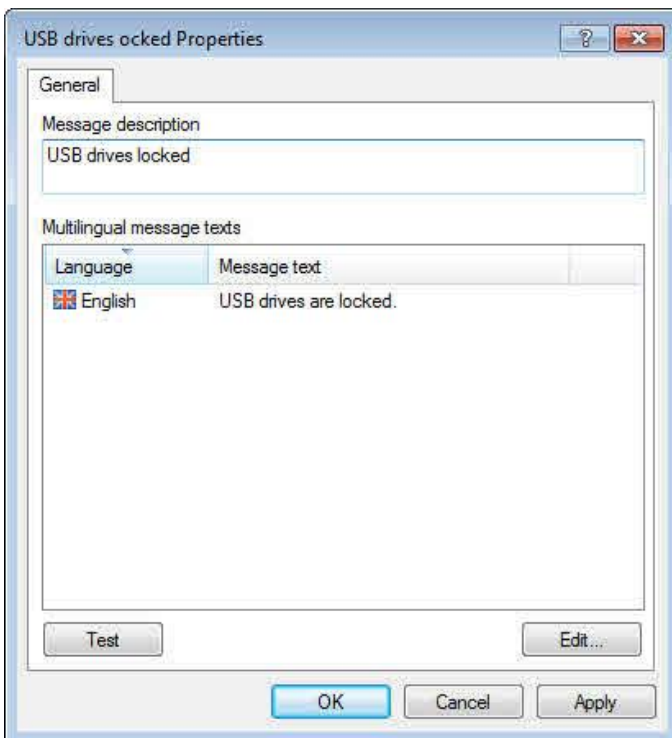


Type a message description. This description will be displayed in a list in the whitelist rule from which you can select the appropriate message for the rule.

All languages you defined are displayed. To enter the message text for a language, click the language and then click **Edit**.

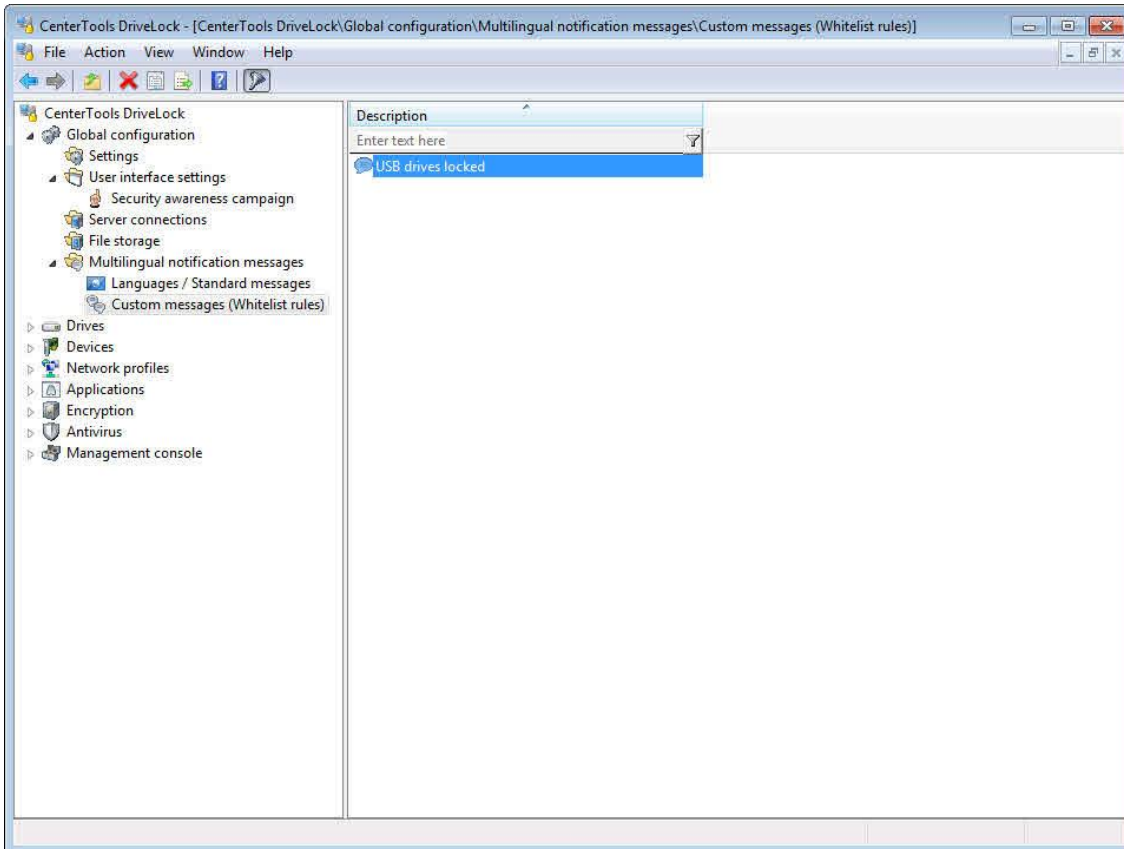


Click **Test** to verify that your message appears correctly. DriveLock displays the message as it will appear to users.



Repeat the procedure to define message texts for each language.

Click **OK** to apply the changes you made and to close the dialog box.



The right pane displays a list of all custom messages you defined.

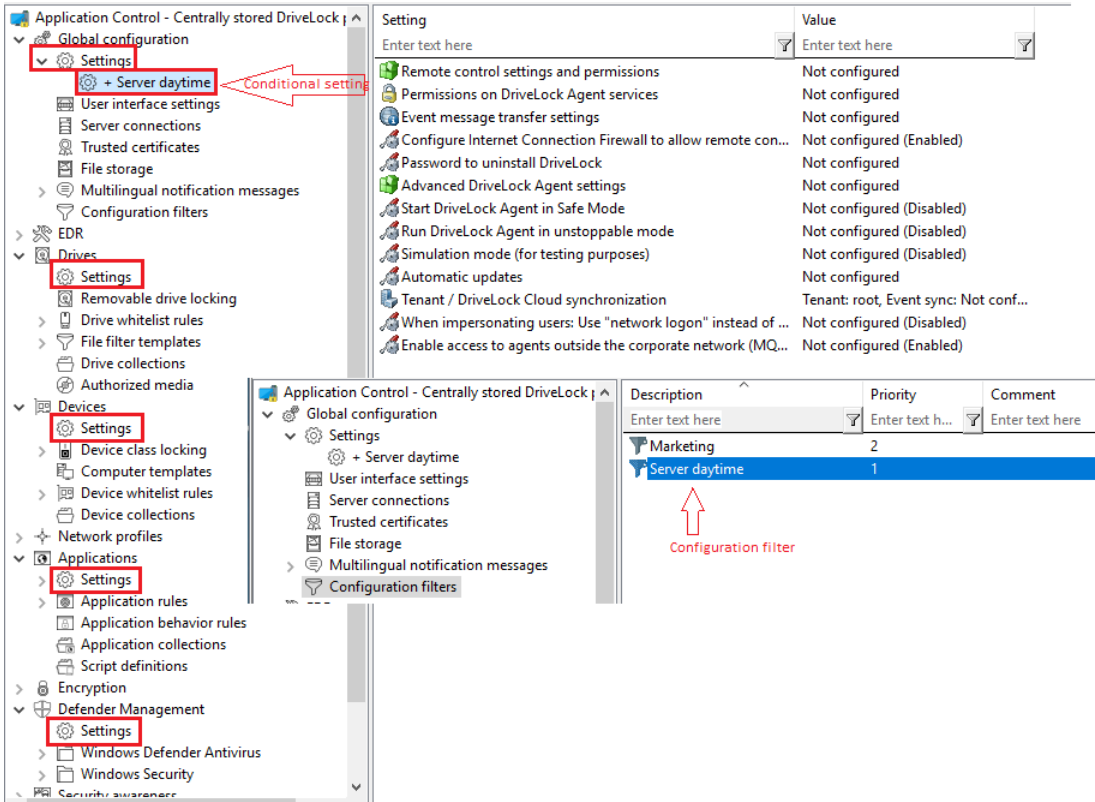
To use a multilingual message in a whitelist rule, select the message when you configure the rule.

6.11 Configuration Filters and Conditional Settings

Background: As a general rule, a setting applies wherever the corresponding policy applies. If you want to configure individual settings differently, you would therefore have to create a second policy. By using configuration filters for different computers, users or times or conditional settings within a single policy, you can save yourself the trouble of creating a new policy and thus the effort of having to maintain a large number of policies with individual settings.

Effect: With configuration filters, you can combine conditions for specific computers, users, or times in a single policy. The configuration filter by itself has no functionality, but it is used as a criterion for conditional settings. It can be used in all **Settings** nodes of the DriveLock Management Console. Proceed [like this](#) to create a configuration filter.

Using the configuration filter in conditional settings: Duplicates of the respective node are created below the individual **Settings** nodes and linked to a configuration filter.



The settings defined in this node only take effect if the filter on the **Computers**, **Logged on users** or **Time limits** tabs is fulfilled.

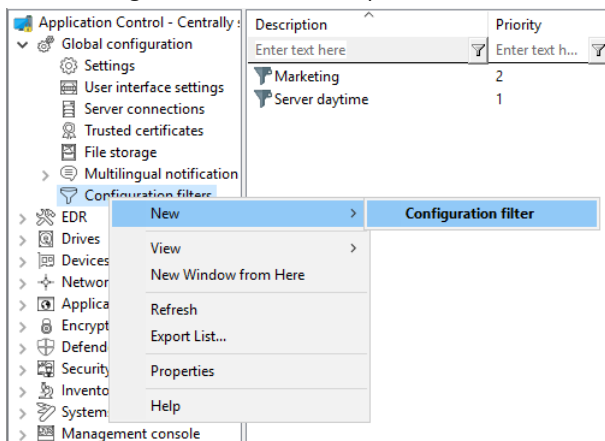
Advantages of conditional settings:

- More setting options are available than in a normal policy (for example, because you can define active times for conditions).
- You do not need to create numerous policies and their assignments
- Individual settings can be overwritten more easily
- You can track your settings more easily because everything is contained in a single policy
- Configuration filters also work offline

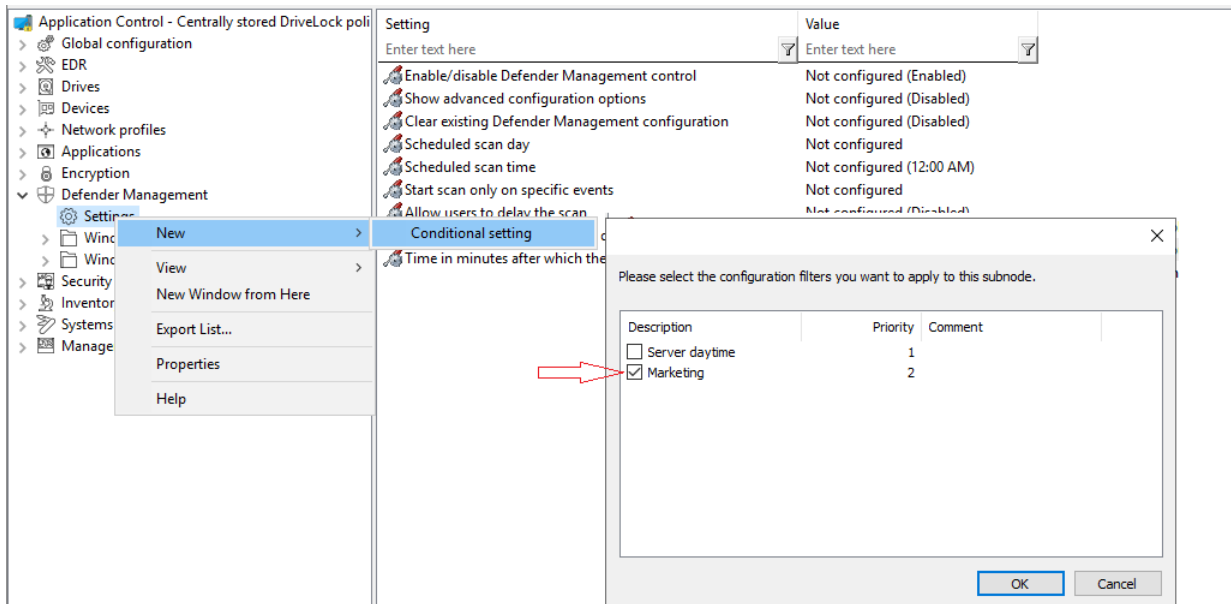
6.11.1 Creating a configuration filter

Create configuration filters as follows:

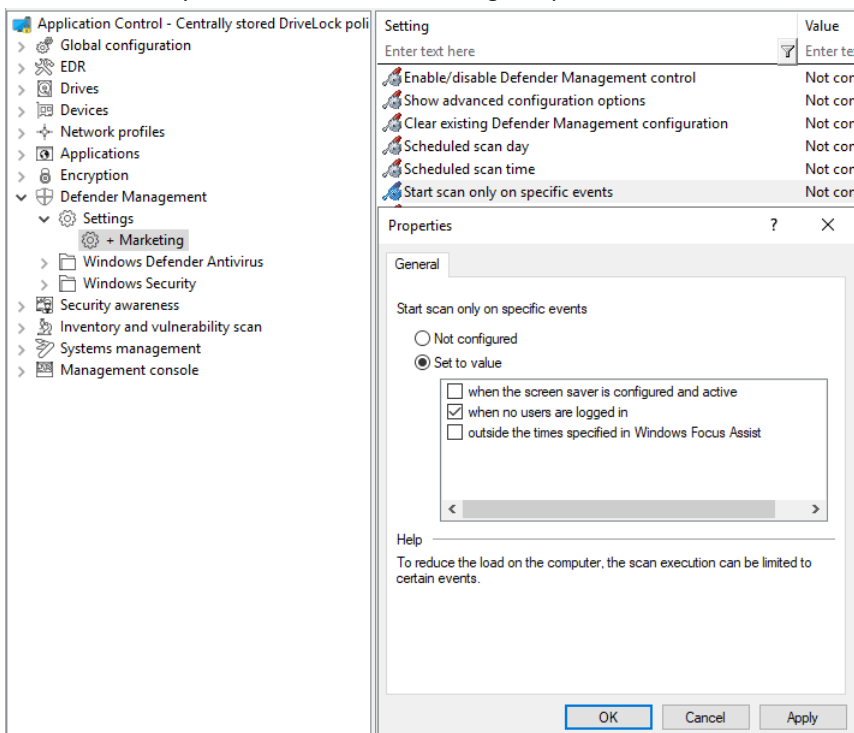
1. In the **Configuration filter** node, open the **New** context menu (see figure).



2. In the configuration filter properties dialog, enter a description and, if necessary, a comment.
3. Depending on the conditions you want to set (specific time limits, computers or users), enter the required settings on the corresponding tabs. You can find a use case [here](#).
4. Save the configuration filter.
5. Next, set the configuration filter as a conditional setting in any settings node of the DriveLock Management Console.
6. For example, if you want to link **Defender Management** settings to a condition for specific client computers (in the example, the computers of the Marketing department), proceed as shown in the figure below:



7. Then select the setting you want to apply explicitly to the marketing computers. In the example, the Defender scan should only be started on the marketing computers when no users are logged in:



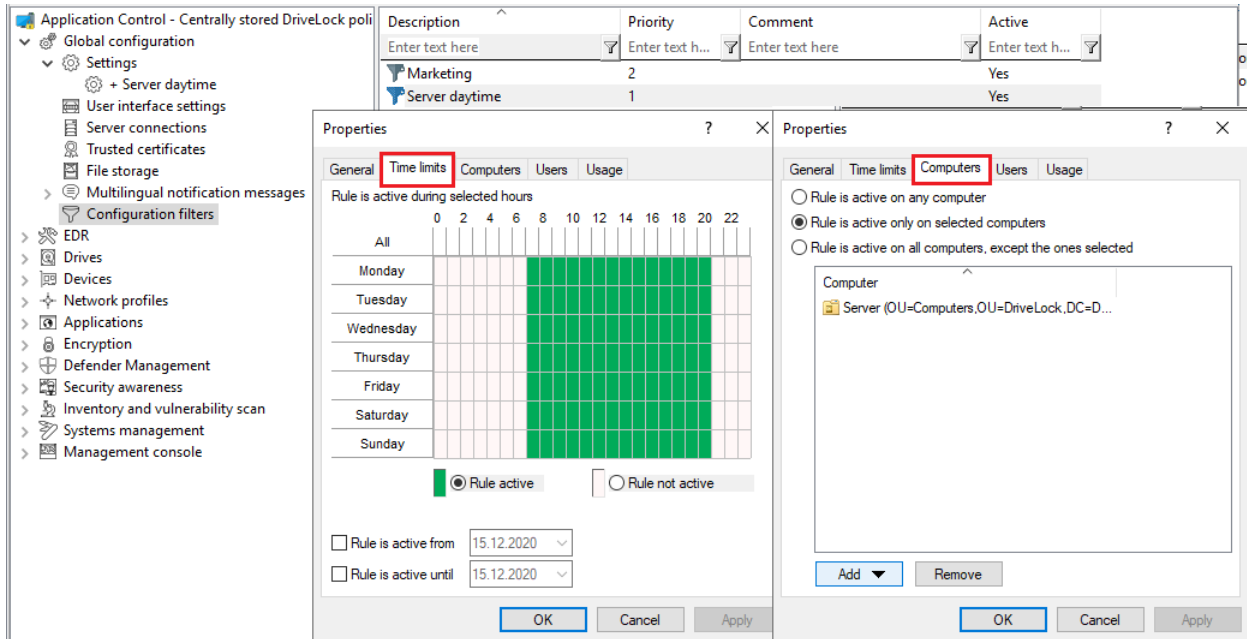
8. Save your setting and then assign the policy.

6.11.2 Use case

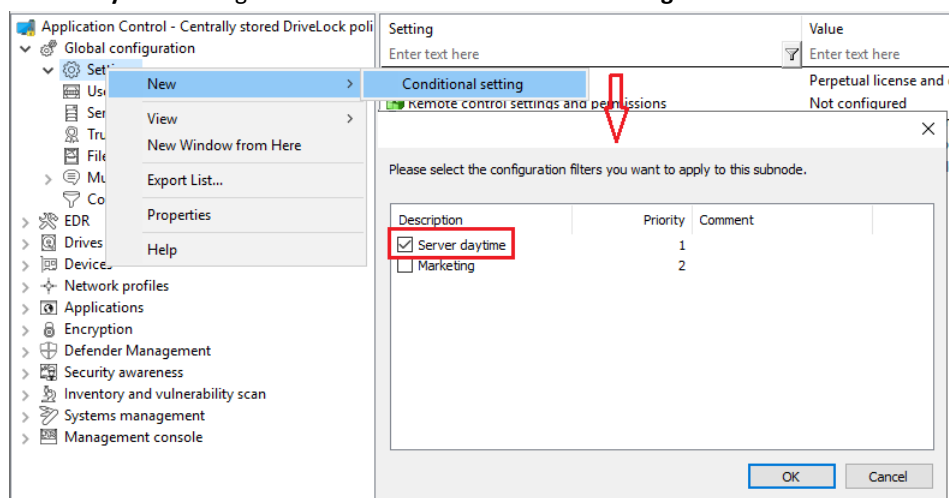
Target: You want to disable automatic updates during the day for certain DriveLock Agents (servers).

Proceed as follows:

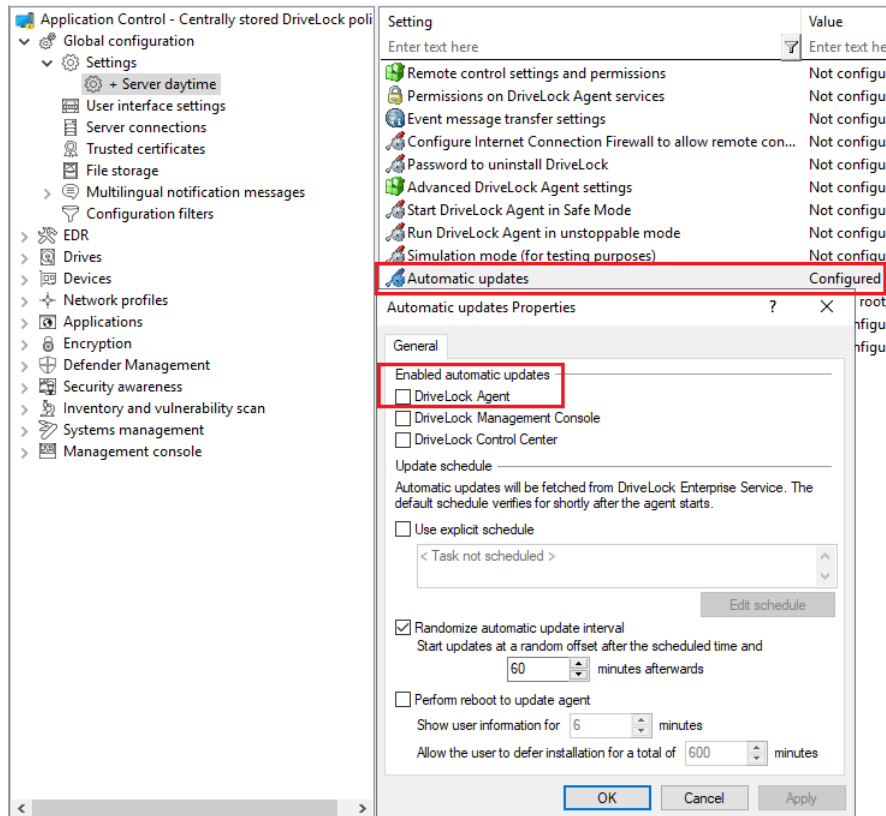
1. Create a new configuration filter.
2. Enter a description (for example **Server daytime**) and a comment in the dialog. **Is active** is ticked by default.
3. On the **Time limits** tab, select when the rule will be active (during the day).
4. On the **Computers** tab select the **Rule is active only on selected computers** option and add the server(s) you want to use from the **Add** drop-down list.



5. Save the configuration filter.
6. The configuration filter you created now appears in the corresponding node and can be used as a conditional setting.
7. To do so, select the **Settings** subnode in **Global configuration**, open the context menu, select **New** and then your **Server daytime** configuration filter as the **Conditional setting**.



8. Next, open the **Automatic updates** option in this conditional setting and uncheck **DriveLock Agent** that is set by default.



The screenshot shows the DriveLock configuration console. On the left is a tree view with 'Settings' expanded. The main pane shows a list of settings. 'Automatic updates' is selected and highlighted with a red box. Below it, the 'Automatic updates Properties' dialog is open, with the 'General' tab selected. In this dialog, the 'Enabled automatic updates' section has 'DriveLock Agent' unchecked, also highlighted with a red box. Other options like 'DriveLock Management Console' and 'DriveLock Control Center' are also unchecked. The 'Update schedule' section is visible, with 'Randomize automatic update interval' checked and set to 60 minutes. At the bottom are 'OK', 'Cancel', and 'Apply' buttons.

9. Save your configuration.

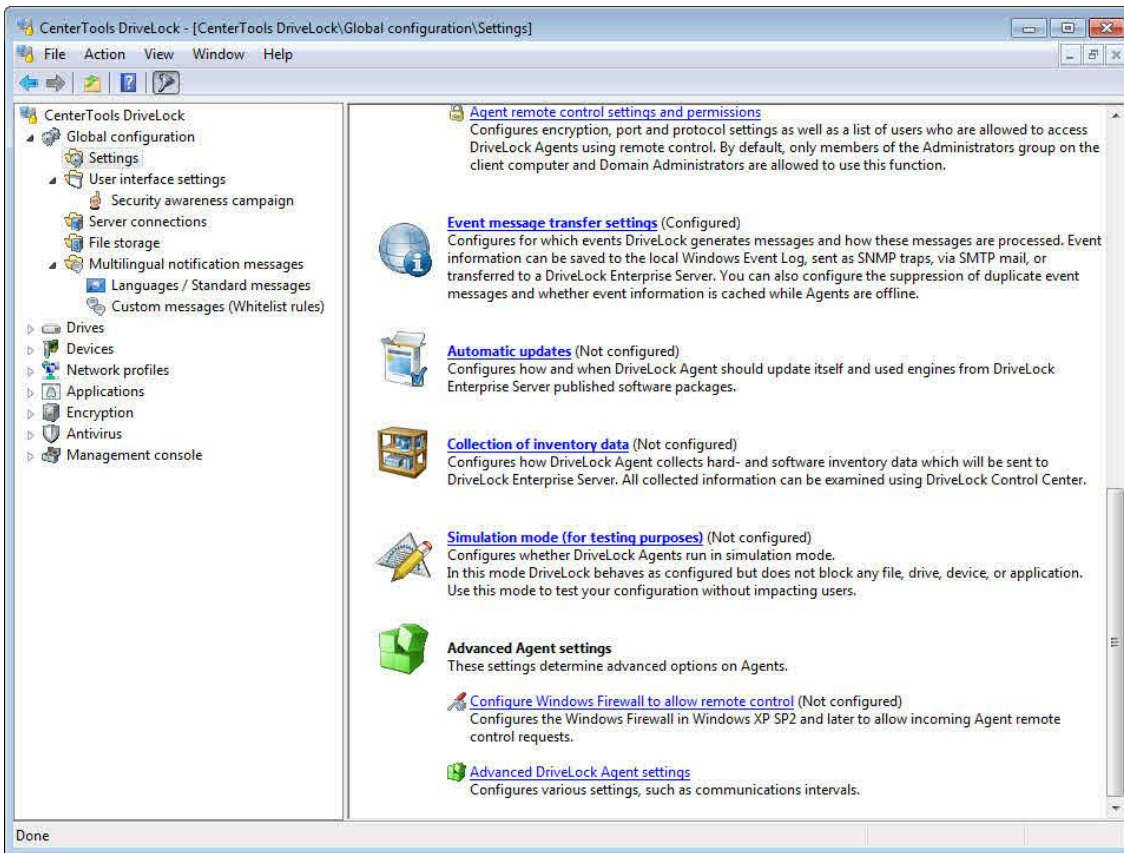
Conclusion: The rule with the conditional setting **Automatic updates** is switched off on the defined servers during the day, but active on all other DriveLock Agents (as defined in the normal settings).

Explanation: Conditional settings override the normal settings

If there are several conditional settings, the priority of the configuration filters determines which one is applied. You can adjust the priority.

6.12 Configuring Additional Settings

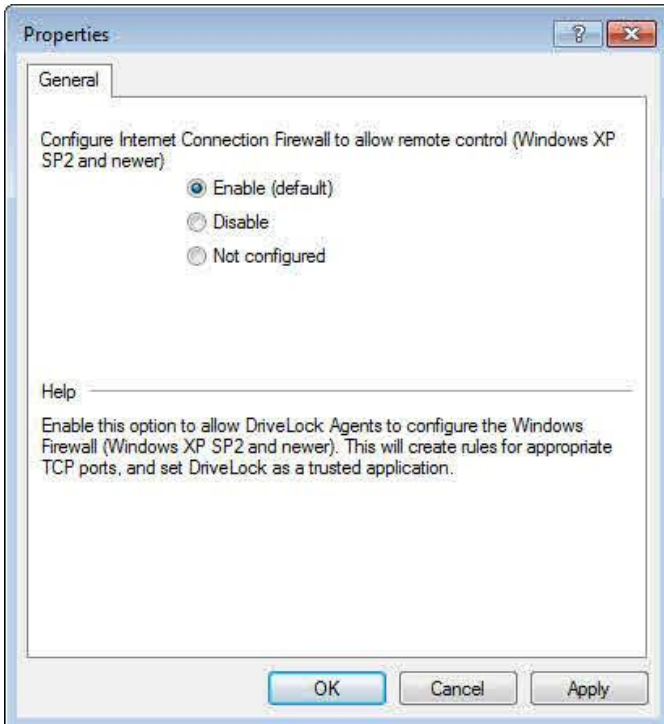
To configure additional settings, go to *Global configuration* -> *Settings* and then scroll to the bottom of the taskpad.



6.12.1 Configure the Internet Connection Firewall to Allow Remote Control

To allow remote control of the DriveLock Agents on computers using the Windows Firewall, you must configure the firewall to allow these connections. Remote control requires that incoming connections on TCP Ports 6064/6065 (default) and the program "DriveLock" are allowed in the exceptions list of the Windows Firewall. DriveLock can create these two rules for you.

Click **Configure Internet Connection Firewall to allow remote control**:



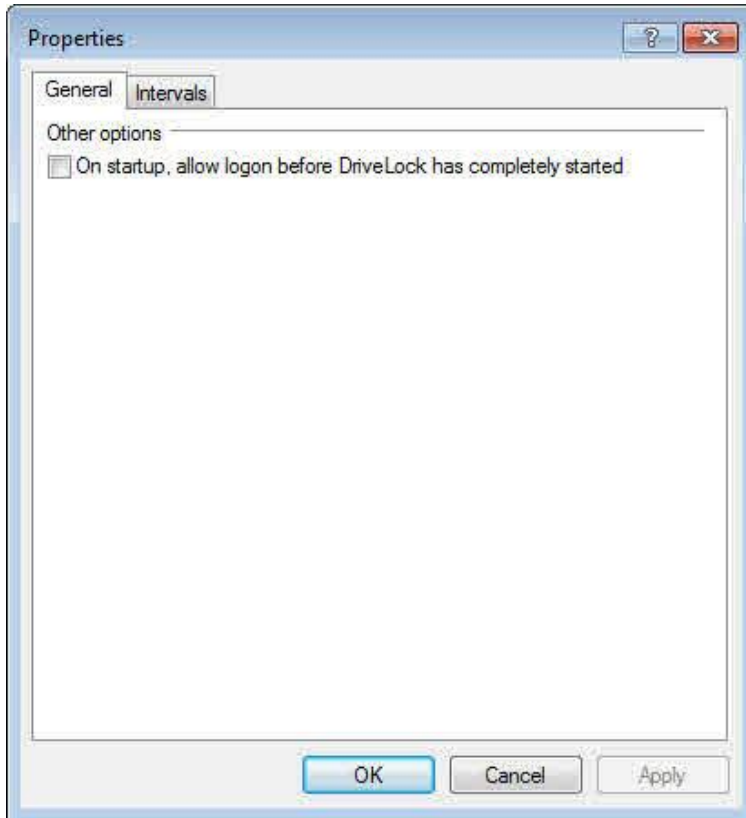
Select **Enable** and then click **OK** to have DriveLock creating the necessary rules for you.

Rules that were previously created by DriveLock are not removed if you later change the selection to "Disable" or "Not configured".

6.12.2 Advanced DriveLock Agent Settings

Use these options to optimize DriveLock Agent operations on client computers.

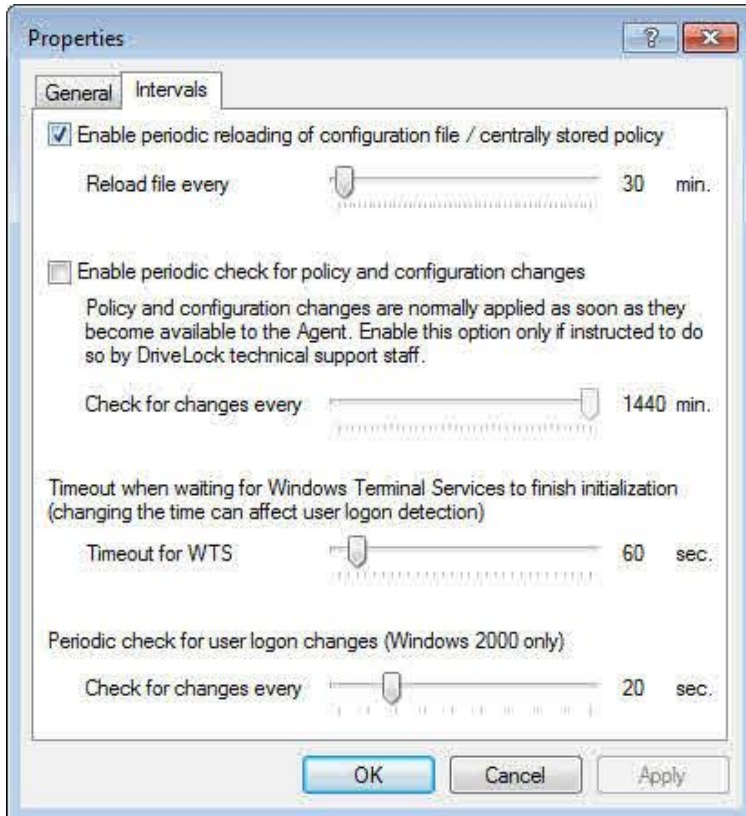
To open the Properties dialog box, click **Advanced DriveLock agent settings**.



To prevent a user from logging on and using Windows Explorer before the DriveLock service has been started, DriveLock has an integrated service dependency. As a result, after the DriveLock agent has been installed the logon screen may not appear as quickly as usual. This mainly occurs on fast computers. The setting **“On start-up, allow local logon before DriveLock has completely started”** let users log on to a computer sooner after starting the computer but DriveLock rules may not be enforced immediately after the user logs on. For example, users may be able to access removable media even though your policy doesn’t allow this access.

When Windows XP starts it displays the logon screen before the boot process is finished. Some services may still start in the background while the user is logging on. By default, DriveLock delays the display of the logon screen until the Agent has started and can enforce policy settings.

Click the **Intervals** tab to configure the intervals of certain recurring Agent tasks.



Select **“Enable periodic reloading of configuration file”** to force a DriveLock Agent to periodically reload the configuration settings from a configuration file or centrally stored policy and configure the reloading interval. Changes to a these types of policies are only applied when the configuration file is reloaded. By default the Agent only reloads the policy settings only when the DriveLock service is started.

Select **“Enable periodic check for policy and configuration changes”** to have DriveLock to check for local configuration changes in addition to Group Policy changes. Usually, DriveLock automatically detects changes to a local configuration or a Group Policy Object in real-time. If this real-time check does not work correctly in your environment, select this option and then configure the interval.

Configure the setting **“Timeout when waiting for Windows Terminal Services ...”** to delay detection of the currently logged-on user until all logon scripts have completed in a Terminal Services environment. Increase this interval if you use logon scripts that take more than 15 seconds to complete.

Use the slider **“Periodic check for user logon changes”** to configure how often DriveLock checks whether the currently logged-on user has changed. This setting applies to computers running Windows 2000 only.

6.13 Self-service groups

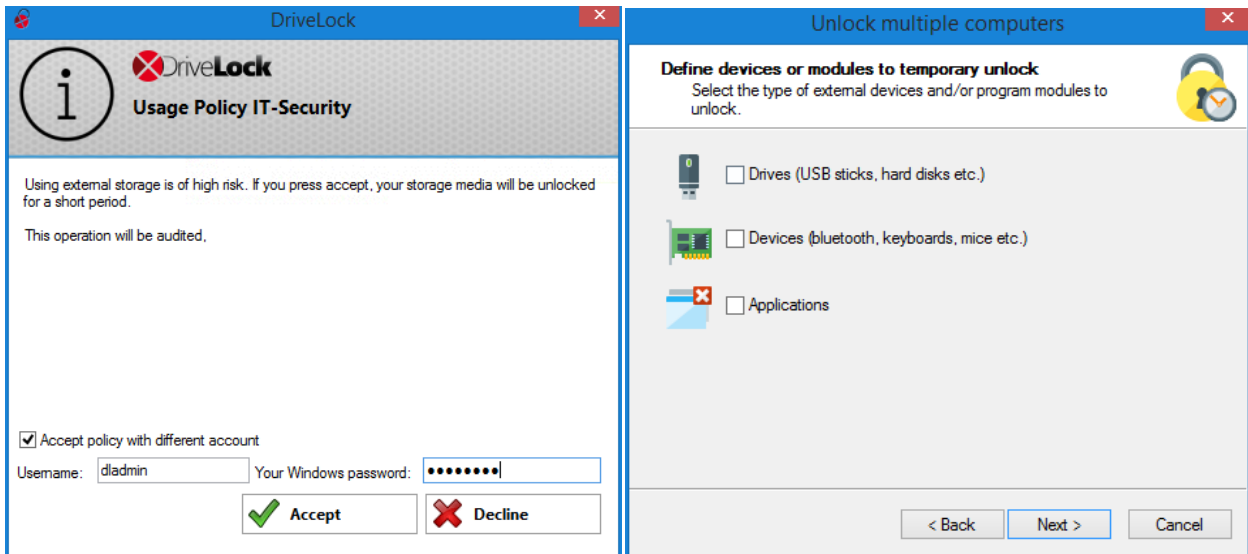
Self-service groups are designed to allow authorized users to temporary unlock DriveLock Agents without using a DriveLock Management Console (MMC) or a DriveLock Control Center (DCC).

If you are not familiar with unlocking Agents read chapter [Unlocking Agents](#) first. Basically unlocking with self-service uses the same settings and mechanism.

Example:

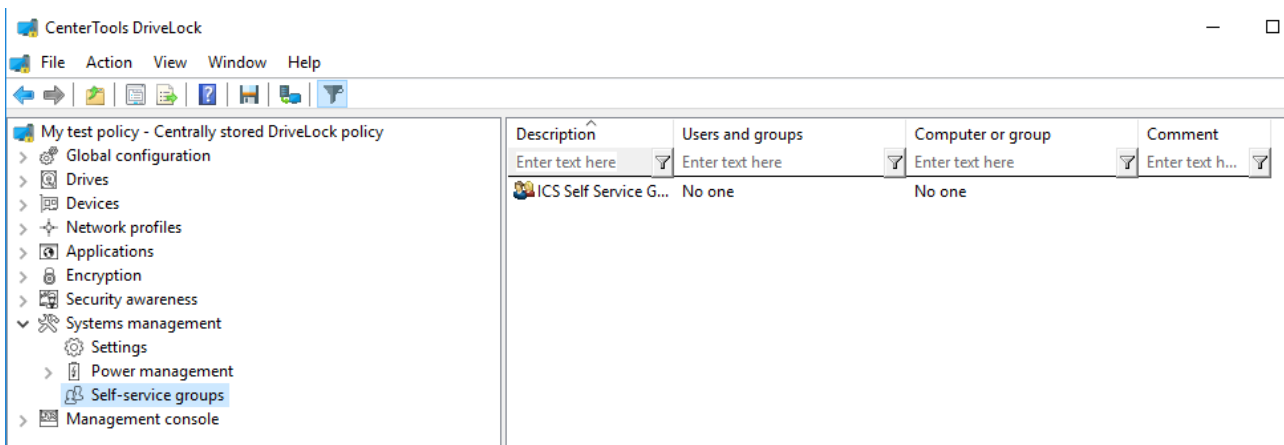
Industrial robots need new software to be installed and the robots are protected by DriveLock Device Control (DC) and DriveLock Application Control (AC). To be able to install the new software from an USB stick the robots have to be unlocked temporarily.

When the machine operator plugs in the USB stick, a logon window appears where they can authenticate. If they are authorized the unlock wizard starts and they can unlock Drives, Devices and Applications. Now they are able to run the setup from the USB stick.



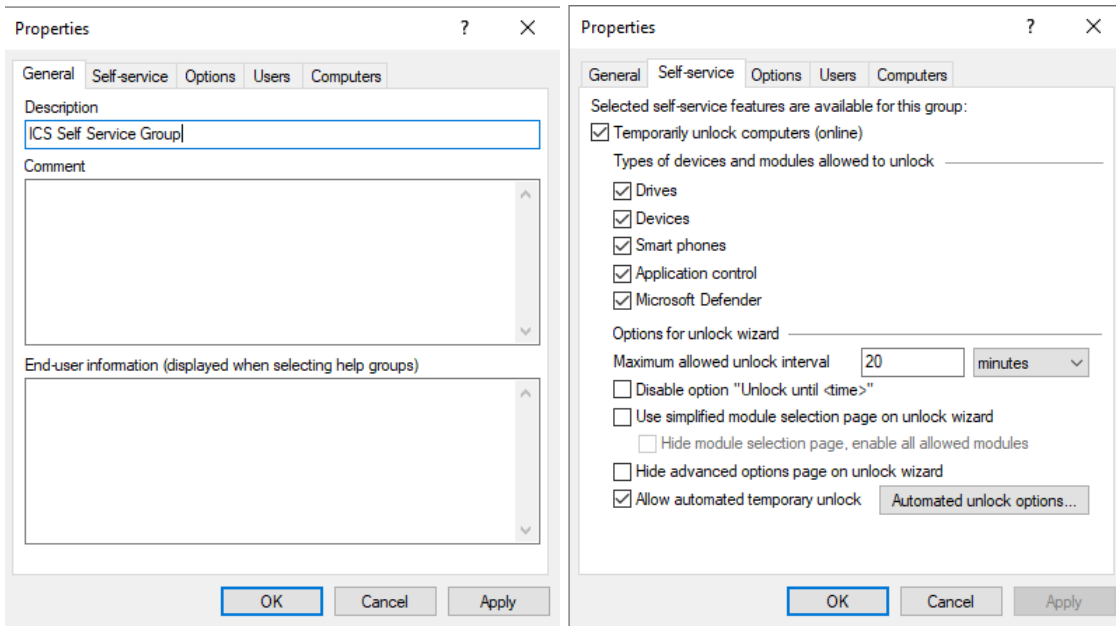
6.13.1 Configuring self-service groups

In your DriveLock Policy open **Systems management / Self-service groups** to add a new group (**right click / New / Self-service group**) or to edit (**double click**) an existing group.



Self-service options

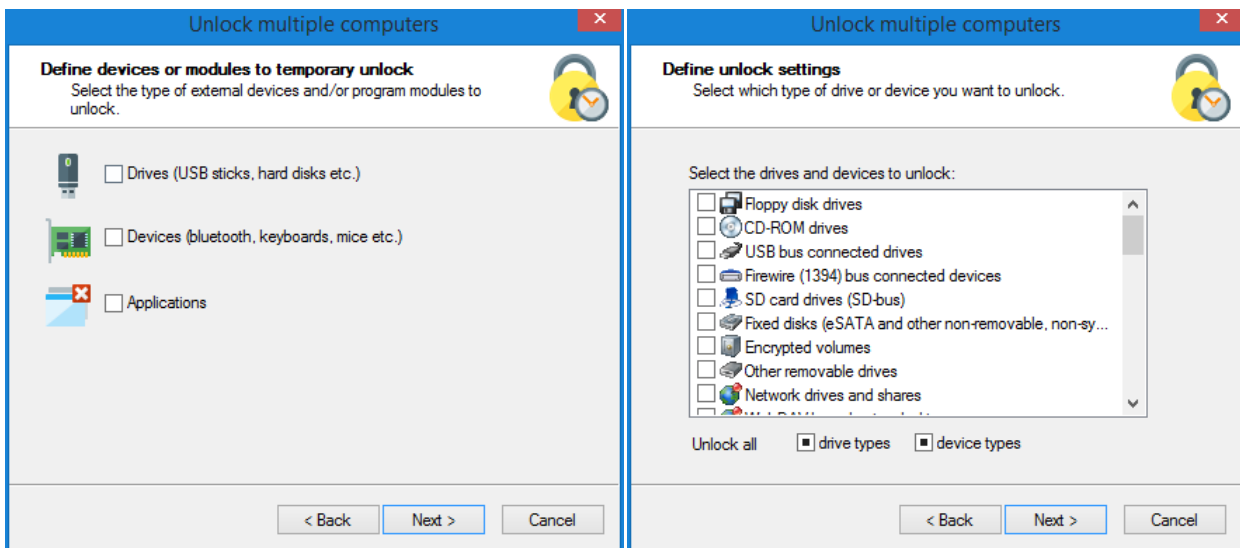
Here you can configure the user experience for the self-service wizard and decide which options the user gets shown.



General tab: enter a short description and a comment to identify this self-service group. Use the field End-user information, to display an explanation for the user, when and how to use this rule. The text will be shown in the wizard if more than one self-service group is configured and the user selects one of them.

Self-service tab : only device types and modules which are checked here can be unlocked through the wizard.

If you select to use the **simple module selection page** in the wizard the user will exactly get these options and no **advanced options** will be offered. Otherwise the user gets the option to select the devices more granular and **advanced options** may be offered on a next page.



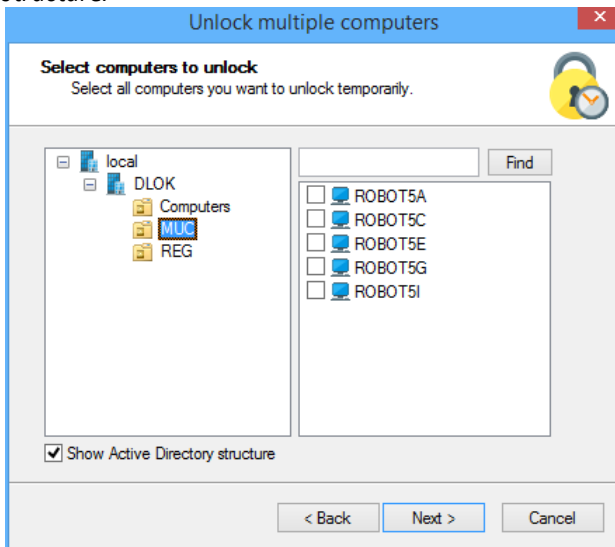
Allow automated temporary unlock: This option is for experts only. Read white paper *Self-Service Automatic Unlock feature* or ask DriveLock Consulting Services for more information.

If you unlock smartphones, other MTP devices are automatically unlocked as well.

Users and Computers

Windows users can be selected who are allowed to use the unlock wizard. Add computers on which these users can unlock agents using the wizard. If you only add **< local computer >** the user can unlock any computer where this policy applies and where they can start the unlock wizard locally. You may also add computers, computer groups or

OUs from the **Active Directory** or just enter computers **By name**. Then the wizard will display a list of computers where the user can select which computers to unlock remotely either from a list or from the Active Directory structure.



Export/import self-service groups

Open **Systems Management / Self-service groups / Right click All Tasks** to export/import self-service groups to/from a CSV file. You may use the export as template to multiply existing groups for other users and/or computers.

For the import:

- don't modify existing headers
- additional columns will be ignored
- if the value for **Unique ID** is empty a new entry will be created, otherwise the existing entry will be updated
- AD read permissions are required, to perform the import

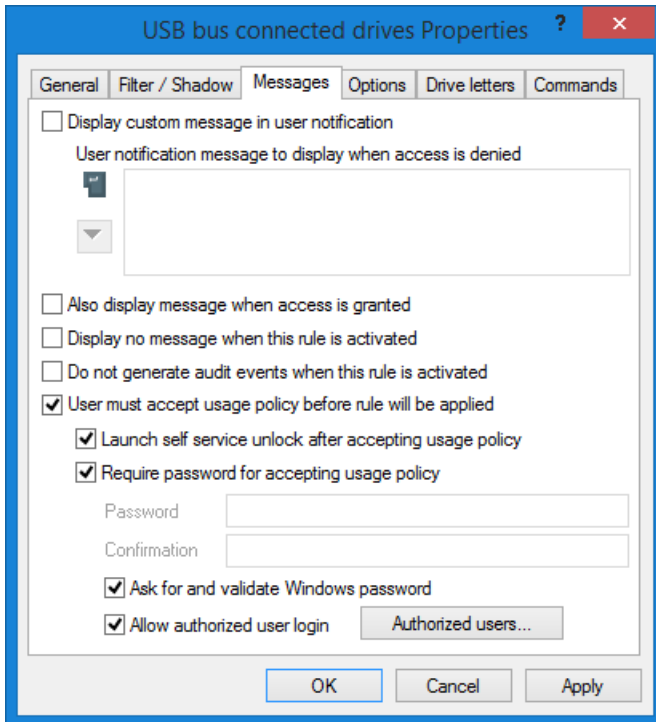
Ask DriveLock consulting services for more information.

6.13.2 Start the self-service wizard

By default, the self-service wizard will not be offered to the end-users. You have to enable your required options in the policy. Open **Global configuration / User interface settings / Agent and awareness campaign user interface settings**.

- Start the self-service wizard in the DriveLock User Interface: tab General - check **Unlock via self-service wizard**.
- Start the self-service wizard from the start menu: tab Start menu - check **Show link to self-service wizard in start menu**.
- Start the self-service wizard from the Taskbar Icon: **Global configuration / User interface settings / Taskbar notification area settings / Tab Options / Add Self-service**.

You may also configure, to start the self-service wizard, when a usage policy applies (see example above).



- In any rule (either basic rules or whitelist rules), including usage policy which the user has to accept before the rule will be applied, you may also configure that the self-service wizard will be started as soon as the user accepts the usage policy. In the rule open tab **Messages** and check **Launch self service unlock after accepting usage policy**.
- If you want that other users but the one logged in to Windows shall accept the policy, check **Require password for accepting usage policy**, **Ask for and validate Windows password** and **Allow authorized user login**. Click **Authorized user** to edit the list of users who shall do so and check **Enable "logon as user" option by default**. The self-service wizard will "run as" the authorized user.



Part VII

Settings in Rules Across Modules

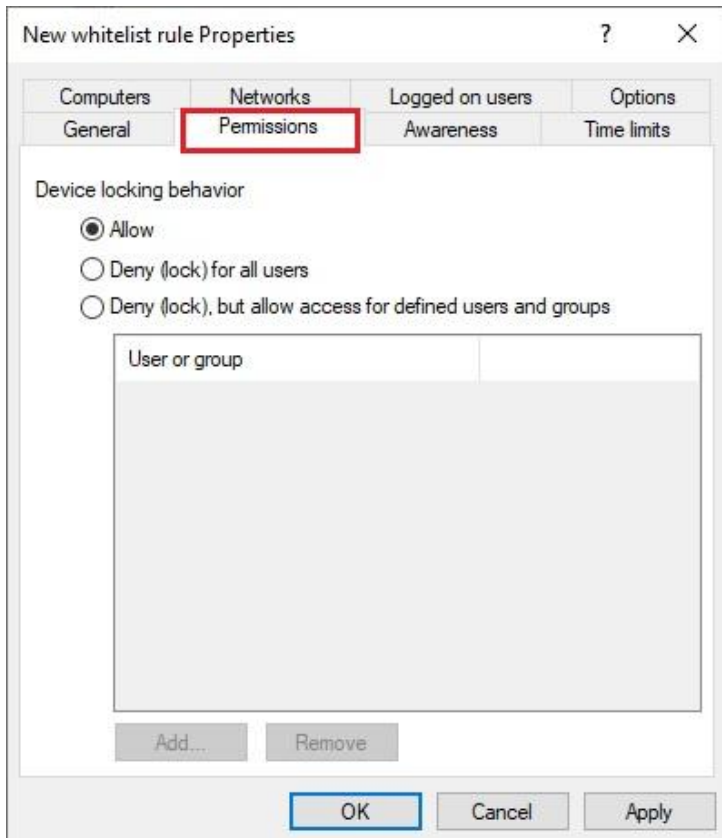


7 Settings in Rules Across Modules

Some settings are cross-module and available in most of DriveLock rules similarly.

7.1 User Permissions

To configure user access, on the “**Permissions**” tab define how users can access the drive.



Select one of the following options:

- *Allow*: Every authenticated user can access this drive.
- *Deny (lock) for all users*: Nobody can access this drive, it is completely locked.
- *Deny (lock), but allow access for defined users and groups*: The drive is locked, but the specified users or groups are allowed to use the drive either in read only mode or with write permissions.

Click **Add** to add a user or group to the list, and then specify whether the user or group can copy files to the drive or only read data from it. To remove a user or group from the list, select the user or group and then click **Remove**.

7.2 Time Limit Settings

If you want a rule to be active only during a certain time (for example only on Wednesdays or on weekdays between 9 A.M. and 5 P.M.) you can specify time limits for the rule. You can also specify start and end dates for a whitelist rule.

New whitelist rule Properties

Computers	Networks	Logged on users	Options
General	Permissions	Awareness	Time limits

Rule is active during selected hours

	0	2	4	6	8	10	12	14	16	18	20	22
All												
Monday												
Tuesday												
Wednesday												
Thursday												
Friday												
Saturday												
Sunday												

Rule active
 Rule not active

Rule is active from 11.05.2021

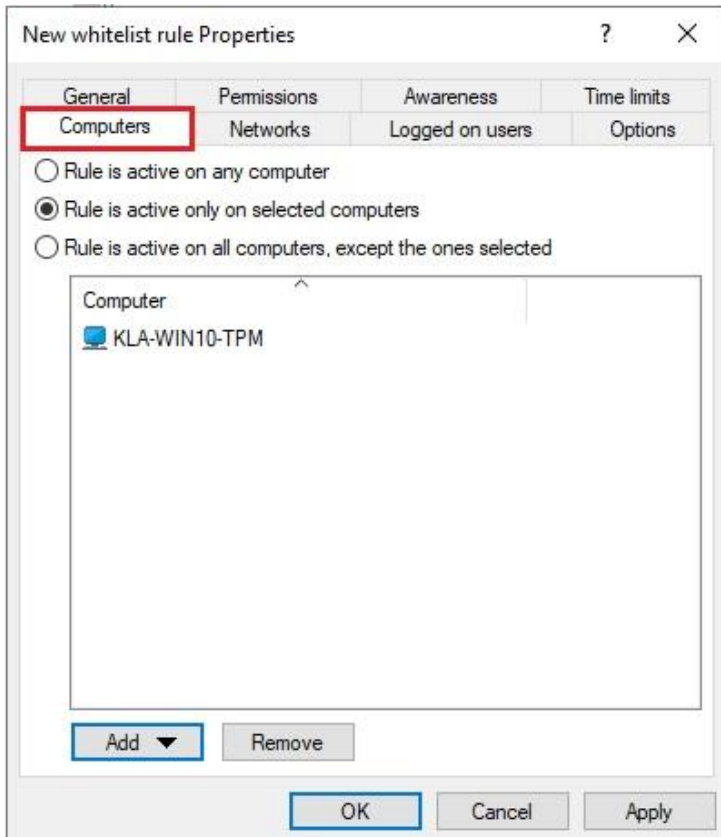
Rule is active until 11.05.2021

OK Cancel Apply

First select the appropriate time block or blocks by clicking one or more rectangles, an entire column or a row, and then click **“Rule active”** or **“Rule not active”**.

7.3 Settings for Computers

On the “Computers” you specify the computers on which a whitelist rule is applied.



Select from the following options:

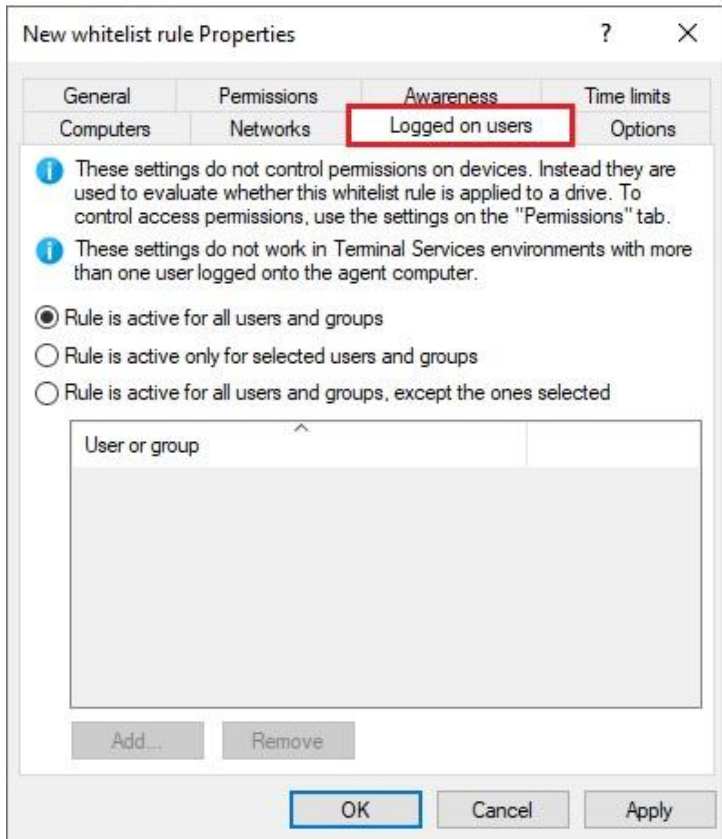
- Activate this rule on all computers
- Activate this rule only on the specified computers
- Exclude specified computers from this rule

Click **Add** to add more computers to the list. You can select a computer, a group of computers or an organization unit from the active directory. Click **Remove** to delete a group or computer from the list.

7.4 Logged on Users

On the **Logged on users** settings tab you specify whether the rule is applied only to certain users and user groups.

User and group validation is different from user permissions defined on the *Permissions* tab. Validation only determines whether a rule is applied to a user. If the rule is applied, DriveLock then allows or denies access based on the rule’s permission settings.



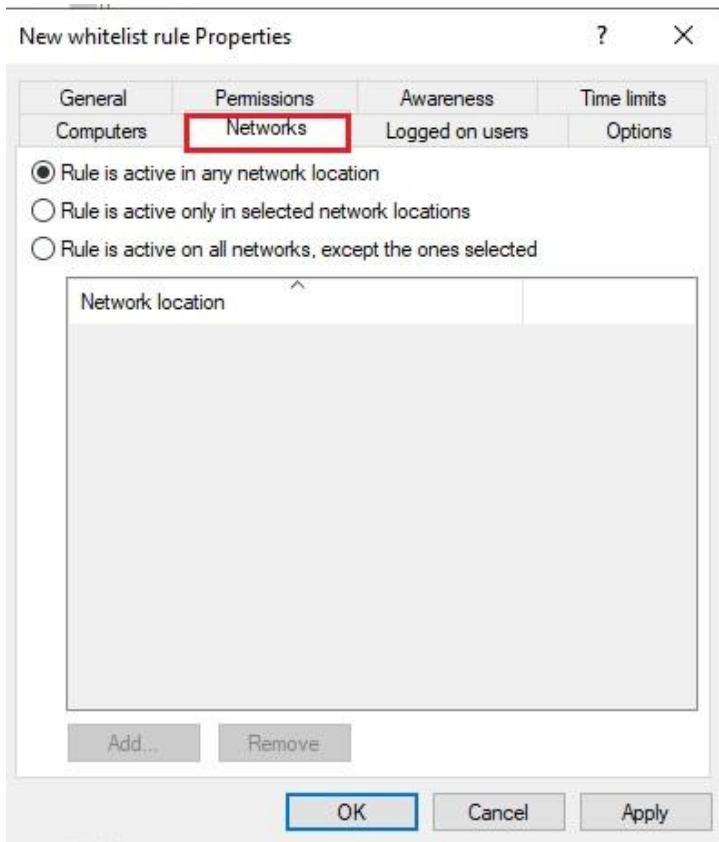
Select from the following options:

- Activate this rule for all users
- Activate this rule only for specified users or user groups
- Exclude specified users or user groups from this rule

Click **Add** to add more users or user groups to the list.

7.5 Network Settings

On the **Network** settings tab you specify whether the rule is applied only in certain network locations.

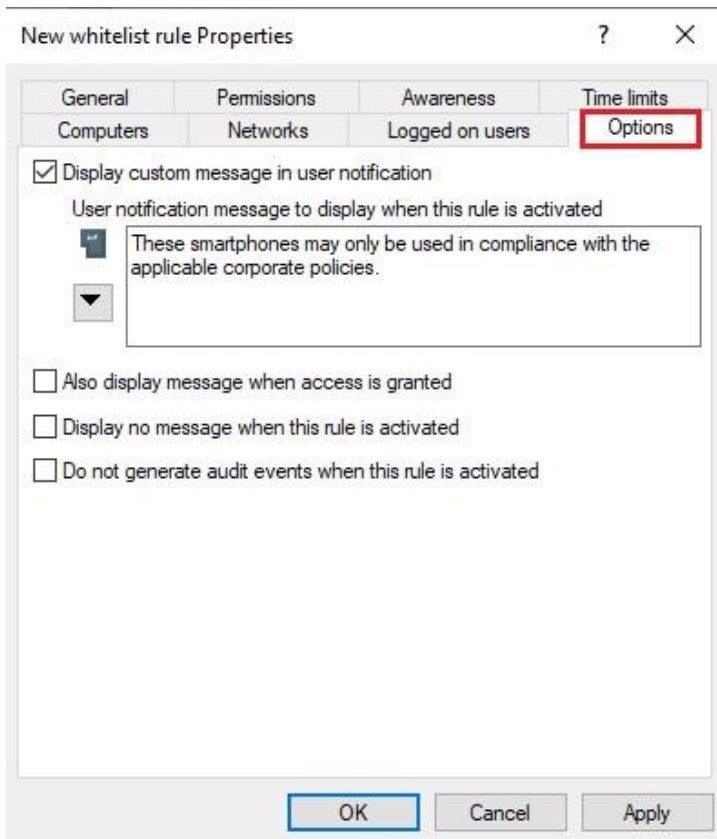


Select from the following options:

- Activate this rule in all network locations
- Activate this rule only in the specified network locations
- Exclude the specified network locations from this rule

Click **Add** to add more defined network locations to the list.

7.6 Additional Options



Select the **“Display custom message in user notification”** checkbox to activate the user notification message for the whitelist rule.

In the text edit box, type the message. DriveLock will display this message regardless of the client computer’s language setting. If you use this type of notification message, DriveLock displays a key icon near the top left corner of the text edit field.

If you have defined multilingual messages you can select such a message instead. To select a multilingual message, click the “down arrow” button and then on the drop-down menu click “Select multilingual message”.

Multilingual messages contain different messages in multiple languages for the same notification. Before you can use such a message you must define it in the *Global configuration* section of the policy. When you select a multilingual notification message, DriveLock displays the text in the language of the currently logged-on user.

Click a message and then click **OK**.

If you use this type of notification message, DriveLock displays a speech bubble icon near the top left corner of the text edit field.

To display the same message when a user connects a drive and the rule allows access, select the **“Also display message also when access is granted”** checkbox.

To not display any notification message when this rule is activated, including any default language message that you defined for all drives, select the **“Display no message when rule is activated”** checkbox.

To not generate any audit events when this rule is activated, select the corresponding check box.



Part VIII

Endpoint Detection and Response (EDR)



8 Endpoint Detection and Response (EDR)

Endpoint Detection and Response (EDR) allows you to monitor and configure all events that are related to DriveLock and its modules.

The basic functionality includes transmission of DriveLock events and the ability to respond to these events.

In addition, the separate EDR license provides you with further functionality:

- Monitor third-party events
- Define and use filters, alerts and responses
- Apply parts of the Application Control functionality
- Use parts of the MITRE Attack Framework, which is supplied as importable DriveLock rules.

For more information about MITRE Attack and Application Control, see the corresponding documentation on [DriveLock Online Help](#).

8.1 Event Transfer

Before you can audit DriveLock operations you must enable the transfer of DriveLock events. Events can be saved to a Windows Event Log, sent by SNMP or e-mail (SMTP) or copied to the central DriveLock database.

There are two event sources that you can configure together:

- DriveLock Agent events (source: *"DriveLock"*).
- DriveLock Management Console events (source: *"DriveLockMMC"*)

The recommended tool for analyzing DriveLock events is the DriveLock Control Center with its flexible, powerful and easy-to-use sorting, filtering and grouping capabilities. You can also monitor DriveLock events by using an event log consolidation tool, such as Splunk.

When storing event data in the central database, the events can be anonymized. This allows for compliance with legal requirements for keeping user-related data private. When you activate this feature, user and computer names that are part of the event data are encrypted and cannot be viewed or printed by regular administrators. Decrypting and viewing this data can only be done with the authorization of multiple individuals. For example, you could require a representative each from your legal department and your personnel department to perform the decryption.

8.1.1 Configuring Event Message Transfers

You can configure which DriveLock event messages to log and where to store them. If you configure a remote destination and the computer is not connected to the network, all messages are temporarily stored on the local computer.

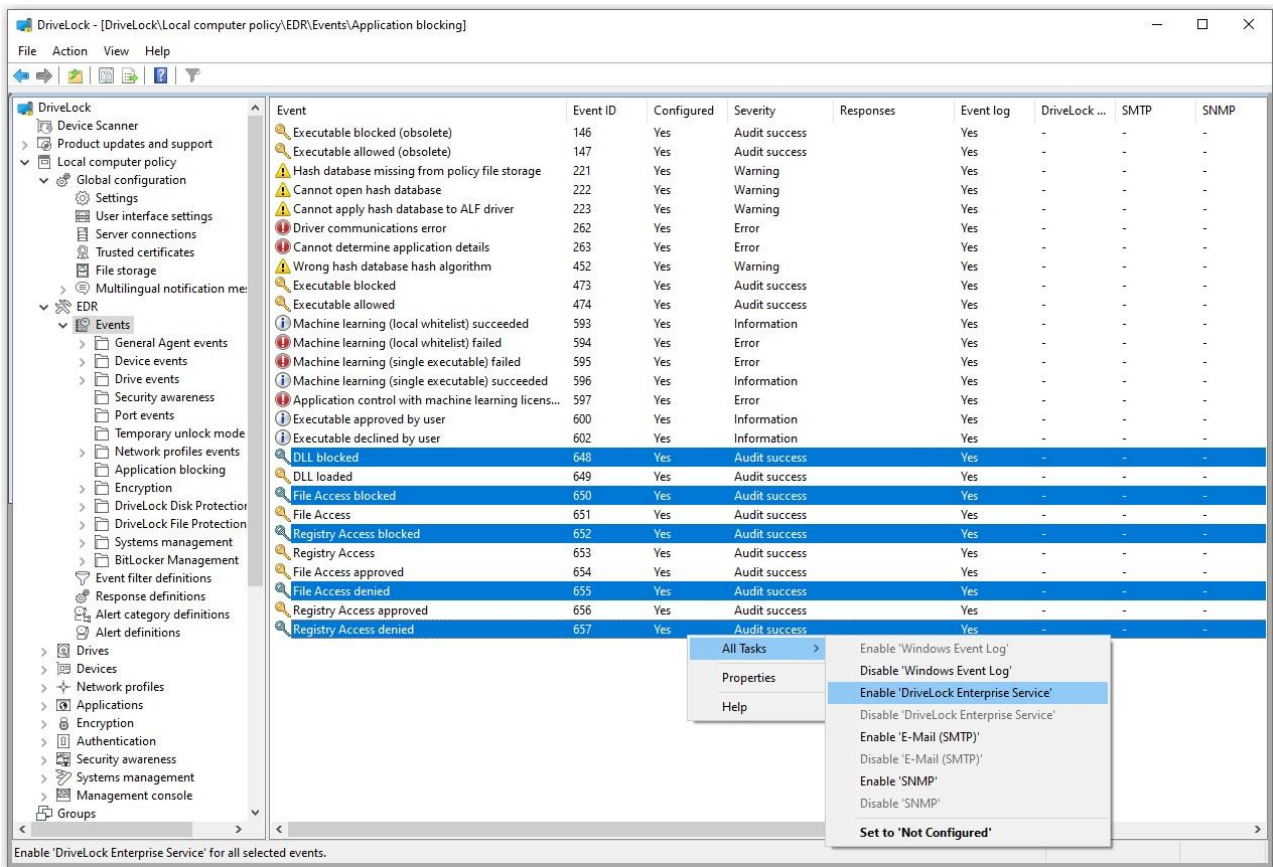
In the DriveLock Management Console, in the console tree on the left, open the **EDR** subtree, then the **Events** subtree. In this subtree all events are grouped according to the components that generate them. Selecting a node displays a list of available events in the pane on the right.

To change settings for a specific event, double-click it to open its **Properties** dialog. The **General** tab allows you to define where this event shall be sent (multiple destinations are possible) and if multiple occurrences in a short time interval should be suppressed to conserve space in the log file(s).

The destinations shown need to be further configured, which is described in section 7.2.

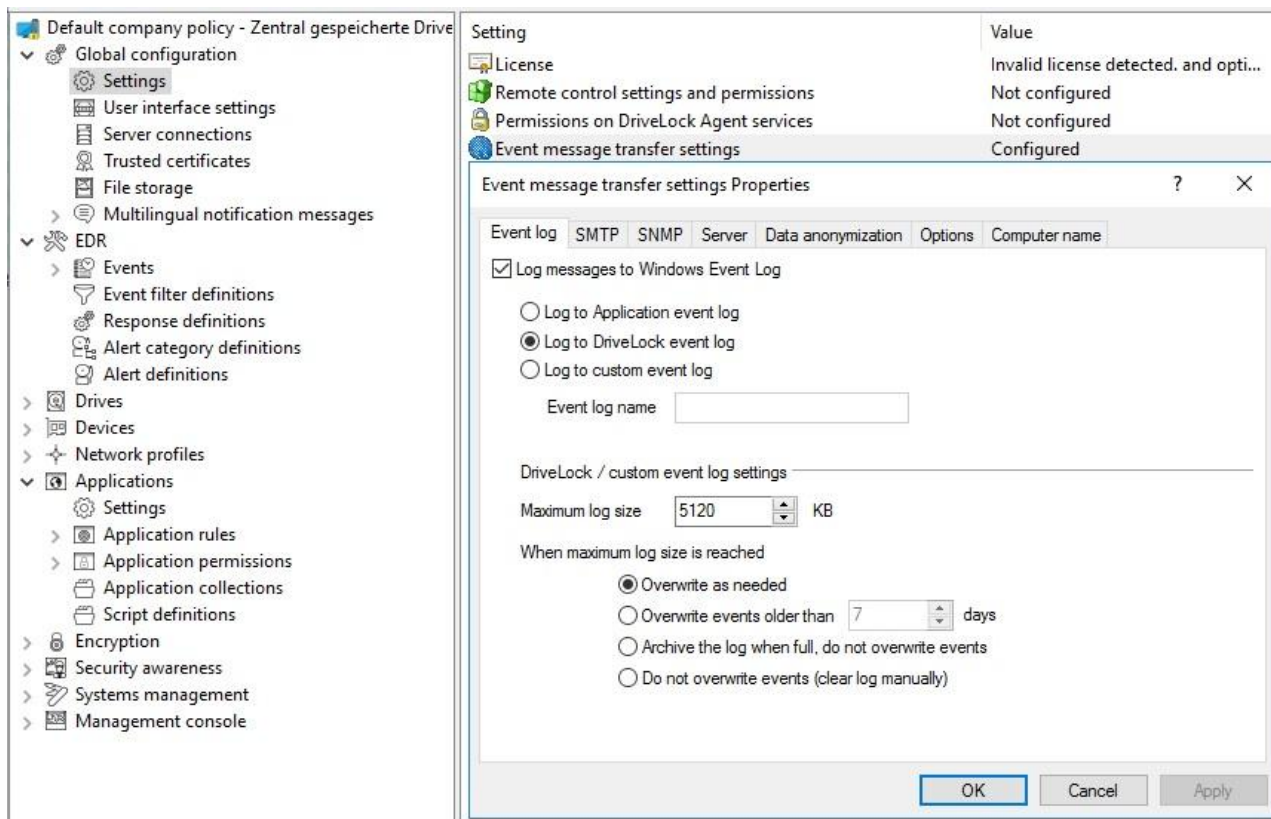
The **Responses** tab can be used to trigger a specific action when this event occurs. The action needs to be described as a Response Definition beforehand; refer to section 7.3 for details. The **Event info** tab shows the event message text and parameters in detail. This information is useful when creating event filters.

To quickly route multiple events to a destination, select them in the right pane (using Shift- and Ctrl-Click), then right-click on the selection. The context menu that opens contains a sub-menu **All Tasks**, which contains options to enable or disable each available event destination for all selected events.



8.1.2 Configuring Event Transfer Destinations

Each of the possible destinations where events can be sent requires different specific settings. To configure event transfer destinations, expand the **Global Configuration** node in the console tree on the left and select **Settings**. Then click on **Event message transfer settings** in the right-hand pane to open the settings dialog. The individual tabs of this dialog are described below.



8.1.2.1 Configure the event log destination

On the **Event log** tab, you configure which event log DriveLock uses to store the events locally.

These settings control whether the Agent sends events to the Windows Application Event Log or to another event log. If you don't use the common Application log, specify the size and the behavior when the DriveLock log file fills up.

8.1.2.2 Configure SMTP server settings

Select the **SMTP** tab to configure SMTP settings for sending event messages using e-mail.

Check **Enable SMTP event messages** to enable messages to be sent using e-mail. Provide information about your mail server, sender, recipient, etc. For successful delivery you also need to ensure that your e-mail server will accept messages with the settings you specify. If your mail server requires authentication you must also supply authentication data.

To configure the content of e-mail notification messages, click **Message text** and complete the information in the dialog box. Click the > buttons to insert placeholders for event-specific parameters into the subject line or body of the message. You can also select the option to send the message as HTML mail instead of plaintext.

Click **OK** to accept the format of the message.

Click **Test** to send a test e-mail to the recipients you specified. After a short time, a notification will appear, informing you whether all settings were specified correctly to send e-mail messages.

8.1.2.3 Configure SNMP server settings

On the **SNMP** tab, check **Enable SNMP trap messages** to activate event log message transfer using SNMP, and then type the destination information.

8.1.2.4 Configuring Enterprise Service connection settings

On the **Server** tab, check **Enable event forwarding to DriveLock Enterprise Service** to activate event message transfers to the DriveLock database.

Select the **Report Agent status to server** checkbox and choose the time interval for sending status messages. By default, the DriveLock Agent sends status messages to the server every 300 seconds. Note that the server connection needs to be configured under **Global Configuration / Server Connections**.

8.1.2.5 Additional Event Transfer Options

The **Settings** dialog provides a few more tabs with settings that apply to more than one of the available event transfer destinations.

8.1.2.5.1 Anonymizing event data

In some jurisdictions, such as Germany, the use and storage of personally identifiable data is tightly regulated. Regulations and legal requirements may also apply to such data when it could be used for surveillance of user activities.

To enable organizations to comply with privacy laws, DriveLock includes functionality that can prevent an administrator or company management from using event data to track the activities of specific users. The DriveLock Agent can anonymize user and computer names in event data, for example data it sends to the DriveLock Enterprise Service. This is done by encrypting these fields in events. You configure the settings for this on the **Data anonymization** tab.

By default, the data for each DriveLock event contains the name of the computer and the name of the user. This data is transmitted over the network if you send event data to the DriveLock Enterprise Service. You can change this by configuring the following settings for user account data, computer account data or both:

- **Encrypt information:** User name and/or computer name are encrypted using one or more public keys before data is transmitted. If needed, the data can be decrypted using the DriveLock Control Center. This setting enables specific events to be tied to a user or group when the need for this arises at a later point.
- **Do not store any information:** User name and/or computer name are not transmitted. This setting completely prevents specific events to be tied to a user or computer.

Only event data that is transmitted to the DriveLock Enterprise Service can be decrypted later. Encrypted fields in events that were transferred using SMTP or SNMP cannot be decrypted later.

If you activate encryption for one or both fields you also need to specify at least one certificate. The keys that are associated with these certificates will be used to encrypt and decrypt user and computer fields in events.

Click the **Add** button and **Select existing** to add an existing certificate, or click **Create new** to generate a new certificate. If you choose to create a new certificate, the Event encryption certificate creation wizard starts.

Click **Next**, then select a folder to which the certificate will be saved or select to store the certificate and associated private key on a smartcard. Certificate files are always stored using the same file names: `DLEventEncrypt.cer` for the certificate file, `DLEventEncrypt.pfx` for the PKCS#12 file that contains both the certificate and the matching private key. If you want to store two certificates in the same folder you need to rename these files before creating the second certificate. If you try to save a certificate in the same folder where another identically named certificate already exists, the wizard warns you and requires you to select a different location for the certificate files.

Click **Next**. If you selected a smartcard for storing the certificate you will be prompted to select or insert the card.

For technical reasons, the smartcard or token you use needs to allow exporting the private key of a certificate. Without this functionality it will not be possible to decrypt data at a later time. If you are not certain whether your smartcard supports private key exporting, conduct a test before encrypting production data.

Store the certificate (.pfx) files or smart cards in a secure location to ensure that they will be available when you need to decrypt event data in the future. If one of the certificates is lost, decryption is no longer possible!

Type a password that will be used to prevent unauthorized access to the certificate's private key, i.e. to the `DLEventEncrypt.pfx` file. Confirm the password and then click **Next**.

To ensure that you will not forget the password in the future, consider storing it in a secure location, such as a safe.

When the certificate files have been created the wizard displays a confirmation.

If you store the certificate and its keys on smartcard you are prompted for the smartcard's PIN.

Click **Finish**.

After you created the certificate it appears in the certificate list. You can create additional certificates. When you configure multiple certificates, all of them are used for decrypting event data and all of them are also required for decrypting this data. This lets you implement policies that require multiple individuals to perform the decryption. For example, you could require someone from both the personnel department and the legal department to perform the decryption. To do this you would need to configure two sets of certificate files and hand one to each department's representative.

To view additional information about a certificate, select the certificate and then click **Properties**.

When you create a certificate, it is also stored in the certificate store of your Windows user account.

Because all certificates and associated private keys are also stored in the Windows certificate store of the user who created them, you may need to delete one or more certificates from this store to implement a policy that requires multiple individuals to jointly perform the decryption.

The selected fields will be encrypted as soon as you accept the settings and DriveLock Agents receive the updated policy.

For information about decrypting event data, refer to the *DriveLock Control Center Manual*.

8.1.2.5.2 Transfer options

Click the **Options** tab to define how DriveLock processes DriveLock Enterprise Service messages when the client is offline. Event messages can be temporarily stored locally if the DriveLock agent is unable to deliver them to the configured destination.

Select **Queue events when offline** to enable temporary storage of messages. DriveLock Agents always use an internal memory-based queue to temporarily hold events when they are generated faster than they can be processed. In addition, you can configure the Agent to store events in a disk-based queue when the Agent is offline and cannot contact the DriveLock Enterprise Service. Events are automatically deleted from both queues once they have been processed. You can configure the maximum number of messages these queues will hold. If either queue exceeds the limit you configured, additional events are no longer forwarded to the DriveLock Enterprise Service and only written to the local event log.

Normally each Agent transmits event data in real time to the locations you configured. In system environments where available network bandwidth is limited, the DriveLock Agent can collect events and send multiple events

together in batches. To activate this setting, select the **Send events in batches** checkbox and configure a packet size and interval suitable for your network environment.

8.1.2.5.3 Customizing the reported computer name

If you do not want the standard Windows computer name reported as the origin for an event, the **Computer Name** tab provides several options to customize the name used. The computer name can be retrieved from a registry key, an INI file, or even provided by a custom DLL that returns the name. Select the applicable radio button and enter the information required for the option chosen.

8.2 Event Responses

In addition to simply sending event messages to various destinations, the DriveLock Agent can also initiate a local event response when the event occurs. Such a response can be the execution of a program or script, or taking a photo using a webcam connected to the system. Responses can be used with individual events (see section 7.1) and Alerts (section 7.5) after they have been defined and named.

To create a new response definition, navigate to the **Response definitions** node under the **EDR** node of the policy. Right-click on **Response definitions** and select **New...** from the context menu. The following Response types are available:

- **PowerShell script:** Executes a named PowerShell script with optional parameters from the event the response relates to.
- **Batch script:** Executes a batch script using the standard command processor, with optional parameters.
- **Command line execution:** Starts an arbitrary executable file, with optional parameters.
- **Show awareness campaign:** Displays a defined awareness campaign when the event occurs.
- **Take picture using webcam:** Takes a photo when the event occurs and transfers it with the event. This option should be used with care, as it can quickly use a lot of storage space if it is triggered too frequently.

Responses are defined using a tabbed dialog. The **General** tab allows setting a name and an optional comment for the response.

The **Script** or **Command line** tab is used to assemble the command or script to be executed, including any parameters. The command line can simply be typed into the text box or created by selecting an executable/script and any parameters required. However, to use the **Insert parameter** button, parameters need to be defined first on the **Parameters** tab.

For all response types a set of options is available to define conditions for use: The **Computers**, **Networks**, and **Time Limits** tabs can be used to enable or disable the response if certain conditions are met. This could e.g. be used to trigger the response only on certain computers while they are connected to the company network and the event occurs outside regular office hours.

When all settings are complete, click **OK** to save the response definition. It is added to the list of response definitions on the right, which is then used to provide a selection of responses to events and alerts (see 7.5 below).

8.3 Event Filters

Event filters can be used to select certain instances of an event based on the event parameters; events often contain additional information besides the event number and message. This information can be used to distinguish instances of an event that are of interest from those that are not. By defining event filters separately, they can quickly be reused in rules requiring a selection of events.

To create an event filter, right-click on the **Event filter definitions** sub-node of the EDR node and select **New...** from the menu. A list of available events is displayed. Select the event this filter will apply to and click **OK**.

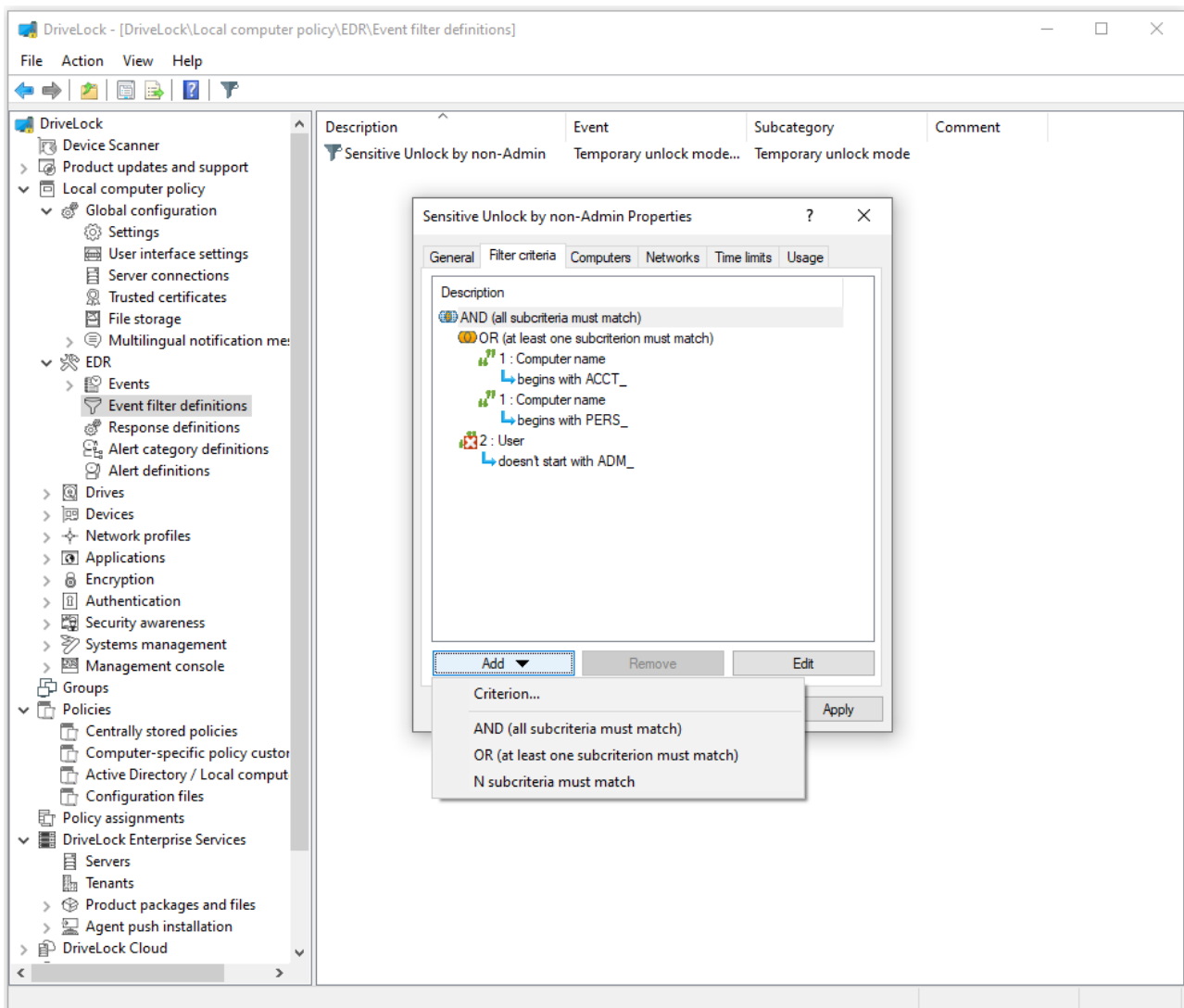
A tabbed settings dialog is displayed. On the **General** tab a name for the filter can be entered in the **Description** field – this is the name that will be displayed in the event filters list after the definition is saved.

The **Filter criteria** tab is used to specify how the various instances of the event are to be filtered. With the **Add** button, criteria and logical operators can be inserted into the filter specification displayed in the box. The available criteria vary with the event type, depending on the additional information logged with the event. The logical operators can be used to combine multiple conditions for event selection.

To describe a condition, start by adding an operator. The following operators are available:

- **AND:** All the criteria associated with this operator must match
- **OR:** At least one of the criteria associated with this operator must match
- **N:** At least n criteria of the listed (more than n) criteria associated with this operator must match. The number n is selected when adding the operator.

To associate a criterion with an operator, select the operator in the list, click **Add**, and select **Criterion**. From the list of event parameters that appears, select one and click **OK**. In the next dialog the criterion is completed by selecting a comparison or match operator and one or more value(s) to compare against. To add the criterion to the filter description, click **OK**.



Operators and conditions can be changed by selecting them and clicking the **Edit** button.

The **Computers**, **Networks**, and **Time Limits** tabs can be used to enable or disable the use of the filter on certain computers connected to specific networks during certain time periods.

When all settings are complete, click **OK** to save the filter definition. It is added to the list of event filter definitions on the right.

8.4 Alerts

Alerts are a means to generate a meta event if e.g. certain combinations of events occur within a short time interval. Instead of looking for patterns in event logs, an alert definition can be used to detect and immediately report such a pattern. In addition to reporting the detection, an alert can also initiate an Event response (see section 7.3).

To create an alert definition, right-click on the **Alert definitions** sub-node of the **EDR** node and select **New...** from the menu. A tabbed settings dialog is displayed.

On the **General** tab a name for the alert can be entered in the **Description** field – this is the name that will be displayed in the alert definitions list after the definition is saved. Furthermore, a **Severity** and **Alert category** can be set to better organize alert reports in the DriveLock Operations Center. Alert categories need to be defined in the **Alert categories** sub-node of the **EDR** node and are maintained on the server.

On the **Conditions** tab the criteria for raising the alert are defined. Use the **Add** button to add logical operators and criteria that describe the condition(s) for the alert.

The simplest condition that can be used for an alert is the match against a single event filter. To do this, simply click **Add**, **Criterion**, and select the proper event filter from the list.

It is also possible to combine multiple event filters: Start by adding one of the logical operators **AND**, **OR**, or **N** (refer to 7.4 for a description of these operators). Then, select the operator in the conditions list and click **Add** again to start adding criteria the operator shall apply to. Selecting **Criterion** opens the event filters list for selection of a filter to be included in the condition. Continue adding a Criterion until all required event filters are listed under the selected operator. Be sure to choose a suitable time window in the **Events must occur within ... seconds** field to prevent the condition from matching completely unrelated events and raising false alerts.

On the **Responses** tab an immediate response can be set up in addition to reporting the alert. In the **Response to execute** drop-down select a response from the response definitions list. The parameter definitions for this response are displayed in the **Parameter mapping** list. Select a parameter and click the **Edit** button to customize the parameter value to use in this alert if the value in the response definition is not suitable.

The **Computers**, **Networks**, and **Time Limits** tabs can be used to enable or disable the use of the filter if certain conditions are met.

When all settings are complete, click **OK** to save the definition. It is added to the list of **Alert definitions** on the right.



Part IX

Locking Drives and Devices



9 Locking Drives and Devices

As the product name implies, the core function of DriveLock is to lock drives and devices. This section describes how to configure all settings related to this function. Even though there are many different types of devices, DriveLock is easy to configure and once you get used to the basics, you will be able to easily configure how to control the use of any type of device.

9.1 Locking Drives

This manual uses a local policy to illustrate the steps required to lock all USB-connected drives, to enable the use of selected flash drives and to introduce the functionality of file filters and shadowing. Most steps also apply to other types of drives. Any such differences will be pointed out along the way.

Configuring Agents by using a Group Policy or a configuration file uses the same settings as those used in a local policy. There are no differences between these methods, except in how you deploy the settings to the Agents.

It is important to understand how DriveLock uses whitelist rules. After activating locking for a drive type, any drive of this type is blocked (the “drive firewall” is up and running and nothing is allowed to pass through). To define any exception to the blocking of drives you need to create whitelist rules. You must define a whitelist rule for each drive (or groups of similar drives) that you need to use on a computer. If a drive is not recognized by the DriveLock Agent as being listed in a whitelist rule, DriveLock blocks the drive and it can’t be used. This ensures that any new drives that are introduced into your network by users are automatically blocked until you explicitly allow their use.

Based on this basic principle, to complete a DriveLock configuration you should first create any required whitelist rules and then enable the locking of drives and devices.

Drives, such as USB-connected drives, are locked by default. If you install a DriveLock Agent on a computer with no DriveLock policy configured, this default setting applies.

Whitelist rules define which drives are accessible even while other drives of the same type can remain locked. To allow for maximum granularity without unnecessary administrative overhead, you can define drive whitelist rules for different scopes of drives (rules are evaluated starting with rules that have a broad scope, continuing towards more detailed rules:

- Drive Class (for example, all floppy disks)
- Size of the drive (for example, all drives larger than 128 MB)
- Vendor (for example, SanDisk)
- Product ID (for example, Ultra II 1 GB Compact Flash)
- Unique drive serial number

In addition to the scope you can specify conditions for when and where a whitelist rule applies:

- Does it apply to all computers or only to certain computers?
- In which defined network location is the rule activated?
- At what time is the rule active? (For example, only on Monday to Friday and between 9 A.M. and 6 P.M.)
- Does the rule apply to all users, or are only certain users allowed to use this drive?
- Must a user confirm a usage policy before getting access?

- Has a drive been encrypted by DriveLock?
- Is the Antivirus service running?
- Which user is currently logged on?
- Does the drive contain malicious software?

By using scopes and conditions, you can minimize the number of rules needed to implement your policy.

To enable policy enforcement for most types of drives you also need to enable locking for the drive class (i.e. you have to activate the “drive firewall”). This is covered in chapter [“Enabling Drive Locking”](#).

During an evaluation of DriveLock you may enable drive locking first and afterwards define some whitelist rules to enable specific drives. In a production environment it is recommended to create all required whitelists rules before activating drive locking.

DriveLock settings may conflict with three Windows Group Policy settings. The symptom of this incompatibility is that users can access USB-connected drives that are blocked by a DriveLock policy. The following three settings are located under **Computer Configuration -> Windows Settings -> Security Settings -> Local Policies -> Security Options**:

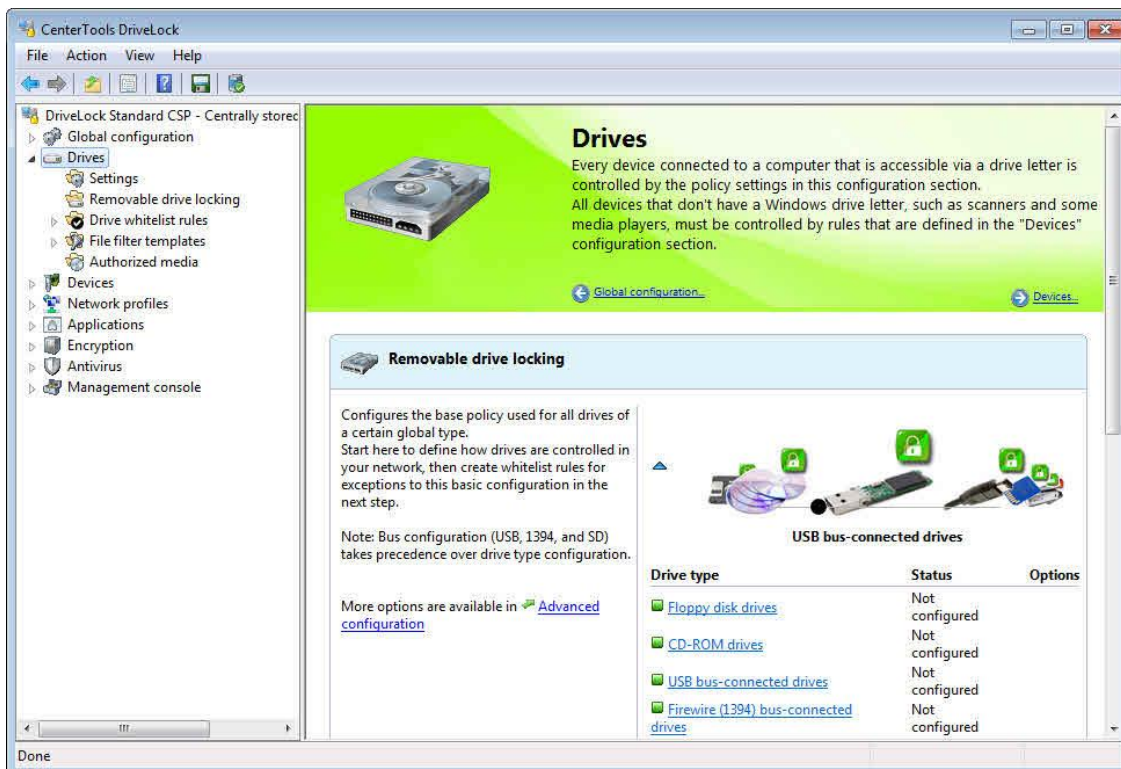
- *Devices*: Allowed to format and eject removable media. Conflicting settings: Administrators and Power Users, Administrators and Interactive Users.
- *Devices*: Restrict CD-ROM access to locally logged-on user. Conflicting setting: Enabled.
- *Devices*: Restrict floppy access to locally logged-on user. Conflicting setting: Enabled.

DriveLock checks these Group Policy settings and creates an entry in the Windows Application Log if any of them are present.

DriveLock recommends that you don't change these Group Policy settings from their defaults to ensure that drive control policies work as expected.

9.1.1 Configuring Drive Locking In Basic Configuration Mode

DriveLock Basic configuration mode lets you easily configure basic drive locking settings.



Click **Drives** to switch to the drive locking task view. It has two sections:

1. Removable drive locking: used to configure the base policies for certain drive classes.
2. Whitelist rules: used to configure whitelist rules that define exceptions from the base rule for specific devices.

Click **Advanced configuration** at any time to configure additional and more advanced drive locking settings. (Refer to the chapter [“Configuring Advanced Drive Locking Settings”](#) for more details.)

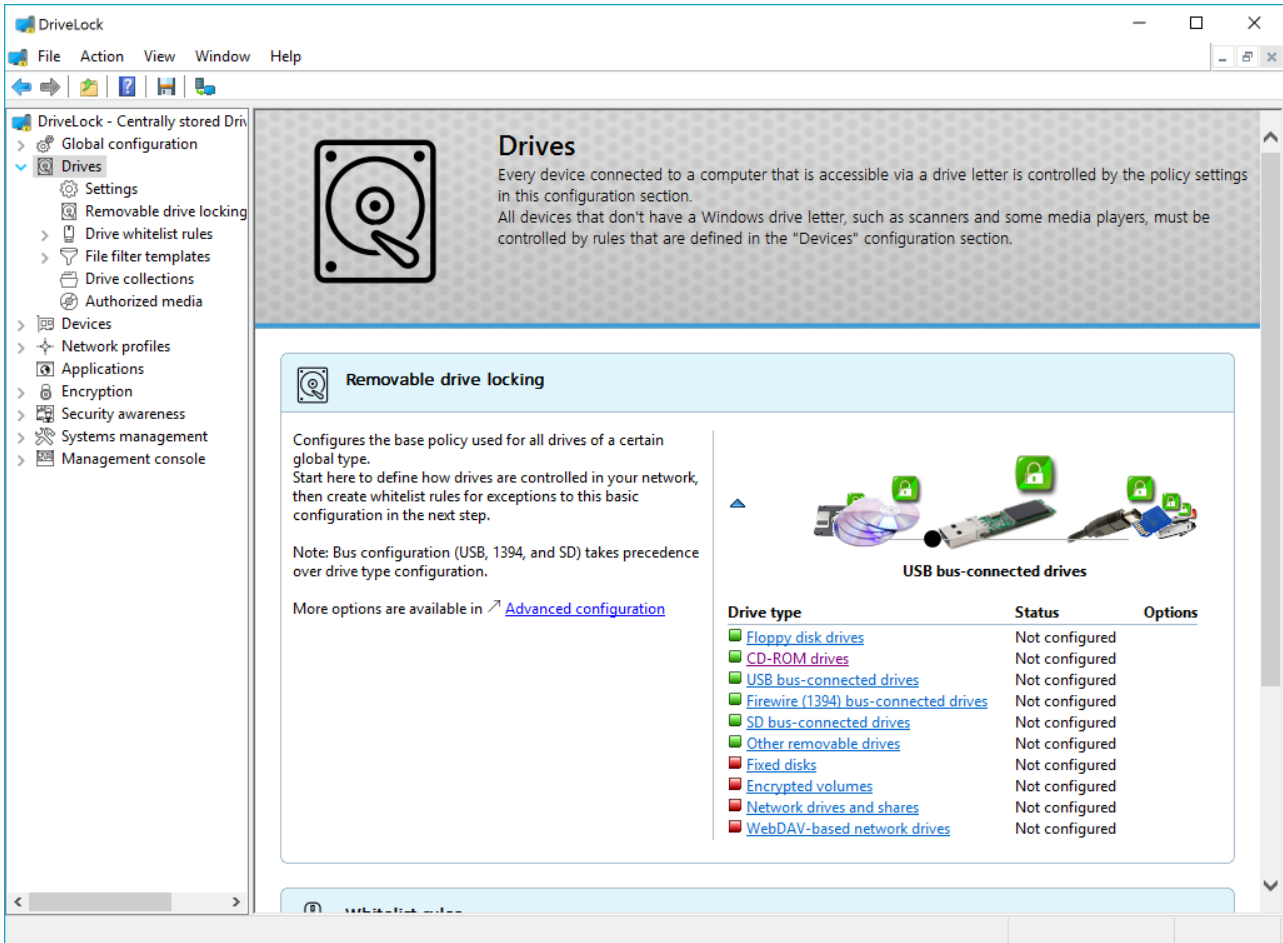
9.1.1.1 Enabling Drive Locking

DriveLock can detect all types of drives which Windows recognizes as removable drives or fixed disks. This includes the following types (classes):

- Floppy disk drives
- CD-ROM/DVD drives
- USB bus-connected drives
- FireWire (1394) bus-connected drives
- SD bus-connected drives (for example, built-in SD card readers)
- Fixed disks (for example, eSATA bus-connected drives)
- WebDAV-based drives
- Network drives and shared folders

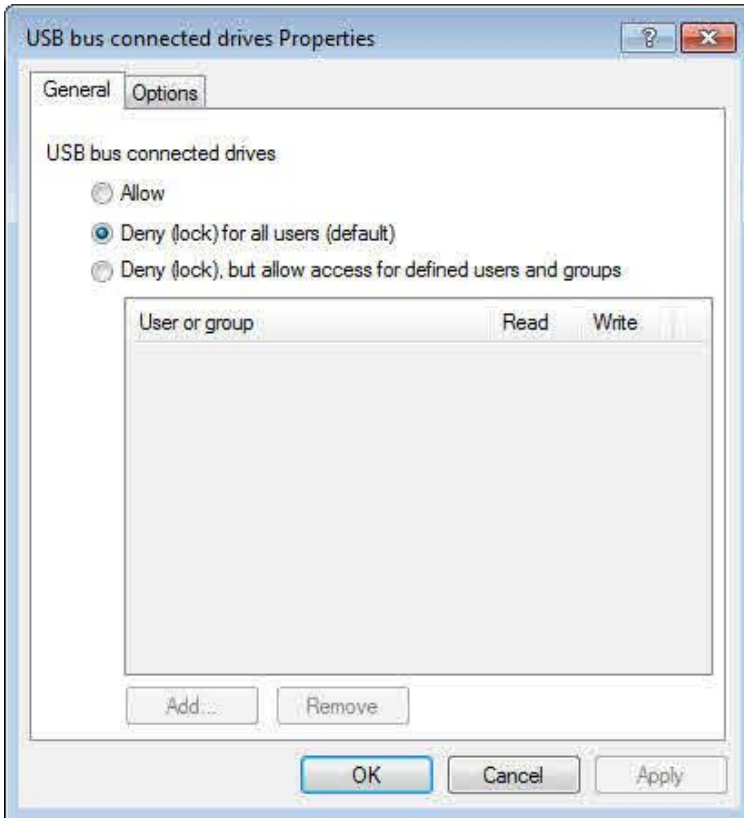
Boot partitions and partitions containing the Windows page file are never blocked.

If a removable drive is connected by using another interface, DriveLock treats it as the type **“Other removable drive”**. DriveLock can also lock CD/DVD drives that have CD/DVD burning capabilities.



To change settings for a drive type (for example, USB bus-connected drives), click the appropriate link. You can also use the slider in the task view to highlight one of the drive icons and then double click the highlighted icon.

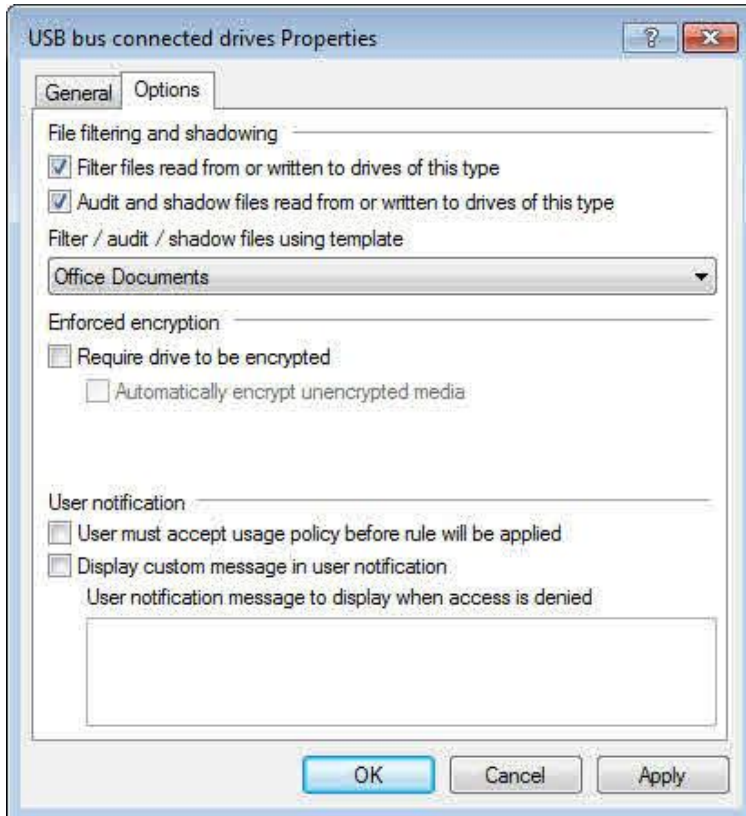
A dialog appears, displaying the current configuration setting.



Select one of the following options:

- *Allow*: Any authenticated user can access this drive.
- *Deny (lock) for all users*: Nobody can access this drive, it is completely locked.
- *Deny (lock), but allow access for defined users and groups*: The drive is locked, but the specified users or groups are allowed to use the drive either in read only mode or with write permissions.

Select the **Options** tab.



To filter access to files based on the file type and to audit file access you must enable file filtering and/or auditing and then specify a template that defines the filtering and auditing settings.

Select **“Filter files read from ...”** to enable file filtering. Select the **“Audit and shadow files...”** checkbox to enable auditing and shadowing. Select one of the built-in file filter templates that are available in Basic configuration mode to define how these functions are performed.

Select the checkbox **“Require drive to be encrypted”** to control whether removable drives must be encrypted.

If you select this option, DriveLock lets users only access encrypted removable drives; unencrypted drives are locked. You can also select whether a user will be prompted to encrypt an unencrypted removable drive when the user connects it to the computer.

If the option *“Automatically encrypt unencrypted media”* is selected and a user connects an unencrypted removable drive that already contains files, you can configure whether existing files will be retained or deleted under the settings for enforced encryption.

To have the user accept a usage policy before granting access, activate the **“User must accept usage policy before rule will be applied”** checkbox.

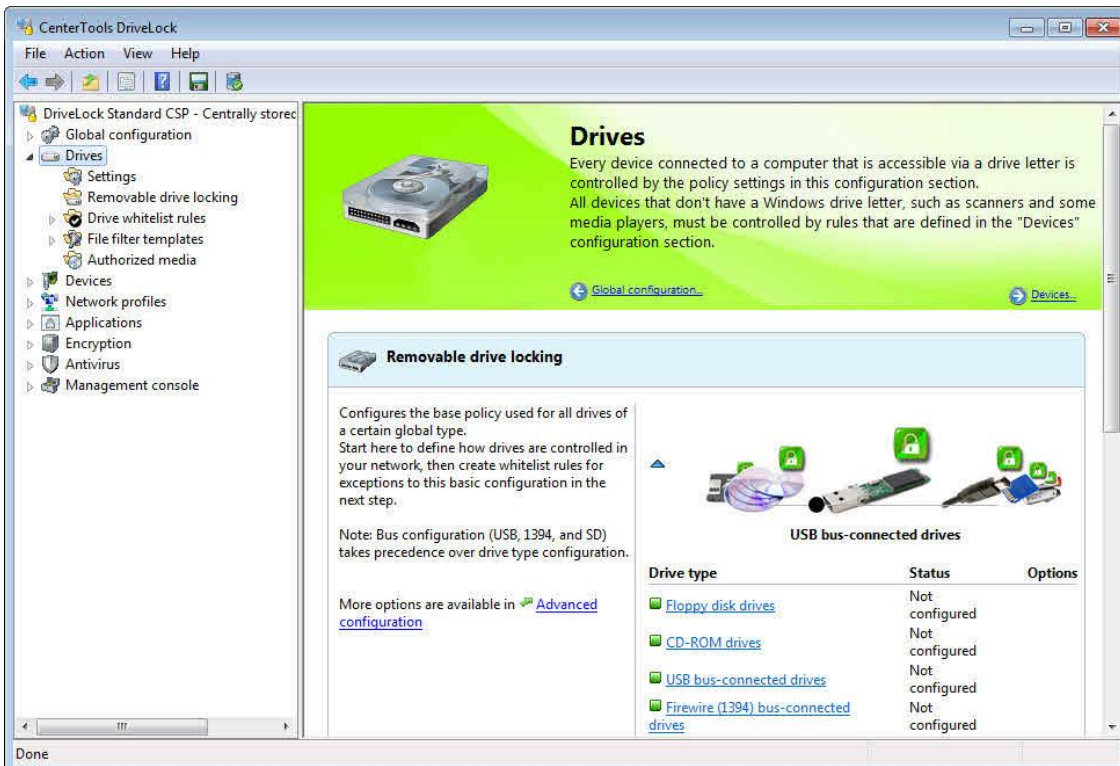
Select the **“Display custom message in user notification”** checkbox to display a custom notification message when a user connects a drive and DriveLock blocks access to the drive.

In the text edit box, type the message. DriveLock will display this message regardless of the client computer’s language setting.

Click **OK** to save the configuration.



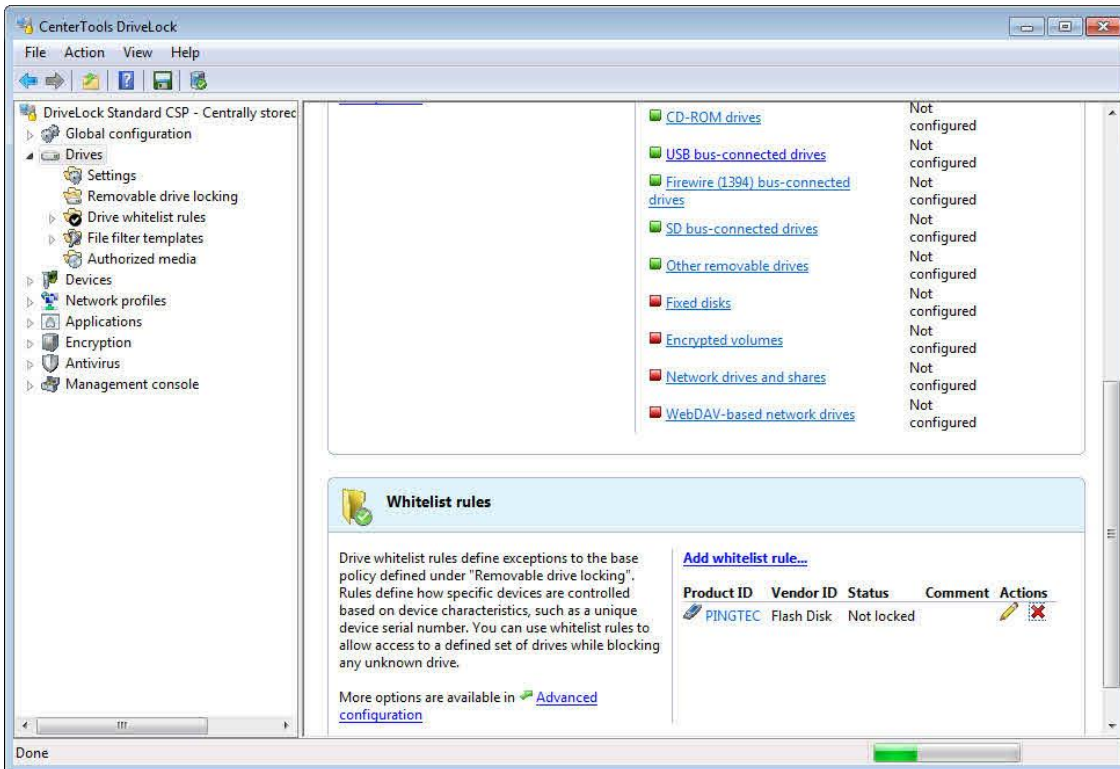
A popup window appears, displaying the new settings. Click **X** to close the window.



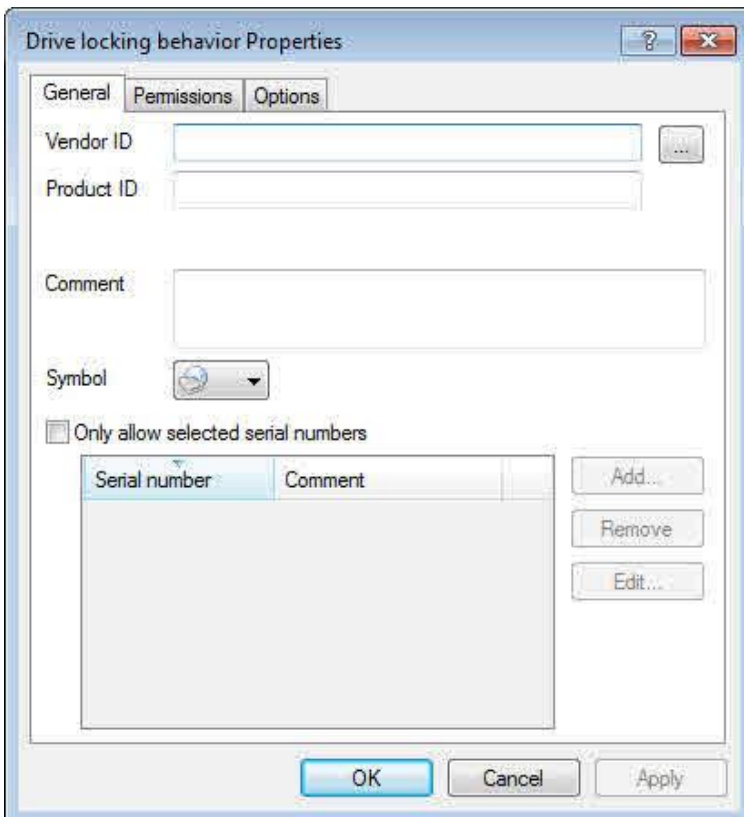
The colors of the drive type icons indicate the security level of your current configuration:

- *Green icon*: this drive type is locked for all users (high security level).
- *Yellow icon*: this drive type is locked for some users and unlocked for others (medium security level).
- *Red icon*: this drive type is unlocked for all users (low security level).

9.1.1.2 Configuring Basic Whitelist Rules



Click **Add whitelist rule** to add a new whitelist rule.

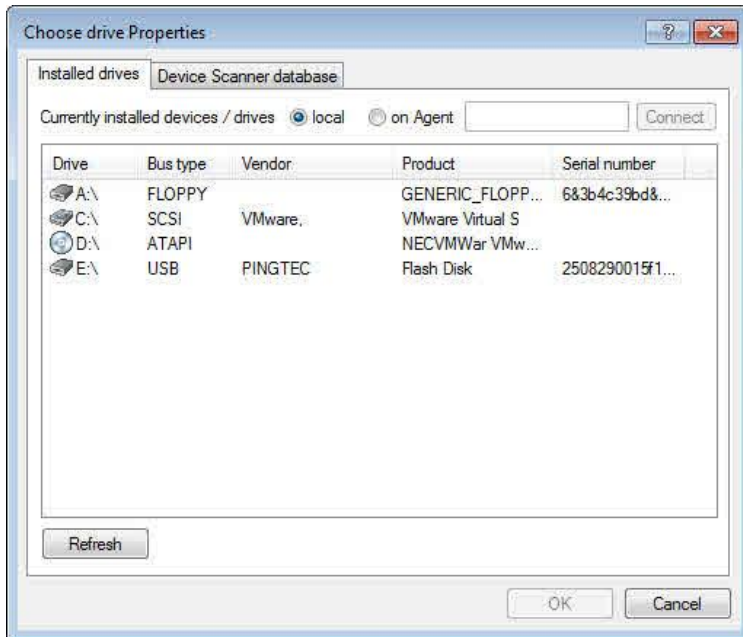


Each drive contains identifying information in its firmware, such as the manufacturer, product name and serial number:

- Vendor ID: Name or abbreviation of the drive manufacturer.
- Product ID: Model name, as defined by the manufacturer.

If you don't know the identifying information of a drive, you can select the drive by clicking the "..." button next to **Vendor ID**. You can use wildcards, like "?" (one character) or "*" (any number of characters) as part of the Product ID or Vendor ID.

DriveLock will display a dialog box that you can use to select a drive that is currently attached to the administration workstation, to a client computer, or that is listed in the Device Scanner database. DriveLock automatically adds the serial numbers of drives you add using this method to the dialog box.



To add a locally attached drive, select this drive and then click **OK**.

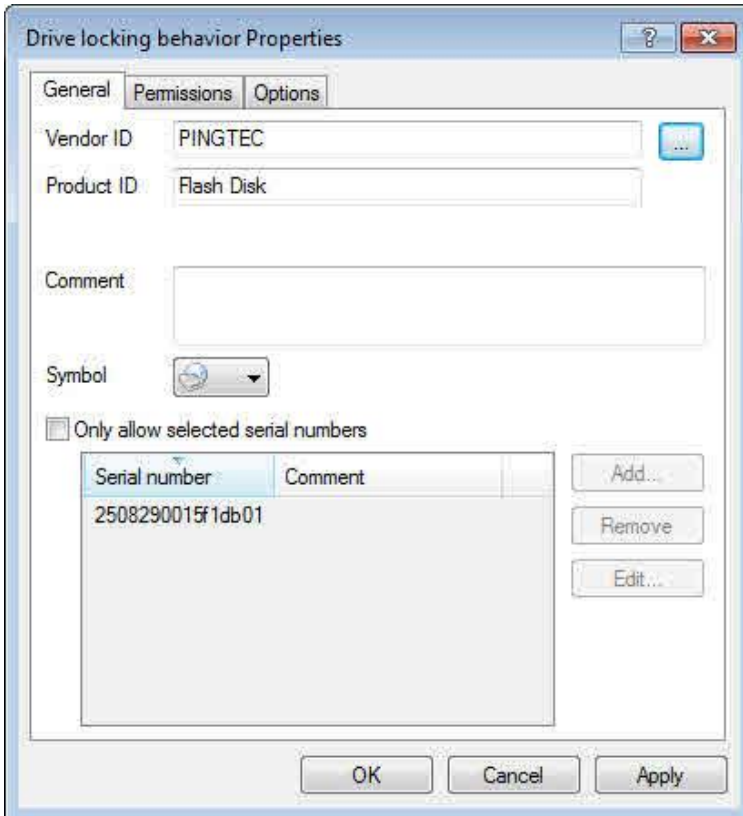
If you need information about other drives, you can connect to a remote client computer and select a drive that is connected it. Select **on agent** and then type the name of the computer to connect to. This requires that the DriveLock Agent is installed and running on the remote computer.

DriveLock reads the hardware information for the drive from Windows. Therefore DriveLock can only display the drives in the format in which they appear to Windows.

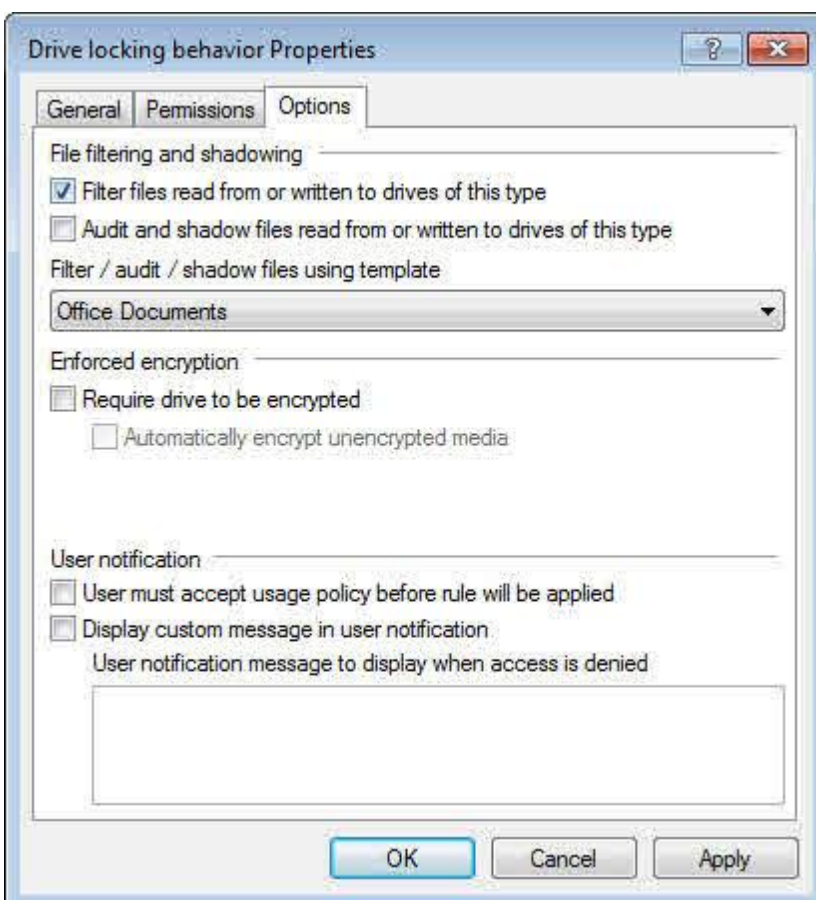
To establish a connection to a remote computer running Windows XP SP2 or higher with the Windows Firewall enabled, you must configure the firewall settings to allow incoming connections from TCP Ports 6064 and 6065 and the program "DriveLock".

When connecting to your local computer, removable drives that are blocked are not displayed. To view any blocked drives on your computer, select **on agent** and then type the name of your computer.

A convenient method to get drive information is to use the results from a hardware scan that has been completed in advance. To do this, on the **Device scanner database** tab, select the appropriate computer, vendor and product ID.



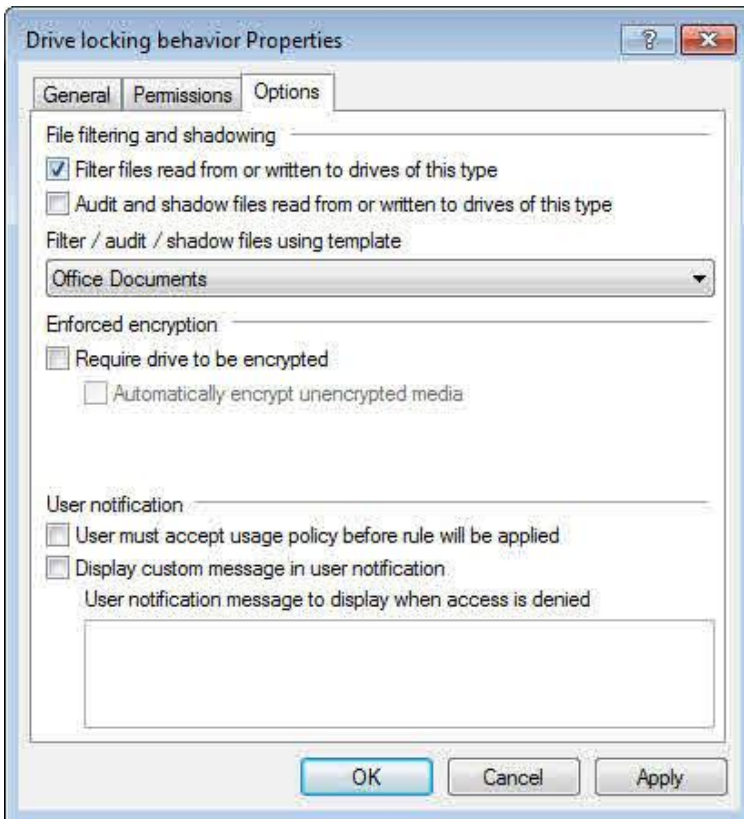
To configure user access, on the **“Permissions”** tab define how users can access the drive.



Select one of the following options:

- *Allow*: Every authenticated user can access this drive.
- *Deny (lock) for all users*: Nobody can access this drive, it is completely locked.
- *Deny (lock), but allow access for defined users and groups*: The drive is locked, but the specified users or groups are allowed to use the drive either in read only mode or with write permissions.

Click **Add** to add a user or group to the list, and then specify whether the user or group can copy files to the drive or only read data from it. To remove a user or group from the list, select the user or group and then click **Remove**.



Select the checkbox **“Require drive to be encrypted”** to control whether removable drives must be encrypted.

If you select this option, DriveLock lets users only access encrypted removable drives; unencrypted drives are locked. You can also select whether a user will be prompted to encrypt an unencrypted removable drive when the user connects it to the computer.

If the option *“Automatically encrypt unencrypted media”* is selected and a user connects an unencrypted removable drive that already contains files, you can configure whether existing files will be retained or deleted under the settings for enforced encryption.



The option **“Require drive to be encrypted”** is not available for CD drives.

To have the user accept a usage policy before granting access, activate the **“User must accept usage policy before rule will be applied”** checkbox.

Select the **“Display custom message in user notification”** checkbox to display a custom notification message when a user connects a drive matching the whitelist rule and the drive is locked.

In the text edit box, type the message. DriveLock will display this message regardless of the client computer’s language setting.

Click **OK** to save the configuration.

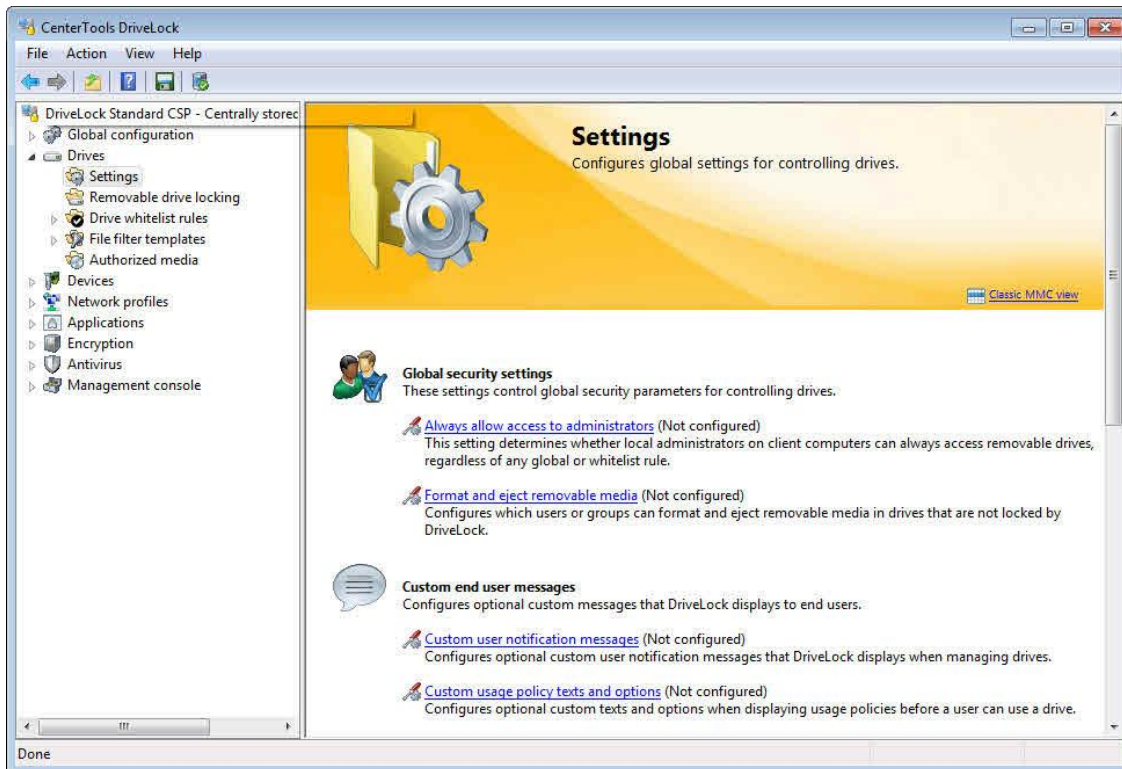
The task view can display up to 50 whitelist rules and some details of these rules. Click  to edit an existing whitelist rule. Click  to delete a rule.

9.1.2 Configuring Advanced Drive Locking Settings

In addition to the settings available in Basic Configuration mode, you can configure more detailed settings using the Advanced Configuration mode.

9.1.2.1 General Drive Locking Settings

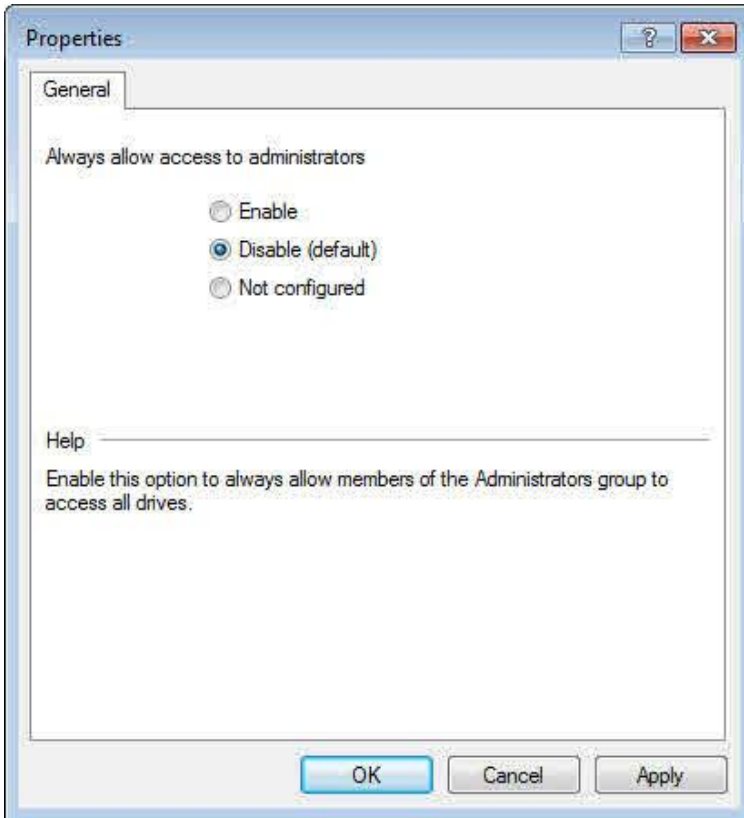
Several general settings apply to drive locking.



To configure these settings, under Drives, click **Settings**.

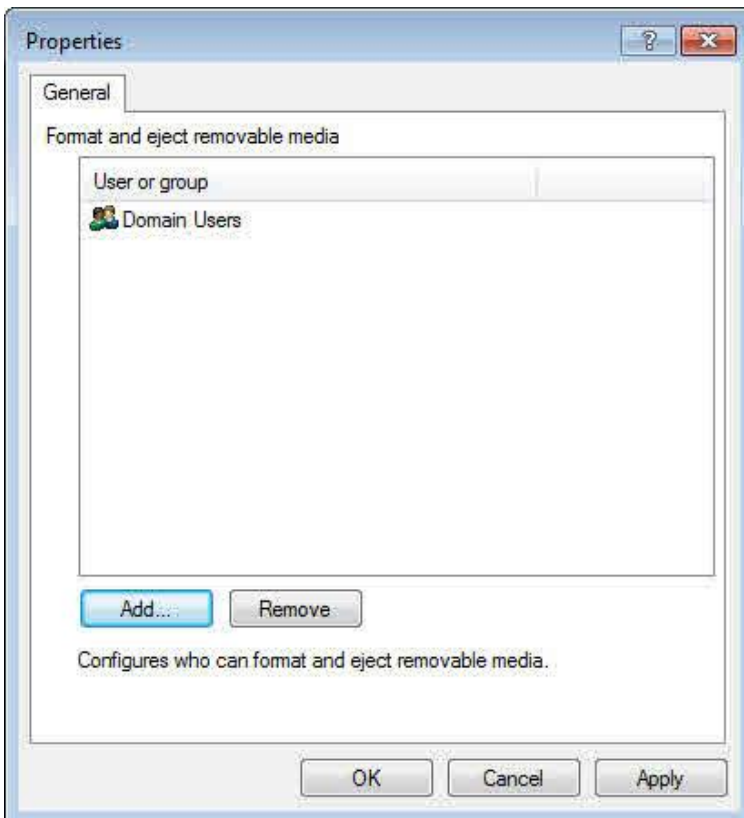
9.1.2.1.1 Global Security Settings for Controlling Drives

To enable access to locked drives for members of the Administrator group, regardless of whether a drive is locked due to a general configuration or a whitelist rule, click **Always allow access to administrators**.



Select **Enable** to enable this function.

To specify which users can format or eject removable media, click **Format and eject removable media**.



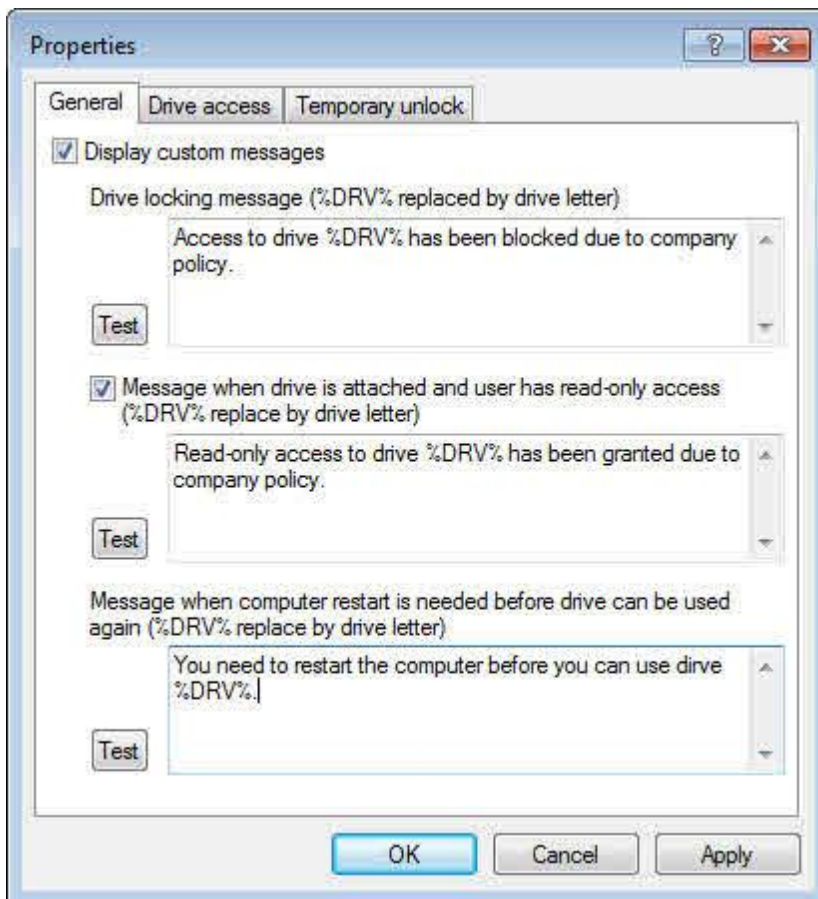
Click **Add** to add users or groups to the list. To remove a user or group from the list, click the user or group, and then click **Remove**.

9.1.2.1.2 Configuring End User Messages

9.1.2.1.2.1 Configuring User Notification Messages for Locking Drives

If you enabled user notification, DriveLock displays a notification message when a drive is connected to the computer and locked. To define the content of such messages, click **Custom user notification messages**.

If you have configured multilingual messages for the current language, DriveLock will display the standard messages defined for this language instead of the message configured in this dialog box.



Select the **“Display custom messages”** checkbox to enable the messages specified on this dialog box. The drive locking message is displayed each time a drive is locked by the Agent.

The messages configured on the **Drive access** tab are displayed each time access to a file or CD/DVD burning is blocked.



The other two messages configured on the **Temporary unlock** tab are displayed when an Agent is temporarily unlocked.

Type the message to be displayed to the user. Click the **Test** button to preview the notification message on your computer.

When the message is displayed, the Agent replaces the variables as follows:

- %DRV% will be replaced by the drive letter when the message is displayed.
- %PATH% will be replaced by the file path.
- %NAME% will be replaced by the file name (without extension).
- %EXT% will be replaced by the file extension.
- %REASON% will be replaced by an indication why a file has been blocked (for example, “wrong content”).
- %TIME% will be replaced by the current time or the number of minutes, depending on how an administrator selected the unlocking duration.

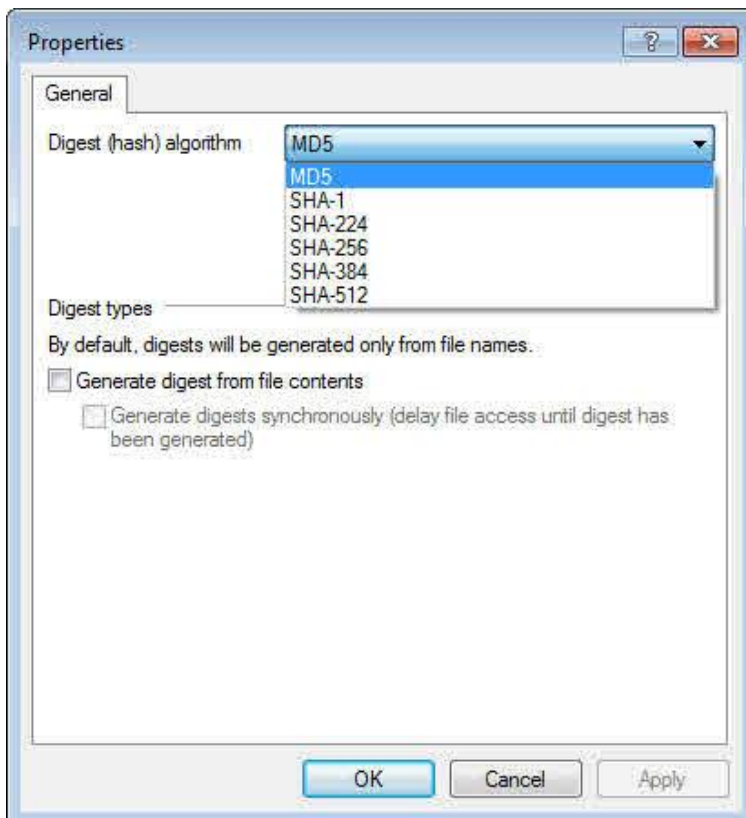
Click the **Test** button to preview the notification message on your computer.

You can use some HTML-tags (for example “Text”) to format your message.

9.1.2.1.3 Configuring File Digest Generation

Each time a file is copied from or to an external drive, renamed on an external drive or deleted on an external drive, DriveLock generates a hash value (digest) of its file name. This file name digest allows for the analysis of file transfer and file use on multiple computers throughout your network by using the DriveLock Control Center.

These settings determine the hash algorithm that is used and whether DriveLock generates an additional hash digest by from the entire file, including its content.



Select the digest hash algorithm from the drop down list. The MD5 hash algorithm is usually faster than any of the SHA algorithms, but your organization may require you to use a different algorithm.

To enable file content digest generation, select the “**Generate digest from file content**” checkbox and then select whether file access will be delayed until the content hash has been generated (hash generation will take some times for larger files) or whether DriveLock will generate the content hash asynchronously.

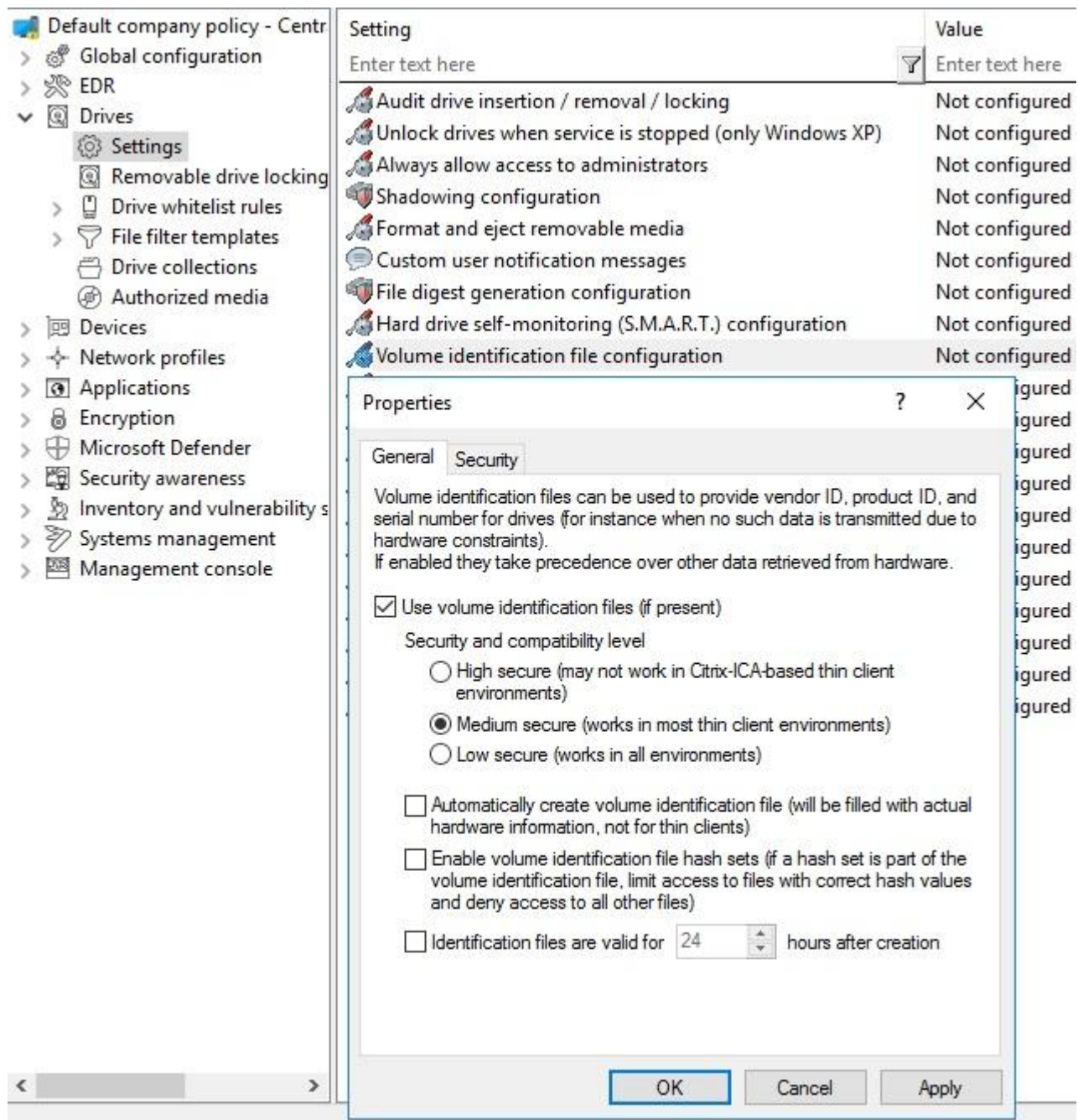
Click **OK** to save your settings.

9.1.2.1.4 Volume Identification Files

Storage media in most cases will be identified by a unique Vendor ID, Product ID and serial number. There are some storage media, like SD Cards or no-name USB sticks with no unique ID or the unique ID is not accessible when the storage media are connected via Thin-Clients (e.g. without DriveLock Virtual Channel) or when SD cards are used in an USB SD card reader.

Volume identification files can be created on such storage media, giving them a unique ID for DriveLock

To enable volume identification files, go to the Policy editor and open *Drives / Settings / Volume identification file configuration*



The screenshot shows the DriveLock Policy Editor interface. On the left is a tree view of policy categories, with 'Drives' expanded to 'Settings'. The main pane shows a list of settings, with 'Volume identification file configuration' selected. A 'Properties' dialog box is open, displaying the configuration options for volume identification files.

Setting	Value
Enter text here	Enter text here
Audit drive insertion / removal / locking	Not configured
Unlock drives when service is stopped (only Windows XP)	Not configured
Always allow access to administrators	Not configured
Shadowing configuration	Not configured
Format and eject removable media	Not configured
Custom user notification messages	Not configured
File digest generation configuration	Not configured
Hard drive self-monitoring (S.M.A.R.T.) configuration	Not configured
Volume identification file configuration	Not configured

Properties dialog box content:

General Security

Volume identification files can be used to provide vendor ID, product ID, and serial number for drives (for instance when no such data is transmitted due to hardware constraints).
If enabled they take precedence over other data retrieved from hardware.

Use volume identification files (if present)

Security and compatibility level

- High secure (may not work in Citrix-ICA-based thin client environments)
- Medium secure (works in most thin client environments)
- Low secure (works in all environments)

Automatically create volume identification file (will be filled with actual hardware information, not for thin clients)

Enable volume identification file hash sets (if a hash set is part of the volume identification file, limit access to files with correct hash values and deny access to all other files)

Identification files are valid for hours after creation

Buttons: OK, Cancel, Apply

Check *Use volume identification* and if a volume identification file is present the ID from the file overrides the hardware ID of the storage media.

Security and compatibility level:

- *High secure*: the volume ID must correspond to the volume serial number of the partition. If the volume ID file is copied to a different partition, the volume ID is invalid. Certain ICA based clients (Citrix Clients) do not send the volume serial number to Windows, then the volume ID cannot be verified by DriveLock.
- *Medium secure*: the volume ID must correspond to the size of the partition. The volume ID is invalid, if the volume ID file is copied to a partition of different size.
- *Low secure*: a volume ID file can be copied to any other partition. DriveLock will accept the volume ID independent from volume serial number and volume size. Only use this option if your thin client does not send the volume serial number and not the volume size.

The volume information file includes all three security levels. Always start with *high* and reduce it only, if required. Existing volume information files remain valid if the security level is changed.

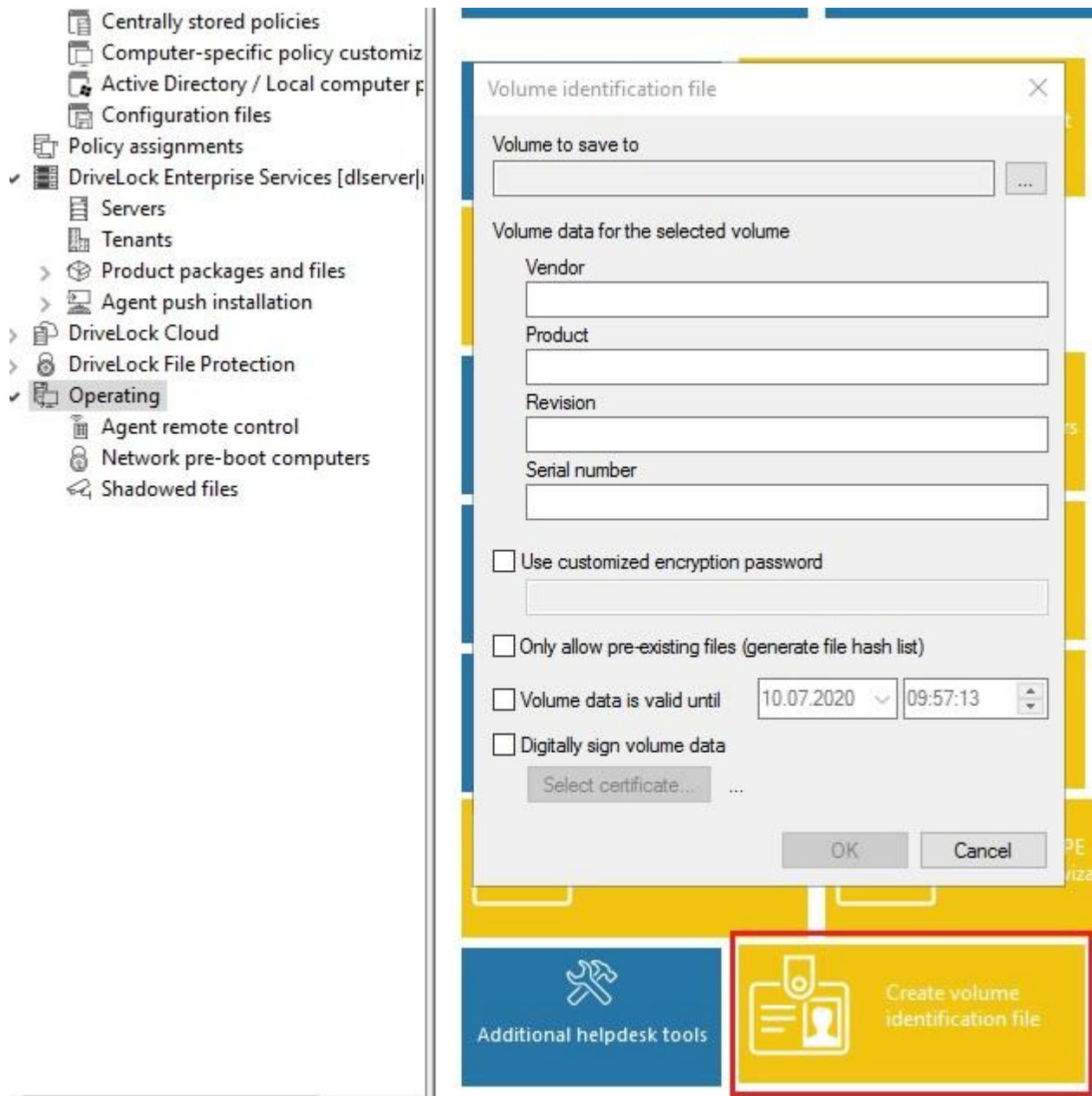
If the option *Automatically create volume identification files* is checked, a volume ID file will be created and filled with the hardware ID values as soon as an external storage media is connected to DriveLock on a FAT Client (not on a Thin Client).

Volume ID files are encrypted with a default key or with a key generated from a defined *custom encryption password*. All existing volume ID files will become invalid if you change this *password*.

Volume ID files are hidden for normal users (attributes hidden, system)

How to manually create volume identification files

Open **MMC / Operating / Create volume identification file** and enter the appropriate values to manually create a volume ID file e.g. for SD cards

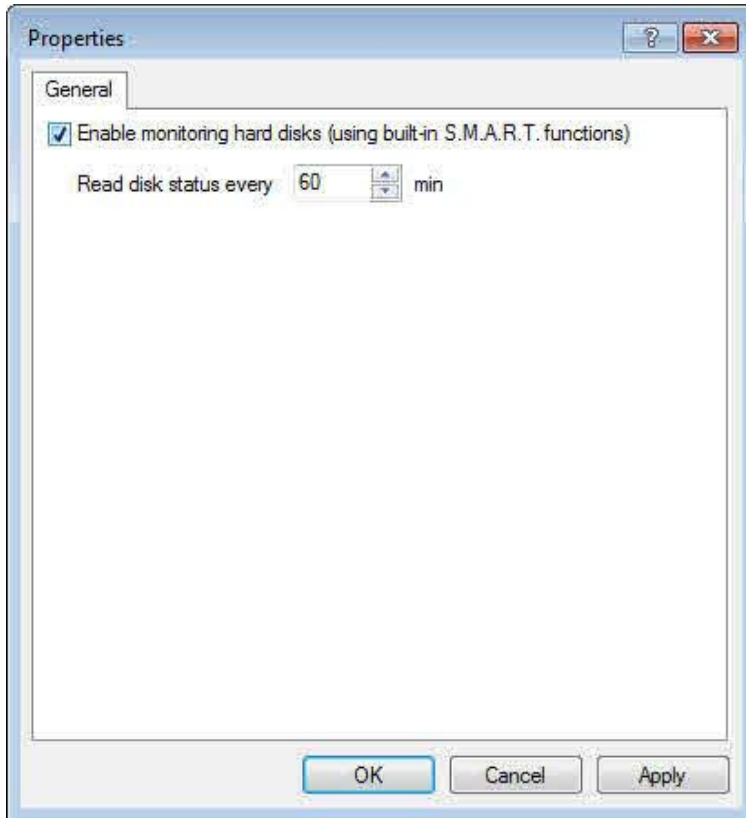


9.1.2.1.5 Shadowing Configuration

For information about how to configure file shadowing, refer to the section [“Configuring Global Shadowing”](#)

9.1.2.1.6 Drive Monitoring Using S.M.A.R.T.

Many hard drives use S.M.A.R.T. (Self-Monitoring, Analysis and Reporting Technology) to report drive health, temperature and other drive status information and to issue alerts when a drive is about to fail. DriveLock can monitor the S.M.A.R.T. status of drives that support this technology. You can enable the monitoring and configure the monitoring interval under *Extended configuration* -> *Drives* -> *Settings* -> *Hard drive self-monitoring (S.M.A.R.T.) configuration*. To enable monitoring, select the checkbox and then select the monitoring interval.



9.1.2.1.7 Advanced Global Settings for Controlling Drives

To define the following additional settings, click the corresponding links in the taskpad:

- *Audit device insertion / removal / lock*: When activated, DriveLock generates an audit event each time a drive is connected, removed or locked.
- *Unlock drives when service is stopped*: When enabled, stopping the DriveLock service temporarily unlocks all drives.
- *Disable file filtering while drives are temporarily unlocked*: When enabled, the Agent suspends file filtering when an administrator temporarily suspends drive locking.

If you disable file filtering when you unlock all drives, this overrides any settings for controlling file filtering while drives are unlocked.

9.1.2.2 Enabling Drive Locking

DriveLock can detect all types of drives which Windows recognizes as removable drives or fixed disks. This includes the following types (classes):

- *Floppy disk drives*: Internal floppy disk drives
- *CD-ROM/DVD drives*: Internal CD-ROM/DVD drives, including burners
- *USB bus-connected drives*: All drivers that are connected using a USB port, including flash drives, hard drives, CD-ROM drives and card readers
- *Firewire (1394) bus-connected drives*: Drives connected using Firewire

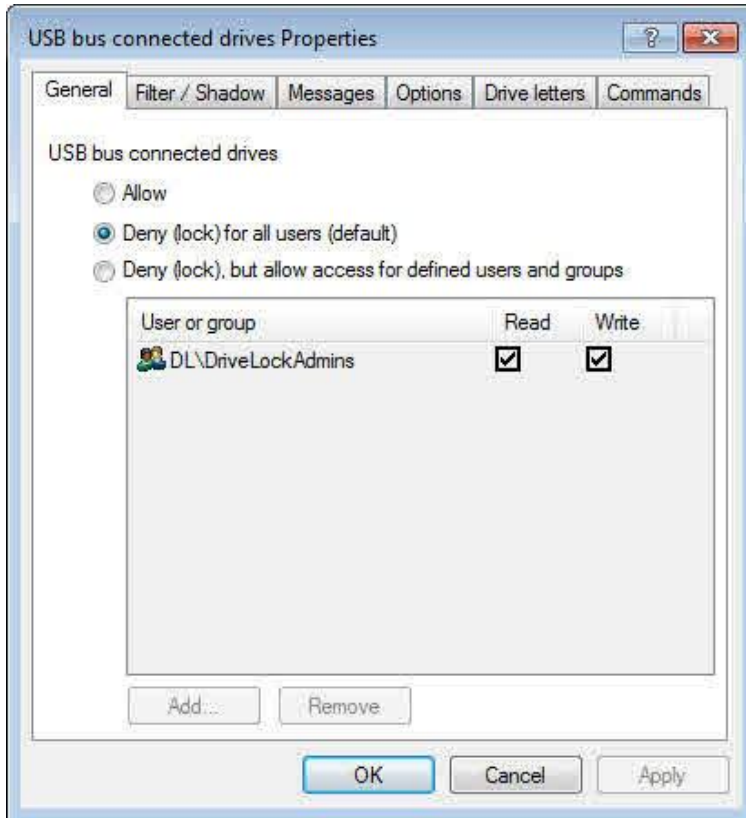
- *SD bus-connected drives*: Drives connected to a built-in SD card reader, which is most frequently found in notebook computers
- *Other removable drives*: All removable drives that are not included in another category, such as ZIP drives
- *Fixed disks*: Drives that are recognized by Windows as not removable and that don't contain the operating system, including drives connected using an IDE, ATAPI, SCSI, RAID, SATA or eSATA bus
- *Encrypted volumes*: Mounted volumes that are encrypted using DriveLock Encryption 2-Go. For more information about encrypted volumes, refer to the chapter *Encryption 2-Go*.
- *Network drives and shares*: Network shares that are accessed using Windows networking.
- *WebDAV-based network drives*: Network drives that are accessed using the WebDAV protocol via HTTP or HTTPS.
- *Windows Terminal Services (RDP) client drive mappings*: Refer to the chapter *Using DriveLock in Terminal Server Environments* for more information about this drive type.
- *Citrix XenApp (ICA) client drive mappings*: Refer to the chapter *Using DriveLock in Terminal Server Environments* for more information about this drive type.

Boot partitions and partitions containing the page file are never blocked by DriveLock.



To enable drive locking, open the DriveLock Management Console and then in the console tree in the left pane click **Drives -> Removable drive locking**.

To open the configuration dialog box for USB drives, in the right pane click “**USB bus-connected drives**”.



Use the tabs in this configuration dialog box to configure settings that apply to all USB drives connected to the computer.

The configuration dialog is almost identical for all drive types, but not all features are available for some drive types or look slightly different from the options for USB drives.

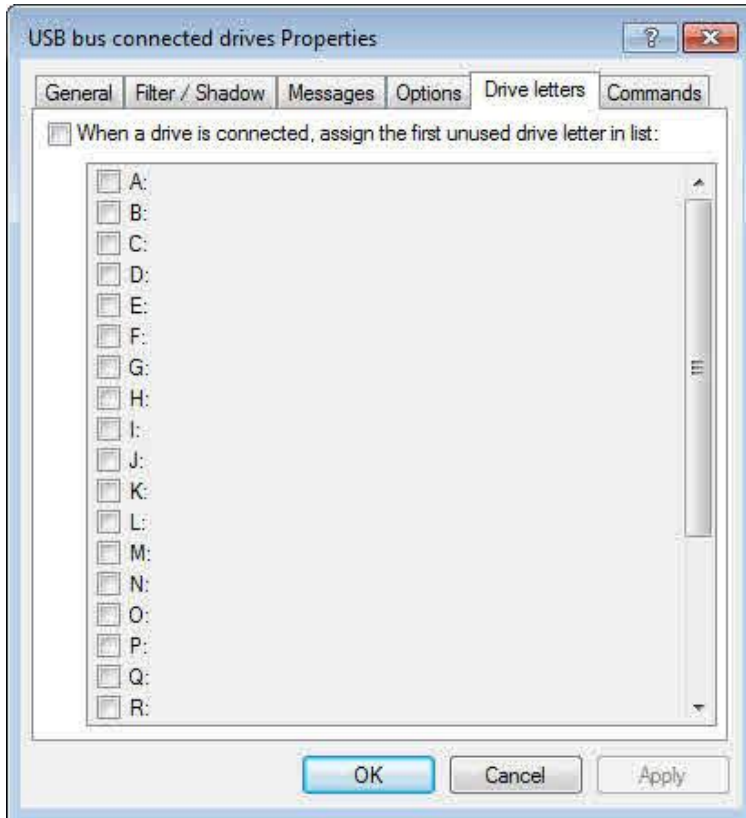
To enable locking of all USB drives on this computer, select “**Deny (lock) for all users (default)**” and then click **OK**.

To lock USB drives, it is not required (and not recommended) to lock down the device class “USB controller”. If you do so, all USB-connected devices are disabled and you cannot utilize any of the fine-grained controls that DriveLock provides for USB drives.

If you allow access to this type of drive, either for all users or for selected groups, you can also configure the type of access. This allows you to restrict access for certain users or group to read operations only.

A note on floppy disk drives: When using read/write permissions on a floppy disk drive, DriveLock needs to load a file filter after you insert a disk. The Windows operating system does not reliably notify applications, such as DriveLock, of disk insertions, so DriveLock must perform this check itself. To do so, DriveLock must check the floppy disk drive at regular intervals (so called “polling”) to determine whether a new floppy disk has been inserted. Unfortunately, this checking may cause the drive to emit a clicking sound. To avoid this, either do not use any file filter rules for floppy disk drives or deactivate floppy disk drive polling (under Advanced Drive Setting, visible in classic MMC view only). If you deactivate polling, the file filter does not work correctly on some floppy disk drives.

To specify which drive letters are assigned to drives of this type that are connected to a computer, on the “Drive letters” tab select one or more drive letters from the list.



You can also specify drive letters in a whitelist rule.

Configuring user access permissions and the settings on other tabs are covered in the section [“Common Settings for Drive Whitelist Rules”](#).

9.1.2.3 Creating Drive Rules

You can use the following types of drive whitelist rules:

- *Vendor/Product ID rule*: Applies to a drive based on its manufacturer, model or serial number (for example a Kingston 1 GB USB flash drive with a specific serial number)
- *Drive collection rule*: These settings apply to a predefined list of drives
- *Network drives rule*: Configuration of a specific network share
- *WebDAV-based network drives rule*: Settings for a network drive accessed over an HTTP/HTTPS connection
- *Drive size rule*: Applies to a drive based on its size
- *Base rule*: Applies to any of the five main drive types (use this type of rule to specify time limit or computer restrictions for all drives of the same type)
- *Terminal services rule*: Applies to specific drive letters in a terminal server client session, including mapped local drives on thin clients.
- *Hardware ID rule*: These settings apply to a specific hardware ID

Rules are processed in the following order, from highest priority to lowest priority:

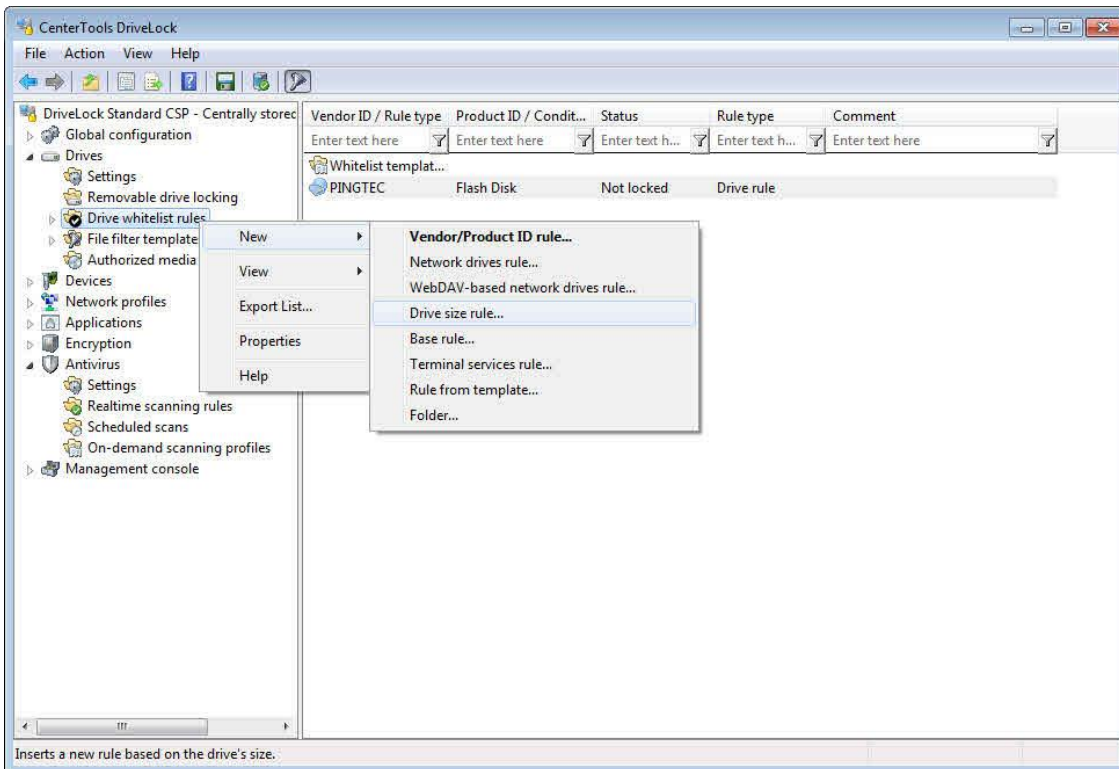
- Vendor/Product ID rule (a rule with a serial number has a higher priority than one without a serial number)
- Drive size rule

- Base rule
- General locking setting

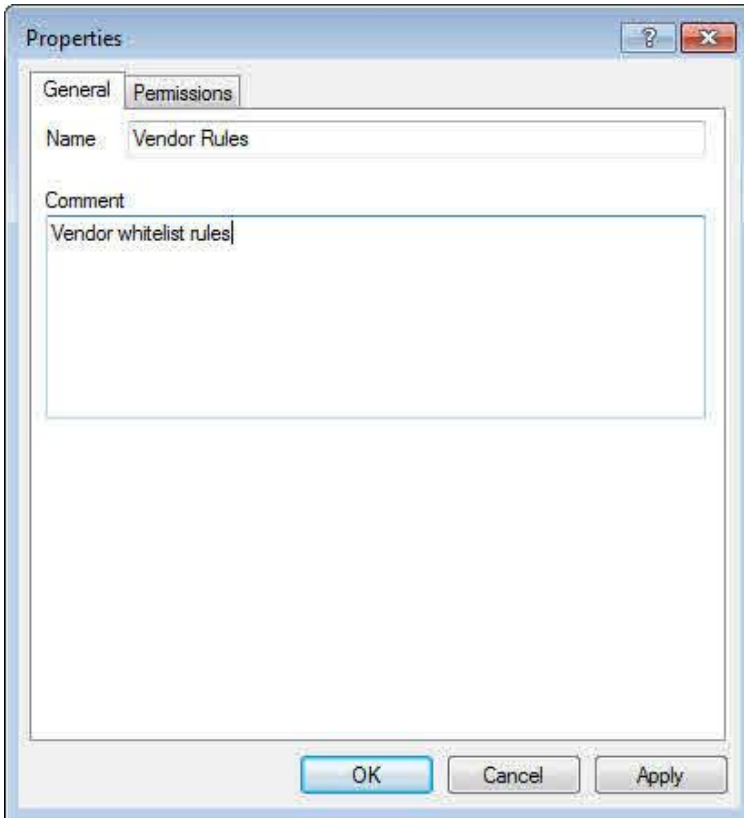
The following sections describe the various rule components. The section “[Common Settings for Drive Whitelist Rules](#)” describes common settings that are available when configuring certain types of whitelist rules.

9.1.2.3.1 Organizing Drive Whitelist Rules

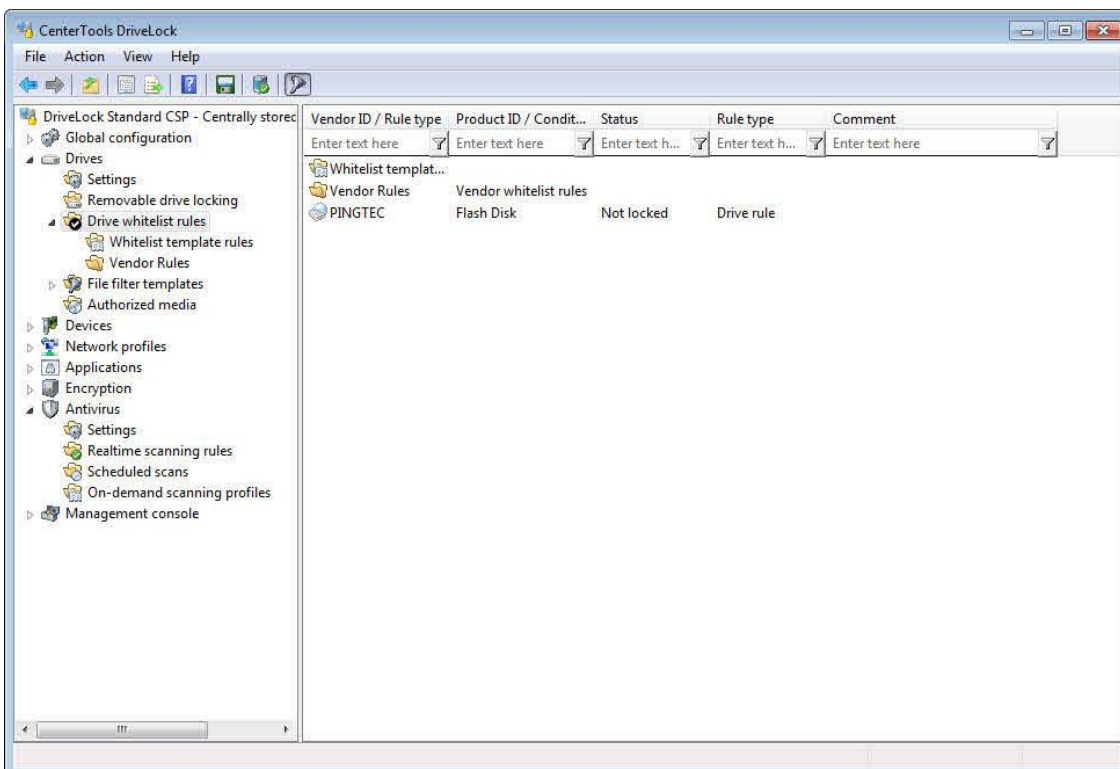
You can organize whitelist rules using folders and sub-folders just as you would organize files using directories.



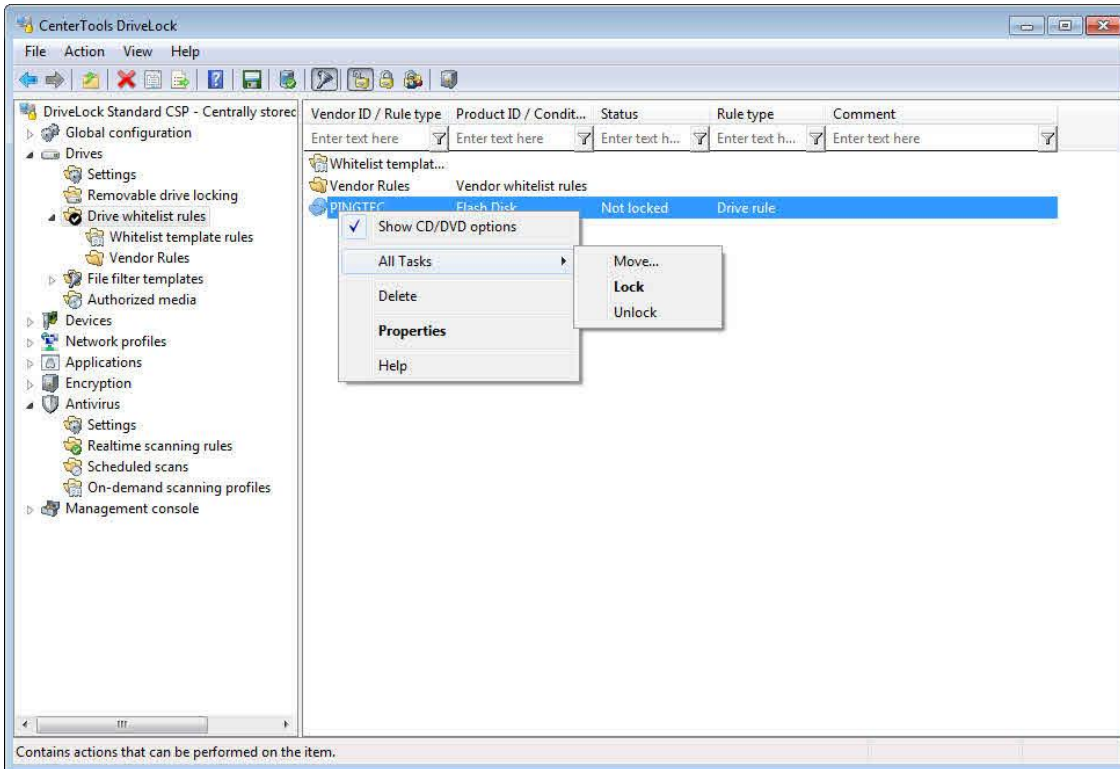
Right-click **Drive whitelist rule** and then click **New -> Folder**.



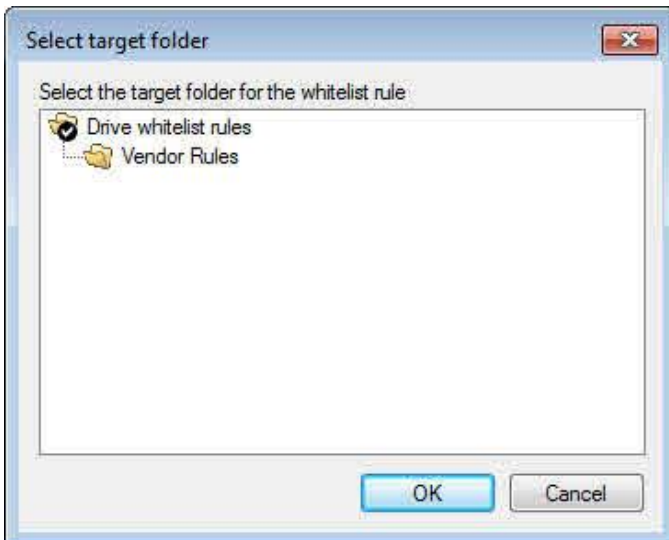
Type the name of the new folder and then click **OK**.



To create a new rule in a specific folder, right click the folder and then select the rule type, for example **New -> Vendor/Product ID rule**.



To move an existing whitelist rule to another location, right click the whitelist rule and then click **All tasks -> Move**.



Select the destination folder and then click **OK**.

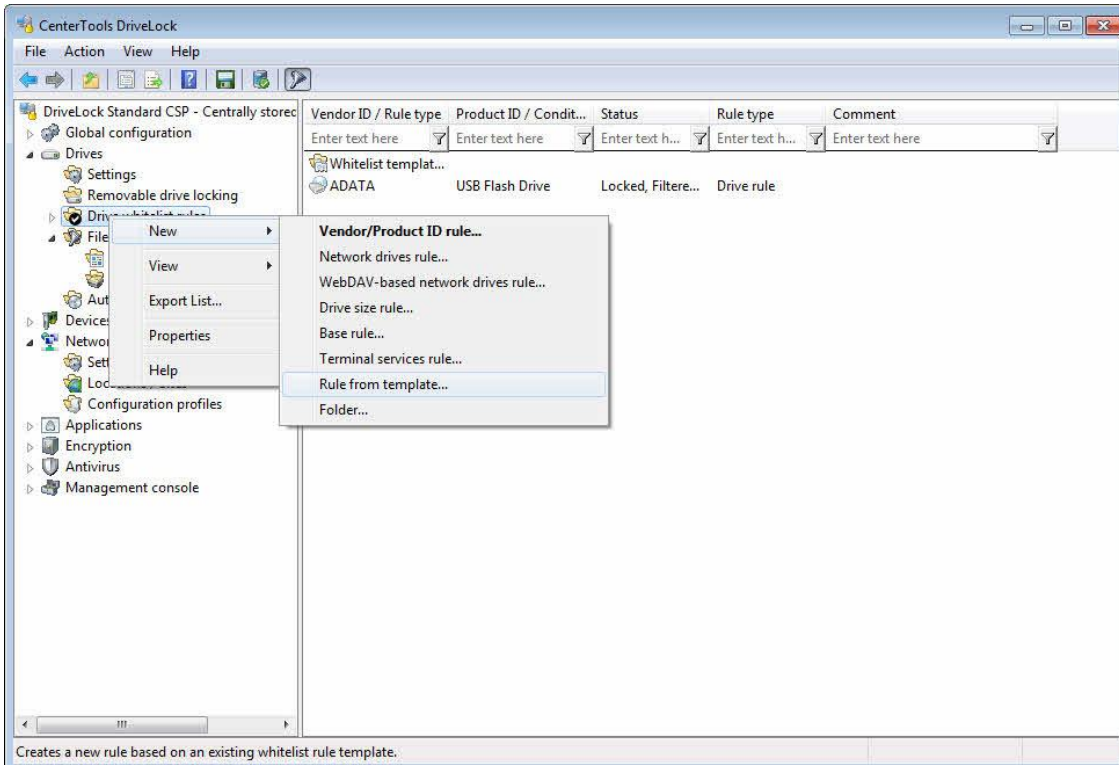
9.1.2.3.2 Creating Whitelist Templates

A whitelist template is a drive whitelist rule that can be used as template for other whitelist rules. You can create whitelist templates for the following rule types:

- *Vendor/Product ID rule*: Applies to a drive based on its manufacturer, model or serial number (for example a Kingston 1 GB USB flash drive with a specific serial number).
- *Drive collection rule*: These settings apply to a predefined list of drives
- *Network drives rule*: Configuration of a specific network share
- *WebDAV-based network drives rule*: Settings for a network drive accessed over an HTTP/HTTPS connection

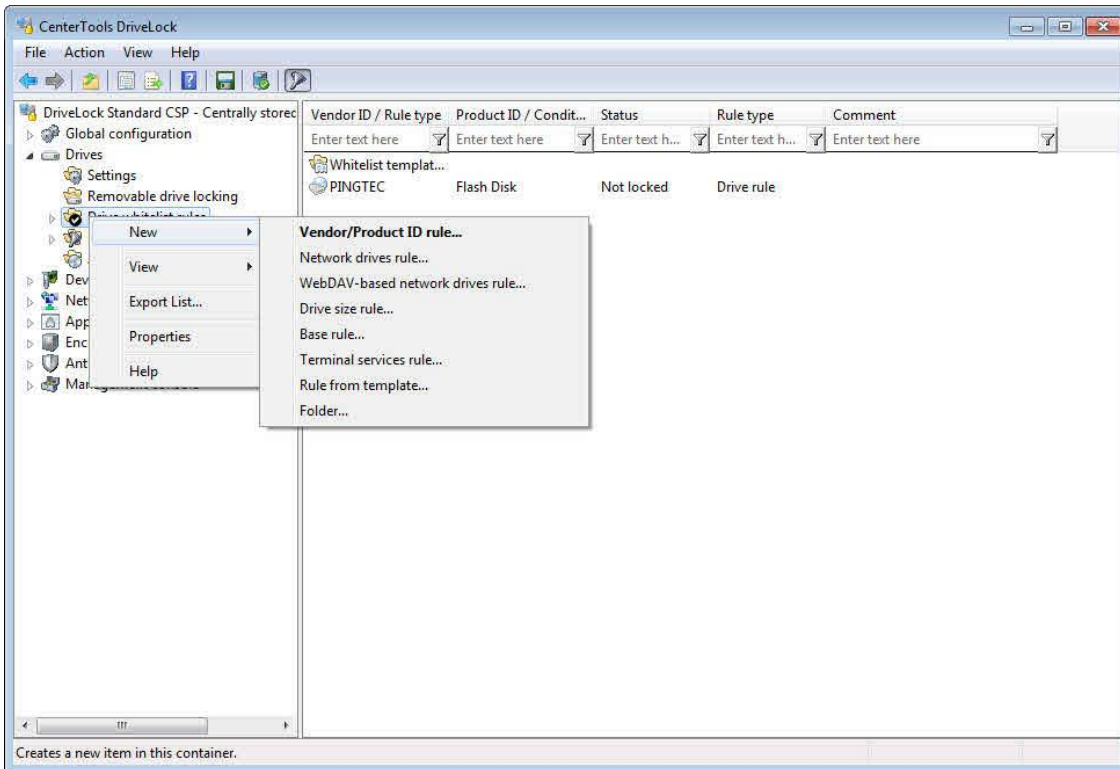
- *Drive size rule*: Applies to a drive based on its size.
- *Basic rule*: Applies to any of the five main drive types (use this type of rule to specify time limit or computer restrictions for all drives of the same type).
- *Terminal services rule*: Applies to drive letters in a terminal server client session, including mapped local drives on thin clients.
- *Hardware ID rule*: These settings apply to a specific hardware ID

Templates can't be used directly to control drive use, but you can create whitelist rules based on a whitelist template (refer to the chapter "[Creating a Rule Based on a Template](#)" for details).



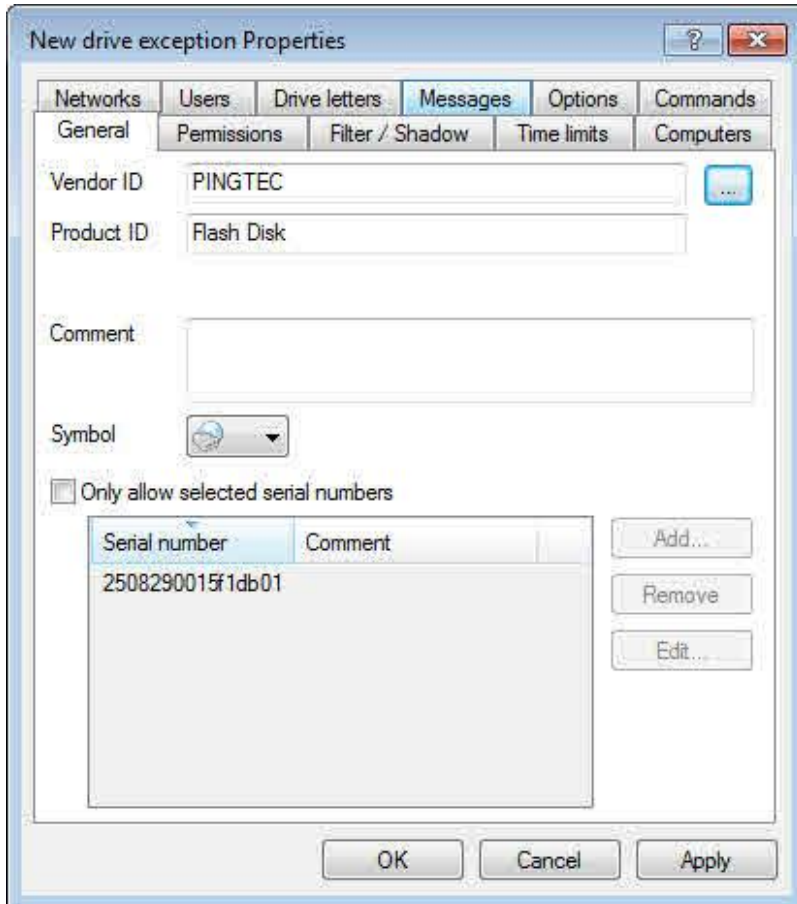
Right-click **Whitelist template**, click **New** and then select the type of whitelist rule to create a template for. Follow the steps described in the chapter "[Creating Drive Rules](#)" to create the template.

9.1.2.3.3 Vendor/Product ID Rule



Right-click **Drive whitelist rule** and then click **New -> Vendor/Product ID rule**.

In the following dialog box, specify the drive to unlock or control. Type the vendor ID and product ID of the device if you know them. You can also specify an optional list of serial numbers to make the rule apply to only certain drives of the same model.

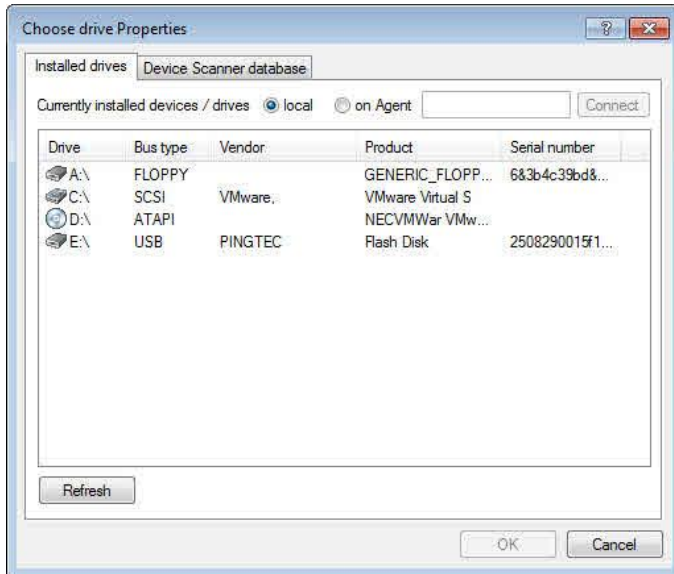


Each drive contains information in its firmware about itself, such as the manufacturer, product name and serial number:

- Vendor ID: Name or abbreviation of the drive manufacturer
- Product ID: Model name, as defined by the manufacturer

If you don't know the identifying information of a drive, you can select the drive by clicking the "..." button next to **Vendor ID**. You can use wildcards, like "?" (one character) or "*" (any number of characters) within the Product ID or Vendor ID. This also applies, if you want to add more serial numbers and after you clicked **Add...**

DriveLock will display a dialog box that you can use to select a drive that is currently attached to the administration workstation, to a client computer, or that is listed in the Device Scanner database. DriveLock automatically adds the serial numbers of drives you add using this method to the dialog box.



To add a locally attached drive, select this drive and then click **OK**.

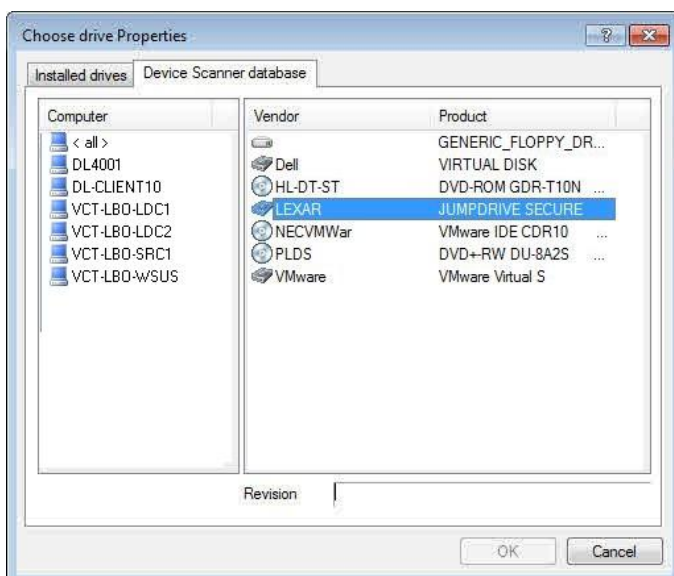
If you need information about other drives, you can connect to a remote client PC and select one of the drives installed on it. Select **on agent** and then type the name of the computer you want to connect to. This requires that the DriveLock Agent is installed and running on the remote computer.

DriveLock reads the hardware information for the drive that is maintained by the Windows operating system. Therefore DriveLock can only display the drives in the format in which they appear to Windows.

To establish a connection to a remote computer running Windows XP SP2 or higher with the Windows Firewall enabled, you must configure the firewall settings to allow incoming connections from TCP Ports 6064 and 6065 and the program "DriveLock".

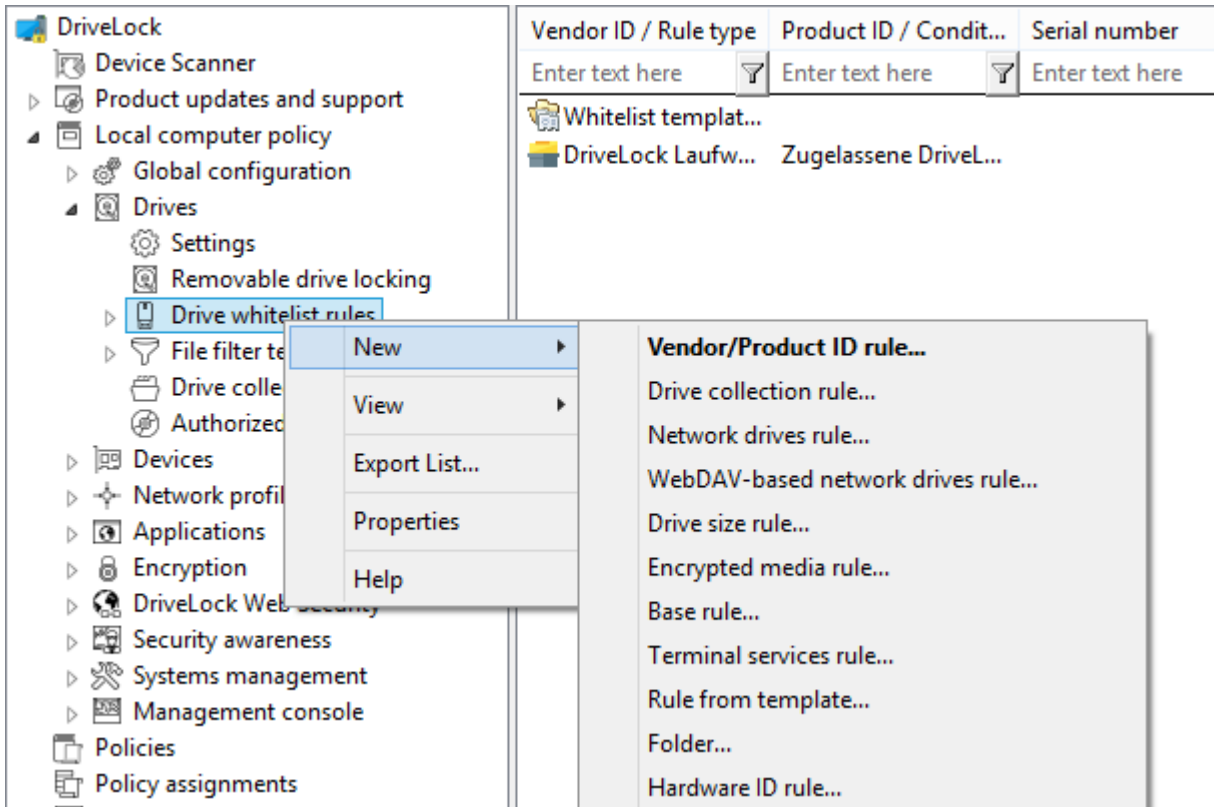
When connecting to the local computer, blocked removable drives are not be displayed. If you also want to view any blocked drives, select **on agent** and then type the name of the local computer.

A more convenient way to get drive information is to use the results from a hardware scan that has been completed in advance. To do this, on the **Device scanner database** tab, select the appropriate computer, vendor and product ID.

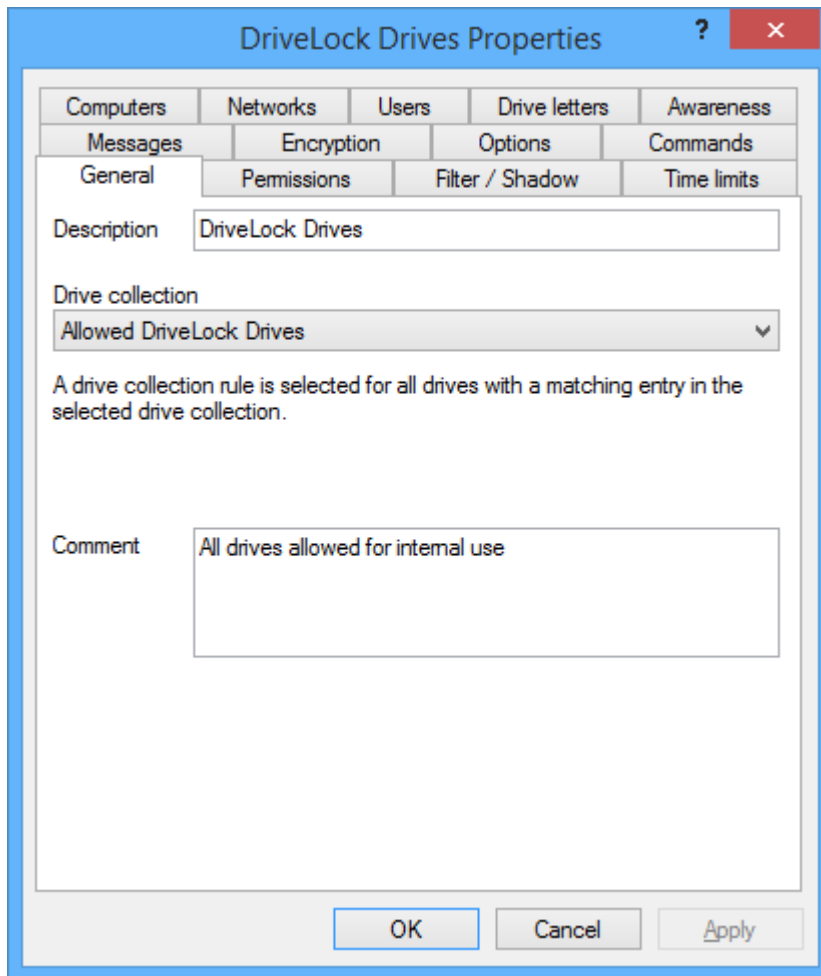


Settings on other tabs are described in the section "[Common Settings for Drive Whitelist Rules](#)".

9.1.2.3.4 Drive Collection Rule



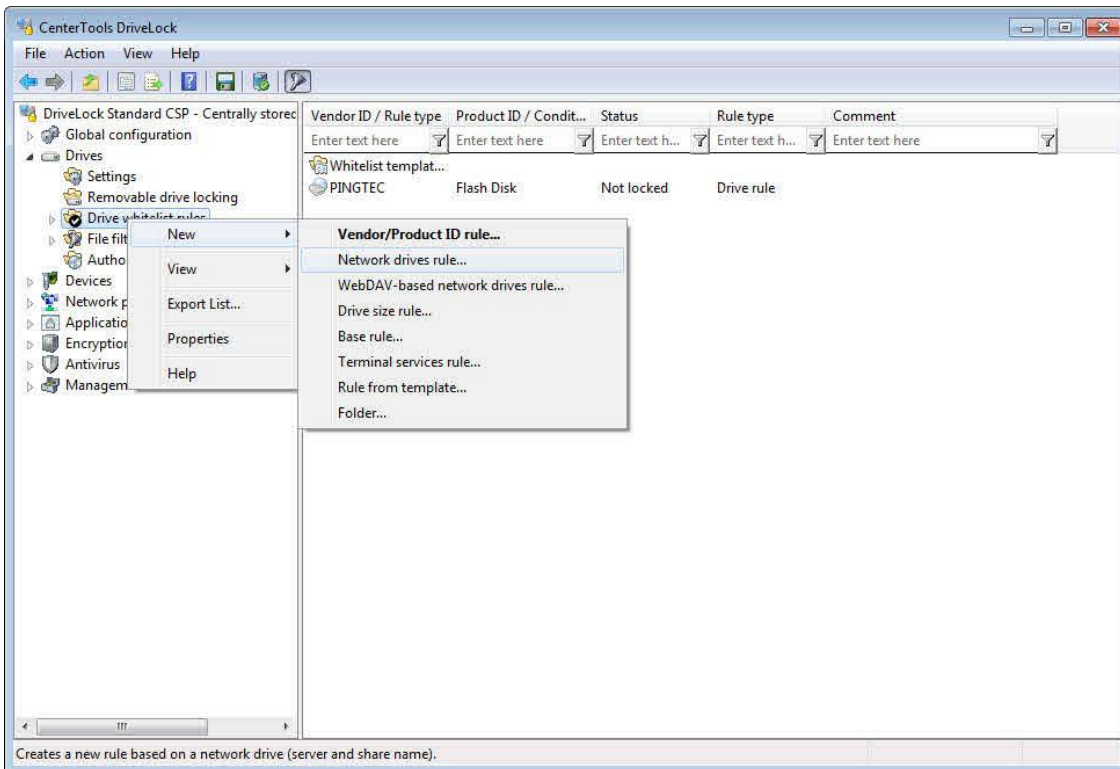
Right-click **Drive whitelist rules** and select **New -> Drive collection rule** from the context menu:



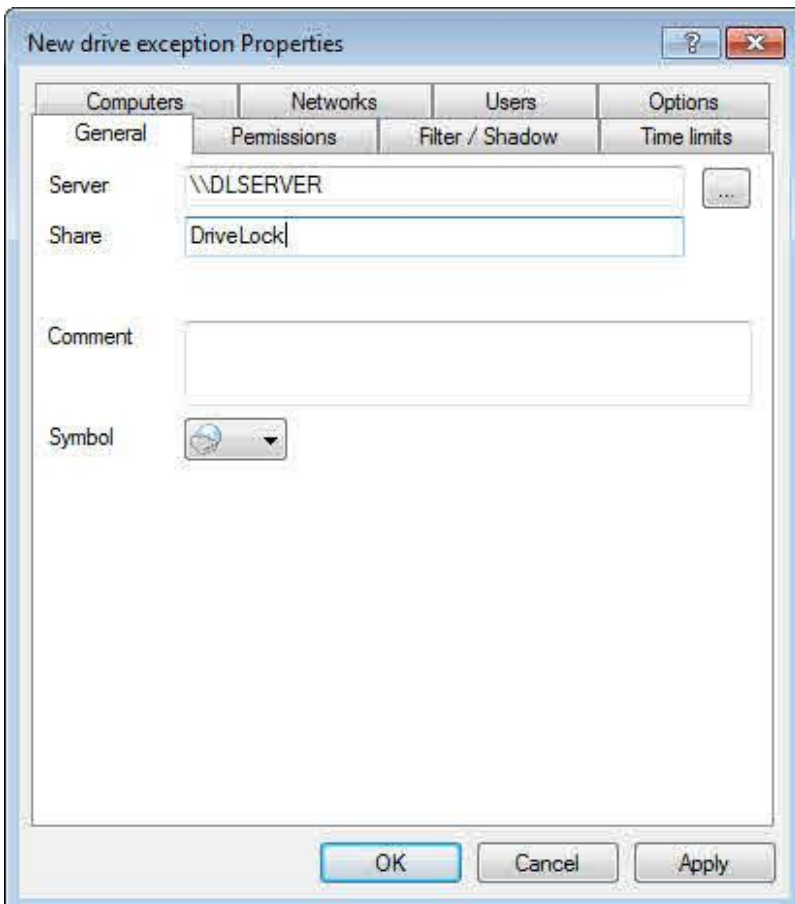
After entering a description, select a drive collection you created earlier. You can also enter a comment.

9.1.2.3.5 Network Drives Rule

Use a network drives rule to control access to network shares.



Right-click **Drive whitelist rule** and then click **New -> Network drives rule**.



Type the name of the server and the share or click “...” to browse the network for the share.

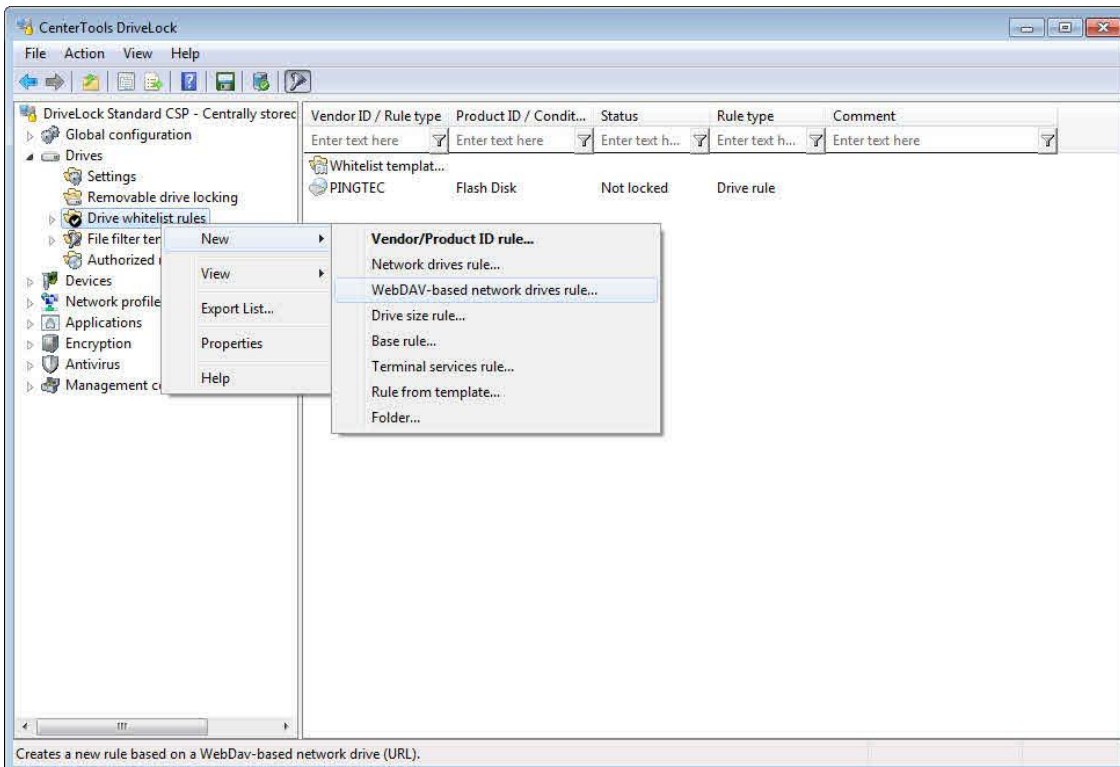


Settings on other tabs are described in the section [“Common Settings for Drive Whitelist Rules”](#).

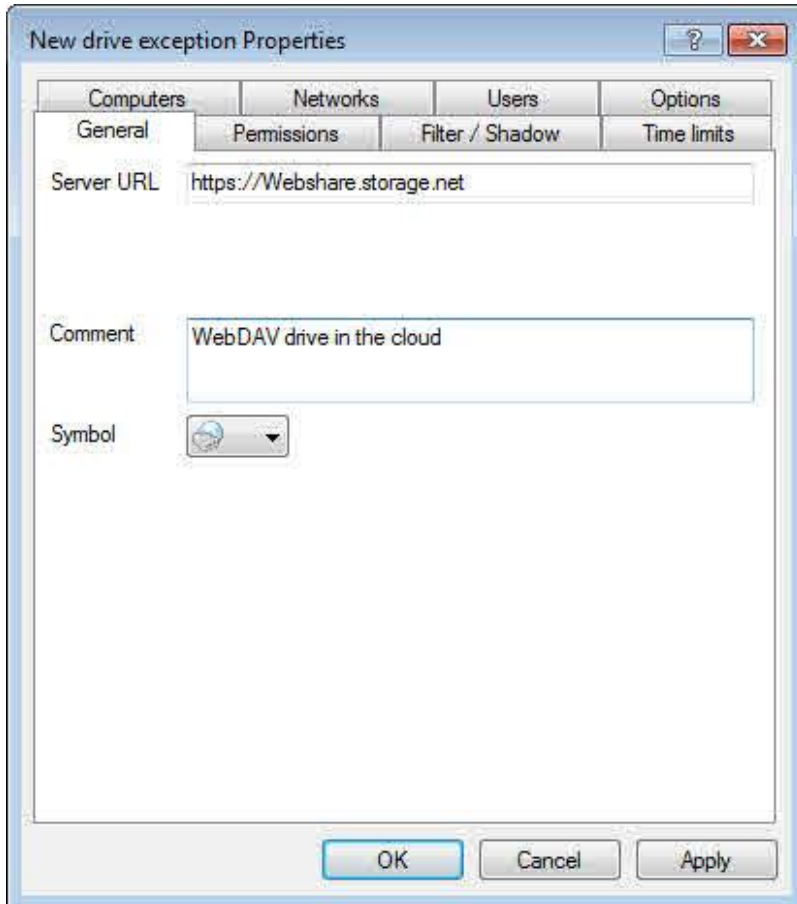
Only a subset of drive configuration options is available when configuring whitelist rules for network drives.

9.1.2.3.6 WebDAV-Based Network Drives

Use a WebDAV rule to control access to network shares that are accesses using HTTP or HTTPS..



Right-click **Drive whitelist rule** and then click **New -> WebDAV-based network drives rule**.

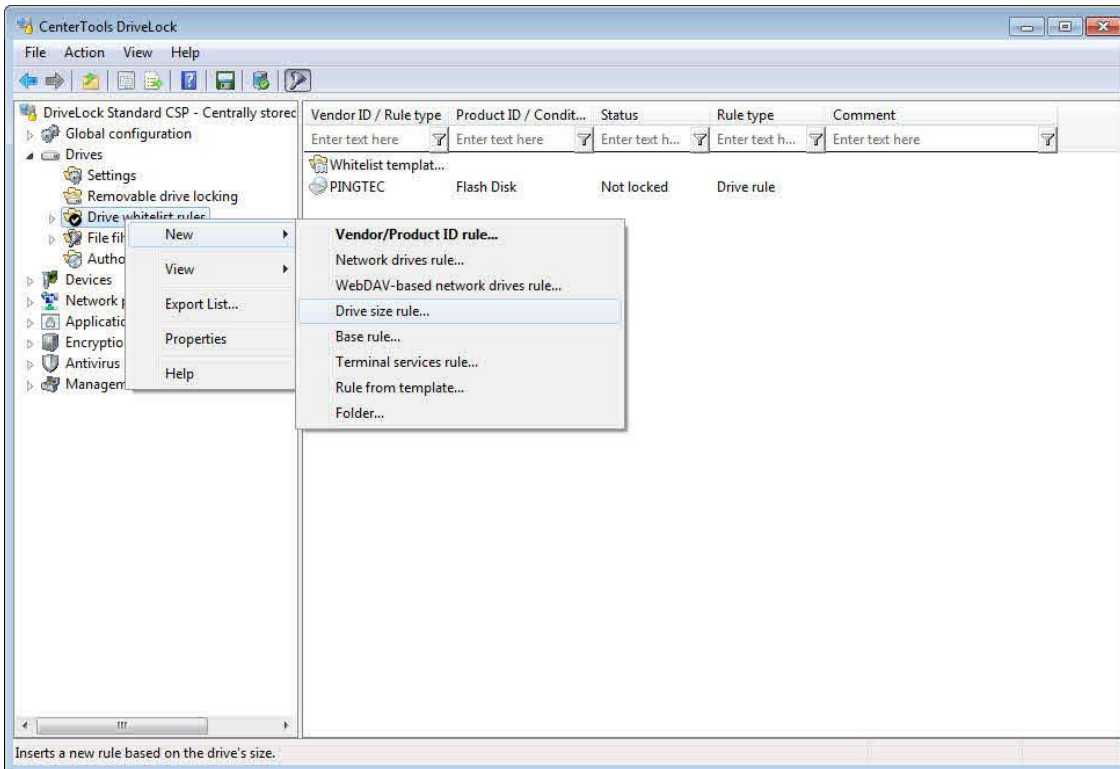


Type the URL of the share, starting with http:// or https://.

Settings on other tabs are described in the section "[Common Settings for Drive Whitelist Rules](#)".

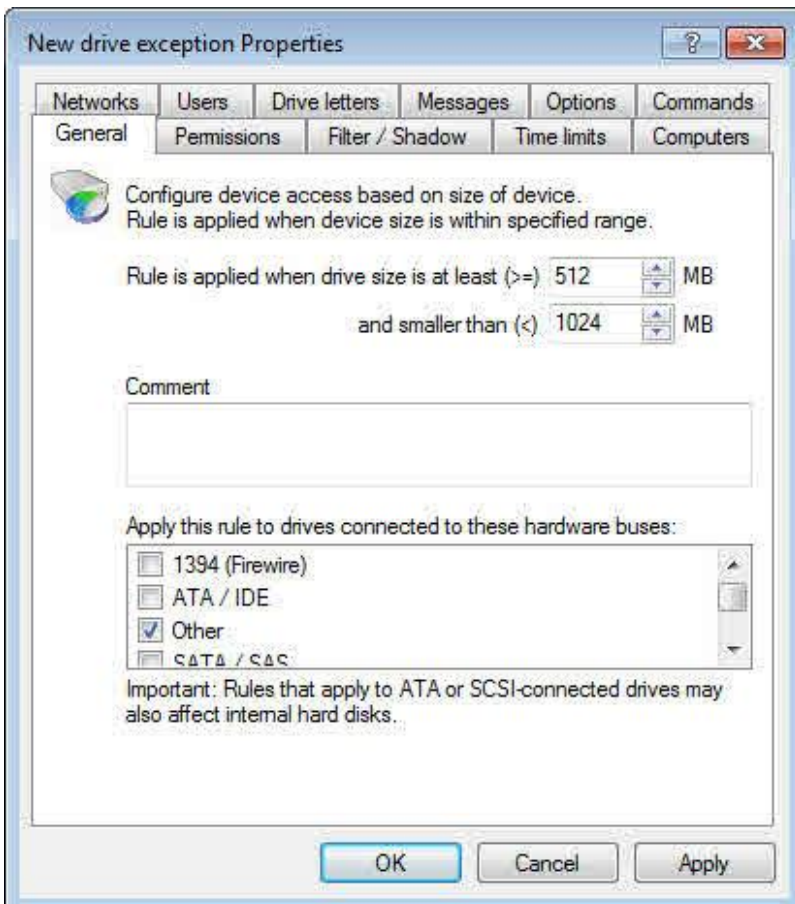
Only a subset of drive configuration options is available when configuring whitelist rules for network drives.

9.1.2.3.7 Drive Size Rule



Use a drive size rule to control drives based on their capacity.

Right-click **Drive whitelist rule** and then click **New -> Drive size rule**.

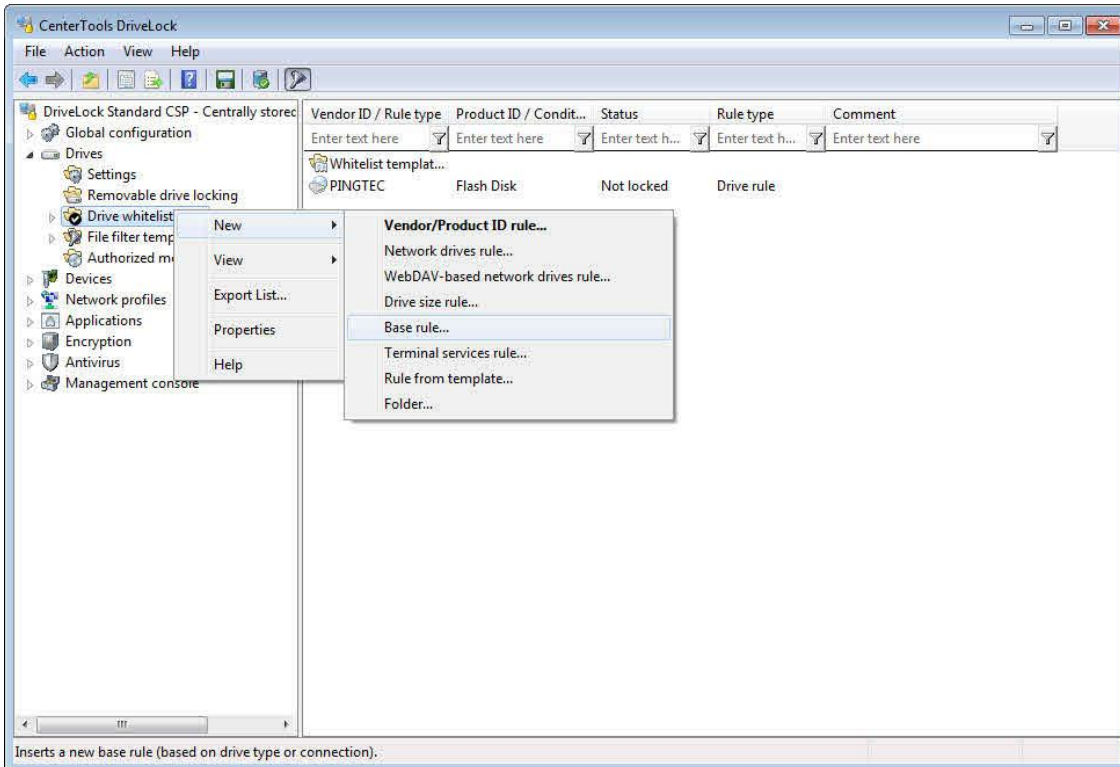


Specify the drive size, and under “**Activate this rule on drives connected to the following buses**” select one or more of the bus types that the drives you want to control are attached to.

If you activate the rule for ATA/SCSI it also applies to local hard drives. If you lock a local hard drive by mistake, you must start the computer in Safe Mode and reverse the configuration setting. This requires that the DriveLock Agent is not configured to start in Safe Mode.

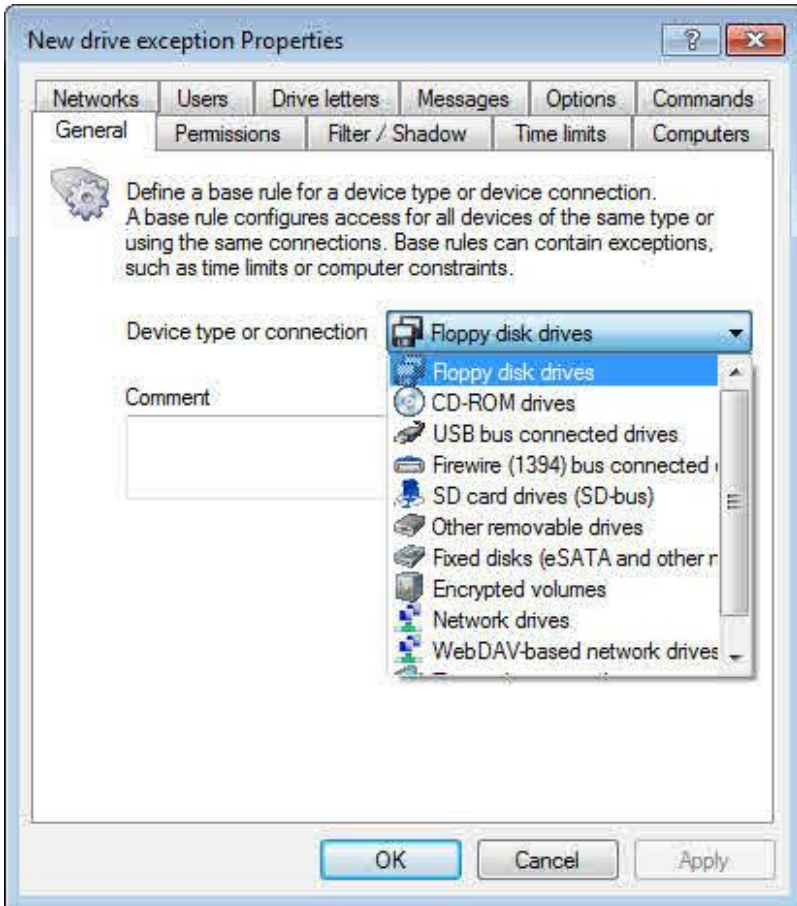
Settings on other tabs are described in the section “[Common Settings for Drive Whitelist Rules](#)”.

9.1.2.3.8 Base Rule



Right-click **Drive whitelist rule** and then click **New -> Base rule**.

Use a base rule to define exceptions for all drives of the same type. Use this rule to specify time limits, computer restrictions or network restrictions for a type of device. Base rules are appropriate if the rules don't need to be device-specific or based on drive size.



Select the drive or connection type to specify which drive type the rule applies to.

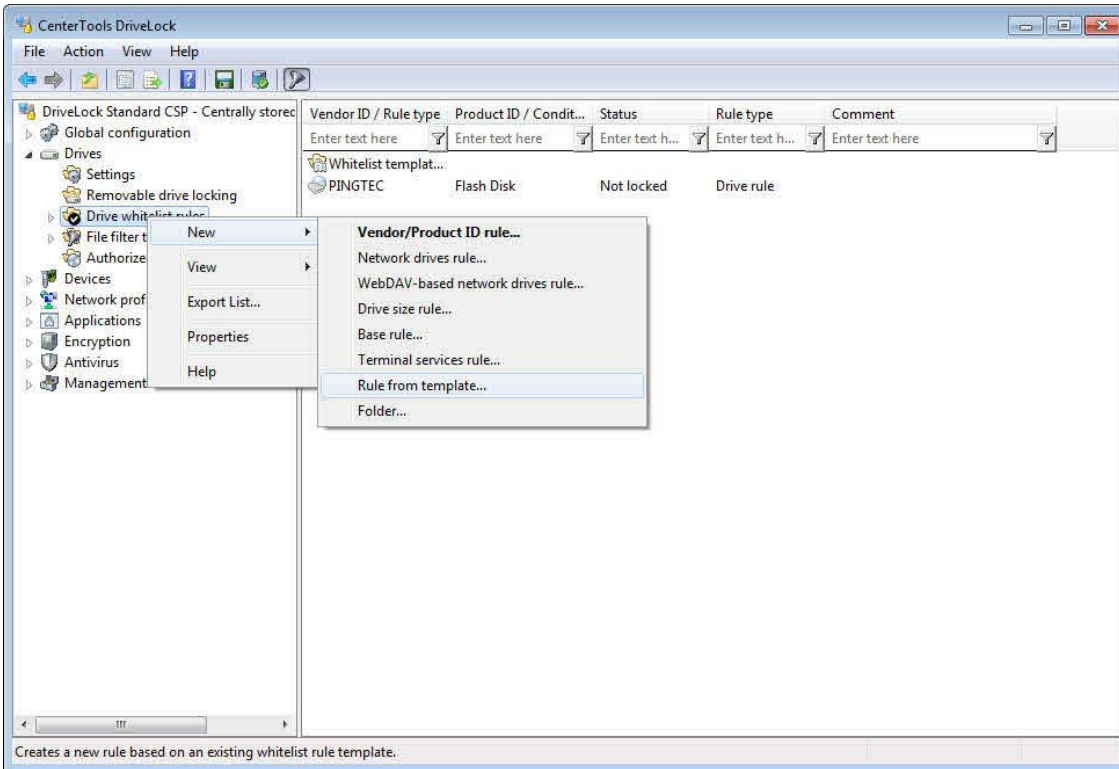
Settings on other tabs are described in the section "[Common Settings for Drive Whitelist Rules](#)".

9.1.2.3.9 Terminal Services Rule

For information about Terminal Services rules, refer to the chapter "[Using DriveLock in Terminal Server Environments](#)".

9.1.2.3.10 Creating a Rule Based on a Template

If you need to create several similar whitelist rules, for example for the same type of flash drive but with different user settings, a whitelist template can save a lot of time. Instead of creating each rule step-by-step, selecting the same configuration settings each time, you can base each rule on a whitelist template that contains the common settings for all rules. Refer to the chapter "[Creating Rule Templates](#)" for details on how to create a whitelist template.

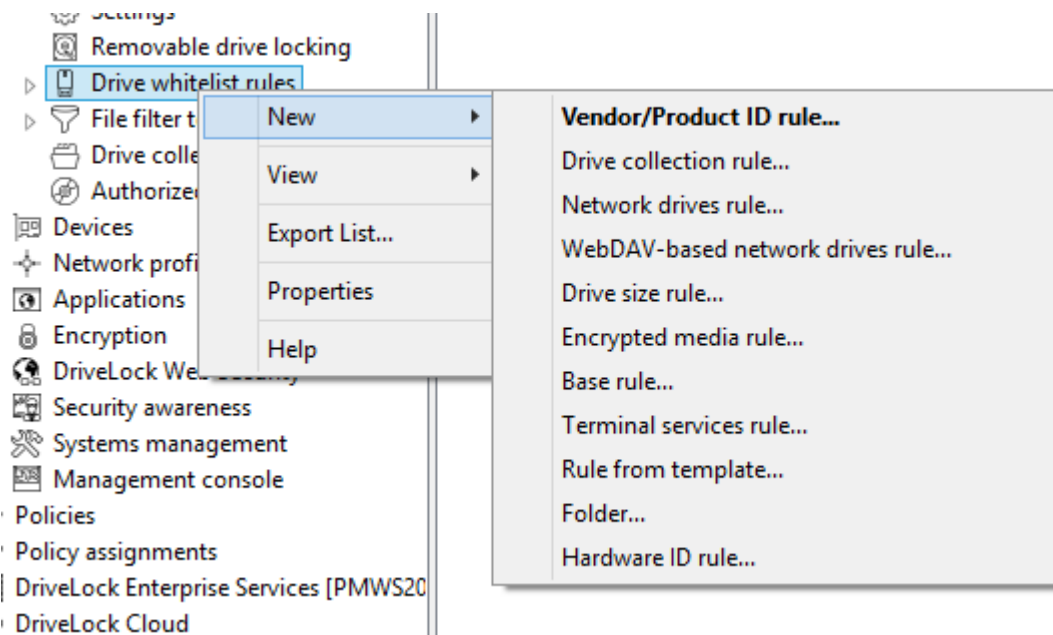


Right-click **Drive whitelist rule** and then click **New -> Rule from template**.

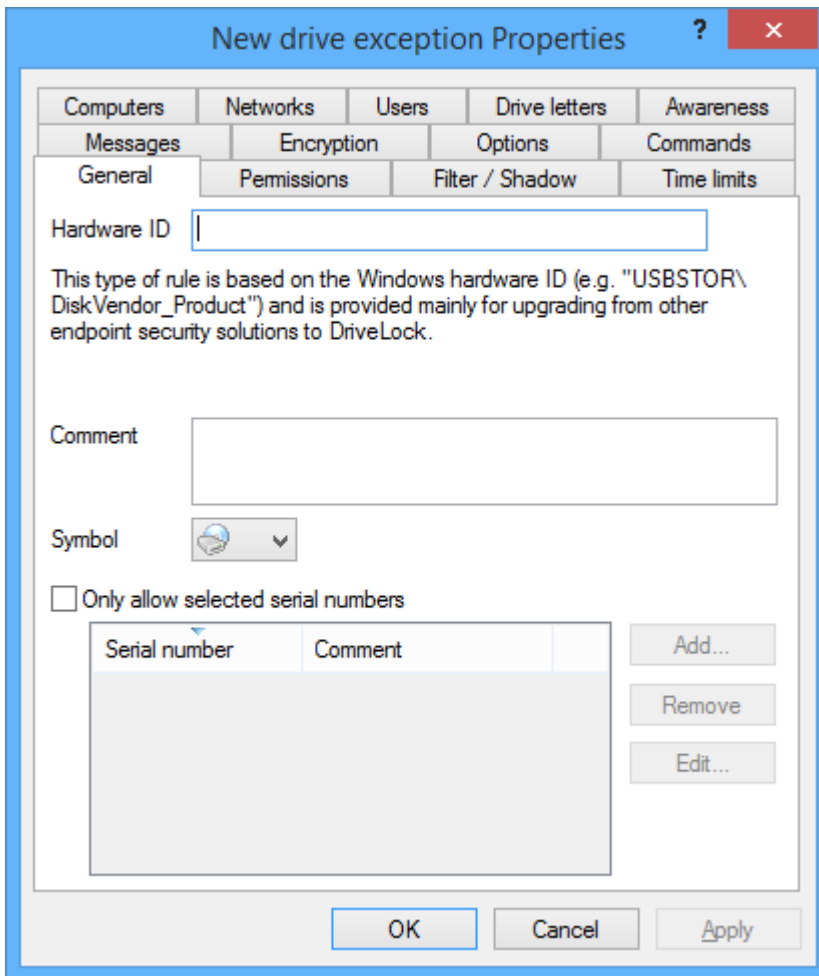
Select a whitelist template. A new whitelist rule is created containing all settings from the template. Add all required additional settings.

Settings on other tabs are described in the section "[Common Settings for Drive Whitelist Rules](#)".

9.1.2.3.11 Hardware-ID Rule



Right-click **Drive whitelist rules** and select **New -> Hardware ID rule** from the context menu:



Enter the hardware ID you want these settings to apply to.

Typically, hardware ID rules are only relevant for customers migrating from another Endpoint Security solution to DriveLock and wishing to adopt or maintain the known configuration. In all other cases, the device rule is a more practical configuration option that uses the product and vendor ID as a parameter.

As with device rules, you can define an additional list of serial numbers to restrict the scope of the rule further.

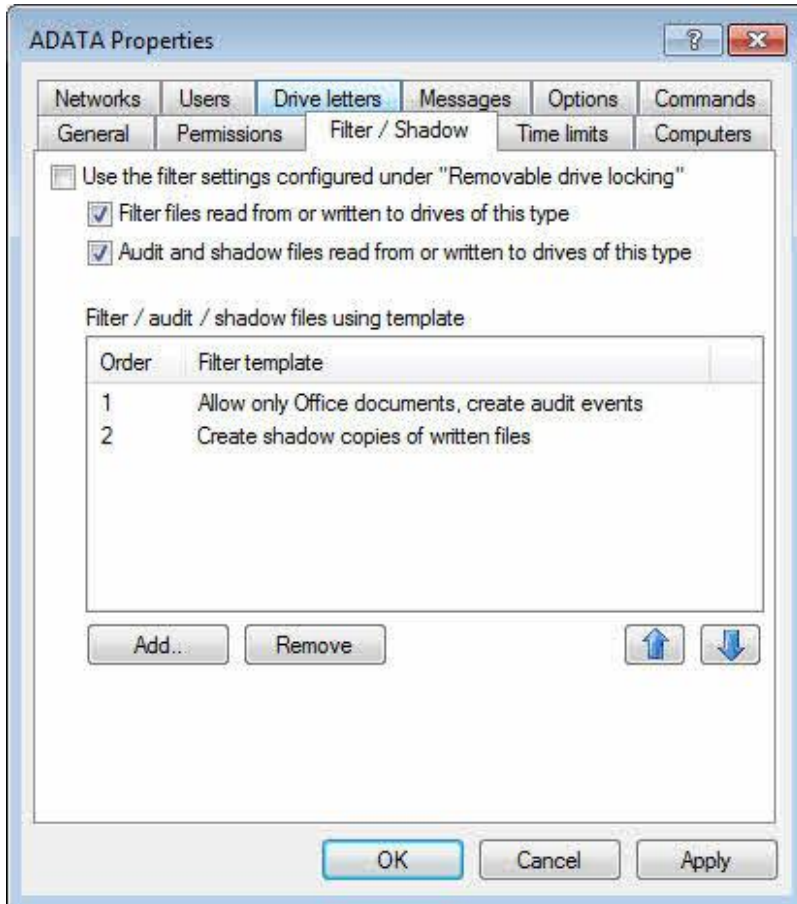
9.1.2.4 Common Settings for Drive Whitelist Rules

The tabs **“Permissions”**, **“Time limits”**, **“Computers”**, **“Networks”**, **“Users”**, **“Drive letters”**, **“Messages”**, **“Options”** and **“Commands”** are available for most types of drive whitelist rules and therefore described in this section.



Settings on the **“Filter / Shadow”** tab are described in the sections [“Using a File Filter Template”](#) and [“Configuring Shadow Copies in Drive Whitelist”](#) of this manual.

9.1.2.4.1 Controlling and Auditing File Access

On the *Filter/Shadow* tab you can configure which files users can access and how this access is audited. By default file filter, auditing and shadowing settings are inherited from the corresponding settings for the drive type. You can instead configure different settings that apply to the current whitelist rule.



To use different settings for the whitelist rule, deselect the checkbox *“Use the filter settings configured under Removable drive locking”* and then select *“Filter files”* and/or *“Audit files”*.

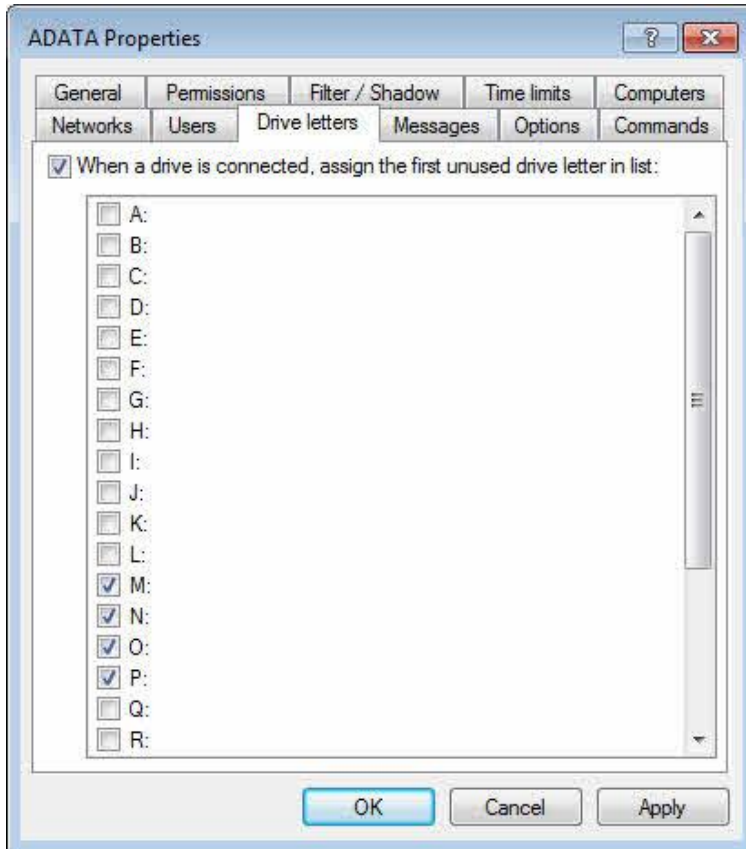
Click **Add** to add one or more previously created filter templates. Click **Delete** to remove the selected template from the list. Click  and  to move the selected template up or down.

When DriveLock applies this whitelist, it evaluates all filter templates in the list, starting from top. The first template matching all specified criteria (*“file size”*, *“exceptions”*, *“user and groups”*, *“computer”* or *“networks”*) is applied, any templates that follow are ignored. The following example illustrates this process: You created two templates: The first template applies to administrators and does not filter files. The second template applies all users and blocks access to program files. If administrator attempts to access a program file, DriveLock applies first template and access is granted. If a user who is not an administrator, DriveLock ignores the first template and instead applies the second template, blocking access to the program file.

9.1.2.4.2 Assigning Drive Letters

Use this option to define which letters are assigned to a drive when it is connected to the computer.

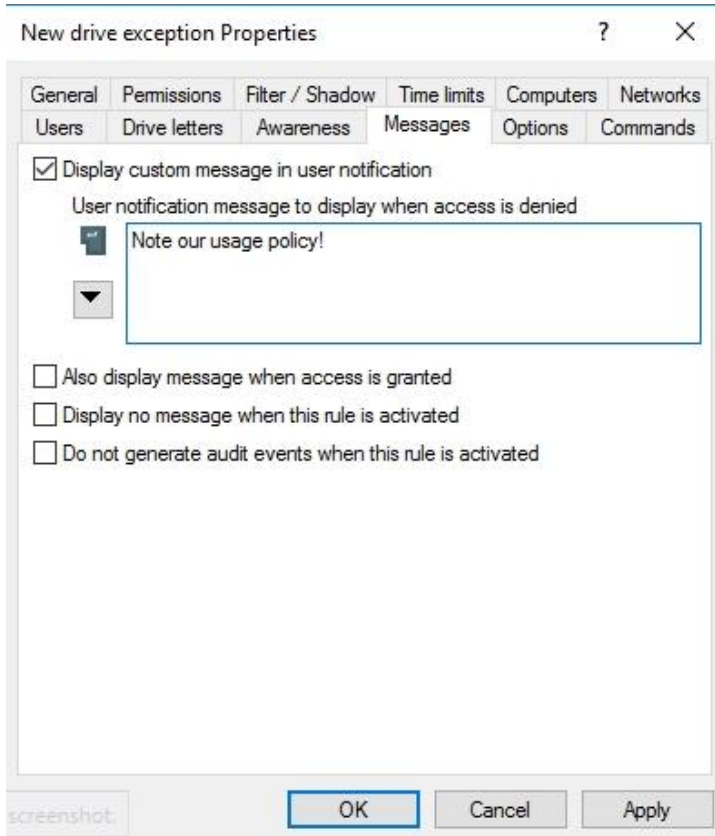
If you select multiple drive letters the DriveLock Agent automatically assigns the first available drive letter from the list.



Be careful not to select drive letters that are currently in use, such as drive letters used for network shares or home directories.

9.1.2.4.3 Defining Custom Notification Messages

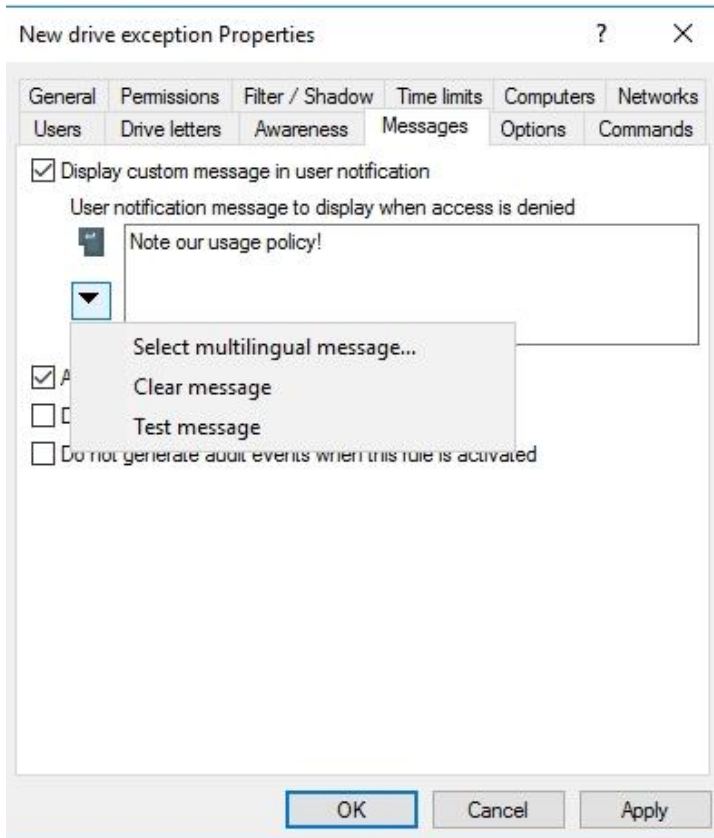
You can define a custom user notification message for each whitelist rule. Unless specified otherwise, DriveLock will display this message when it denies access to a drive because of the whitelist rule.



Select the “**Display custom message in user notification**” checkbox to activate the user notification message for the whitelist rule.

In the text edit box, type the message. DriveLock will display this message regardless of the client computer’s language setting. If you use this type of notification message, DriveLock displays a key icon near the top left corner of the text edit field.

If you have defined multilingual messages you can select this message type instead. To select a multilingual message, click the “down arrow” button and then on the drop-down menu click **Select multilingual message**.



Multilingual messages contain separate messages in multiple languages for the same notification. Before you can use such a message, you must define it in the *Global configuration* section of the policy. When you select a multilingual notification message, DriveLock displays the text in the language of the currently logged-on user.

Click the message and then click **OK**.

If you use this type of notification message, DriveLock displays a speech bubble icon near the top left corner of the text edit field.

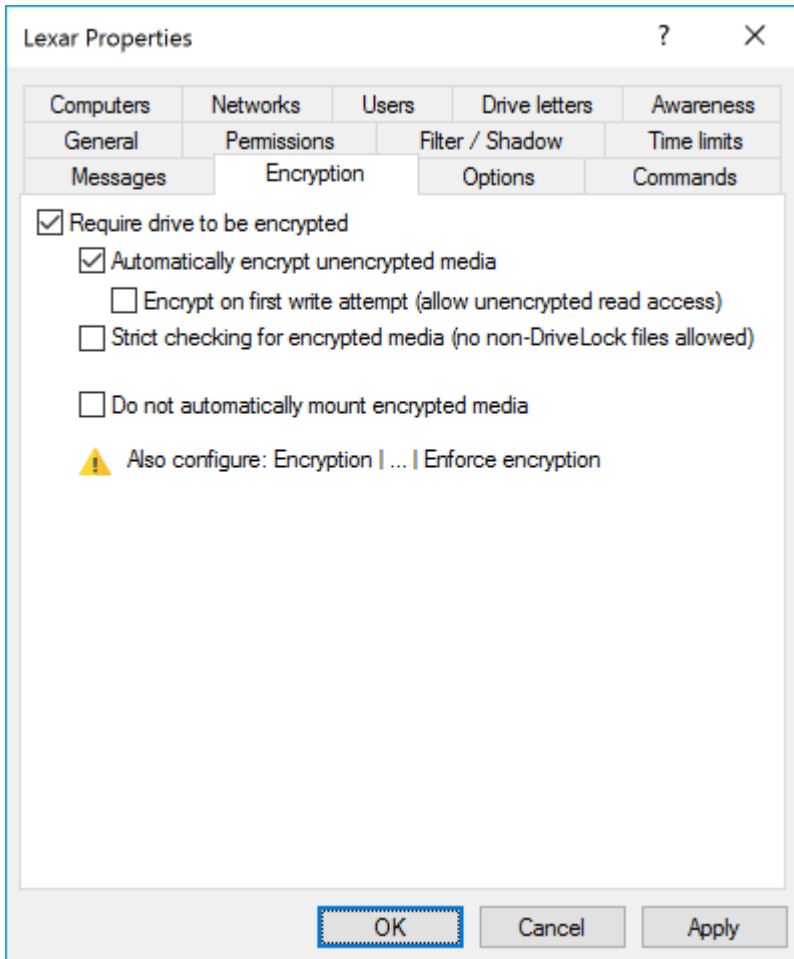
To also display the message when a user connects a drive and the rule allows access, select the **“Also display message when access is granted”** checkbox. To not display any notification message when this rule is activated, including any default language message that you defined for all drives, select the **“Display no message when rule is activated”** checkbox.

To not generate any audit events when this rule is activated, select the corresponding check box.

9.1.2.4.4 Additional Options

Encryption

On the **Encryption** tab you can configure settings for enforced encryption.



Select the **“Require drive to be encrypted”** checkbox to control whether removable drives must be encrypted.

If you select this option, DriveLock lets users access only encrypted removable drives; unencrypted drives are locked. You can also select whether a user will be prompted to encrypt an unencrypted removable drive when the user connects it to the computer.

If you select the **“Strict checking for encrypted media”** checkbox, DriveLock treats a removable drive as being encrypted only if it contains no files other than the following three:

- **.DLV (required)*: A DriveLock encrypted container file. The drive must contain exactly one encrypted container file to be treated as an encrypted drive by DriveLock.
- *DLMobile.exe (optional)*: The DriveLock Mobile Encryption Application.
- *Autorun.inf (optional)*: A file that instructs Windows to start the Mobile Encryption Application when the drive is inserted.

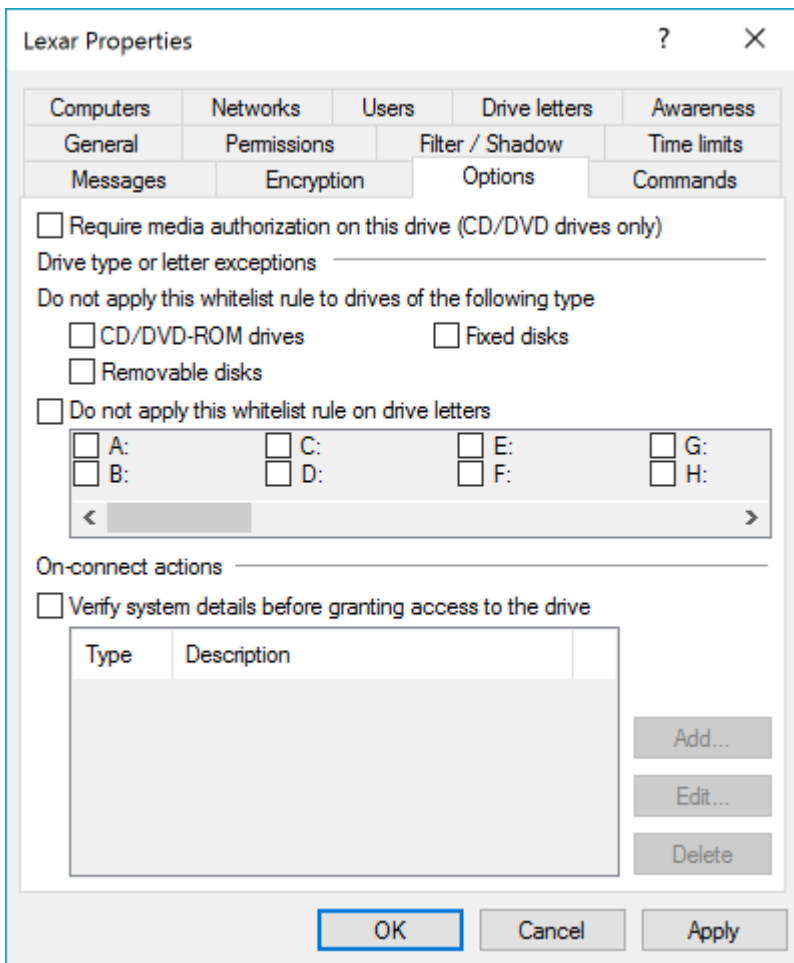
If the option **“Automatically encrypt unencrypted media”** is selected and a user connects an unencrypted removable drive that already contains files, you can configure under the settings for enforced encryption whether any existing files are retained or deleted.

When you want your users to mount encrypted drives manually, select **“Do not automatically mount encrypted media”**.

Due to technical limitations, the option “Require drive to be encrypted” is not available for CD drives, network drives and WebDAV drives.

Options

On the **Options** tab you can configure the following settings:

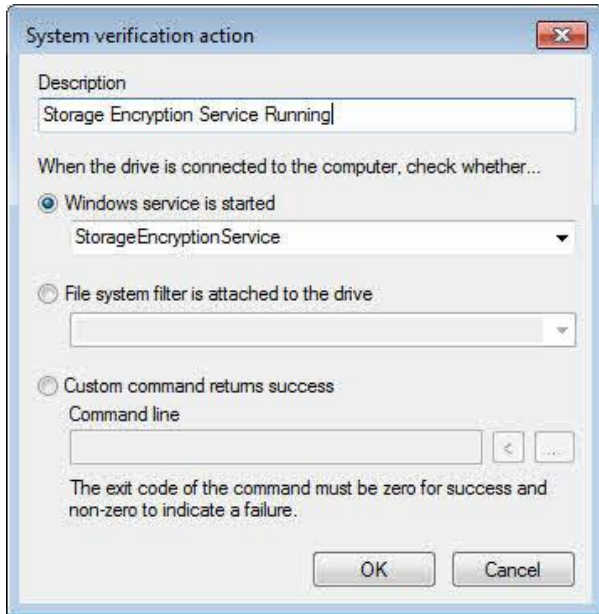


Select **“Require media authorization on this drive”** to only unlock a drive when it contains authorized media. Refer to the section [“Using Media Authorization”](#) for more information about this feature.

To enable the display of a usage policy each time a CD or DVD is inserted, you need to select the Require media authorization on this drive option. Without selecting this option the usage policy is only displayed when a CD/DVD drive is attached to the computer.

Some devices register with Windows as multiple drive types. For example, U3 drives appear both as a removable drive and a CD-ROM drive with identical manufacturer, model and serial number information. To configure unique settings for only one of these drives, select the drive types or drive letters to which the whitelist rule will not be applied. For example, to apply a whitelist rule only to the removable disk component of a U3 device, deselect the *CD/DVD-ROM* checkbox. With this setting DriveLock will apply the general rules to the CD/DVD-ROM drive, or you can create a separate whitelist rule for the CD drive.

To verify certain system settings on the client computer before granting access, select the **“Verify system details before granting access to the drive”** checkbox. Click **Add** to add system verifiers.



Type the display name in the Description field and then select from the following test types:

- To check whether a Windows service is running, select **“Windows service is started”** and then select a Windows service from the drop-down list.
- To check whether a DriveLock file system filter is attached to the drive, select **“File system filter is attached to the drive”**.
- To run a custom command, select **“Custom command returns success”**. A command can be any program that you can run from a command line, including program files, (.exe), Visual Basic scripts (.vbs) and Windows PowerShell scripts, that signals successful execution with a return code of 0.

Custom commands can be located in the file system on the client computer or the DriveLock Policy File Storage .

The DriveLock Policy file storage is a file container that is stored as part of a Local Policy, Group Policy Object or a DriveLock configuration file. The Policy File Storage can contain any file, such as a script that must be deployed to DriveLock Agents automatically along with the configuration settings.

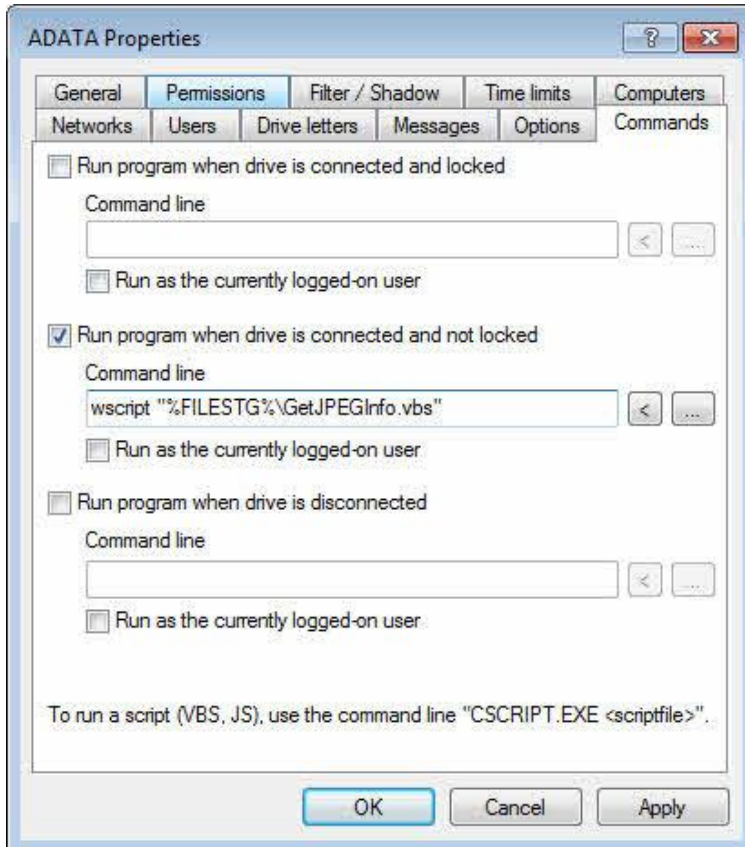
Files in the Policy File Storage are prefixed with an asterisk (*). You must use the Policy File Storage path variable along with any file stored in the Policy File Storage.

Click **OK** to save the action.

9.1.2.4.5 Specifying Commands

DriveLock can run a command that you specify each time one of the following events occur for a drive that a rule applies to:

- A drive is connected to the computer and is locked by the Agent
- A drive is connected to the computer and is not locked by the Agent
- A drive is disconnected from the computer



A command can be any program that you can run from a command line, including program files, (.exe), Visual Basic scripts (.vbs) and scripts for the new Windows PowerShell.

Common examples for actions you can perform by using a script are: Every time a specific external hard disk is connected to the computer, a backup script copies files from the internal hard disk to the external drive without requiring any user interaction. A PowerShell script can copy images from a digital camera to a network share automatically each time a camera is connected to the computer.

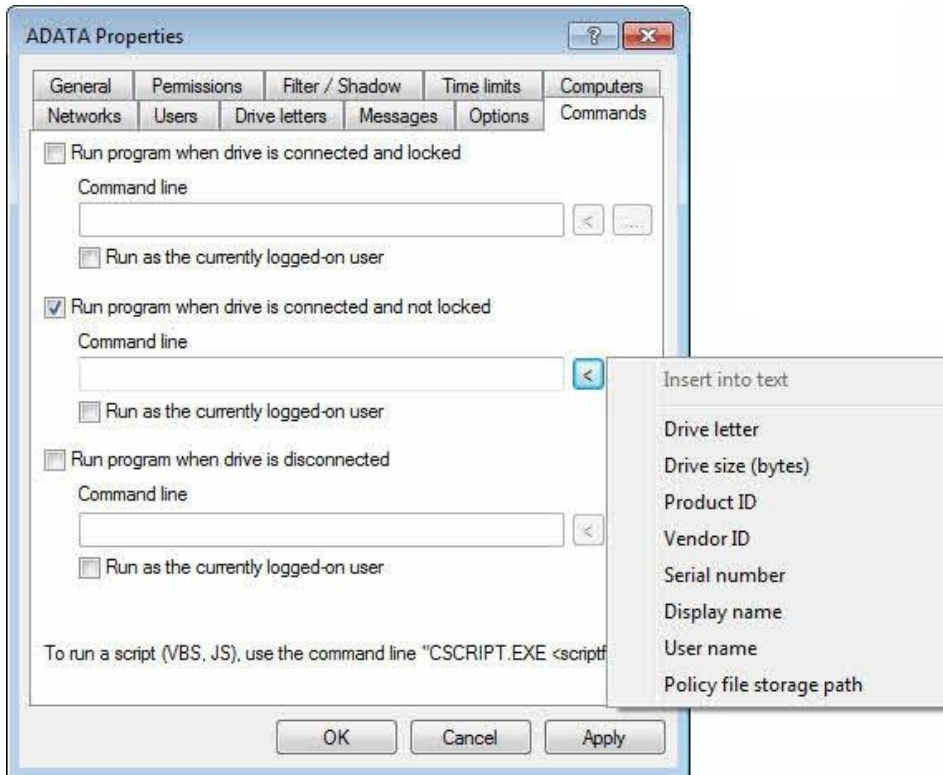
Or for example, you could use the command line script to have your anti-virus program check the external drive.

To start a VB script, you must type the complete path to the script file (for example, "wscript C:\Program Files\scripts\myscript.vbs").

You can use variables in commands and scripts that the Agent replaces with the actual values when running the command:

%LTR%	Letter assigned to the drive
%NAME%	Display name of the drive
%SIZE%	Size of the drive
%USER%	Name of the user who is logged on
%SERNO%	Serial number of the drive
%HWID%	Hardware ID of the drive

%PRODUCT%	Product ID of the drive
%VENDOR%	Vendor ID of the drive
%FILESTG%	Path to a file in the Policy file storage



To insert a variable into the command line, at the cursor position where you want the variable to appear, click “<” and then click the variable to insert.

Click the “...” button to select a file name and insert it at the cursor position. You can select a file from the following locations:

- The file system on the local computer
- The DriveLock Policy File Storage

The DriveLock Policy File Storage is a file container that is stored as part of a Local Policy, Group Policy Object or a DriveLock configuration file. The Policy File Storage can contain any file, such as a script that must be deployed to DriveLock Agents automatically along with the configuration settings.

Files in the Policy file storage are prefixed with an asterisk (*). You must use the Policy File Storage path variable along with any file stored in the Policy File Storage.

You can also specify whether the command is run using the identity of the local System account or the account of the user who is logged on at the computer when the command is run.

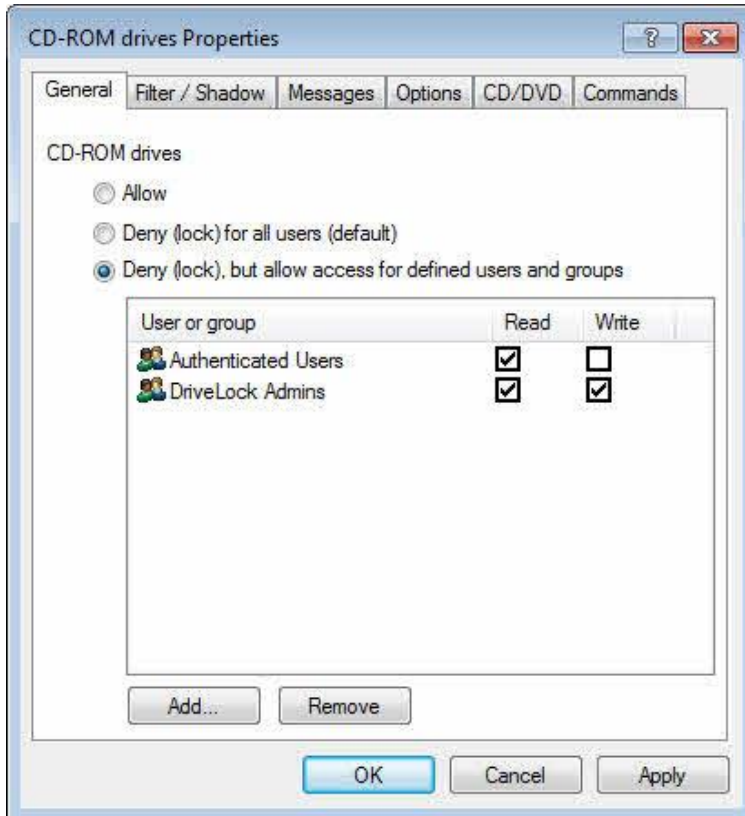
9.1.2.5 Locking and Controlling Recording to CDs/DVDs

To lock CD/DVD devices you configure settings for the CD/DVD drive class as described in the chapter “[Enabling Drive Locking](#)”.

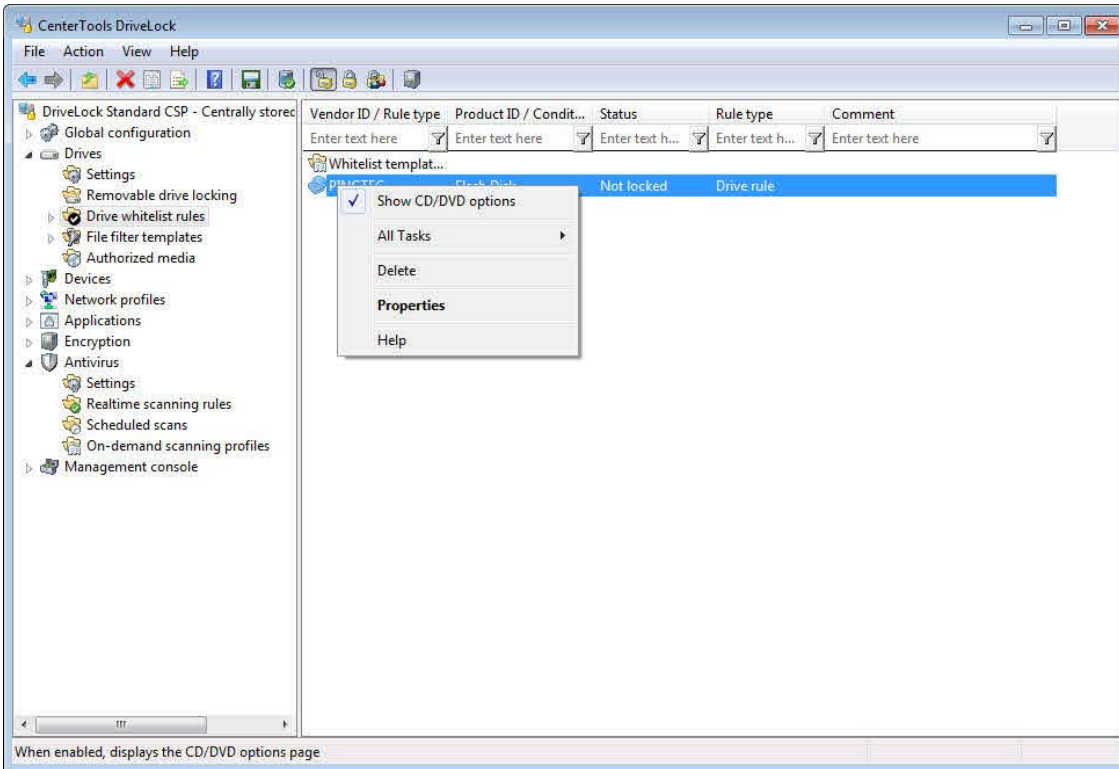
Often recording software bypasses Windows file system drivers to burn CDs or DVDs. DriveLock includes a system driver that is linked into CD/DVD drives as a lower filter to prevent bypassing normal file drivers in most cases.

Supported recording software includes Roxio (WinOnCD), Nero, Windows (IMAPI) and Infra-Recorder.

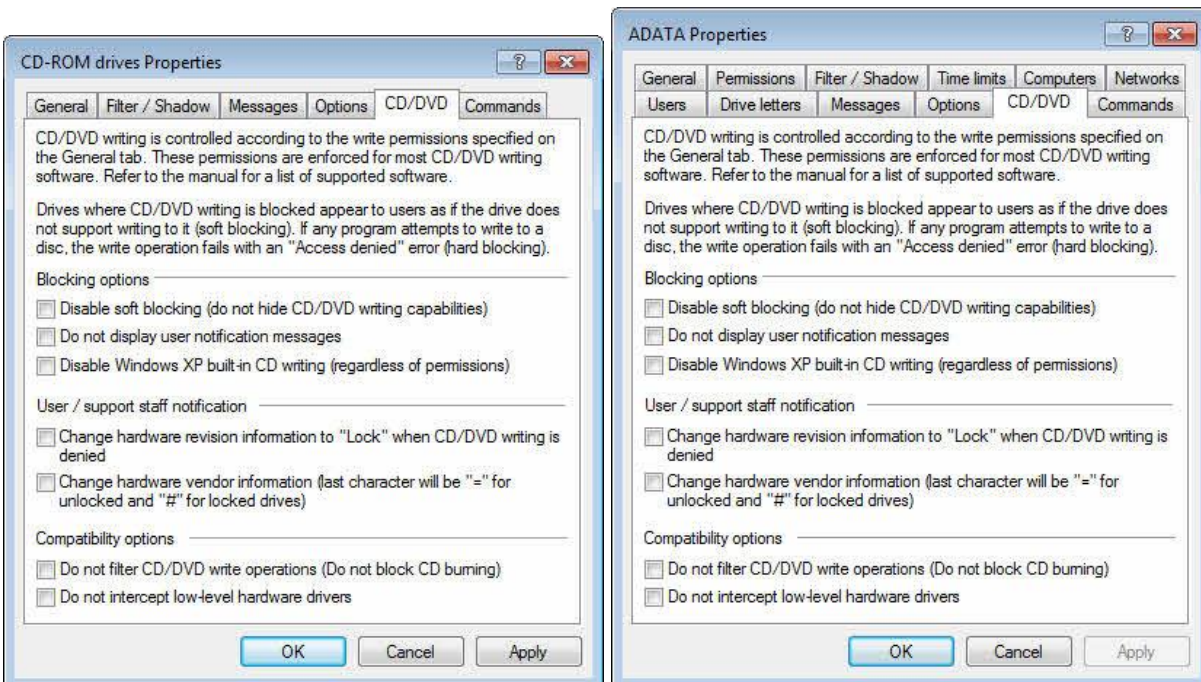
To allow some users to use recording software, while blocking others, configure the user permissions in a whitelist rule (or for the drive class) and allow or deny write access for specific groups.



You can also configure CD/DVD writing settings in a whitelist rule.



By default, the **CD/DVD** tab is disabled in whitelist rules. To enable the **CD/DVD** tab in a whitelist rule, right click the whitelist rule and then click Show CD/DVD options.



The configuration options for the CD-ROM class and whitelist rules are identical.

By default, DriveLock hides the recording device (soft blocking), and recording software usually will recognize the drive as non-recordable CD/DVD-ROM drive. Activate the **“Disable soft blocking (...)”** checkbox to deactivate soft blocking.

If you disable soft blocking (or when a recording software like Roxio bypasses the soft blocking capabilities of DriveLock), the user will get an “access denied” message when trying to write to a CD/DVD.

Select the “Do not display user messages” to prevent user messages from being displayed when soft blocking is active.

To disable Windows recording capabilities regardless of user permissions, select the “Disable Windows XP built-in CD writing (...)” checkbox.

To enable administrators to recognize DriveLock soft blocking, select one or both of the “User / support staff notification” checkboxes. DriveLock will change the hardware revision or vendor information, respectively.

For compatibility reasons you can turn off soft and hard blocking of CD/DVD recording completely by selecting the two compatibility option checkboxes.

9.1.2.6 Creating File Filters

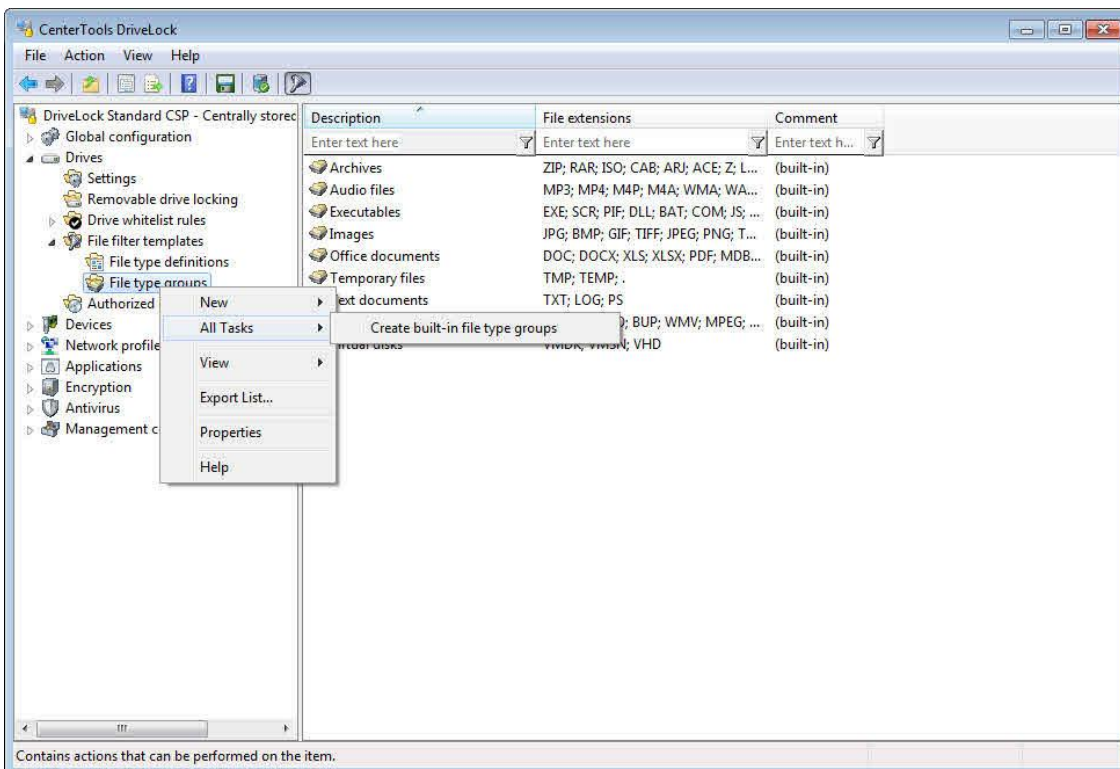
Use file filters to control access to specific file types in removable media rules and drive whitelist rules. File filters control which types of files users can read or write. For example, you can create a file filter template with read permissions for .jpg files and write permissions for .doc files. A single file filter template can include multiple permissions entries to match your security requirements.

DriveLock can check the headers of files to ensure that a file’s extension matches the file type that’s indicated by the extension. For example, it can check whether a file with a .doc extension is really a Microsoft Office file and not a graphics file that a user renamed. Note that some file formats share the same file header such as some Microsoft Office, while others have no file header at all or a variable file header.

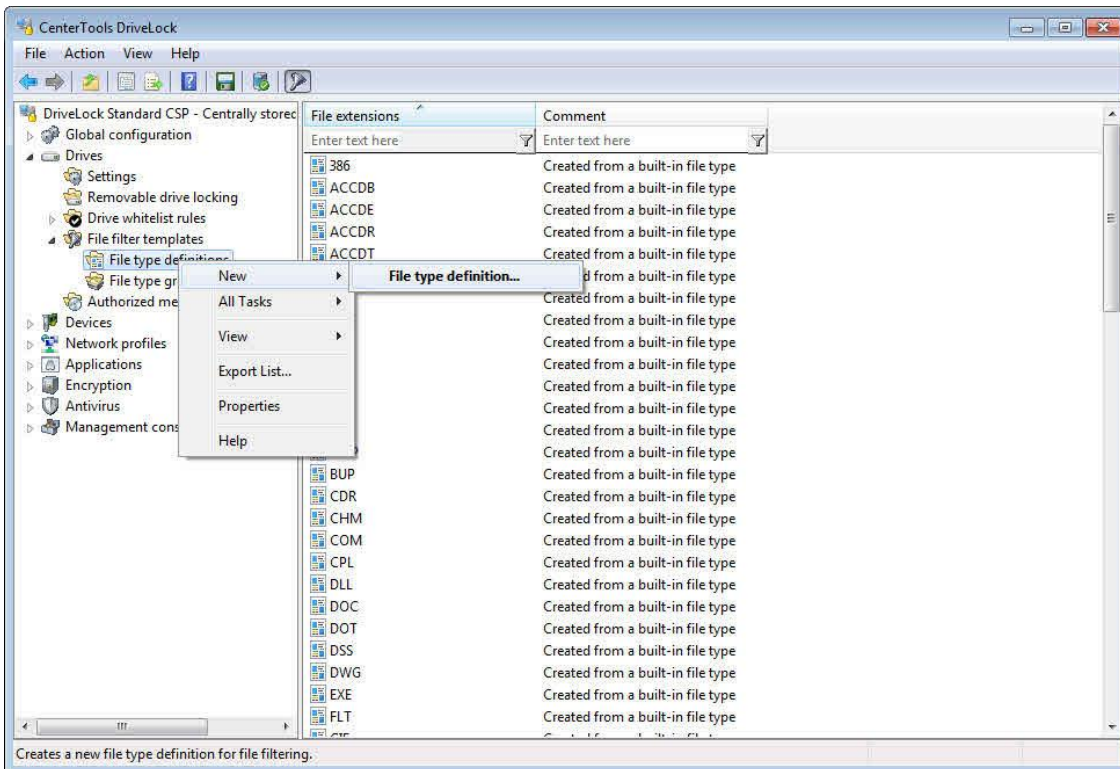
After you have configured a file filter template, you can use it in a drive class or a drive whitelist rule.

9.1.2.6.1 Defining File Types

DriveLock includes built-in file type definitions for many common file formats. You can define file types for additional file extensions by defining the content of these files.

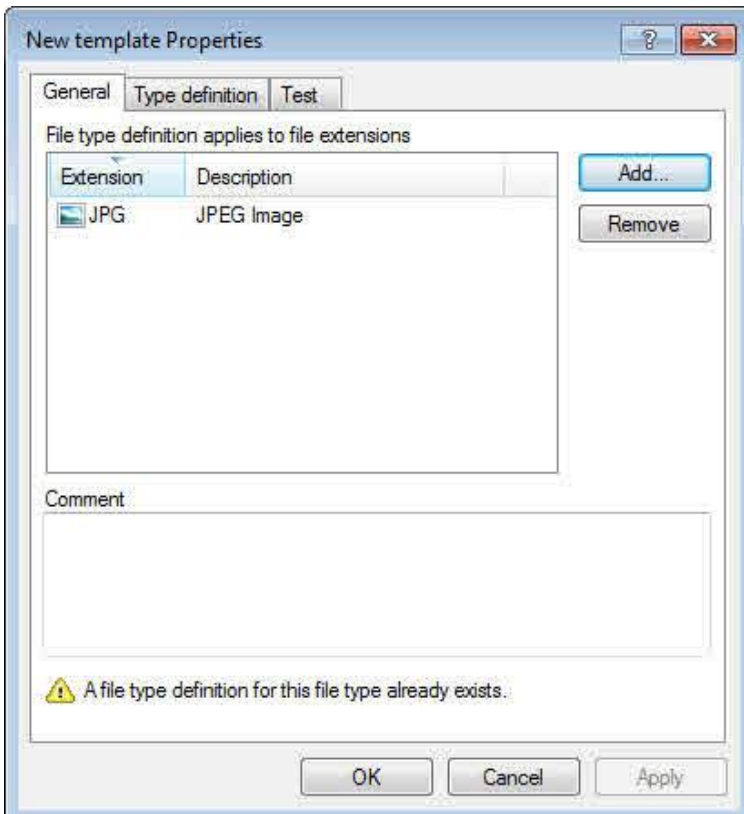


Before you can use built-in definitions you must generate a list containing the file extensions that are recognized by Windows on your computer. To create this list, right-click **File type definitions** and then click **All Tasks -> Create built-in definitions**.



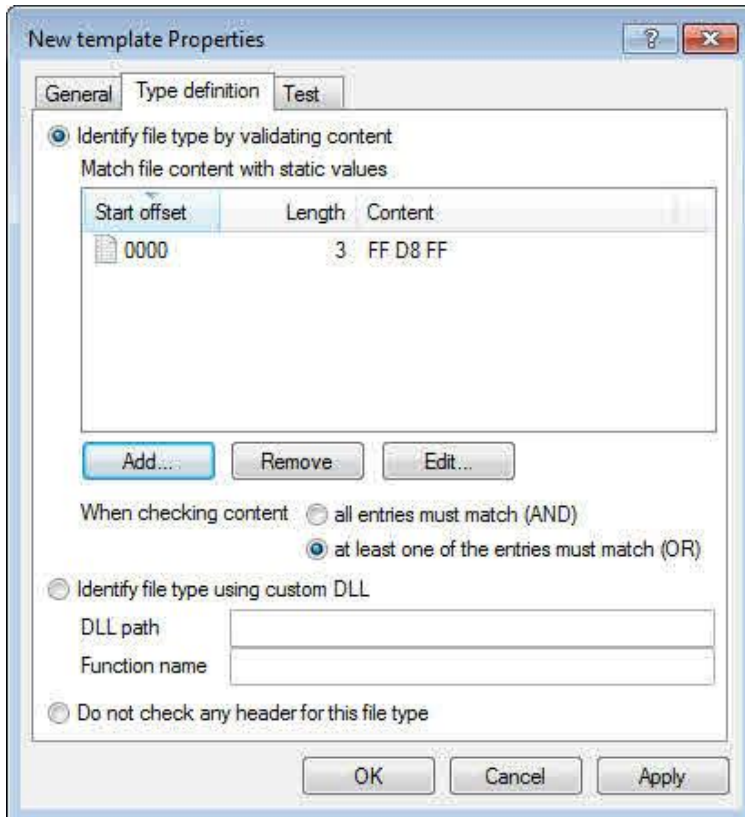
To create a new file type, right-click **File type definitions**, and then click **New -> File type definition**.

To change the definition of a file type in the list, double-click it.



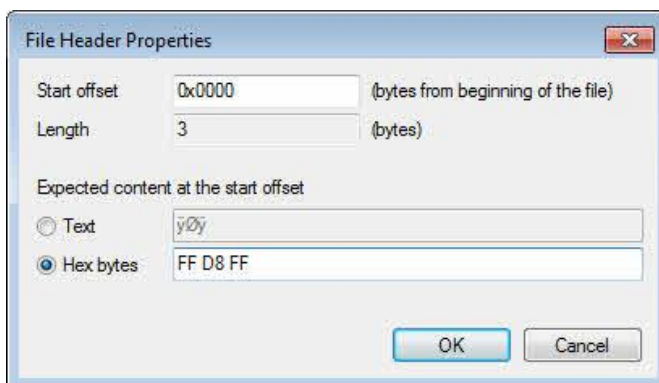
Click **Add** to add one or more file extensions to the file type definition.

Click the **Type definition** tab.



DriveLock can validate a file by checking its content or by using a custom Dynamic Link Library (DLL). Such custom DLLs contain code that you design to check the contents of a file.

Click **Add**, **Remove** or **Edit** to edit the list of content check conditions.



A content check conditions contains an offset (a hexadecimal value) and a content value that you can specify as text or as hexadecimal byte values. For the condition to match, the content must be present at the specific location in the file. DriveLock automatically calculates the length. Click **OK** to save changes.

Configure whether a file must match all conditions or only one of them needs to be validated.

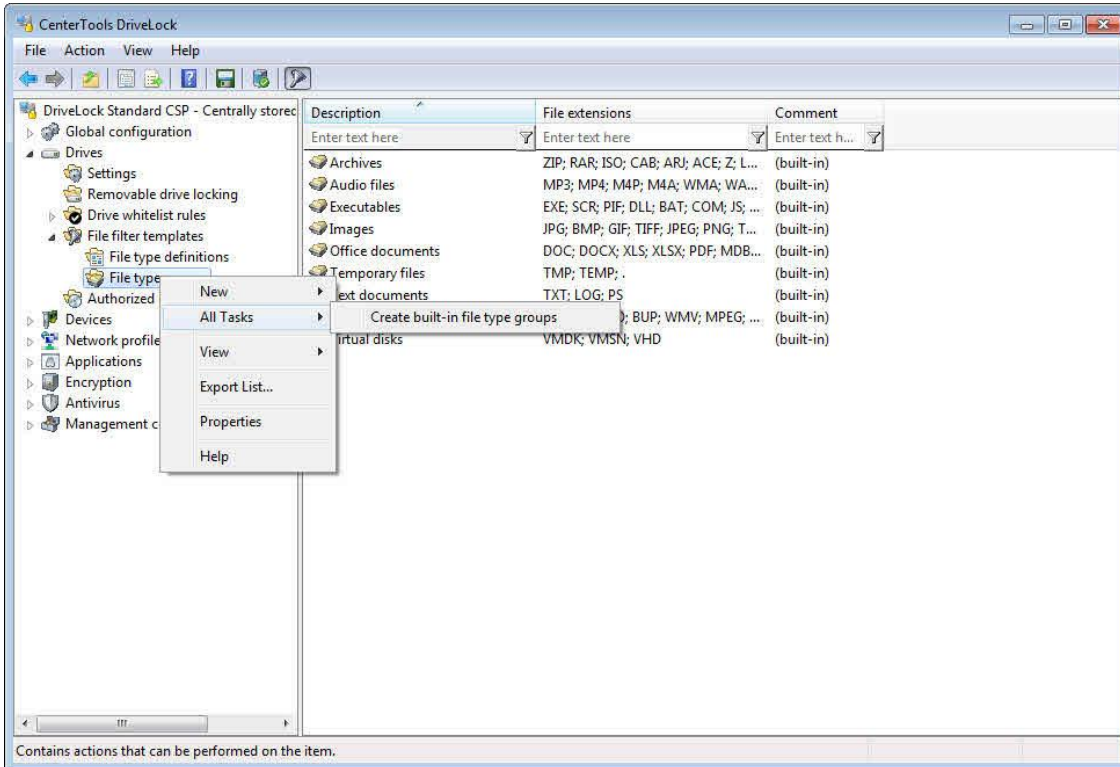
To use a Dynamic Link Library that you have developed, type the full path for the DLL file and the function name.

The DLL file must be stored locally on the disk. You can't use an UNC path or the Policy File Storage as a location.

Click **OK** to save the changes.

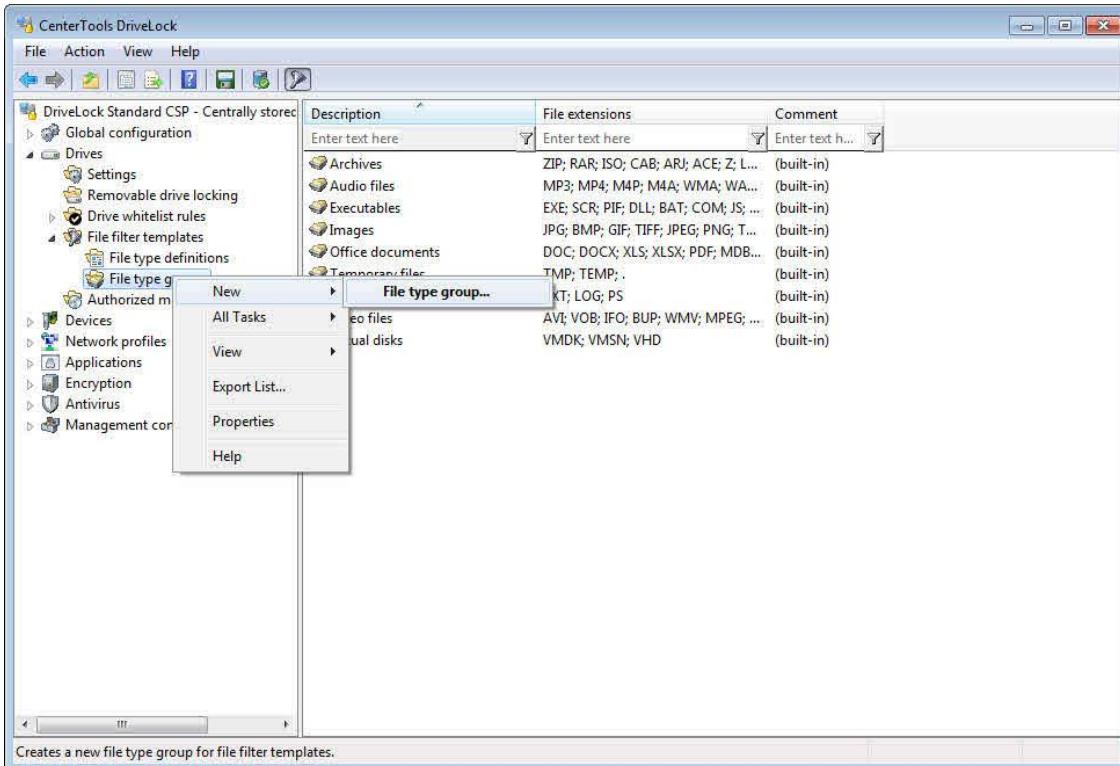
9.1.2.6.2 Defining File Type Groups

Use file type groups containing two or more file type definitions to add multiple file types to a rule in a single step. You can create your own groups in addition to the built-in file type group definitions, which cover many common scenarios, such as video files and images.

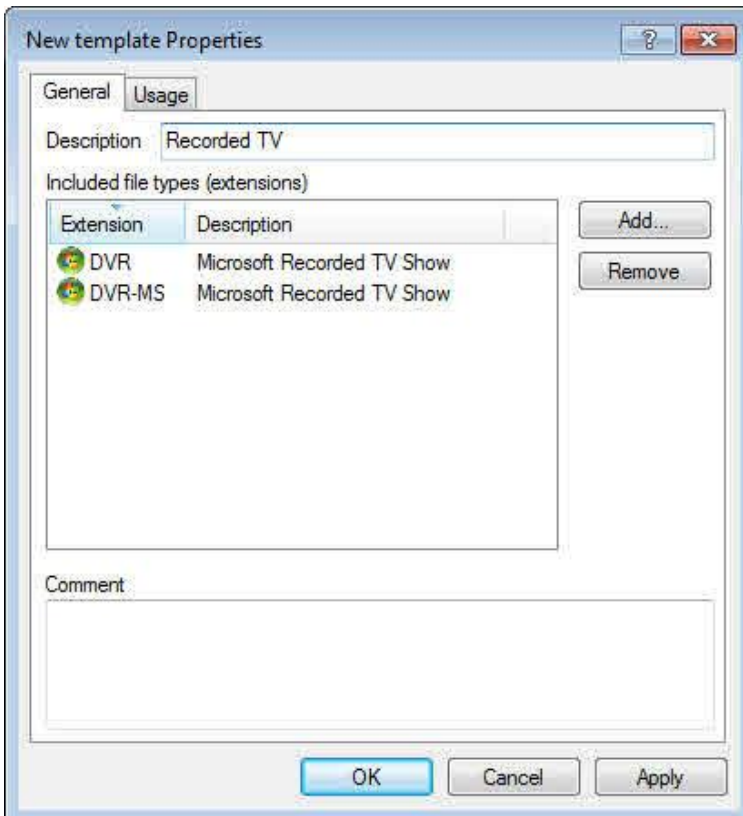


Before you can use a built-in group definition you must generate the group list. To create this list, right-click **File type groups** and then click **All Tasks -> Create built-in definitions**.

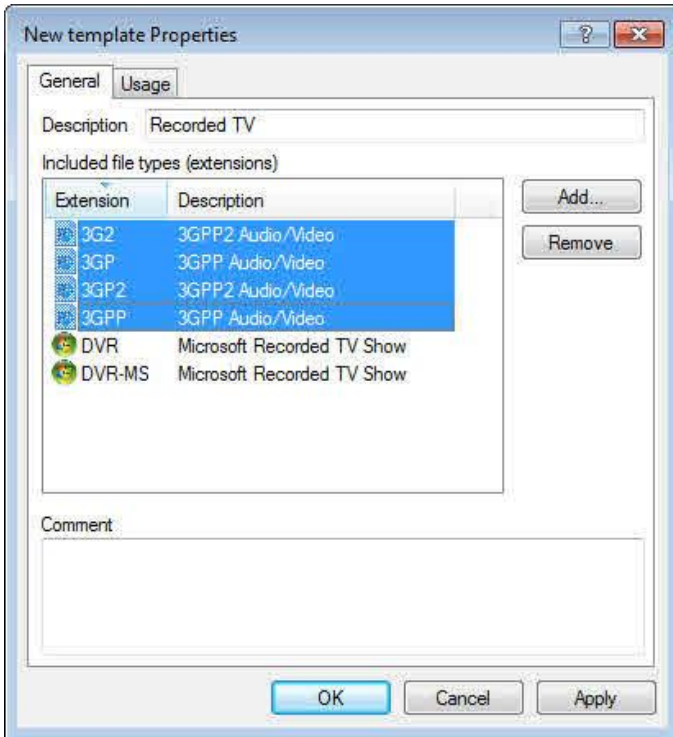
To change the definition of a file type group in the list, double-click it.



To create a new file type group, right-click **File type groups**, and then click **New -> File type group**.



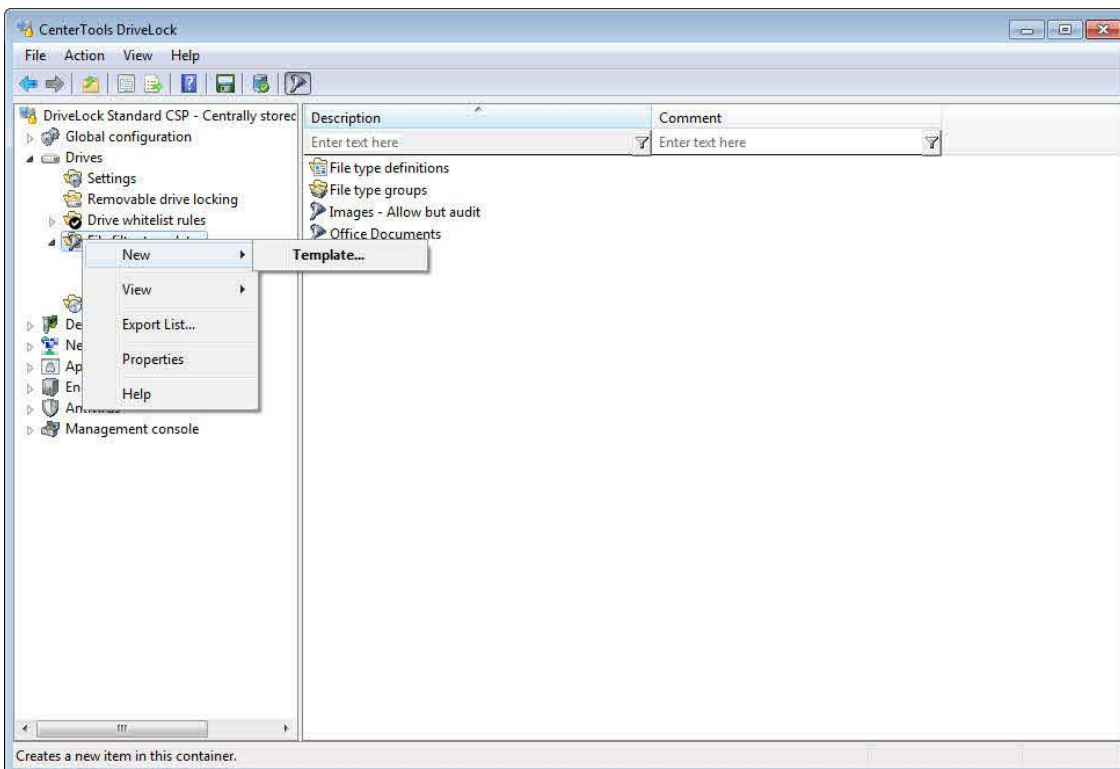
In the description field, type a group name. Click **Add** to add existing file types to the group. Select a file type and click **Remove** to remove the selected type from the list.



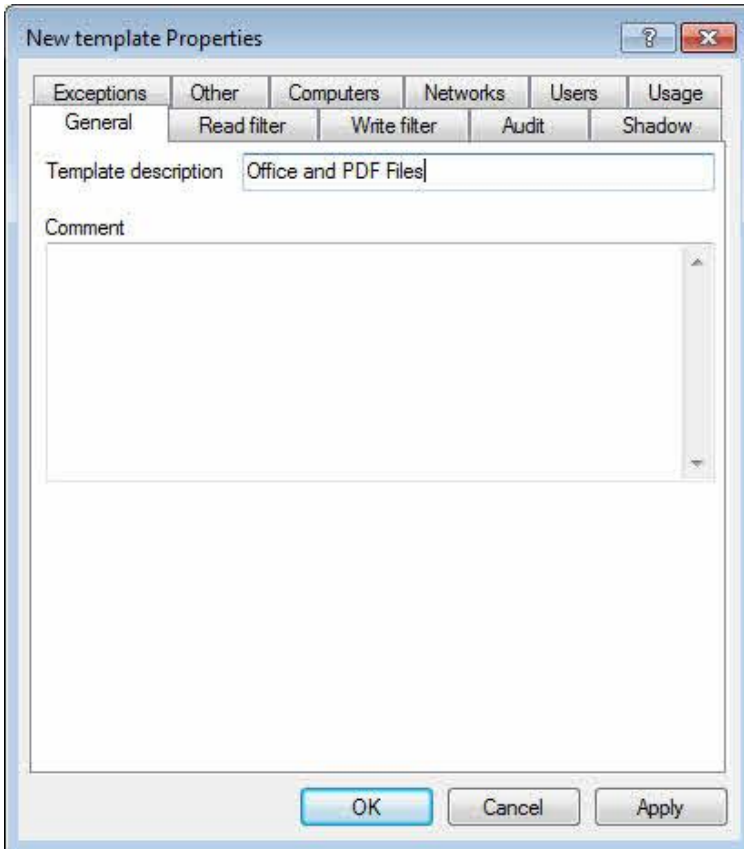
To select more than one file type, press and hold the **CTRL** key, and then click each file type. Click **OK** to add the selected file types to the list.

Click **OK** to save the file type group.

9.1.2.6.3 Creating a New File Filter Template

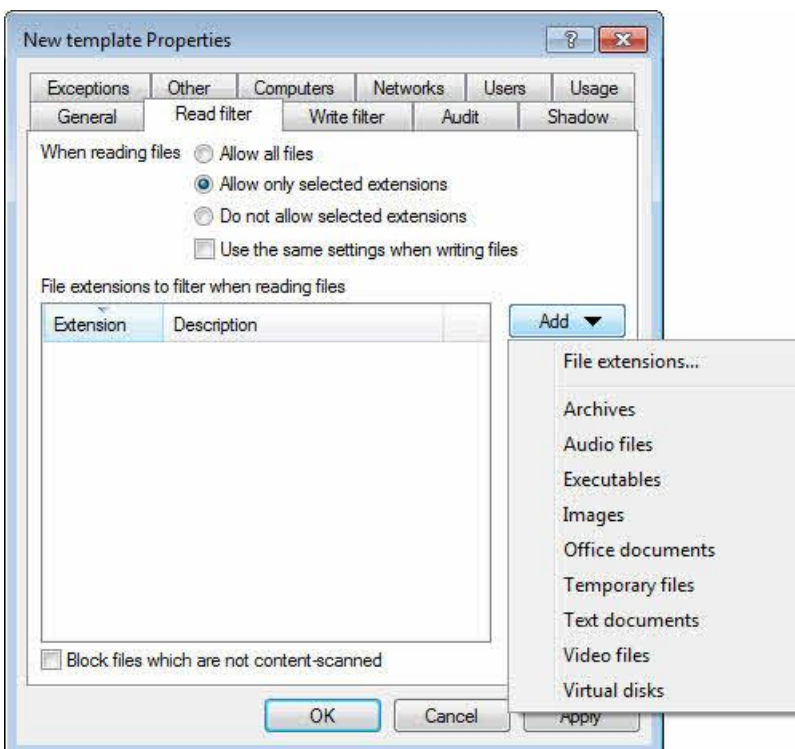


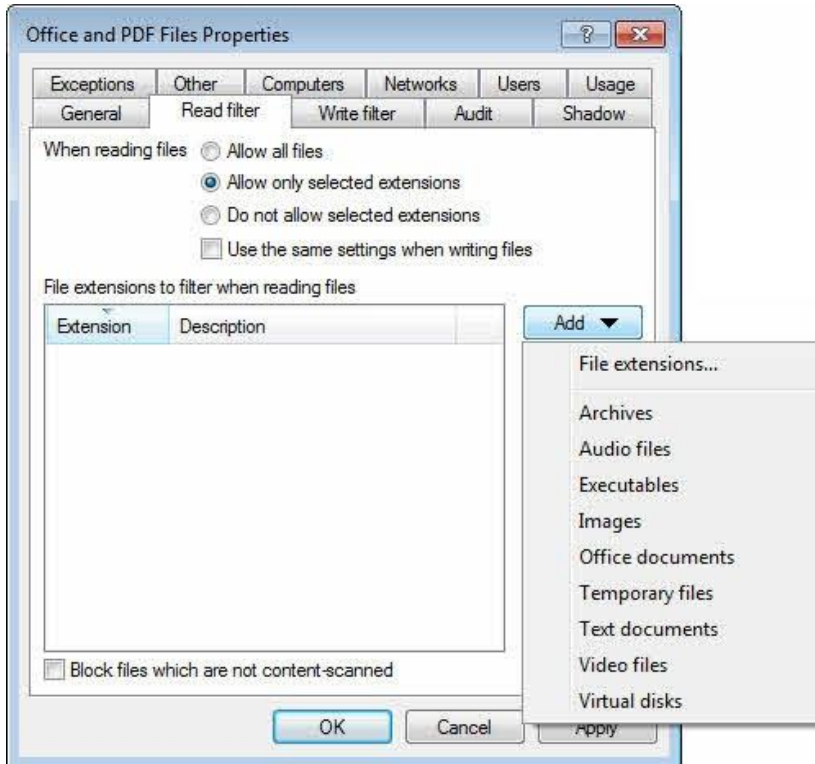
In the console tree, expand **Drives**, right click **File filter templates** and then click **New -> Template**



In the description field, type a name for the template. If desired, type a comment.

Click the **Read filter** tab.



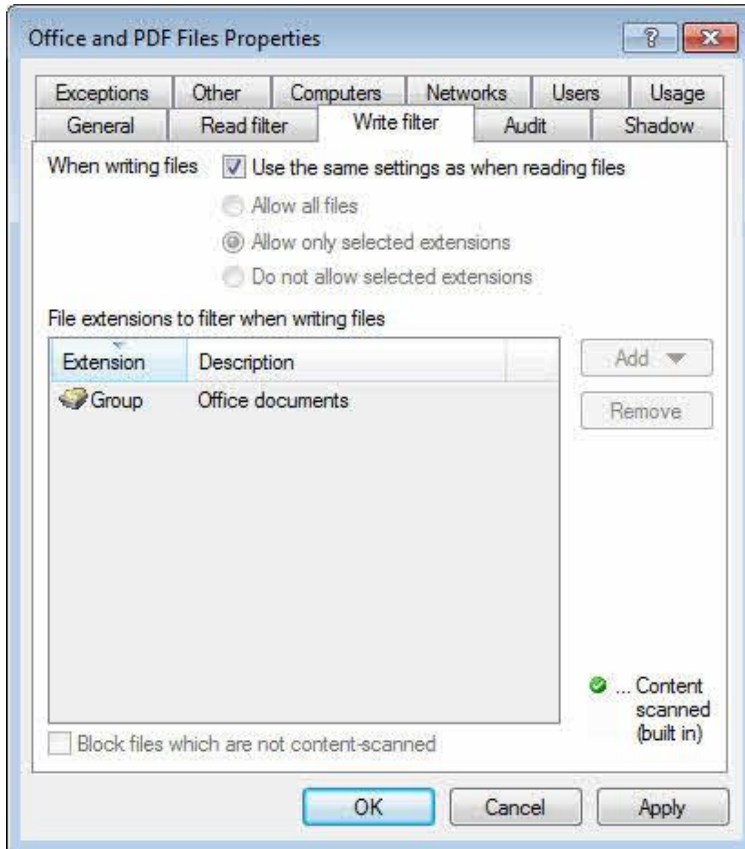


The file extensions specified on this page are checked when a file is copied or read from a drive.

To allow all file extensions, select “**Allow all files**”. To allow only certain file types, select “**Allow only defined extensions**”. To block certain files, select “**Do not allow defined extensions**”.

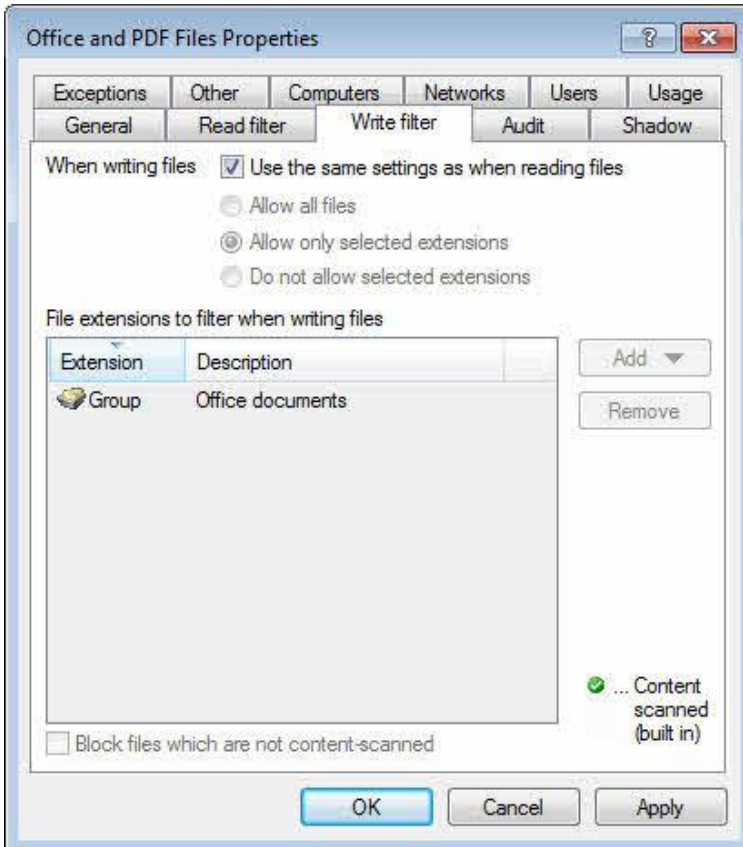
Click **Add** -> **File extensions** to add one or more file extensions to the list. To add a file type group to the list, click **Add** and then select the group.

Select or type the appropriate file extension, and then click **OK** to add the file extension to the list.

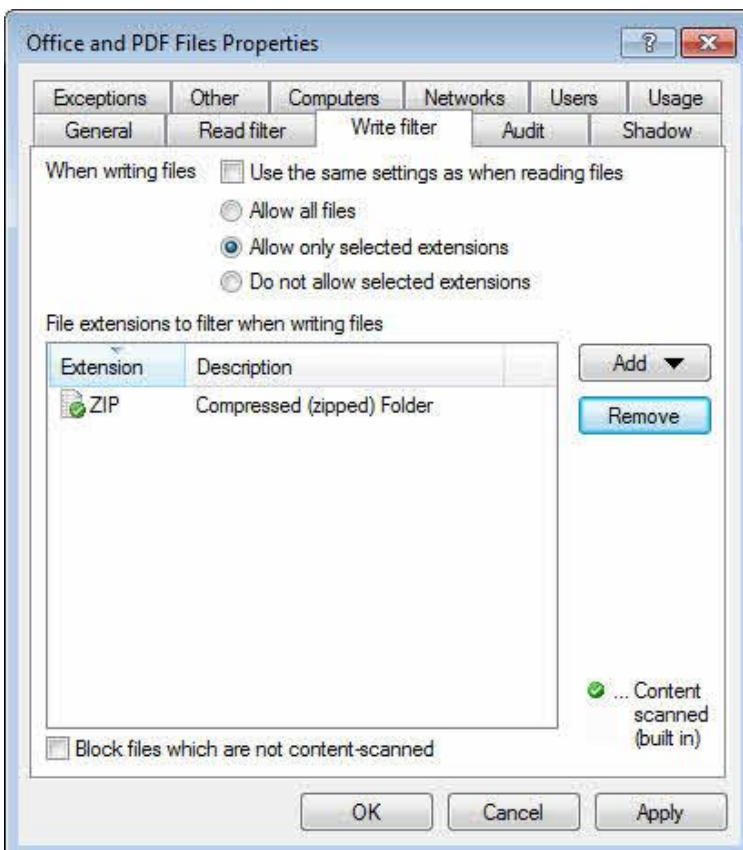


To specify files without an extension, type a period (.) instead of an extension. For example, this may be required for files created by Microsoft Excel 2003 and earlier. These versions of Excel save a file by first creating a temporary file without an extension and then creating a file with the extension .xls.

Click the **Write filter** tab.



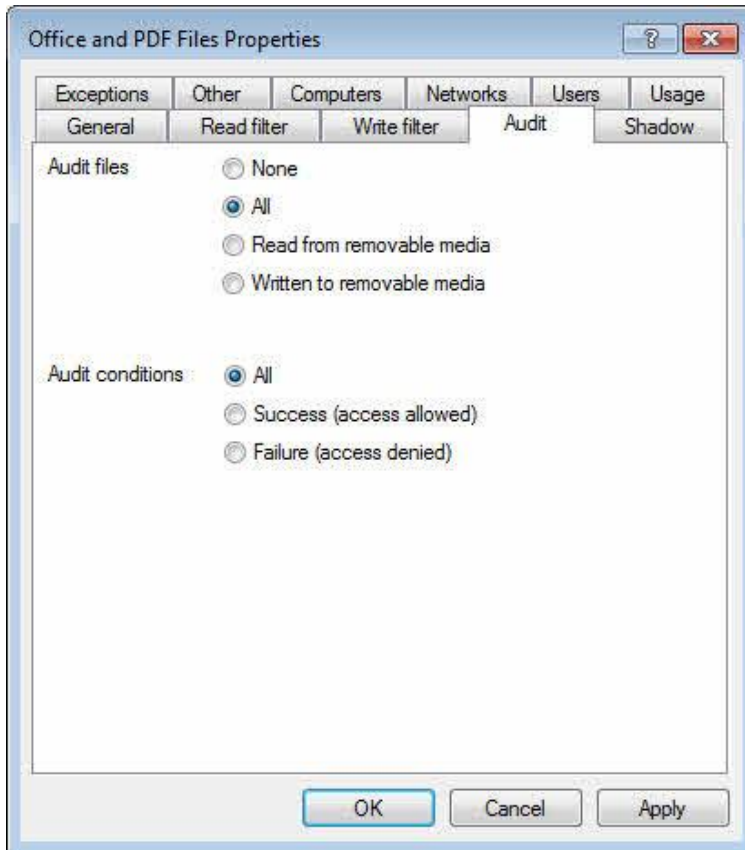
The file extensions specified on this page are checked when a file is copied or written to a drive.



To allow all file extensions, select **“Allow all files”**. To allow only certain file types, select **“Allow only defined extensions”**. To block certain files, select **“Do not allow defined extensions”**.

Click **Add** to add one or more file extensions to the list.

Click the **Audit tab**.



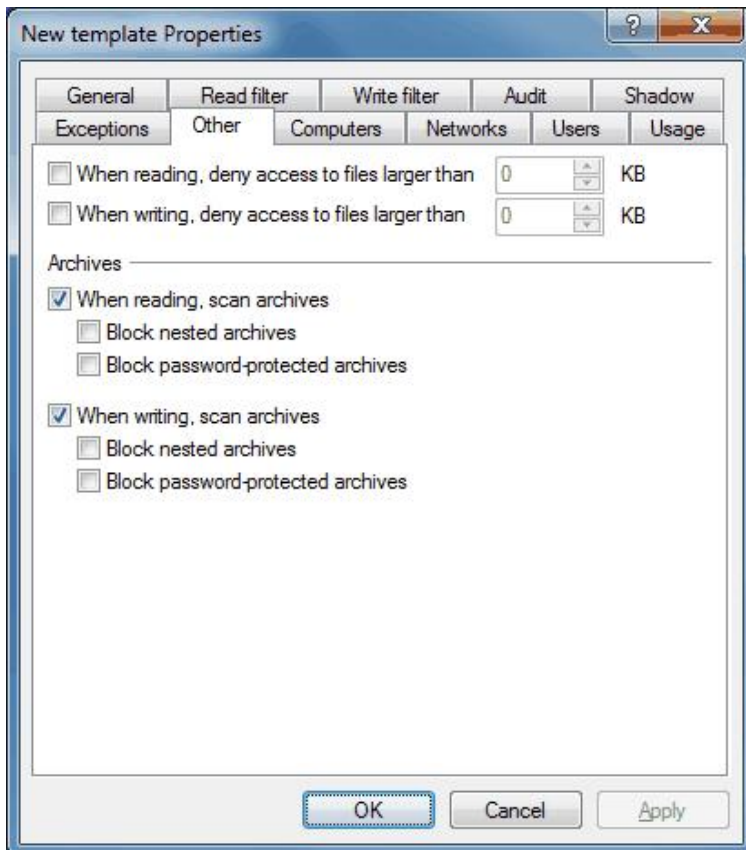
The file audit settings define when an audit event is generated. Configure the audit settings to match your audit policy.

Audit events can be sent to the Windows Event Log and, if configured, to the DriveLock database.

File auditing can impact system performance. Also some user actions may generate multiple audit events. For example, opening a Word document may generate three separate events because Word reads the file, writes some information to it (last time accessed) and then reads the file again.

Settings on the tabs **Shadow** and **Exceptions** are explained in the section [“Configuring Shadow Copies in Drive Whitelist Rules”](#)

Click the **Other** tab.



Select one of the “... deny access to files larger than” checkboxes and specify a size to prevent read and/or write access to large files.

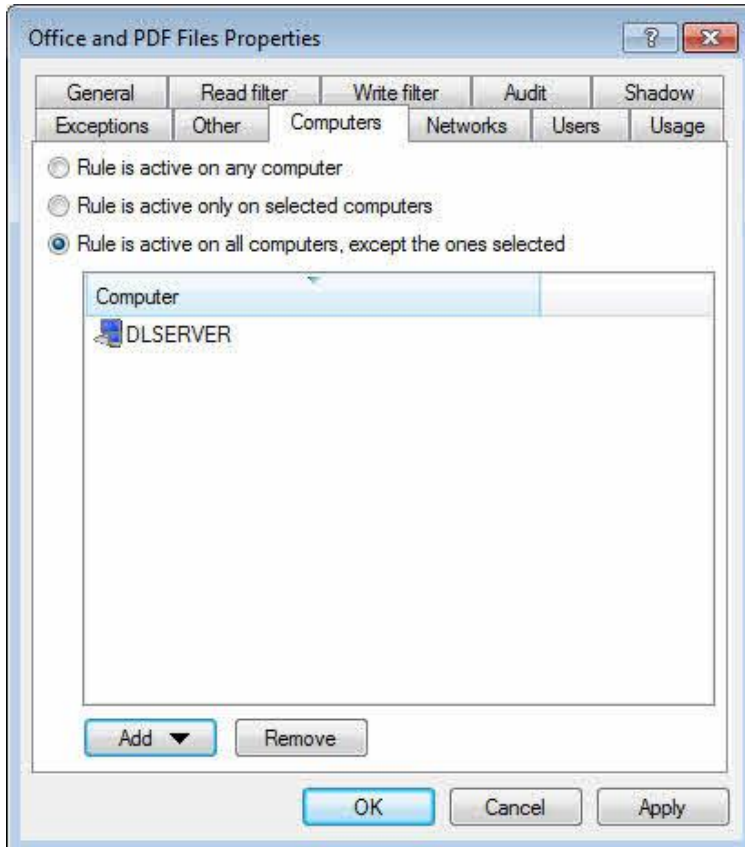
To enable DriveLock to apply the file filter to compressed archive files (ZIP and RAR), additional options exist for reading and writing such files. To enable DriveLock to apply the file filter settings to files contained in an archive, select one or both of the “...scan archives” checkboxes.

To block access to compressed archives that contain other compressed archives, select one or both of the “Block nested archives” checkboxes.

To block access to password-protected archives, select one or both of the “Block password-protected archives” checkboxes.

Scanning compressed archive files on network and WebDAV drives is currently not supported.

Click the **Computers** tab.

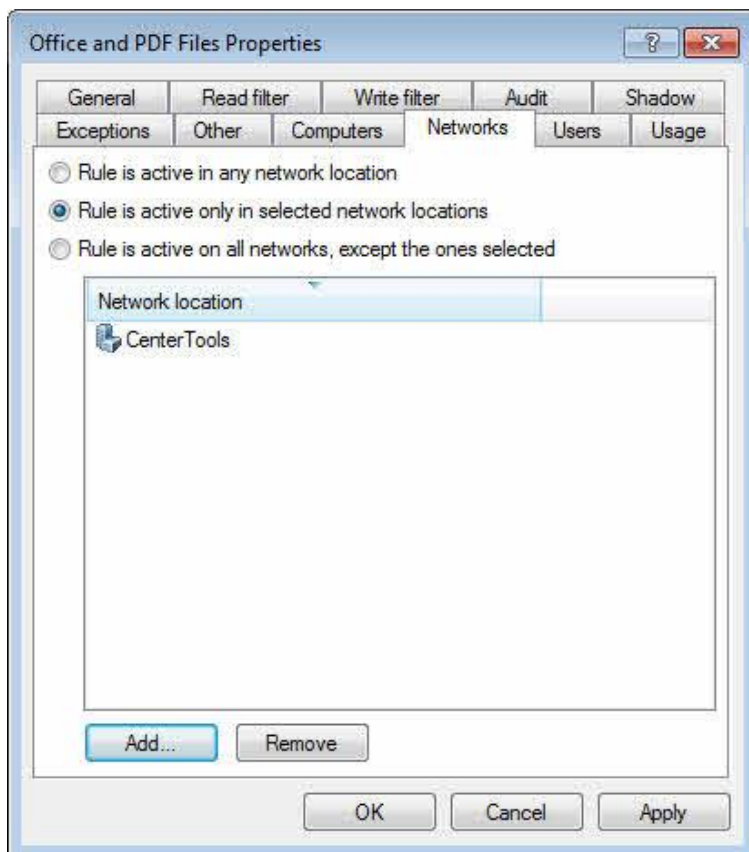


Select from the following options:

- Activate this template on all computers
- Activate this template only on the specified computers
- Exclude the specified computers from this template

Click **Add** to add more computers to the list.

Click the **Networks** tab.

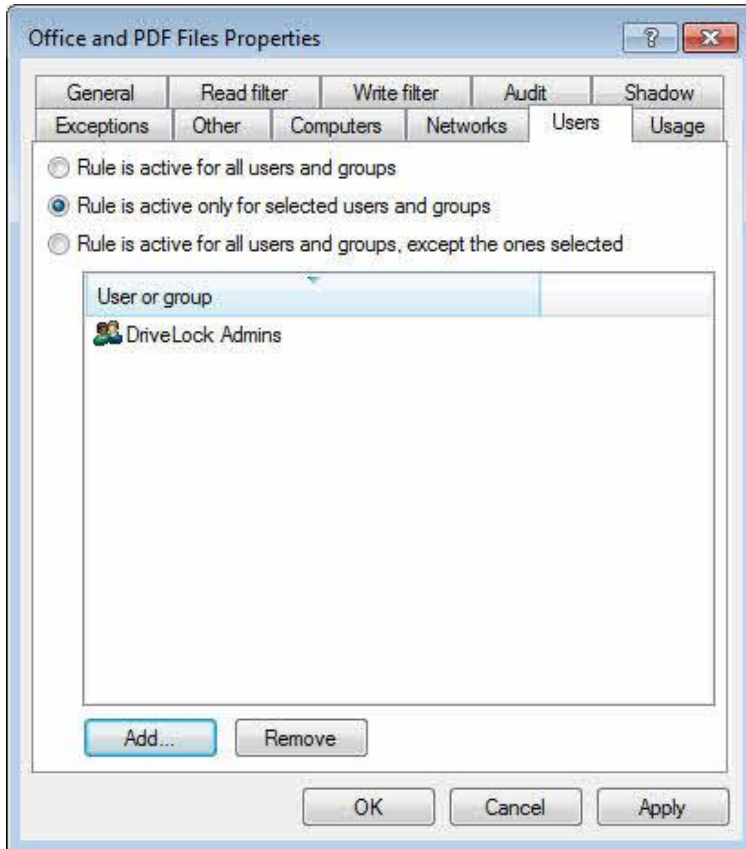


Select from the following options:

- Activate this template in all network locations
- Activate this template only in the specified network locations
- Exclude the specified network locations from this template

Click **Add** to add more defined network locations to the list.

Click the **Users** tab.



Select from the following options:

- Activate this template for all users
- Activate this template for the specified users
- Exclude the specified users from this template

Click **Add** to add more users or user groups to the list.

Select the **Usage** tab to view the drive whitelist rules that use the current template.

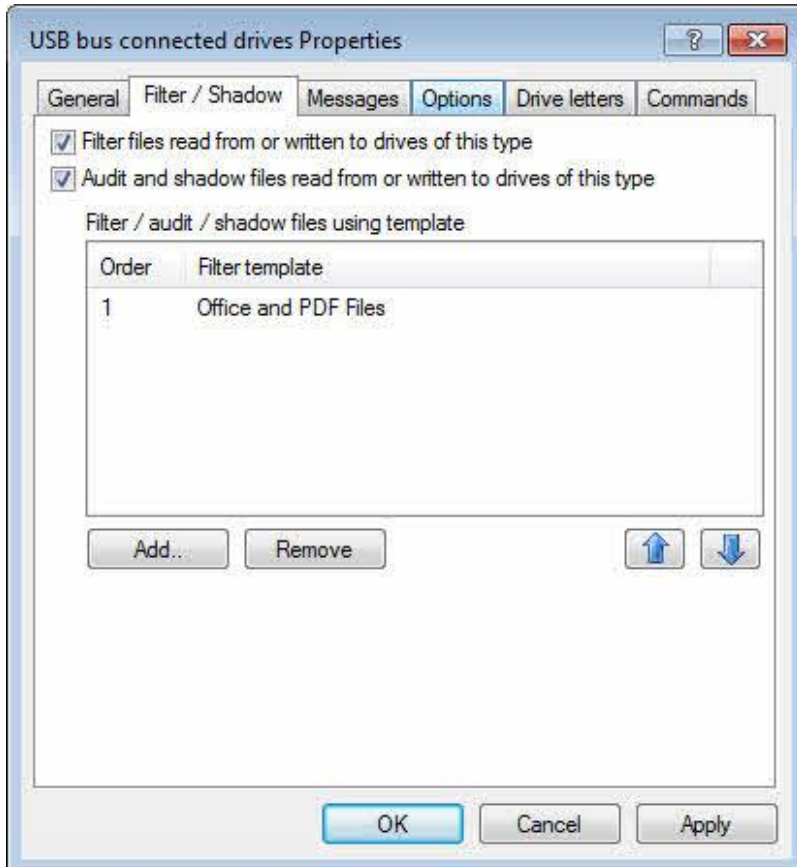
Click **OK** to save the template.

9.1.2.6.4 Using a File Filter Template



Use a filter template to configure filter settings for one of the drive classes or a drive whitelist rule.

To assign a filter template to a class rule, open the Properties dialog box for the rule, and then click the **Filter/Shadow** tab.

Select **“Filter files...”** to apply the file filter settings in the selected filter template(s). Select the **“Audit and shadow files...”** checkbox to enable the auditing and shadowing settings.



You can also use file filters in whitelist rules. By default a whitelist rule uses the filter settings you configured for the corresponding drive class. To configure a different filter, clear the “**Use the filter settings ...**” checkbox, and then select the “**Filter files...**” and/or “**Audit and shadow files ...**” checkboxes.

Click **Add** to add one or more previously created filter templates. Click **Delete** to remove the selected template from the list. Click  and  to move the selected template up or down.

When DriveLock applies this whitelist, it evaluates all filter templates in the list, starting from top. The first template matching all specified criteria (“file size”, “exceptions”, “user and groups”, “computer” or “networks”) is applied, any templates that follow are ignored. The following example illustrates this process: You created two templates: The first template applies to administrators and does not filter files. The second template applies all users and blocks access to program files. If administrator attempts to access a program file, DriveLock applies first template and access is granted. If a user who is not an administrator, DriveLock ignores the first template and instead applies the second template, blocking access to the program file.

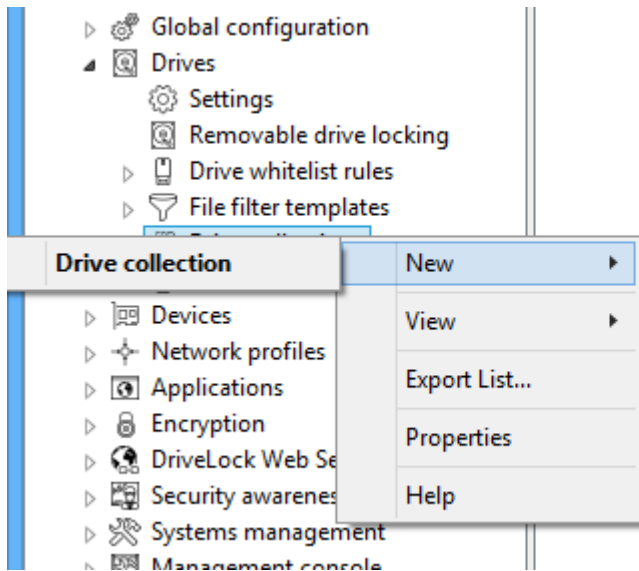
9.1.2.6.5 Using File Filter Templates with Encrypted Drives (Encryption 2-Go)

An additional step is required to use a file filter template for removable drives that have been encrypted using DriveLock removable media encryption (Encryption 2-Go). When you configure a file filter for the removable drive, this filter only applies to any unencrypted portion of the drive, which users are commonly not allowed to access. Once the encrypted container on such a drive is mounted using a drive letter, DriveLock treats it as belonging to the class *Encrypted volumes*, even though the physical drive may be connected using a USB port.

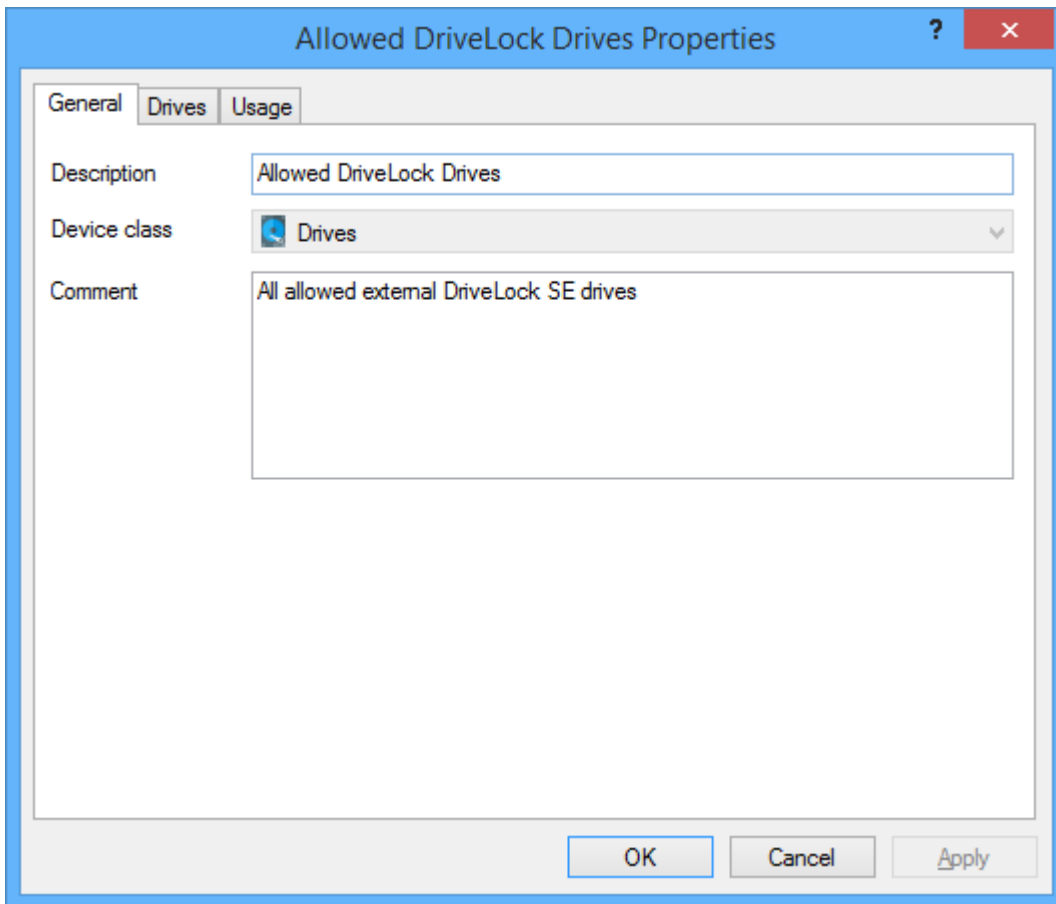
For a file filter template to apply to an encrypted volume, you need to enable filtering and/or auditing and select the template on the *Filter Shadow* tab under *Drives -> Removable drive locking -> Encrypted volumes*.

9.1.2.7 Creating Drive Collections

A method of simplifying the configuration of settings and rules and reducing the number of whitelist rules required is to group all drives to which the same settings apply first into a drive collection and then create a drive collection rule for that collection with all settings.

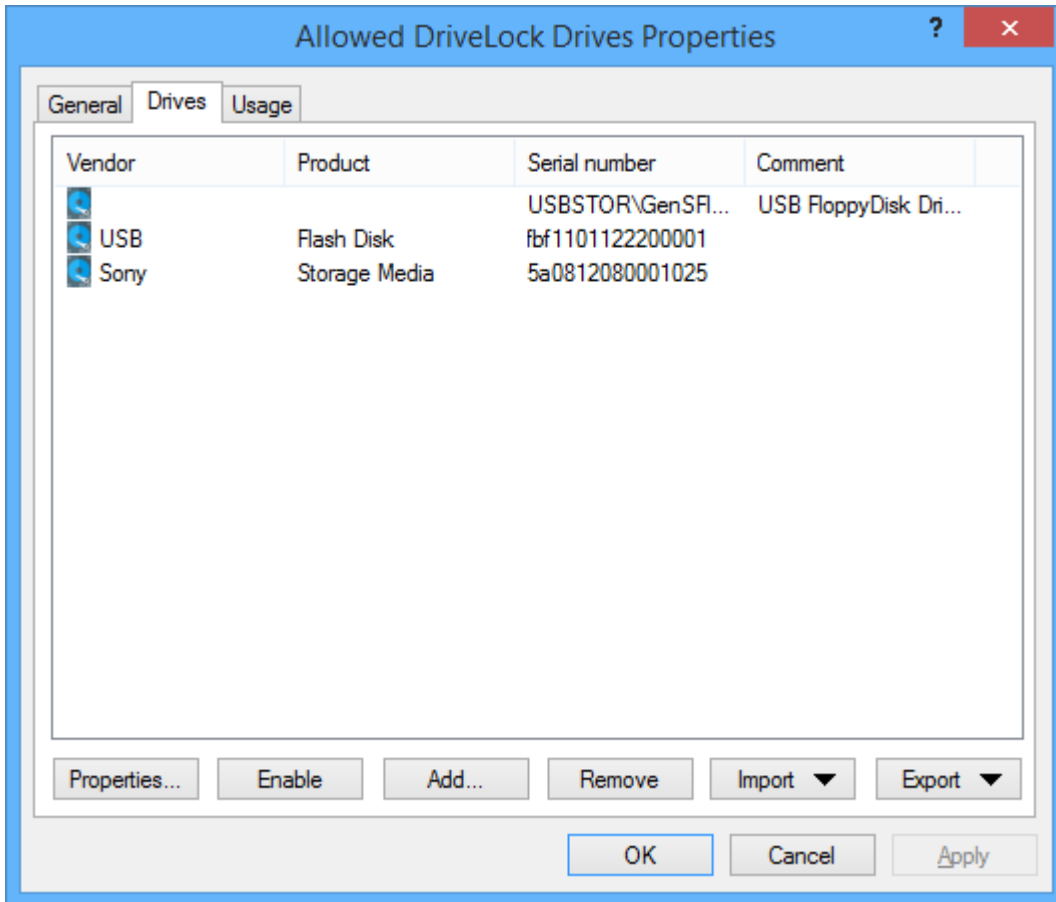


To create a new drive collection, right-click **Drive collections** and select **New -> Drive collections** from the context menu.



Enter a description and an optional comment. The "Device class" is automatically set to "Drives" and cannot be changed here.

Select the **Drives** tab.



Here you can display, deactivate, edit and remove existing entries. You can also add new entries.

To add new entries, click **Add** and select whether you want to add a drive based on its product or vendor ID, or by its hardware ID. Enter the required information in the next dialog or select it as usual from the currently connected devices or the Device Scanner database by clicking "...".

If you do not want to delete existing drives completely, but only remove them from the collection for a certain time, select the drive you want and then click **Disable**. A small additional icon now indicates that the entry is currently not enabled and cannot be locked/unlocked using this collection. Disabled items can be re-enabled later.

Use the **Import** button to import multiple drives in either CSV or INI format. A CSV file could look like this, for example:

HardwareID	Comment	Vendor	Product	SerialNumber
		USB	Flash Disk	fbf1101122200001
		Sony	Storage Media	5a0812080001025
USBSTOR\GenSFloppy	USB FloppyDisk Drive			

Click **Export** to save the current list as a CSV or INI file.

Tip: If you created some entries individually and then exported them as a file, you can use this file as the basis for an import, since it already has the correct structure and/or the necessary columns.

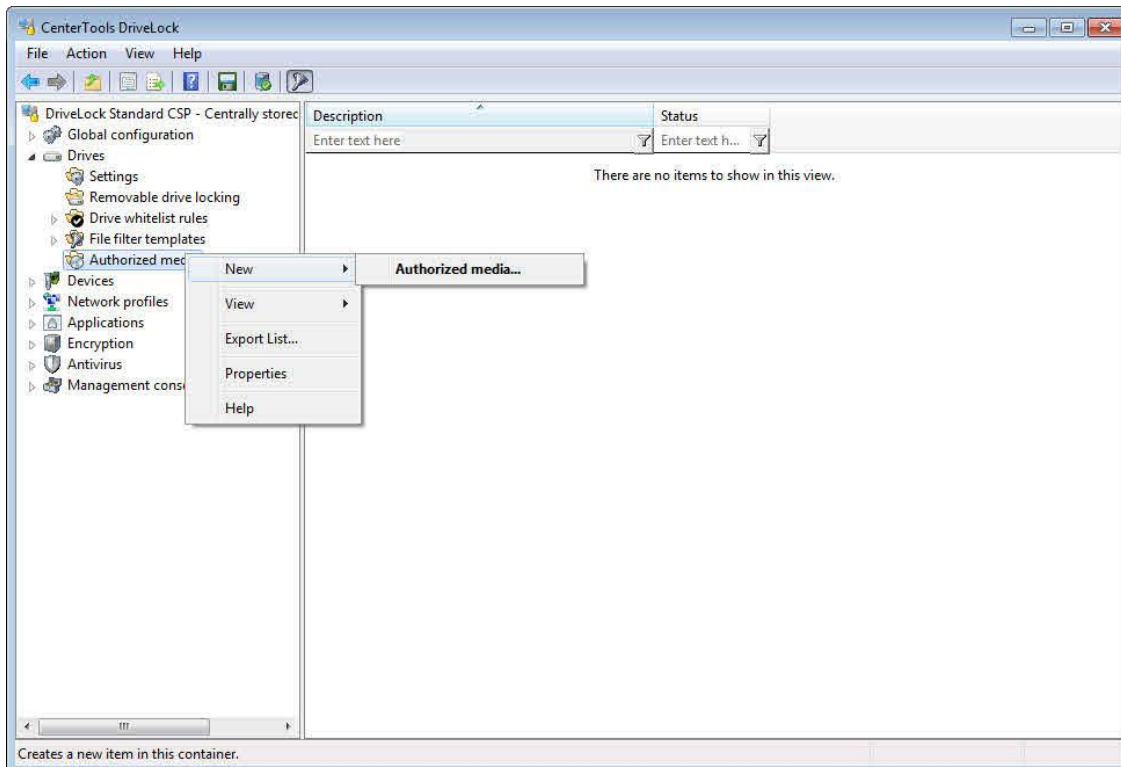
The **Usage** tab shows you the drive collection rules where the collection is used already.

9.1.2.8 Using Media Authorization

Use the Authorized Media option to unlock specific media even though CD/DVD drives are locked. For example, you can allow the use of a DVD containing training videos while blocking the use of all other DVDs.

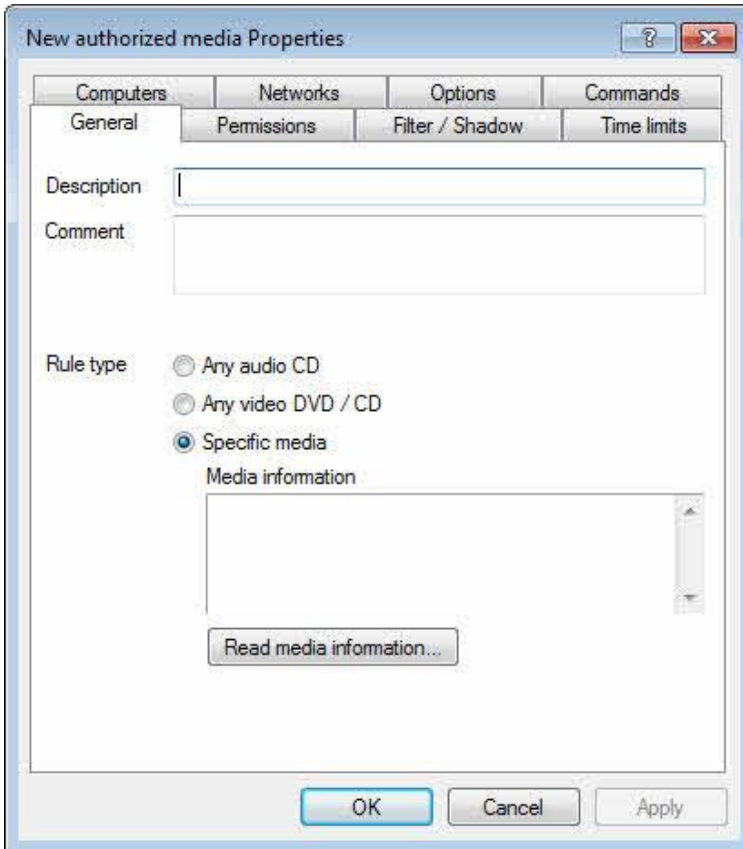
When creating a new “Authorized Media” rule for a permitted disk, DriveLock calculates a unique identifying “hash value” from the CD and unlocks the disk when this value matches the hash value of an authorized disk. Because the hash value changes when any data on the disk changes, you can use media authorization only for disks that are not writeable, but not for writable removable drives such as USB flash drives. Therefore “**Authorized Media**” rules should only be used for read-only media (CDs/DVDs).

To create a new authorized media rule, in the console tree, expand Drives, and then click **Authorized media**.



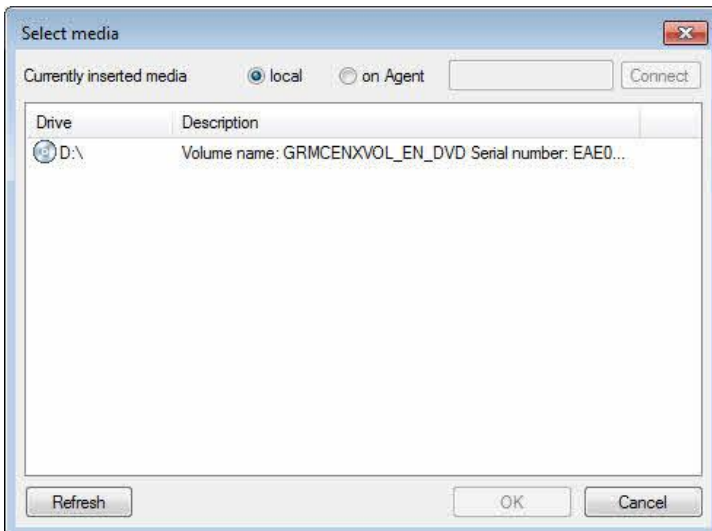
Right-click **Authorized Media** and then click **New** -> **Authorized media**.

The New authorized media Properties Dialog box opens.

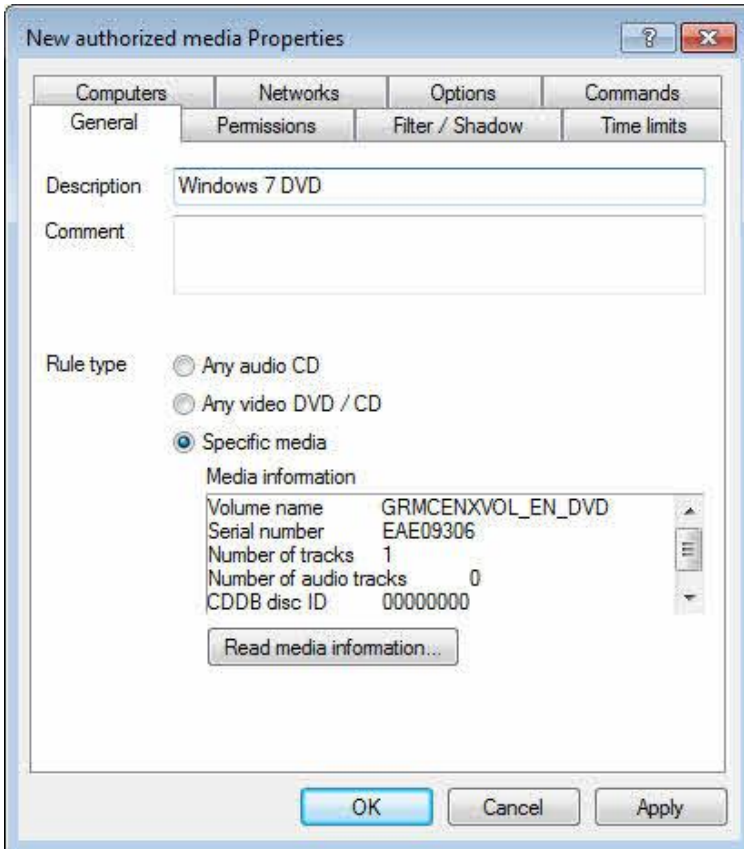


Type a description and an optional comment describing the Authorized Media rule.

DriveLock includes two predefined rule types, **Audio CD** and **Video CD/DVD**. Use these rules to authorize the use of audio and video disks, respectively. To create a custom rule for a specific disk, click **Specific media**. Click **Read media information** to calculate the hash value of the disk you want to allow.



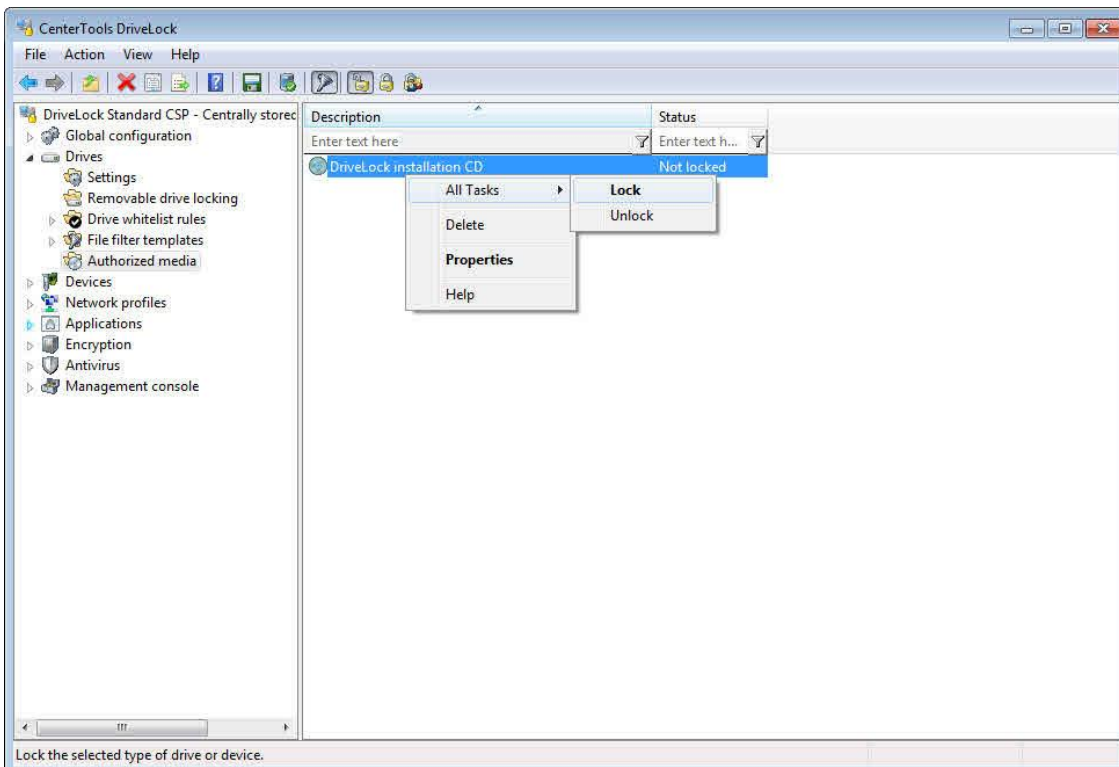
Select the drive with the CD or DVD you want to allow, and then click **OK**.



DriveLock reads the media information and adds it to the rule.

Settings on other tabs are described in the section [“Common Settings for Drive Whitelist Rules”](#).

Click **OK** to save the rule.



To quickly lock or unlock the selected rule for all users, right-click a configured rule and then click **All Tasks -> Lock** (or **Unlock**).

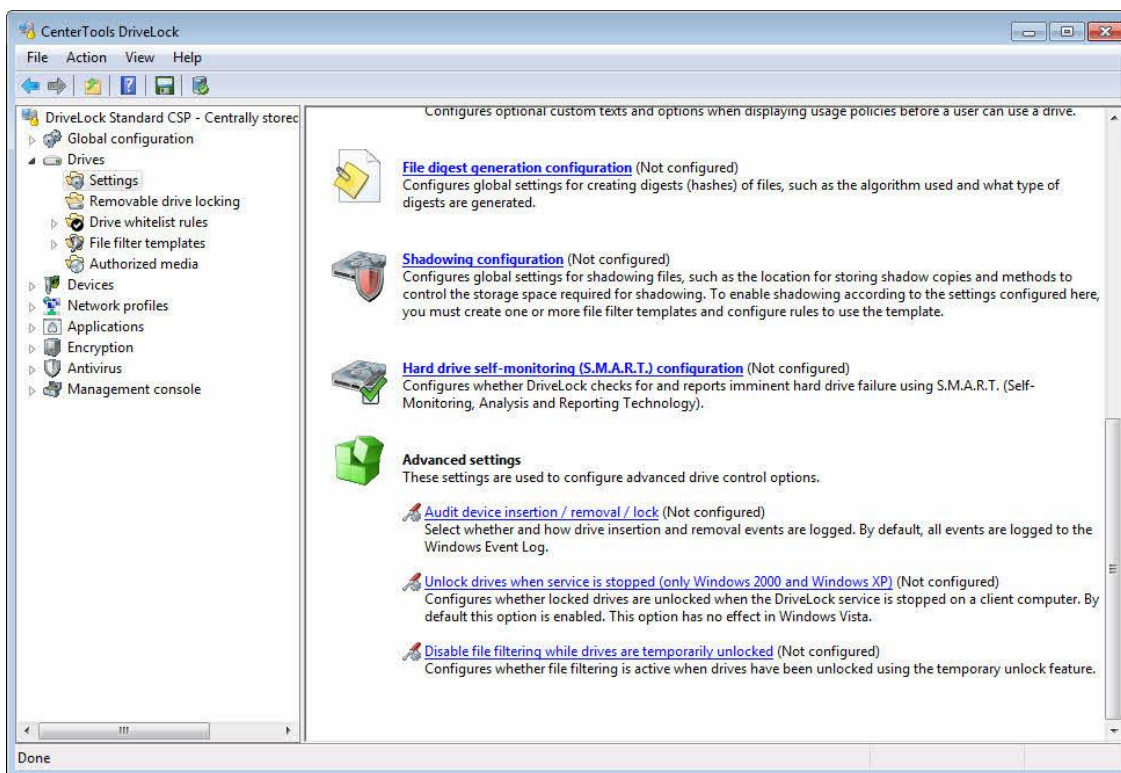
9.1.2.9 Monitoring Data Transfers by Using Shadowing

Shadowing creates copies of files transferred to or from removable media to allow administrators to review what data users accessed. DriveLock can store these shadow copies on client computers and a server. You can define which files DriveLock shadows.

If shadowing is enabled for CD/DVD recording devices, DriveLock creates an ISO image file each time a CD or DVD is recorded and saves the image in the location you configured.

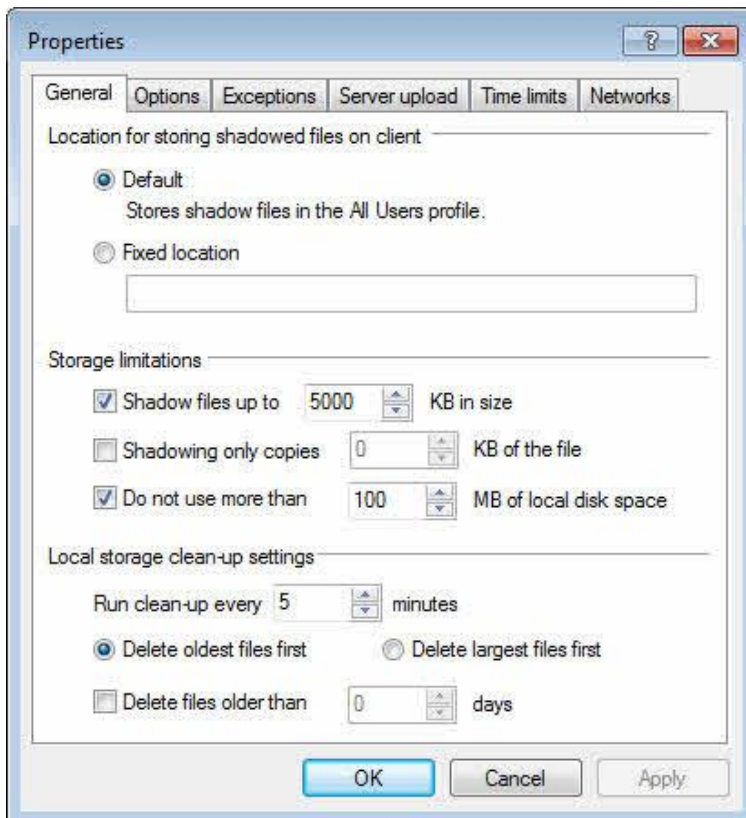
9.1.2.9.1 Configuring Global Shadowing Settings

Define global shadowing in the settings for drive locking.



Click **Shadowing configuration** to configure the settings for shadowing.

9.1.2.9.1.1 General Settings



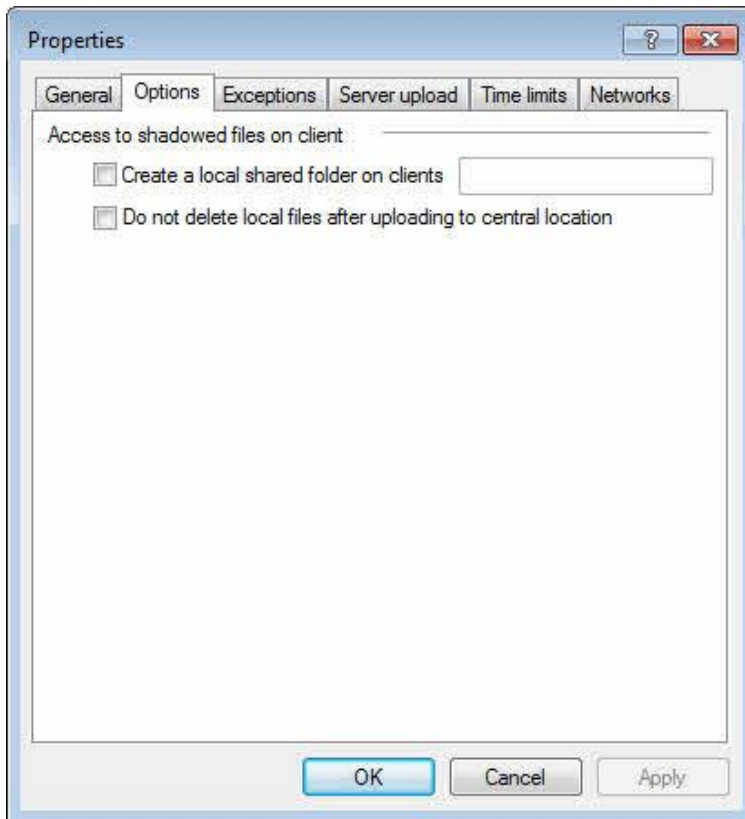
By default DriveLock stores shadow copies in the **C:\ProgramData\CenterTools DriveLock\ShadowFiles** folder. To select a different location, select “Fixed location” and then type the name and path of the shadow files folder. By default, only the Administrator account has full access to the shadow files folder.

Use the “**Storage limitations**” option to specify the maximum size of files to be shadowed or the maximum storage space used by shadow copies. By default, only individual files of up to 5 MB are shadowed and no more than 100 MB of hard disk space is used for shadow copies. To reduce the impact of shadowing on performance you can limit shadowing to the first part of each file. Configure how many KB of data of each shadowed file DriveLock retains. If you only retain portions of files you will not be able to open shadow copies using regular applications but you can use an editor to view enough information to identify the original file.

Configure in which order files are deleted when the maximum storage space has been reached and how often the cleanup process runs on client computers, or select a period after which shadow copies of files are automatically deleted. These settings only relate to storage space on client computers; you must remove files in a central storage location (network share) manually. The default for running the local cleanup process is every five minutes.

9.1.2.9.1.2 Client Options for Shadowing

Use the “Options” tab to control access to shadow copies.

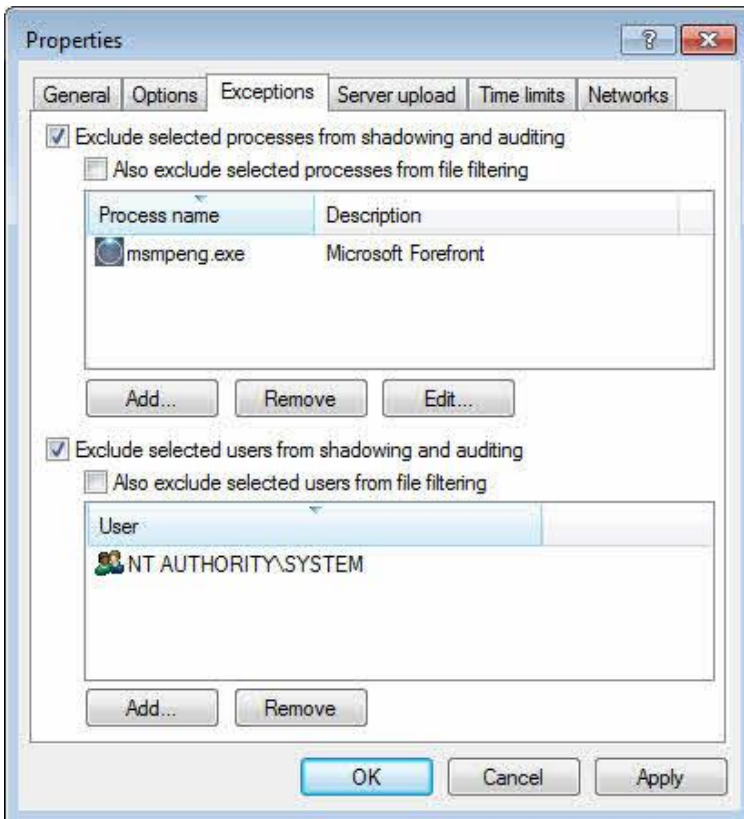


When you select the “**Create a local shared folder on clients**” checkbox, DriveLock shares the local shadow files folder on the client and assigns permissions to that folder. By default, the built-in Administrators group is assigned Full Access permissions to access the files on the computer over the network. Users and Power Users are assigned permissions to read the data.

After copying shadowed files to a central location, the DriveLock Agent deletes the local shadow copies. To retain the files on the client after they are uploaded, select the “**Do not delete files after uploading to central location**” checkbox.

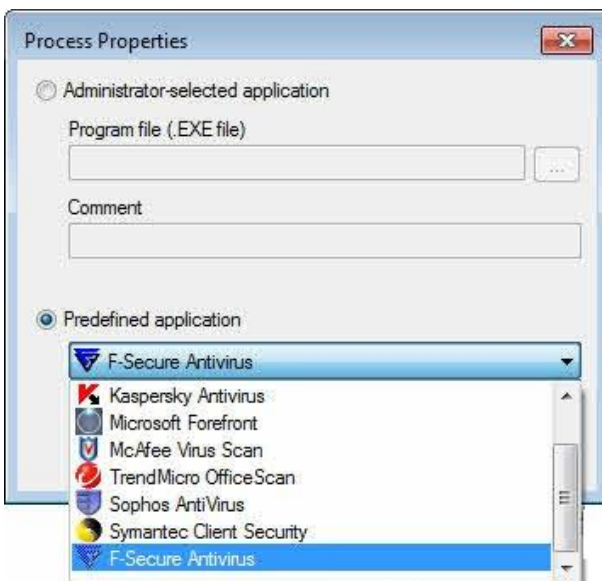
9.1.2.9.1.3 Shadowing Exceptions

Use the “Exceptions” tab to exempt certain processes or users from file shadowing.



You can define processes and users or groups that are excluded from shadowing by selecting the corresponding settings. The main purpose of such exclusions is to avoid the creation of shadow files each time a virus scanner or other automated process accesses a file.

Click **Add** or **Remove** to configure processes, users or groups to exclude from shadowing.

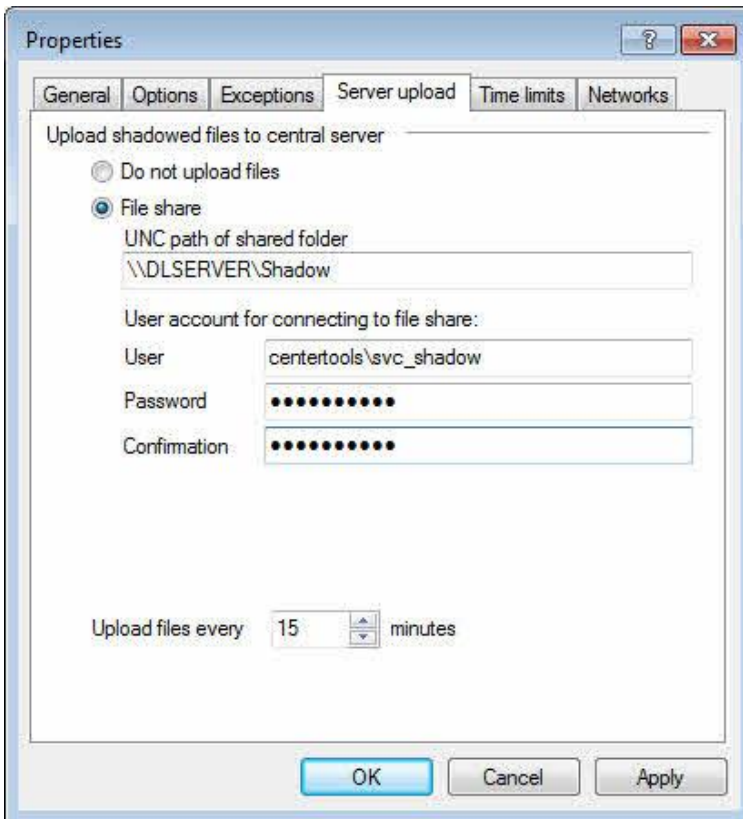


Specify a program file or select one of the pre-defined applications and then click **OK**.

To also exempt users or processes from file filtering, select the corresponding checkbox.

9.1.2.9.1.4 Server Upload Settings for Shadowing

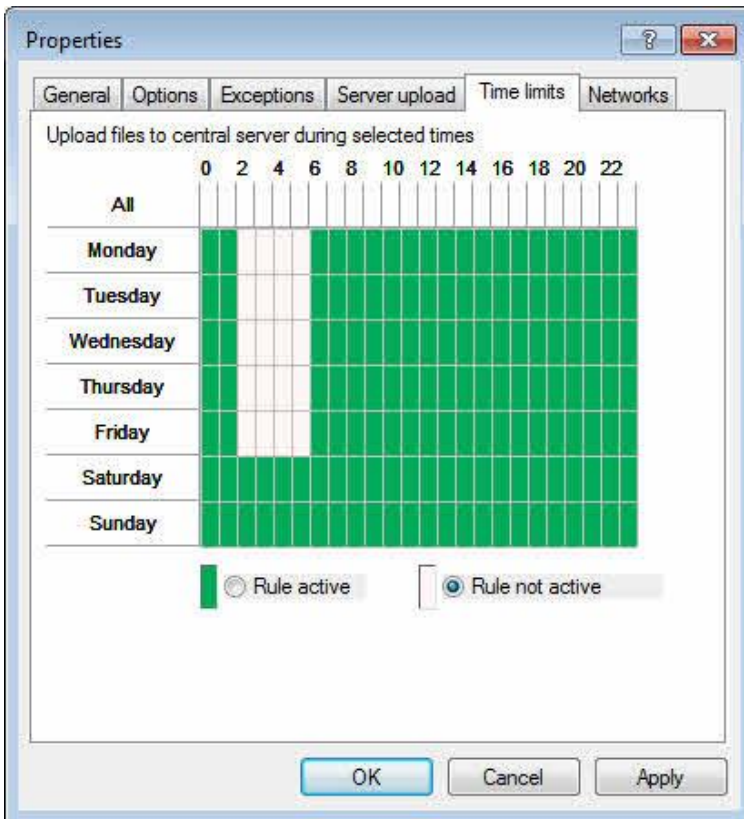
Define settings for uploading shadow copies of files to a central location on the “**Server upload**” tab.



DriveLock can copy shadowed files to a central network location so that administrators can review shadowed files from a single location. To configure server uploads, type the UNC path of the shared folder that will store the files and the credentials of a user account that can write to that folder. You must also specify the interval at which the DriveLock agent copies files to the central location.

9.1.2.9.1.5 Shadowing Time Limitations

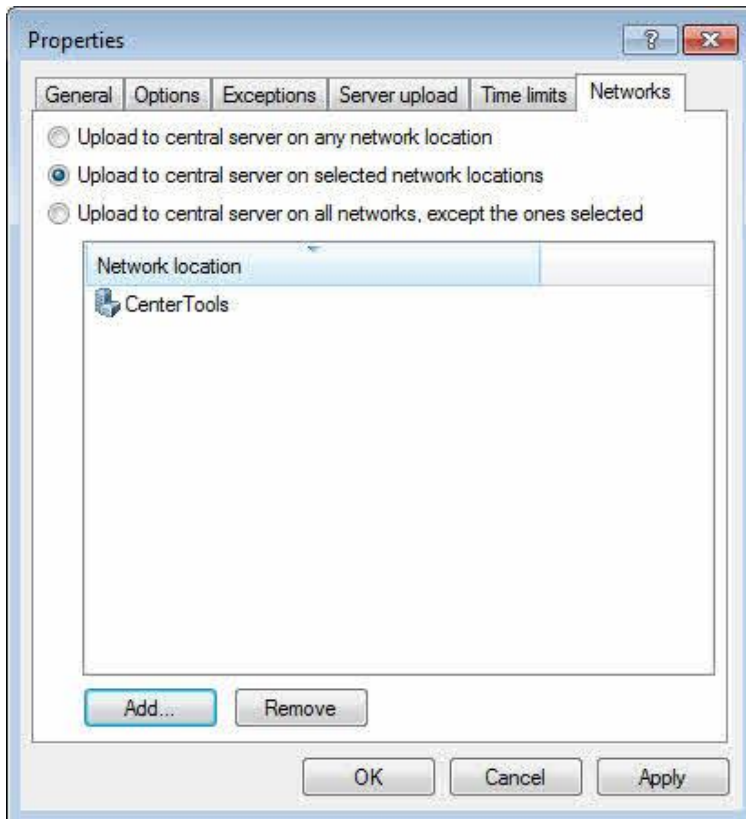
You can define the times when shadow copies are generated on the **“Time limits”** tab.



Select the appropriate time block or blocks by clicking one or more rectangles, an entire column or a row, and then click **“Rule active”** or **“Rule not active”**.

9.1.2.9.1.6 Network Limitations

On the **Network** settings tab you specify whether shadowing is applied only in certain network locations.



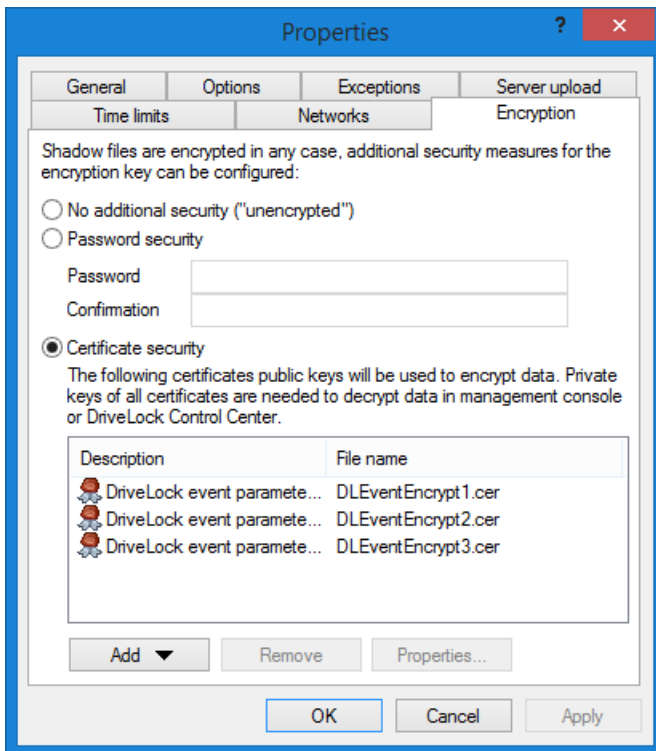
Select from the following options:

- Activate this rule in all network locations
- Activate this rule only in the specified network locations
- Exclude the specified network locations from this rule

Click **Add** to add more network locations to the list.

9.1.2.9.1.7 Encryption

In analogy to [Anonymizing Event Data](#) you may want to protect the shadow copies against access from non authorized persons. DriveLock always encrypts the shadow copies before uploading with an internal key. Additionally you can protect that key either by a password or by the public keys of one ore more certificates (Four-Eyes-Principle). If you do so, you need to enter the password or the corresponding private keys of the certificate each time you open the shadow copy storage.

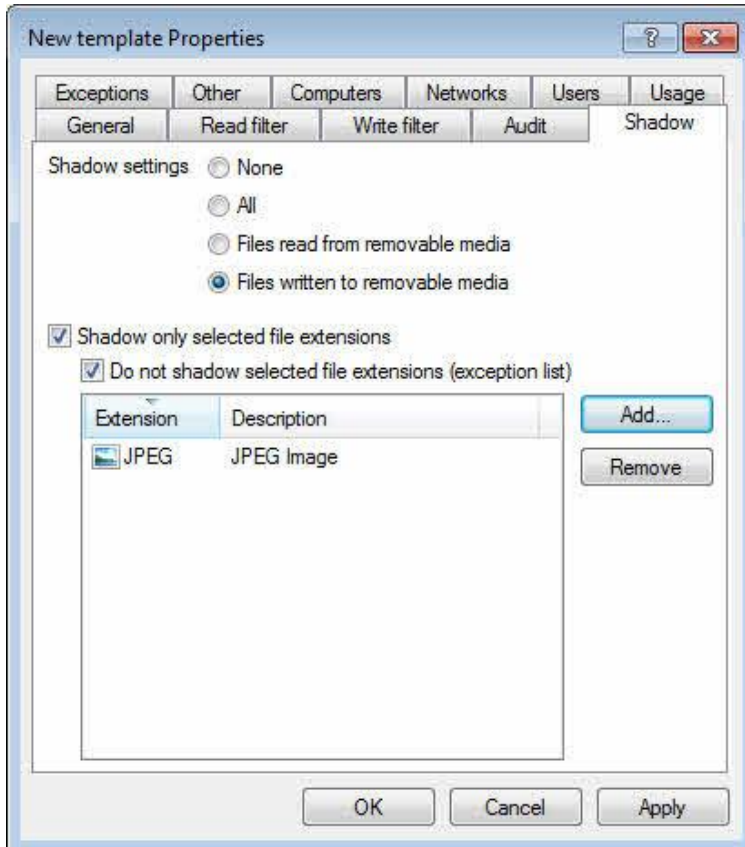


If you loose the keys, you can no longer access the content of the shadow copies.

9.1.2.9.2 Configuring Shadow Copies in Drive Whitelist Rules

To activate file shadowing you must create a file filter template. Refer to the section "[Creating a New File Filter Template](#)" for more information about creating file filter templates.

In a file filter template specify which files DriveLock creates a shadow copy of.

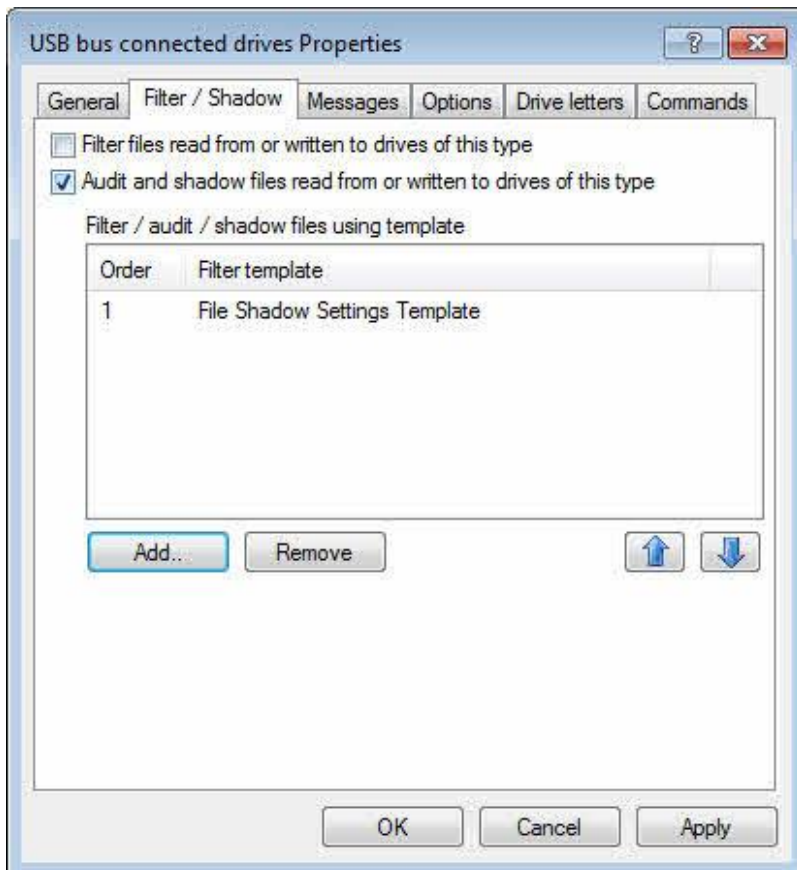


Configure whether DriveLock shadows no files, all files, or files written to or read from removable media. You can additionally limit shadowing to specific file extensions or exclude files with specific extensions from shadowing.

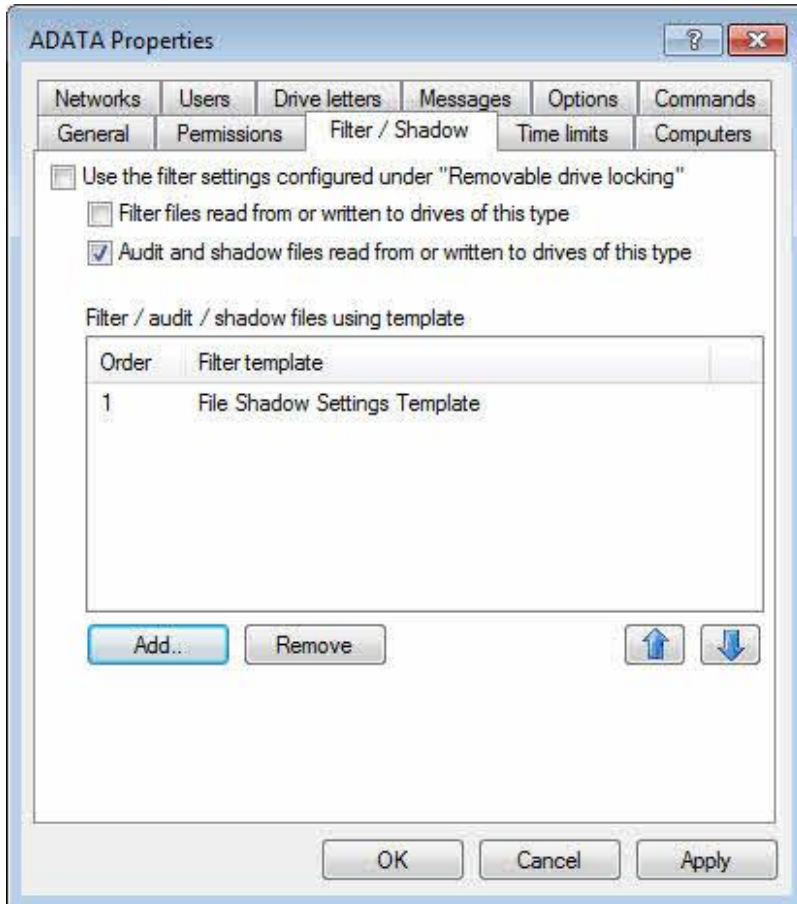
You can create a separate file filter template specifically for the creation of shadow copies.

After configuring a shadowing template, assign it to a class of drives or a drive whitelist rule.

To assign a template to one of the drive classes (for example USB-connected drives), in the Properties dialog box for the drive class, select the **“Filter / Shadow”** tab.



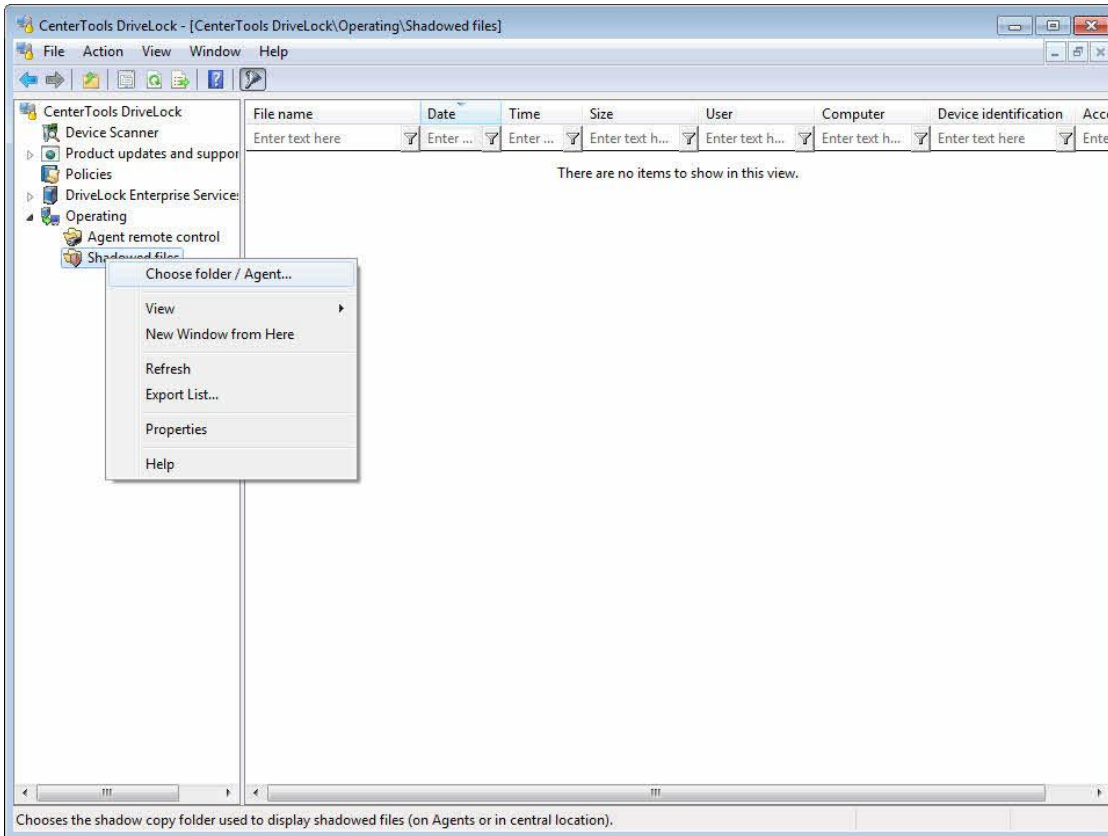
To activate shadowing, select “**Audit and shadow files ...**” and then add a shadowing template.



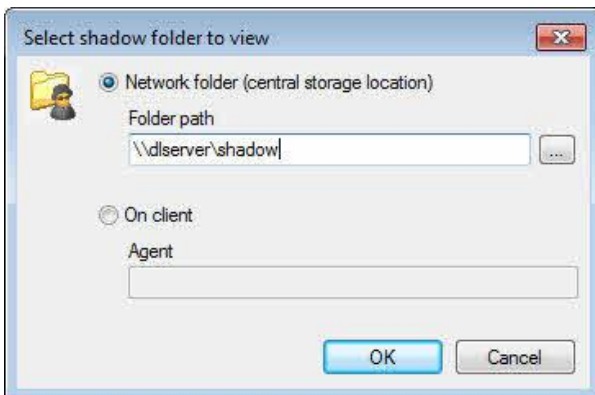
To activate shadowing settings for a whitelist rule that differ from the general settings you configured for drives, deselect "Use filtering settings ...", select "Audit and shadow files ..." and then select a shadowing template.

9.1.2.9.3 Viewing Shadow Copies

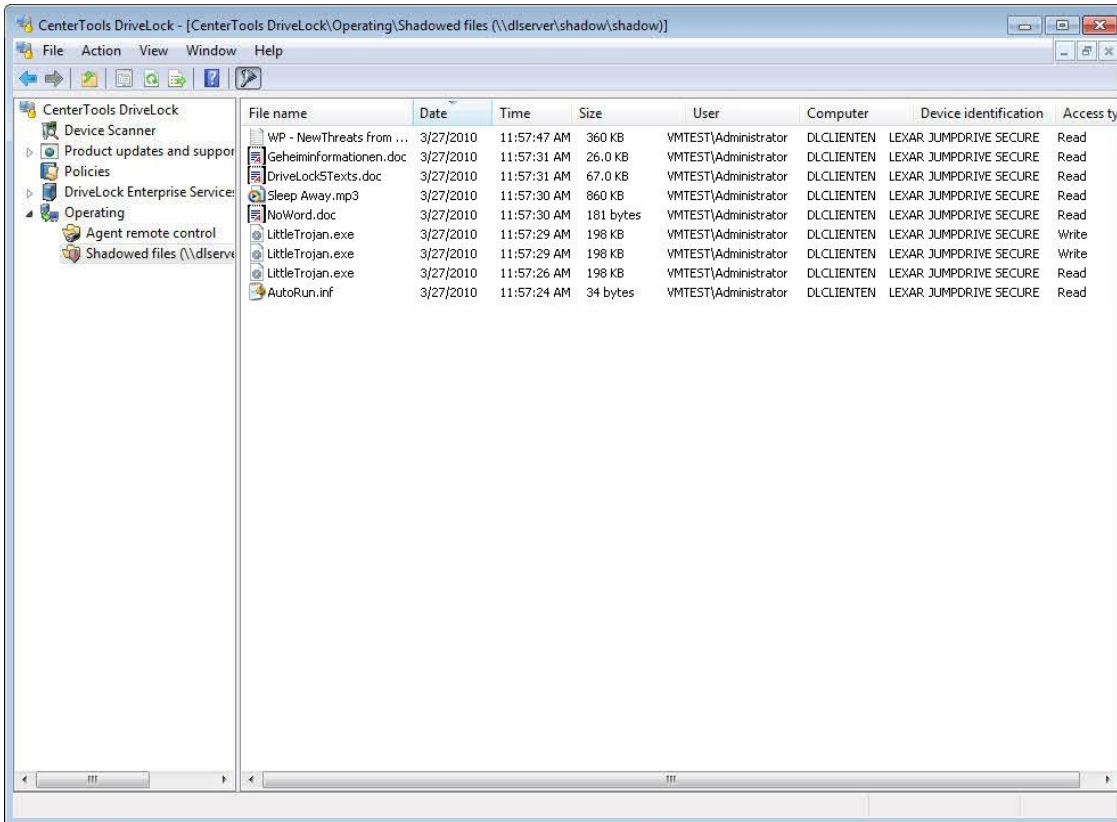
You can view shadowed files by using the DriveLock Management Console. In the console tree, expand Operating and then click **Shadowed files**.



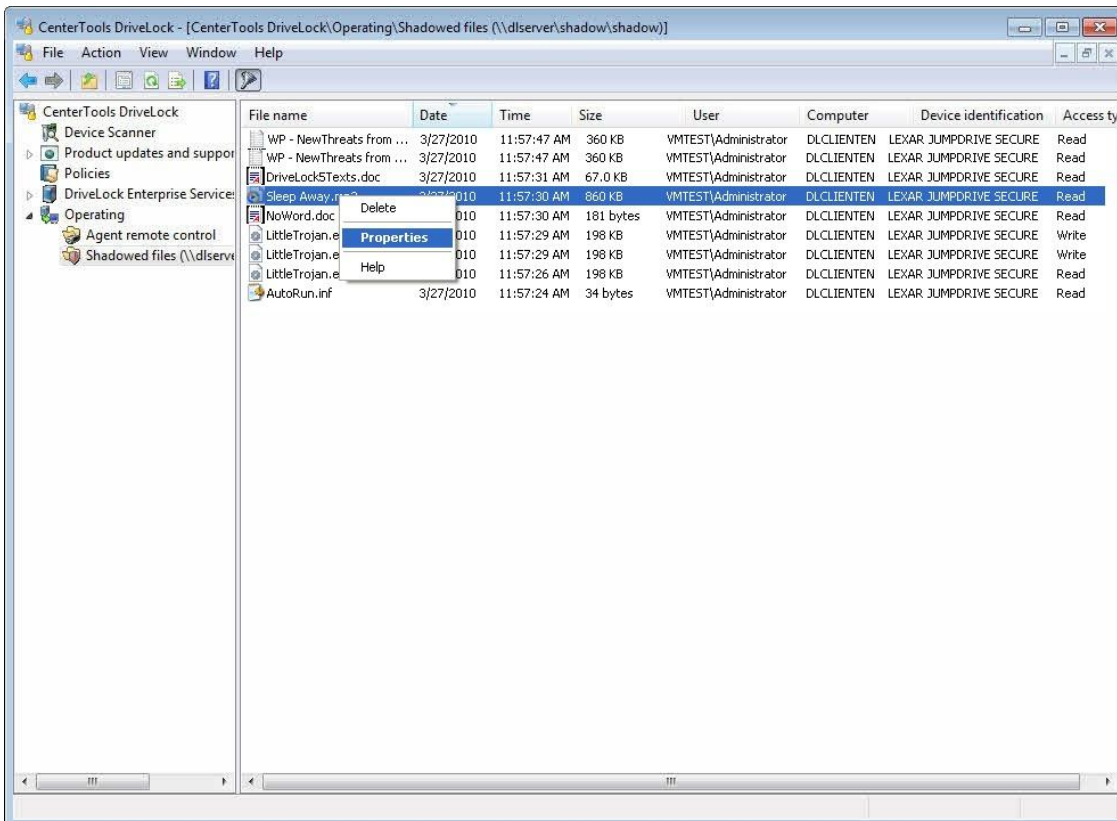
Right-click **Shadowed files** and then click **Choose folder/agent**.



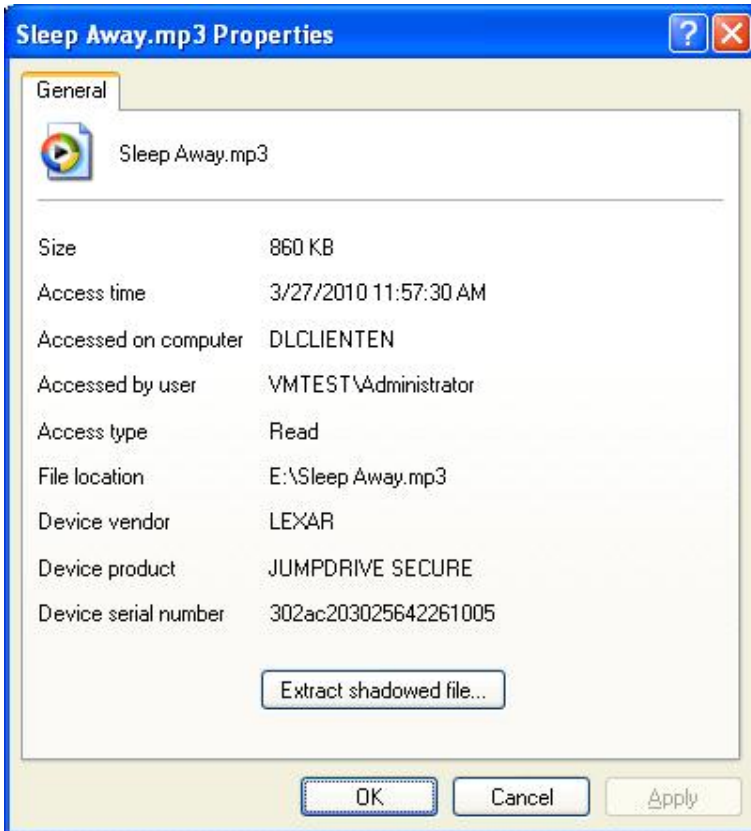
Type the UNC path of the central location where shadow copies are stored or type the name of a DriveLock Agent computer with locally stored shadow copies. Click **OK** to to view all shadow copies in the selected location.



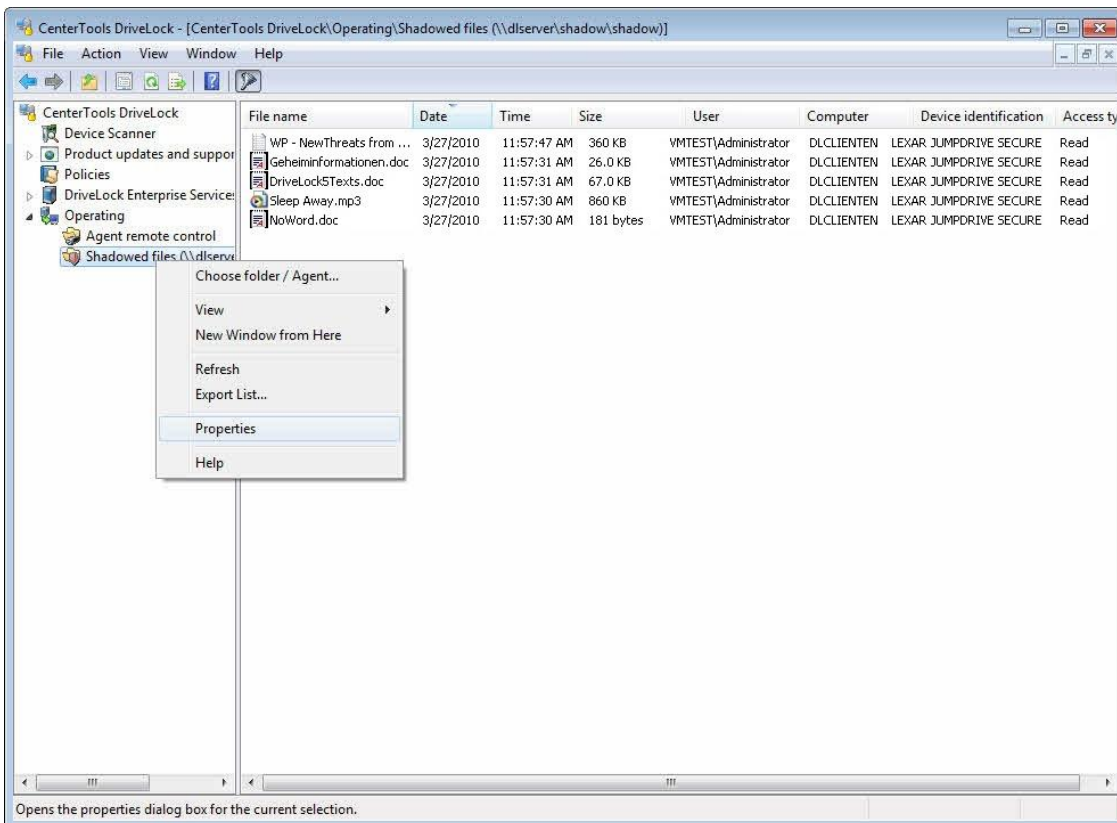
After connecting to the location you specified the DriveLock management console displays the shadow copies in the right pane.



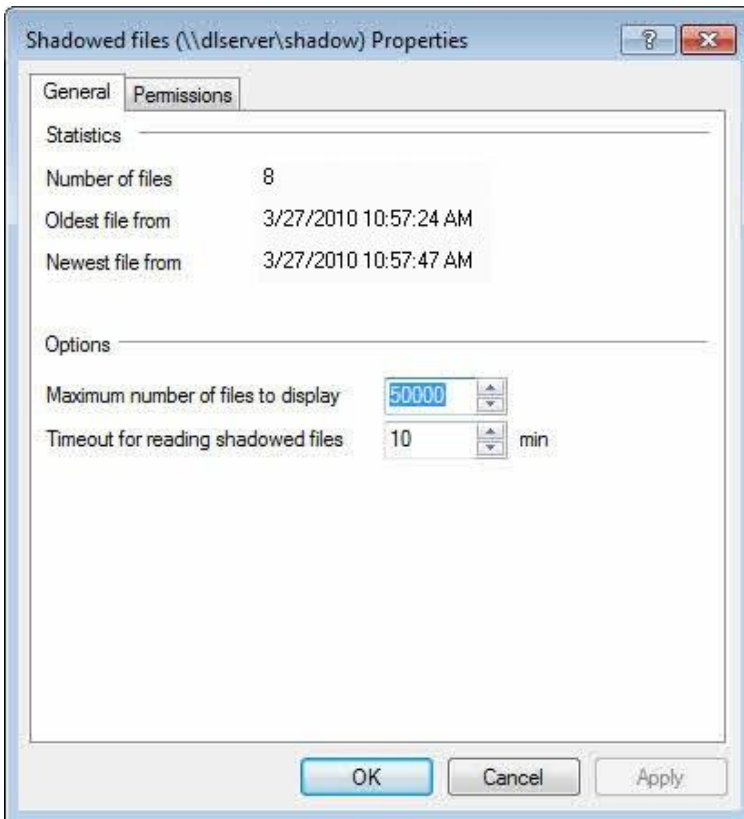
To view the properties of a shadow copy, double-click it or right click it and then click **Properties**.



Click “Extract shadowed files” to copy the shadowed file to another location, such as your administration workstation. If you configured a password or certificates to protect the shadow copies, now please authenticate with the corresponding key.



To view information about the location where shadowed files are stored, right-click **Shadowed files** and then click **Properties**.



The number of files in the shadow location and the timestamp of the oldest and newest file are displayed.

To customize the display of shadow files in the Management Console, configure the maximum number of files to display and for how long the Management Console will try reading shadow files before timing out.

Click **OK** to close the dialog box.

9.2 Locking Devices

This manual uses a centrally stored policy to illustrate device locking. The example used shows how to control the use of Windows Mobile devices, and how to allow connecting a specific Windows Mobile device to a computer. Most steps also apply to other types of devices. Differences that may exist for other device types will be pointed out along the way.

Configuring Agents by using a Group Policy or a configuration file uses the same settings as those used in a local policy. There are no differences between these methods, except in how you deploy the settings to the Agents

It is important to understand that DriveLock uses whitelist rules. After activating locking for a class of devices, any device of this class is blocked (the “device firewall” is up and running and nothing is allowed to pass through). To define any exception to the blocking of devices you need to create whitelist rules. This means that you must define a whitelist rule for each devices (or groups of similar devices) that you need to use on a computer. If a device is not recognized by the DriveLock Agent as being listed in a whitelist rule, DriveLock blocks the device and it can’t be used. This ensures that any new devices that are introduced into your network by users are automatically blocked until you explicitly allow their use.

Based on this basic principle, to complete a DriveLock configuration you should first create any required whitelist rules and then enable the locking of devices.

Whitelist rules define which devices are accessible even while other devices of the same type can remain locked. To allow for maximum granularity without unnecessary administrative overhead, you can define device whitelist rules for different scopes of devices (rules are evaluated starting with rules that have a broad scope, continuing towards more detailed rules).

You can define device whitelist rules for the following scopes:

- Device class (for example, all Bluetooth transmitters)
- Device bus (for example, all PCI network cards)
- Hardware ID (for example, a specific smartcard reader model)

In addition to the scope you can specify conditions for when and where a whitelist rule applies:

- Does it apply to all computers or only to certain computers?
- In which defined network location is the rule active?
- At what time is the rule active? (For example, only on Monday to Friday and between 9 A.M. and 6 P.M.)
- Does the rule apply to all users, or are only certain users allowed to use this device?

By using scopes and conditions, you can minimize the number of rules needed to implement your policy. (Computer templates can also be used to create policy rules. Computer templates are covered in chapter [“Using Computer Templates”](#).)

To enable policy enforcement for most types of devices you also need to enable locking for the device class (i.e. you have to activate the “device firewall”). This is covered in chapter [“Enabling Device Locking”](#).

During an evaluation of DriveLock you may enable device locking first and afterwards define some whitelist rules to enable specific devices. In a production environment it is recommended to create all required whitelists rules before activating device locking.

9.2.1 Configuring Device Locking Using Basic Configuration Mode

The procedures for locking devices are similar to those for locking drives. By default, DriveLock doesn't monitor any devices other than drives, serial ports and parallel ports. You need to explicitly configure DriveLock to monitor devices belonging to any device classes it recognizes. When you enable locking of a device class, all devices of this class, including all devices connected to type of controller or port you lock, are blocked, except those that are allowed by a whitelist rule.

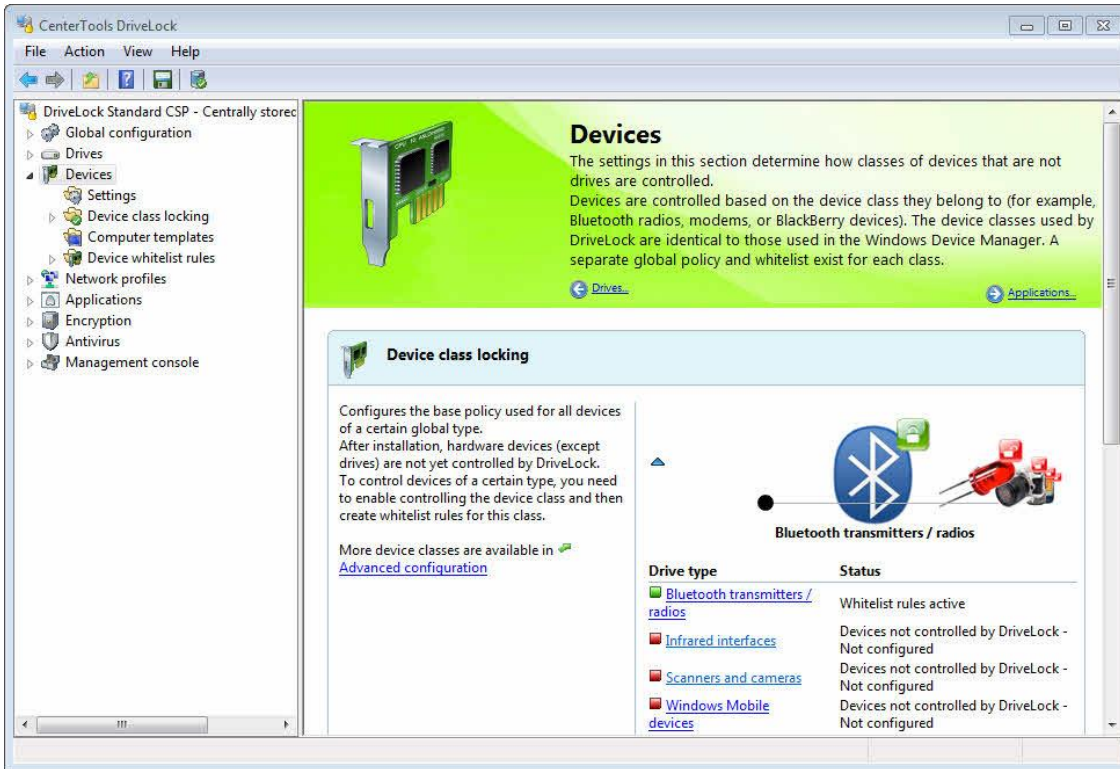
DriveLock distinguishes between controllers, ports and devices. You can lock the following types of controllers and ports:

- Serial (COM) and Parallel (LPT) ports
- Bluetooth transmitters (interface)
- Infrared interfaces
- USB controllers
- FireWire (1394) controllers
- PCMCIA controllers

You can lock the following types of devices:

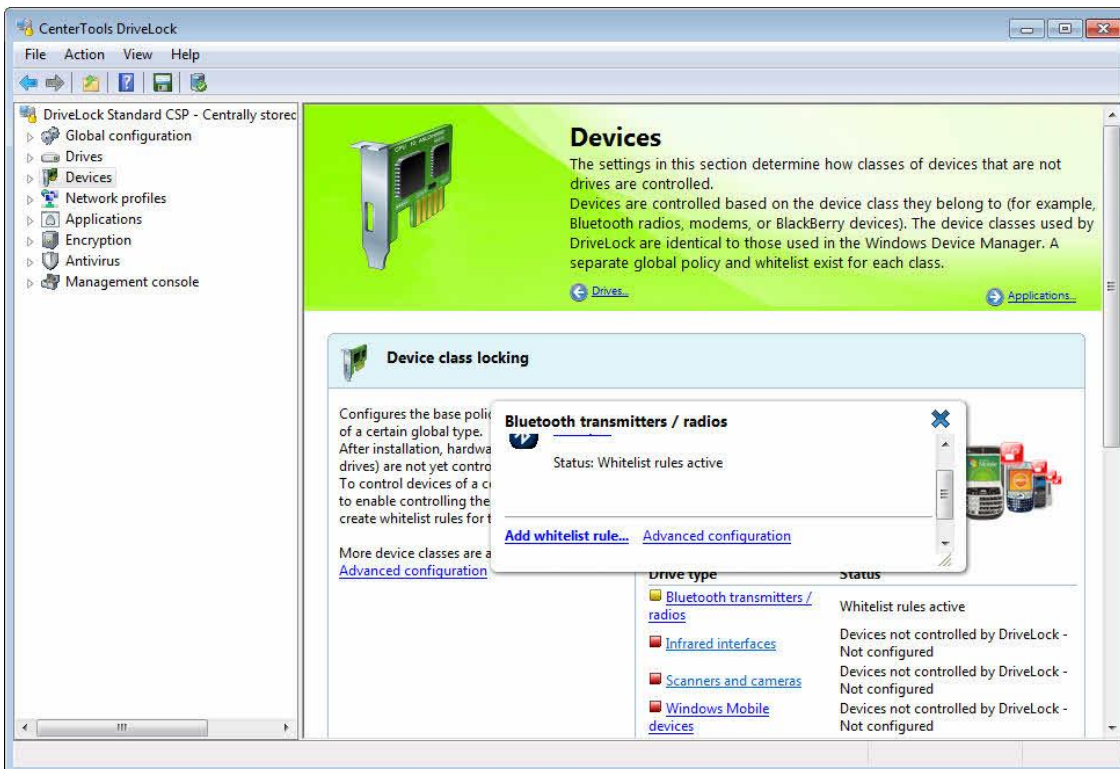
- Windows Mobile handheld devices and Smartphones
- Palm OS handheld devices and Smartphones

- Scanners and cameras
- Modems
- Printers
- Network adapters
- Smartcard readers
- Audio, video, and game controllers
- Blackberry devices
- Virtual devices (VMware)
- Mobile phones
- Human interface devices (for example, keyboards and mice)
- Media player devices
- Biometric devices
- Software protection devices (dongles)
- Secure Digital Host controllers
- Tape drives
- PCMCIA and flash memory devices
- IEC 61883 (AVC) bus devices
- Windows Media Center Extender devices
- Windows SideShow devices
- Sensor devices

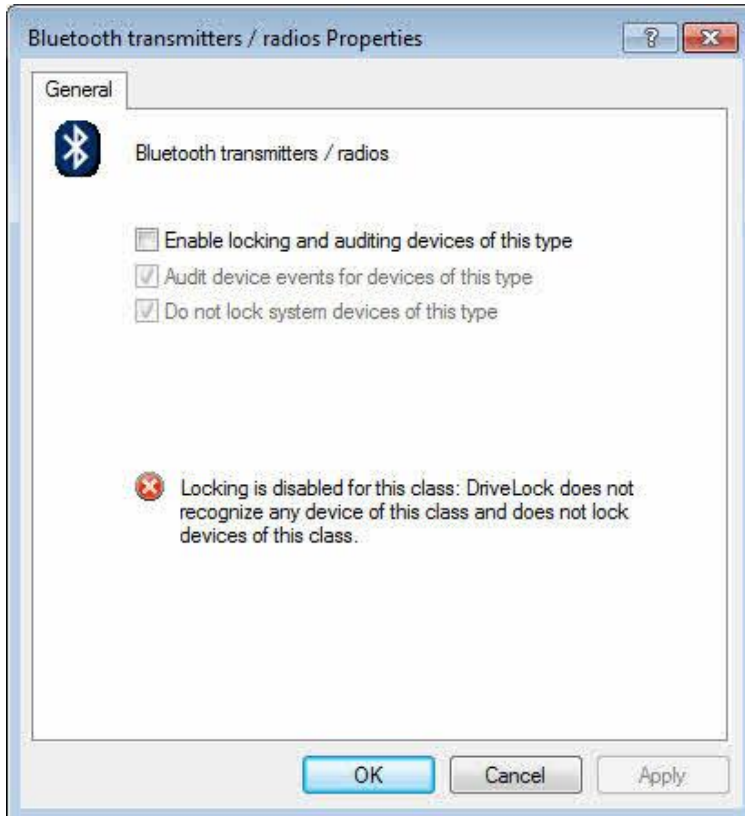


Use the small arrows ▼ and ▲ to toggle the display of device type details.

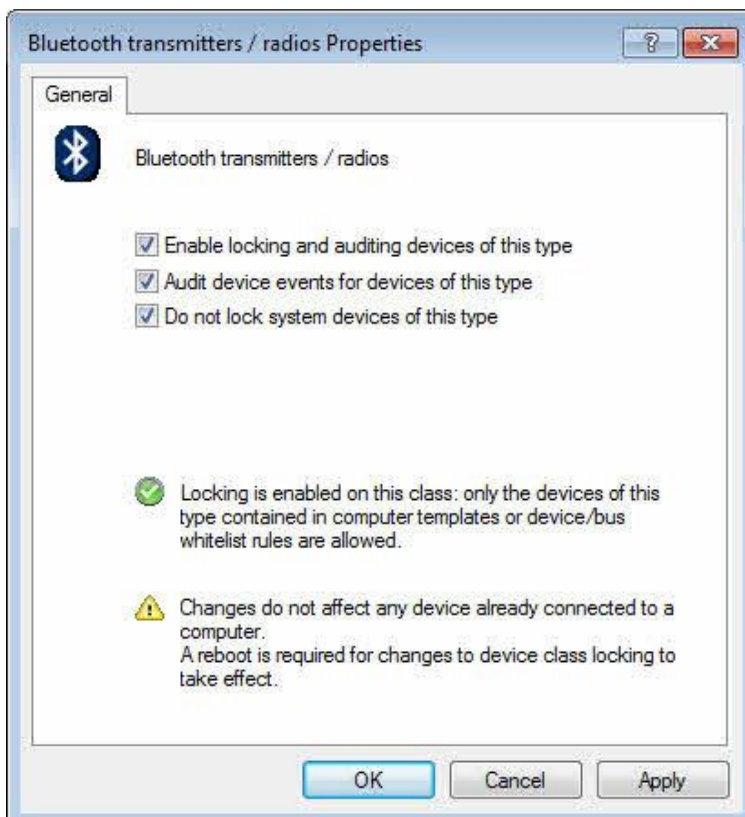
To change settings for a device type (for example, Bluetooth radios), click the appropriate link. You can also use the slider in the task view to highlight one of the device icons and then double click the highlighted icon.



A popup window appears, displaying the current configuration setting. Click **Change**.



The configuration dialog box is identical for all device types, except for serial and parallel ports. For information about locking serial and parallel ports, refer to the section [“Configuring Serial and Parallel Port Locking”](#).



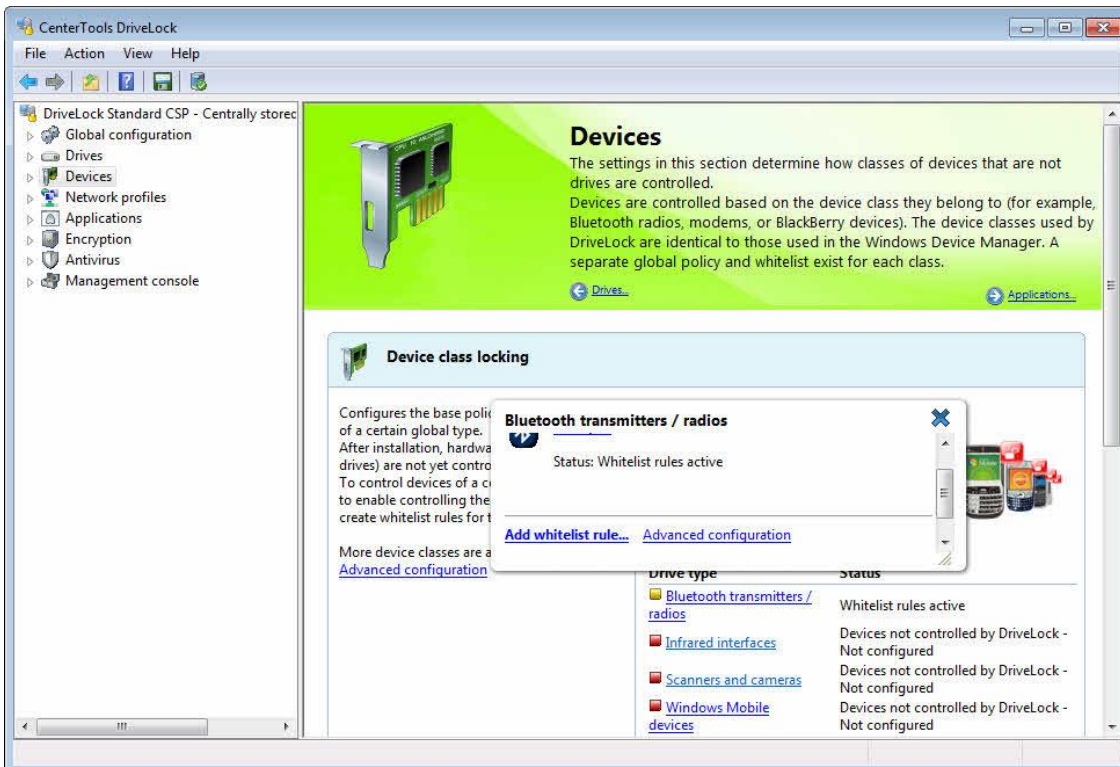
To activate locking of devices in the selected class, select the **“Enable locking and auditing devices of this type”** checkbox.

When DriveLock locks a device, a yellow exclamation mark is displayed next to it in Windows Device Manager.

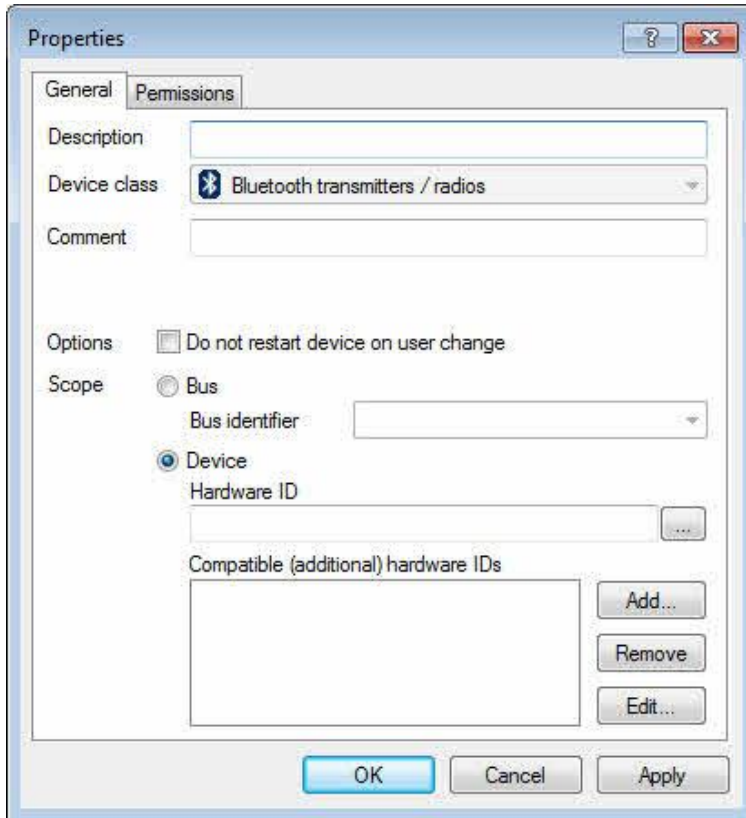
You can also specify whether events for devices in this class are audited. If selected, the DriveLock Agent sends event messages to destinations you defined, such as the Windows Application Log and the DriveLock Enterprise Service.

To exempt system devices, such as network miniport drivers or UBS hubs from device locking, select the corresponding checkbox. To avoid configuring whitelist rules for such “software” devices, this option is enabled by default. If you disable this option, you must define whitelist rules for all system devices that are required for normal computer operations.

Click **OK** to save your settings.



Click **Add whitelist** rule to configure a new whitelist rule for this device class.



In the description field, type a name for the rule. To record additional information about the rule, you can type a comment in the Comment field.

Define the scope of the rule by identifying the device. To specify all devices of the selected type that are connected to a specific hardware bus, select **Bus** and then select the bus from the dropdown menu.

When you specify a bus in a whitelist rule, the rule is activated when any device in the selected class (for example, **Windows Mobile handhelds and Smartphones**) is connected to the computer using the selected bus.

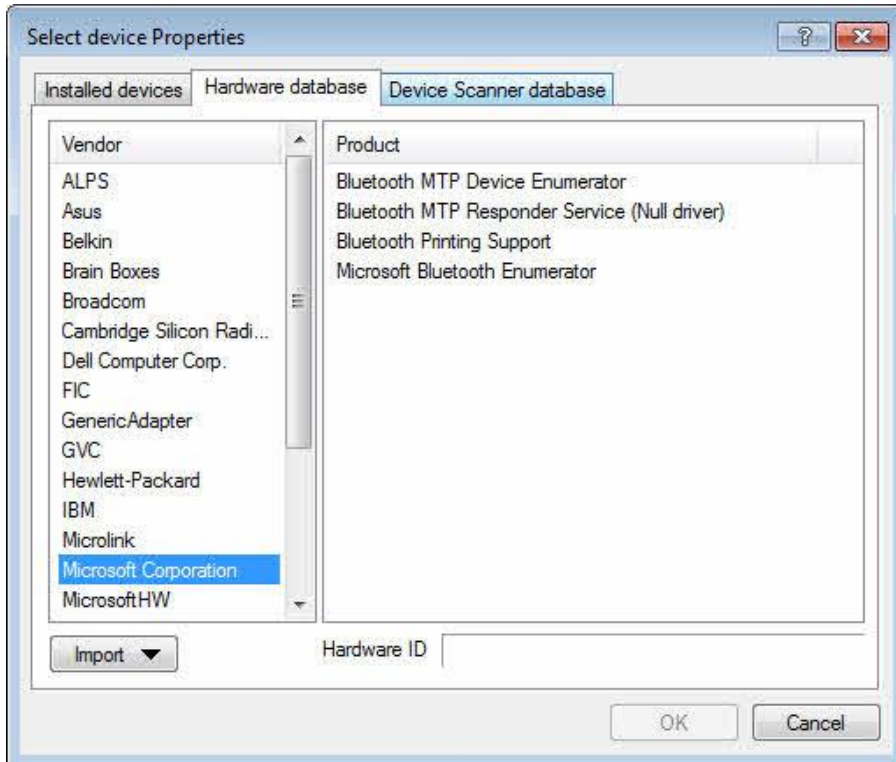
Example: To enable all PCI network cards in a computer, create a new whitelist rule for network adapters and select "PCI" as the identifier. This enables all internal network adapters connected to the PCI bus while locking all network adapters that are connected to an external bus, such as PCMCIA and USB.

For more granular device control you can create rules for devices with a specific hardware ID and compatible IDs. Each device has a unique hardware ID. In addition Windows maintains a list of compatible hardware IDs. Windows uses this hardware ID and any compatible IDs to find a driver for the device when it is connected to a computer. Most hardware IDs can also contain a revision number that is assigned by the manufacturer but which is not used when selecting the device driver. If a hardware ID contains a revision number, Windows uses one of the compatible IDs that does not contain the number.

You can find the hardware ID in the Registry. It may also appear in Event Log messages. Type this hardware ID in the corresponding field of the dialog box.

Ensure that there are no empty spaces before or after the hardware ID.

To easily determine the hardware ID, click "..." next to the hardware ID field and then locate the device in the list of installed devices or the Windows hardware database.

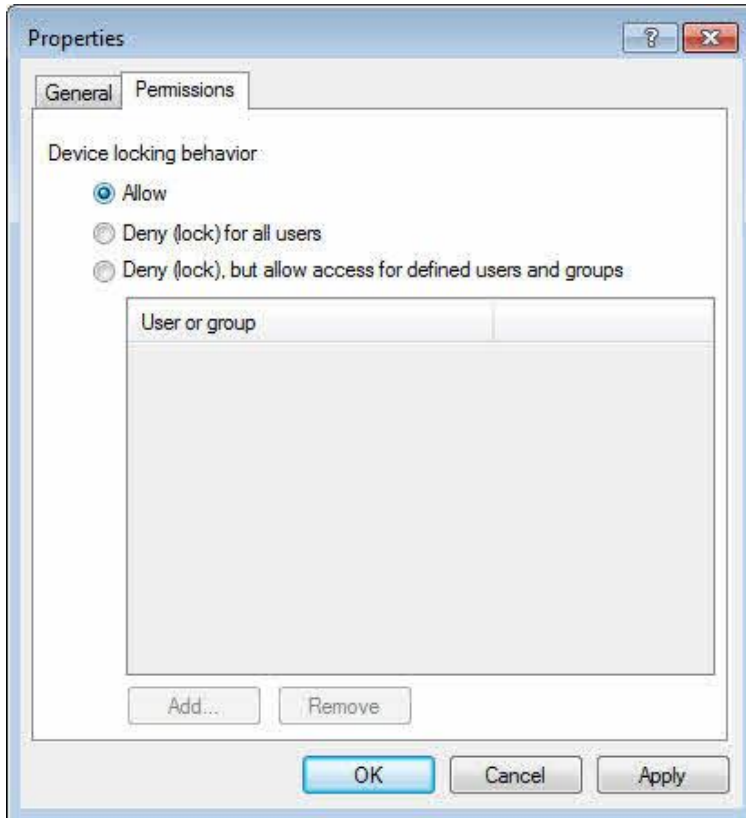


Click **Refresh** to display recently connected devices. Palm or Windows Mobile-based handheld computers are usually connected to the computer while the HotSync or ActiveSync process is running.

In the list of installed devices, you can select **“Hide system devices”** to hide all Windows system devices. By default, these devices are not locked. (You can change this by deselecting the option **“Do not lock system devices”** in the device class configuration dialog box).

Select a device from one of the lists and then click **OK**.

To configure user access, click the **“Permissions”** tab and then specify which users can use the device.

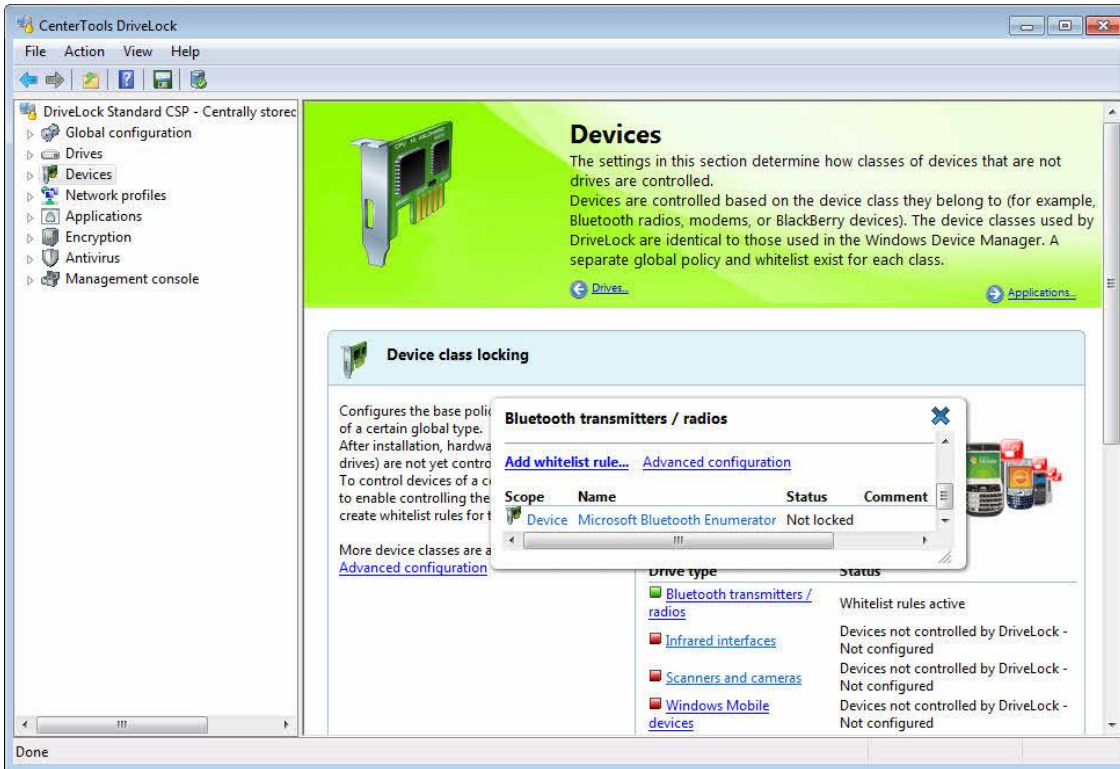


Select one of the following options:

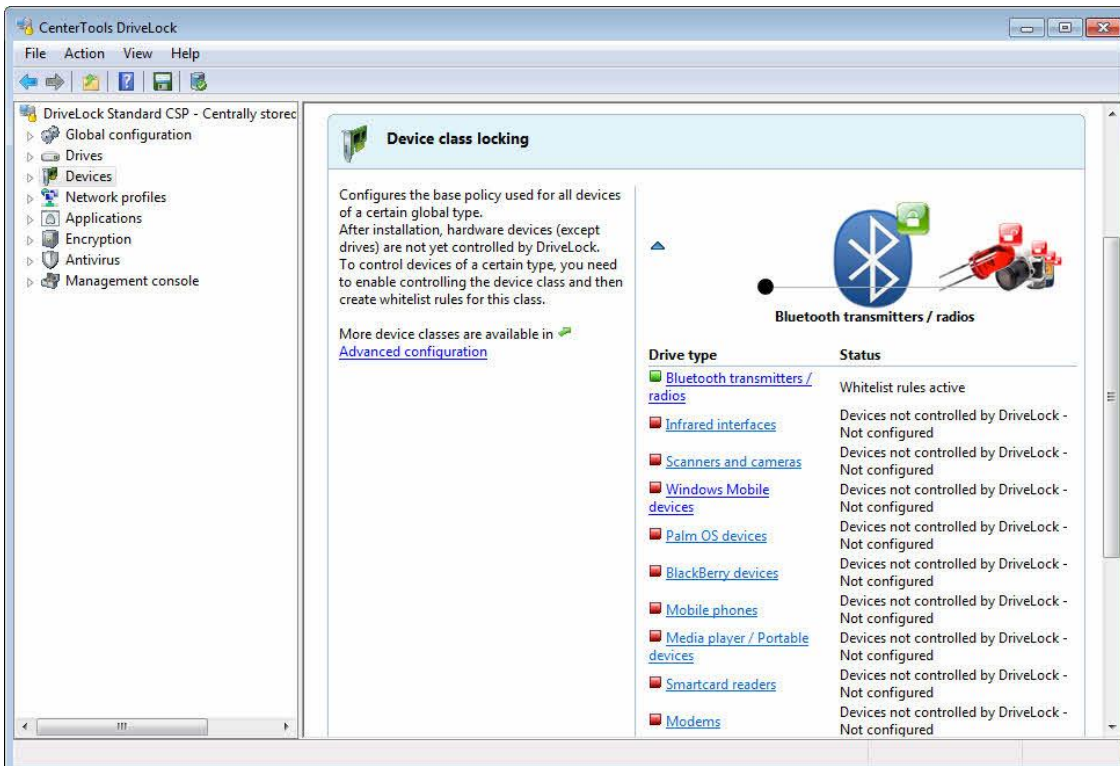
- *Allow*: Any authenticated user can use this device.
- *Deny (lock) for all users*: Nobody can use this device, it is completely locked.
- *Deny (lock), but allow access for defined users and groups*: The device is locked, but the specified users or groups are can use the device.

Click **Add** to select a user or group to add to the list. To delete an entry from the list, select the entry, and then click **Remove**.

Click **OK** to save the whitelist rule.



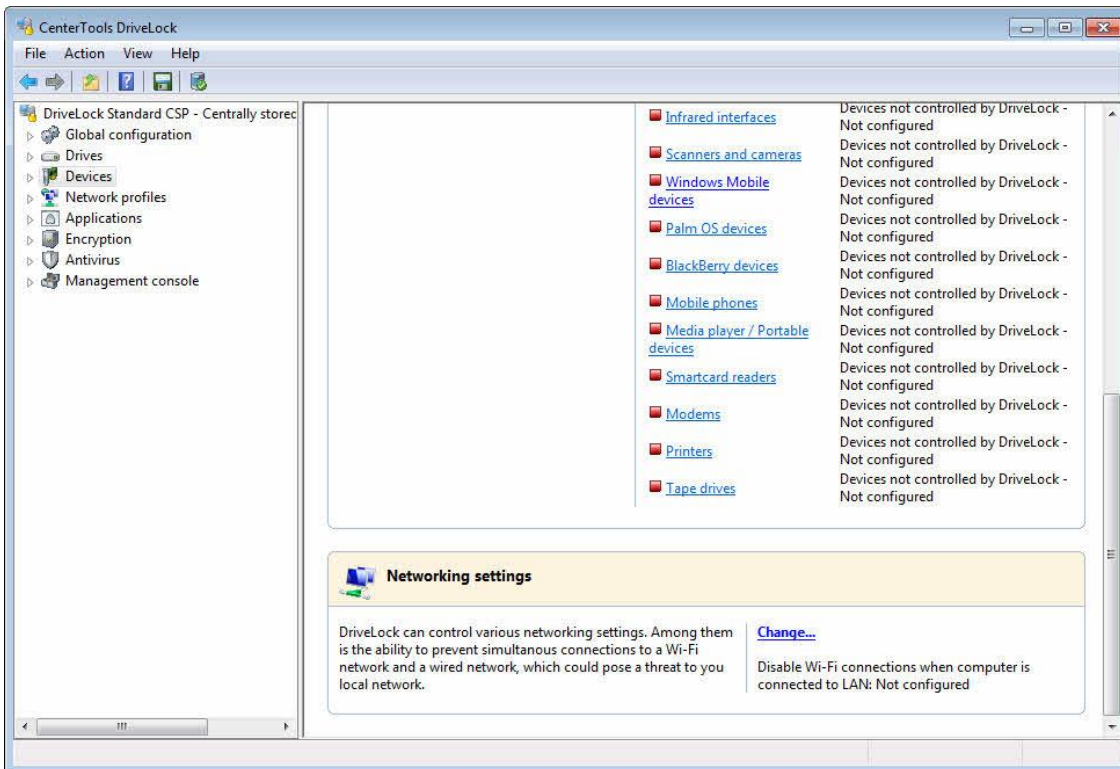
A popup window appears, displaying the new settings. Click **X** to close the popup window.



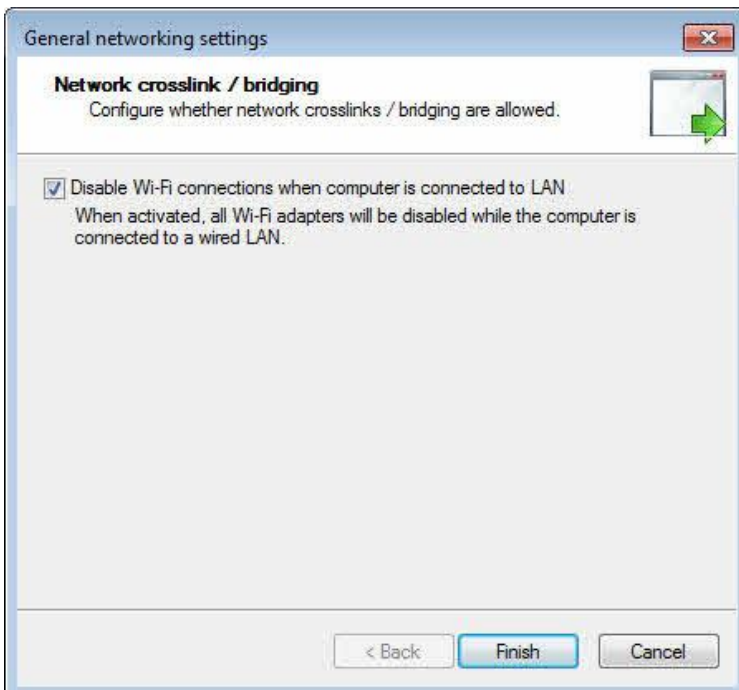
The colors of the device type icons indicate the security level of your current configuration:

- *Green icon*: this device type is locked for all users (high security level)
- *Yellow icon*: this device type is locked for some users and unlocked for others (medium security level)
- *Red icon*: this device type is unlocked for all users (low security level)

Scroll down in the taskpad to the Network settings section.



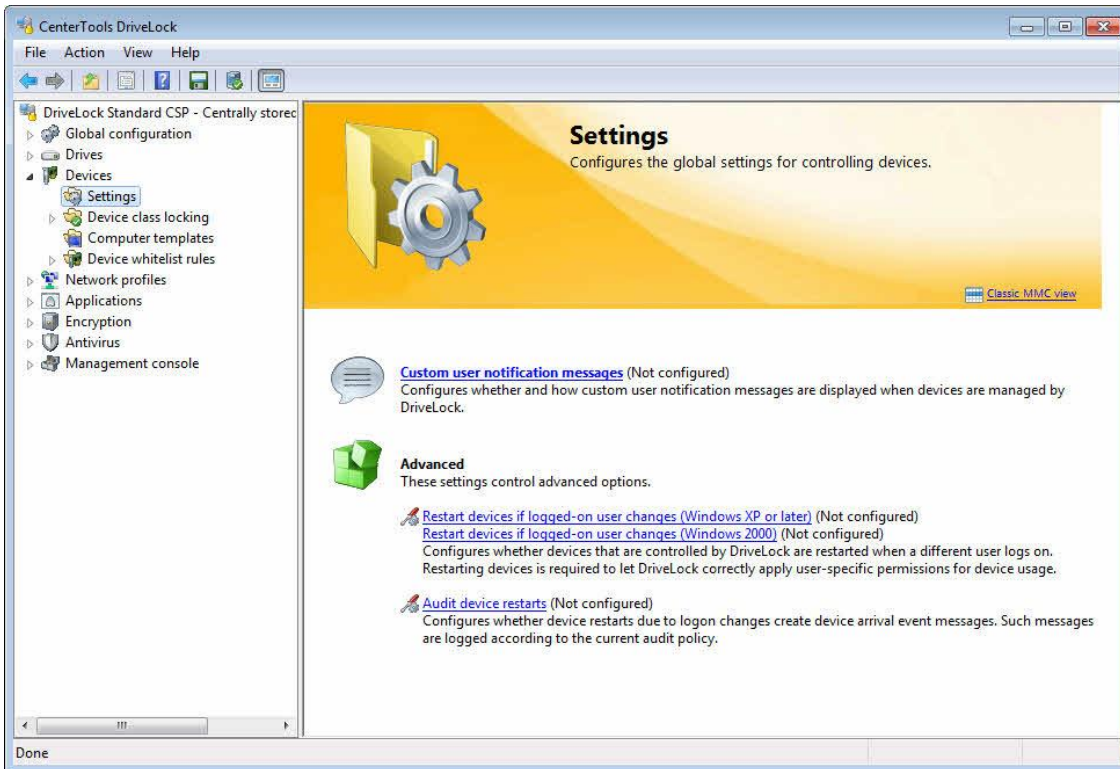
Click **Change** to configure whether Wi-Fi connections are disabled when the computer is connected to a wired network.



Select the checkbox to disable cross-network links. Click **Finish** to save the settings.

9.2.2 Configuring Advanced Device Locking Settings

Additional settings are available for controlling devices. To configure these settings, go to *Devices -> Settings*.



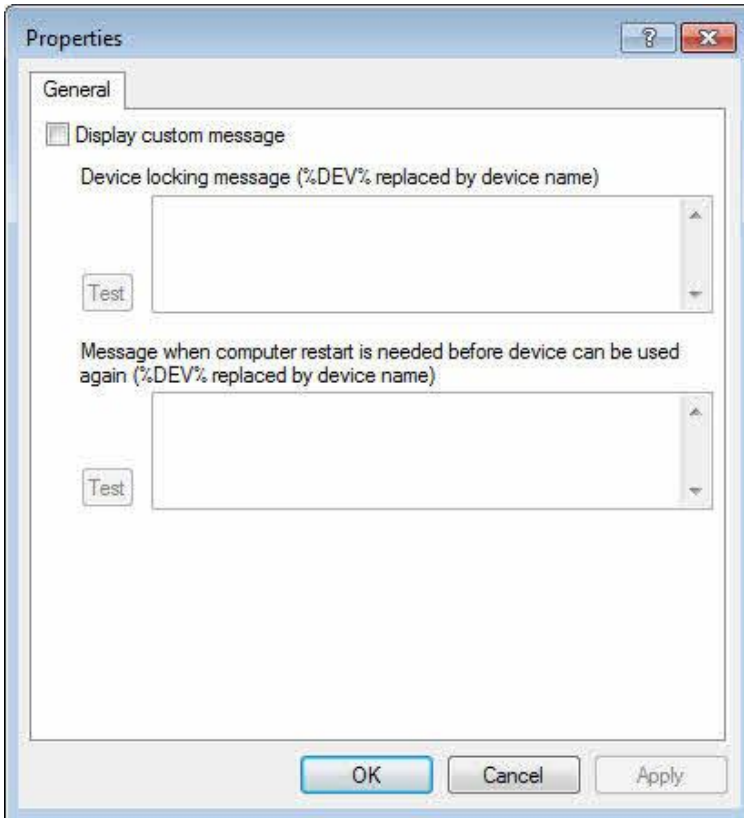
9.2.2.1 General Device Locking Settings

To configure general settings for locking devices, click **Settings**.

9.2.2.1.1 Configuring User Notification Messages for Locking Devices

By default, DriveLock displays a notification message when a device is connected to the computer and locked. To modify the content of these messages, click **Custom user notification messages**.

If you configured multilingual messages for the current language, DriveLock will display the messages you defined for this language instead of the messages configured in this dialog box.



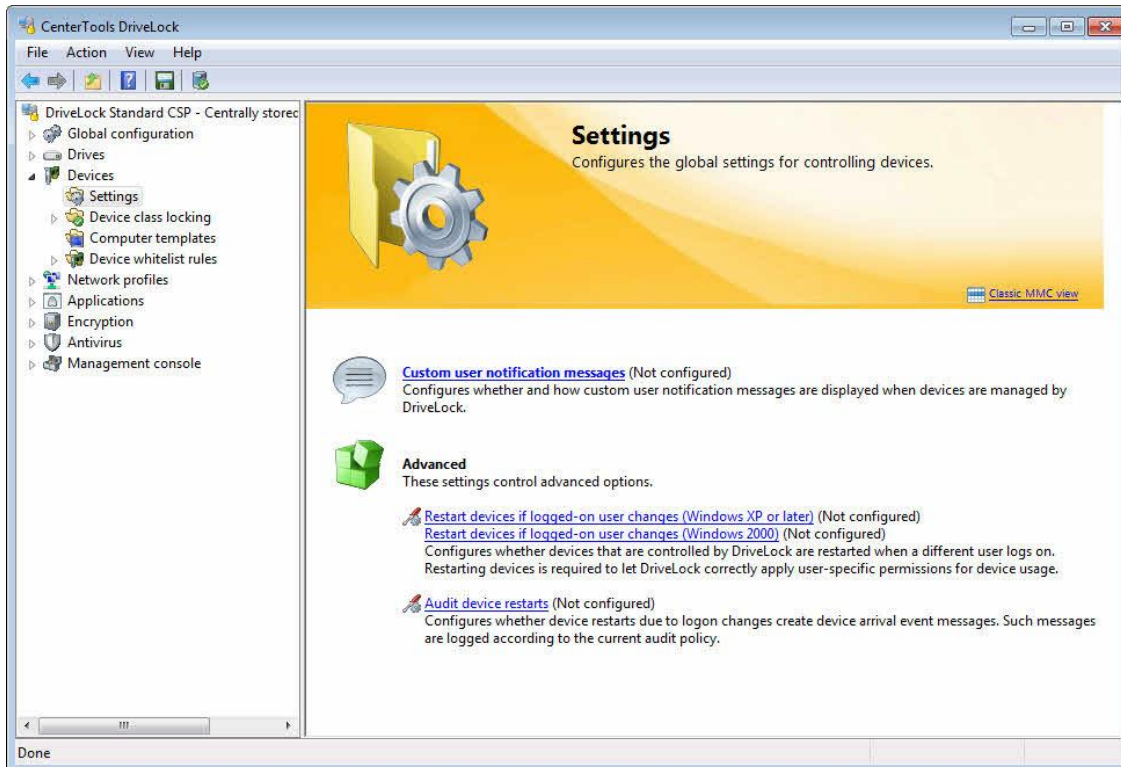
Select “**Display custom messages**” to enable the messages specified on this dialog box. The device locking message is displayed each time a device is locked by the Agent.

Type the message to be displayed to the user. When the message is displayed, the Agent replaces the variable “%DEV%” with the actual name of the locked device.

Click the **Test** button to preview the notification message on your computer.

You can use certain HTML-tags, such as “`Text`”, to format a message.

9.2.2.1.2 Advanced Global Settings for Controlling Devices



To define the following additional settings, click the corresponding links in the task view:

- *Restart devices when logged-on user changes*: When activated, each time a new user logs onto the system, DriveLock restarts all devices.
- *Audit device restart*: When activated, DriveLock generates audit events each time a device is restarted.

Available options for configuring each of global settings are **Enable**, **Disable**, and **Not configured**.

9.2.2.2 Enabling Device Locking

Procedures for locking devices are similar to those for locking drives. By default, DriveLock doesn't monitor any devices other than drives, serial ports and parallel ports. You need to explicitly configure DriveLock to monitor devices belonging to any device classes it recognizes. When you enable locking of a device class, all devices of this class, including all devices connected to type of controller or port you lock, are blocked, except those that are allowed by a whitelist rule.

DriveLock distinguishes between controllers, ports, devices and smartphones. You can lock the following types of controllers and ports:

- Serial (COM) and Parallel (LPT) ports
- Bluetooth transmitters (interface)
- Infrared interfaces
- USB controllers
- Firewire (1394) controllers
- PCMCIA controllers

You can lock the following types of smartphones:

- Apple iTunes-synchronized devices

- iTunes software restrictions
- Palm OS handheld devices and Smartphones
- Windows Mobile handheld devices and Smartphones
- BlackBerry devices
- Nokia mobile phones

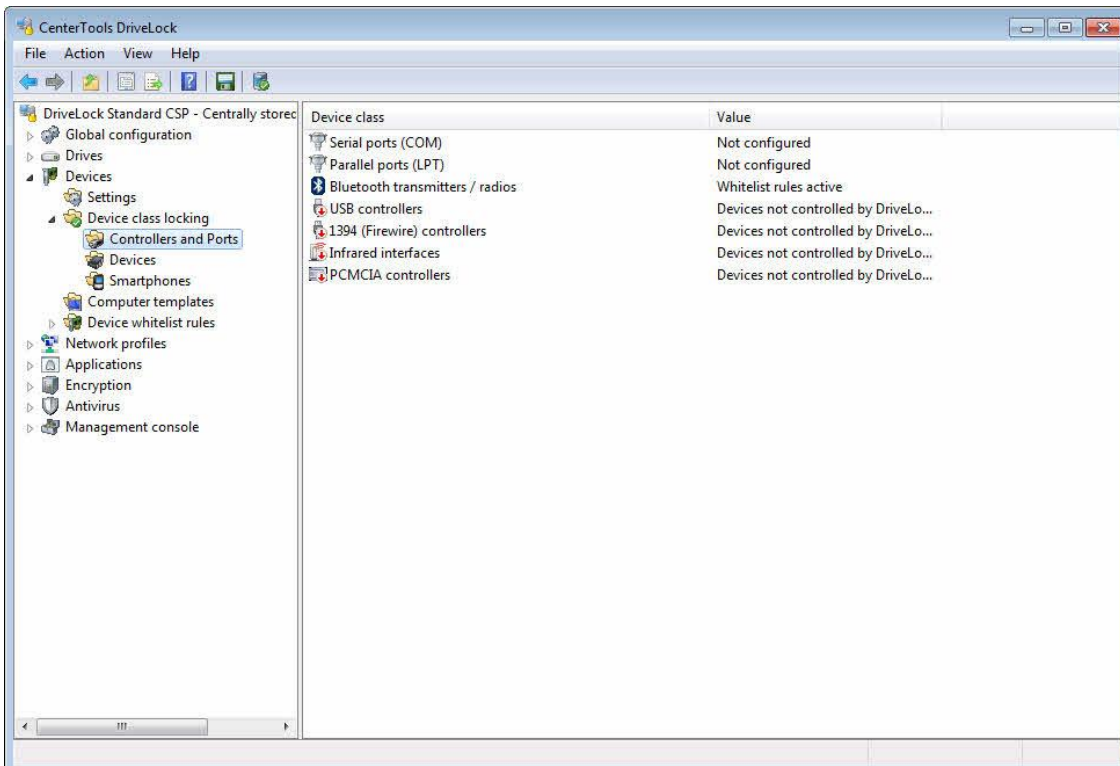
You can lock the following types of devices:

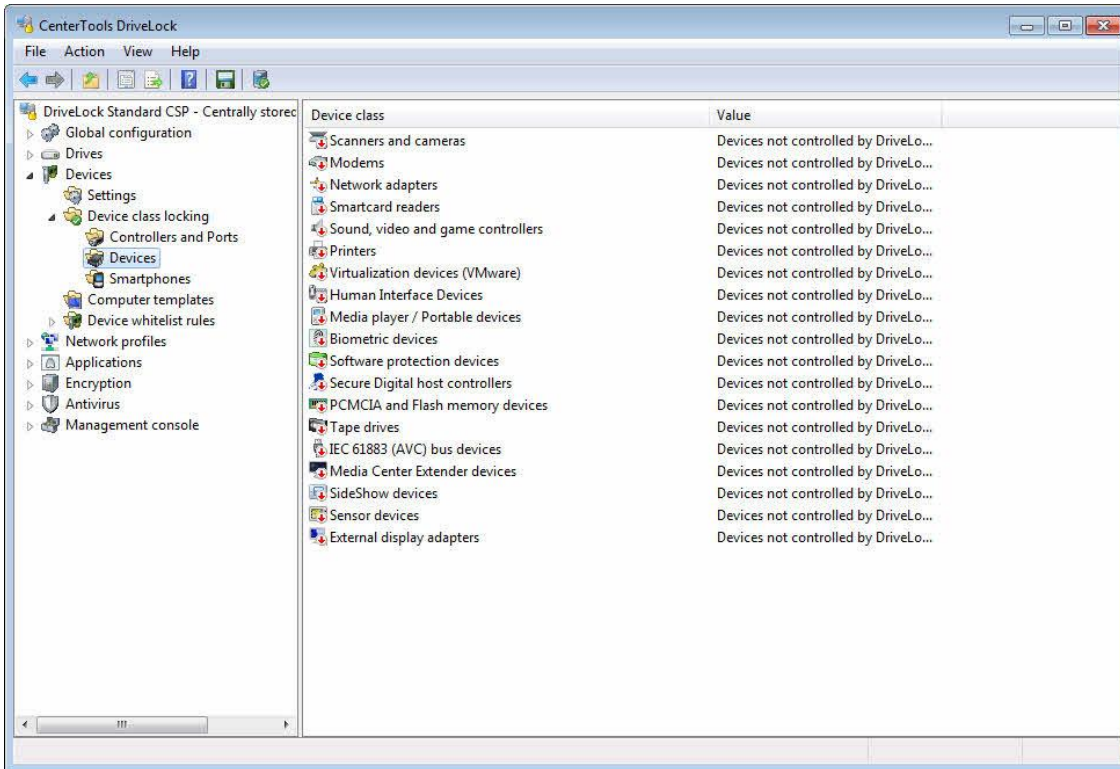
- Scanners and cameras
- Modems
- Printers
- Network adapters
- Smartcard readers
- Audio, video, and game controllers
- Virtual devices (VMware)
- Human interface devices (for example, keyboards and mice)
- Media player devices
- Biometric devices
- Software protection devices (dongles)
- Secure Digital Host controllers
- Tape drives
- PCMCIA and flash memory devices
- IEC 61883 (AVC) bus devices
- Media Center Extender devices
- Windows SideShow devices
- Sensor devices

To enable device locking, in the DriveLock Management Console, in the console tree, click **Local policy -> Devices -> Device class locking**.

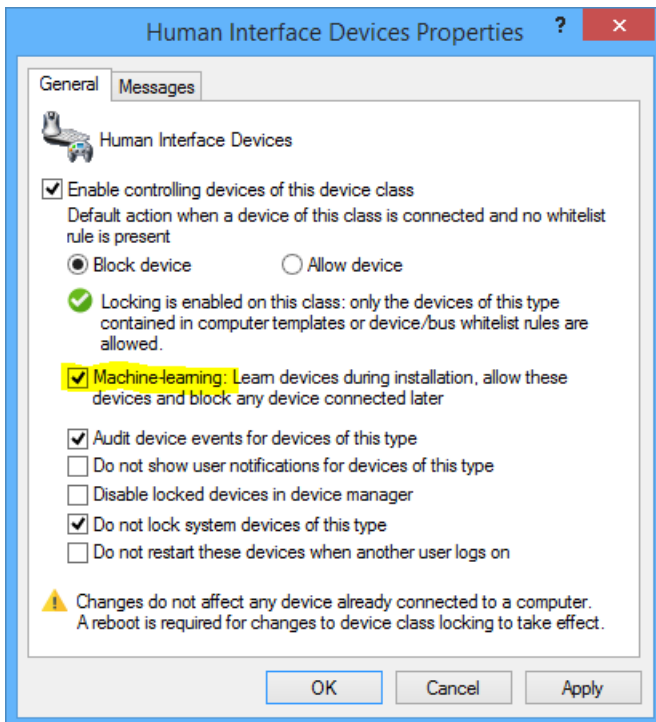


Click **Controllers and Ports**, **Devices** or **Smartphones** to display the list of all device classes in that category.





Double-click a device class (such as **Human Interface Devices**) to open the configuration dialog box for that class.



Machine Learning

For many device types you may activate **Machine Learning**. If activated for the first time the devices which are connected at installation time are learned in a local whitelist and will be allowed during boot time in the future. Devices of the same type which are connected later will be blocked. In the example above, a BAD-USB Stick which simulates to be a keyboard will be blocked. To relearn the local whitelist, run `drivelock - recreatebootdevs` from the command line.

The configuration dialog box is identical for all device types, except for serial and parallel ports. For information about locking serial and parallel ports, refer to the section "[Configuring Serial and Parallel Port Locking](#)".

When you lock a device, the Windows Device Manager displays a yellow warning icon next to it.

Also, in the configuration dialog box, you can specify whether events for devices in this class are audited. If selected, the DriveLock Agent sends event messages to destination you defined, such as the Windows Application Log and the DriveLock Enterprise Service.

To exempt system devices, such as network miniport drivers or UBS hubs from device locking, select the corresponding checkbox. To avoid configuring whitelist rules for such "software" devices, this option is enabled by default. If you disable this option, you must define whitelist rules for all system devices that are required for normal computer operations.

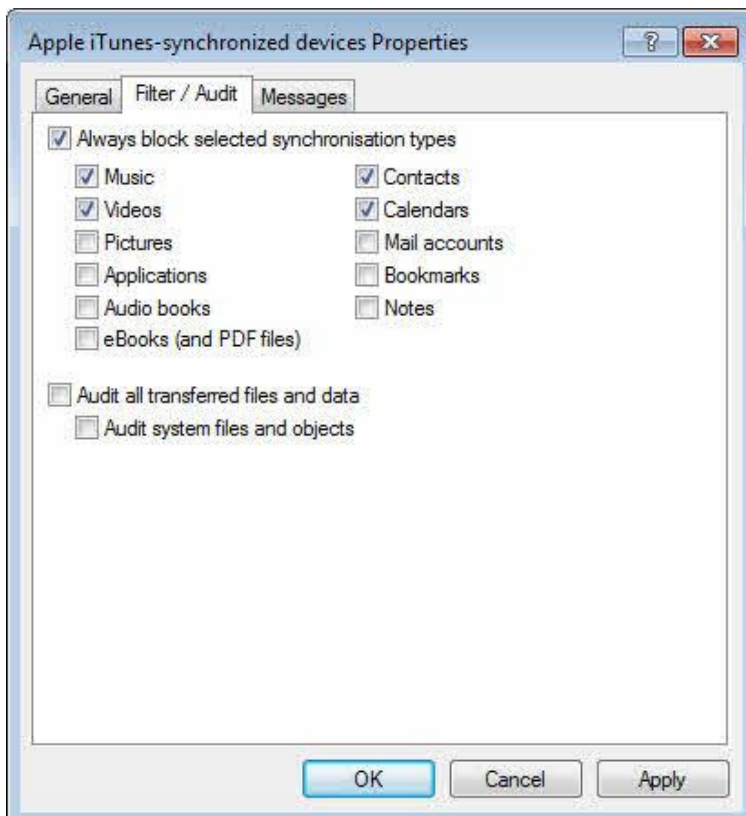
9.2.2.3 Granular Control of iTunes-Synchronized Devices

For iTunes-synchronized devices granular control options are available. This differs from other device classes, which only let you allow or deny access. This granularity lets you control the use of mobile Apple devices, such as iPhones and iPods and monitor data transfers between computers and such devices. This functionality is in addition to the restrictions you can configure in iTunes itself, such deactivating Apple TV.

You can configure restrictions on these devices under *Extended configuration -> Devices -> Device class locking -> Smartphones -> Apple iTunes-synchronized devices*. On the *Filter/Audit* tab, select which of the following data types will be blocked during synchronization:

- Music
- Videos
- Pictures
- Applications
- Audio books
- eBooks (and PDF files)
- Contacts
- Calendars
- Mail accounts
- Bookmarks
- Notes

Select the *Audit all transferred files and data* to create audit events for all data transfers. This functionality is similar to file auditing for drives.

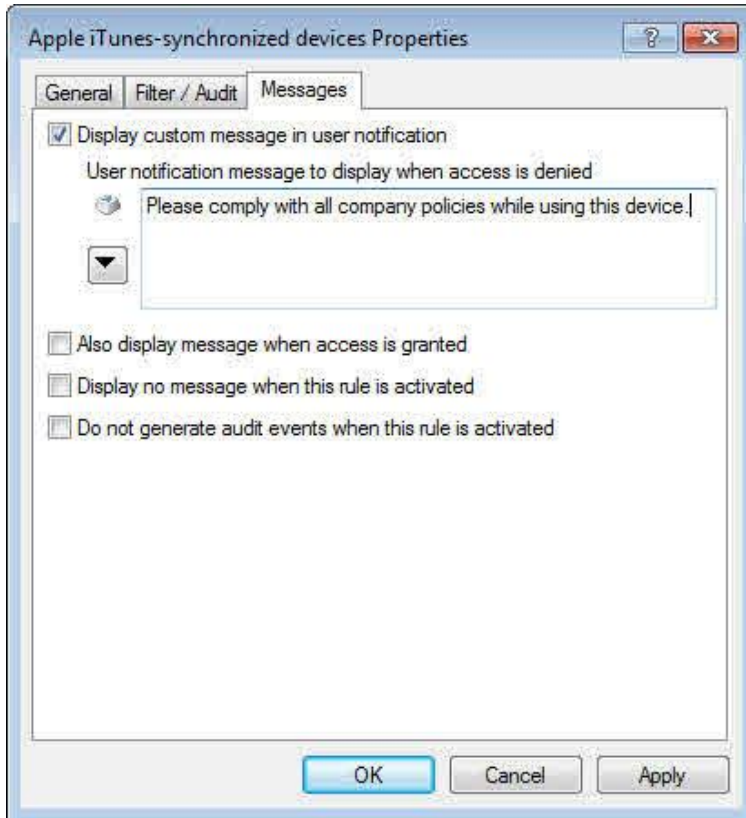


To restrict data transfers using iTunes, click *Extended configuration -> Devices -> Device class locking -> Smartphones -> iTunes software restrictions*. Select *Set to value* and then select any of the following options:

- Device synchronization
 - Require encrypted device backups

- Disable registering new devices
- Disable automatic device synchronization
- Software updates
 - Disable checking for iTunes updates
 - Disable checking for App updates
 - Disable checking for device firmware updates
- Media functions
 - Disable podcasts
 - Disable iTunes store
 - Disable explicit content
 - Disable Internet radio
 - Disable iTunes ministore
 - Disable loading album artwork
 - Disable plugins
 - Disable opening streams
 - Disable Apple TV
 - Disable diagnostics
 - Disable sharing
 - Disable home sharing
 - Disable iTunes Ping!
 - Allow access to iTunes U

You can configure custom user notifications on the “*Messages*” tab.



Select the **“Display custom message in user notification”** checkbox to activate the user notification message for the whitelist rule.

In the text edit box, type the message. DriveLock will display this message regardless of the client computer’s language setting. If you use this type of notification message, DriveLock displays a key icon near the top left corner of the text edit field.

If you have defined multilingual messages you can select this message type instead. To select a multilingual message, click the “down arrow” button and then on the drop-down menu click “Select multilingual message”.

Multilingual messages contain separate messages in multiple languages for the same notification. Before you can use such a message, you must define it in the *Global configuration* section of the policy. When you select a multilingual notification message, DriveLock displays the text in the language of the currently logged-on user.

Click the message and then click **OK**.

If you use this type of notification message, DriveLock displays a speech bubble icon near the top left corner of the text edit field.

To also display the message when a user connects a drive and the rule allows access, select the **“Also display message when access is granted”** checkbox. To not display any notification message when this rule is activated, including any default language message that you defined for all drives, select the **“Display no message when rule is activated”** checkbox.

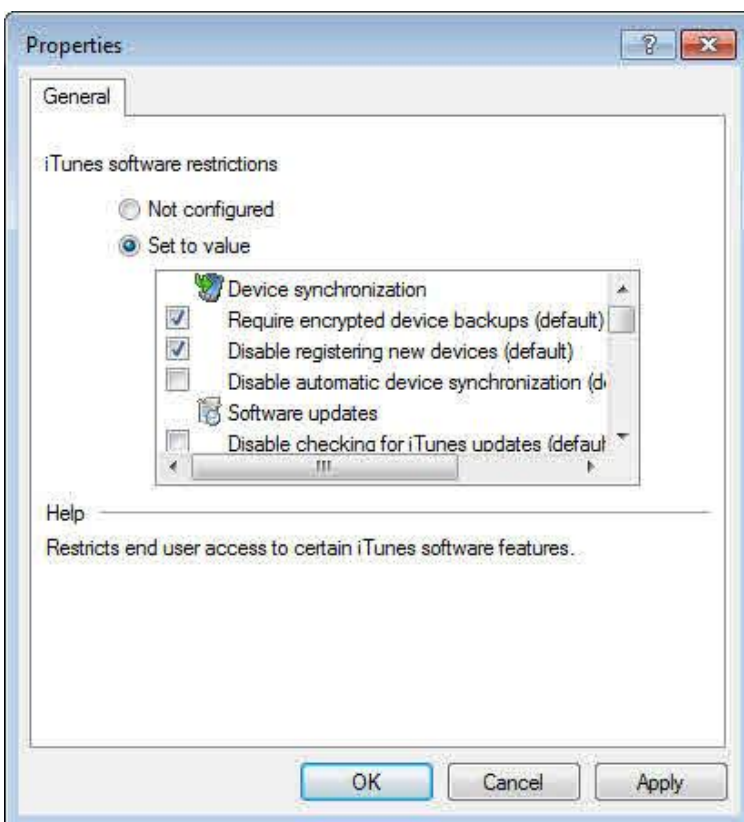
To not generate any audit events when this rule is activated, select the corresponding check box.

To have the user accept a usage policy before granting access, activate the **“User must accept usage policy before rule will be applied”** checkbox. To also require a password, type and confirm the password that a user needs provide to access the drive.

Click **OK** to accept the settings.



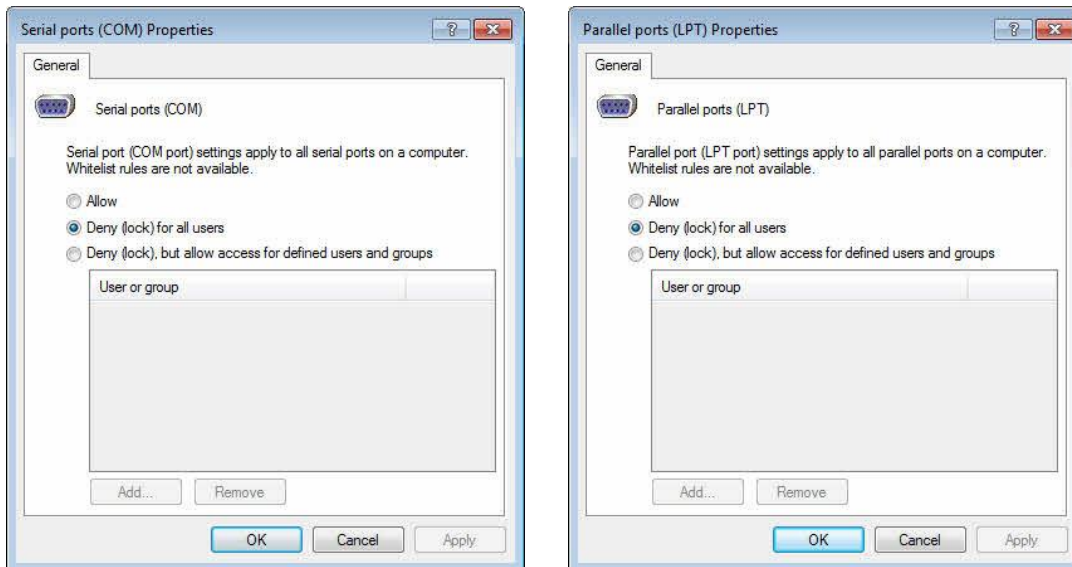
Click **iTunes software restrictions** to specify which iTunes functions user can access and how iTunes will be configured on users' computers.



Select **"Set to value"** and then select each setting that you want to enable and clear all settings you want to disable. Click **OK** to accept the settings.

9.2.2.4 Configuring Serial and Parallel Port Locking

You can lock serial (COM) and parallel (LPT) ports for all users or allow access only for selected users and groups. Additional granularity and whitelist rules are not available for these types of ports.



Select from the following options:

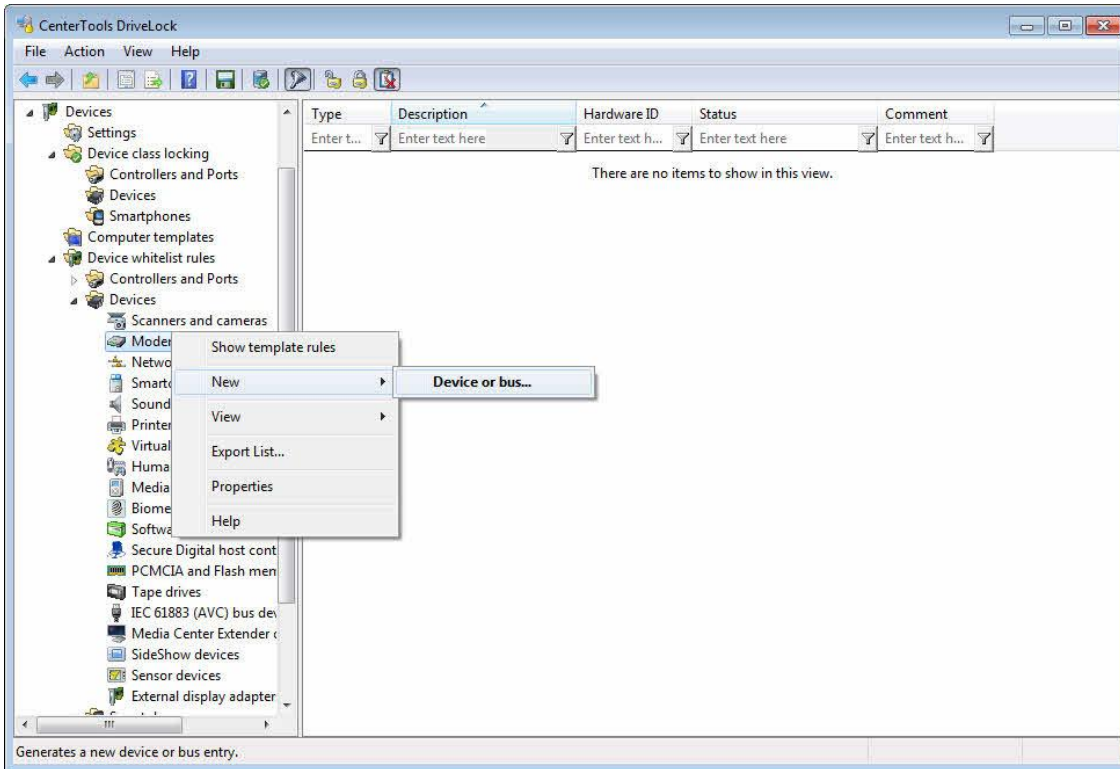
- *Allow*: All authenticated users can access the ports.
- *Deny (lock) for all users*: Nobody can access the ports, they are completely locked.
- *Deny (lock), but allow access for defined users and groups*: The ports are locked, but the specified users or groups are allowed to use the ports.

To add an entry, click **Add** and then select a user or group. To remove an entry, select the user or group and then click **Remove**.

Palm OS and Windows CE devices that are connected using a serial port can only be controlled by blocking serial ports altogether. You can't control such devices by using the device classes "Windows CE Handhelds and Smartphones" or "Palm OS Handhelds and Smartphones" because Windows can't identify which specific devices are connected to a serial port.

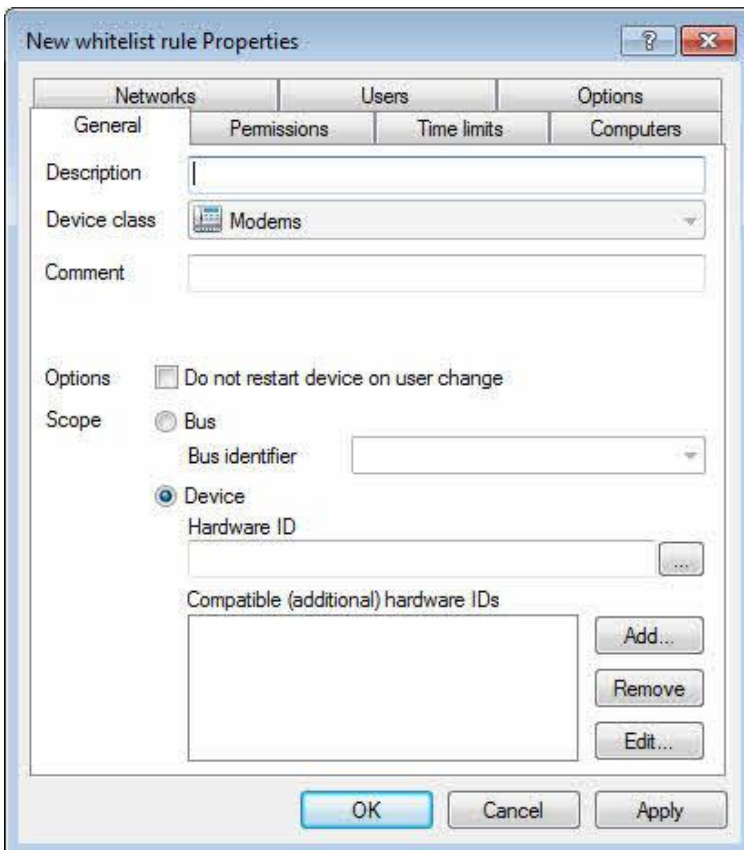
9.2.2.5 Creating Device Rules

You configure whitelist rules for devices the same way as drive whitelist rules. The following example illustrates how to create a whitelist rule for a modem.



In the console tree, expand Devices, expand Device whitelist rules, expand Modems, right-click **Modems**, and then click **New -> Device or bus**.

In the “New whitelist rule Properties” dialog box, configure the settings for locking the device.



In the description field, type a name for the rule. To record additional information about the rule, you can type a comment in the Comment field.

Define the scope of the rule by identifying the device. To specify all devices of the selected type that are connected to a specific hardware bus, select **Bus** and then select the bus from the dropdown menu.

When you specify a bus in a whitelist rule, the rule is activated when a device in the selected class (for example, **Modems**) is connected to the computer using the selected bus.

Example: To enable all PCI network cards in a computer, create a new whitelist rule for network adapters and select "PCI" bus as the identifier. This enables all internal network adapters connected to the PCI bus while locking all network adapters that are connected to an external bus, such as PCMCIA and USB.

If no predefined device bus matches your needs, specify a new adapter type by typing the bus identifier in the corresponding field.

In some cases whitelist rules can conflict with each other. In such cases, DriveLock uses the following rules to determine whether a drive is locked or access is allowed:

- Bus locked and device allowed -> device allowed
- Bus locked and device locked -> device locked
- Bus allowed and device locked -> device locked
- Bus allowed and device allowed -> device allowed

If a device or bus is locked by one rule and access is allowed by another, access to the device or bus is allowed.

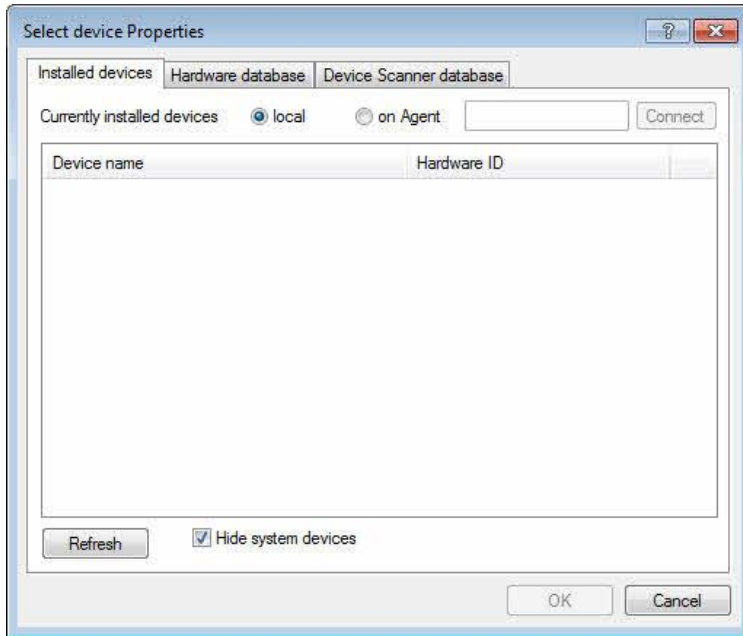
Rules that are defined by using computer templates are processed the same way as manually created whitelist rules.

For more granular device control you can create rules for devices with a specific hardware ID and compatible IDs. Each device has a unique hardware ID. In addition Windows maintains a list of compatible hardware IDs. Windows uses this hardware ID and any compatible IDs to find a driver for the device when it is connected to a computer. Most hardware IDs can also contain a revision number that is assigned by the manufacturer but which is not used when selecting the device driver. If a hardware ID contains a revision number, Windows uses one of the compatible IDs that does not contain the number.

To specify a device, type its hardware ID in the corresponding field. You can find the hardware ID in the Windows Event Log or in the registry of the computer.

Ensure that no blank spaces precede or follow the hardware ID.

To determine the hardware ID more easily, click "..." next to the hardware ID field and then use the built-in hardware database results to find the device.



Select currently installed local devices or connect to an Agent running on another computer to obtain a list of devices currently connected to that computer.

Click **Refresh** to display recently connected devices. Palm or Windows Mobile-based handheld computers are usually connected to the computer while the HotSync or ActiveSync process is running.

Select "**Hide system devices**" to hide all Windows system devices, which are not locked by default (as determined by the option "**Do not lock system devices**" in the device class configuration dialog box).

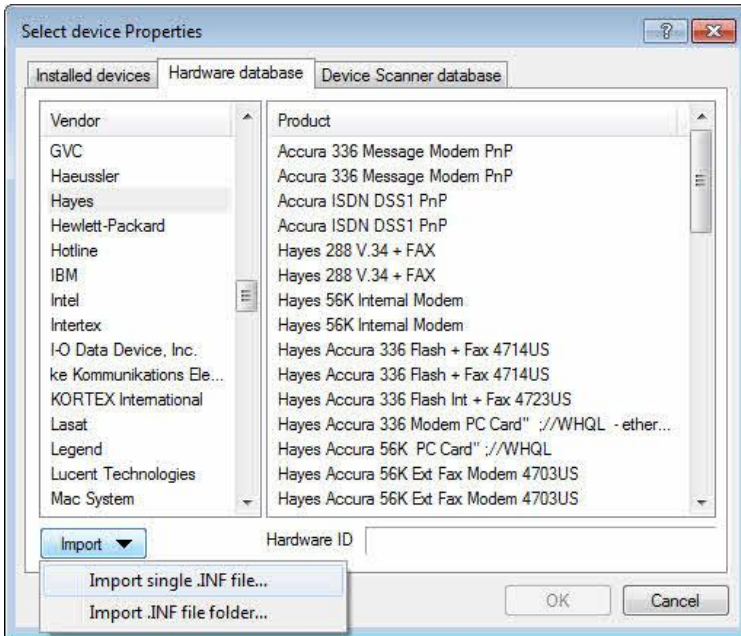
You can select additional devices by remotely connecting to another agent and selecting an existing device. Select "**up**" and enter the name of the computer you want to connect to. Make sure that the DriveLock Agent must be installed on the target computer.

Note that the hardware ID is also read out in this way and included in the whitelist rule. When using a virtual environment (e.g. VMWare), this rule may be ignored because devices are emulated in these virtual environments and the hardware ID is not present or different.

Additionally, click the **Hardware database** or **Device Scanner database** tabs and then select a device from the list.

The hardware database contains information about all devices for which drivers are included with the operating system. DriveLock provides access to this list to make it easy to configure devices, but DriveLock has no control over this list. You can add devices to the hardware database by using an INF file that contains information about the device. Such .INF files are typically included with device drivers that hardware manufacturers include with their products.

To import new device data from an .INF-file into the database, click **Import**.



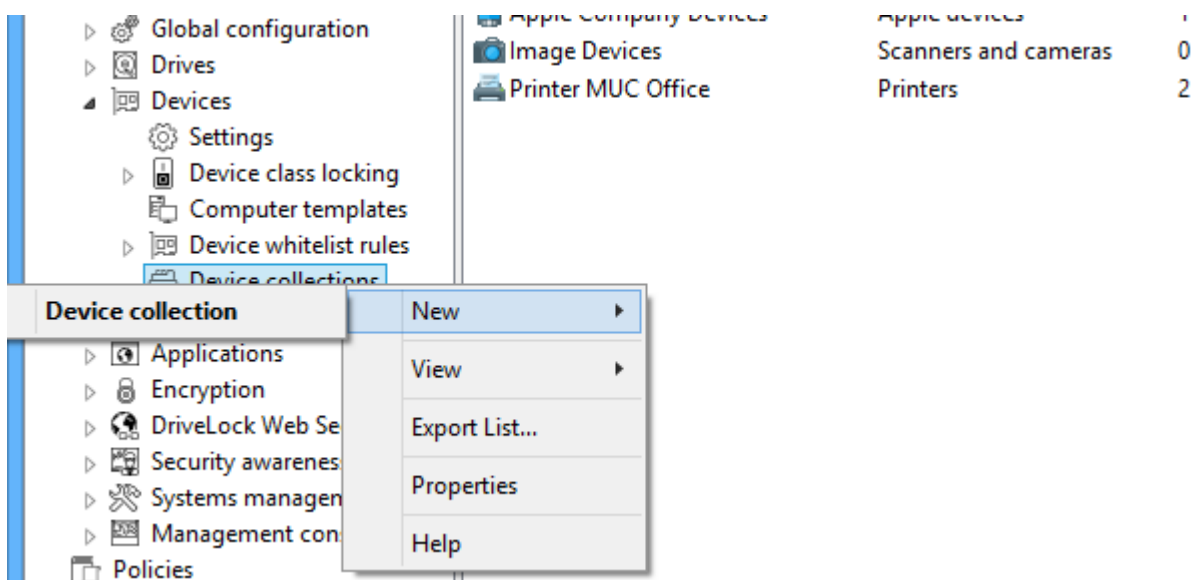
Select whether to import data from a single file or from all .INF-files in a directory, and then select the file or directory.

9.2.2.6 Creating Device Collections

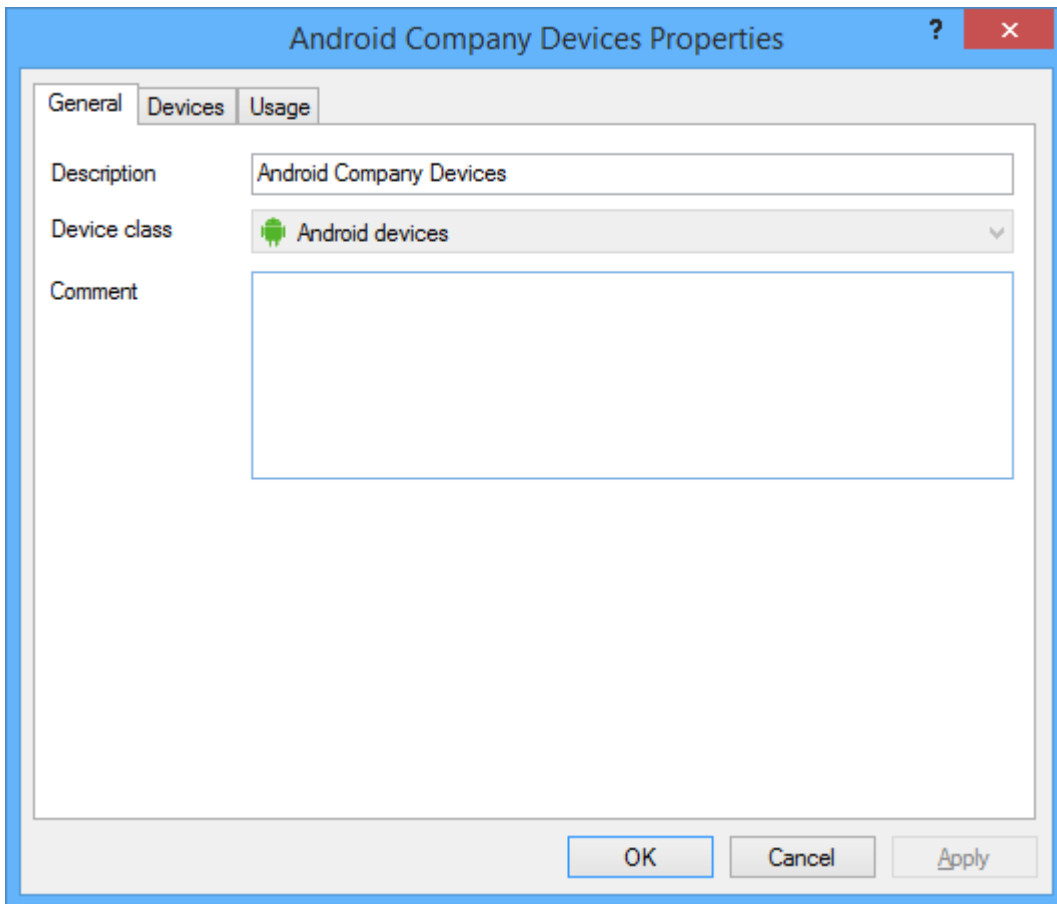
Device collections make it easier to manage devices of the same type if the same settings should apply and they reduce the number of required whitelist rules. Device collections may contain several similar devices and can be used to configure whitelist rules - similar to using individual devices based on their hardware ID.

At the same time, you can separate the management of the device collections from the configuration of the security and lock settings.

Creating a device collection



To create a new list, right-click **Device collections**. Then select **New -> Device collection** from the context menu.

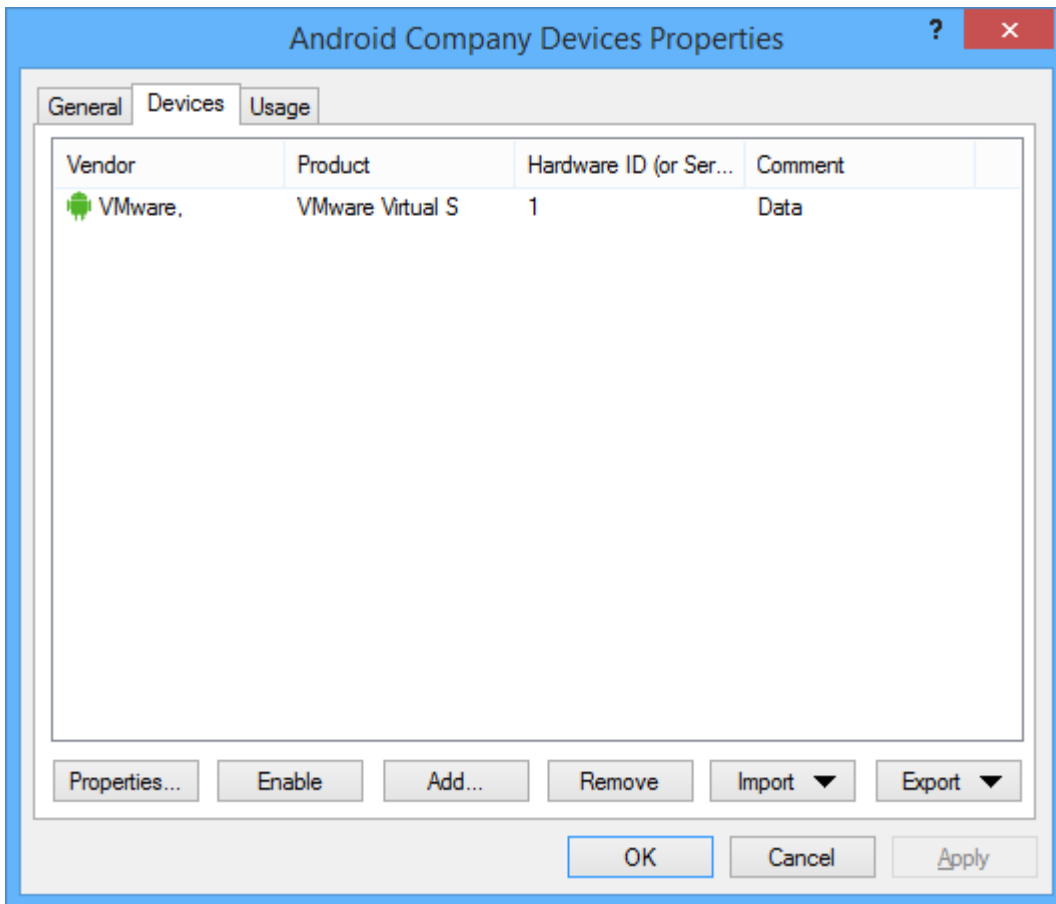


You can enter a description and a comment for the collection.

You can also select the device class from the list of available classes when creating a new collection. This device class determines which types of devices you can add to the collection and can not be changed after you have saved it.

The choice of device class determines which class this collection may be used for configuration and which technical options are available for controlling these devices.

Click the **Devices** tab to manage the devices contained in this list



Here you can display, deactivate, edit and remove existing entries. You can also add new entries.

To add new entries, click **Add** and select whether you want to add a device based on its product or vendor ID, or by its hardware ID (only for devices that provide this information - if not, only the hardware ID is requested). Enter the required information in the next dialog or select it as usual from the currently connected devices or the Device Scanner database by clicking "...".

If you do not want to delete existing drives completely, but only remove them from the collection for a certain time, select the drive you want and then click **Disable**. A small additional icon now indicates that the entry is currently not enabled and cannot be locked/unlocked using this collection. Disabled items can be re-enabled later.

Use the **Import** button to import multiple drives in either CSV or INI format. A CSV file could look like this, for example:

HardwareID	Comment	Vendor	Product	SerialNumber	Enabled	ClassId
MF\BRMFC860LPT_PRT0,Brother_MFC-860	Brother MFC-8600				1	{4D36E979-E325-11CE-BFC1-08002BE10318}
Xerox4520CCAD,Xerox_4520_PS	Xerox 4520 PSS				1	{4D36E979-E325-11CE-BFC1-08002BE10318}

Click **Export** to save the current list as a CSV or INI file.

Tip: If you created some entries individually and then exported them as a file, you can use this file as the basis for an import, since it already has the correct structure and/or the necessary columns.

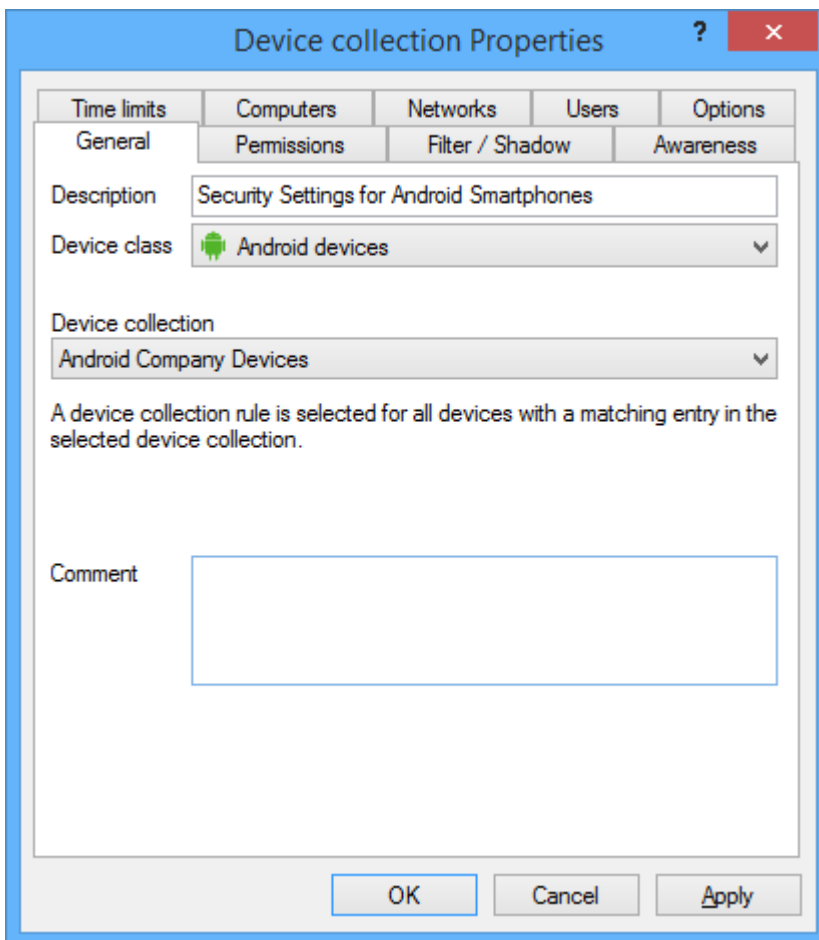
The **Usage** tab shows you the device collection rules where the collection is used already.

You cannot delete the collection as long as a device collection is being used in a rule.

Click **OK** to save the collection and/or your changes and return to the list view.

Using a device collection for configuration

You can now use the device collection for a specific device class to configure settings for that class. To do so, navigate to the device settings (e.g. **Device whitelist rules** -> **Smartphones** -> **Android devices**) in the DriveLock Management Console and right-click Android devices. Then select **New** -> **Device collection rule** from the context menu.



Now you can add a description and a comment. Select the collection you created previously from the device collection.

The system only displays collections with the same device class.

You can now use the other tabs to configure the security settings for the DriveLock policy in the same way as the device rule.

If you want to save the settings, click **Apply**. If you click **OK**, the changes are also saved and the properties window is closed.

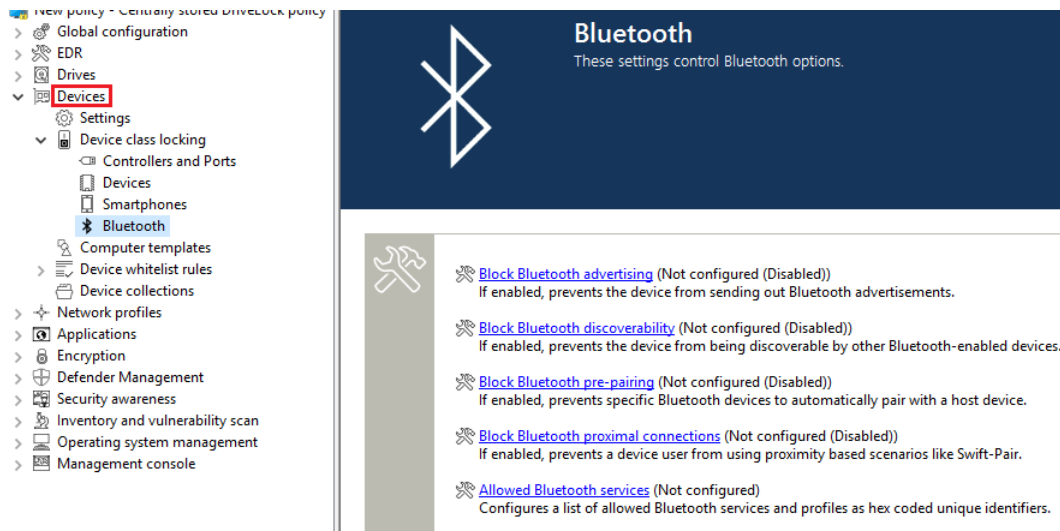
9.2.3 Bluetooth Devices

DriveLock version 2021.1 and higher provides settings for connecting devices via Bluetooth, allowing you, for

example, to prevent pairing with new devices or to configure restrictions on preferred Bluetooth services.

Use case: You want to control the use of some Bluetooth devices (e.g. mouse, keyboard or Microsoft Surface Pen). These devices will be allowed but all other Bluetooth devices (including their functions such as file transfer) will be blocked.

Go to the **Devices** node in the DriveLock Management Console and select the **Bluetooth** sub-node in the **Device class locking** section.



You can choose from the following settings here. By default, they are disabled.

- **Block Bluetooth advertising**
 Select this option if you want to prevent the device from sending Bluetooth advertisements and for it to be detected by other devices.
- **Block Bluetooth discoverability**
 Use this setting to specify whether the device will be discoverable by other Bluetooth devices, such as a headset.
- **Block Bluetooth pre-pairing**
 Select this option if you want certain bundled Bluetooth peripherals to automatically pair with the host device.
- **Block Bluetooth proximal connections**
 This option prevents users from applying fast pairing and other short-range technologies.
- **Allowed Bluetooth services**
 This setting allows you to add allowed Bluetooth services and profiles to a list (using strings in hexadecimal format).

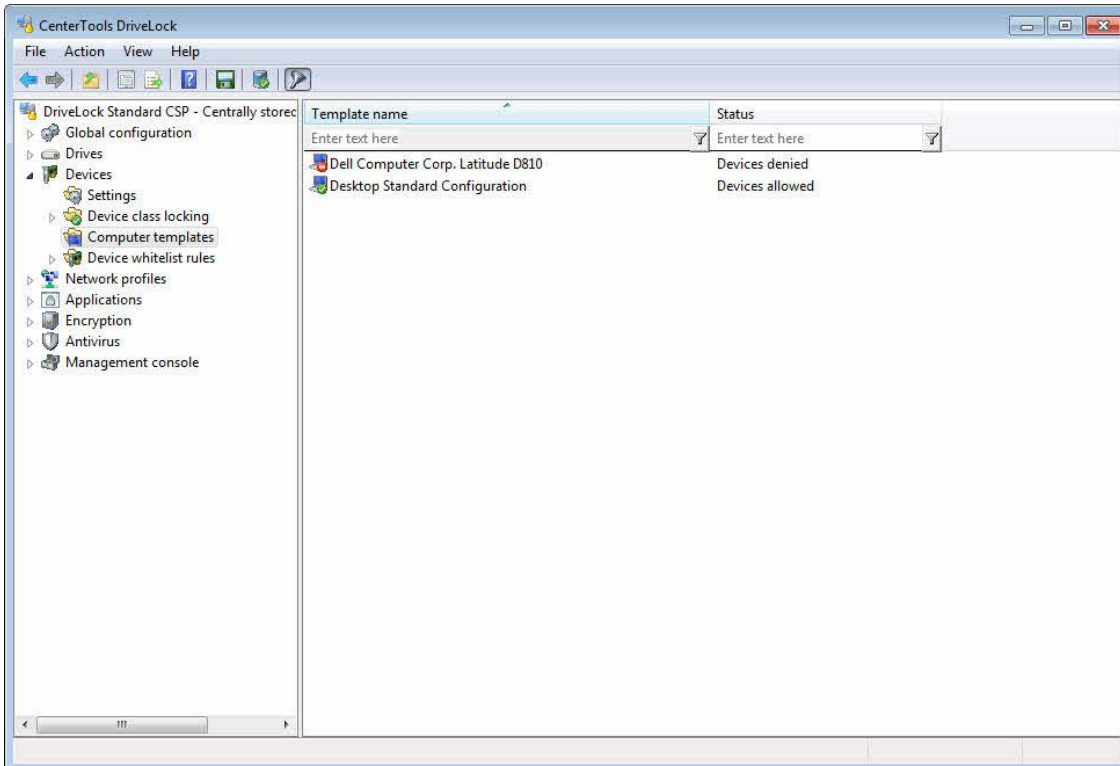
9.2.4 Using Computer Templates

Use computer templates to allow access all standard devices on a computer model.

Access to devices that you include in a computer template is always allowed without requiring you to create separate device whitelist rules for them.

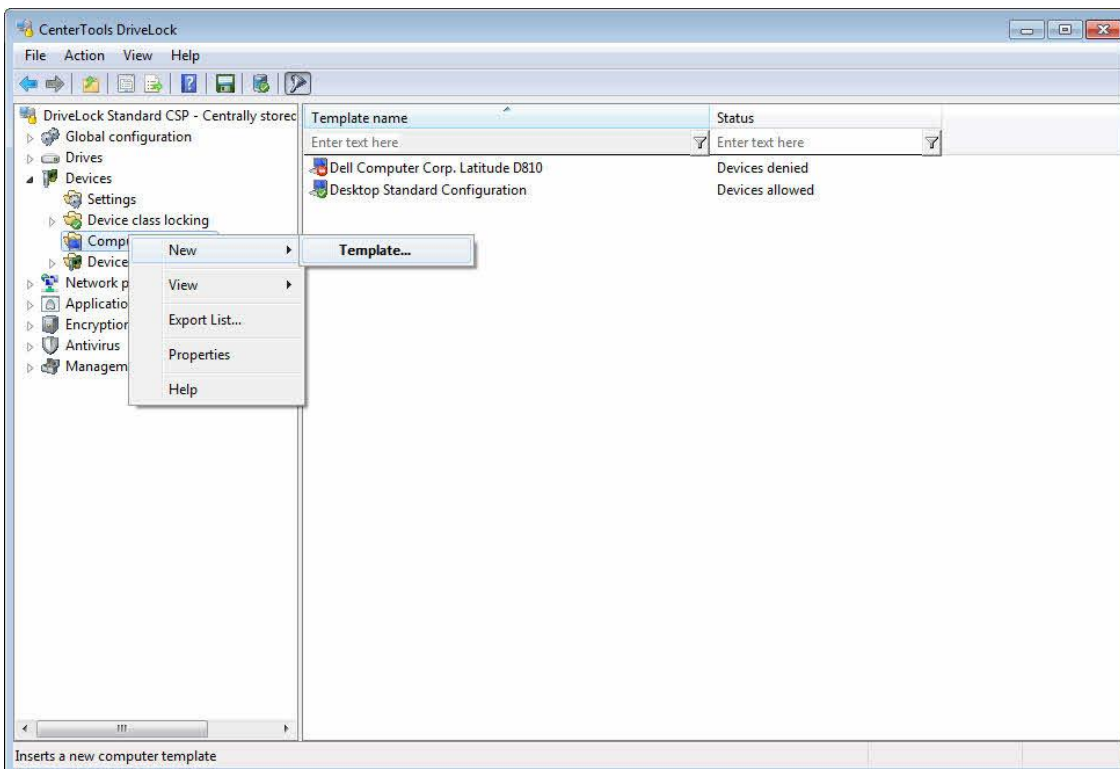
You can base a computer template on devices in the DriveLock hardware database or on the devices currently connected to your own computer. The built-in hardware database already contains information about many popular and widely deployed computer-models.

You can also create a template based on device types. Use this method to define a collection of devices that you want to allow or deny access to, such as a pool of scanners.

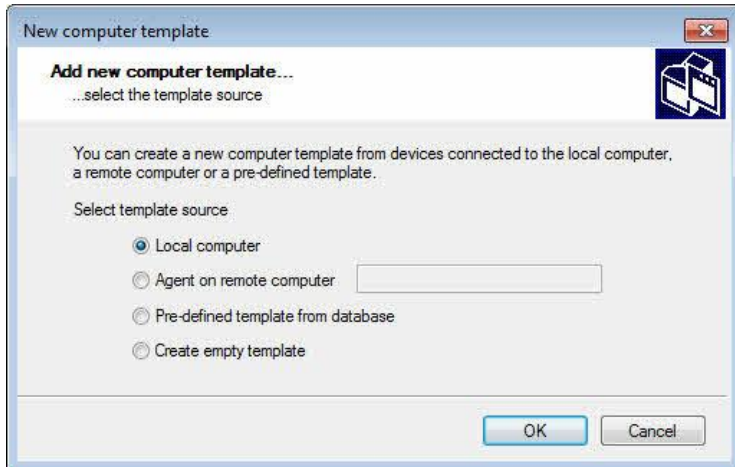


To display all devices that are allowed because of templates you have configured along with any whitelist rules, right-click **Device whitelist rules** and then click **Show template rules**. Use the rule icon to distinguish between the two types of rules.

9.2.4.1 Creating a New Computer Template

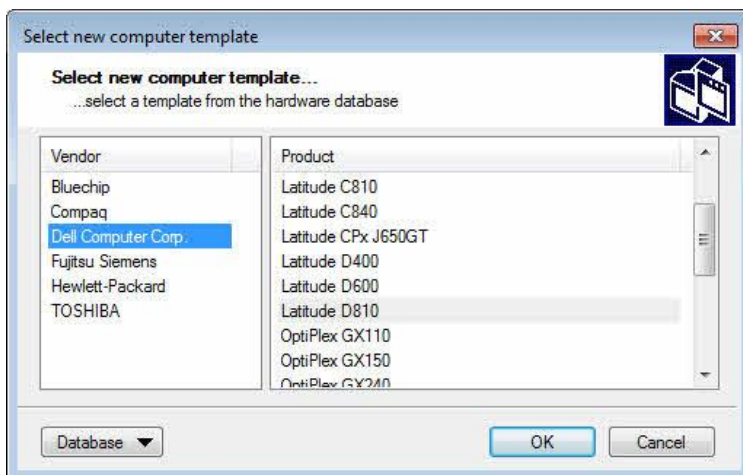


To create a new computer template, right click **Computer templates** and then click **New -> Template**.



9.2.4.1.1 Creating a Computer Template Based On the Local Computer

Select **Local System** as the template source and then click **OK**.



Type a name for the computer template (for example the computer name or type).

Click the **Device** tab to have DriveLock detect all devices that are currently connected to your computer and add them to the device list.

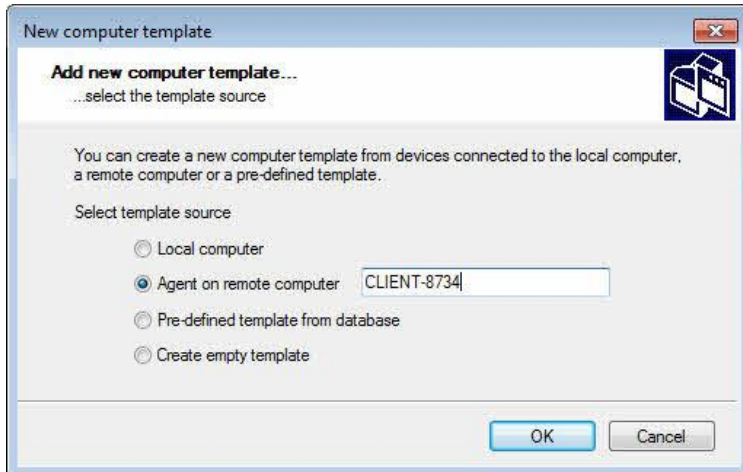
Refer to the section [“Working with Computer Templates”](#) for information about how to add additional devices and configure permissions.

9.2.4.1.2 Creating a Computer Template Based On a Remote Computer

The steps for creating a computer template from a remote computer are almost identical to those for creating a template from local information.

To create a template based on a remote computer, the DriveLock Agent must be installed and running on that computer.

Select **Remote agent on computer**, type the name of the remote computer, and then click **OK**.



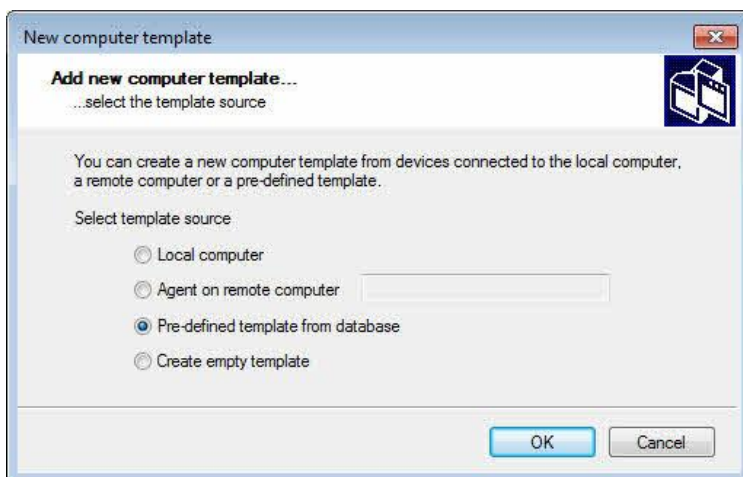
To establish a connection to a remote computer running Windows XP SP2 or later with the Windows Firewall enabled, you must configure the Windows Firewall to allow incoming connections from TCP Ports 6064 and 6065 (default) and access by the program "DriveLock".

Click the **Device** tab to have DriveLock detect all devices that are currently connected to your computer and add them to the device list.

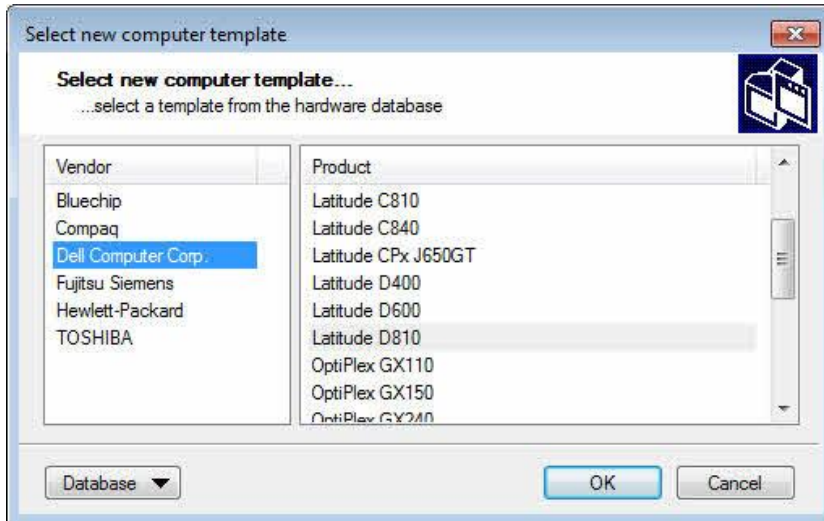
Refer to the section "[Working with Computer Templates](#)" for information about how to add additional devices and configure permissions.

9.2.4.1.3 Creating a Pre-Defined Template from the Database

Use a pre-defined template from the hardware database to create a new template that is based on built-in information or information based on a previous scan.



Check **Pre-defined template from database** and then click **OK** to open the hardware database.



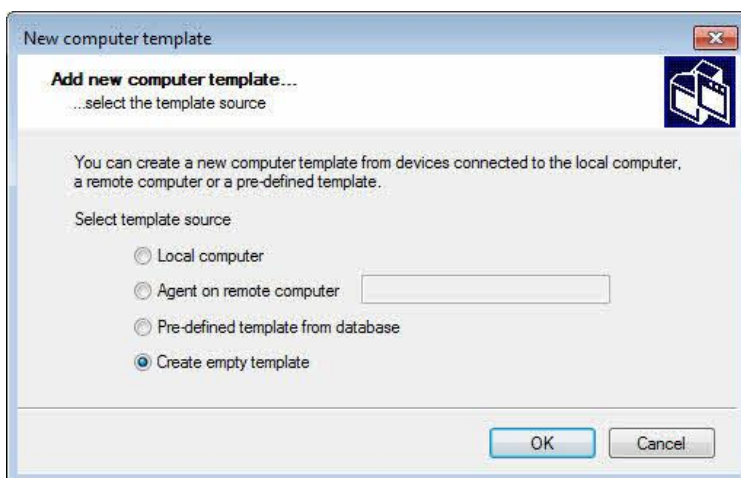
Select the existing template that you want to use, and then click **OK**.

DriveLock reads the template information from the database and adds them to the template's device list.

Refer to the section "[Working with Computer Templates](#)" for information about how to add additional devices and configure permissions.

9.2.4.1.4 Creating an Empty Template

Check **Create empty template** and then click **OK** to create a new empty template. You can add device information to this template later.



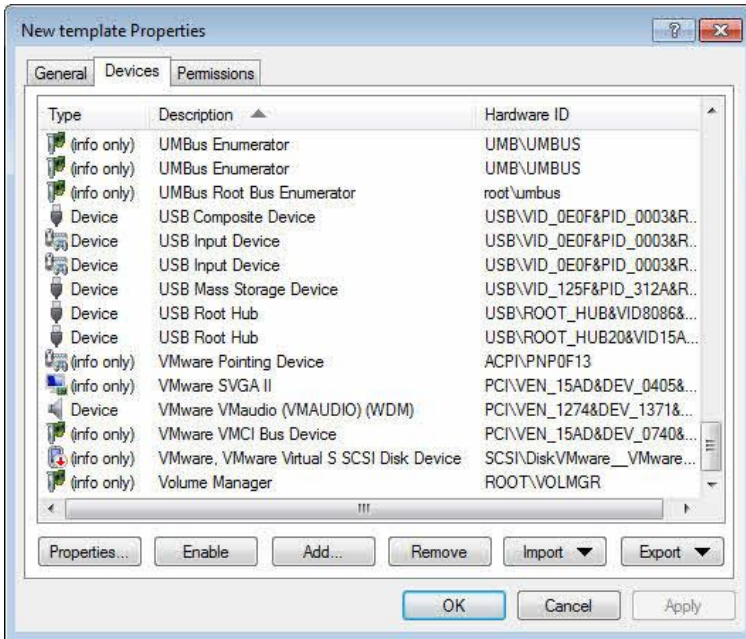
On the **device** tab no device are listed.

Refer to the section "[Working with Computer Templates](#)" for information about how to add additional devices and configure permissions.

9.2.4.2 Working with Computer Templates

Unless you created an empty template, DriveLock has automatically added devices to the template, either from the local computer, a remote computer or the built-in hardware database.

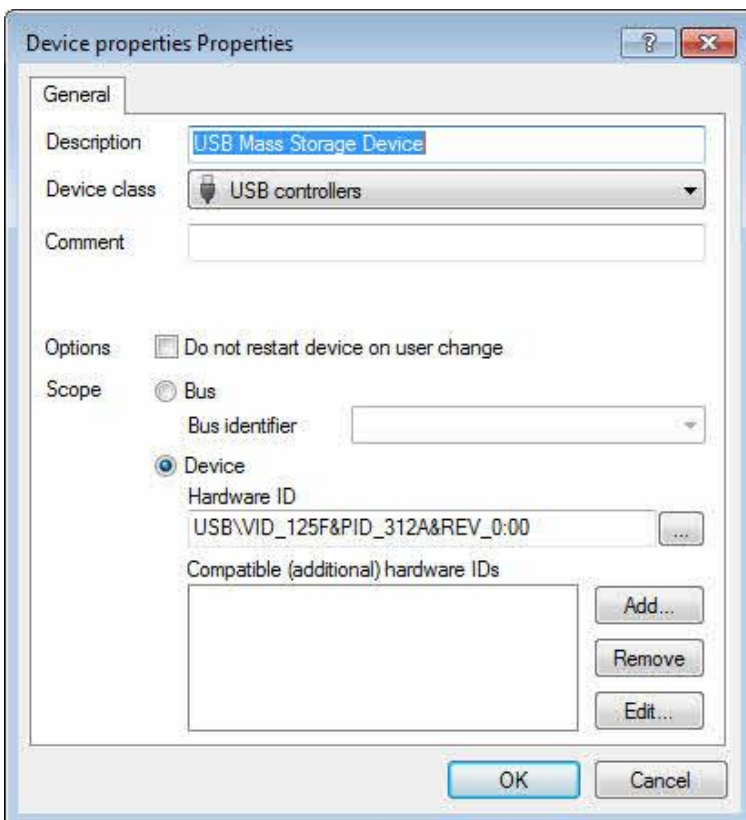
Use the device list to edit, add or delete listed devices.



The type “*info only*” indicates that DriveLock recognizes the device but cannot lock this type of device.

9.2.4.2.1 Editing a Computer Template Device List

Select a device and then click **Properties** to change its description, device class or type (bus or single device).



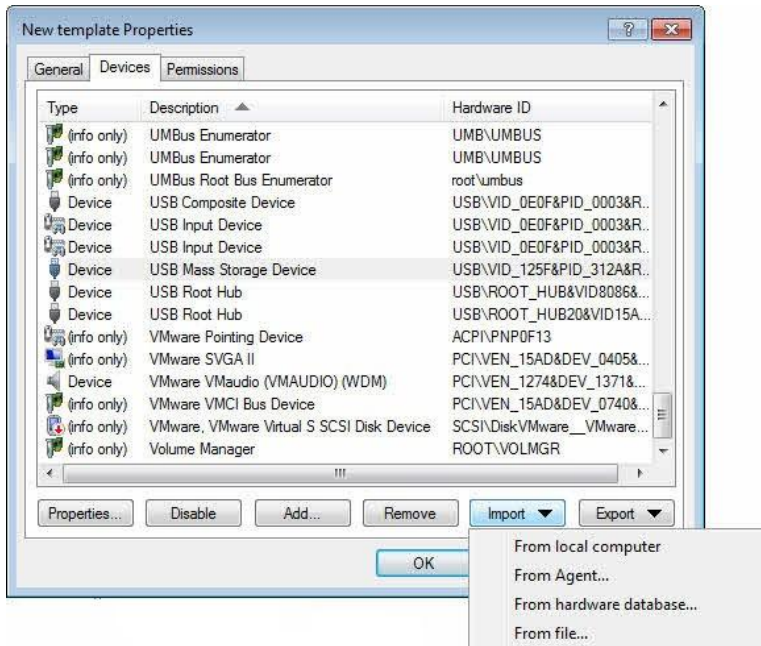
Configuring the properties of a device that is part of a template is similar to configuring a device whitelist rule. See the section “[Creating Device Rules](#)” for more information about configuring devices by using whitelists.

Click **Disable** to deactivate the selected device in the current template. The device remains in the template but is locked. You can later simply re-activate the device, if required.

Click **Add** or **Remove** to add devices to or remove devices from a template. This procedure is identical to adding a device to or removing a device from a whitelist rule (see the section “[Creating Device Rules](#)” for more information).

9.2.4.2.2 Importing New Devices into a Computer Template

To import devices into a template, click **Import** and then select a source to import device data from.



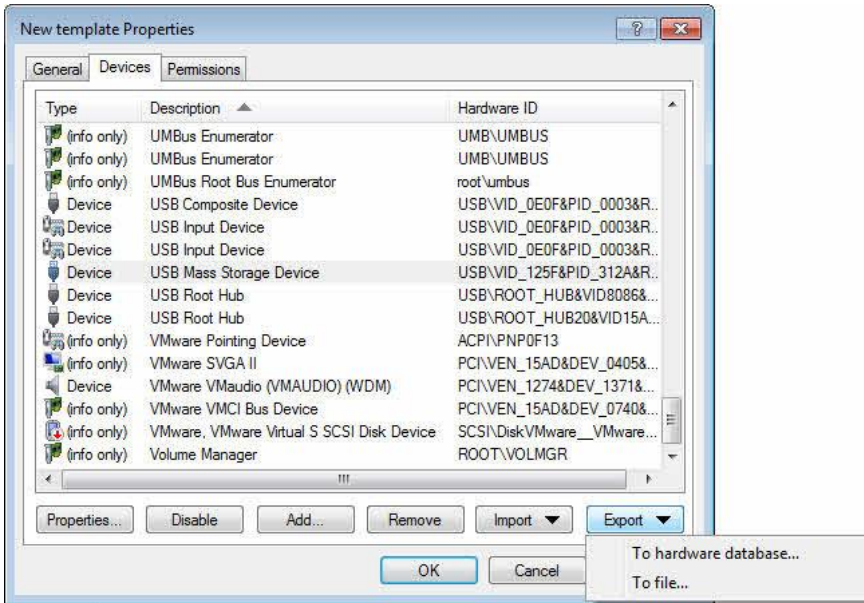
You can import device information from a local computer, a remote computer or the hardware database by performing the same steps as those for selecting a template source when creating a new template.

To import devices from an .INF file, for example an .INF supplied by a device manufacturer, click **From file** and then select the file to import device information from.

9.2.4.2.3 Exporting Devices from a Computer Template

Click **Export** to save a device list to an .INI-File or to your hardware database.

Ensure that the template has been named and saved before exporting its data to the hardware database.



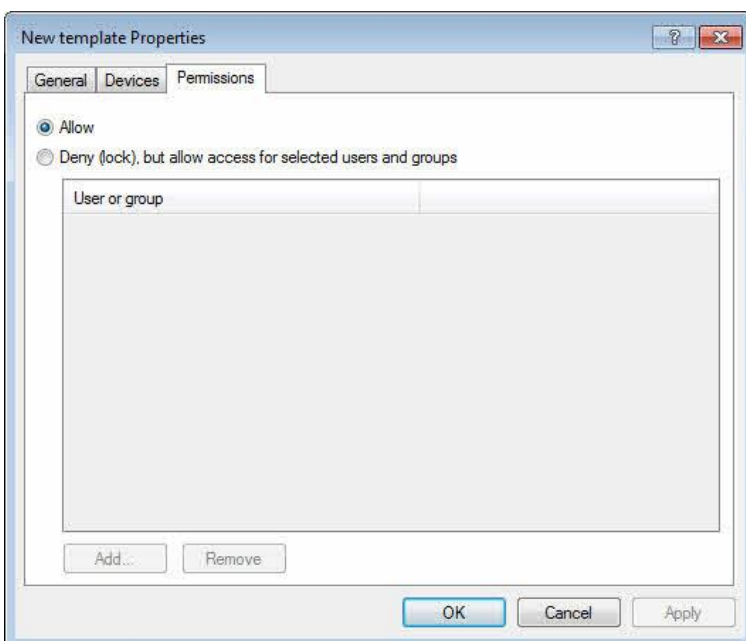
To save device data in the hardware database, click **To hardware database** and then select a manufacturer from the list. The data will be associated with that manufacturer in the database.

Click **OK** to proceed.

To export the current device list to an .INI-file, select **To file** and select a file name.

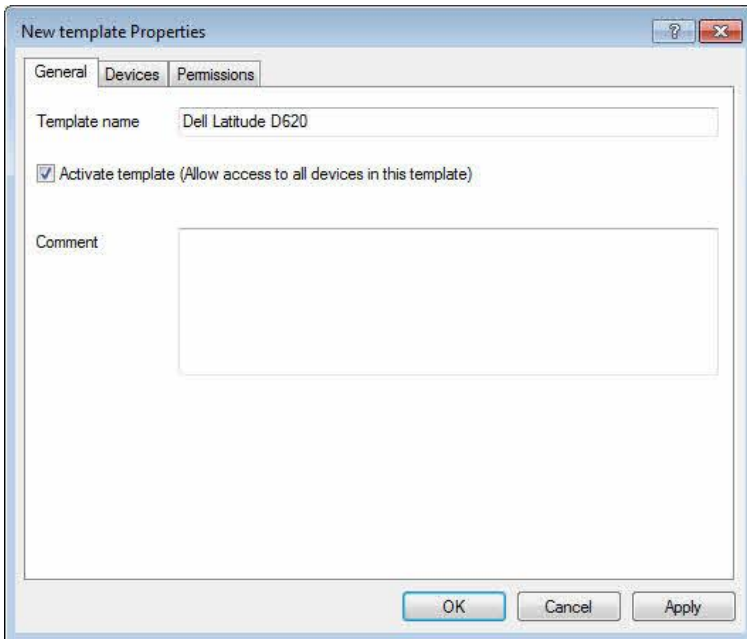
9.2.4.2.4 Defining Computer Template Permissions

By default a template allows access to all the devices in it for all users. To change this, click the Permissions tab of the template.



Check **“Deny (lock), but allow access for defined users and groups”** to allow access to the devices in the template only to specific users. Click **Add** to add users and groups who are allowed to use the devices. Click **Remove** to remove the selected user or group from the list.

9.2.4.2.5 Activating a Computer Template



To enable a computer template, on the General tab, select “**Activate template**” and then click **OK**. Once the template has been activated, DriveLock allows access to all devices in it, according to the template settings you defined.

9.2.4.2.6 Displaying Devices Defined By a Computer Template



This option displays all computer template rules you created along with the whitelist rules for the corresponding device class. To enable the display of template-based rules, right-click **Device** and then click **Show template rules**. Template rules are identified by an icon with a yellow cogwheel.

You can't edit whitelist rules created by a template directly. Instead, to modify or delete such a rule, edit the corresponding template.



Part X

Configuring Network Profiles



10 Configuring Network Profiles

DriveLock allows you to configure setting and rules for computers based on the network the computer is connected to. This functionality is especially useful for laptop computers and other mobile computers because they often connect to various in multiple locations, such as an office, at home or at a customer's site.

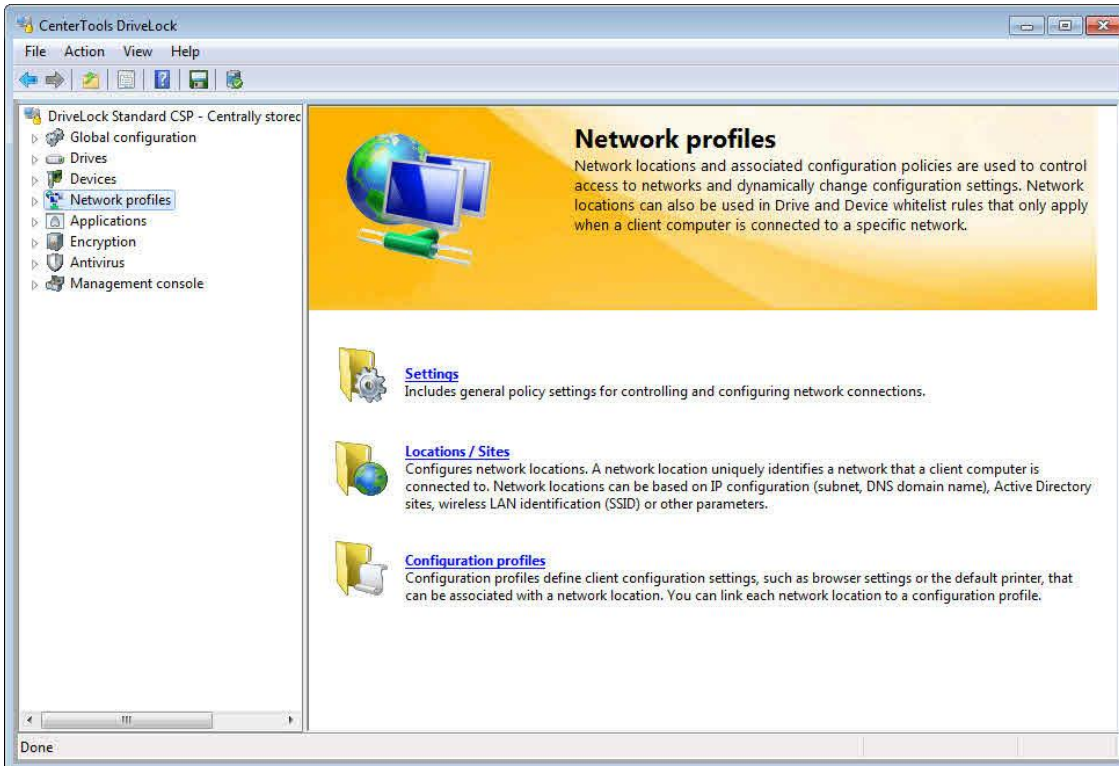
Connections to unmanaged networks create new security threats and risks because you don't control these networks. While you can enforce that all employees must use your internet gateway to access the Internet while the computer is connected to your company's network, you can't maintain this control when a sales engineer connects his laptop to his private network at home. When a corporate computer is connected to an unmanaged network you can't rely on the security components, such as firewalls and antivirus software being in place. As a result, your security policy and standard mobile computer configuration must be restrictive enough to be effective when a computer is connected to either a managed or an unmanaged network. Often these added security measures can make it more difficult to perform business task while a computer is connected to your network.

DriveLock lets you define whitelist rules that are applied depending on the network a computer is connected to. For example, you can block a network adapter whenever a computer attempts to connect to a network other your corporate network (although this particular policy may be overly restrictive in most environments). You can also use DriveLock to automatically configure some common computer settings based on the current network to make it easier for users to roam between networks. These settings include the Internet Explorer network configuration, Windows Messenger settings and the default printer. DriveLock can also initiate a Group Policy update whenever it detects that the network has changed.

You can use network profiles in conjunction with DriveLock Application Control. This lets you allow or deny programs depending on the current network environment. For example, you can prevent users from using Skype or Microsoft Messenger while at work, but allow them to use these programs at home or while traveling.

Network profiles can also be used for configuring antivirus scan engine settings. For example, you can set scanning heuristics to a higher level when client computers are connected to unknown networks to scan more aggressively for malware.

You define network locations and configuration policies by using the DriveLock Management Console or the Group Policy Object Editor.

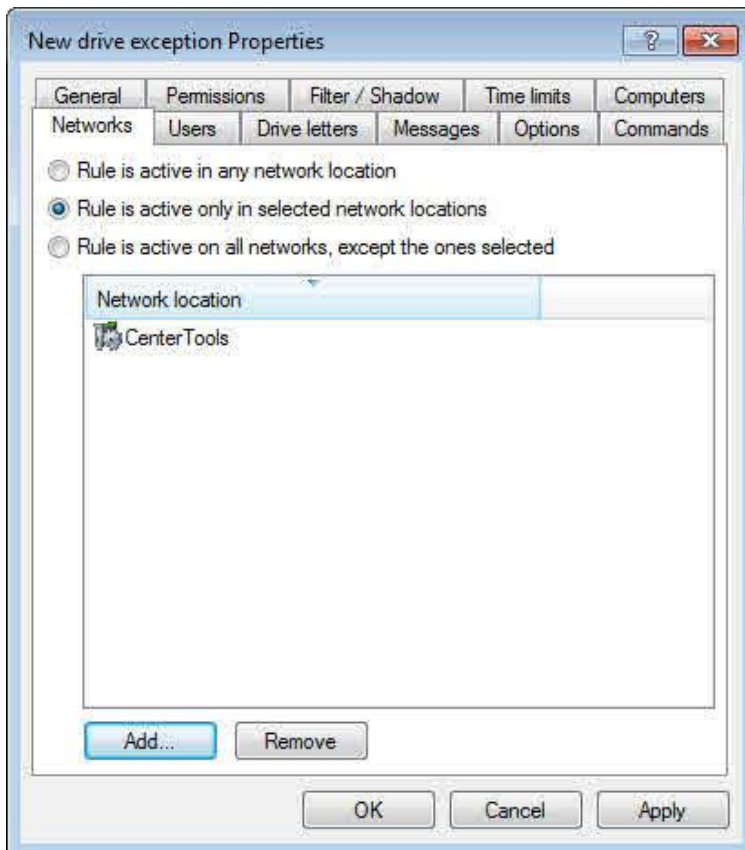


This section covers how DriveLock identifies networks and how to use network locations to define policies.

When a network cable is disconnected during sleep or hibernation mode and the computer doesn't connect to a network after resuming, DriveLock does not connect that the computer is offline until you restart the computer.

Once you have configured network locations, you can use them in whitelist rules, including drive rules, device rules and Application Launch Filter rules.

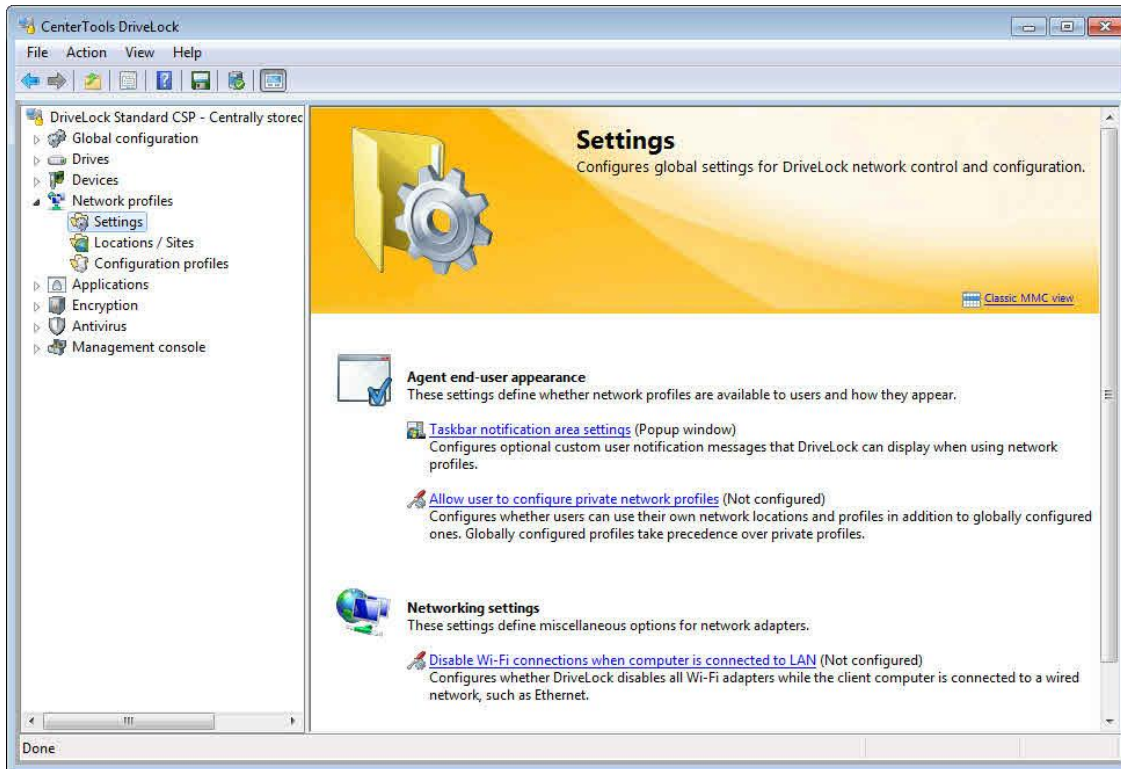
When configuring whitelist rules, click the “**Networks**” tab and select one of the options.



“Rule is activated at any network location” is the default selection when you create a new whitelist rule.

If you change the default settings, add at least one existing network location. To add a network location, click **Add**, select one or more locations, and then select whether the rule is active in these locations.

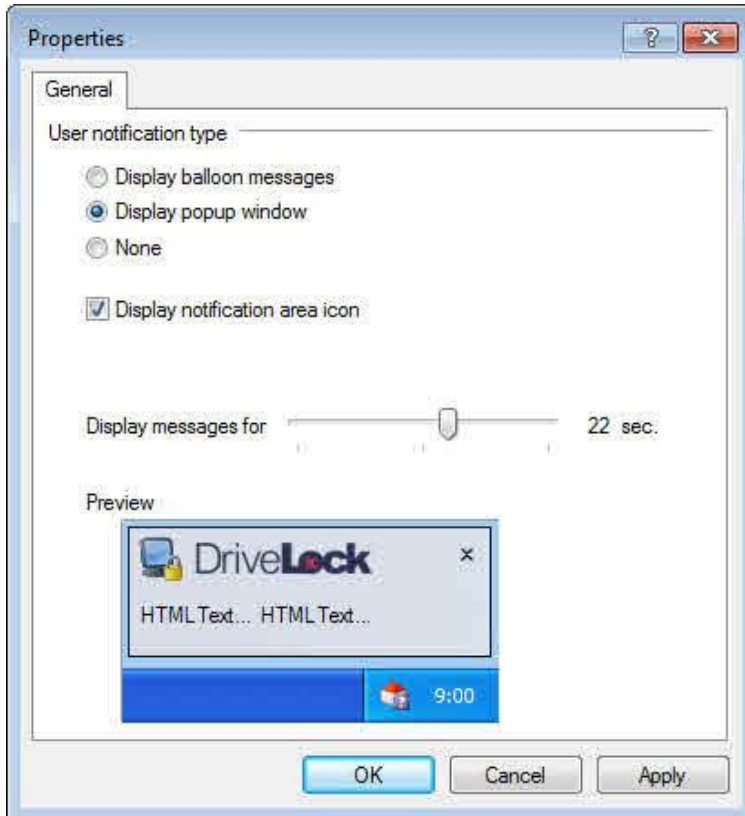
10.1 Configuring Global Network Profiles Settings



There are three global network profile settings that are not specific to any particular network profile and will work for all of the configured locations. Two of these settings define how network profiles appear to users and the third specifies whether Wi-Fi connections are allowed while a computer is connected to a wired network. You can find more information about private network profiles in the section [“Defining User-Specific Network Profiles”](#).

10.1.1 Defining Network Profile End-User Appearance

Select **Taskbar notification area setting** to configure whether users are alerted to network connection changes and how these notifications are displayed.



To hide network profiles completely, deselect **Show notification area icon**. When this option is selected, icons defined in network profiles are displayed as tray icons in the taskbar. You can also select whether the icon is also displayed or only when a message is displayed.

Use the slider to select for how long messages are displayed.

10.1.2 Disabling Simultaneous Wi-Fi and LAN Connections

DriveLock can disable a wireless network adapter while the computer is connected to a wired LAN to prevent the bridging of networks, which can endanger the security of your company's network.

To prevent bridging between wired and wireless networks, select **Disable Wi-Fi connections when computer is connected to a LAN** and then select **Enable**.

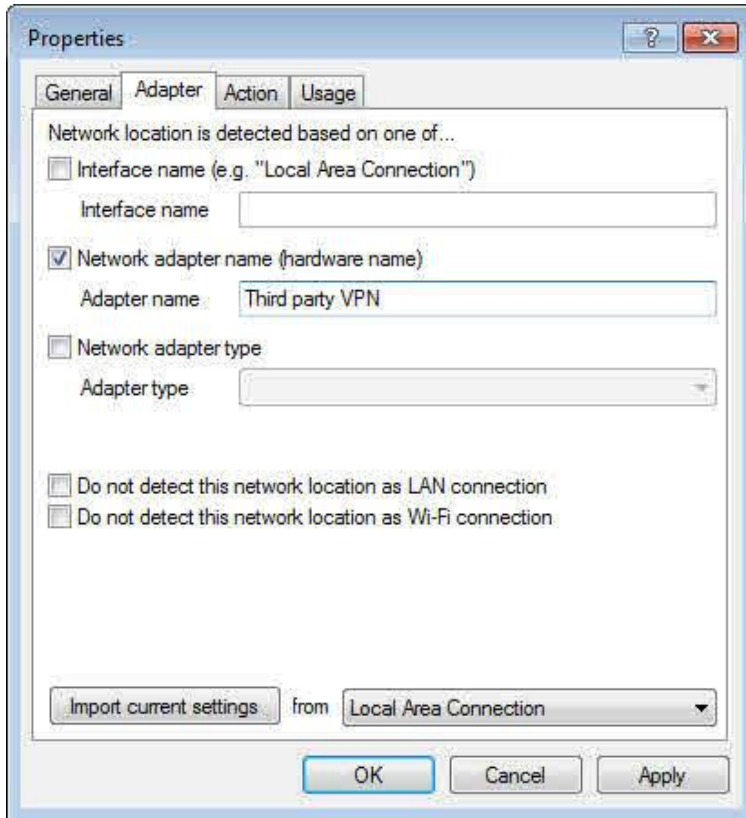


10.1.2.1 Using Third-Party VPN Clients

When you select the option to disable Wi-Fi connections while connected to a LAN and you use a third-party VPN client (i.e. not the VPN client built into Windows) to connect to a corporate LAN, an additional configuration step is required.

Many third-party VPN clients appear in Windows as a virtual network adapter and are indistinguishable to DriveLock from wired network connections. When a user connects to the corporate network using such a VPN client, DriveLock detects that a LAN connection exists and disables the Wi-Fi connection if your configuration prohibits simultaneous connections. If the VPN connection was established over a Wi-Fi network, the VPN connection will fail. To prevent this from happening you need to create an exception for the VPN client's virtual network adapter.

To do this, right-click *Network profiles* -> *Locations / Sites*, point to *New* and then click *Network adapter*.



In the *Properties* dialog box, on the *Adapter* tab, configure the following settings:

Select a method to uniquely and reliably identify the VPN client's virtual network adapter. If the virtual network adapter is installed on the local computer, you can import its current settings. Otherwise, you need to select one or more of the following checkboxes and define the associated settings:

- *Interface name*: Name of the network connection. This is not very reliable as network interfaces can be renamed.
- *Network adapter name*: Name of the network adapter. This name generally doesn't change.
- *Adapter type*: Type of the virtual network adapter. The type varies based on the VPN client's vendor.

To ensure that DriveLock correctly identifies the adapter, select one or both of the following checkboxes:

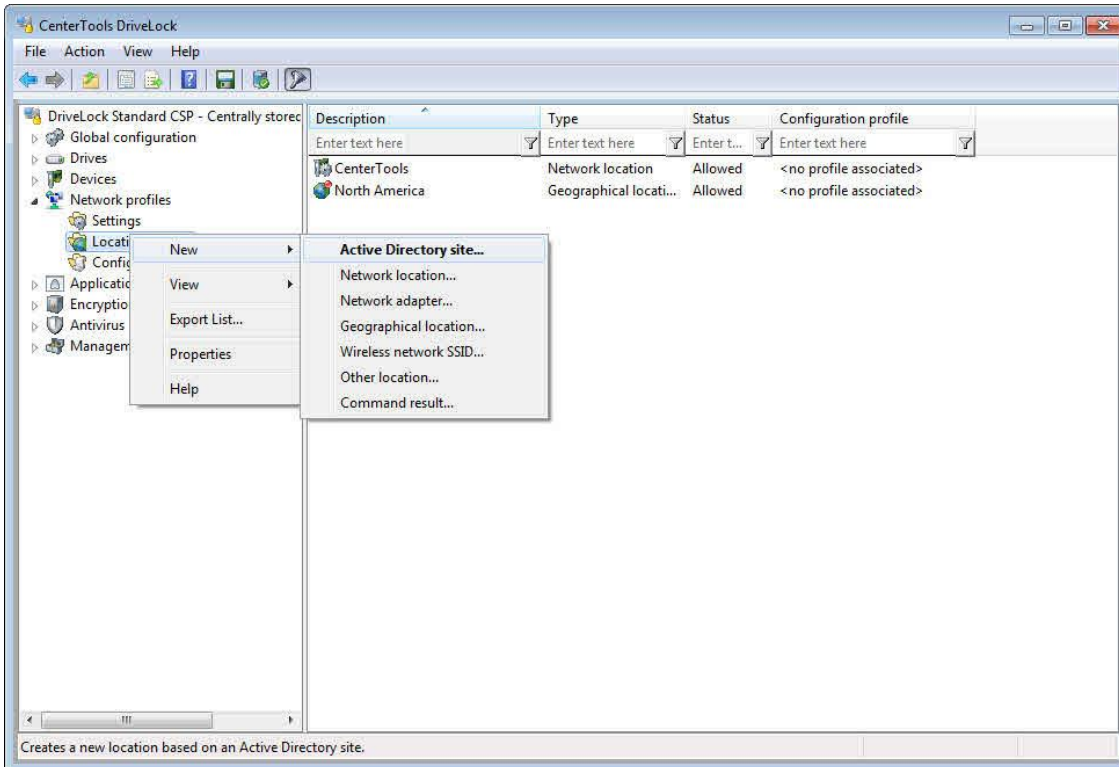
- *Do not detect this network location as LAN connection*: DriveLock does not identify the connection as a LAN connection and any rules that apply to LAN connections are not applied.
- *Do not detect this network location as Wi-Fi connection*: DriveLock does not identify the connection as a Wi-Fi connection and any rules that apply to Wi-Fi connections are not applied.

10.2 Defining Network Locations

To configure settings and assign whitelist rules based on a network connection, you must define how DriveLock identifies networks. You can define the following types of locations:

- Active Directory site
- Network location (based on IP address information)
- Network adapter
- Geographic location

- Wireless network SSID
- Special location
- Command result

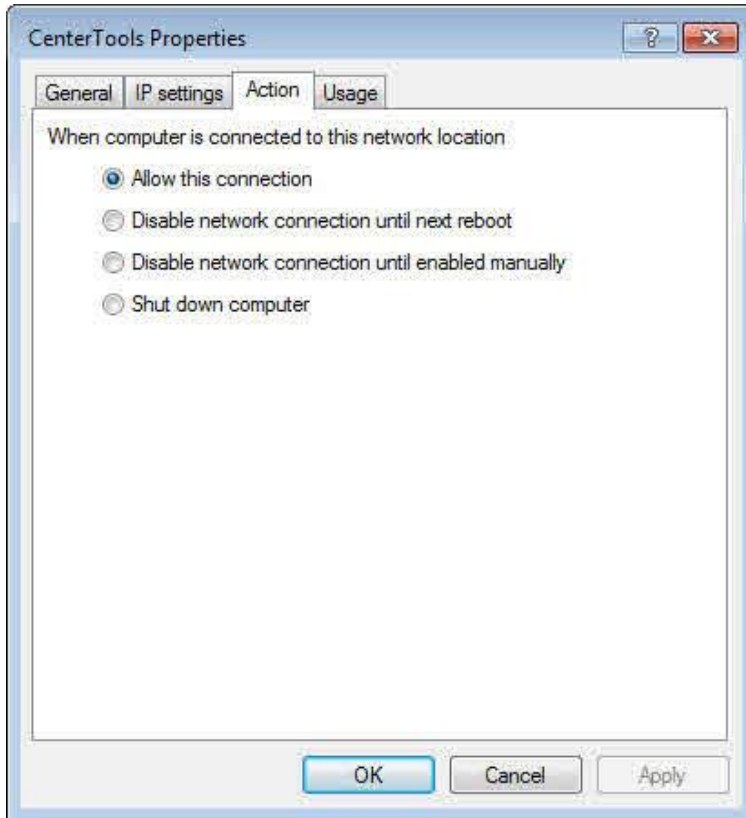


To define a network location, right-click **Location/Sites**, point to **New**, and then click the type of network to define. For each type you must select an associated configuration profile from the dropdown list.

If you have not created any configuration profiles yet, don't select a profile at this time. Instead, finish creating locations and then specify profiles later by double-clicking each network location to open the configuration dialog box and selecting the appropriate profile.

You can also select an icon to be displayed in the computer's system tray when the computer is connected to the network you are defining.

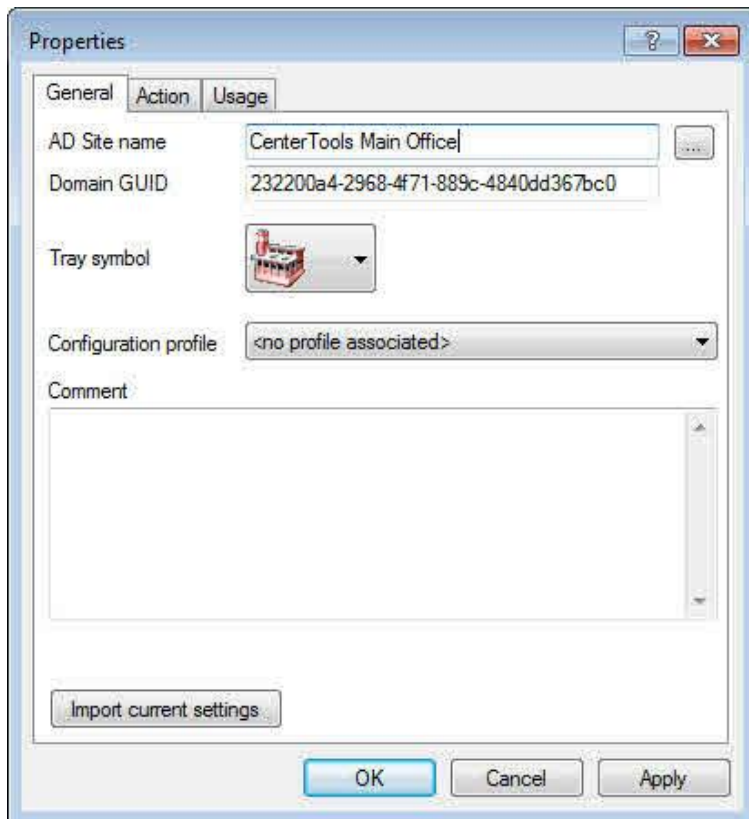
When you configure a network location you must specify what the DriveLock Agent will do when the computer is connected to the location. Select one of the actions on the **"Action"** tab:



Use caution when configuring Agents to disable network connections. If you inadvertently configure DriveLock to block network connection until manual intervention, you must manually undo this configuration on each computer because remote control connections to that computer are no longer possible.

10.2.1 Active Directory Site

When you select an Active Directory site, the location is determined by using the name of site that the computer is currently connected to.

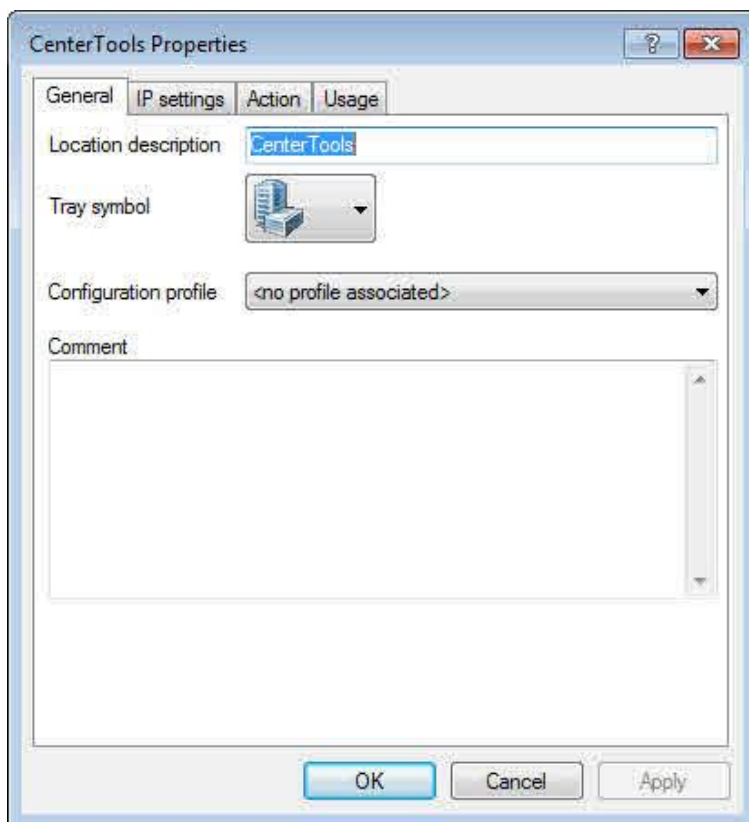


Import the current settings by clicking **Import current settings**. DriveLock uses the current site information from Active Directory and automatically completes fields **AD Site name** and **Domain GUID**. To specify a different site, type the name of that site, or click "...", to select the appropriate site from Active Directory.

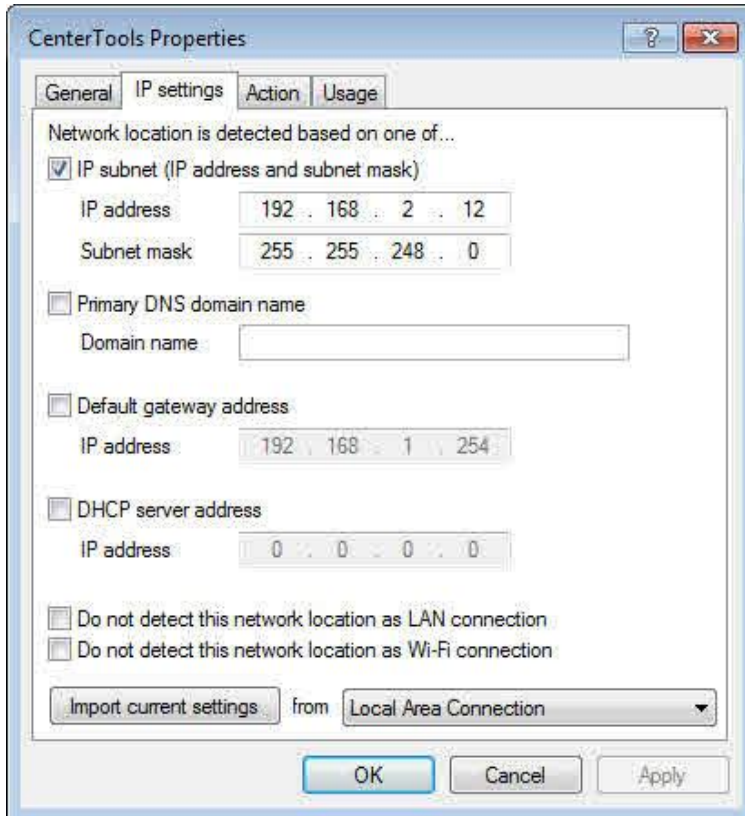
Select an icon to display in the system tray when the connection is detected by the DriveLock Agent.

10.2.2 Network Location Based on IP Information

To define a network location based on an IP address range, click **Network location** on the context menu.



Type the name of the location and select a symbol to be used for the taskbar icon. On the “**IP settings**” tab, configure the location by providing its IP information.



You can import the network setting from one of the current network connections or type the information. Select one or more address criteria, such as the IP address range, the name of the primary DNS domain, the default gateway address or the DHCP server address.

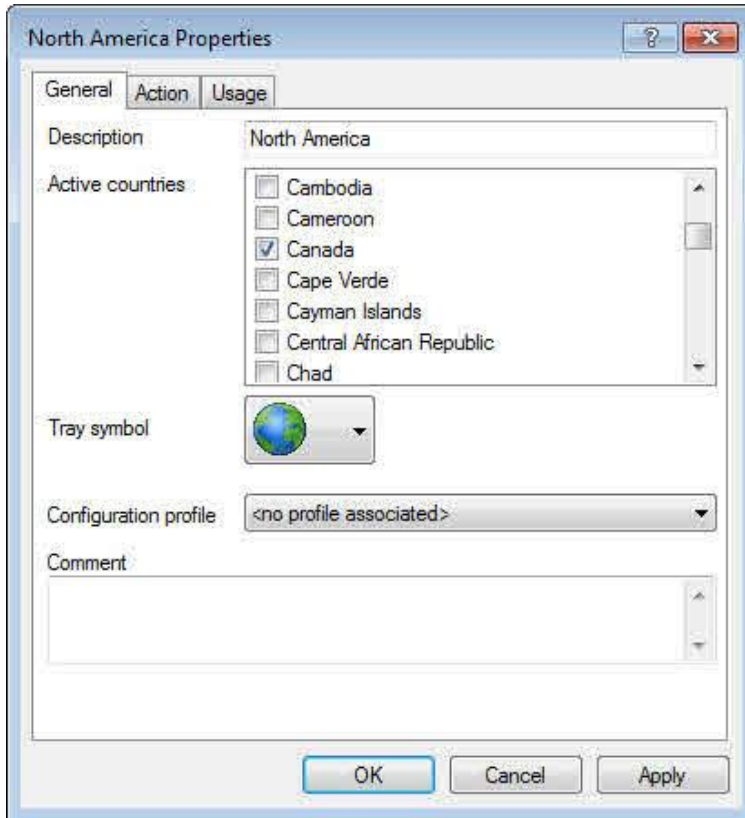
10.2.3 Network Adapters

Network locations based on the network adapter are normally used to identify third-party VPN client connections. For more information about defining such network locations, refer to the section "[Using Third-Party VPN Clients](#)".

10.2.4 Geographic Locations

You can create network locations that are based on a computer's external IP address. When you define such a location, DriveLock attempts to detect the computer's public IP address, compares the result to its local GEO-IP database, and then assigns the computer to the country that the address is registered in.

To identify a client computer based on the country where it is located, right-click *Extended configuration* -> *Network profiles* -> *Locations / Sites*, point to *New* and then click *Geographical location*.



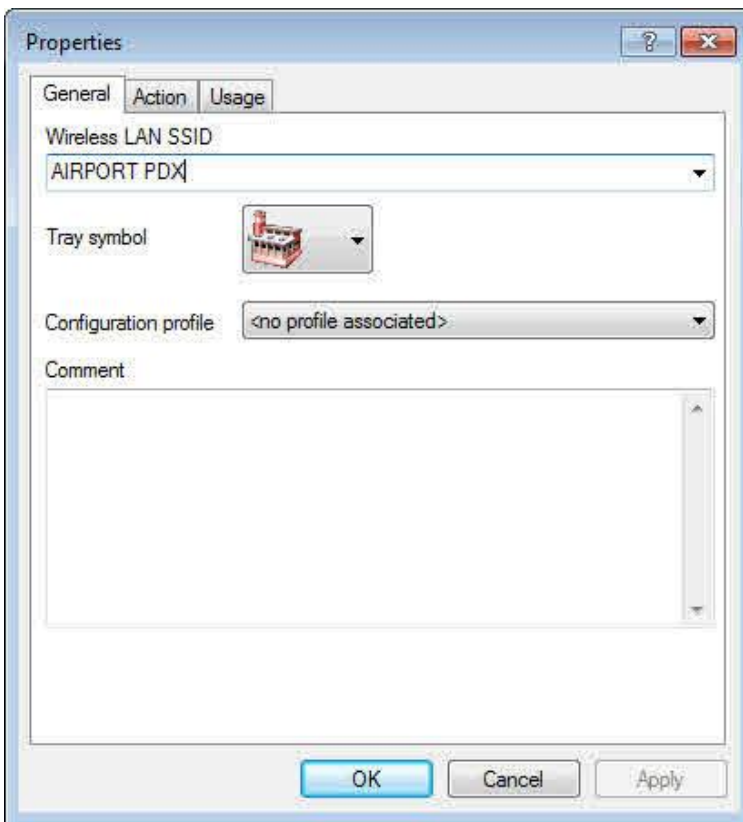
Type a description of the location and then select one or more countries. Once you have configured a geographic location, you can use it like any other network location in DriveLock rules or to prevent network connections while a computer is in the location you defined.

For example, to ensure that notebook computers can only communicate over a network while they are traveling inside the United States or Canada, create a network location that contains these two countries and, on the *Action* tab, select *Allow this connection*. Then create another rule for the *Other location* “No defined network location is active” and, on the *Action* tab, select *Disable network connection until next reboot*.

To detect the network location based on a computer’s public IP address, DriveLock needs to have an active Internet connection.

10.2.5 Wireless Network SSID

If your network can be determined by using a Wireless-LAN SSID, click **Wireless network SSID** on the context menu.



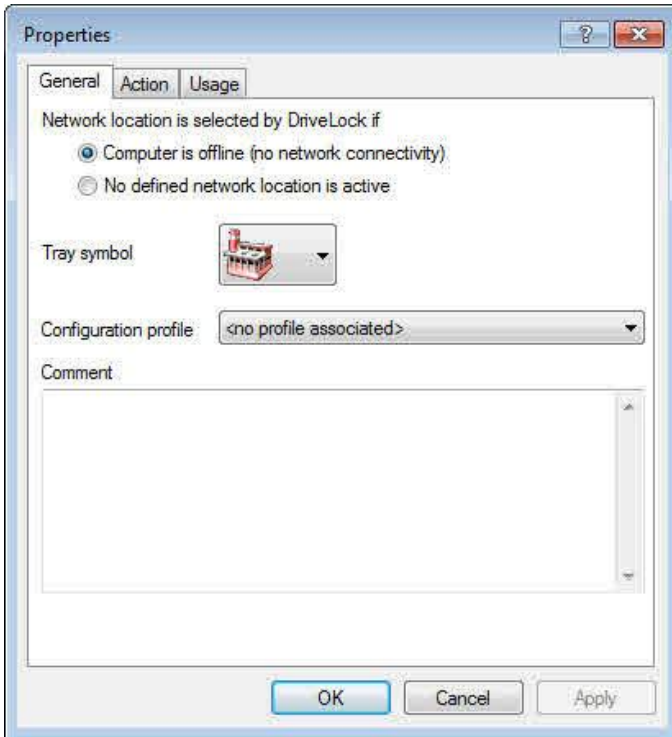
Type the SSID name as shown above.

10.2.6 Other Locations

Use “other location” in the following scenarios:

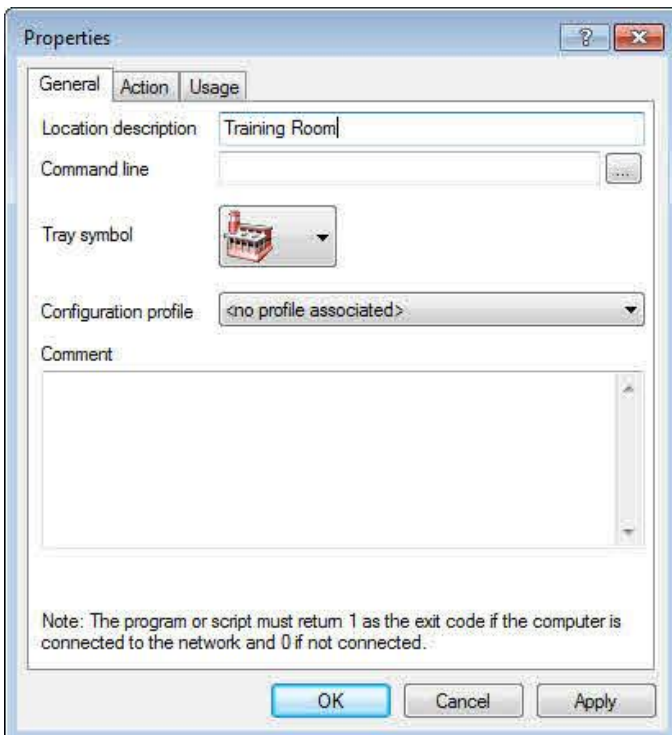
- To define settings that apply when the computer is offline and not connected to any network
- To define settings that apply the computer is connected to an unknown network

You can select an icon for this connection from the dropdown list.



10.2.7 Command Result

In some situations network detection that is based on Active Directory information or an IP address range may not be accurate or dependable enough to meet your security requirements. In such cases you can create a custom script or program to determine the network. Such a script or program must return the environment value “1” if the network is detected. For example, a script could check whether certain servers or services are available, or it could examine the computer’s security configuration before allowing it to connect to your company’s network.



A command can be any program that can run from a command line, including program files, (.exe), Visual Basic scripts (.vbs) and scripts for the new Windows PowerShell.

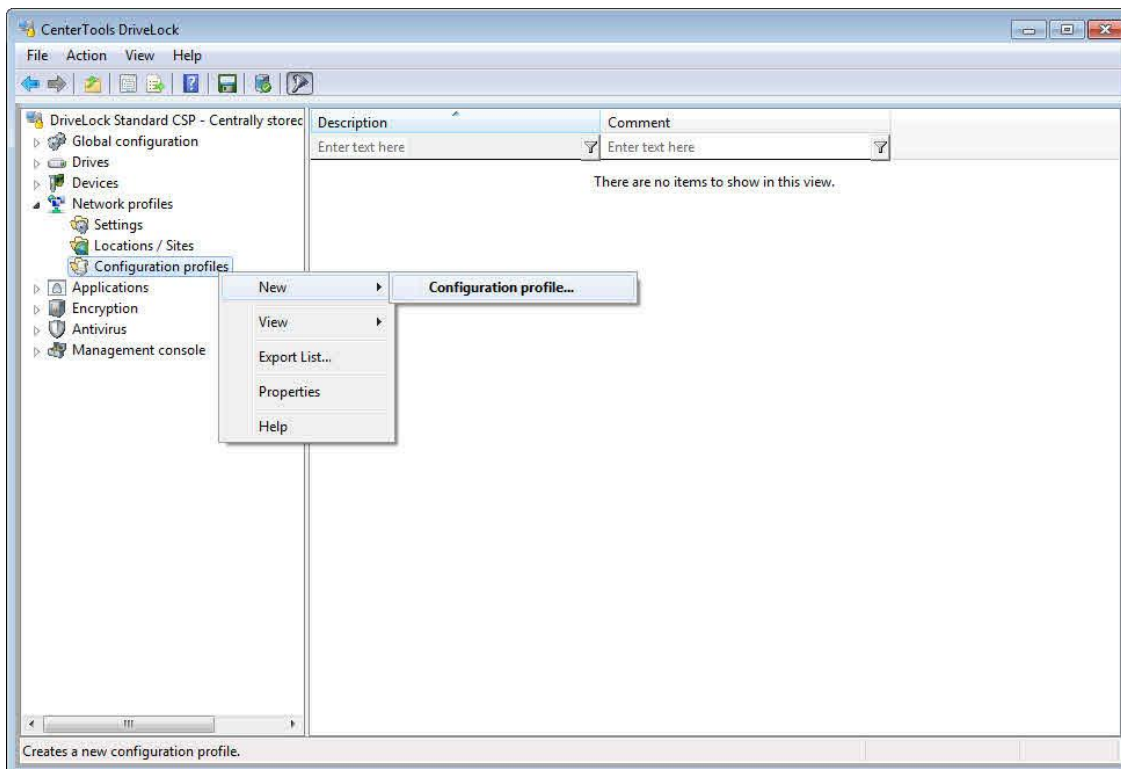
To start a VB script you must enter the complete path to the script file (“*cscript c:\programming\scripts\myscript.vbs*”).

10.3 Creating Configuration Profiles

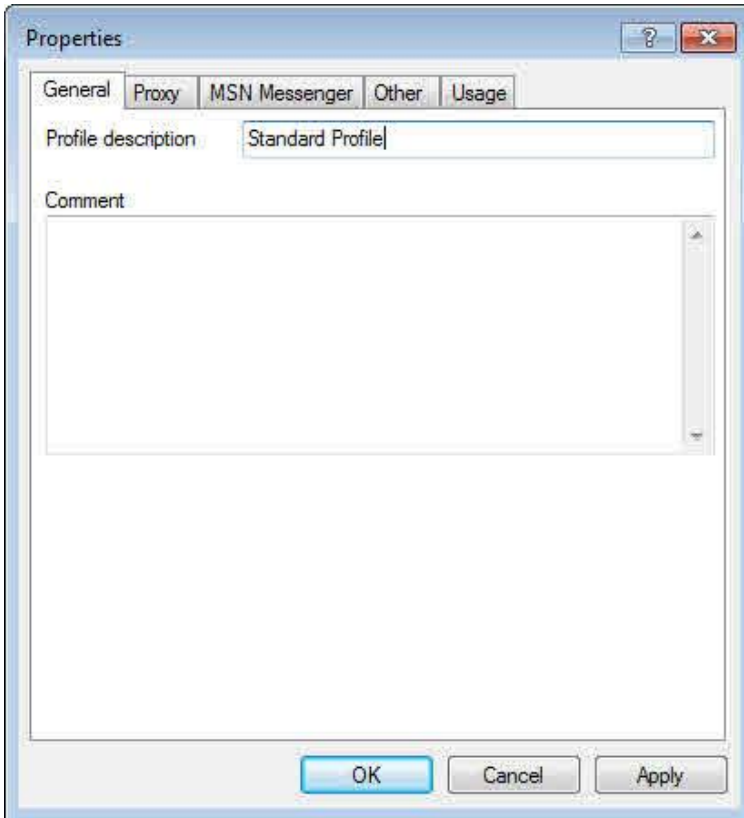
DriveLock can use a network configuration policy in conjunction with a network location to change certain computer settings automatically after identifying a network. Such a policy defines how the following types of settings are configured:

- Internet Explorer LAN settings
- Windows Live Messenger / MSN Messenger settings
- Default printer

DriveLock can also refresh the Group Policy for the computer and the user when it detects a network location change, execute a program or run a script.



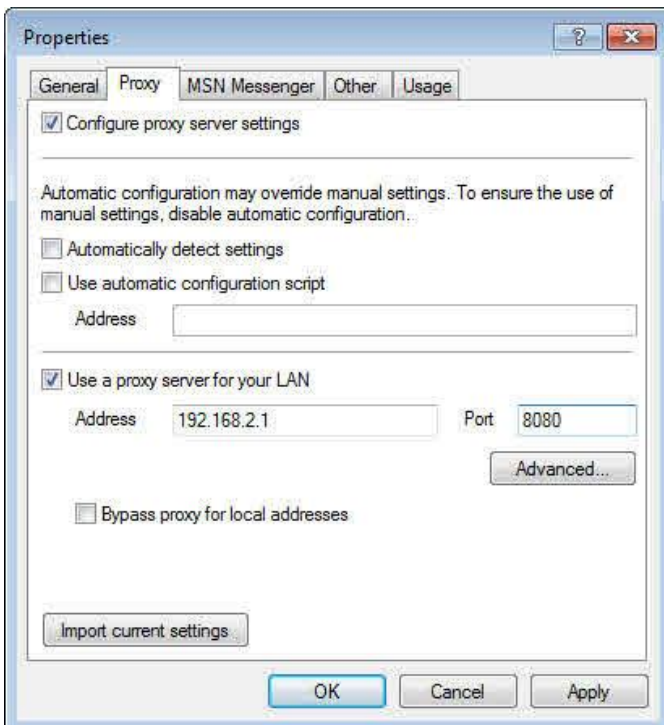
Right-click **Configuration profiles** and then click **New -> Configuration profile**.



In the **Profile description** field, type a name for the profile and type an optional descriptive comment.

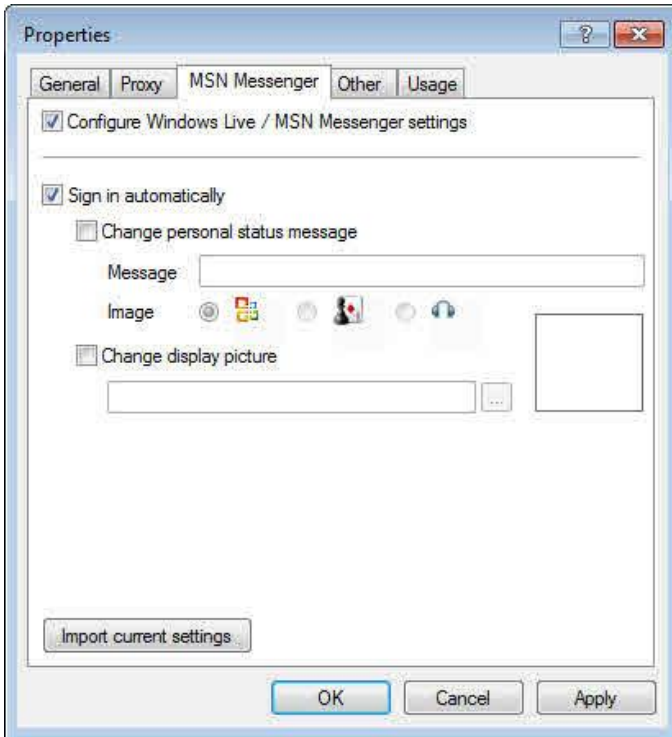
10.3.1 Internet Explorer Proxy Settings

In the network profile settings dialog box, click the **Proxy** tab.



To configure proxy server settings for Internet Explorer, select the **“Adjust proxy settings”** checkbox, and then import the current settings from Internet Explorer or enter other settings. (See the Internet Explorer documentation for more information about how to configure Internet Explorer proxy settings.)

10.3.2 Windows Live Messenger / MSN Messenger Settings



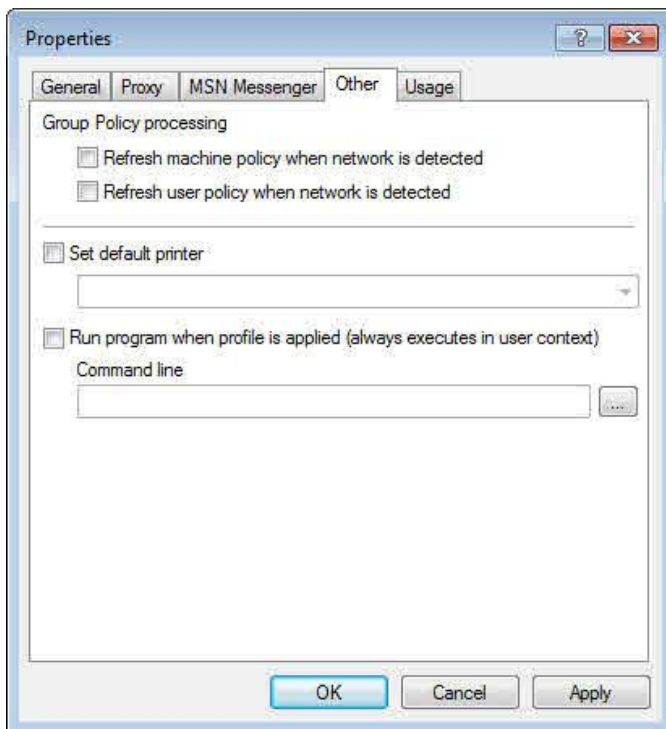
Click the **MSN Messenger** tab and then select the **“Adjust MSN Messenger settings”** checkbox to enable automatic configuration of Messenger settings, and then select the appropriate settings, or import the setting from your local Messenger configuration.

Type a status message and select an image to be displayed to your Messenger contacts. To change the display picture, select **Change display picture** and then click “...” to the right of the field to select an image file.

(Refer to the Windows Live Messenger and MSN Messenger documentation for more information about how to configure these programs.)

10.3.3 Default Printer and Group Policy Processing

To change the default printer, click the “Other” tab and then select the **Change default printer checkbox**.



Select a printer from the dropdown list.

To refresh the Active Directory Group Policy for the compute or user after a connection to the network has been detected, select the corresponding checkboxes.

DriveLock can run a command each time it detects a new network connection. A command can be any program that you can run from a command line, including program files, (.exe), Visual Basic scripts (.vbs) and scripts for the new Windows PowerShell.

To start a VB script, you must type the complete path to the script file (for example, “*cscript C:\Program Files\scripts\myscript.vbs*”).

Click the “...” button to select a file name and to insert it at the current cursor position. You can select a file name from two locations:

- The file system on the local computer
- The DriveLock Policy file storage.

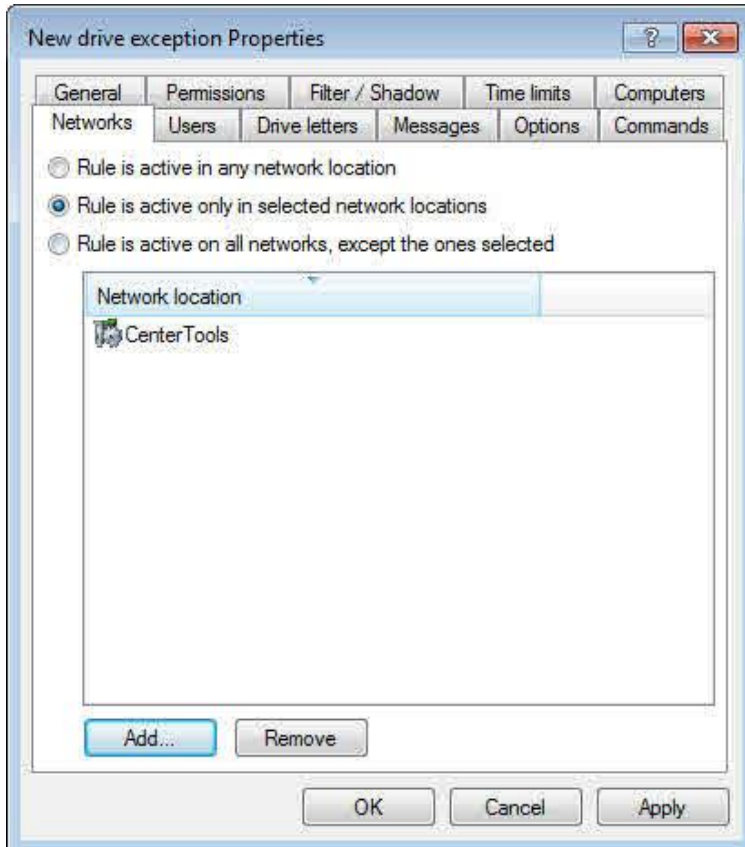
The DriveLock policy file storage is a file container stored as part of a Local Policy, Group Policy Object or DriveLock Configuration file. It can contain any file, such as a script that will be deployed to the DriveLock Agents automatically along with the configuration.

Files selected from the Policy file storage are prefixed with an asterisk (*).

10.4 Using Network Locations in Whitelist Rules

Once you have configured network locations, you can use them in whitelist rules, including rules that control the use of drives, devices or applications.

To use a network location in a whitelist rule, on the rule’s *Network* tab, select one of the following options:



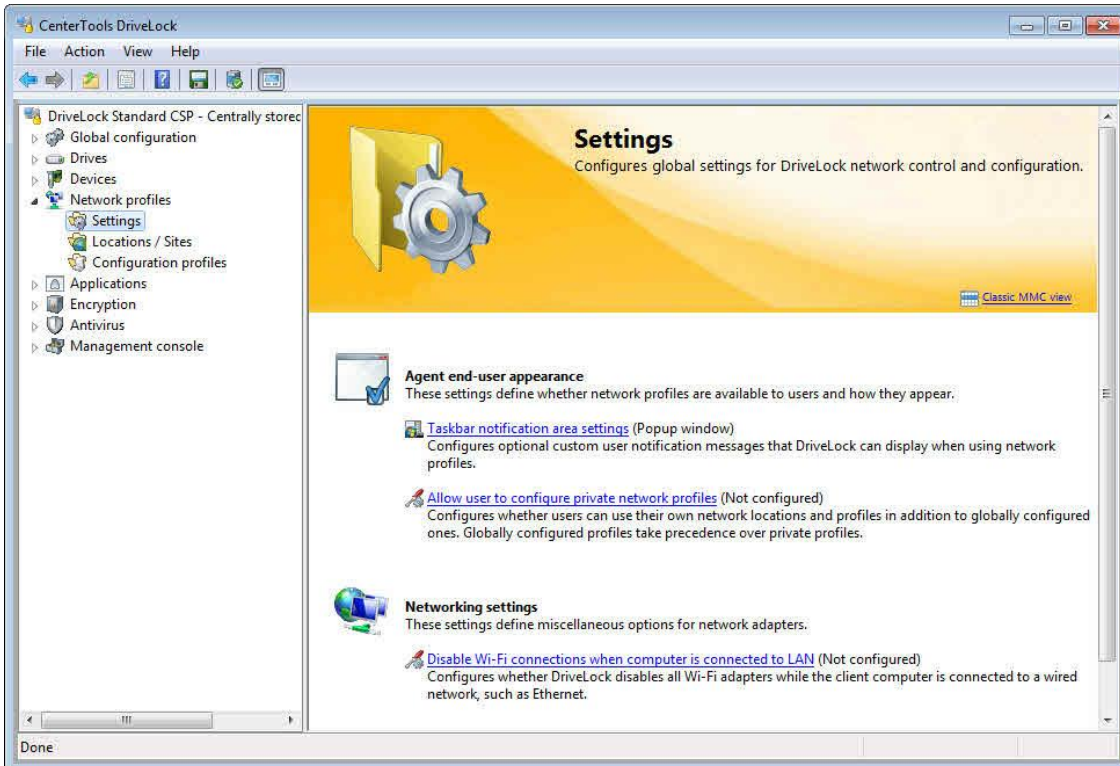
- Rule is active in any network connections
- Rule is active only in selected network connections
- Rule is active on all networks, except the ones selected

Rule applies to all network connections is the default setting for all new whitelist rules.

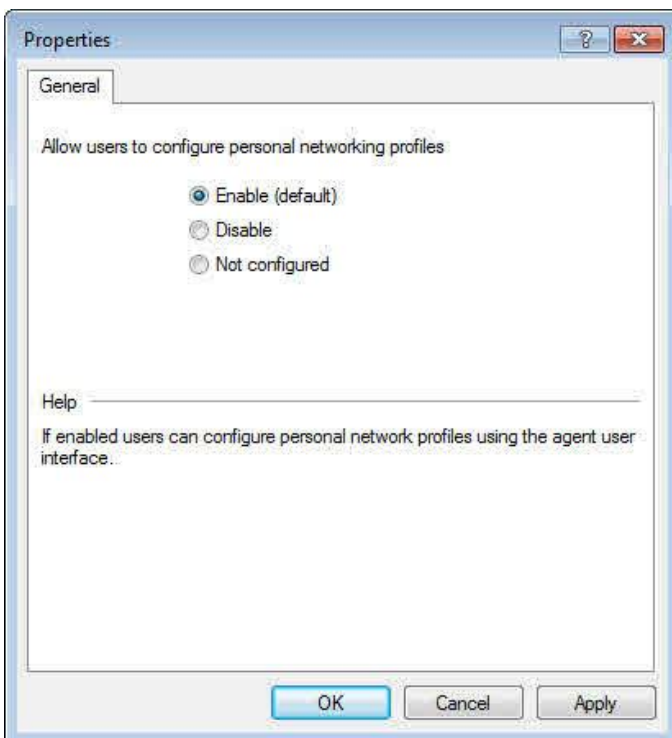
If you change the default network setting for a whitelist rule, ensure that you add at least one network connection. Use the **Add** and **Remove** buttons to edit the network list.

10.5 Defining User-Specific Network Profiles

Administrators can use network locations and configuration profiles to enforce company policies on mobile computers. Some of the settings enforced by the DriveLock Agent are not designed for security but automate the configuration of network settings for users. If you want to enable users to select these configuration settings themselves, you can allow them to specify their own private network profiles to automate changes to their configuration settings.



To allow users to define their own user-specific network profiles, on the “**Network profiles**” node, click **Allow user to configure private network profiles**, and then click **Settings**



Select whether or not users can configure their own profiles.

Refer to the *DriveLock User Guide* for information about managing user defined profiles.



Part XI

DriveLock Application Control



11 DriveLock Application Control

This chapter remains in the Administration Guide until further notice, but it will not be updated. Please note that the current documentation on application control can be found in a separate manual available at [DriveLock Online Help](#) starting with version 2020.1.

Use DriveLock Application Control to limit or allow the use of applications on your company computers.

Please note that application control is not automatically part of the standard DriveLock functionality. If you do not have a license for it, this node will not appear in your DriveLock Management Console.

DriveLock has two different scopes of application control functionality:

1. With the help of blacklists or whitelists you can set up simple rules that define *which* applications can be executed and *which* are blocked. For more details, please refer to [Basic DriveLock application control](#) and [Extended DriveLock application control](#).
2. By using [application permissions](#), you can configure, *what* the applications are allowed to do. For example, you can define which permissions the applications have, which directories they write to, or which processes they are allowed to start. You can also group different application permissions.

Depending on the licenses you have purchased, some application control functionality may not be available to you, for example Predictive Whitelisting or application permissions require separate licenses.

11.1 Standard Application Control

This chapter remains in the Administration Guide until further notice, but it will not be updated. Please note that the current documentation on application control can be found in a separate manual available at [DriveLock Online Help](#) starting with version 2020.1.

This section contains information about how to configure and use DriveLock Application Control. This document describes the criteria used by the Agent to determine whether an application is allowed to start and how to configure application policies.

Application Control is an optional component.

You need a license for the DriveLock application control, which activates all functions of our established application control plus the advanced intelligent functions of predictive whitelisting.

Application Control lets administrators control which applications can run on a computer that has the DriveLock Agent installed. You can use several types of rules and strategies to specify which application are allowed and which are blocked by the Application Control.

You can use the following types of application rules to specify an application:

- Hash database rule
- Publisher certificate rule
- File owner rule
- MD5 hash rule
- Special rule

File path rules and template rules are additional types that can be useful in certain situations. They are primarily included for backward compatibility with older versions of DriveLock.

Using application hash databases is the easiest method for defining a collection of applications. Configure **hash database rules** to quickly create one or more collections of applications that users are allowed to run or that are blocked. DriveLock can automatically create a hash database by scanning all applications in directories that you specify. For example, you can create a hash database whitelist rule by automatically scanning the complete hard disk of a reference client computer that has all your business applications installed. When you apply this whitelist rule to other computers in your organization, users can start all applications installed on the reference client while any other application is blocked by DriveLock.

A more flexible approach, which provides more flexibility in an environment with frequent changes and updates, is to use **publisher certificate rules**. Software publisher certificates can be used to determine which company published an application. For example, all software products developed by Microsoft are signed with a certificate issued by Microsoft Code Signing PCA. DriveLock products are signed with a certificate issued by VeriSign. A publisher certificate rule can be used to verify the authenticity of a program file and then allow users to run applications based on certain properties, such as the software publisher or the program version. For example, you can allow all applications that were signed by Microsoft, any application signed with a certificate that was issued by VeriSign, or a single application with a specific certificate ID. You can use wildcards in publisher certificate rules for maximum flexibility.

Whitelist rules can also be based on file ownership. In Microsoft Windows every file has a file owner. For example, when an administrator installs a new application, Windows assigns ownership of all files that are part of this application to the administrator's user account or the local Administrators group. You can create a **file owner rule** to allow users to start any application that was installed by an administrator. If you deploy client software using a service account with administrative rights, you can create whitelist rules based on this account.

An **MD5 hash rule** is based on a calculated value that uniquely identifies a file. This type of rule is most appropriate for a whitelist rule or blacklist rule that covers a single application.

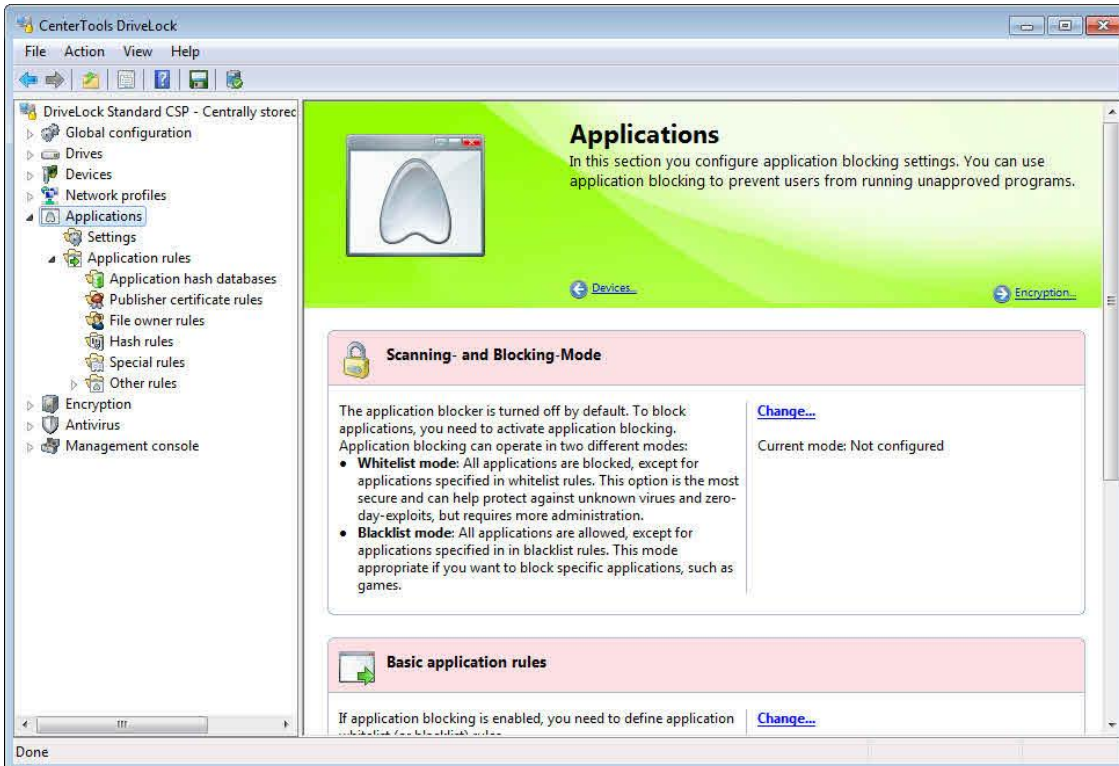
Special rules let you easily refer to all program files on a computer that match certain common criteria, for example whether the file is part of the Microsoft operating system, is part of DriveLock or is a .NET application. You can also use a special rule to override a blacklist rule and allow some users, such as a service administrator, to run all applications.

The flexibility of combining blacklist rules with whitelist rules makes the Application Control both easy to configure and powerful enough to secure your client environment.

11.1.1 Basic configuration

This chapter remains in the Administration Guide until further notice, but it will not be updated. Please note that the current documentation on application control can be found in a separate manual available at [DriveLock Online Help](#) starting with version 2020.1.

The Basic Configuration mode of the DriveLock Management Console lets you configure the most common settings for Application Control. To access advanced configuration settings, navigate to the appropriate subnodes in the console tree.



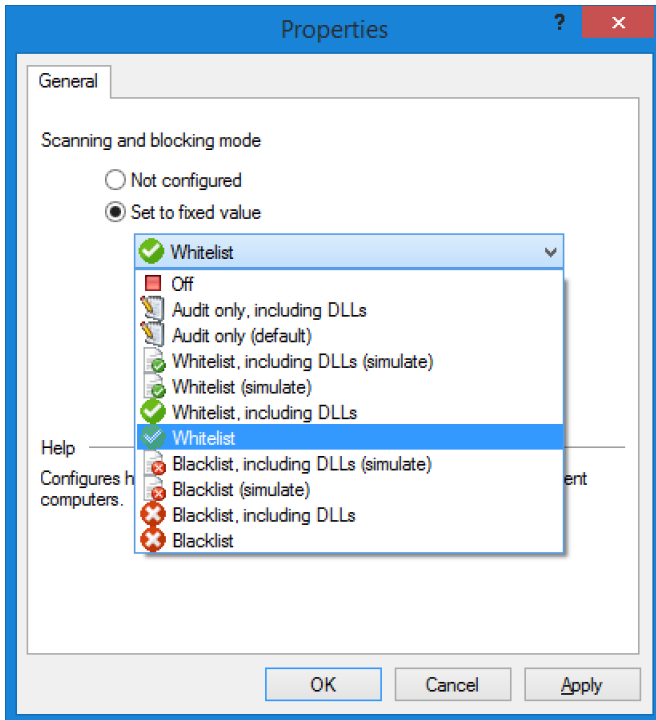
To view the taskpad for the Application Control configuration, in the left pane of the DriveLock Management Console, click **Applications**.

11.1.1.1 Configuring the Scanning and Blocking Mode

This chapter remains in the Administration Guide until further notice, but it will not be updated. Please note that the current documentation on application control can be found in a separate manual available at [DriveLock Online Help](#) starting with version 2020.1.

The scanning and blocking mode determines the overall operations of Application Control. Open **Applications / Settings / Scanning and Blockingmode**. To select one of the operation modes, follow the steps in the following sections. To disable the Application Control, select **Off**.

Scanning/Blocking DLLs is available in DriveLock Versions 7.7.8 and newer versions. Carefully read chapter [Scanning/Blocking DLLs](#), before using an "including DLLs" mode.



11.1.1.1.1 Auditing and simulation

This chapter remains in the Administration Guide until further notice, but it will not be updated. Please note that the current documentation on application control can be found in a separate manual available at [DriveLock Online Help](#) starting with version 2020.1.

To monitor the execution of programs on computers without preventing any of these programs from starting, select **Audit-only**. The DriveLock Agent creates events for all programs that are started on a computer without enforcing any application templates or rules. This mode is most appropriate if you allow user to run any program but you need to record which programs users run.

Use one of the two simulation modes, **Whitelist (simulate)** or **Blacklist (simulate)**, to test templates or rules before actually blocking programs. In simulation mode the DriveLock Agent creates events when an application is started that is controlled by a template or rule, but no programs are blocked.

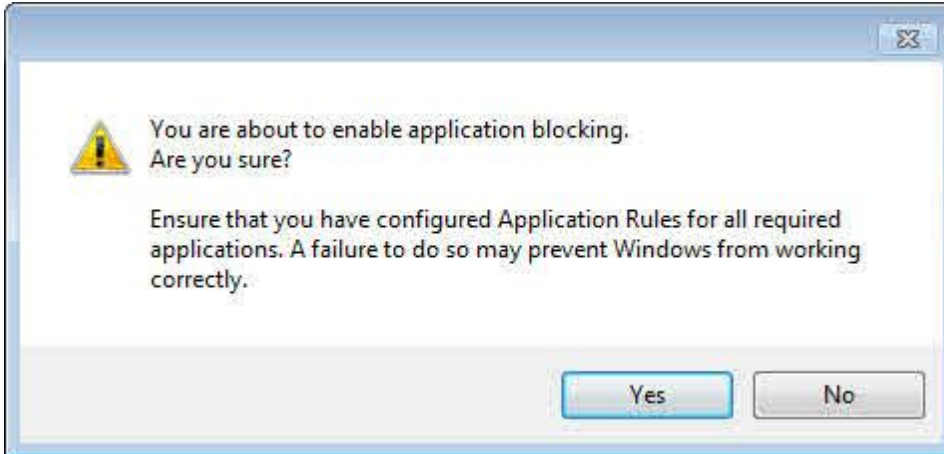
Use the simulation modes to identify applications that users are running before you enforce any blocking rules. Review the local Windows event logs or the DriveLock Control Center for events that indicate that applications were allowed to start or blocked. If the events indicate that application control does not work as intended, modify the rules to correctly enforce the intended settings.

11.1.1.1.2 Whitelist mode and Blacklist mode

This chapter remains in the Administration Guide until further notice, but it will not be updated. Please note that the current documentation on application control can be found in a separate manual available at [DriveLock Online Help](#) starting with version 2020.1.

To activate Application Control, select **Whitelist** or **Blacklist**. In **Whitelist** mode, all applications, except those allowed by your policy, are blocked. In **Blacklist mode**, all applications can be started except for applications that are blocked by the rules and templates you configured.

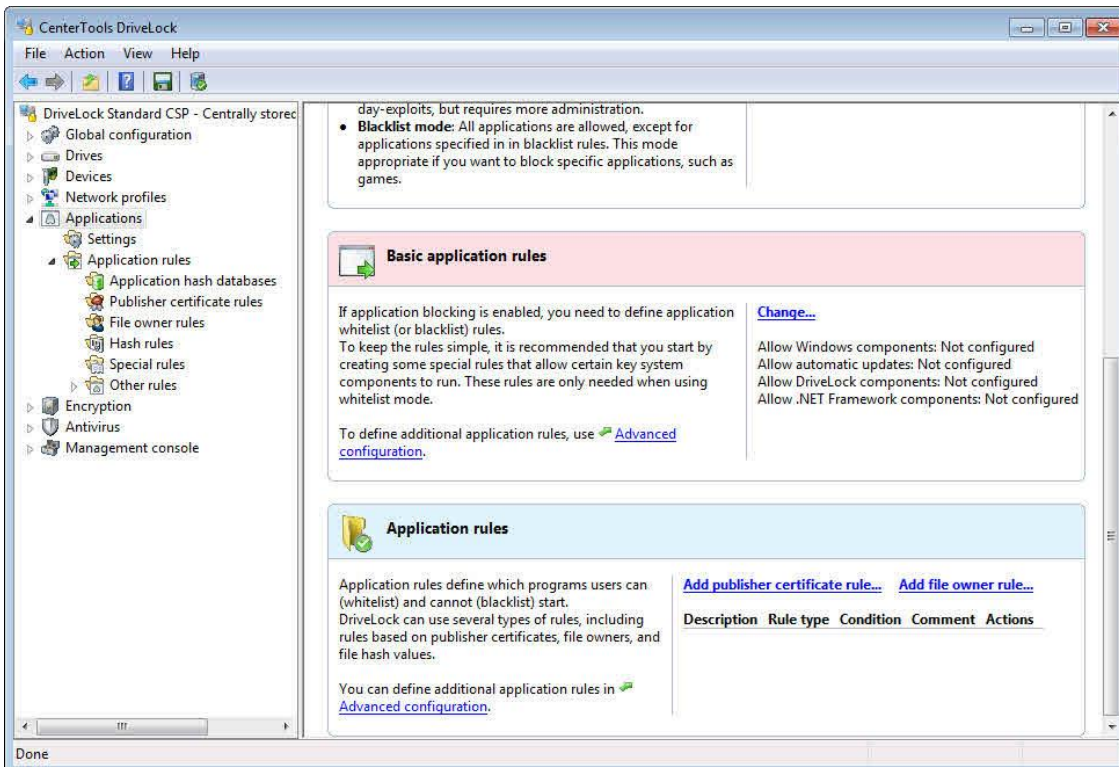
Whitelist and blacklist rules and templates define exceptions to the overall behavior of the blocking mode. You can create both whitelist rules and blacklist rules in either blocking mode. For more information about how rules and templates work in each mode, refer to the sections "[Whitelist mode](#)" and "[Blacklist mode](#)".



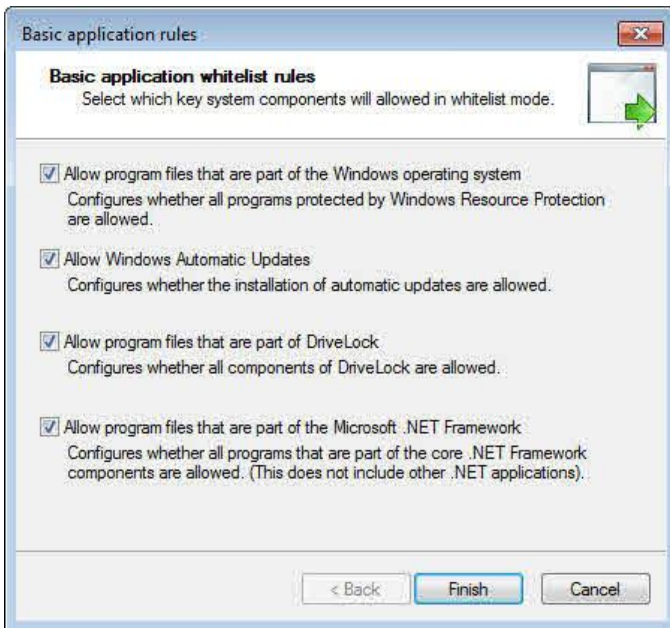
When you select one of the blocking modes, DriveLock displays a warning message. Click **Yes** to activate Application Control or click **No** to cancel the current operation.

11.1.1.2 Configuring basic application rules

This chapter remains in the Administration Guide until further notice, but it will not be updated. Please note that the current documentation on application control can be found in a separate manual available at [DriveLock Online Help](#) starting with version 2020.1.



To change the default application rules created during setup, in the “**Basic application rule**” area, click Change.

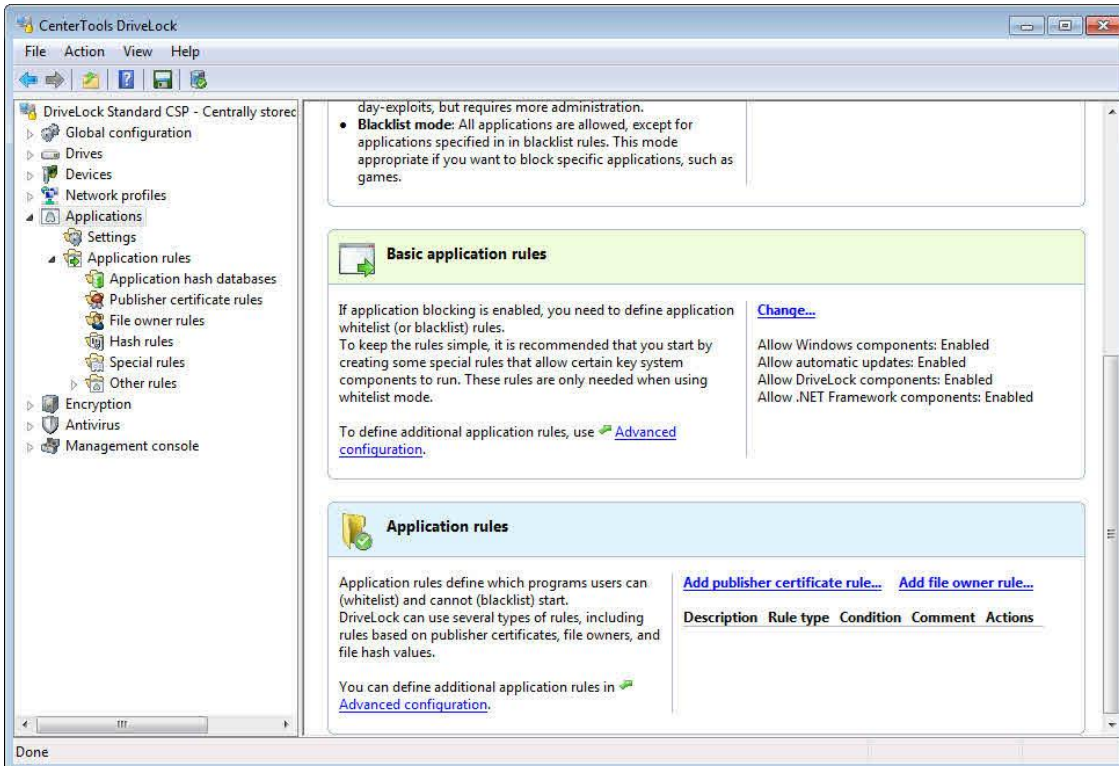


Select the type of rules to use and then click **Finish**. DriveLock creates the corresponding special rules. For more information about special application rules, refer to the section “[Using special rules](#)”.

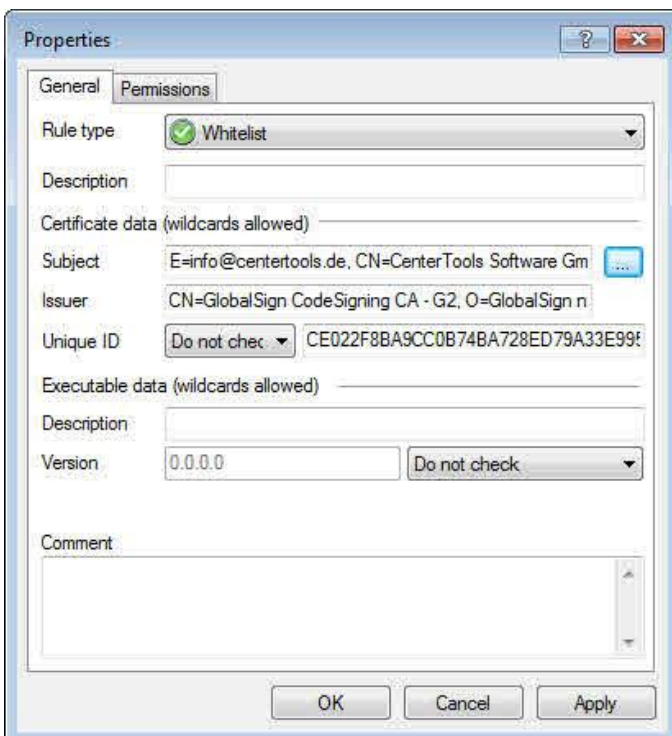
11.1.1.3 Configuring Simple Application Rules

This chapter remains in the Administration Guide until further notice, but it will not be updated. Please note that the current documentation on application control can be found in a separate manual available at [DriveLock Online Help](#) starting with version 2020.1.

In Basic configuration mode you can configure publisher certificate rules and file owner rules. To create other rule types you need to switch to the Extended Configuration task view.

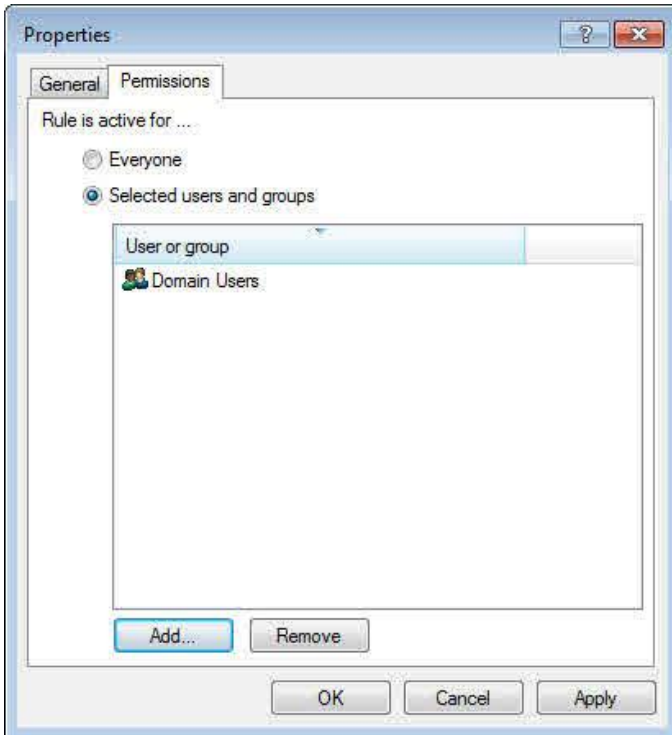


Click **Add publisher certificate rule...** to generate a new publisher certificate rule.



When you create a rule in Basic Configuration mode, the options to limit the rule to specific computers or network locations are not available. To create rules that contain these elements you must switch to the Extended Configuration mode.

For more information about publisher certificate rules, refer to the section [“Using publisher certificate rules”](#).



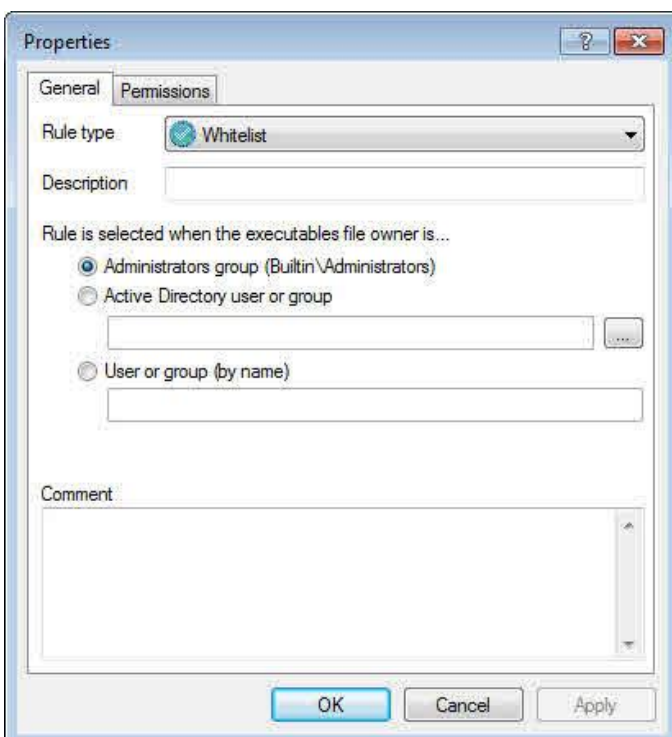
Select one of the following options:

- *Everyone*: The rule applies to all users.
- *Defined users and groups*: The rule only applies to the users or groups you add to the list.

Click **Add** to add a user or group to the list. To remove a user or group from the list, select the user or group and then click **Remove**.

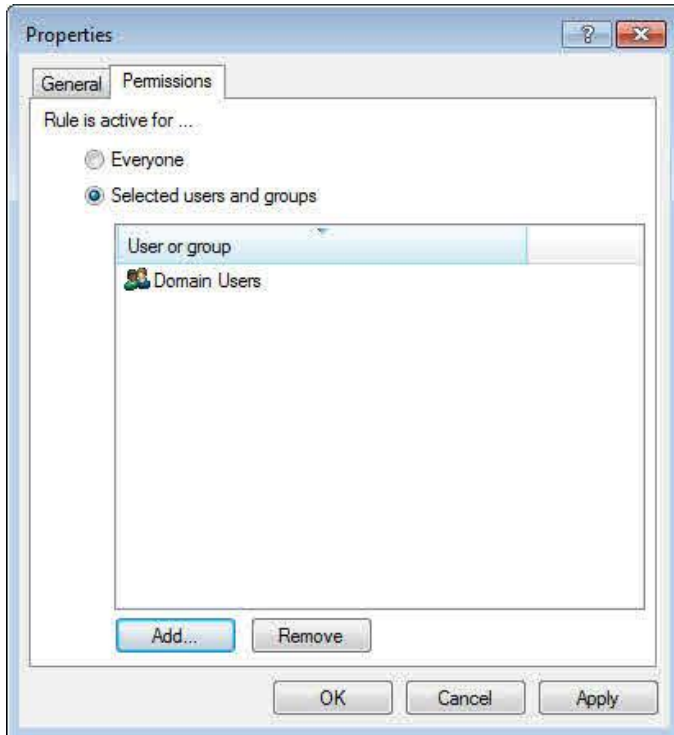
Click **OK** to create the rule.

To create a new file owner rule, click **Add file owner rule...**



When you create a rule in Basic configuration mode, the options to limit the rule to specific computers or network locations are not available. To create rules that contain these elements you must switch to the Extended Configuration mode.

For more information about file owner rules, refer to the section [“Using file owner rules”](#).



Select one of the following options:

- *Everyone*: The rule applies to all users.
- *Defined users and groups*: The rule only applies to the users or groups you add to the list.

Click **Add** to add a user or group to the list. To remove a user or group from the list, select the user or group and then click **Remove**.

Click **OK** to create the rule.

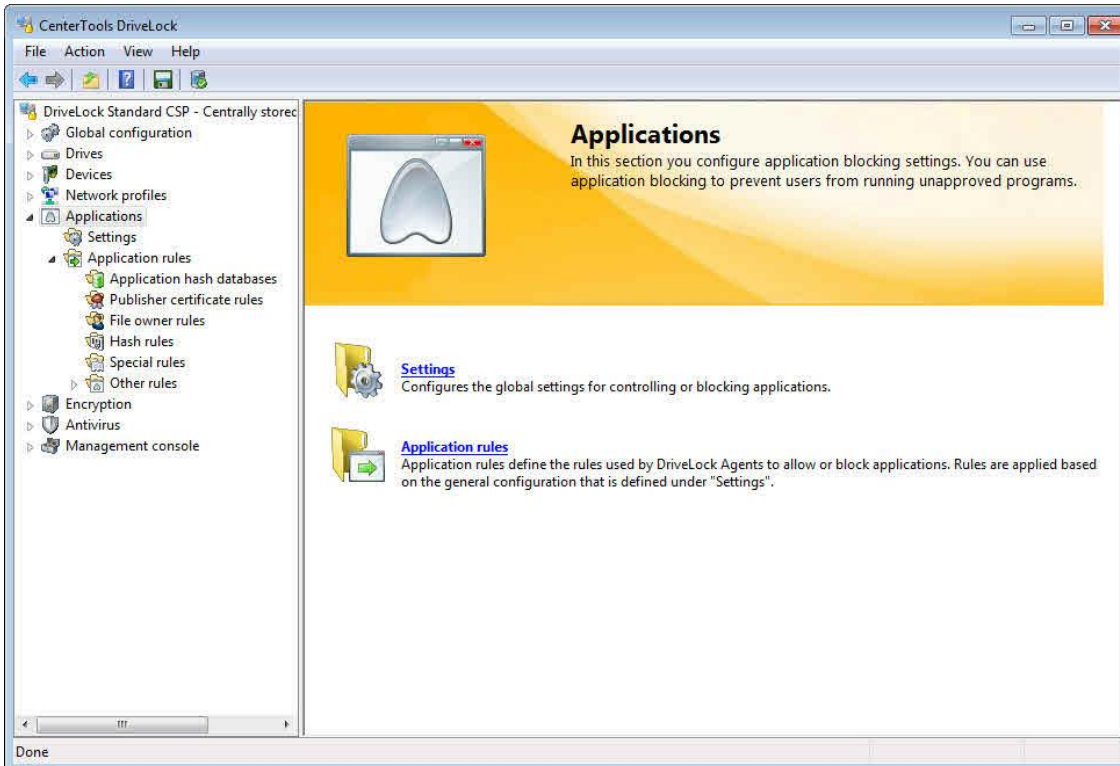
11.2 Extended Application Control

This chapter remains in the Administration Guide until further notice, but it will not be updated. Please note that the current documentation on application control can be found in a separate manual available at [DriveLock Online Help](#) starting with version 2020.1.

With the extended application control, you can define and restrict special application rules more precisely.

11.2.1 Extended Configuration

This chapter remains in the Administration Guide until further notice, but it will not be updated. Please note that the current documentation on application control can be found in a separate manual available at [DriveLock Online Help](#) starting with version 2020.1.



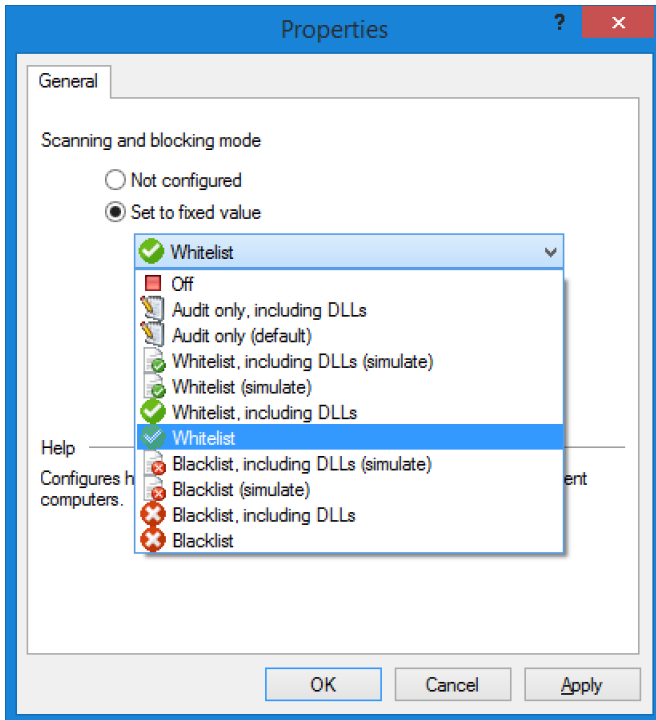
To configure more detailed Application Control settings, navigate to the nodes below Applications in the console tree, expand **Extended configuration** and then click **Applications**. If Basic Configuration mode is currently disabled, click **Applications** instead.

11.2.1.1 Configuring the Scanning and Blocking Mode

This chapter remains in the Administration Guide until further notice, but it will not be updated. Please note that the current documentation on application control can be found in a separate manual available at [DriveLock Online Help](#) starting with version 2020.1.

The scanning and blocking mode determines the overall operations of Application Control. Open **Applications / Settings / Scanning and Blockingmode**. To select one of the operation modes, follow the steps in the following sections. To disable the Application Control, select **Off**.

Scanning/Blocking DLLs is available in DriveLock Versions 7.7.8 and newer versions. Carefully read chapter [Scanning/Blocking DLLs](#), before using an "including DLLs" mode.



11.2.1.1.1 Auditing and simulation

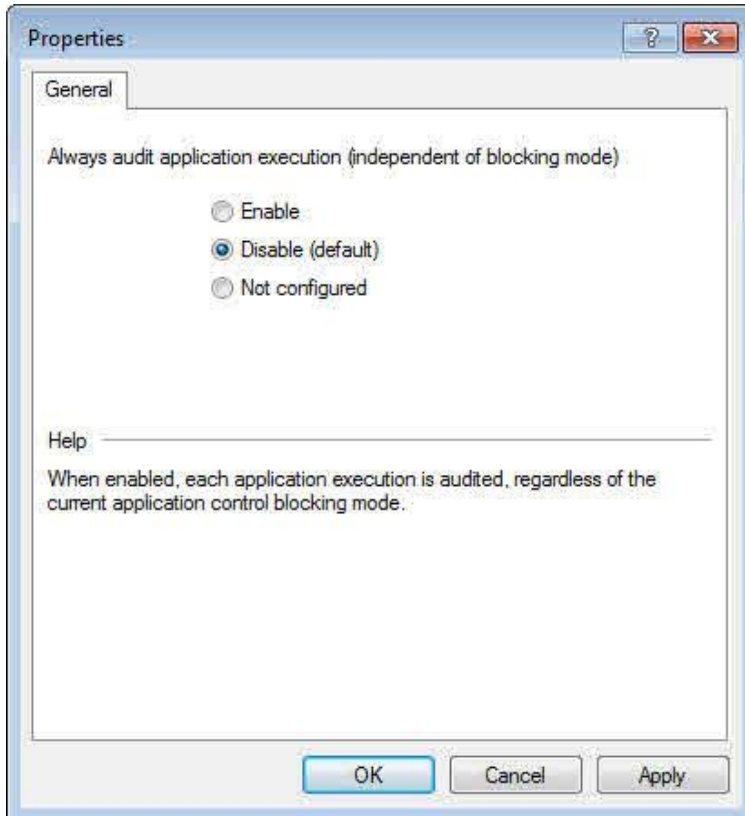
This chapter remains in the Administration Guide until further notice, but it will not be updated. Please note that the current documentation on application control can be found in a separate manual available at [DriveLock Online Help](#) starting with version 2020.1.

To monitor the execution of programs on computers without preventing any of these programs from starting, select **Audit-only**. The DriveLock Agent creates events for all programs that are started on a computer without enforcing any application templates or rules.

Use one of the two simulation modes (**Whitelist (simulate)** or **Blacklist (simulate)**) to test templates or rules before blocking programs. During simulation the DriveLock Agents creates events when applications are started that are controlled by templates and rules, but it doesn't prevent any programs from running.

Use the simulation modes to identify applications that users are running before enforcing any blocking rules. Review the local Event Logs or the DriveLock Control Center for such application starts and then modify the policy to allow programs that you initially overlooked. When the event information no longer indicates that required programs would be blocked by your rules, you can start enforcing the policy.

Once you have enabled Whitelist or Blacklist mode, DriveLock creates an event for each blocked application. To also audit successful application execution, click **Always audit application execution (independent of blocking mode)**.



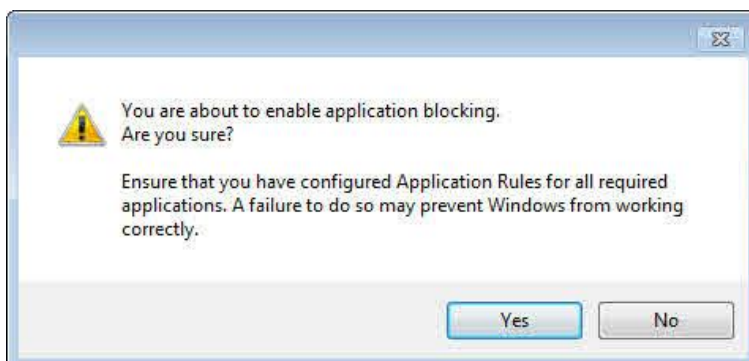
By default auditing is disabled. Select **Enable** to create events for all successful application starts.

Enabling auditing of every successful program start may decrease computer performance. If events are sent to the DriveLock Enterprise Service, it may also increase network traffic and the database size.

11.2.1.1.2 Whitelist mode and Blacklist mode

This chapter remains in the Administration Guide until further notice, but it will not be updated. Please note that the current documentation on application control can be found in a separate manual available at [DriveLock Online Help](#) starting with version 2020.1.

To activate Application Control, select **Whitelist** or **Blacklist**. In **Whitelist** mode, all applications except those allowed by your policy are blocked by default. If you select **Blacklist**, all applications can be used except those blocked by the rules and templates you configure.



When you select one of the blocking modes, DriveLock displays a warning message. Click **Yes** to activate Application Control or click **No** to cancel the current operation.

In addition to the blocking mode, whitelist and blacklist rules and templates control program execution. You can create both whitelist rules and blacklist rules in either blocking mode. The following sections describe how rules and templates work in each mode.

11.2.1.1.2.1 Whitelist mode

This chapter remains in the Administration Guide until further notice, but it will not be updated. Please note that the current documentation on application control can be found in a separate manual available at [DriveLock Online Help](#) starting with version 2020.1.

When using the whitelist mode, only applications listed in whitelist rules or templates are allowed to run. Additionally, you can use blacklist rules to disable selected applications even though they may be included in a whitelist template or rule. In effect, in this mode blacklists define exceptions to your whitelist rules.

In whitelist mode, the priority of rules is: Blacklist rules – whitelist rules – all others

Example: To allow all users to run all programs in the Program Files folder, create a directory rule and allow all applications within this folder to run. To prevent one of these applications from running on one computer, create a blacklist rule for only this application and apply it to the computer.

11.2.1.1.2.2 Blacklist mode

This chapter remains in the Administration Guide until further notice, but it will not be updated. Please note that the current documentation on application control can be found in a separate manual available at [DriveLock Online Help](#) starting with version 2020.1.

When using the blacklist mode, all applications are allowed to run unless they are listed in blacklist rules or templates. Use blacklist rules or templates in this mode to specify the applications that users are not allowed to start. Use whitelist rules in this mode to define exceptions to blacklist templates or rules.

In blacklist mode, the priority of rules is: Whitelist rules – blacklist rules – all others

Example: Users in your organization are not allowed to run the program “Skype”. However, your CIO must use Skype while he is out of the office. To allow this, create a blacklist rule to block Skype for all uses. Then define a whitelist rule allowing the Skype application and configure it to apply to only the CIO’s account.

11.2.1.2 Configuring a Hash Algorithm for Hash-Based Rules

This chapter remains in the Administration Guide until further notice, but it will not be updated. Please note that the current documentation on application control can be found in a separate manual available at [DriveLock Online Help](#) starting with version 2020.1.

To configure a hash algorithm to be used with all rules that use hash values, click **Settings** and then click **Hash algorithm for hash-based rules** to open the Properties window.

To configure DriveLock to always use a hash algorithm, click **Set to fixed value** and then select the algorithm from the list. If this is set to *Not configured*, the MD5 algorithm is used.

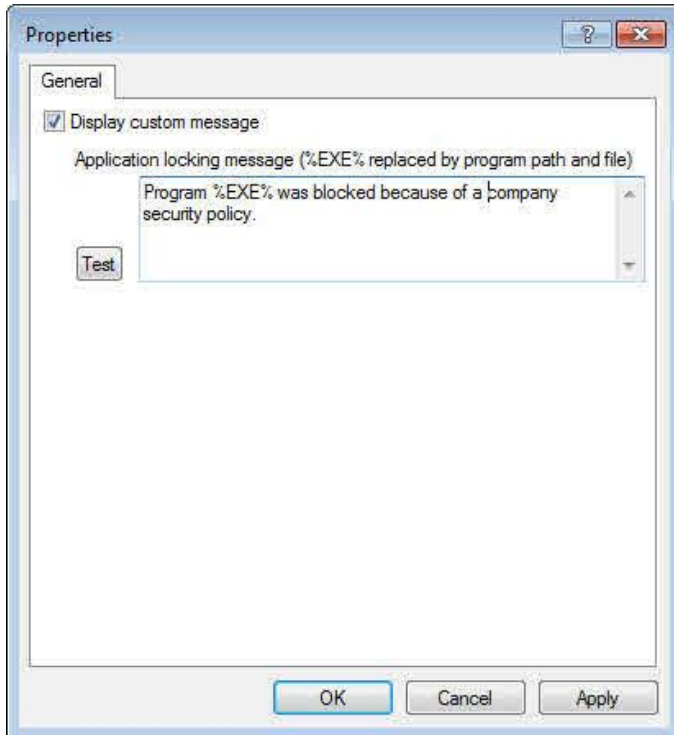
11.2.1.3 Configuring User Notifications

This chapter remains in the Administration Guide until further notice, but it will not be updated. Please note that the current documentation on application control can be found in a separate manual available at [DriveLock Online Help](#) starting with version 2020.1.



You can define a custom user notification messages for each whitelist rule. Unless specified otherwise, DriveLock will display this message when the Application Control blocks an application.

If you configured a multilingual message text for the current language, DriveLock will display the standard messages defined for this language instead of the message configured in this dialog box. For information about how to configure multilingual messages, refer to the DriveLock Management Console manual.



Select **“Display custom messages”** to enable the messages specified on this dialog box. Type the message to be displayed to the user. When the message is displayed, the Agent replaces the variables **“%EXE%”** with the path and file name of the blocked application.

Click **Test** to display a message with the current text on your computer.

Click **OK** to close the window.

11.2.1.4 Special Settings

This chapter remains in the Administration Guide until further notice, but it will not be updated. Please note that the current documentation on application control can be found in a separate manual available at [DriveLock Online Help](#) starting with version 2020.1.

These settings are only visible in the classic MMC view of Application Control Settings. Do not change without advice of DriveLock Support or DriveLock Consulting Services.

- Caching mode
- Time values are kept in cache
- Paths without hash generation for executed applications
- Directories learned for local whitelist
- Trusted processes
- Upload local whitelist to DES

11.2.2 Configuring Application Rules

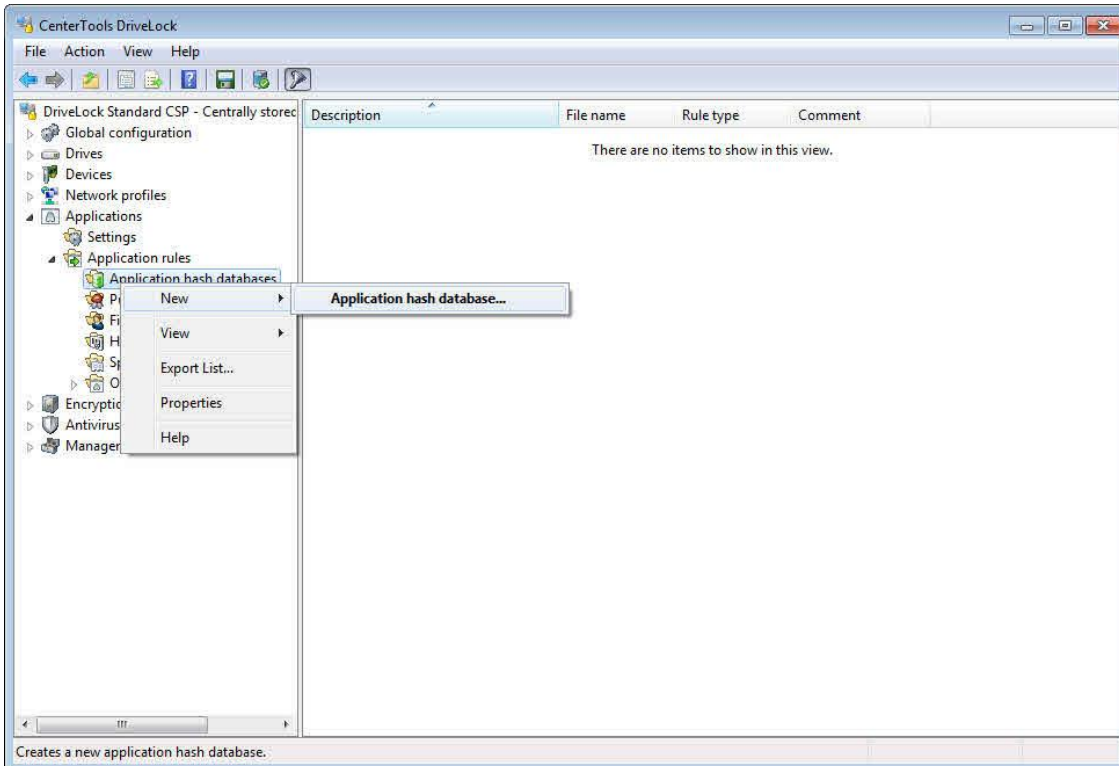
This chapter remains in the Administration Guide until further notice, but it will not be updated. Please note that the current documentation on application control can be found in a separate manual available at [DriveLock Online Help](#) starting with version 2020.1.



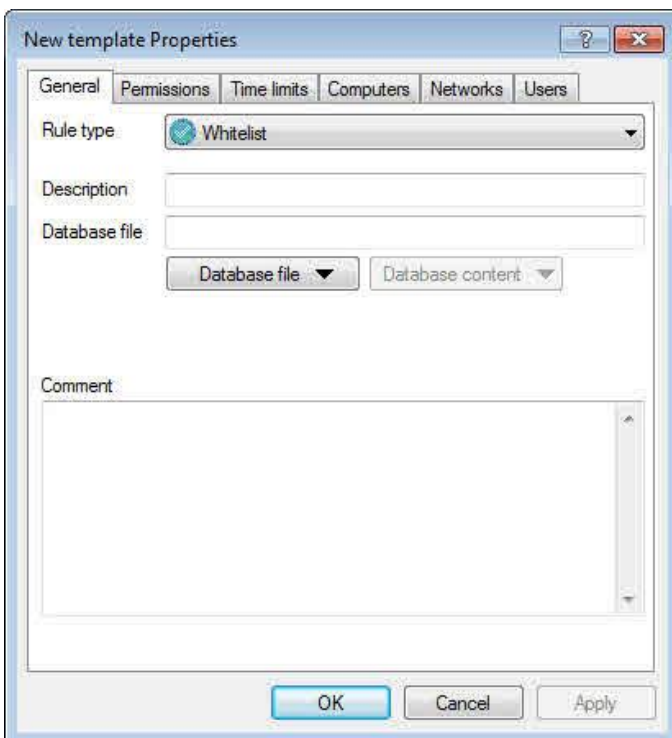
11.2.2.1 Using Application Hash Databases

This chapter remains in the Administration Guide until further notice, but it will not be updated. Please note that the current documentation on application control can be found in a separate manual available at [DriveLock Online Help](#) starting with version 2020.1.

To simplify using Application Control, DriveLock can create application hash databases that you can use to easily allow or block multiple applications. To create an application hash database, DriveLock can scan directories on your computers, including any subdirectories, for installed applications and calculate a hash for each of them. These hashes are then added to the hash database. You can use this procedure to create a hash database that includes all applications on a computer. When you whitelist all applications in this database, DriveLock prevents any programs from running that are not included or that are installed after the computer was scanned.



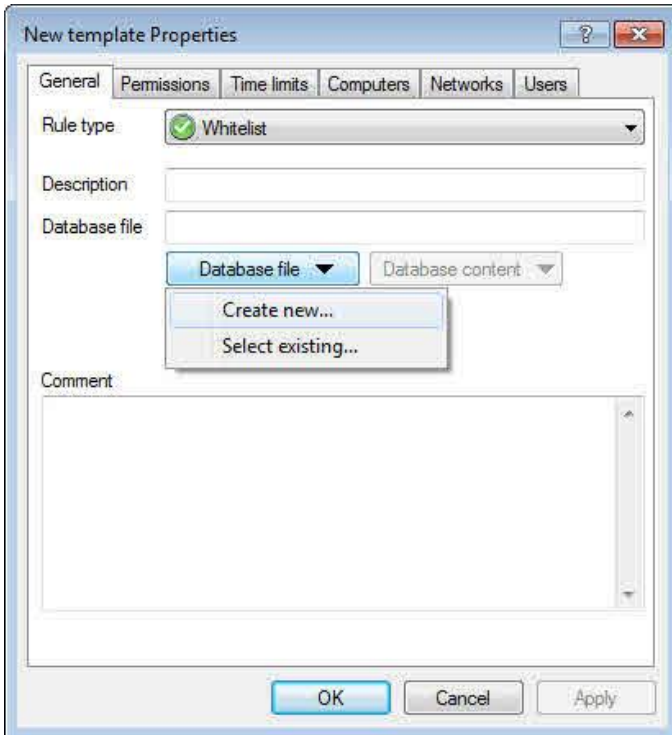
To create a hash database, right-click **Application hash databases** and then click **New -> Application hash database**.



You base a hash database rule on an existing hash database or create a new hash database.

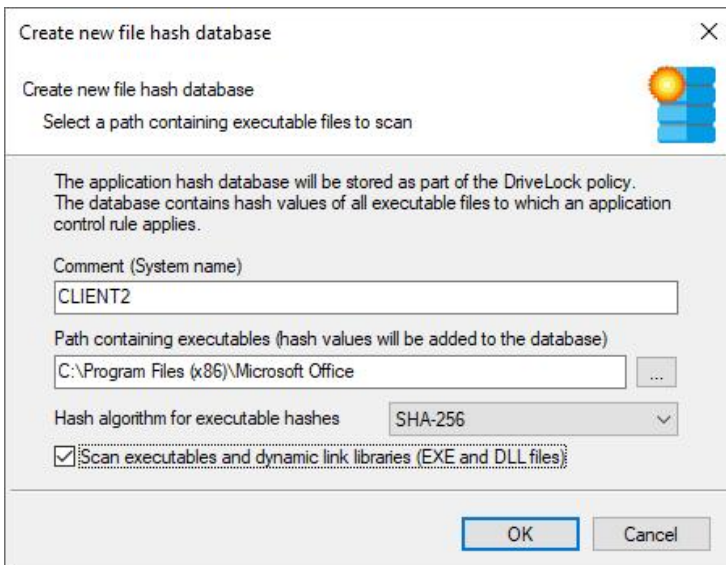
You can also use the standalone Application Hash Database Tool to create and manage hash databases. You can find the program file "*DLExeHasher.exe*" in the directory where you installed the DriveLock Management Console (C:\Program Files\CenterTools\DriveLock MMC\Tools\DLExeHasher.exe).

If a hash database already exists you can view or edit it.



To view or edit an existing database, click **Database file**, click **Select existing** and then select the database.

To create a new database, click **Database file** and then click **Create new**.



In the **Comment (System name)** box, type the name of the computer to be scanned. Recording the computer name can make it easier to keep track the origin of a hash database when managing or merging multiple databases.

Type or select the directory to be scanned for applications.

You can scan a directory on a remote computer by specifying the UNC path for this directory.

The **Hash algorithm for executable hashes** defines the algorithm used for this database. To ensure interoperability between multiple databases and rules, we recommend that you define this algorithm globally with the **Hash algorithm for hash-based rules** setting before you create any hash databases. Select **Scan executables and dynamic link libraries** to scan DLL files in addition to EXE files.

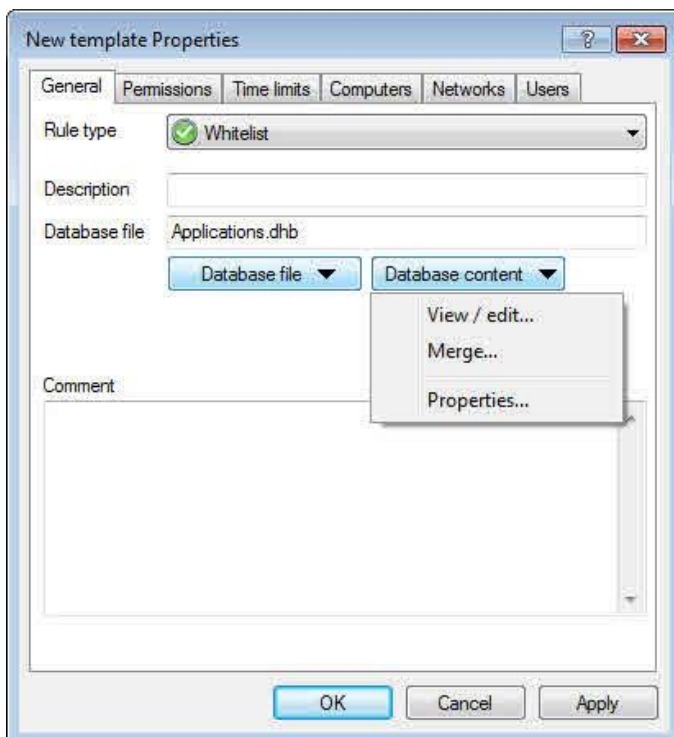
Click **OK**. DriveLock starts a recursive scan of the specified directory and all subdirectories below it.

Scanning a directory that contains many files can take several minutes to complete. Scanning may take longer if the directory is located on a remote computer. If you cancel the scan, the results will not be complete.

When processing the scan results, DriveLock eliminates duplicates. As a result, identical files that are located in more than one directory are listed only once. This has no effect on how the rule is applied because applications are evaluated based on their hashes and not a specific location. Also, this behavior allows for differential scanning, which only adds applications that are not already in the database.

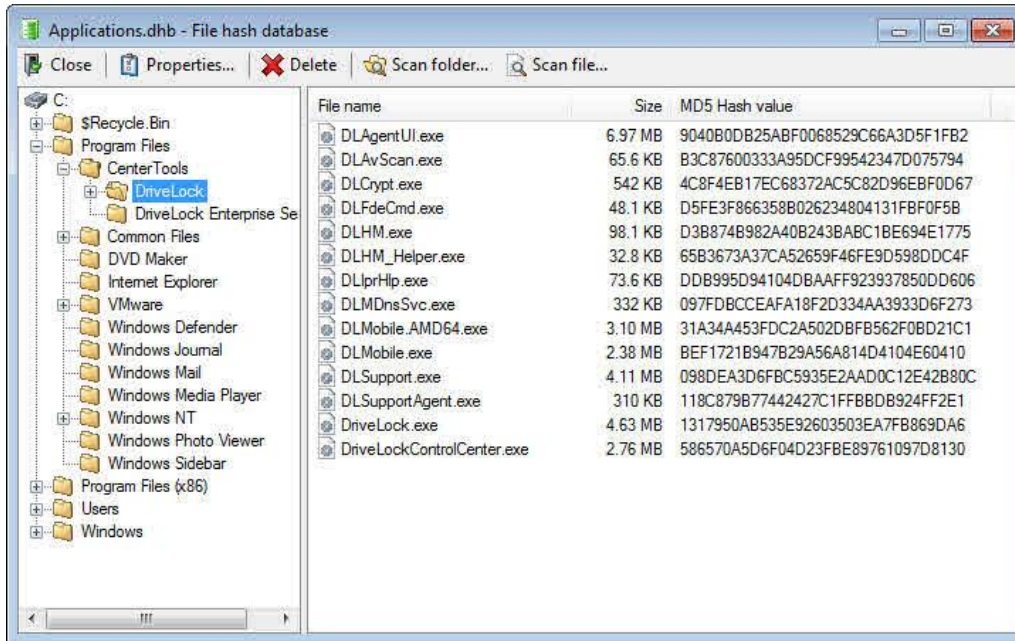
When DriveLock has finished detecting all program files and has calculated all hashes, it adds all applications it detected to the template and displays the previous dialog box.

In the **Description** field, type a description to help you identify the template later.



Click **Database content** to view, edit or merge the programs that are included in the database.

Click **Database content** and then click **View / edit** to view the database content.



The left pane displays the folders that were scanned. Select a folder to display all programs that were found in this folder in the right pane.

To add additional hashes, click **Scan folder** or **Scan file**. Click **Delete** to remove the selected application hash or folder. To view additional information about the hash database, click **Properties**.

To close the hash database viewer, click **Close**.

You can also use the standalone Application Hash Database Tool, DLExHasher.exe, to view, edit and merge hash databases.

Click **Database content** and then click **Merge** to add the content of another database.

Type or select the path of the database file containing the entries to be added and then click **OK**.

DriveLock merges the database content and then displays the template properties again.

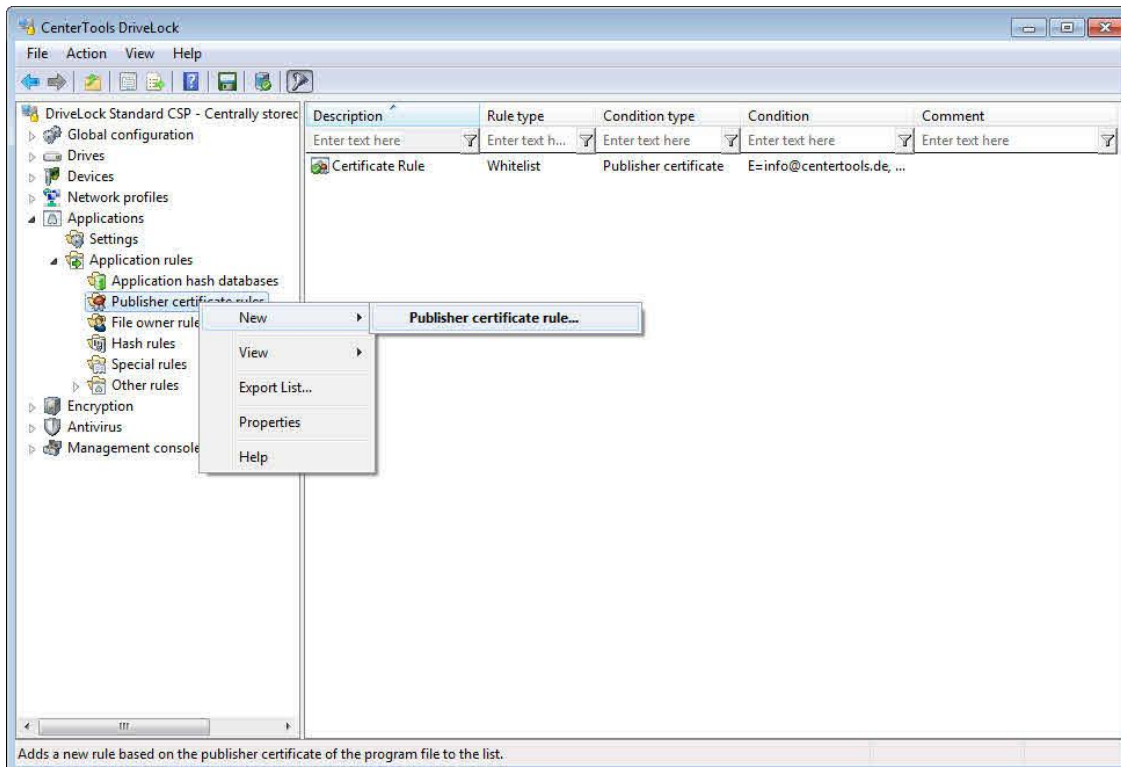
Even if you are using a whitelist rule based on a hash database of all installed applications to control a computer, it is recommended that you also use some special application rules for programs that are part of the operating system. DriveLock loads these special rules faster than data from the hash database and they are available earlier to the DriveLock Agent when Application Control starts. For more information about special rules, refer to the section " [Using Special Rules](#) ".

11.2.2.2 Using Publisher Certificate Rules

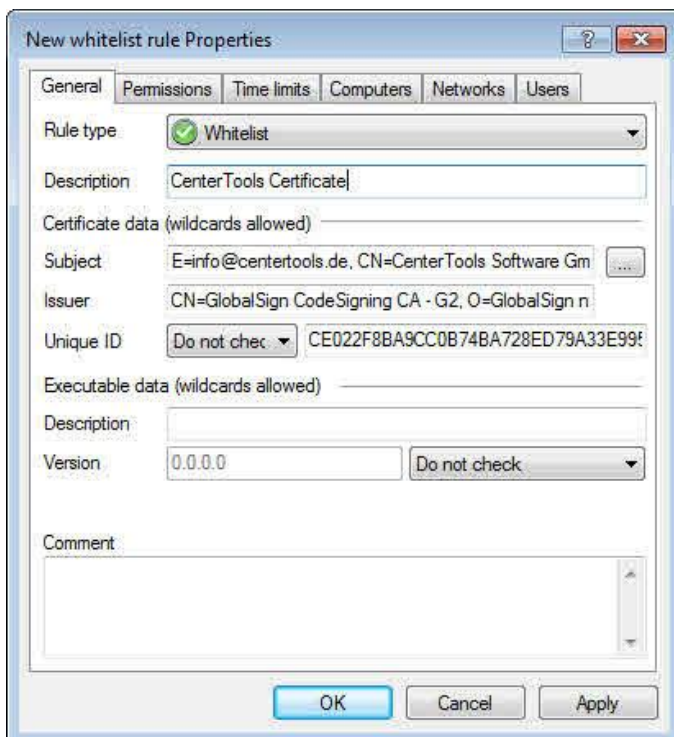
This chapter remains in the Administration Guide until further notice, but it will not be updated. Please note that the current documentation on application control can be found in a separate manual available at [DriveLock Online Help](#) starting with version 2020.1.

Software publisher certificates can be used to verify the publisher of software, the software version and other attributes of a program file. Certificates are issued by a Certificate Authority (CA) that verifies a software publisher's identity. The publisher then signs the software with this certificate. DriveLock can check program files to verify that they were signed using a certificate that was issued by a trusted CA and to ensure that the program file was not modified since it was signed. Once the validity of the program file has been verified, the DriveLock Agent compares the information in the software publisher's certificate and the program version with the rules in your policy and

allows or blocks access according to these rules. Use publisher certificate rules to configure which information DriveLock checks and whether programs are allowed or blocked based on this information.



To create a certificate rule, right-click **Publisher certificate rules** and then click **New -> Publisher certificate rule**.

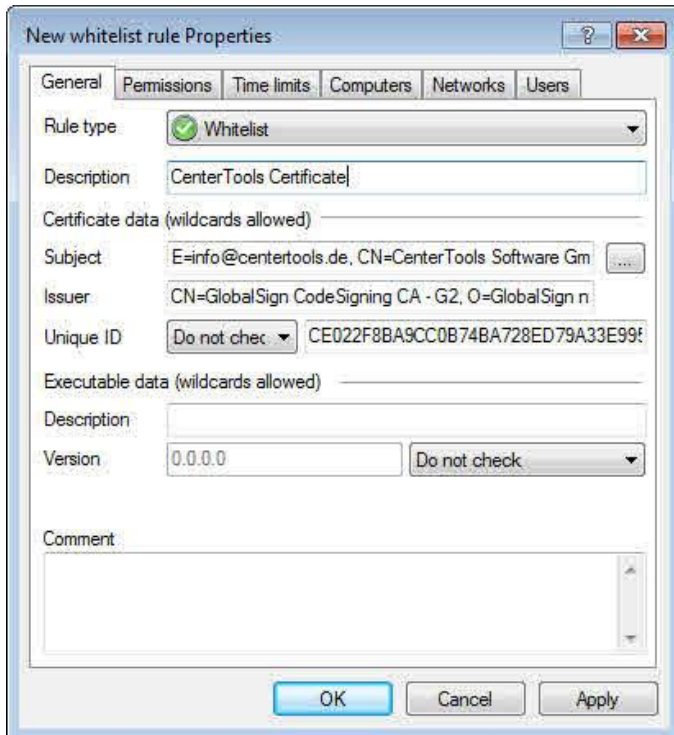


You can enter whitelist rule values manually. However, it is easier and quicker to select a program file on the computer's hard disk and let DriveLock extract the information from it. To extract the information, click the button "... " and then select a program.

If the program was signed using a software publisher certificate, DriveLock automatically populates the text fields with the data from the certificate.

In the Description field, type a description and then click **OK** or **Apply**.

You can edit the data in the dialog box. You can also use wildcards (* or ?) to create rules that match multiple certificates. The fields Subject and Issuer must contain data. Use the asterisk (*) wildcard character to create a rule that matches all data in a certificate field.



You can only use wildcard characters at the end of a text field. Rules that contain wildcard characters in any other position are not enforced correctly.

The unique ID can be the serial number or the certificate's thumbprint. If use a serial number, you must select Serial number from the drop-down menu before you click the "..." button to select a file. Otherwise the thumbprint is read from the certificate.

When using a publisher certificate rule you can specify a version number to prevent users from running a different version of the program or an older version of the program. For example, you can allow Acrobat Reader® version 8.1 or higher and block all older versions that may contain known security flaws. Select one of the appropriate option from the version drop-down menu and then type a version number in the field on the left in one of the following formats: ## or ##.# or ##.##.

By default the rule type is set to whitelist rule. You can change it to blacklist rule by selecting this rule type from the drop-down menu. Type a comment in the comment field to save additional information about this rule.

Click **OK** to close the Properties window and save the rule.

11.2.2.3 Using File Owner Rules

This chapter remains in the Administration Guide until further notice, but it will not be updated. Please note that the current documentation on application control can be found in a separate manual available at [DriveLock Online Help](#) starting with version 2020.1.

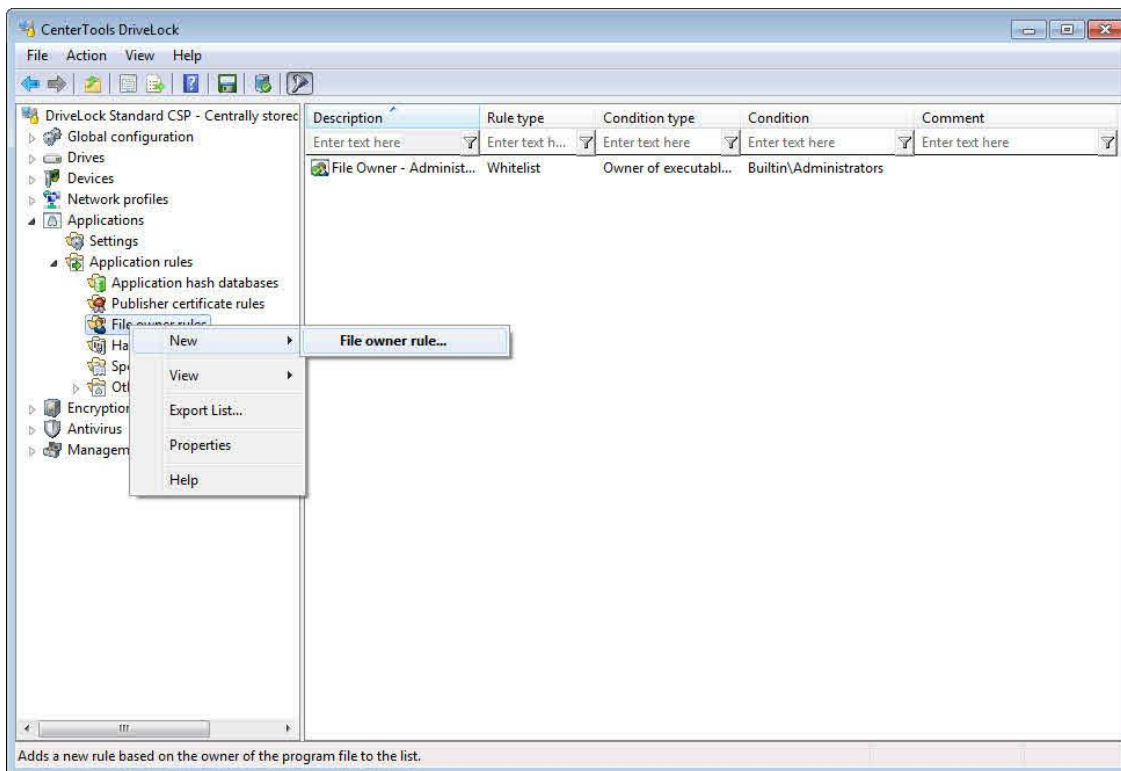
In Microsoft Windows all files, including program files, are assigned an owner. In most cases the file owner is "SYSTEM", the local administrators group or a user account. Each time new software is installed on the computer the file owner attribute is set as follows:

- If the current logged-on user is a member of the local administrators group, this group becomes file owner.
- If the current logged-on user is not a member of the local administrators group, the user becomes file owner.

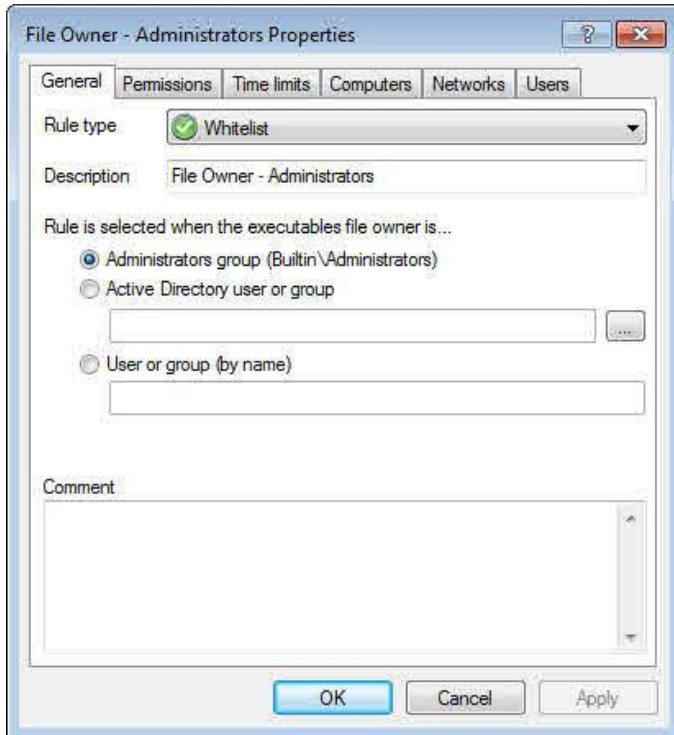
You can also manually set the file owner for a single file, a single folder or for a folder and all files and directories below it.

You can use file owner rules to allow users to start all applications that have a specific file owner. For example, you can use such a rule to authorize all programs that were installed by an administrator or by a trusted installer account, while blocking all applications that were installed by other users. When you use a file owner rule, all applications that run without needing to be installed first are also blocked.

If your software deployment mechanism uses a dedicated installation account with administrative rights, or if users don't have local administrative rights, file owner rules are the easiest and most effective solution to allow authorized applications with a minimum number of rules.



To create a file owner rule, right-click **File owner rules** and then click **New -> File owner rule**.



Select **Administrators group (Builtin\Administrators)** to create a rule that covers all local administrators.

Click the “...” button to select a user or group from Active Directory.

To manually specify a user name or group, select **User or group (by name)** and type the name.

By default the rule type is set to whitelist rule. You can change it to blacklist rule by selecting this rule type from the drop-down menu. Type a comment in the comment field to save additional information about this rule.

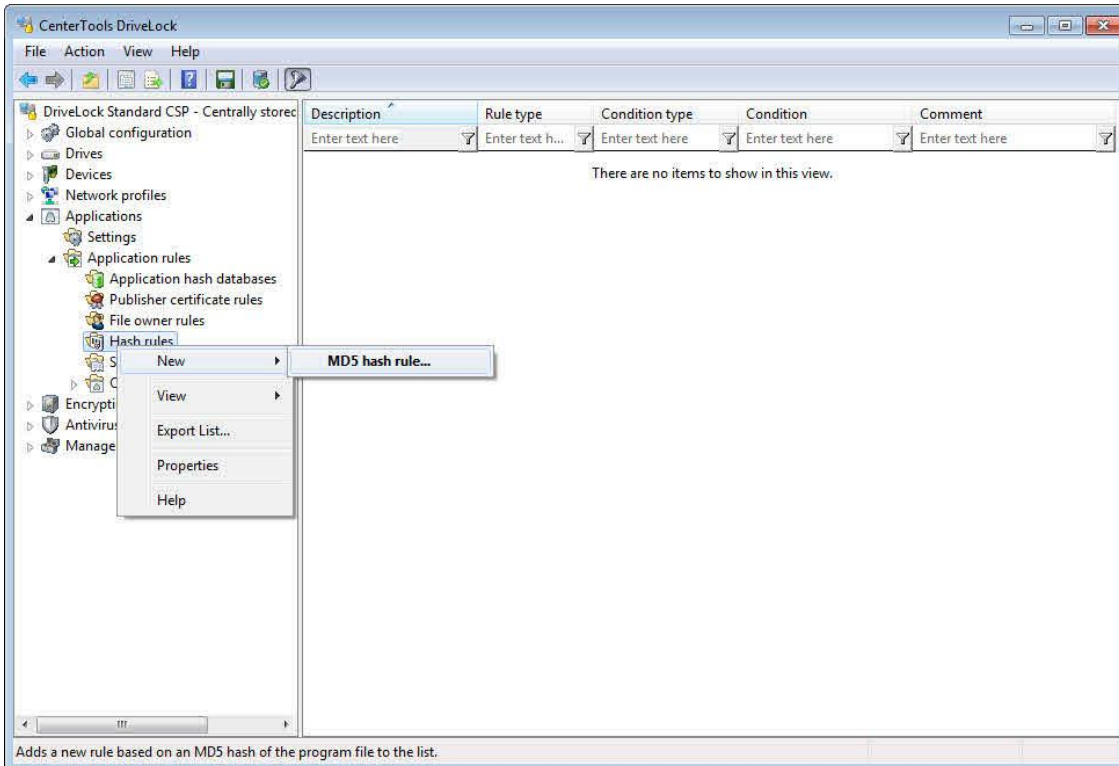
Click **OK** to close the Properties window and save the rule.

If you assign a group, the file owner must be the group, not a member of that group.

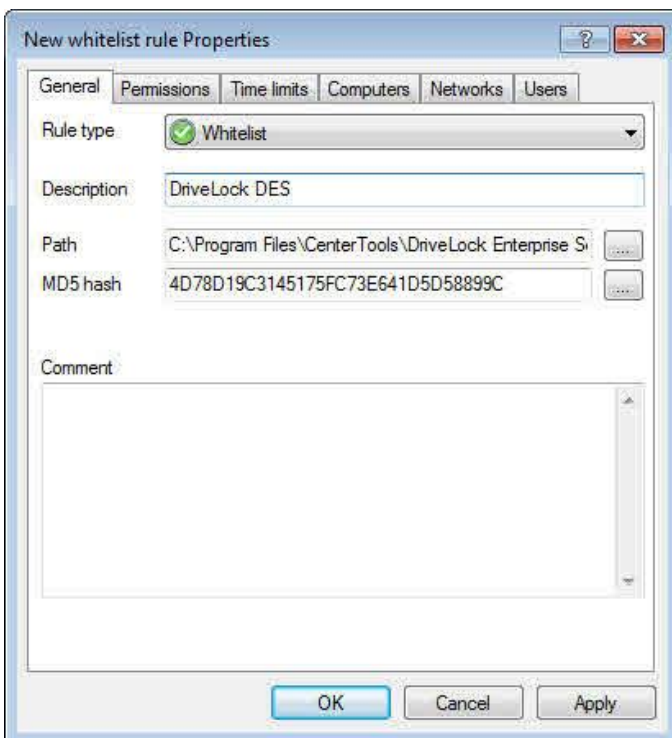
11.2.2.4 Using Hash Rules

This chapter remains in the Administration Guide until further notice, but it will not be updated. Please note that the current documentation on application control can be found in a separate manual available at [DriveLock Online Help](#) starting with version 2020.1.

A hash rule specifies a single application based on a unique hash value of the program that DriveLock compares to the hash value of programs that users attempt to start. If the values match, the rule is applied.

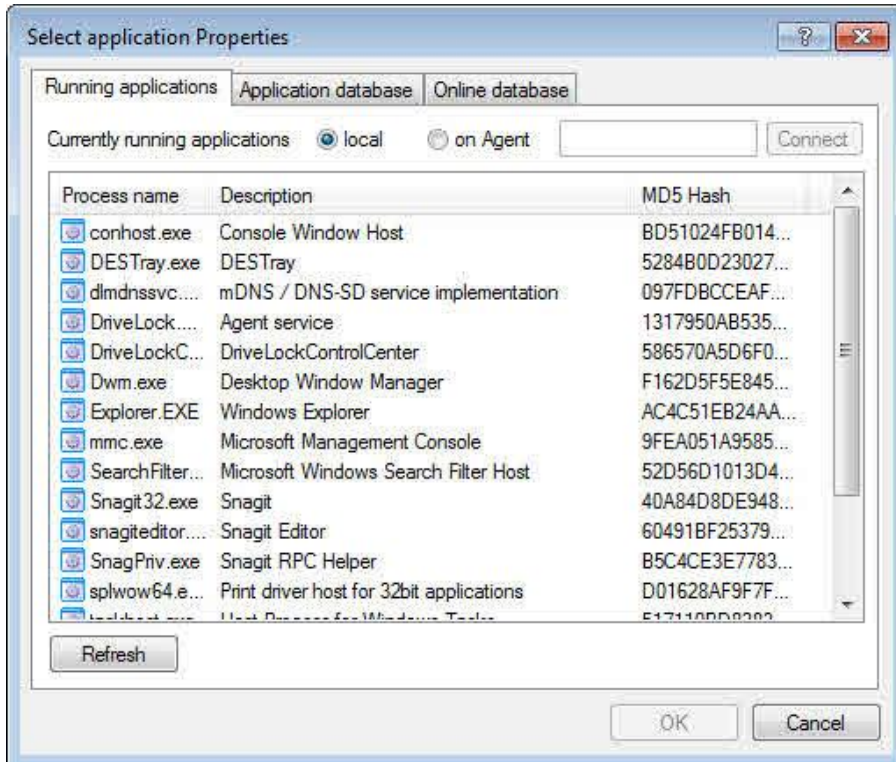


Right-click **Hash rules** and then click **New -> MD5 hash rule**.



To identify the application by using its file name, type the full path and file name or click “...” next to the **File Name** field and then select the file.

To select a currently running application, or to select an application from the application database that is included with DriveLock or the online database, click the “...” button next to the MD5 Hash field.



You can also connect to a remote computer where the DriveLock Agent is installed to scan for programs that are currently running on that computer.

To establish a connection to a remote computer running Windows XP SP2 or higher with the Windows Firewall enabled, you must configure the firewall settings to allow incoming connections from TCP Port 6061 (default) and the program "DriveLock".

To access the application database, click the corresponding tab.

Click **OK** to add the program to the rule.

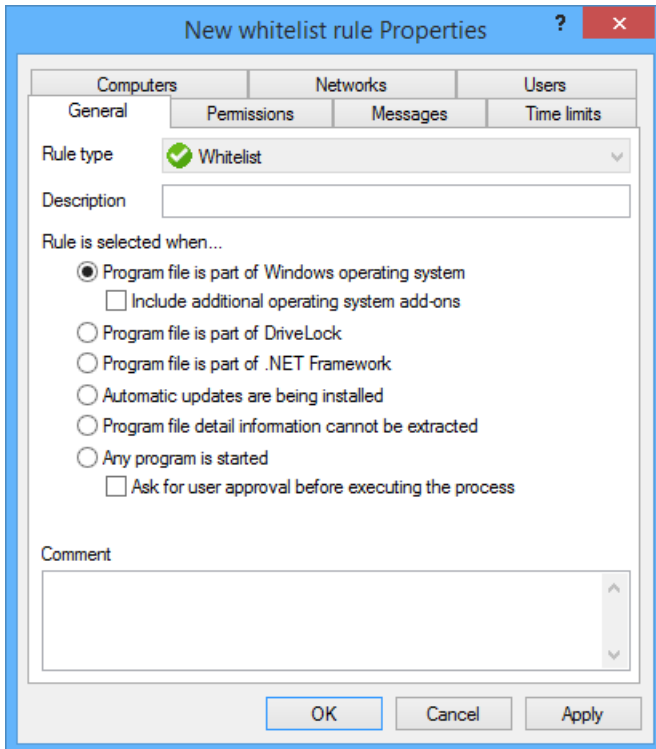
When you have selected the application, DriveLock adds automatically the application name, file name and file hash. You may also add a comment.

Click **OK** to complete the rule.

11.2.2.5 Using Special Rules

This chapter remains in the Administration Guide until further notice, but it will not be updated. Please note that the current documentation on application control can be found in a separate manual available at [DriveLock Online Help](#) starting with version 2020.1.

Open **Applications / Applications rules / Special rules /** right click **New / Special rule.**



These special rules shall only be used as whitelist rule.

Program file is part of the Windows operating system

- includes all programs protected by the Windows System File Protection (WFP)

Include additional operation system add-ons addresses programs in:

- C:\windows
- C:\windows\system32
- C:\windows\servicing
- C:\windows\pchealth\helpctr\binaries (Help Center)
- C:\windows\application compatibility scripts
- C:\windows\explorer.exe
- C:\Program Files\Internet Explorer
- C:\Program Files\Windows Defender

The program is a component of DriveLock

- all programs in the DriveLock installation directories

The program is part of the .NET Framework

- all programs in C:\Windows\Microsoft.NET

Windows Automatic Updates are being installed

- all processes initialized by the Windows Update Agent

Program file detail information cannot be extracted

- can be used as a fallback if for any reason DriveLock is not able to access or read information details from a specific file

Any program is started.

- can be used in conjunction with rule limitations for example, to allow access to all programs for the Administrators group, optionally including a user approval before executing the process.

Predictive whitelisting (machine learning)

Open **Applications / Applications rules / Special rules / right click New / Predictive whitelisting rule.**

- This rule overwrites the global **Predictive and local whitelist** settings. For more information read chapter [Predictive Whitelisting](#).

11.2.2.6 Other Application Rules

This chapter remains in the Administration Guide until further notice, but it will not be updated. Please note that the current documentation on application control can be found in a separate manual available at [DriveLock Online Help](#) starting with version 2020.1.

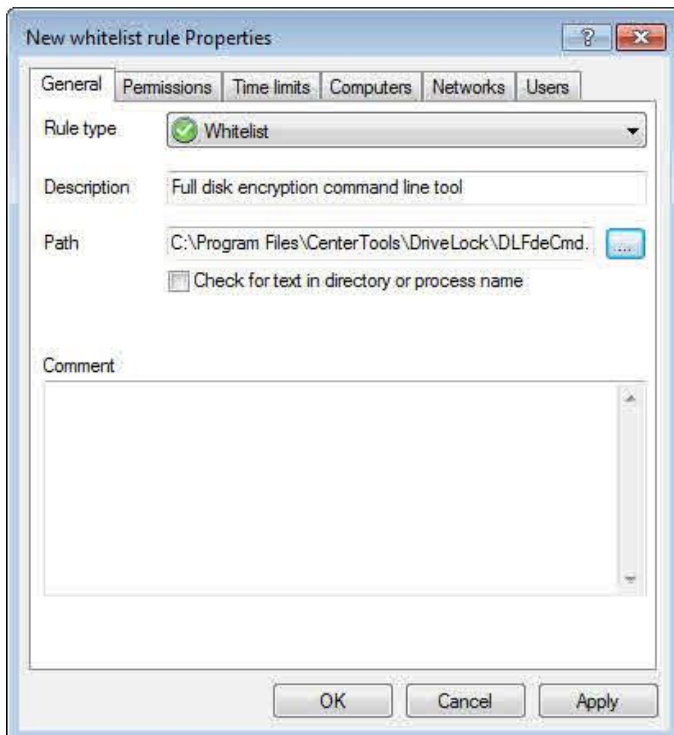


11.2.2.6.1 Using file path rules

This chapter remains in the Administration Guide until further notice, but it will not be updated. Please note that the current documentation on application control can be found in a separate manual available at [DriveLock Online Help](#) starting with version 2020.1.

A file path rule specifies a folder or file on the computer. When a user attempts to start this program or a program from this folder, the rule is applied.

Right-click **Other rules** and then click **New -> File path rule**.



Click “...” next to the Path field to select the file or folder, depending whether you have selected the “**Check for whole directory (not file name)**” checkbox. DriveLock automatically adds information to the Description field, but you can change this information and type an optional comment.

If you select the *Check for whole directory (not file name)* checkbox, DriveLock checks the entire directory for the specified path when a program is started. This means that the rule also applies to programs that are started from a subdirectory.

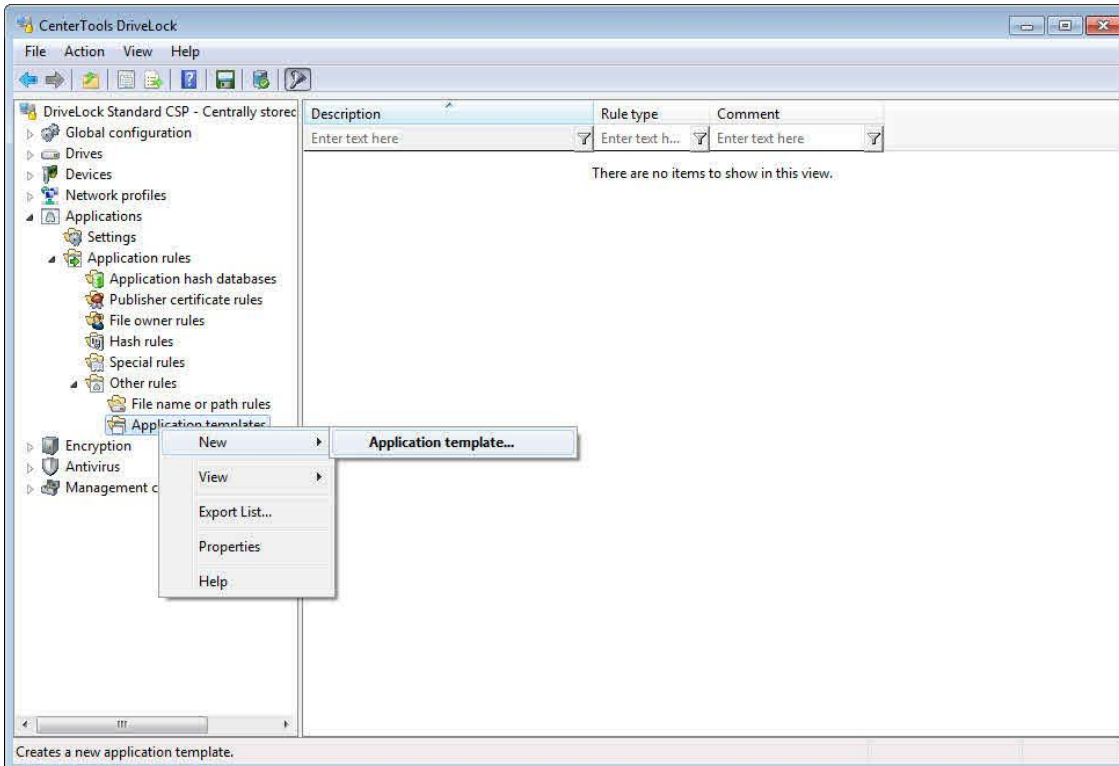
When you have selected the application, DriveLock automatically adds the application name to the **Description** field. You can also add an optional comment.

You can use wildcard characters (? For a single character or * for multiple characters to make a single rule apply to multiple programs.

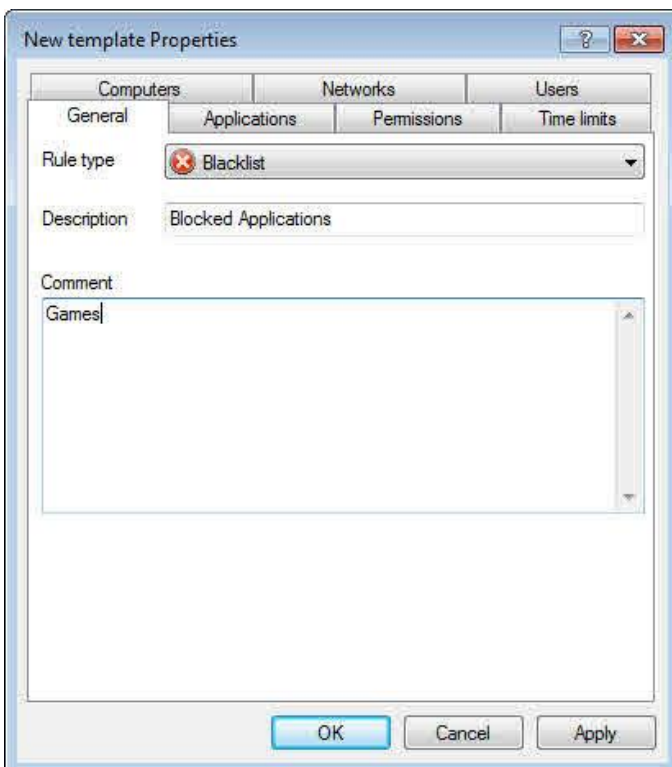
11.2.2.6.2 Using Application Templates

This chapter remains in the Administration Guide until further notice, but it will not be updated. Please note that the current documentation on application control can be found in a separate manual available at [DriveLock Online Help](#) starting with version 2020.1.

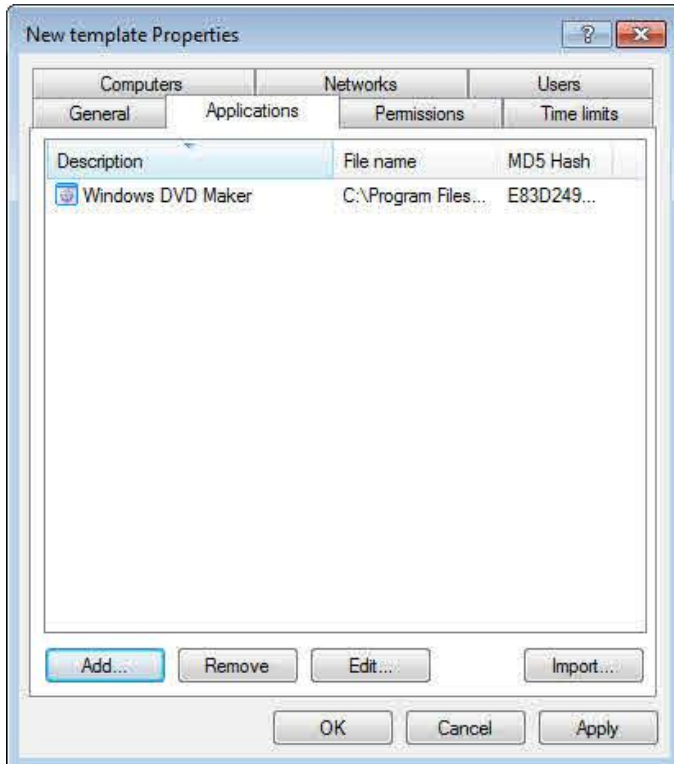
Application templates can contain one or more applications that the DriveLock Agent blocks (blacklist) or allows to be started by a user (whitelist).



Right-click **Application templates** and then click **New -> Application template**.



Select the rule type and then type a description and an optional comment with more information about the template. Click the **Applications** tab to configure the applications in the template.

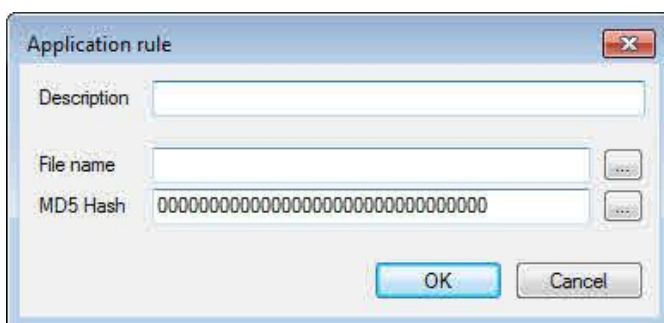


To edit the settings for an application in the list, select the application and then click **Edit**. Click **Remove** to delete an application from the list.

11.2.2.6.2.1 Adding a single application

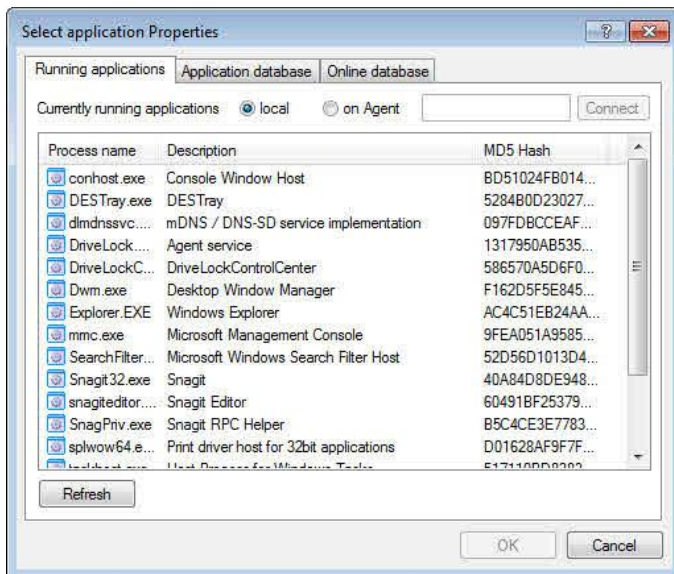
This chapter remains in the Administration Guide until further notice, but it will not be updated. Please note that the current documentation on application control can be found in a separate manual available at [DriveLock Online Help](#) starting with version 2020.1.

To add a single application to the list, click **Add**.



To identify the application by using its file name, type the full path and file name or click “...” next to the File Name field and then select the file.

To select a currently running application or select an application from the application database that is included with DriveLock click the “...” button next to the MD5 Hash field.



You can also connect to a remote computer running the DriveLock Agent to list the programs that are currently running on that computer.

To establish a connection to a remote computer running Windows XP SP2 or higher on which the Windows Firewall is enabled, you must configure the firewall settings to allow incoming connections from TCP Port 6061 (default) and the program "DriveLock".

To access the application database, click the corresponding tab.

You can select applications from an online database that contains several million applications. To select a program from this database, click the **Online database** tab.

DriveLock connects to the online database over the Internet. If the connection fails, an error message appears.

Otherwise DriveLock displays the contents of the online database.

Select the manufacturer of the application you want to add, select the application, and then click **OK**. When you have selected the application, DriveLock automatically adds the application name, file name and file hash.

Click **OK** to add the program to the template. To add additional applications, repeat the preceding procedure.

11.2.2.6.2.2 Adding a set of applications

This chapter remains in the Administration Guide until further notice, but it will not be updated. Please note that the current documentation on application control can be found in a separate manual available at [DriveLock Online Help](#) starting with version 2020.1.

To add a set of application to the list, click **Import**.

Use the import function to configure application templates for well-known software products that are included in the extensive DriveLock online database, such as Microsoft Office and Adobe Acrobat. Many of these products contain multiple program files, and selecting the product from the database adds all of these program files in a single step.

To select a program from the online database, click the **Online database** tab.

Select a vendor and product.

Click **OK** to import all program files that are included in the selected product or application.

DriveLock connects to the online database and imports the hash values for all program files.

11.2.3 Scanning/Blocking DLLs

This chapter remains in the Administration Guide until further notice, but it will not be updated. Please note that the current documentation on application control can be found in a separate manual available at [DriveLock Online Help](#) starting with version 2020.1.

When executable programs are scanned/blocked, DriveLock scans the executable while the Windows Operating System is loading it into memory. Depending on the result of the scan and the rules configured in the DriveLock policy then DriveLock allows or denies the execution of the program.

Scanning/Blocking DLLs in principle works the same way. When programs are loading DLLs, all these DLLs will be scanned and assessed while loading. If a DLL must be blocked, the calling program will be terminated.

You need a license for the DriveLock application control, which activates all functions of our established application control plus the advanced intelligent functions of predictive whitelisting.

If you plan to activate Application Control in whitelist mode including DLLs, make sure that you do not block any DLLs which are required for your system to run proper.

Windows installs a lot of DLLs which neither are marked to be a part of the operation system, the .NET Framework nor are all of these DLLs located in the windows system directory. Some DLLs might not even have a (valid) Microsoft signature. Because of that, none of the predefined special rules will cover such DLLs.

Example:

By default some Windows versions install Microsoft OneDrive. OneDrive is installed in the user profile and is not part of the operation system. Unfortunately OneDrive EXEs/DLLs get loaded by the Windows Explorer. The Windows Explorer will be terminated if such executables are not whitelisted in your rule set.

Best Practice:

We strongly recommend that you configure [Predictive Whitelisting](#) before you activate blocking DLLs. In any case start in simulation mode, validate the application control events and whitelist any DLLs your system expects to be allowed.

11.2.4 Predictive Whitelisting

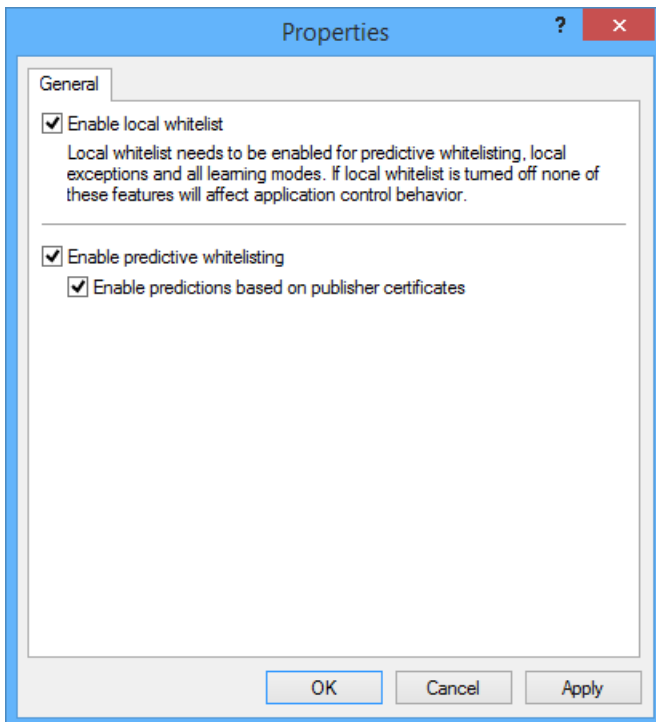
This chapter remains in the Administration Guide until further notice, but it will not be updated. Please note that the current documentation on application control can be found in a separate manual available at [DriveLock Online Help](#) starting with version 2020.1.

Machine learning is designed for computers in the industrial environments which control the manufacturing. In difference to computers in the administration these computers have a wide variety of software and require a local individual whitelist for Application Control. If a computer is switched into the learning mode all programs written or executed are added to the local whitelist (hash database) automatically. When the learning is completed the local whitelist becomes automatically active and only the programs "learned" can be executed now. To install or update programs at a later time the learning mode can be activated temporarily during the installation or the update.

You need a license for the DriveLock application control, which activates all functions of our established application control plus the advanced intelligent functions of predictive whitelisting.

Predictive and local whitelist

Open **Applications / Settings / Predictive and local whitelist**.



Enable local whitelist

If the rule is applied to a computer for the first time, the DriveLock Agent starts the learning mode and if done applies the local whitelist it has learned. If the local whitelist already exists the existing one will be used. Thus you may switch off predictive whitelisting to deactivate it and when you switch it on again the existing whitelist will be used again.

To check the state of the local whitelist [use Agent Remote Control](#), connect to a computer and open **Properties / Application Control**. Click **relearn local whitelist** to recreate the local hash database.

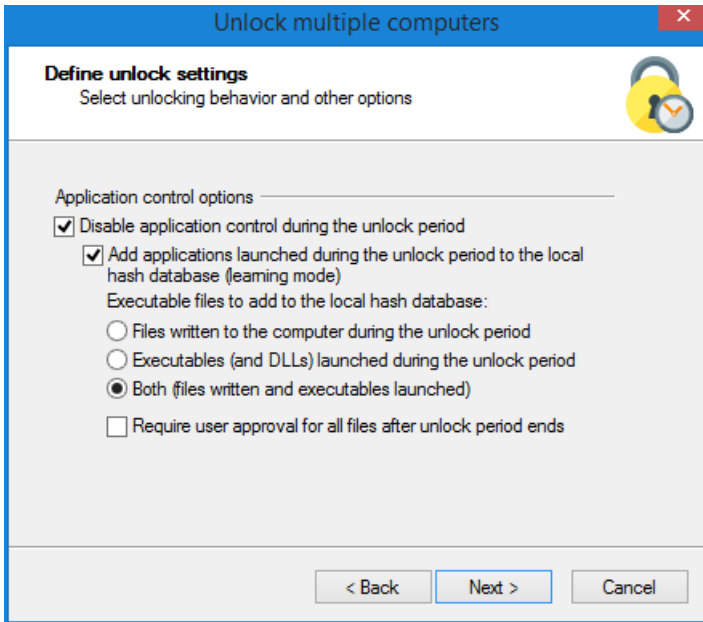
The local whitelist will be incrementally merged to the application database stored on the DriveLock Enterprise Service (DES). You can select hashed applications from the global application database, when you create a hash rule.

Enable predictive whitelisting

Predictions based on publisher certificates means, that DriveLock uses intelligent algorithms to recognize updates of installed software although the publisher certificate is not identical. DriveLock automatically adds such updates to the local whitelist.

Install or update new software with machine learning on

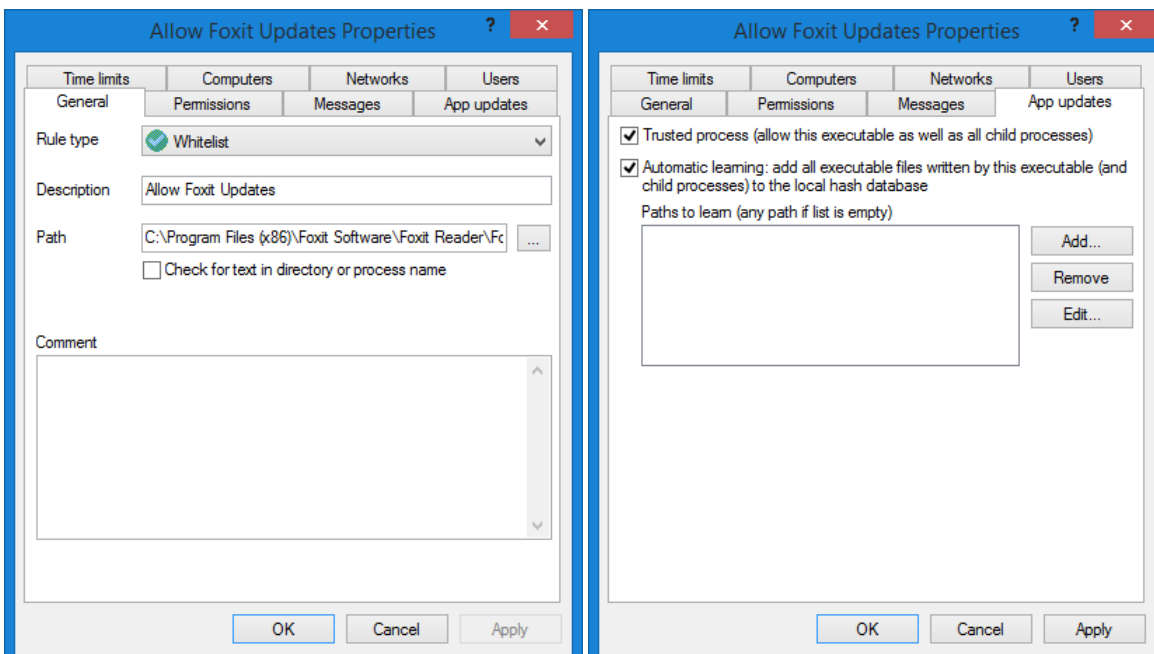
To install or update (if not recognized "predictive") programs while the local whitelist is active you have to temporarily unlock Application Control and switch learning mode to On. Select the appropriate settings (see example below) on the application control page of the unlock wizard. During the unlock period install or update the new software.



Autoupdate of software when machine learning is On

If you run software which includes an auto update like e.g. google chrome or foxit pdf reader and predictive whitelisting is active you have to configure rules for the auto update process to allow the process to be run and using the learning mode.

In your policy open **Applications / Application rules / Other rules / Filename or path rules / right click New / File path rule**. The example below make the updater process of the foxit reader (C:\Program Files (x86)\Foxit Software\Foxit Reader\FoxitUpdater.exe) to be a trusted process and enables machine learning for all executables written by FoxitUpdater and their child processes during the update.



11.2.5 Configuring Common Rule Settings

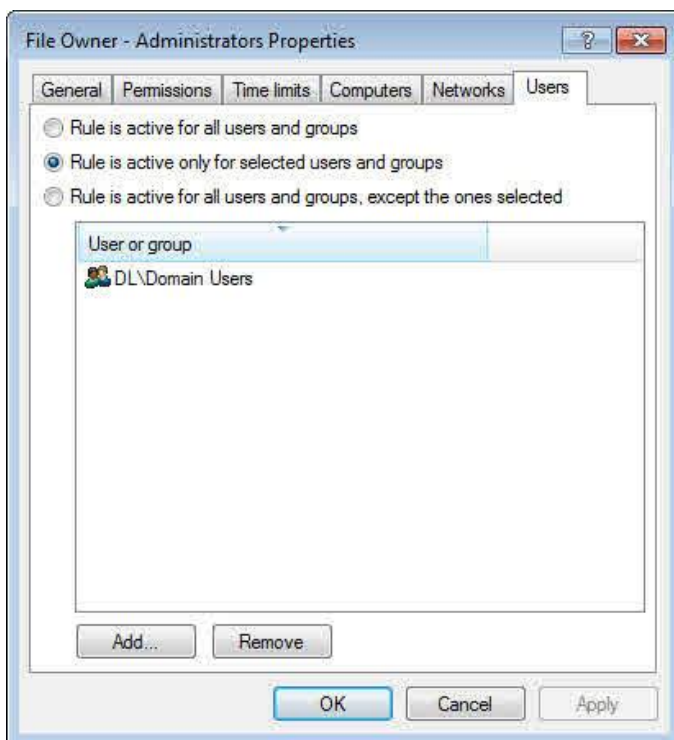
This chapter remains in the Administration Guide until further notice, but it will not be updated. Please note that the current documentation on application control can be found in a separate manual available at [DriveLock Online Help](#) starting with version 2020.1.

You can limit how and when application rules are applied by configuring the following settings. To save the changes, click **Apply** or **OK**.

11.2.5.1 Configuring User Settings

This chapter remains in the Administration Guide until further notice, but it will not be updated. Please note that the current documentation on application control can be found in a separate manual available at [DriveLock Online Help](#) starting with version 2020.1.

To configure which users the rule applied to, click the “Permissions” tab.



Select one of the following options:

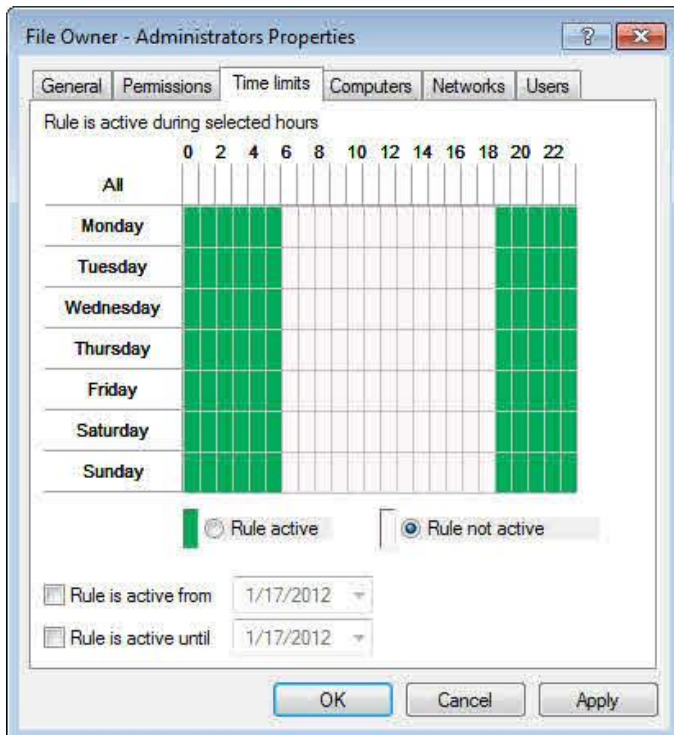
- *Everyone*: The rule applies to any user.
- *Defined users and groups*: The rule only applies to the users or groups you add to the list.

Click **Add** to add a user or group to the list. To remove a user or group from the list, select the user or group and then click **Remove**.

11.2.5.2 Configuring time limits

This chapter remains in the Administration Guide until further notice, but it will not be updated. Please note that the current documentation on application control can be found in a separate manual available at [DriveLock Online Help](#) starting with version 2020.1.

Click the **Time limits** tab to configure when a rule applies. If you want a rule to be active only during a certain time (for example only on Wednesdays, or on weekdays between 9 A.M. and 5 P.M.) you can specify time limits for the rule. You can also specify a start and end date for a whitelist rule.

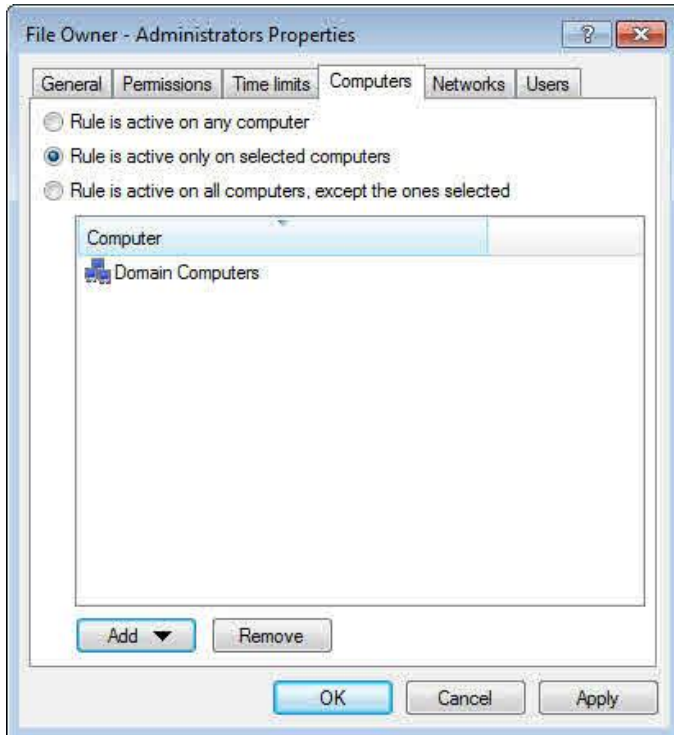


First click one or more rectangles to select the appropriate time block or blocks, an entire column or a row, and then select “Rule active” or “Rule not active”.

11.2.5.3 Configuring Computer Settings

This chapter remains in the Administration Guide until further notice, but it will not be updated. Please note that the current documentation on application control can be found in a separate manual available at [DriveLock Online Help](#) starting with version 2020.1.

Use the “Computers” tab to select the computers to which the rule is applied.



Select from the following options:

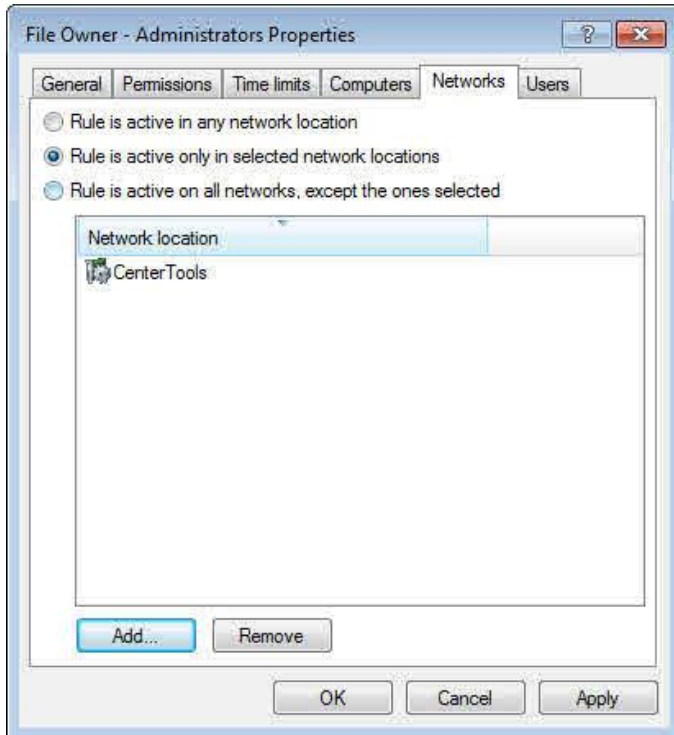
- Activate this rule on all computers
- Activate this rule only on the specified computers
- Exclude the specified computers from this rule

Click **Add** to add more computers to the list.

11.2.5.4 Configuring network limitations

This chapter remains in the Administration Guide until further notice, but it will not be updated. Please note that the current documentation on application control can be found in a separate manual available at [DriveLock Online Help](#) starting with version 2020.1.

Click the **Networks** tab to configure whether the rule is applied only in certain network locations. For more information about network locations, refer to the DriveLock Administration Guide.



Select from the following options:

- Activate this rule in all network locations
- Activate this rule only in the specified network locations
- Exclude specified network locations from this rule

Click **Add** to add network locations to the list.

11.3 Application Permissions

This chapter remains in the Administration Guide until further notice, but it will not be updated. Please note that the current documentation on application control can be found in a separate manual available at [DriveLock Online Help](#) starting with version 2020.1.

Use application permissions to accomplish the following results:

- Prevent an application (or process, script) from being started from within an allowed application, thus causing a potential danger to your system.
- Specify which type of access you want to grant a particular application (e.g. read or write access to files or the registry).

For this purpose, the following options are available. You can...

- determine the order (priority) for processing application permissions,
- specify the action to be taken when a particular application is accessed (for example, the application is blocked or not),
- determine whether an application permission can be passed on to child processes,
- specify different file and folder filters or

- specify script types that are allowed for running scripts.

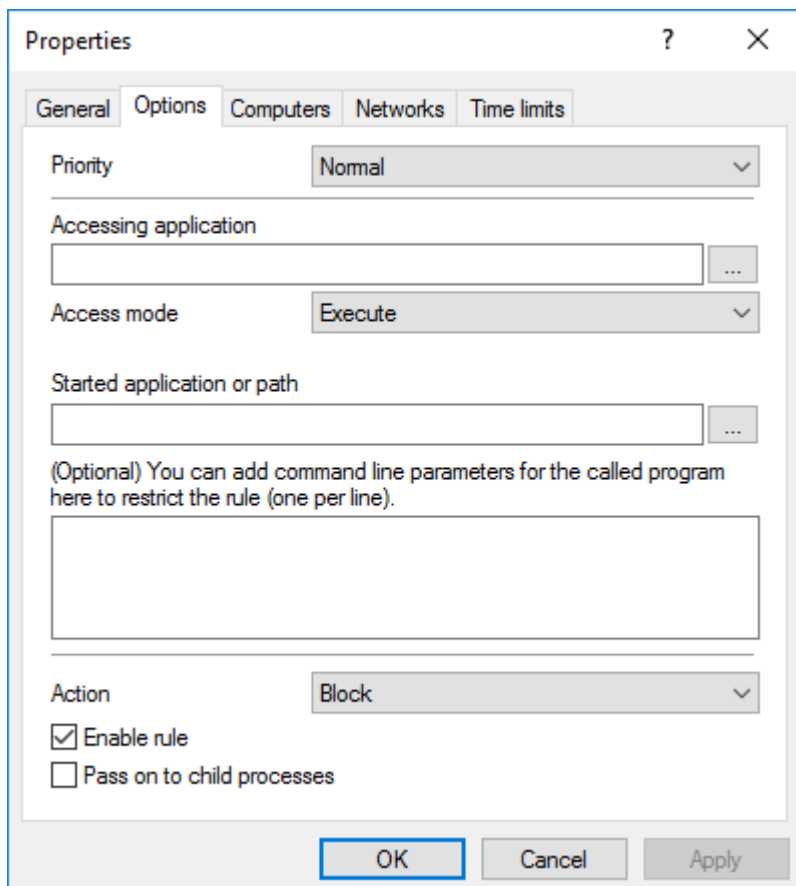
All application permissions can be arranged in the DriveLock Management Console in a user-defined folder structure.

11.3.1 Defining Application Permissions

This chapter remains in the Administration Guide until further notice, but it will not be updated. Please note that the current documentation on application control can be found in a separate manual available at [DriveLock Online Help](#) starting with version 2020.1.

Please proceed as follows:

1. Select **Application permissions** in the DriveLock Management Console and open the context menu.
2. Click **New** and then **Application permission**. If you select **Folder...** you can create a folder where you can store the application permissions you want to group.
3. The **Properties** dialog opens (see figure). Enter your settings. Find sample use cases below.
4. Start out with entering a description and a comment if required on the **General** tab.



The screenshot shows the 'Properties' dialog box with the 'General' tab selected. The dialog has a title bar with a question mark and a close button. Below the title bar are five tabs: 'General', 'Options', 'Computers', 'Networks', and 'Time limits'. The 'General' tab contains the following fields and controls:

- Priority:** A dropdown menu set to 'Normal'.
- Accessing application:** A text input field with a browse button ('...').
- Access mode:** A dropdown menu set to 'Execute'.
- Started application or path:** A text input field with a browse button ('...').
- (Optional) You can add command line parameters for the called program here to restrict the rule (one per line):** A large text area.
- Action:** A dropdown menu set to 'Block'.
- Enable rule:** A checked checkbox.
- Pass on to child processes:** An unchecked checkbox.

At the bottom of the dialog are three buttons: 'OK', 'Cancel', and 'Apply'.

11.3.1.1 Options in the Dialog

This chapter remains in the Administration Guide until further notice, but it will not be updated. Please note that the current documentation on application control can be found in a separate manual available at [DriveLock Online Help](#) starting with version 2020.1.

Note the following details on the different dialog options:

11.3.1.1.1 Priority

This chapter remains in the Administration Guide until further notice, but it will not be updated. Please note that the current documentation on application control can be found in a separate manual available at [DriveLock Online Help](#) starting with version 2020.1.

There are different **Priority** settings you can choose from on the **Options** tab.

Priority	Normal
Accessing application	Very low
	Low
	Normal
Access mode	High
	Very high

Note: Application permissions that are generally valid take a lower priority, special 'rules' a higher priority. The priorities vary according to the use cases. High-priority rules are processed before low-priority rules. The system checks the rules in the specified order, and if a rule matches, it is applied.

You can reduce or increase the priority in the DriveLock MMC.

Example: Combine rules, e.g. create a rule that allows the Browser to start Windows Media Player with high priority and another rule that forbids the Browser to start any other programs with a lower priority.

11.3.1.1.2 Accessing Application

This chapter remains in the Administration Guide until further notice, but it will not be updated. Please note that the current documentation on application control can be found in a separate manual available at [DriveLock Online Help](#) starting with version 2020.1.

Here you can either specify the full path or the name of the application you want to control, e.g. `C:\Program Files\Mozilla Firefox\firefox.exe` or just `firefox.exe`. You may use wildcards as well. Note that you can select [application collections](#) here, provided you've created such a list already. Open the chapter to find more information.

11.3.1.1.3 Access Mode

This chapter remains in the Administration Guide until further notice, but it will not be updated. Please note that the current documentation on application control can be found in a separate manual available at [DriveLock Online Help](#) starting with version 2020.1.

The access mode is a filter parameter for the application permission. Here you can define the action the accessing application should take.

11.3.1.1.4 Target

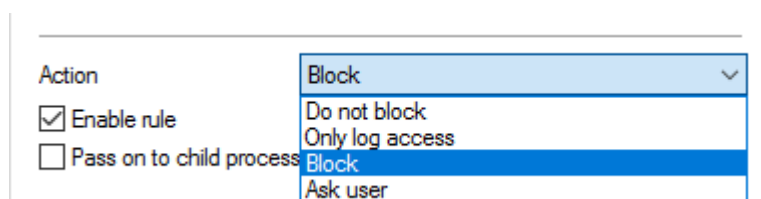
This chapter remains in the Administration Guide until further notice, but it will not be updated. Please note that the current documentation on application control can be found in a separate manual available at [DriveLock Online Help](#) starting with version 2020.1.

According to the access mode you select, you specify different information in the next text field; you can enter a path in all cases:

Access mode	Entry	Description
Execute	Started application	Enter the name of the application that is not supposed to be started (in this case, you would choose Block as an action). You can enter command line parameters optionally; they limit the application's execution even more. <i>Note that you cannot enter parameters in Windows XP!</i> Use case 1
Load DLL	DLL name	Enter the DLL that may only be loaded from a specific directory, for example. Use case 2
Run script	Script name	Enter the script you want to restrict from running. Use case 3 <i>Please note that DriveLock only considers the script types defined in the Script definition subnode.</i>
Read / Write file	File name	Enter a file name or a directory the accessing application is allowed (or not allowed) to read or write to. Use case 4 for read access Use case 5 for write access
Read / Write registry	Registry key	Enter the respective registry key (e.g. HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\), that may or may not be accessed (read or write access). You can use wildcards but you cannot enter values. Use case 6 <i>Please note that this access mode is only available for Windows 7 and higher!</i>

11.3.1.1.5 Action

This chapter remains in the Administration Guide until further notice, but it will not be updated. Please note that the current documentation on application control can be found in a separate manual available at [DriveLock Online Help](#) starting with version 2020.1.



- **Do not block:** Select this option if you do not require any further action. This setting corresponds to 'Allow'.

- **Only log access:** Select this option if you only want to monitor a specific folder, for example. This is well suited for logging file or registry accesses. An event is generated and displayed in the DriveLock Control Center. Use this option in simulation mode.
- **Block:** Choose Block if you want to prevent specific events depending on the access mode or the target. For example, this action prevents an application or script from running, or a DLL from loading. This is the default setting.
- **Ask user:** To let users decide which action they want to allow, select this option. Then, for example, it is up to the user to decide whether a Powershell script is run or not.

Please note that these actions provide additional protection for particularly vulnerable processes. 'Do not block' can still be blocked by a setting in a white or black list, but 'Block' overwrites the setting in a whitelist rule!

11.3.1.1.6 Activating and Inheriting

This chapter remains in the Administration Guide until further notice, but it will not be updated. Please note that the current documentation on application control can be found in a separate manual available at [DriveLock Online Help](#) starting with version 2020.1.

Note the following options:

- **Enable rule**

This option is checked by default, which means that the application permission is automatically set. You can quickly enable or disable these rules in the DriveLock Management Console without having to open the Properties dialog or delete the entire rule.

- **Pass on to child processes**

Select this setting so that your application permission is valid not only for the processes that meet the Accessing application requirement, but also for all children. This setting affects not only the immediate child processes, but all of their children as well.

This is particularly useful if you select Block as an action because it prevents your application permissions from being bypassed by starting another process.

Example: You create an application permission that prohibits your browser from starting Powershell. By selecting this option you can prevent Powershell from being started from the command line anyway (which is a child process).

11.3.1.1.7 Computers, Networks, Time Limits

This chapter remains in the Administration Guide until further notice, but it will not be updated. Please note that the current documentation on application control can be found in a separate manual available at [DriveLock Online Help](#) starting with version 2020.1.

On the **Computers** tab you specify the computers the application permission applies to.

For example, you could create an application permission for a specific computer group that s können beispielsweise eine Anwendungs-Berechtigung that contains computers running a newer version of the DriveLock Agent.

On the **Networks** and **Time Limits** tabs you specify where and when the application permission applies.

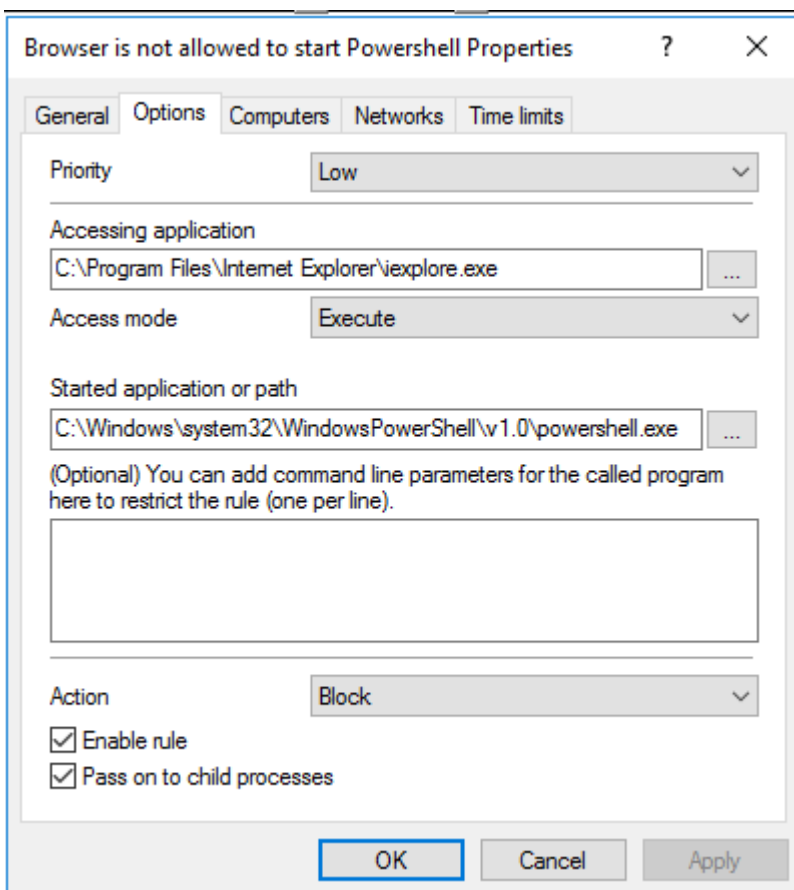
11.3.1.2 Use Cases

This chapter remains in the Administration Guide until further notice, but it will not be updated. Please note that the current documentation on application control can be found in a separate manual available at [DriveLock Online Help](#) starting with version 2020.1.

11.3.1.2.1 Use Case 1: Prevent PowerShell from Being Started

This chapter remains in the Administration Guide until further notice, but it will not be updated. Please note that the current documentation on application control can be found in a separate manual available at [DriveLock Online Help](#) starting with version 2020.1.

Scenario: You want to prevent Powershell from being started and possibly installing malware on the agent computers when the user opens a browser (here Internet Explorer).



1. Start out with entering a **Description** and a **Comment** if required on the **General** tab..
2. On the **Options** tab, enter the following information:
3. As this is a rather general 'rule', enter a low **Priority** for it.
4. Enter the full path to the `iexplore.exe` in the **Accessing application** text box.
5. Since you want to prevent PowerShell from starting from Internet Explorer, specify **Execute** as access mode.
6. Browse for a file or for a folder in the **Started application or path** text box; here it is the `powershell.exe` file.

It is useful to specify only the file name with blocking rules so that all instances can be included. When you specify the full path, please note that several program instances may exist, e.g. `powershell.exe` may be located in two different directories C :

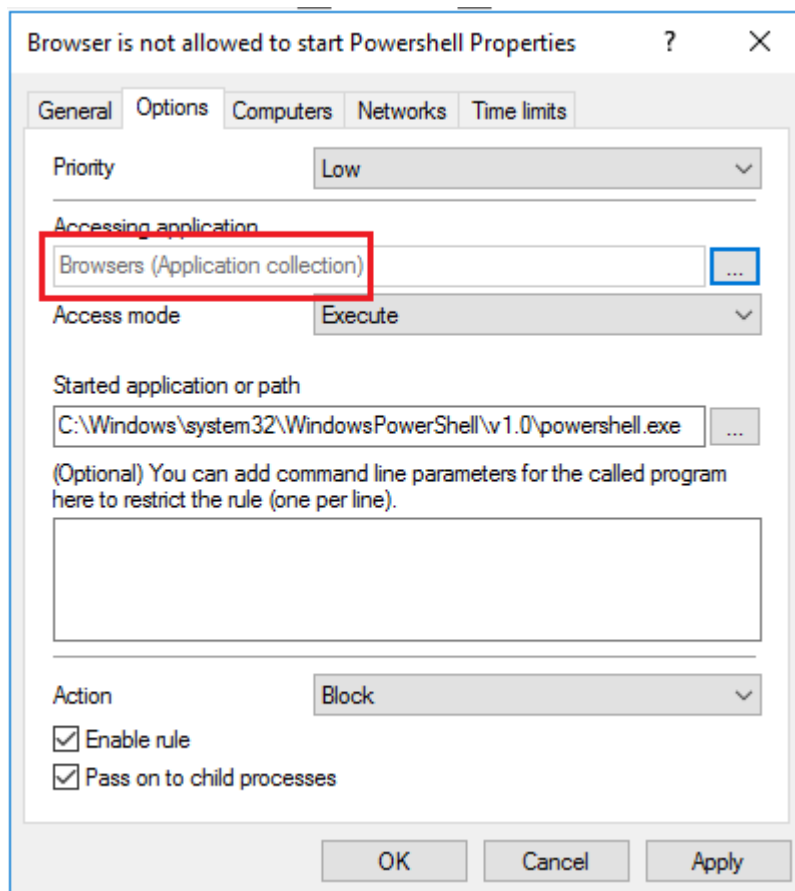
```
\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe or in C :
\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.
```

7. You want to **Block** PowerShell.
8. The check mark indicates that the rule is enabled.
9. Since you want to prevent the browser from starting `Powershell.exe` from the command line (`cmd.exe`) (which is a child process), tick **Pass on to child processes**.

Conclusion: Every time the `iexplore.exe` is called and it tries to start PowerShell, PowerShell will be blocked.

11.3.1.2.1.1 Use Case 1 with Application Collection

1. Proceed as described in Use Case 1.
2. Click the Browse button to select an application collection for the **Accessing application** text box. The application permission is now valid for all of the applications in the collection.



Conclusion: In this example, none of the browsers listed in the **Browsers (Application collection)** may start PowerShell.

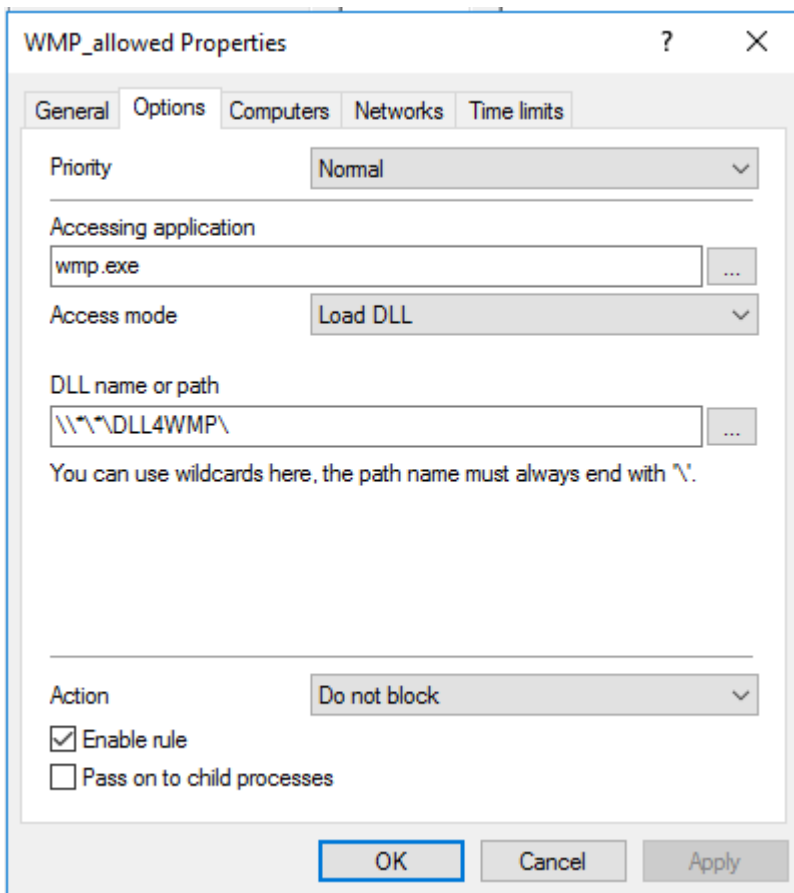
11.3.1.2.2 Use Case 2: Restrict Loading a DLL

This chapter remains in the Administration Guide until further notice, but it will not be updated. Please note that the current documentation on application control can be found in a separate manual available at [DriveLock Online Help](#) starting with version 2020.1.

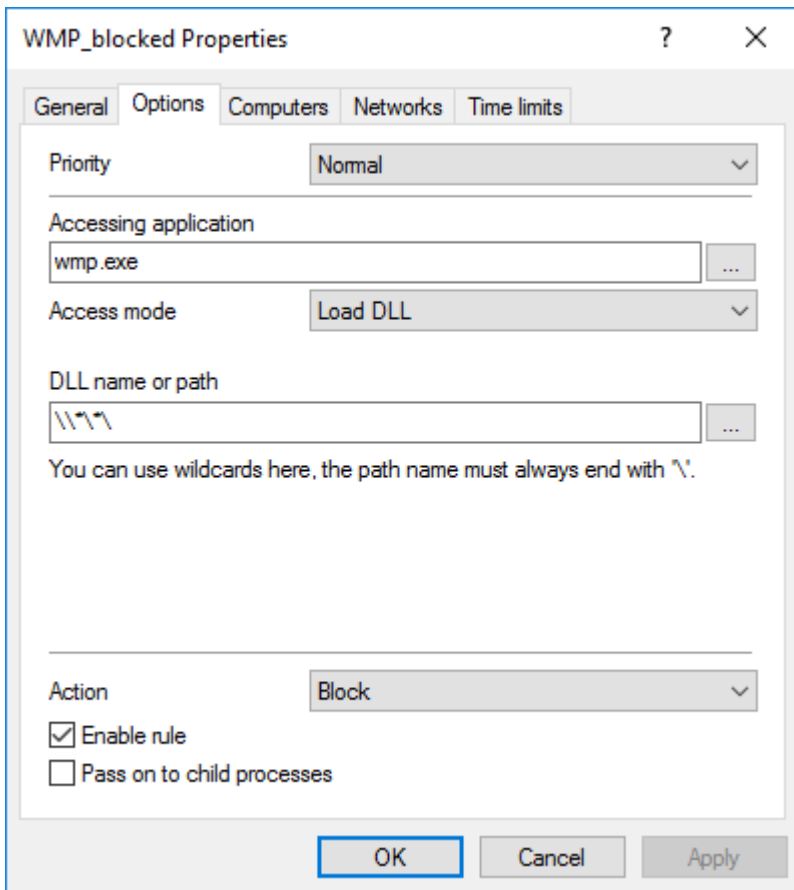
Scenario: You want to determine that DLLs may be loaded only from specified directories.

In this specific case, you want to prevent Windows Media Player from loading DLLs from network drives.

1. Create one application permission where you define that the Windows Media Player application `wmp.exe` may only load DLLs from `**\DLL4WMP\`.



2. Create a second application permission which blocks loading the DLL from all other directories on this network drive.

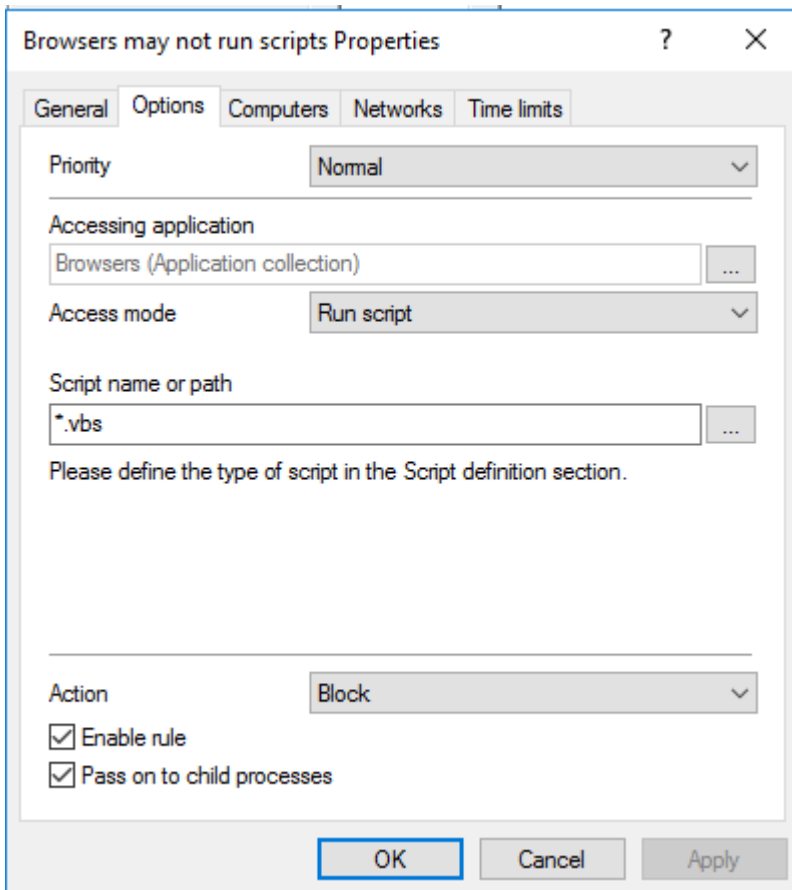


Here, you can set the same priority for both application permissions, since the rule with 'Do not block' (i.e. allow) overrides 'Block' by default.

11.3.1.2.3 Use Case 3: Run Scripts

This chapter remains in the Administration Guide until further notice, but it will not be updated. Please note that the current documentation on application control can be found in a separate manual available at [DriveLock Online Help](#) starting with version 2020.1.

Scenario: You don't want browsers to run VB scripts (*.vbs). You use the same application list as in use case 1.



Check the **Pass on to child processes** option to prevent VB scripts from being started from a child process (e.g. the cmd.exe).

Please remember to specify the script type and the corresponding file extensions in the **script definitions**.

11.3.1.2.4 Use Case 4: Read a Specific Directory

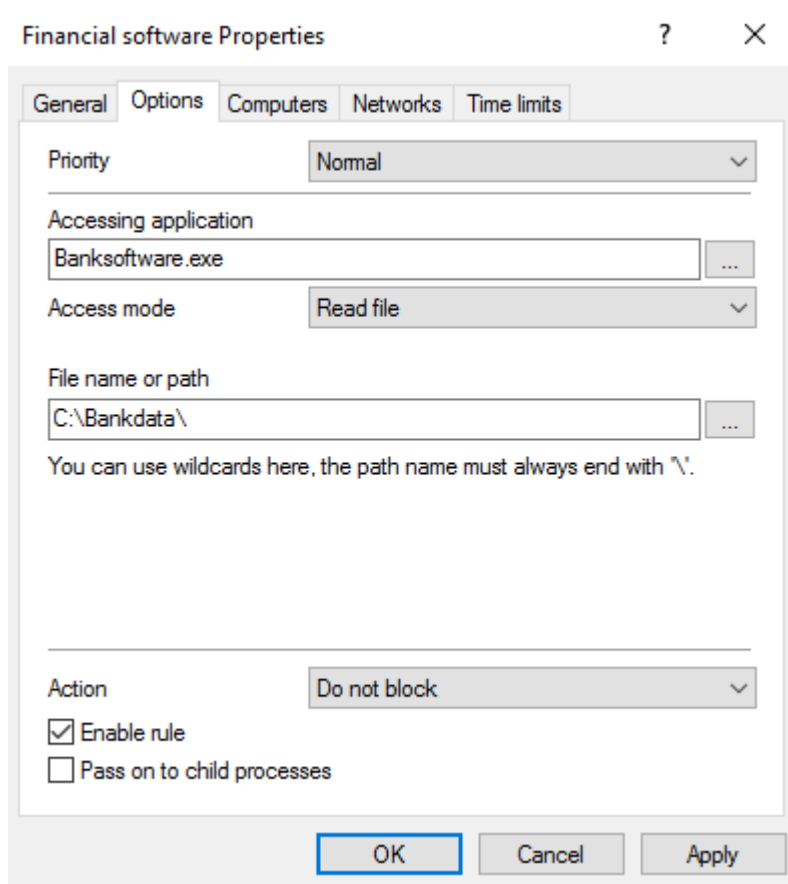
This chapter remains in the Administration Guide until further notice, but it will not be updated. Please note that the current documentation on application control can be found in a separate manual available at [DriveLock Online Help](#) starting with version 2020.1.

Scenario: You want to make sure that only your own financial software can read a specific directory. No other application should have read access to this directory.

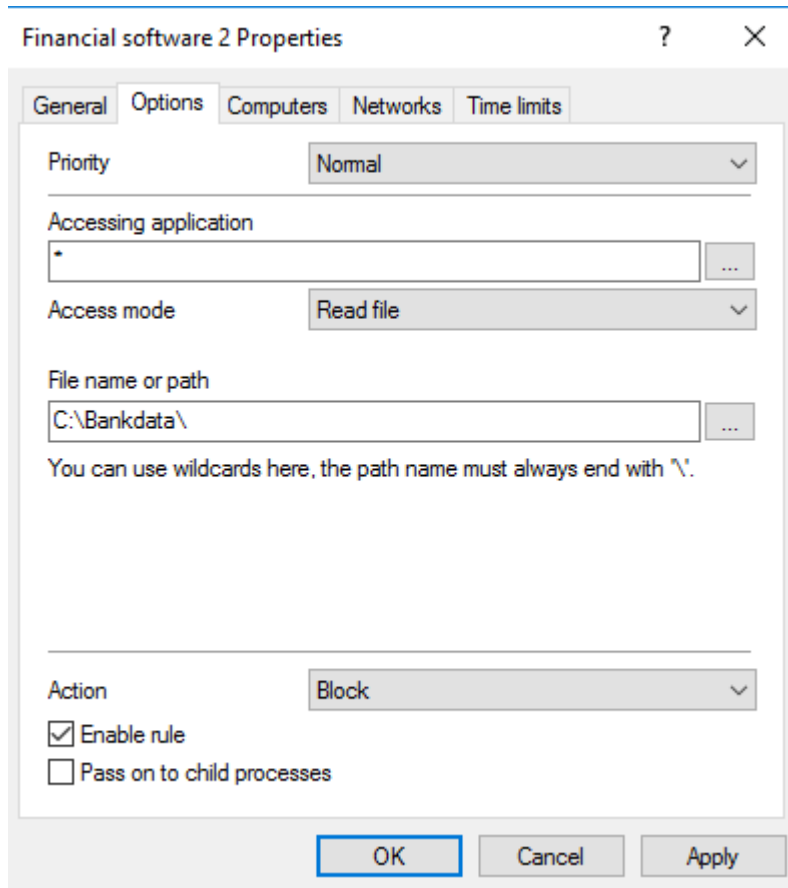
A security vulnerability in the browser could lead to malware gaining read access to this directory and thereby reading out your bank data. You have to prevent this.

Create two application permissions:

1. One application permissions allows your `Banksoftware.exe` application read access to the directory `C:\Bankdata\`.



2. Your second application permission has the wildcard * as **Accessing application**, so that no other application can access your C:\Bankdata\ directory.

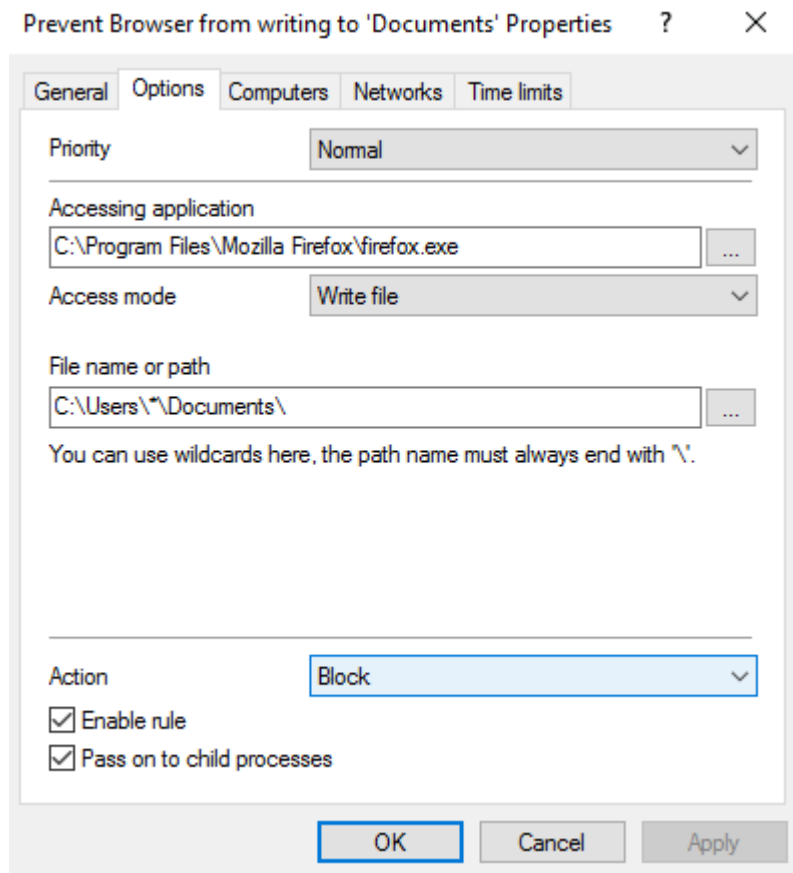


As far as priorities are concerned, the same applies as outlined in use case 2. 'Do not block' takes priority over 'Block'.

11.3.1.2.5 Use Case 5: Write to a Specific Directory

This chapter remains in the Administration Guide until further notice, but it will not be updated. Please note that the current documentation on application control can be found in a separate manual available at [DriveLock Online Help](#) starting with version 2020.1.

Scenario: You want to specify that a particular browser (here it's Mozilla Firefox) is not allowed to write to the Documents folder. Since you want to specify this for all users and not just for some users, use a wildcard.



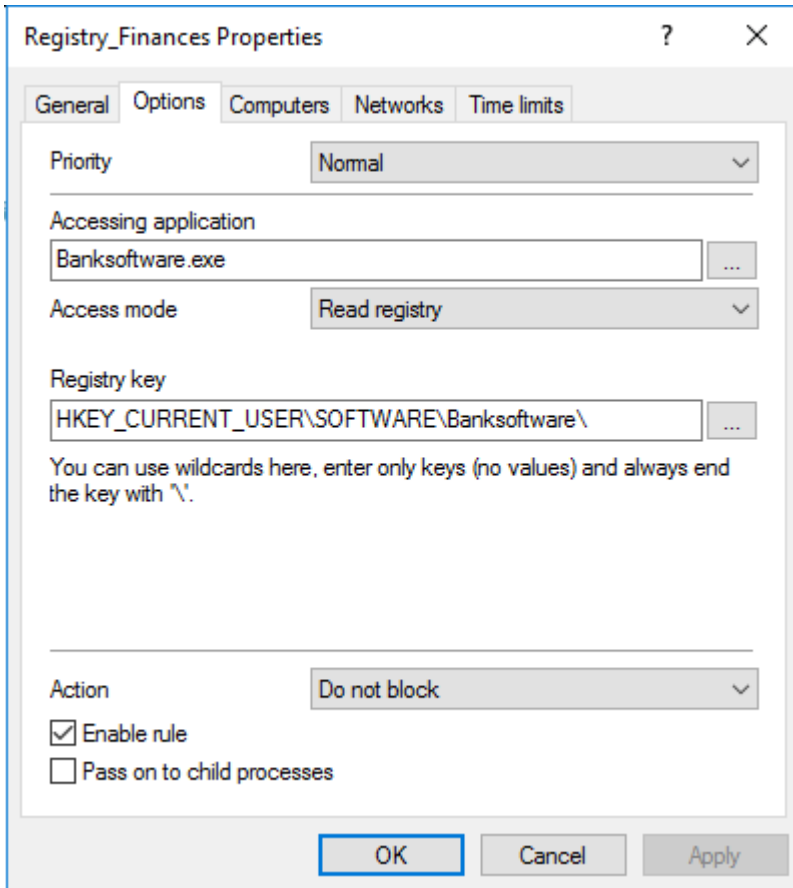
To prevent the browser from writing to the directory through child processes, check the **Pass on to child processes** option.

11.3.1.2.6 Use Case 6: Restrict Registry Access

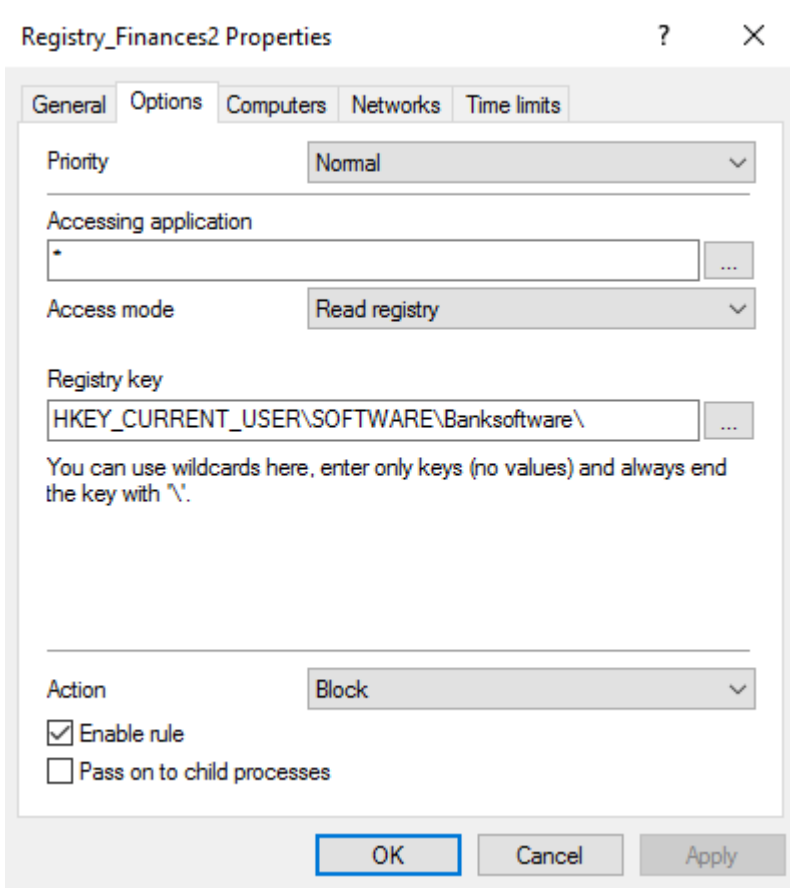
This chapter remains in the Administration Guide until further notice, but it will not be updated. Please note that the current documentation on application control can be found in a separate manual available at [DriveLock Online Help](#) starting with version 2020.1.

Scenario: You now want to control registry access for your financial software from use case 4. Create two application permissions so that only the `Banksoftware.exe` is allowed to read the registry in the specified key.

1. In the first case you allow the `Banksoftware.exe` application read access to the `HKEY_CURRENT_USER\SOFTWARE\Banksoftware\ registry` key.



2. In the second case you enter the wildcard * as **Accessing application**, so that no other application gets read access to the registry key.



11.3.2 Application Collections

This chapter remains in the Administration Guide until further notice, but it will not be updated. Please note that the current documentation on application control can be found in a separate manual available at [DriveLock Online Help](#) starting with version 2020.1.

Application collections are a set of applications that belong together in terms of subject or application. You can use them in the corresponding application permission.

Rather than creating individual rules for each application, you can create a rule for multiple applications (on the application collection) at once. This reduces your set of rules and keeps it simple.

Example: Three application permissions (rules) are to apply to three applications each:

- Rule no. 1 defines that no other applications are allowed to start from within a specific application.
- Rule no. 2 defines that applications are not allowed to write to a specific directory.
- Rule no. 3 defines that applications may only write text files to a specific directory.

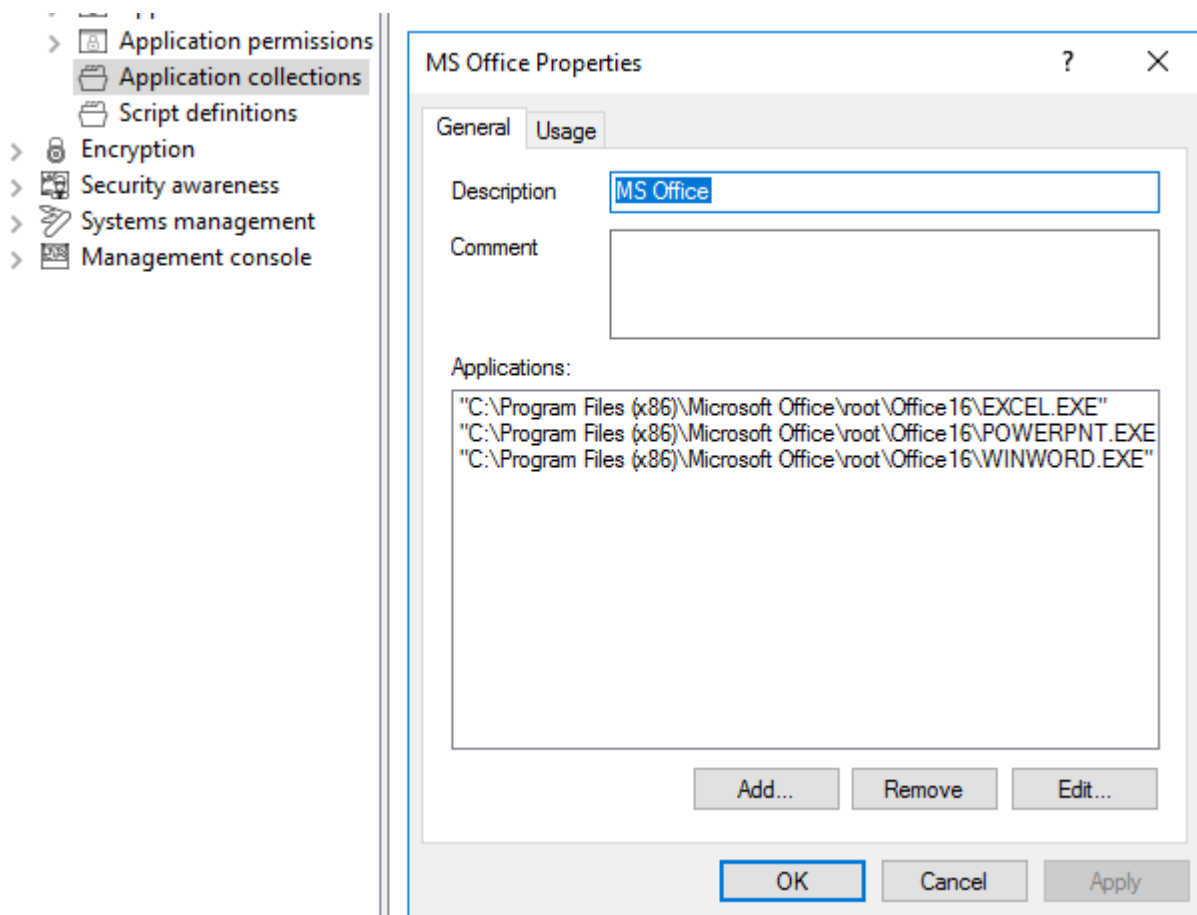
If you created individual rules for individual applications, you would have to create a total of 9 rules; by using collections, you reduce the number to 3 rules and 1 collection.

Create application collections based on the following example.

11.3.2.1 Application Collection for Microsoft Office

This chapter remains in the Administration Guide until further notice, but it will not be updated. Please note that the current documentation on application control can be found in a separate manual available at [DriveLock Online Help](#) starting with version 2020.1.

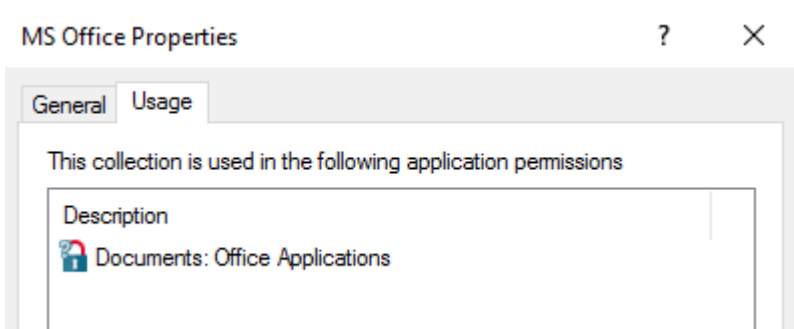
Scenario: You want to group different Microsoft Office applications in one application collection so that you can use it later in application permissions.



1. Select **Application collections** and open the context menu.
2. Click **New** and then **Application collection**.
3. Enter a **Description**, here **MS Office**.
4. If you want, add a comment.
5. Use the **Add** button to add the paths to the applications you want to include. You can remove applications from the collections later or edit the paths.
6. Save your collection and start using it in application permissions.

On the **Usage** tab you can see where your collection is being used.

In the figure below you can see that this list is being used in the **Documents: Office Applications** application permission.



11.3.3 Script Definition

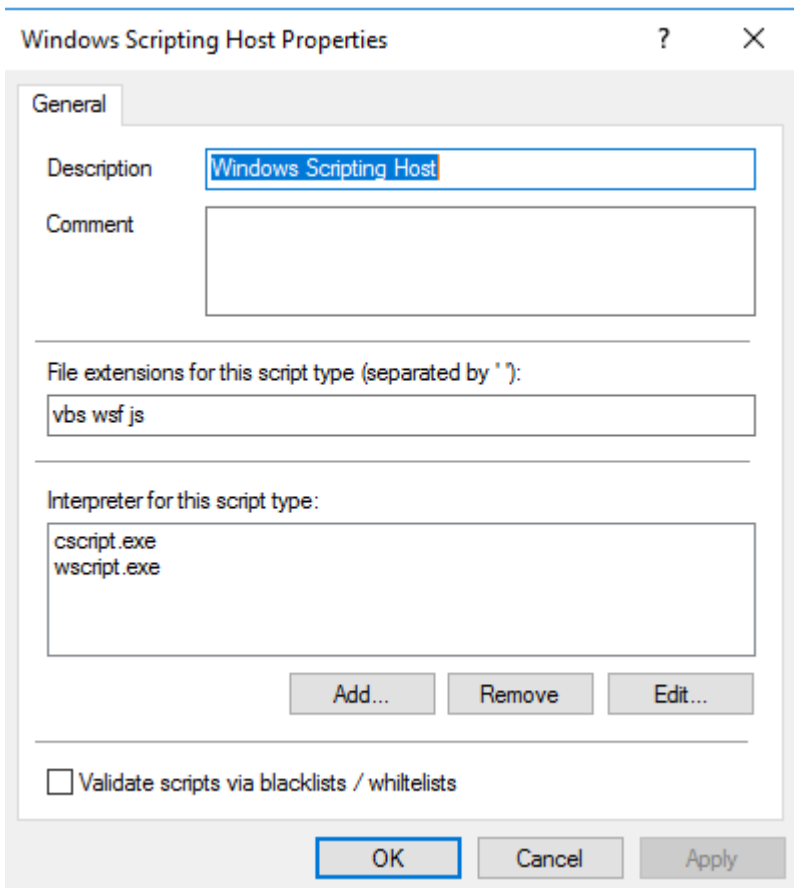
This chapter remains in the Administration Guide until further notice, but it will not be updated. Please note that the current documentation on application control can be found in a separate manual available at [DriveLock Online Help](#) starting with version 2020.1.

To use the **Run script** access mode you have to define the relevant script types. This definition tells DriveLock's application control feature which file accesses it should interpret as script execution.

Please proceed as follows:

1. Open the context menu of **Script Definition**.
2. Click **New** and enter your definition in the following dialog.

The example below defines the **Windows Scripting Host**.



- Enter the extensions that apply to the script in the **File extensions for this script type** text box. Simply enter a space between the extensions.

- Enter the interpreters that can interpret your script in **Interpreter for this script type**. One per row.
- With the **Validate scripts via blacklists / whitelists** option, you can specify to have scripts checked in blacklists or whitelists in the same way as DLLs or EXE files. For more information on blacklisting and whitelisting, see the corresponding chapters.



Part XII

DriveLock Disk Protection



12 DriveLock Disk Protection

DriveLock Disk Protection is a central component of DriveLock DiskProtect and in earlier versions was also referred to as DriveLock Full Disk Encryption (FDE).

In today's computing environment, hard disk drives have become mass repositories of proprietary information. The widely used Windows operating system provides adequate data privacy for stand-alone or networked computers in most operating environments. However, Windows does not sufficiently protect the data on a computer's hard disk against disclosure when the computer is lost or stolen. Unless additional data protection measures are taken, anyone with access to the hard drive can read all data on it.

To mitigate this data security risk, DriveLock has integrated a system security and data encryption solution.

DriveLock Disk Protection can be used for the following BIOS versions and operating systems:

- Legacy BIOS: Windows 7 SP1, Windows 8.1 and Windows 10, either 32-bit or 64-bit
- UEFI BIOS: Windows 10, only 64-bit

DriveLock Disk Protection (FDE) provides the following functionality:

Disk Encryption

DriveLock Disk Protection can automatically encrypt and decrypt multiple hard disk partitions. All data encryption is transparent to the end user, the operating system and applications. When encrypted data is being read, DriveLock FDE decrypts it "on the fly"— the data immediately becomes available to the user or applications. All data written to the disk is automatically encrypted. As a result, normal system operations remain unaffected.

Pre-boot User Authentication (PBA)

DriveLock Disk Protection authenticates users before the operating system starts. Upon successful authentication the pre-boot process retrieves a computer-specific key that is used to decrypt the disk sectors that store the operating system files and all other files on the encrypted drive as they are accessed. Users can authenticate using their Windows logon credentials, smartcards or tokens.

After successful pre-boot authentication, the disk key is decrypted and used to provide access to the disk so that the operating system can start. DriveLock Disk Protection maintains its own *Pre-boot User Database* to authenticate users.

The Pre-boot User Database has the following characteristics:

- Maximum number of credential (users or certificates) — 2,000
- User name length — 1 to 20 characters
- Password length — up to 127 **case-sensitive** characters (same maximum length as Windows passwords, no minimum length)

DriveLock Disk Protection can authenticate users with passwords on standalone computers and computers belonging to a Windows domain. Smartcards and tokens with a PIN can also be used to authenticate.

Single sign-on or manual Windows authentication

DriveLock Disk Protection provides automatic Windows domain user authentication following successful pre-boot authentication so users don't need to authenticate twice. As an alternative to the single sign-on mode, you can configure DriveLock Disk Protection to present the standard Windows authentication screen each time the operating system starts, allowing the user to first authenticate during the pre-boot phase, and then manually authenticate using different Windows credentials.

You can configure DriveLock Disk Protection to *automatically* log users on to Windows using their domain or local Windows credentials following successful pre-boot authentication. This chaining of authentication processes is called *single sign-on*. Single sign-on simplifies the user experience as users only need to authenticate once.

Emergency pre-boot logon Recovery and token logon

Disk Protection provides emergency logon procedures to allow smartcard / token or Windows domain users to authenticate once at the pre-boot logon, e.g. if they forget their password or PIN.

Prior to installing DriveLock Disk Protection, you must create a recovery file set. These files are required to perform recovery of disk data in case of a disaster and to perform emergency logon procedures. The recovery file set consists of the following files:

- **Master Security Certificate** — The **DLFDEMaster.cer** file contains the Master Security Certificate with the public key that is used to encrypt a backup copy of the computer's disk encryption key. The **DLFDEMaster.pfx** file also contains the corresponding private key that is required to gain access to this disk encryption key. Access to this key is required if you need to decrypt a damaged hard disk. The **DLFDEMaster.pfx** file is intended to be private. It should be securely stored and only accessible to individuals who are authorized to perform disaster recovery. The corresponding **DLFDEMaster.cer** file contains the public key component of the Master Security Certificate. It does not contain confidential information and is used during each DriveLock FDE installation.
- **Recovery Support Certificate** — The **DLFDERecovery.cer** file contains the **Recovery Support Certificate** with a public key that is used to control access to the pre-boot authentication database. The **DLFDERecovery.pfx** file contains the corresponding private key that is required to gain access to the pre-boot authentication database when creating emergency logon credentials for users. The **DLFDERecovery.pfx** file is intended to be private. It should be securely stored and only accessible to individuals who can perform password recovery, such as helpdesk and support personnel. The corresponding **DLFDERecovery.cer** file contains the public key component of the Recovery Support Certificate. It does not contain confidential information and is used during each DriveLock FDE installation.
- **Recovery Envelope** — A unique **RecoveryEnvelope.env** file is created for each client computer when you install DriveLock FDE. It contains recovery data that is specific to the computer and is required for emergency logon procedures or disk decryption, in conjunction with the appropriate private key. If you save the recovery envelop to a shared folder instead of the DriveLock database, the client computer name is included in the file name in the following format: **<computer name>_RecoveryEnvelope.env**.

For standalone installations, disaster recovery preparation begins with periodic system data backups. DriveLock FDE creates recovery files that can be used to later decrypt a disk that has become damaged or that cannot be accessed normally for other reasons. These keys are sent to the central DES and should not be backed up on the client system as such. The backup files that are created and used in combination with the main certificate (MSC) are used for disk recovery.

DriveLock Disk Protection includes a command line recovery tool to perform disaster recovery tasks such as data decryption. This recovery tool is included in the DriveLock Disk Protection installation and is generally used only by system administrators.

Disaster Recovery and Administration Tools

Various system administration functions not related to DriveLock Disk Protection may at times require an unattended computer restart, followed by automatic pre-boot authentication. DriveLock Disk Protection enables this functionality by using a special user account. A command line program is required to use this functionality.

Disk Protection provides tools for decrypting data on a damaged hard disk in the event of a hard disk failure.

DriveLock Disk Protection provides a mechanism for helpdesk personnel to enable logon for users who can't access their authentication credentials. This may include users who have misplaced their smartcard or token or who forgot their Windows password.

DriveLock Disk Protection provides automated procedures for handling these pre-boot authentication scenarios.

12.1 Preparing to Deploy DriveLock Disk Protection

Review the sections below and ensure that you have performed the appropriate procedures prior to installing DriveLock Disk Protection.

Best practices for preparing to deploy DriveLock Disk Protection include:

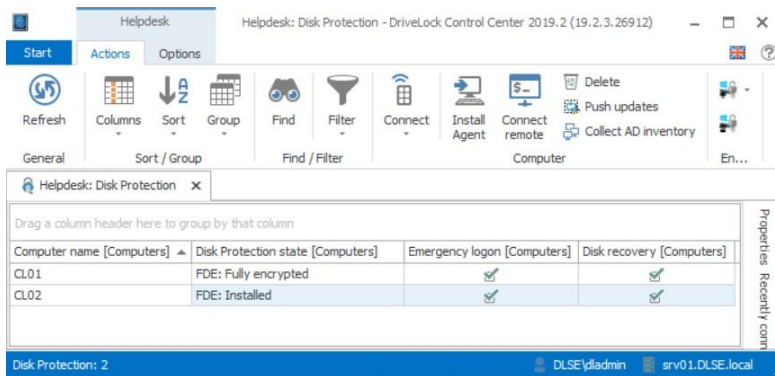
- Defragment all drives that will be encrypted by DriveLock Disk Protection.
- Repair any existing disk errors.
- Ensure that the data storage on each computer is well organized and that no further rearranging of any partitions will be required later. Use Windows Disk Management as needed to configure all partitions and disk mirroring before installing DriveLock Disk Protection.
- Run `CHKDSK /f` and the hard disk manufacturer's diagnostic utility to ensure file system health on all drives you intend to encrypt. Repair any bad sectors, as DriveLock Disk Protection cannot encrypt such sectors.
- Back up all important data prior to disk encryption.
- If you are using the DriveLock Application Launch Filter in whitelist mode, deactivate it during the Disk Protection installation to prevent the blocking of required applications.

Utilities provided by a hard disk's manufacturer are typically the most robust tools for repairing disk errors.

DriveLock recommends that the Disk Protection deployment steps are performed in the following order:

1. **Plan for recovery operations:** Become familiar with the recovery mechanism, recovery scenarios and learn about the methods for securely storing recovery files. Making recovery files available is required to restore access to a computer when a user has forgotten a pre-boot password or when a hard disk has become damaged.
2. **Encrypt hard disks in a test environment:** The DriveLock Disk Protection components have been extensively tested to work on a wide range of desktop and laptop computers.
To ensure a smooth deployment in your production environment, we recommend that you first test Disk Protection on test computers that are representative of the computer models used in your organization. Such testing may reveal, for example, possible incompatibility with old or brand-new hardware.
3. **Generate and back up the encryption certificates:** Before using Disk Protection you must generate the central certificates that are needed for all recovery scenarios. The certificates are automatically stored by DriveLock. Because of the importance of these certificates for recovery operations, DriveLock recommends that you also manually back up these certificates to an additional secure location.
4. **Determine the deployment schedule:** Create a plan for deployment before starting the process. To minimize downtime and to ensure adequate support for users, a deployment in several stages may be appropriate.
5. **Deploy Disk Protection by configuring the deployment and recovery options in your DriveLock policy:** You can initiate the deployment by installing the Disk Protection component on the client computers without enabling pre-boot authentication or encryption. After successful installation each client computer generates its own recovery data and stores it as a "recovery envelope". This recovery envelope is required for all recovery operations.

6. Review the Event Log to confirm that the installation succeeded and that the recovery information was uploaded to the DriveLock database or saved in a central location: Ensure that the recovery envelope files for all computers are stored centrally and not on the client computers themselves. Storing the recovery envelopes in the DriveLock database automates this process. When you store recovery envelopes in the DriveLock database you can use the DriveLock Control Center to easily confirm whether the recovery envelopes have been created and can be retrieved.



7. Configure and activate pre-boot authentication: Pre-boot authentication is the only point where users notice that Disk Protection has been deployed. When pre-boot authentication has been enabled, users are prompted for authentication immediately after the computer is started and the logon screen that is displayed looks different from the Windows logon screen. Before activating pre-boot authentication you should create a central emergency logon account if you intend to use this account for scenarios such as initial authentication or technical assistance. An emergency logon account does not need to be a domain account.
8. Help users become familiar with pre-boot authentication: Users may require some initial training to use the new logon mechanism. Also, users and administrators should become familiar with the procedures for emergency logon recovery.
9. Configure and activate encryption: Activation of disk encryption should be the last step of the Disk Protection deployment. Once encryption has been activated, each client computer starts encrypting the hard disk in the background. This process requires some system resources, and until encryption is complete regular computer operations will be slower than normal. Users may notice this impact on performance, particularly when running applications that require high disk or processor resources. When the encryption process has completed, the client computer generates a unique disk recovery file that is required to decrypt any data on the drive.
10. Verify that all data recovery files (backup.zip) have been sent centrally to the DES or stored in a file: Ensure that the disk recovery files for all computers were generated and stored in a location other than on the client computer itself. Storing the recovery disk recovery files in the DriveLock database automates this process. When you store these files in the DriveLock database you can use the DriveLock Control Center to easily confirm whether the files have been created and can be retrieved.

The new DriveLock Operations Center will not display all information relevant to Disk Protection properly yet, so please use the DriveLock Control Center for Disk Protection.

DriveLock strongly recommends backing up the recovery data. Recovery files are required to perform a recovery process for a computer where Disk Protection is installed. If you use the DriveLock Enterprise Service to store recovery data, back up the entire DES database (default).

12.2 Basic Configuration of Disk Protection

At first, you need to configure some basic settings:

- Licensing
- Generating the recovery keys

Open the **Encryption** node in the policy and scroll to the bottom of the Taskpad view until you see the **Disk Protection** pane in full.

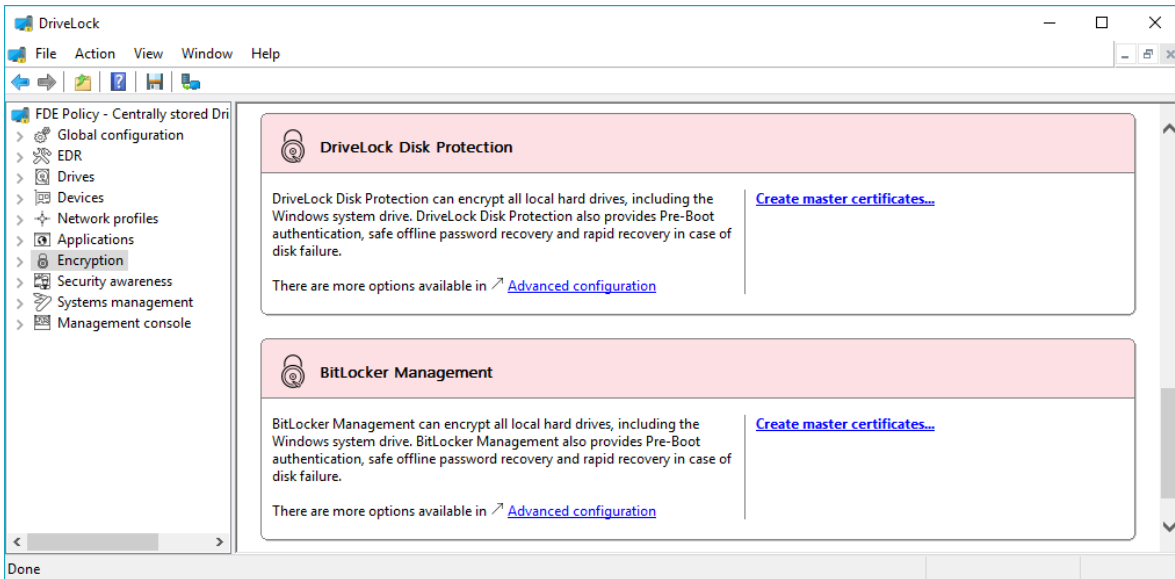
12.2.1 Creating Recovery Keys

Before you can install DriveLock Disk Protection, you need to create central encryption certificates and the corresponding keys. These certificates are required to perform key recovery and emergency logon procedures. The following certificates are required:

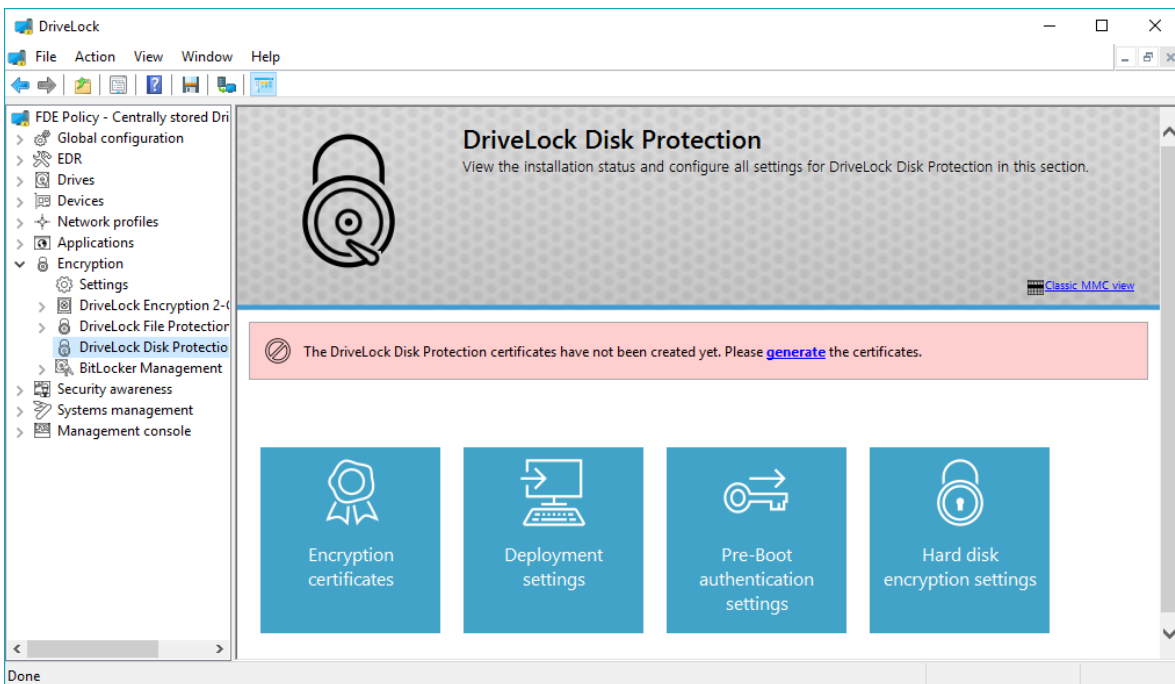
- *Master Security Certificate* — The **DLFDEMaster.cer** file contains the Master Security Certificate with the public key that is used to encrypt a backup copy of the computer's disk encryption key. The **DLFDEMaster.pfx** file also contains the corresponding private key that is required to gain access to this disk encryption key. Access to this key is required if you need to decrypt a damaged hard disk. The **DLFDEMaster.pfx** file is intended to be private. It should be securely stored and only accessible to individuals who are authorized to perform disaster recovery. The corresponding **DLFDEMaster.cer** file contains the public key component of the Master Security Certificate. It does not contain confidential information and is used during each DriveLock FDE installation.
- *Recovery Support Certificate* — The **DLFDERecovery.cer** file contains the Recovery Support Certificate with a public key that is used to control access to the pre-boot authentication database. The **DLFDERecovery.pfx** file contains the corresponding private key that is required to gain access to the pre-boot authentication database when creating emergency logon credentials for users. The **DLFDERecovery.pfx** file is intended to be private. It should be securely stored and only accessible to individuals who can perform password recovery, such as helpdesk and support personnel. The corresponding **DLFDERecovery.cer** file contains the public key component of the Recovery Support Certificate. It does not contain confidential information and is used during each DriveLock Disk Protection installation.

Without the encryption keys and the corresponding passwords you will not be able to recover any data or help users who don't have access to their credentials log on.

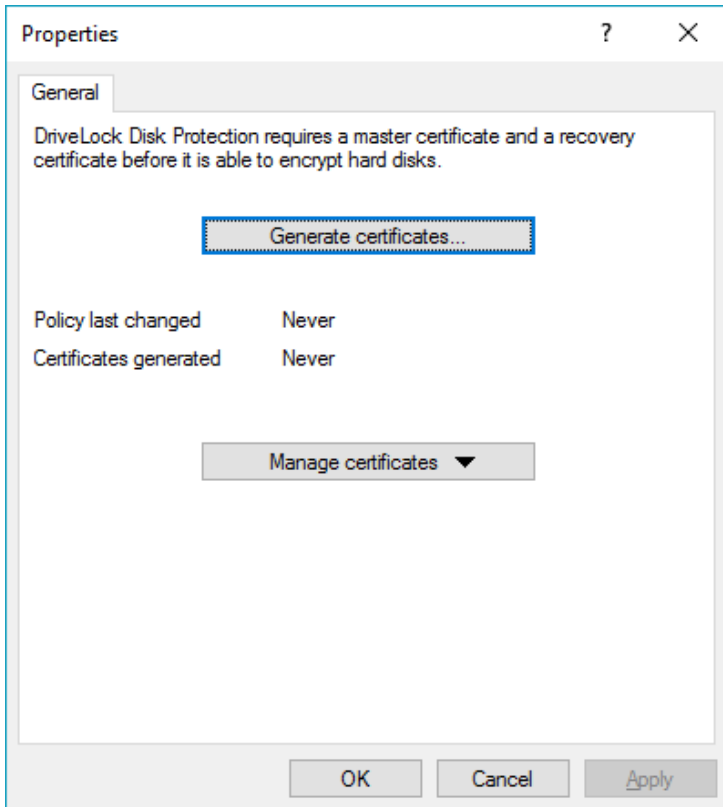
When you start **DriveLock Disk Protection** for the first time the encryption certificates and keys have not been created yet.



Click **Create master certificates** to create new encryption certificates and keys. This starts the wizard where you can create the certificates.



You can also start the wizard by clicking **DriveLock Disk Protection** and then **Encryption certificates**.

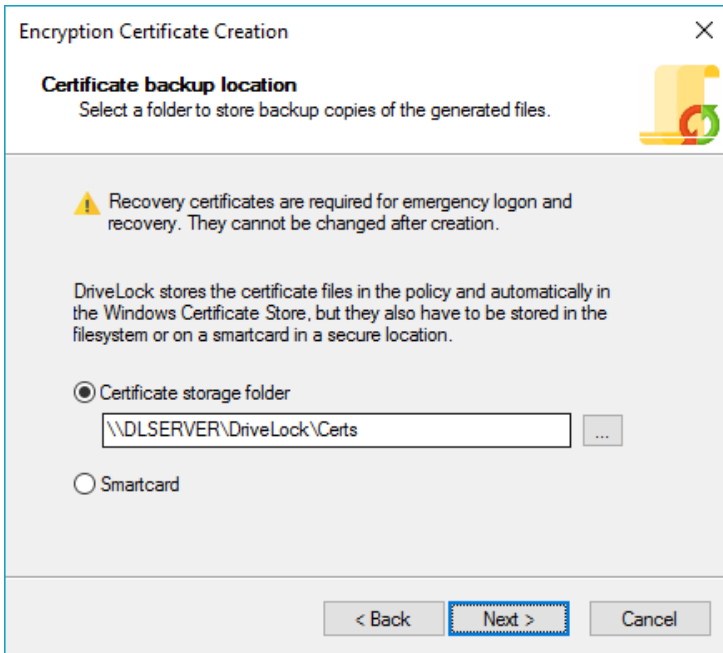


Click **Generate certificates** to create new encryption certificates and keys.

Create the encryption keys



Click **Next**.



Encryption Certificate Creation

Certificate backup location
Select a folder to store backup copies of the generated files.

Warning: Recovery certificates are required for emergency logon and recovery. They cannot be changed after creation.

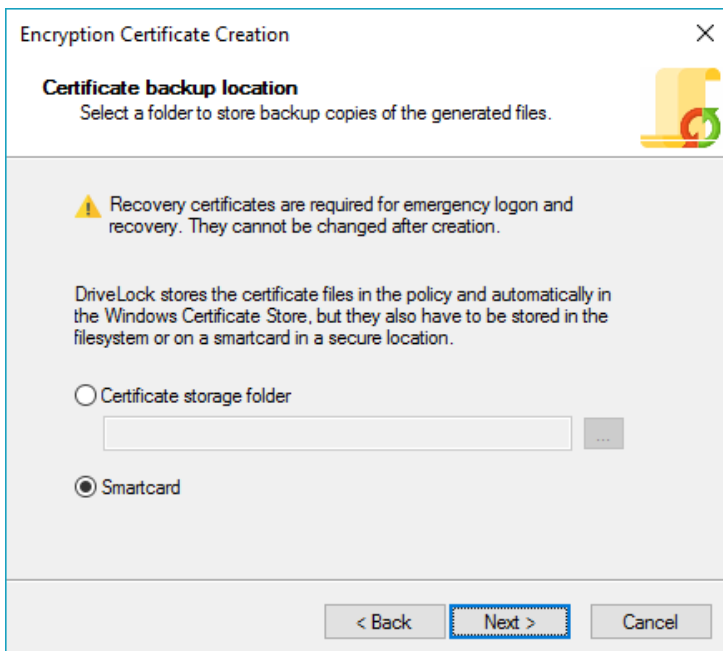
DriveLock stores the certificate files in the policy and automatically in the Windows Certificate Store, but they also have to be stored in the filesystem or on a smartcard in a secure location.

Certificate storage folder
\\DLSERVER\DriveLock\Certs

Smartcard

< Back **Next >** Cancel

Specify the location to save the certificate files to or select a smartcard as the storage location.



Encryption Certificate Creation

Certificate backup location
Select a folder to store backup copies of the generated files.

Warning: Recovery certificates are required for emergency logon and recovery. They cannot be changed after creation.

DriveLock stores the certificate files in the policy and automatically in the Windows Certificate Store, but they also have to be stored in the filesystem or on a smartcard in a secure location.

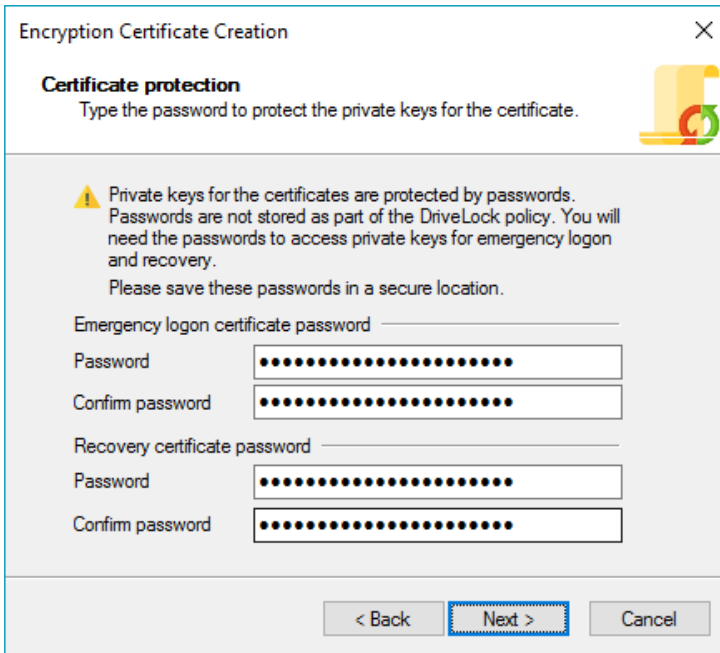
Certificate storage folder

Smartcard

< Back **Next >** Cancel

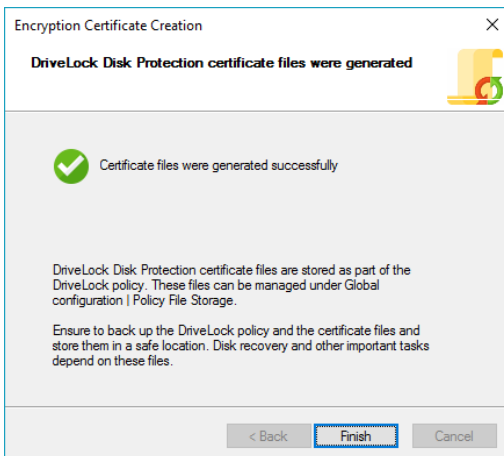
Click **Next**. If you selected a smartcard, you will be prompted to insert and select the smartcard.

Store the encryption certificate files and their passwords in a safe location, as they are needed in conjunction with the Recovery Files Set for user password and data recovery. Without the certificate files and their passwords, data recovery will not be possible.



Type the passwords for both the master and recovery certificates and confirm each password by typing it again. Click **Next** to continue.

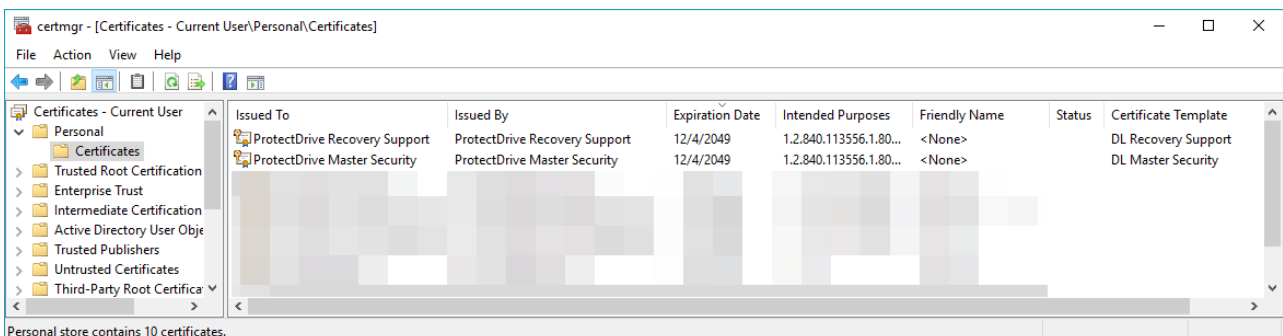
The wizard notifies you when it has finished creating the certificates. If you selected a smartcard, you will be prompted for the PIN that is required to access the smartcard.



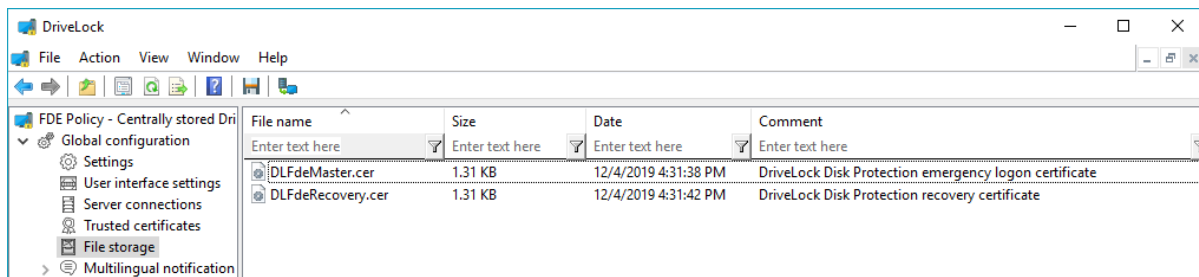
Click **Finish**.

When the encryption certificates have been created the DriveLock Management Console displays the creation time and date.

The certificates are also added to the private certificate store of the user who created them.



The two public keys are also stored in the DriveLock File Storage.

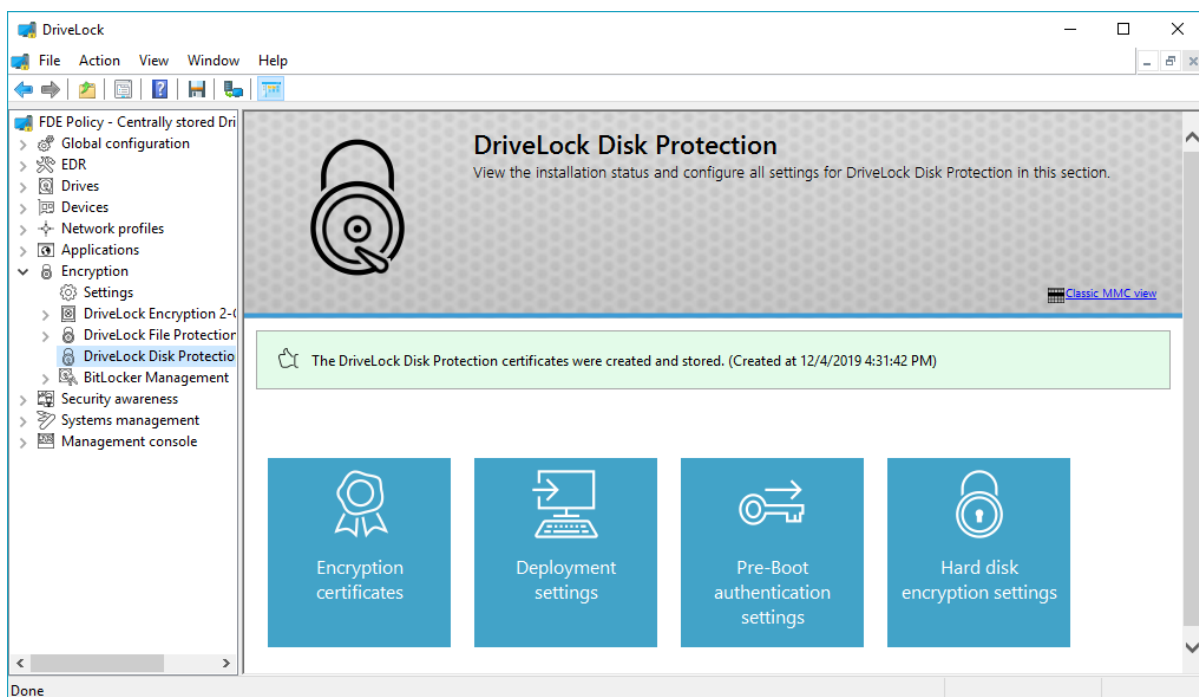


Once the certificates have been created and DriveLock Disk Protection has been installed on client computers, you can no longer create new certificates. The reason for this is to prevent the old certificates from being overwritten, which would make recovery impossible.

If you cancelled the certificate creation wizard or if the certificate creation failed, DriveLock displays an error message and you must start the certificate creation process again.

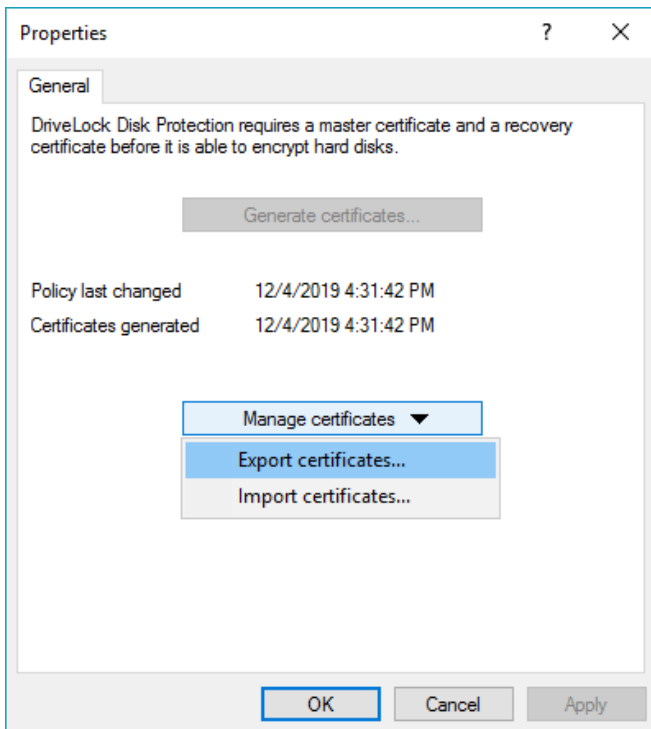
12.2.2 Exporting and Importing Encryption Certificates

After you have created the encryption certificates you can export the public keys from the DriveLock Policy File storage.



In the DriveLock Management Console, click **Encryption certificates**.

Only import the master and recovery certificates if you are certain that this is the appropriate action. For example, you might install certificates when restoring a policy or then cloning a policy. Changing the certificates after they have been used to install and configure Disk Protection on client computers is not supported and may prevent you from performing most recovery tasks

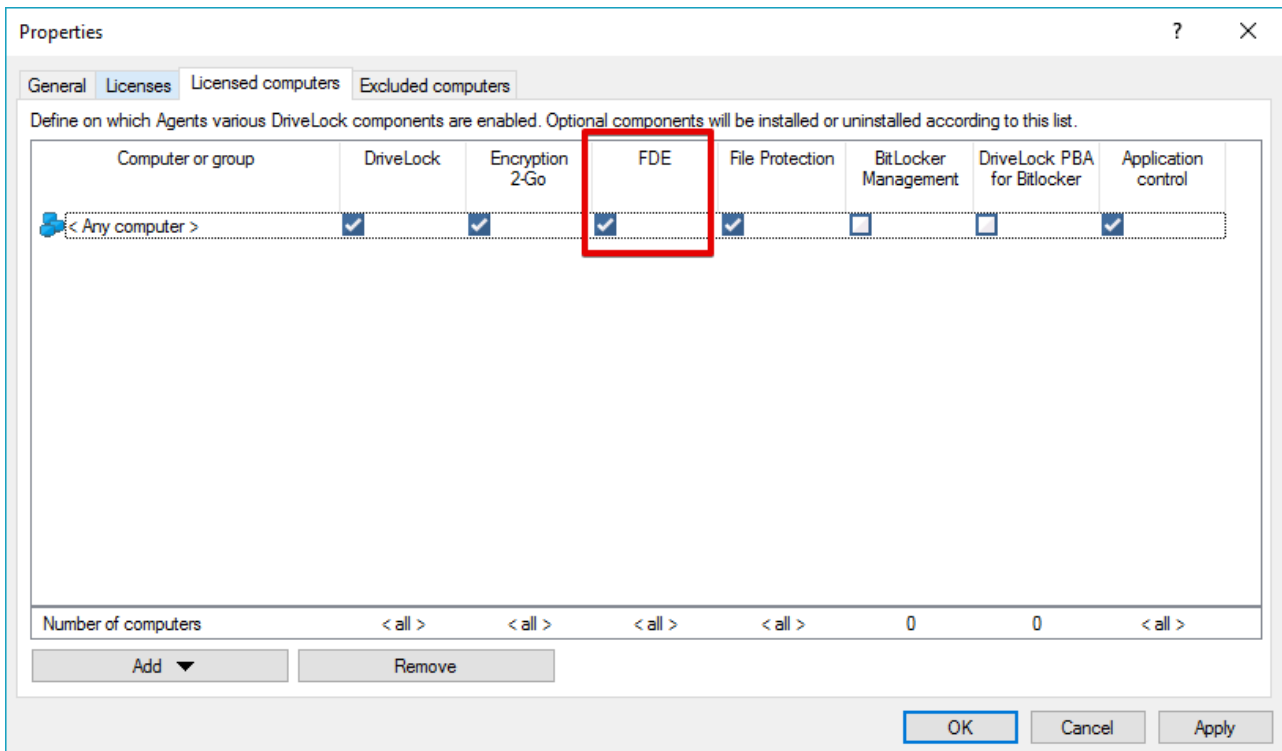


To export the two certificate files, click **Manage certificates** and then on the drop-down menu click **Export certificates**. Select a directory to save the files to.

You can also import previously created certificates (public keys) into the DriveLock Policy File storage. To import the two certificate files, click **Manage certificates** and then on the drop-down menu click **Import master certificates**. Select the directory containing the certificate files.

12.2.3 License Settings

When a computer where the DriveLock Agent is running is licensed to use Disk Protection, the Agent automatically installs all components and services that are required for Disk Protection on this computer. To license a computer or group of computers to use Disk Protection, under *Global configuration* -> *License* click **Change**. In the *Properties* dialog box, on the *Licensed computers* tab, add the computer or group and then select the *FDE* checkbox for the computer or group.



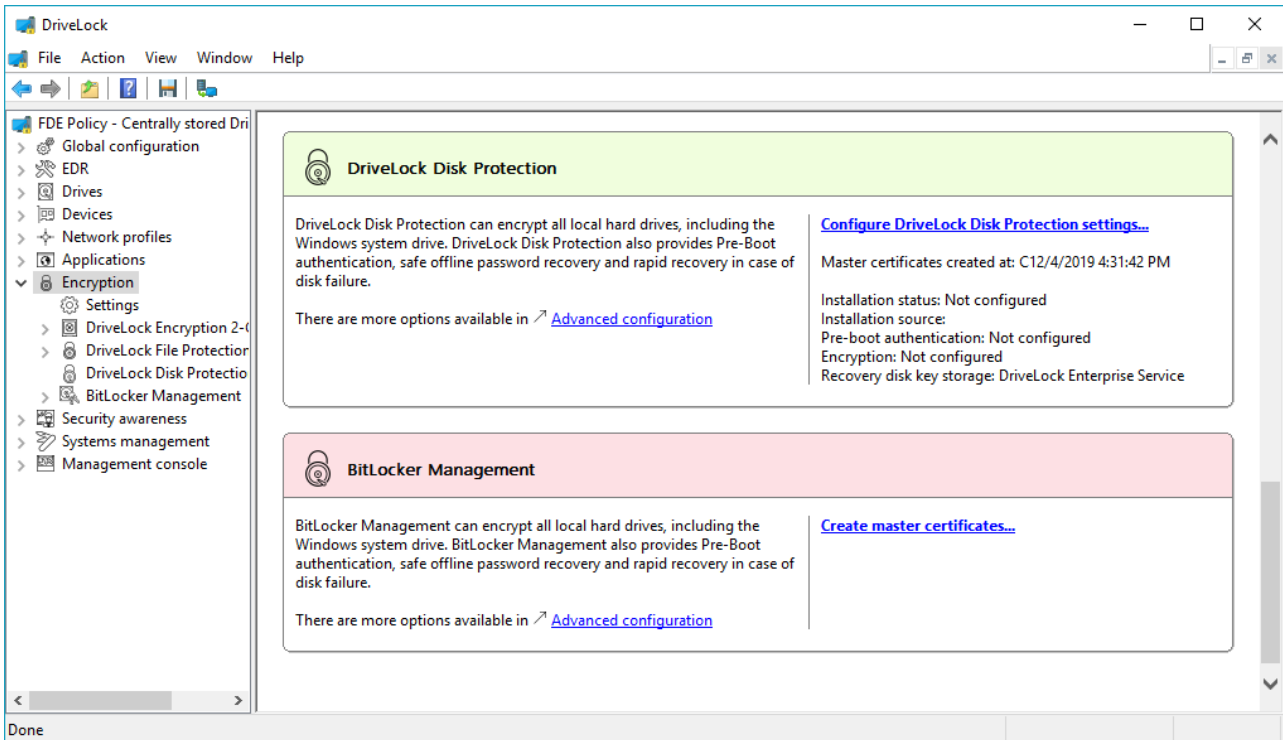
The installation is entirely determined by a computer's license status.

If you can't select the FDE checkbox, your license may not include the FDE option. To update your license, contact your DriveLock sales partner.

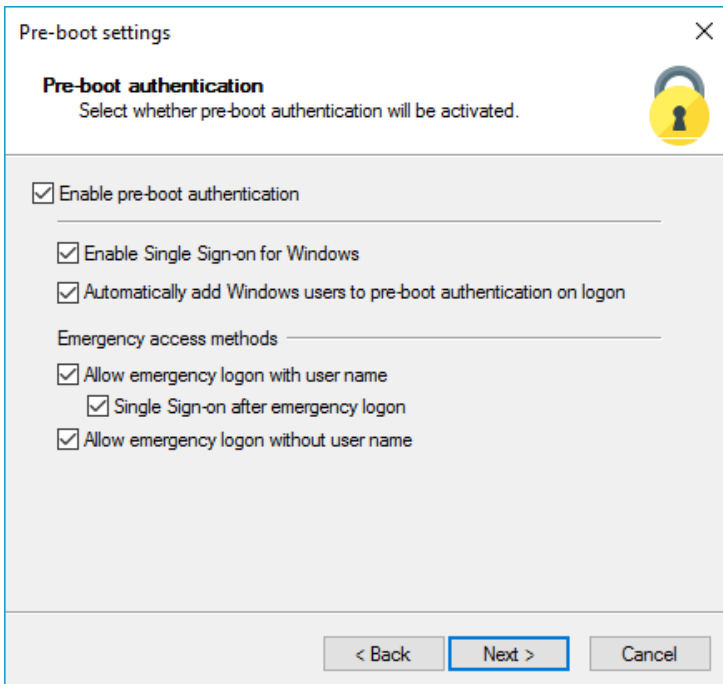
To remove Disk Protection from a computer, remove the checkmark in the FDE column. Once a computer is no longer licensed to use FDE, the DriveLock Agent will automatically uninstall the Disk Protection. You can specify a setting to delay this uninstallation by up to 3 days.

12.2.4 Disk Protection Settings

This section explains how to configure the most important settings in the basic configuration. All additional settings are described in the following section.



Open **Encryption / Configure DriveLock Disk Protection settings** to configure the settings that are required for DriveLock Disk Protection.



To enable pre-boot authentication on client computers, select the **“Enable pre-boot authentication”** checkbox.

As soon as the DriveLock Agent detects the new configuration settings, pre-boot authentication is activated and takes effect the next time the computer is restarted. Ensure that all other required parameters in this dialog box have been configured and that users are aware of the change. DriveLock displays the following message to the user when pre-boot authentication is first activated.

To disable DriveLock Disk Protection without uninstalling it, clear the *“Enable pre-boot authentication”* checkbox. Without pre-boot authentication, all features of DriveLock Disk Protection, including disk encryption, are disabled. If you clear this checkbox you can make still changes to other settings in this dialog box, but changes do not take effect until DriveLock Disk Protection is re-enabled by selecting the **“Enable pre-boot authentication”** checkbox.

To gain access to a computer protected by DriveLock Disk Protection, both pre-boot and Windows authentication are mandatory.

In single sign-on mode, a user needs to log on only once to authenticate both during pre-boot authentication and to Windows. This option is only available when at least one authentication method is enabled for both pre-boot and Windows authentication.

Select the **“Enable Single Sign-on for Windows”** checkbox to enable single sign-on mode.

By default DriveLock Disk Protection adds any user who has successfully logged on to Windows to the pre-boot authentication database. Clear the **“Automatically add Windows user to pre-boot authentication on logon”** checkbox if you don’t want Windows users to be automatically added.

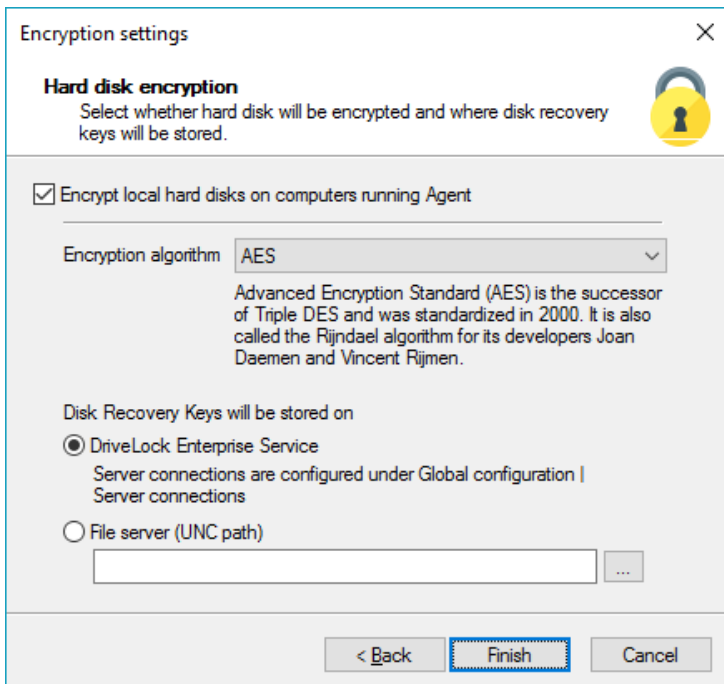
Emergency logon settings are available when authentication is enabled at the pre-boot level:

- *Allow emergency logon with user name* – When enabled, this option lets a user initiate the emergency logon with user name procedure. This procedure is used when a user has forgotten the pre-boot authentication password. It also applies to local Windows or domain accounts that have been added to DriveLock Disk Protection but who have not been assigned an initial password. Emergency logon with user name enables one-time-only pre-boot access to the system.

This feature requires that a user was authenticated by pre-boot authentication on the computer at least once or that the user was added to the pre-boot authentication database by an administrator. A user who is not in the pre-boot authentication database must initiate the emergency logon without username procedure.

- *Single Sign-on after emergency logon* – When enabled, this option allows the user to automatically authenticate to Windows immediately after the successful completion of the emergency logon with username procedure.
- *Allow emergency logon without username* – When enabled, local Windows or domain users may initiate the emergency logon without username procedure. This allows for one-time-only pre-boot access to the system for users who don’t have a pre-boot user account. This procedure also adds the user to the pre-boot authentication database. Once the user logs on to Windows, the Windows password is automatically synchronized with the pre-boot authentication database. This synchronization enables future pre-boot authentication using the Windows password.

Click **Next** to proceed.



To globally enable hard disk encryption, select the “**Encrypt local hard disks on Agent computers**” checkbox.

Depending on the drive size, encryption or decryption may take some time. However, the computer can still be used during this time, a slight reduction in system performance is possible. The computer can also be shut down or restarted during this phase. In this case, the process will be continued afterwards. The current state of the encryption on a computer can be checked via the DriveLock Management Console by connecting to the agent and viewing its properties.

You can choose between different encryption algorithms, but we recommend AES (AES 256-bit).

DriveLock Disk Protection creates the recovery files and sends them to the location you configured immediately after the Agent has finished installing DriveLock Disk Protection on a client computer.

The recovery files should be stored in the DriveLock Enterprise Service database or in a central shared folder. It is not recommended to store these files on the local computer because of security and recovery considerations.

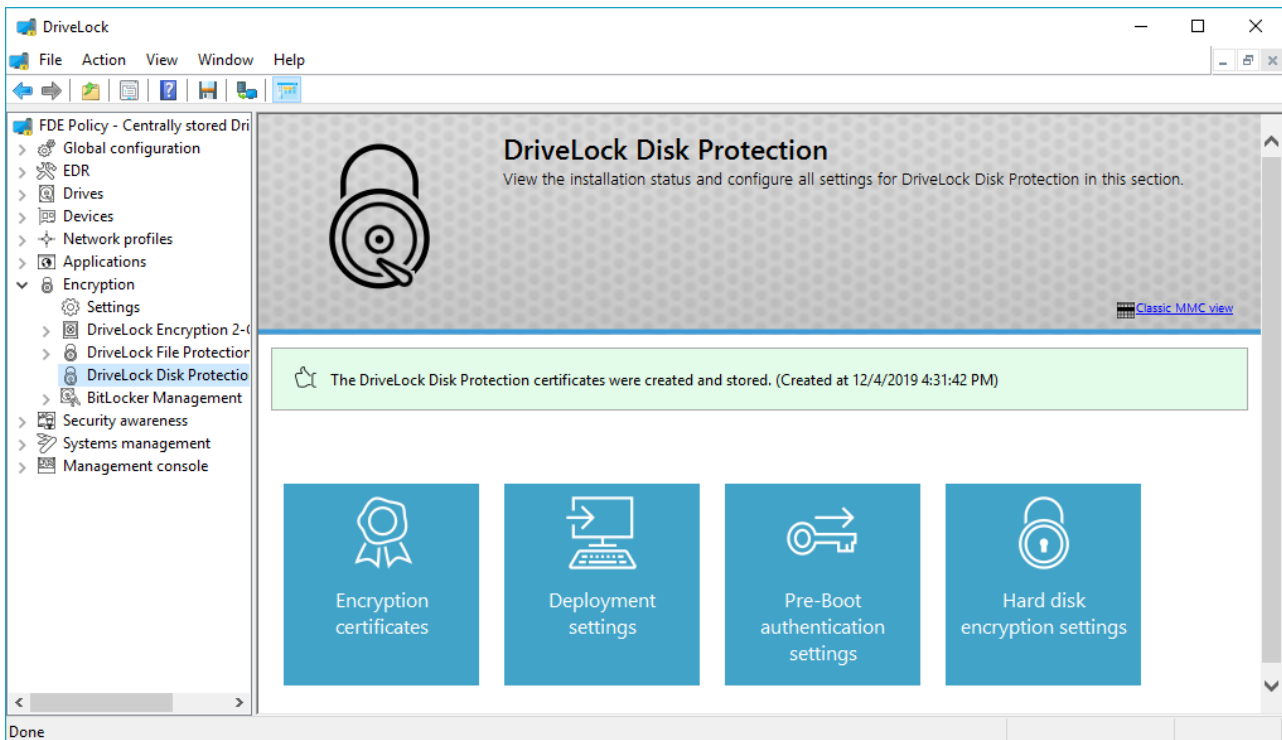
If you store the files on a central shared folder, the following file names are used: `<computer>.envelope.env` and `<computer>.backup.zip`

12.3 Configuring Disk Protection in Extended Configuration Mode

This section covers all possible DriveLock Disk Protection settings for the

- Installing the software
- Pre-boot authentication PBA
- Encryption of hard disks

You can configure all settings in the DriveLock Management Console via the menu item *DriveLock Disk Protection*:



12.3.1 Installation Settings

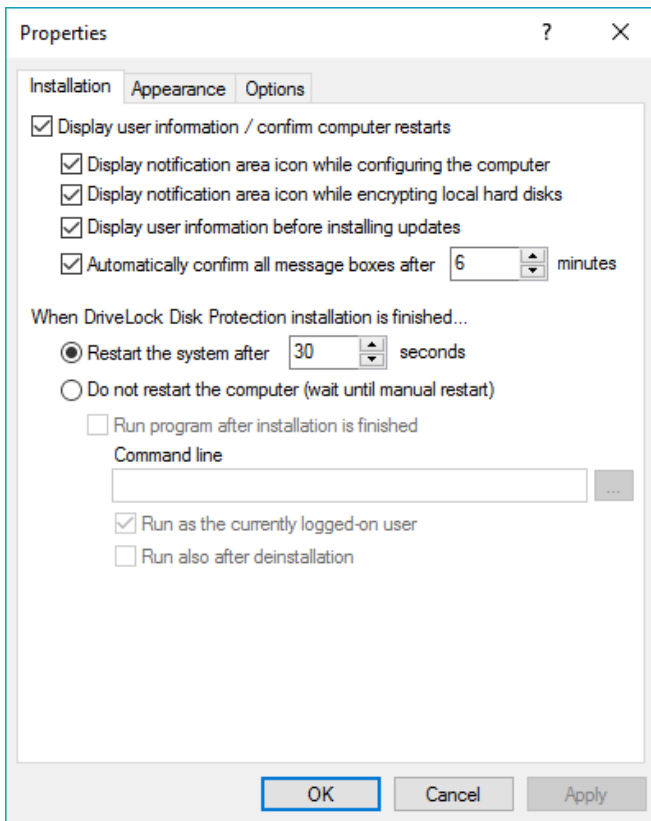
After you created the recovery certificates you can configure DriveLock Disk Protection deployment settings.

Before configuring the settings for a new installation, determine where DriveLock will store the computer-specific recovery envelope files that are needed for emergency logon. To specify the storage location, click **Hard Disk encryption settings**, and then follow the procedure in the section [“Configuring the Backup of Recovery Data”](#).

Configure the installation parameters

To configure the installation parameters, in the right pane of the DriveLock Management Console, click **Deployment settings**.

Select the **Installation** tab.



If you don't want to show information messages on the client computer while DriveLock Disk Protection is installed, clear the **“Display notification area icon while configuring the system”** checkbox.

You can also specify the individual options separately:

- You can disable/enable the display of an icon that is displayed in the Information pane during installation.
- You can disable/enable the display of an icon that is displayed in the Information pane during encryption.
- You can show or hide user notifications before installing a Disk Protection update.
- Additionally, you can specify whether displayed messages should be confirmed automatically after a certain number of minutes or not.

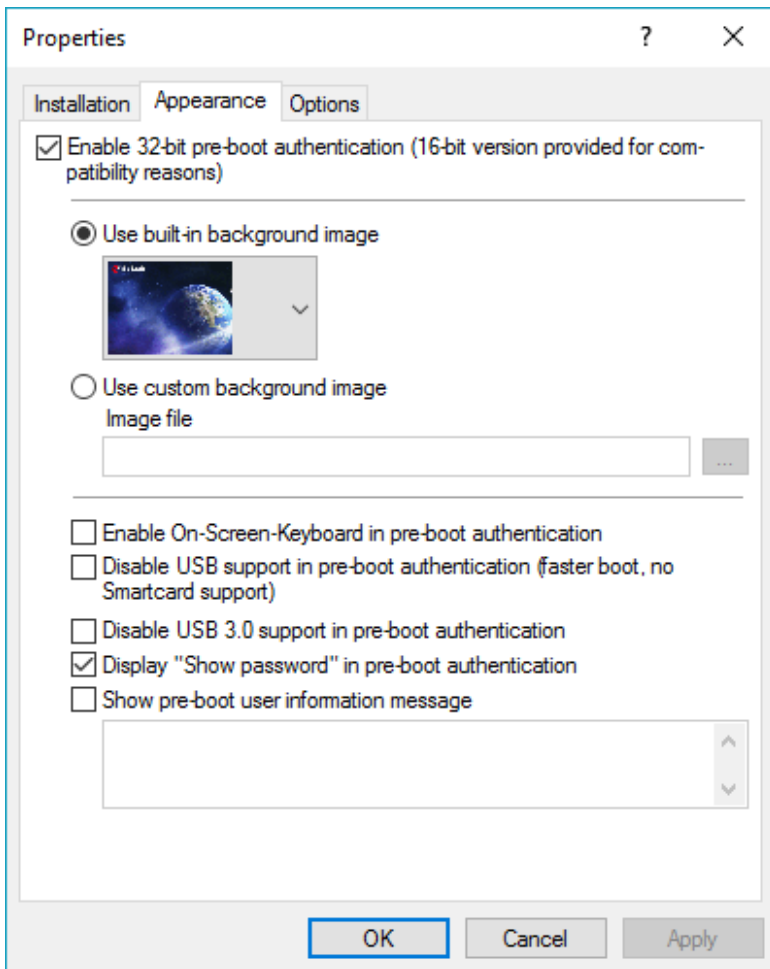
You can select whether information messages are automatically confirmed after being displayed for a specified number of minutes. Because the installation of Disk Protection requires a computer restart, you can also configure whether this restart will be delayed or must be performed manually.

If you selected to not automatically restart the computer, you can also specify a program or script that is started when the installation has completed. There are also two script specific options which can be set:

- *Run as the currently logged-on user* -> The specified script will run under the credentials of the currently logged on user. By default it runs as local system.
- *Run also after deinstallation* -> The script will not only run after installation but also after deinstallation.

Configure the appearance / PBA behavior for users

Select the **Appearance** tab to configure how Disk Protection is displayed to the users.



Keep the *Enable 32-bit pre-boot authentication* setting. The 16-bit version of the PBA is only available for compatibility with legacy BIOS systems.

New DriveLock Pre-Boot Authentication and UEFI BIOS no longer support 16-bit PBA.

This is where you can specify the background image for the pre-boot authentication. Disk Protection provides predefined background images for you to choose from.

It is possible to use a customized background image (format PNG, max. 32 MB, best resolution 1024x768) on the pre-boot authentication screen. This image needs to be configured before Disk Protection installation and can't be changed later. Select the *Use custom background image in pre-boot authentication* checkbox. Then select the file from the policy file storage or from the file system.

You can also choose one of the following options:

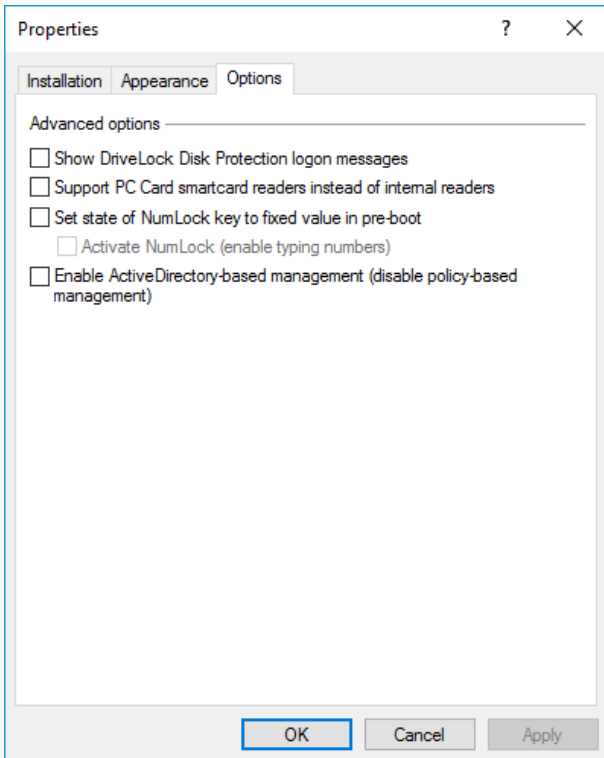
- On-screen keyboard (UEFI PBA only): With the help of a virtual keyboard, users can also enter data without having a real keyboard.
- USB support: If disabled, the PBA can be loaded faster. However, devices connected via the USB interface, e.g. mouse or smartcard reader, will not work.
- USB 3.0 support: This option disables the support of modern USB 3.0 devices within the PBA.
- Show password: This can prevent an entered password from being displayed in plain text.

To display your own user information within the PBA, e.g. for usage notes or contact persons / contacts for password recovery, select the **Show pre-boot user information message** and enter the text in the text box.

Additional Options

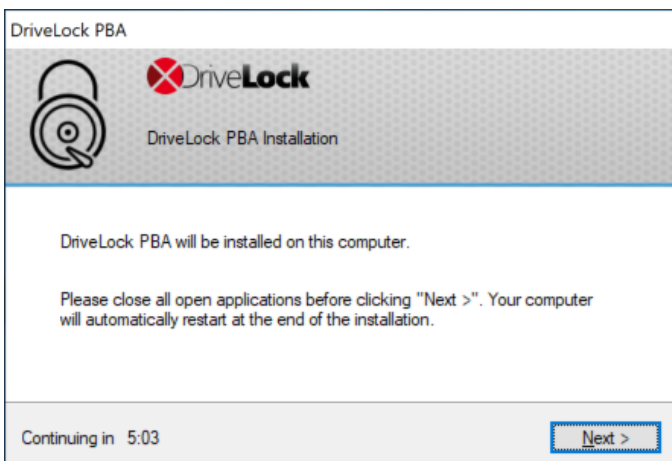
Select the *Options* tab to configure additional settings for BIOS systems after consulting DriveLock support or as needed.

These options do not apply to the new UEFI-PBA.



Click **OK** or **Apply** to save the settings, or click **Cancel** to discard any changes you made.

Once the agent gets its new configuration and Disk Protection is installed, the agent displays the following information to the logged in user:



The envelope file is created and sent to the location you configured immediately after the Agent has finished installing DriveLock Disk Protection on a client computer. Therefore make sure you have configured the corresponding recovery settings. (Refer to the section "Configuring the Backup of Recovery Data" for details.).

You can override the installation policy by configuring the following registry key on a computer:

```
HKEY_LOCAL_MACHINE\SOFTWARE\CenterTools\DLStatus
```

If this registry key (DWORD) contains the value `NoFDEInstallation` and the value is set to 1, DriveLock Disk Protection will not be installed on the computer even if installation is specified in the policy. You can also use the command-line commands `dlfdecmd enabledelayinst` and `dlfdecmd disabledelayinst` to create or remove this registry value.

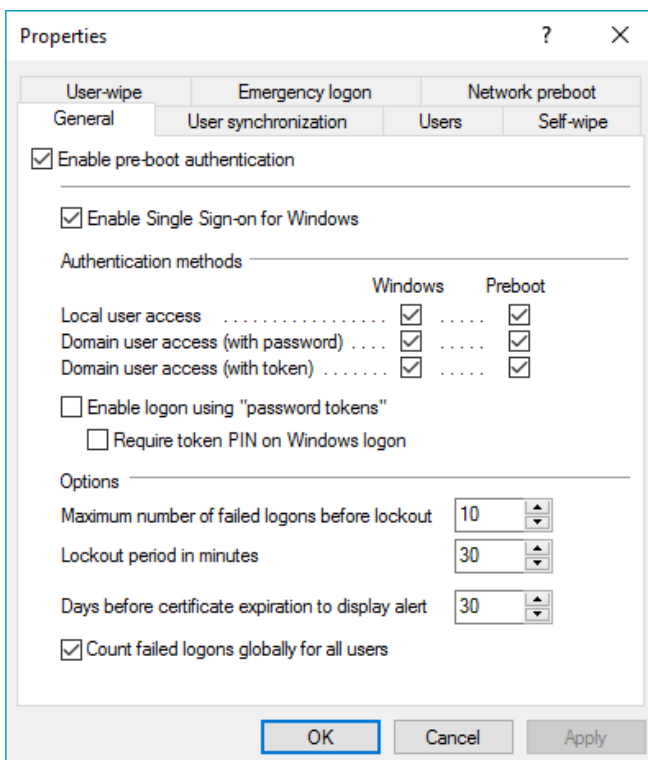
12.3.2 Configuring Pre-Boot Authentication

Once you have deployed DriveLock Disk Protection to client computers you can configure drive encryption and pre-boot authentication settings.

You can activate and configure pre-boot authentication before you begin to encrypt hard drives on client computers. This can help divide the deployment process in larger environments or help users get familiar with the new logon procedure.

Click **Pre-boot authentication settings** to open the configuration dialog box.

12.3.2.1 Authentication Methods and Logon Settings



The screenshot shows the 'Properties' dialog box with the 'Pre-boot authentication' settings. The 'Enable pre-boot authentication' checkbox is checked. Under 'Authentication methods', 'Local user access', 'Domain user access (with password)', and 'Domain user access (with token)' are all checked for both 'Windows' and 'Preboot'. The 'Options' section shows 'Maximum number of failed logons before lockout' set to 10, 'Lockout period in minutes' set to 30, and 'Days before certificate expiration to display alert' set to 30. The 'Count failed logons globally for all users' checkbox is also checked.

To enable pre-boot authentication on client computers, select the **“Enable pre-boot authentication”** checkbox.

As soon as the DriveLock Agent detects the new configuration settings, pre-boot authentication is activated and takes effect the next time the computer is restarted. Ensure that all other required parameters in this dialog box have been configured and that users are aware of the change.

DriveLock displays the following message to the user when pre-boot authentication is first activated:



To disable DriveLock PBA (without decryption), clear the *“Enable pre-boot authentication”* checkbox.

Attention: although the hard disk remains encrypted, the security will be decreased, as Windows boots, before an authorized user has been authenticated. DriveLock recommends to disable the PBA only for test and maintenance reasons.

If you clear this checkbox you still change other settings in this dialog box, but changes do not take effect until DriveLock Disk Protection is re-enabled by selecting the **“Enable pre-boot authentication”** checkbox.

To gain access to a computer protected by DriveLock Disk Protection, both pre-boot and Windows authentication are mandatory.

You can require users to use one or more authentication methods for pre-boot authentication and Windows logon, based on the settings you configure. These authentication methods are described in detail below.

To make an authentication method available to users, select the **Windows checkbox**, the **Pre-boot checkbox**, or both, to match the security requirements of your organization. You must select at least one check box each for Windows and pre-boot authentication.

Do not configure DriveLock Disk Protection to allow only tokens and smart cards for Windows logon unless your network is configured for certificate-based logon. If users don't have tokens or if required drivers are not installed and the computer is locked, it can't be unlocked using a password. If DriveLock Disk Protection is configured to only allow token logon, ensure that valid tokens have been distributed to users and that they can be used for pre-boot authentication, Windows logon and unlocking computers.

- *Local user access* – Enabled by default. This method lets users authenticate by typing a local Windows user name and password and selecting the computer name.
- *Domain user access (with password)* – This method lets users authenticate by typing a Windows domain user name, password and selecting the domain name.
- *Domain user access (with token)* – This method lets Windows domain users authenticate by using a smartcard or token with a PIN.
- *Enable logon using password tokens* – This method lets users perform pre-boot authentication for a password token users. If this option is selected, at least one Windows authentication method must also be selected.

Select the **“Enable Single Sign-on for Windows”** checkbox to enable single-sign on mode. In single sign-on mode, a user needs to log on only once to authenticate both during pre-boot authentication and to Windows. This option is only available when at least one authentication method is enabled for both pre-boot and Windows authentication.

To protect the authentication database against automated brute-force attacks, DriveLock Disk Protection can lock out a user after a configurable number of failed logons for a number of minutes. Adjust the values to match your organization's security policy. By default the failed logon attempt counter applies to all users. To maintain a separate counter for each user, deselect the checkbox **Count failed logons globally for all users**.

If you use certificates for authentication you can also configure how many days before the expiration of a certificate DriveLock Disk Protection notifies the user of the upcoming expiration.

12.3.2.2 AD User Synchronization

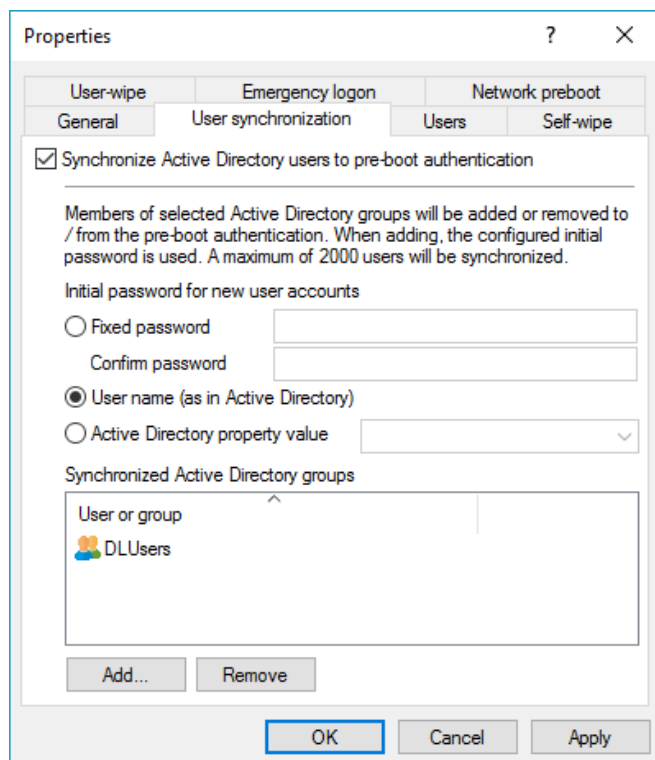
DriveLock distinguishes 4 different types of pre-boot users.

Added by	Description
DIFdeUser	Users added locally via <i>DIFdeUser.exe</i>
Policy	Users added in the policy - will be synced/removed according to policy changes
WinLogon	Users added by the windows logon - the password will be synced after each successful login to windows
AD sync	Users synchronized from AD groups - will be removed, if removed from the AD group resp. the user synchronization, the password will be synced after each successful login to windows

The command `DIFdeUser.exe` can remove users of the other types, but they will be added again at the next time, when the user logs on to windows resp. the policy is executed.

Users, who want to login the first time to a PC protected by DriveLock Disk Protection with Pre-Boot Authentication (PBA) are not yet synced to the PBA database with their Windows credentials (WinLogon user). They have to authenticate at the PBA either with a pre-configured DIFde- or a Policy user or someone else authenticates at the PBA to show the Windows logon dialog.

If you want to pre-configure the PBA to contain users from your AD, you must enable the **AD User synchronization**.



Check **Synchronize Active Directory users to pre-boot authentication**. Add the appropriate AD users and/or groups, which you want the users to be synced to the PBA database.

Note that the members of the Domain Users group are not synchronized. The domain user group uses a "calculated" mechanism based on the user's "primary group ID" to determine membership and does not normally store members as multi-valued associated attributes.

As an initial password you can either use a **fixed password**, which is identical for all users, the **user name** or any of the available **Active Directory property values**.

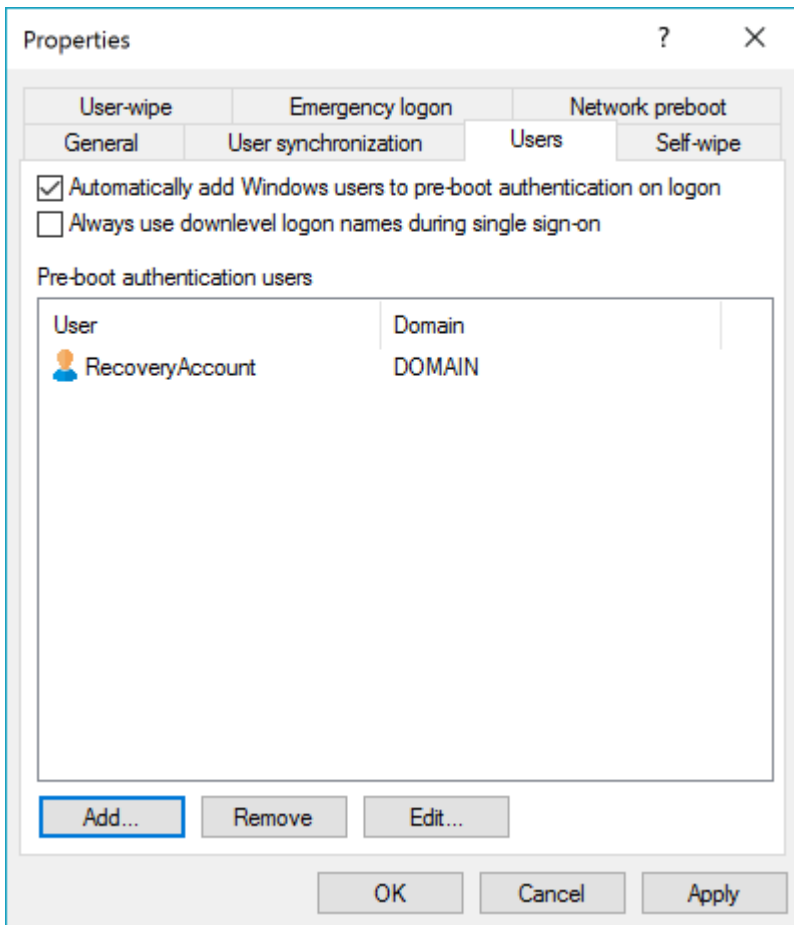
The given password is used at creation time only, but not synced/changed for users already existing in the PBA database. As soon as a user of type *AD sync* logs on to windows, the initial password will be replaced by his windows password locally.

The AD sync users are synced each time, when the policy is executed. If you add or remove users from the configured AD groups they will be added/removed to/from the PBA database of all related PCs with the next synchronization.

Although the PBA database can hold up to 2,000 credential sets, we recommend to use not more than 500 users for AD user synchronization. If you want to configure more systems, you may use separate policies assigned to different computer groups.

12.3.2.3 Users

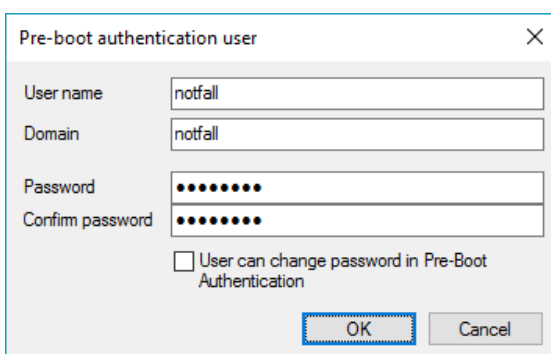
DriveLock Disk Protection can hold up to 2000 sets of credentials in its pre-boot authentication database. You can manually add users to this database. A pre-boot authentication user does not need to correspond to a specific Windows user account. If required, you can configure separate credentials that are used for pre-boot authentication only, for example an account to be used for emergency logon.



By default DriveLock FDE adds any user who has successfully logged on to Windows to the pre-boot authentication database. Clear the **“Automatically add Windows user to pre-boot authentication on logon”** checkbox if you don’t want Windows users to be automatically added.

By activating the option **“Always use downlevel logon names during single sign-on”** you can enforce users to use down-level logon names only (format: DOMAIN\username). Then logon with user principal names (format: username@domain.org) is no longer possible.

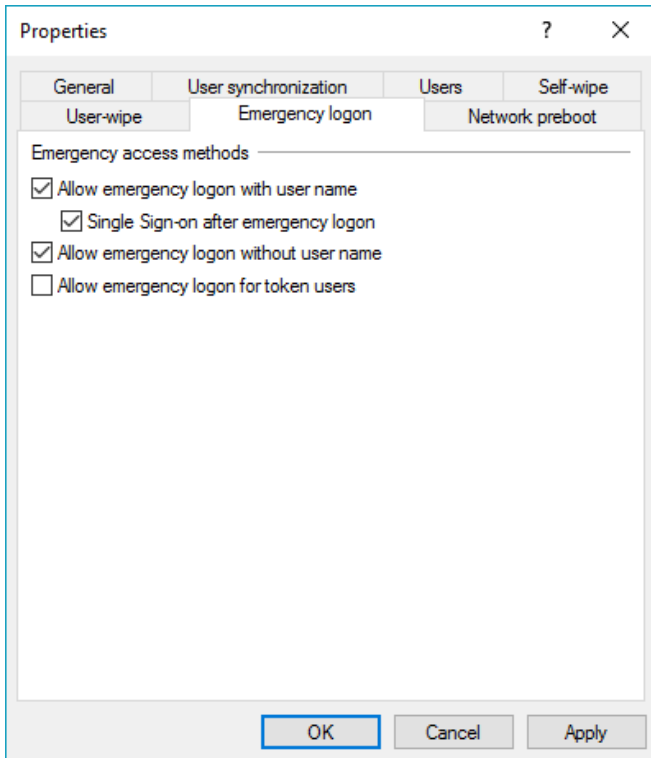
Use the **Add**, **Remove** or **Edit** buttons to change or remove existing users or to add new users to the database.



After you have entered the information and confirmed the password, click **OK** to save the user.

12.3.2.4 Emergency Logon

Emergency logon parameters specify which logon procedures are available for users when they are not able to log on by using normal procedures. For example, this includes users who forgot their password.



Emergency logon settings are available when authentication is enabled at the pre-boot level and the **Local user access** or **Domain user access** check boxes are selected.

- *Allow emergency logon with user name* – When enabled, this option lets a user initiate the emergency logon with user name procedure. This procedure is used when a user has forgotten the pre-boot authentication password. It also applies to local Windows or domain accounts that have been added to DriveLock FDE but who have not been assigned an initial password. Emergency logon with user name enables one-time-only pre-boot access to the system.

This feature requires that a user was authenticated by pre-boot authentication on the computer at least once or that the user was added to the pre-boot authentication database by an administrator. A user who is not in the pre-boot authentication database must initiate the emergency logon without username procedure.

- *Single Sign-on after emergency logon* – When enabled, this option allows the user to automatically authenticate to Windows immediately after the successful completion of the emergency logon with username procedure.
This feature allows users who forgot their password to still log in to Windows and work with it - even if an administrator has not yet reset the password.
- *Allow emergency logon without username* – When enabled, local Windows or domain users may initiate the emergency logon without username procedure. This allows for one-time-only pre-boot access to the system for users who don't have a pre-boot user account. This procedure also adds the user to the pre-boot authentication database. Once the user logs on to Windows, the Windows password is automatically synchronized with the pre-boot authentication database. This synchronization enables future pre-boot authentication using the Windows password.
- *Allow emergency logon for token users* – This option is available only if at least one of the following pre-boot authentication method options is selected: Domain user access (with token) or Shared Key access. If this option is enabled, smartcard and token users who have misplaced a token or forgotten the PIN are permitted to initiate the "Emergency logon for token users" procedure. This procedure allows for a one-time-only pre-boot access to the computer without having to use a token.

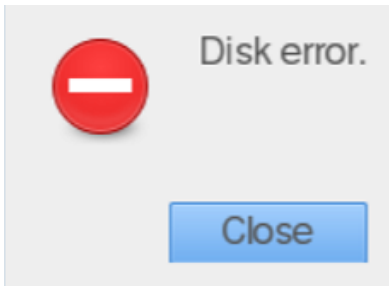
12.3.2.5 Wipe the PBA database

Wiping the PBA database is equivalent to destroying the data of a single PC. The wipe removes all users from the PBA database. No more logon is possible. As no disk key is available anymore, the disks cannot be decrypted. To get access again an administrator has to perform a disk recovery as described in [Recovering Encrypted Disks](#).

There are three different ways to wipe the PBA database.

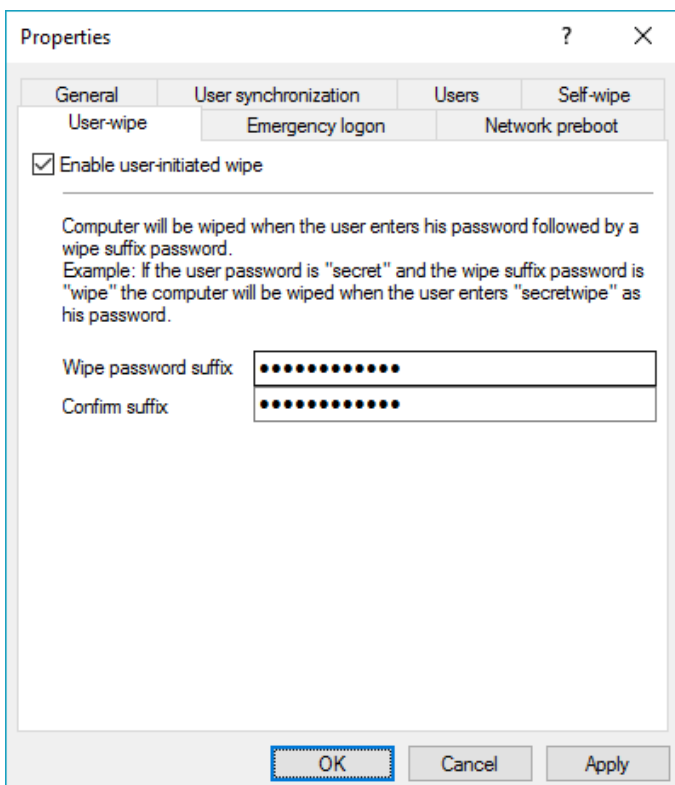
User Wipe

Imagine, a user has sensitive data on his laptop. He is forced by somebody, to enter his credentials in the PBA. He will do so. Instead of being logged in will get a disk error. If he reboots the logon screen will not be shown any more.



Instead of his true password the user has entered the password plus a defined suffix. This triggers the DriveLock PBA to immediately delete the PBA database.

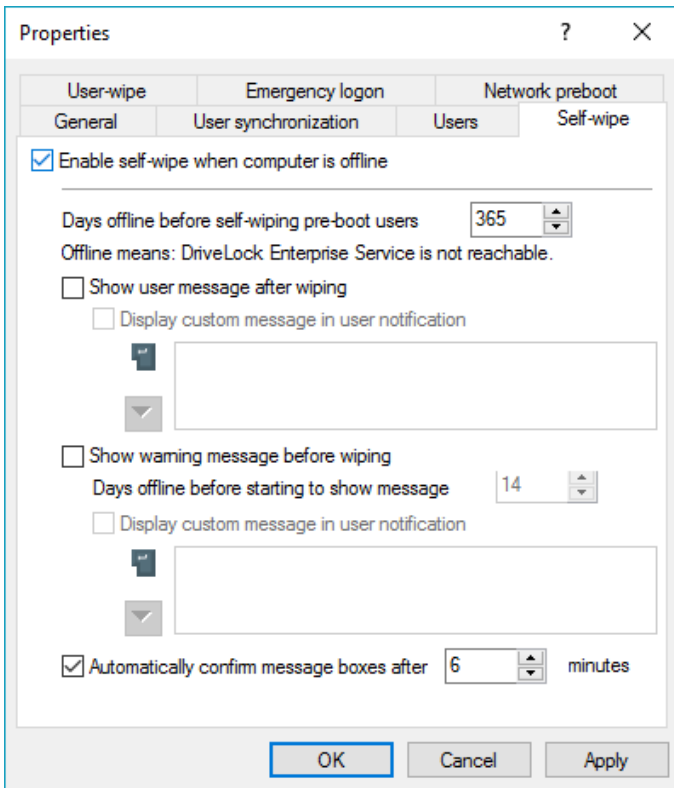
To configure the *user wipe* in the policy open **Encryption / Disc Protection / Pre-Boot authentication settings / User-wipe**. Check **Enable user-initiated wipe** and enter the **password suffix**.



Self Wipe

The self wipe has primarily two use cases. Either you want to protect the data of a lost PC which does not connect to the DES any more and/or you want to force mobile users to connect regularly to your company network.

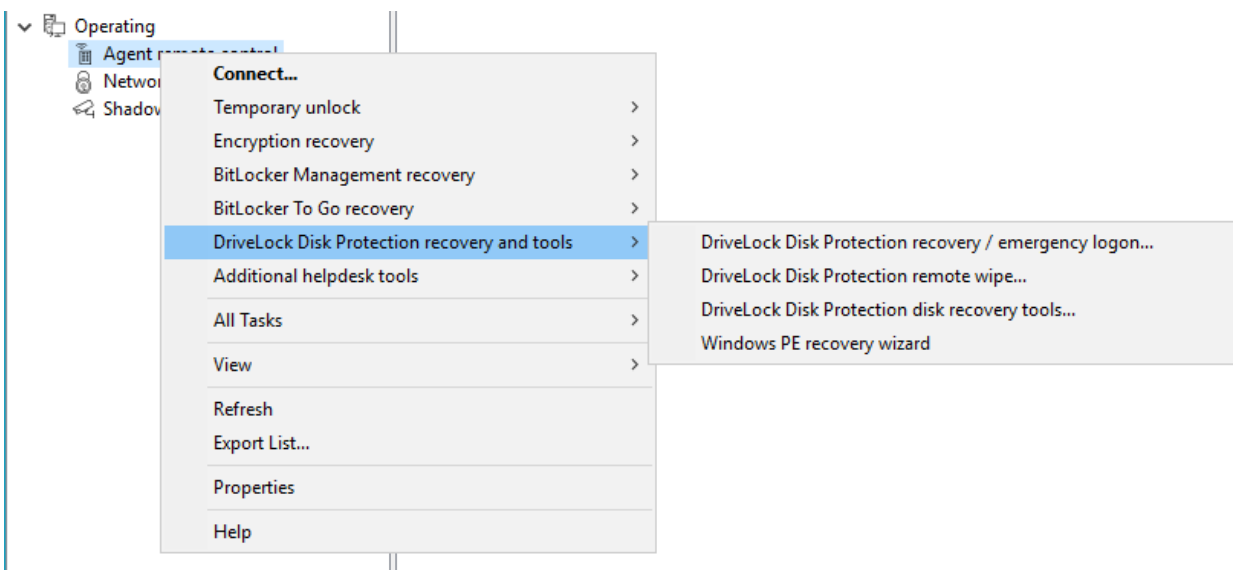
To configure the *self wipe* in the policy open **Encryption / Disc Protection / Pre-Boot authentication settings / Self-wipe**, check **Enable self-wipe when computer is offline** and configure the appropriate settings as described in the dialog.



At the end of the configured days offline, the DriveLock agent deletes the PBA database.

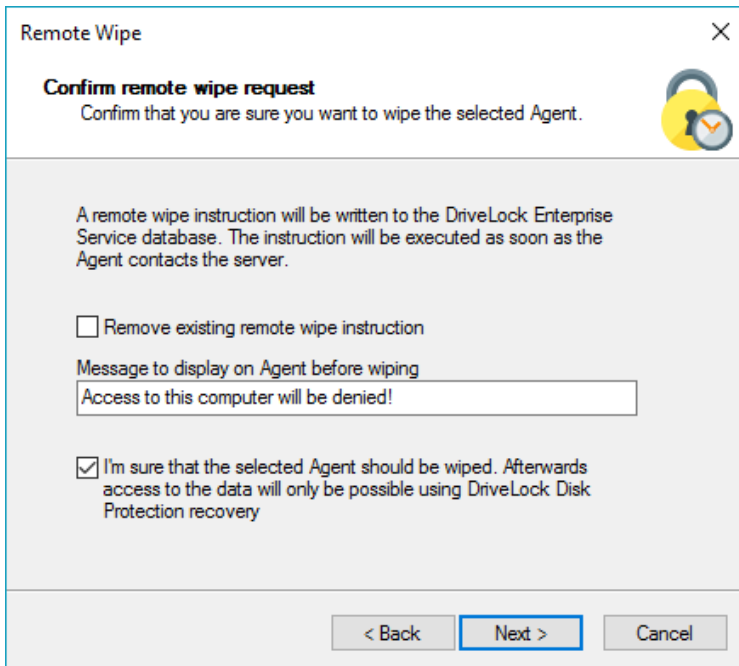
Initiating a Remote Wipe

To initiate a remote wipe, in the DriveLock Management Console (MMC) select **Operating**, then **Agent remote control**. Open the context menu and select **DriveLock Disk Protection recovery and tools / DriveLock Disk Protection remote wipe....**



You are prompted to provide the private key of the recovery certificate (DIFdeRecovery.pfx) and to select the computer you want to wipe. In the next dialog **Confirm** the **remote wipe request**. The settings that you configure on

this page are applied to the client you selected the next time it connects to the DES. To enable remote wiping of computers that are not connected to your internal network, the DES server must be accessible from the Internet.



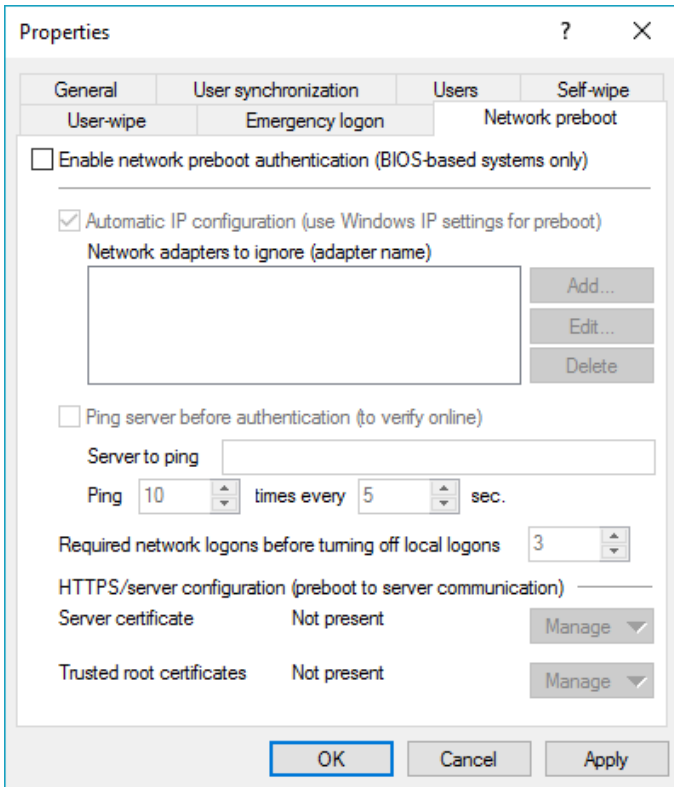
Configure the following settings as shown in the dialog.

Check **Remove existing remote wipe instruction**, if you want to revoke a previous remote wipe instruction (if the PBA database has not yet been wiped).

12.3.2.6 Network PBA

For some legacy BIOS systems, Disk Protection provides network-capable pre-boot authentication that can automatically detect whether a computer is part of a pre-defined corporate network and deactivates logon to the PBA (auto-boot).

This functionality is only available for some systems and can only be activated with the appropriate assistance of a DriveLock Professional Service Team member. We do not provide a description here.

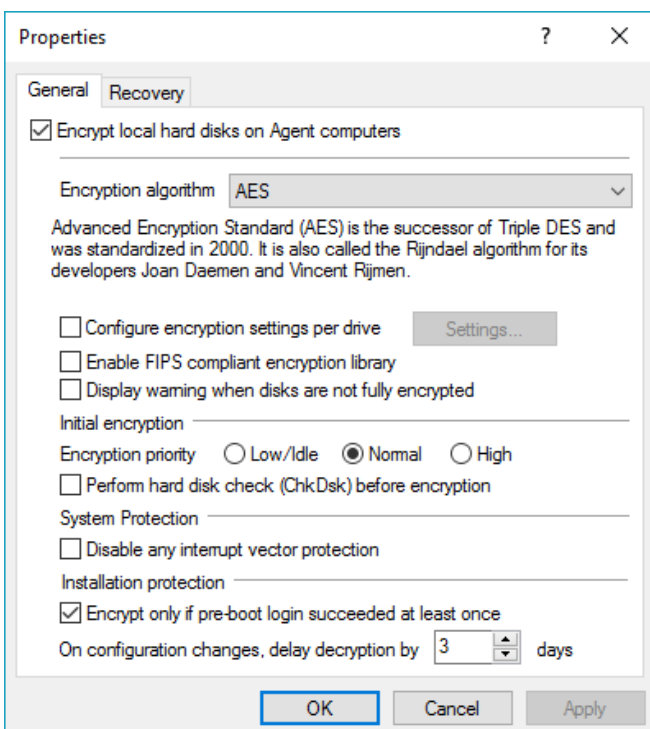


12.3.3 Encryption Settings

This chapter contains information on how to configure DriveLock FDE, how it stores emergency recovery information centrally, and how Agents save this data.

Click **Hard disk encryption settings** to open the Properties dialog box.

12.3.3.1 Configuring Encryption Settings



To globally enable hard disk encryption, select the “**Encrypt local hard disks on Agent computers**” checkbox.

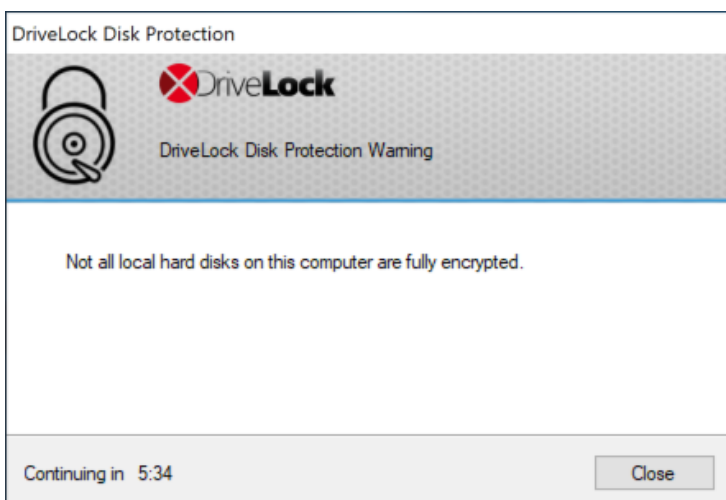
Depending on the drive size, the encryption or decryption may take some time. However, you can still use the computer during this time, a minimal reduction in system performance is possible. You can also shut down or restart the computer during this phase. If this happens, the process will continue afterwards. To check the current state of encryption on a computer, use the DriveLock Management Console to connect to the agent and view its properties.

You can select from several encryption algorithms. DriveLock recommends using AES (AES 256-bit).

By default DriveLock Disk Protection encrypts all local hard disks. To configure encryption separately for each local hard disk, select the “**Configure encryption settings per drive**” checkbox and then click **Settings**.

If your organization’s policy requires compliance with Federal Information Processing Standard (FIPS) standard 140-2, select the “**Enable FIPS compliant encryption library**” checkbox. If this option is not selected, DriveLock instead uses a secure, Common Criteria EAL-2 approved, non-FIPS library that provides better performance for encryption and decryption operations and, if supported by your computers, automatically activates the hardware support AES NI (Intel® Advanced Encryption Standard (AES) Instructions Set).

To display a warning message at Windows logon that informs users when disks are not completely encrypted, select the “**Display warning when disks are not fully encrypted**” checkbox. This warning message is displayed immediately after the Windows logon has completed.



DriveLock Disk Protection maintains a record of some BIOS interrupt vector addresses. This allows DriveLock Disk Protection to detect attacks that depend on changing the interrupt vector address. When detecting a discrepancy between the BIOS interrupt vector address and the copy it stored previously, Disk Protection displays an error message. Select the corresponding check boxes to automatically update the stored copy of the interrupt vector addresses after the user has been notified.

When an interrupt vector address changes for legitimate reasons, for example after updating the BIOS, the warning message is still displayed. The *System Protection* settings provide a mechanism to accept a legitimate change by updating DriveLock Disk Protection’s copy of the disk, keyboard, and clock tick interrupt vector addresses.

To deactivate the check for hardware changes altogether, deselect all interrupt vector address checkboxes.

Enable the option **"Encrypt only if pre-boot logon was successful at least once"** to delay the encryption of the hard disks until a user has successfully logged on to the pre-boot authentication once and has thus been stored in the user database of the PBA.

The decryption of hard disks can start for the following reasons:

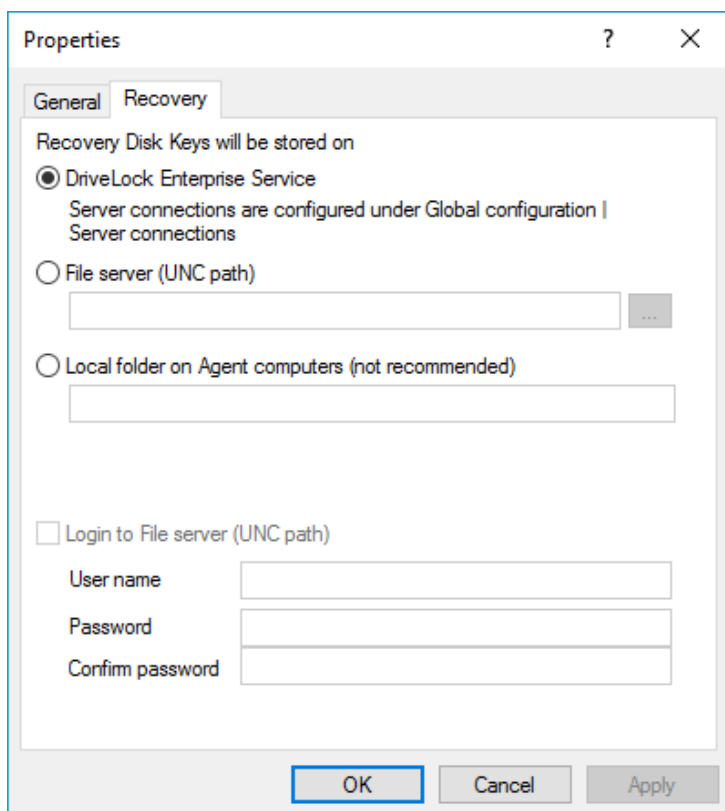
- The option "Encrypt local disks on agent computers" was disabled within the policy.
- The assignment of the policy with the Disk Protection settings to computers is removed or canceled.
- The "FDE" license option within an assigned policy is removed

To prevent unintentional, immediate decryption of hard disks, this can be delayed by a few days. Set the days value to 0 to configure immediate decryption.

This delay value is also useful in environments with a bad network connection. If an agent temporarily receives an incorrect or incomplete policy and the locally stored policy (cache) has been removed, this can prevent immediate decryption and bridge the period until the agent receives a full policy again.

12.3.3.2 Configuring the Backup of Recovery Data

To configure where the client's recovery disk keys will be stored, open the **Recovery** tab.



The recovery disk keys consist of two files:

- *Recovery.env* – The envelope file for emergency logon recovery
- *DiskKeyBackup.zip* – A ZIP files that contains the EFS recovery files for disk decryption procedures

DriveLock Disk Protection creates the envelope file and sends it to the location you configured immediately after the Agent has finished installing DriveLock Disk Protection on a client computer. The ZIP file containing the disk recovery files is created and copied only after all drives have been completely encrypted.

The recovery files should be stored on the DriveLock Enterprise Server or in a central shared folder. It is not recommended to store these files on the local computer because of security and recovery considerations.

If you store the files on a central shared folder, the following file names are used: <computer>.envelope.env and <computer>.backup.zip.

If the file server requires credentials for logon, specify them on the Recovery tab.

You must type domain user names in the format <domain>\<user>.

Verify that you have stored these recovery files for all your client computers, as they are required to perform any of the recovery procedures described in this manual. If you use the DriveLock database to store the recovery files, you can easily confirm which recovery files are available. You can find more information about using the DriveLock Control Center to view recovery information in the *DriveLock Control Center manual*.

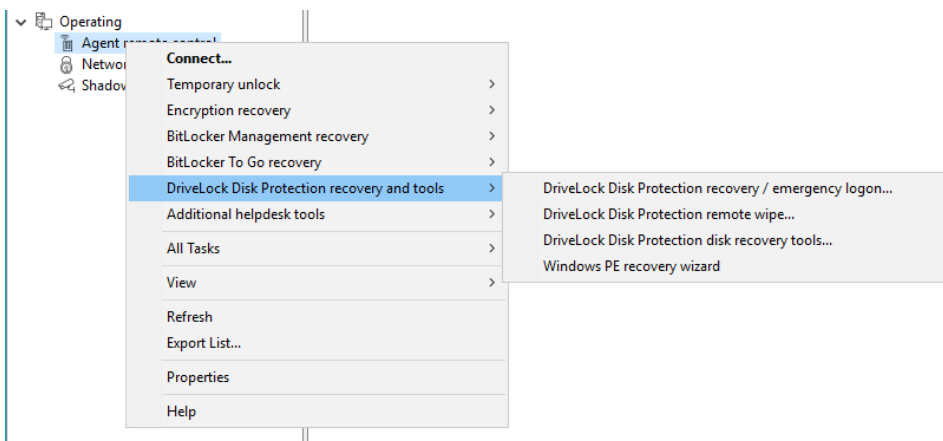
12.4 Recovery Procedures

DriveLock Disk Protection contains tools for two types of recovery scenarios:

- Emergency logon procedures
- Recovering encrypted disks

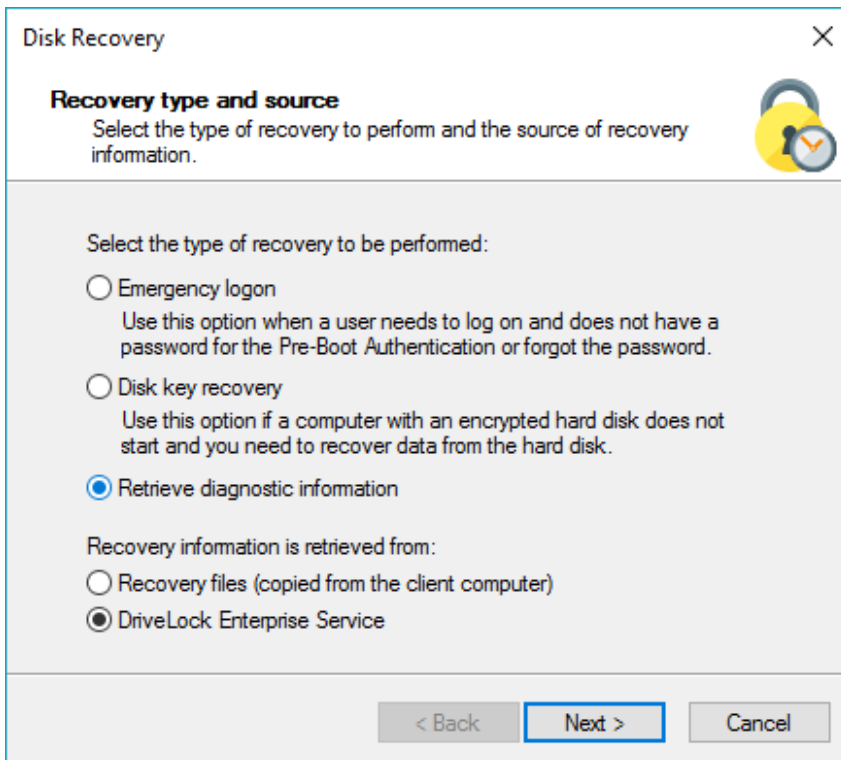
The emergency logon procedures are used when a user can't log on to the pre-boot authentication database, for example, because of a forgotten password or PIN. Disk recovery is used when a local disk drive becomes inaccessible, for example, when data sectors of the drive have become corrupt or you cannot logon to Windows anymore.

To start the recovery wizard, open the DriveLock Management Console, select **Operating -> Agent remote control**, right-click **Agent remote control** and then click **DriveLock Disk Protection recovery and tools**.



12.4.1 Viewing Diagnostics Data

When DriveLock Disk Protection is installed, the DriveLock Agents send the installation log file to the DriveLock Enterprise Services. You can retrieve this file from the DriveLock database to find out more details, if a Disk Protection installation has failed.



Disk Recovery [Close]

Recovery type and source
 Select the type of recovery to perform and the source of recovery information.

Select the type of recovery to be performed:

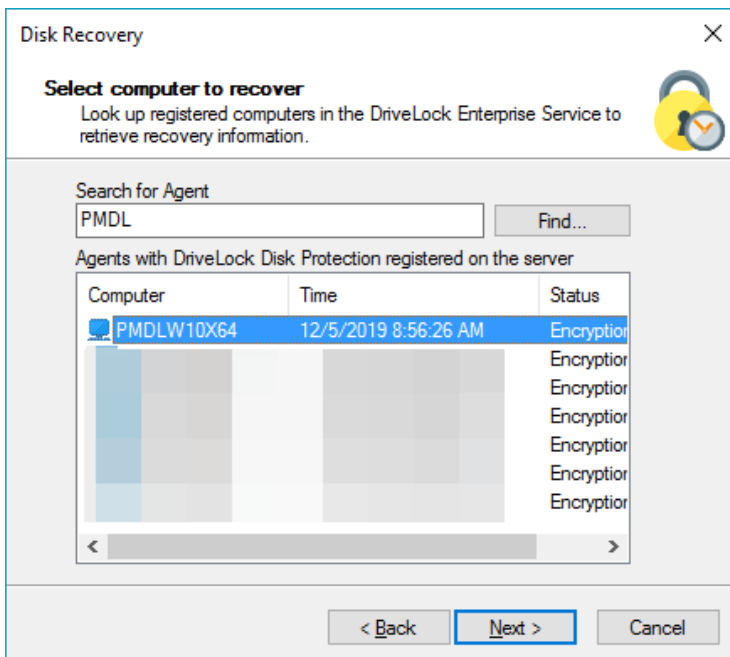
- Emergency logon
 Use this option when a user needs to log on and does not have a password for the Pre-Boot Authentication or forgot the password.
- Disk key recovery
 Use this option if a computer with an encrypted hard disk does not start and you need to recover data from the hard disk.
- Retrieve diagnostic information

Recovery information is retrieved from:

- Recovery files (copied from the client computer)
- DriveLock Enterprise Service

< Back **Next >** Cancel

Select “Retrieve diagnostic information” and select “DriveLock Enterprise Service”. Click **Next**.



Disk Recovery [Close]

Select computer to recover
 Look up registered computers in the DriveLock Enterprise Service to retrieve recovery information.

Search for Agent
 PMDL Find...

Agents with DriveLock Disk Protection registered on the server

Computer	Time	Status
PMDLW10X64	12/5/2019 8:56:26 AM	Encryption
		Encryption
		Encryption
		Encryption
		Encryption
		Encryption

< >

< Back **Next >** Cancel

Select the DES Server connection from the list.

To search for Agents registered in the DriveLock database, type the computer name or part of the name and then click **Find**. DriveLock Disk Protection displays all registered computers that contain the text you typed as part of their names. To view a list of all registered computers, don't type any text and the click **Find**.

Select the appropriate computer from the list and then click **Next** to continue.

Click “...” to select the path where to store the diagnostic file. Click **Next** to retrieve the file from the DriveLock database.

After the file has been retrieved, click **Finish**.

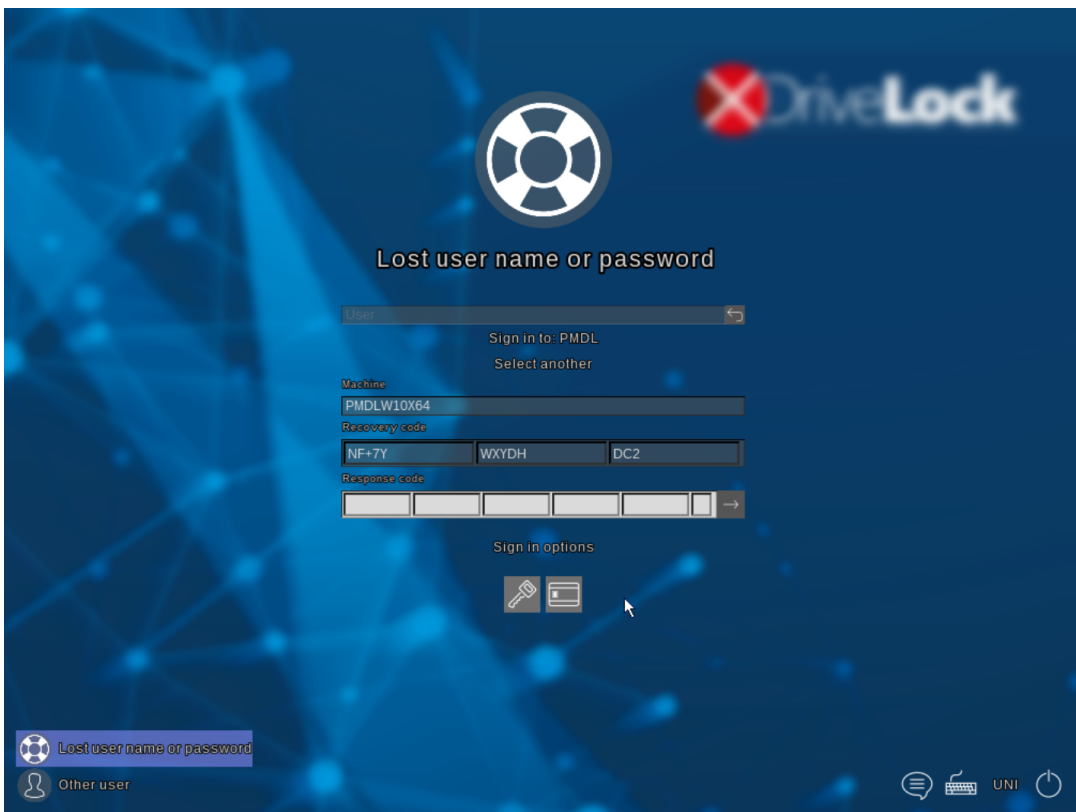
A ZIP file containing the diagnostic information is created in the location you specified.

12.4.2 Emergency Logon Procedure

There are three types of emergency logon procedures:

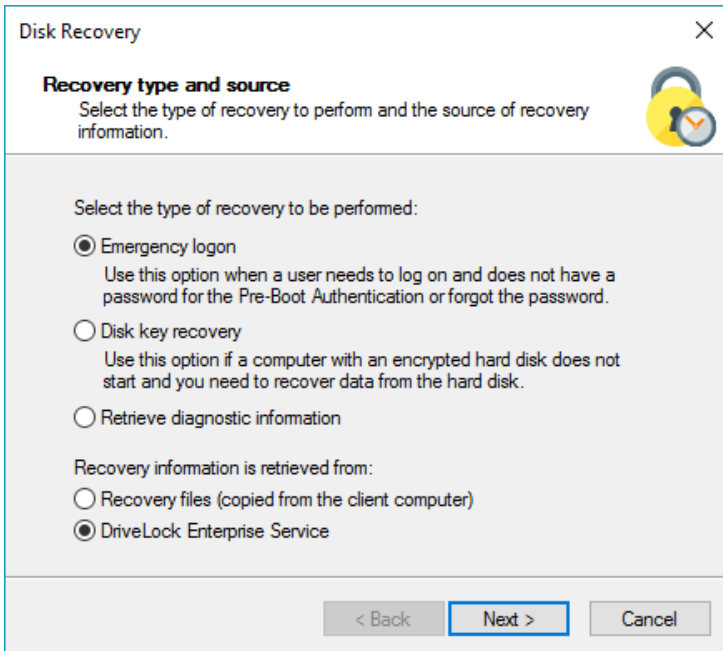
- Emergency logon with username
- Emergency logon without username
- Emergency logon for token users

You can configure which of these procedures are available to users during pre-boot authentication. Refer to the section [Configuring Emergency Logon Parameters](#) for details on how to configure these settings.



Click the *Lost user name or password* option in the PBA (new UEFI-PBA for Windows 10).

Open the DriveLock Management Console, select *Operating / Agent remote control*, open the context menu and select *Disk Protection recovery and tools / DriveLock Disk Protection recovery / emergency logon*.



Disk Recovery [Close]

Recovery type and source
Select the type of recovery to perform and the source of recovery information.

Select the type of recovery to be performed:

- Emergency logon
Use this option when a user needs to log on and does not have a password for the Pre-Boot Authentication or forgot the password.
- Disk key recovery
Use this option if a computer with an encrypted hard disk does not start and you need to recover data from the hard disk.
- Retrieve diagnostic information

Recovery information is retrieved from:

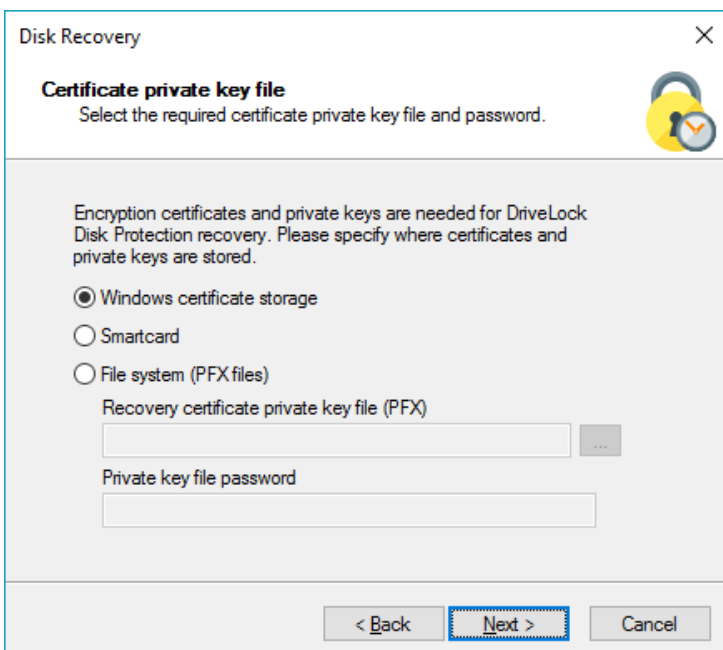
- Recovery files (copied from the client computer)
- DriveLock Enterprise Service

< Back **Next >** Cancel

Select *Emergency logon*.

If you have configured Disk Protection to send the client recovery keys to the DriveLock Enterprise Service, select the **DriveLock Enterprise Service** option. If you want to specify the path to the required recovery keys later, select '**Recovery files (copied from the client computer)**'.

Click **Next** to continue.



Disk Recovery [Close]

Certificate private key file
Select the required certificate private key file and password.

Encryption certificates and private keys are needed for DriveLock Disk Protection recovery. Please specify where certificates and private keys are stored.

- Windows certificate storage
- Smartcard
- File system (PFX files)
Recovery certificate private key file (PFX)
 ...
- Private key file password

< Back **Next >** Cancel

To perform emergency logon procedures you need to access the private key of the recovery certificate. To access a private key that was stored in a file, specify the path where the file **DLFDERecovery.pfx** file is located and type the password that is used to protect the private key. To access a private key that was stored on a smartcard, select "**Smart card**".

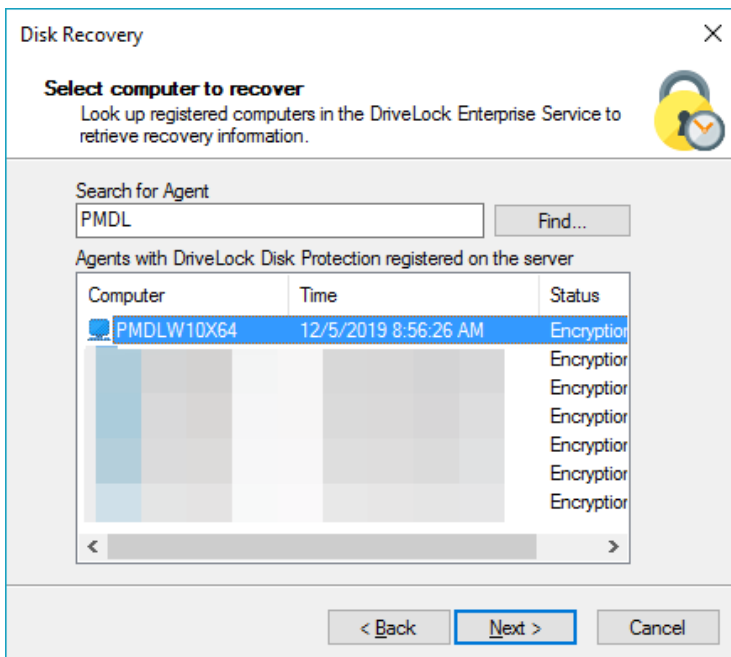
If you previously imported the certificate and private key into your local certificate store, select "**Windows certificate storage**".

If you lost access to the private key, recovery is no longer possible.

Click **Next** to continue.

If you selected a smartcard, you will be prompted to insert the smartcard. Details depend on the smartcard you are using.

If you selected the option to retrieve recovery information from the DriveLock database, the following dialog box appears.



To search for Agents registered within the DriveLock database, type the computer name or part of the name and then click **Find**. DriveLock FDE displays all registered computers that contain the text you typed as part of their names. To view a list of all registered computers, don't type any text and then click **Find**.


Select the appropriate computer from the list and then click **Next** to continue.

If you selected to retrieve recovery information from a file, type the path for the location of the recovery file or click the "..." button to open the file selection dialog box.

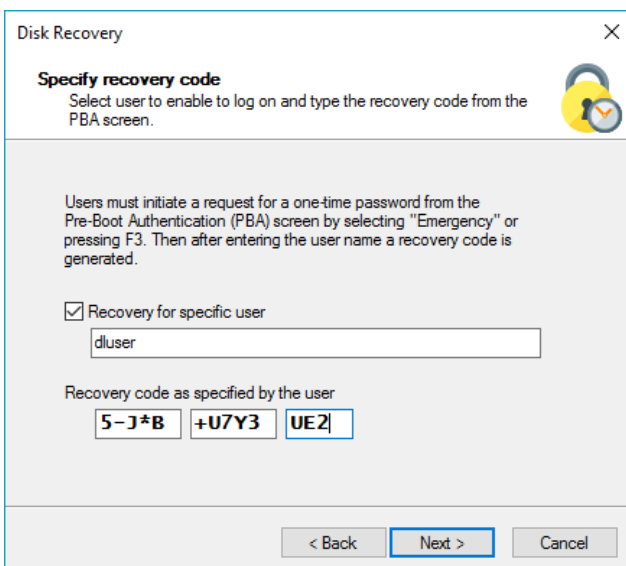
Each client computer has its own envelope file, which must be used for emergency logon recovery procedures. If you have configured DriveLock FDE to upload this file automatically to a central shared folder, the file name is prefixed with the name of the client computer (for example: DE2319WX_ RecoveryEnvelope.env).

Click **Next** to continue.

If the user has previously logged in to pre-boot authentication, ask them to enter their user name (*emergency logon procedure with user name*) and press **Enter** (new UEFI PBA for Windows 10):



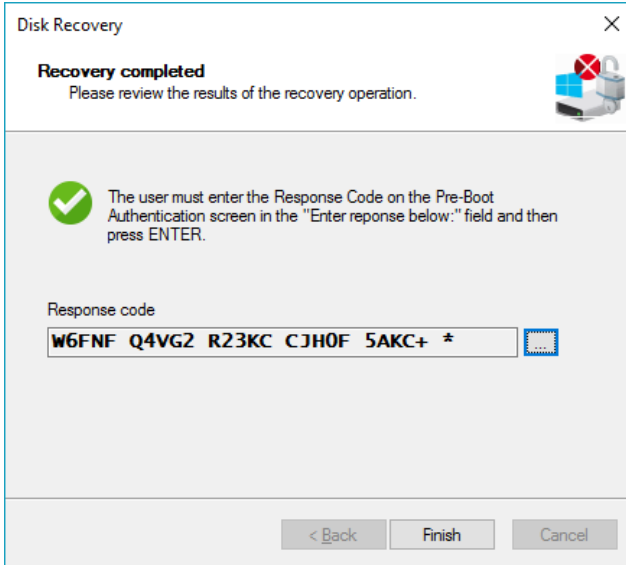
If the user has never logged in to pre-boot authentication or if PIN authentication is used, it is not necessary to enter a name (*emergency login procedure without user name or emergency login procedure for token users*).



Enter the user name (for recovery with a user name) and the recovery code provided by the user.

The user must enter or select correct values for user name and domain first.

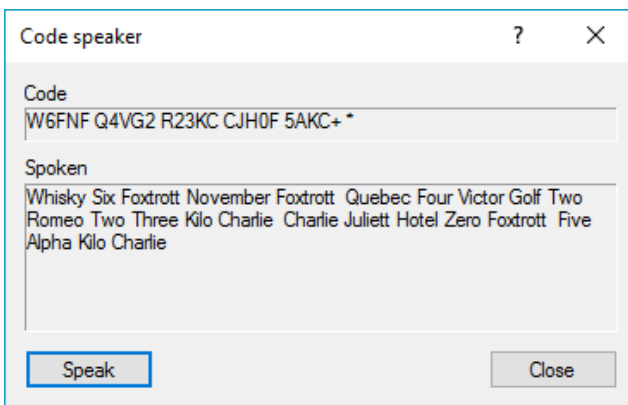
Click **Next** to generate the response code for the user.



If you selected a smartcard, you will be prompted for the PIN that is required to access the smartcard.

If an error occurs when generating the response code, DriveLock displays a warning message.

Click "..." to get help with the transmission of the code:



In this case, click **Finish** and restart the restore process.

The user must enter the generated response code in the following field and click the arrow icon to the right (or press **Enter** after entering the last character) (new UEFI-PBA for Windows 10):



At this point, Windows will continue to start normally.

12.4.3 Recovering Encrypted Disks

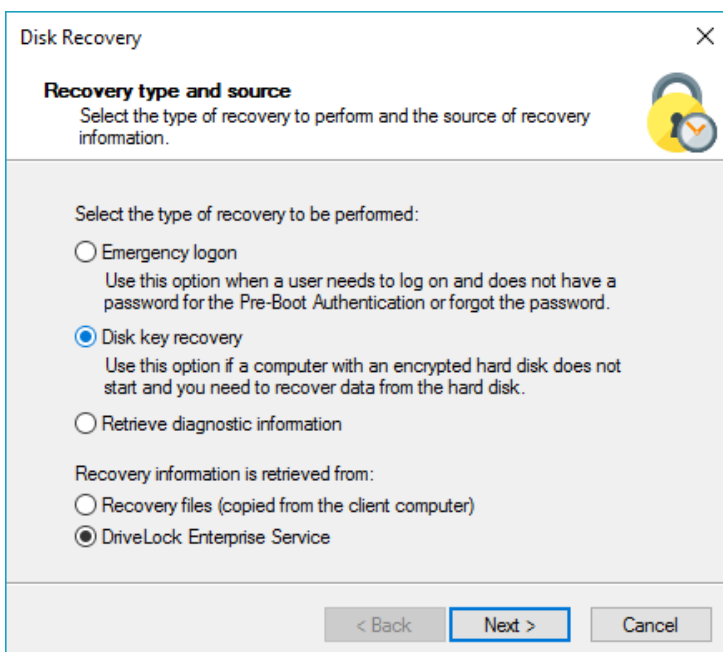
Disk recovery is necessary when local disk drives can no longer be accessed. This can occur, for example, when data sectors of the drive have become corrupt.

To recover (decrypt) an encrypted disk you must perform the following steps:

1. Create the recovery files
2. Copy all the files that are required for decryption to a floppy disk, removable USB drive or to a recovery CD.
3. Start the computer using the recovery CD or other bootable media.
4. Use the files on the recovery media to decrypt the inaccessible hard disk.

The steps for creating a Recovery CD are described in more detail below.

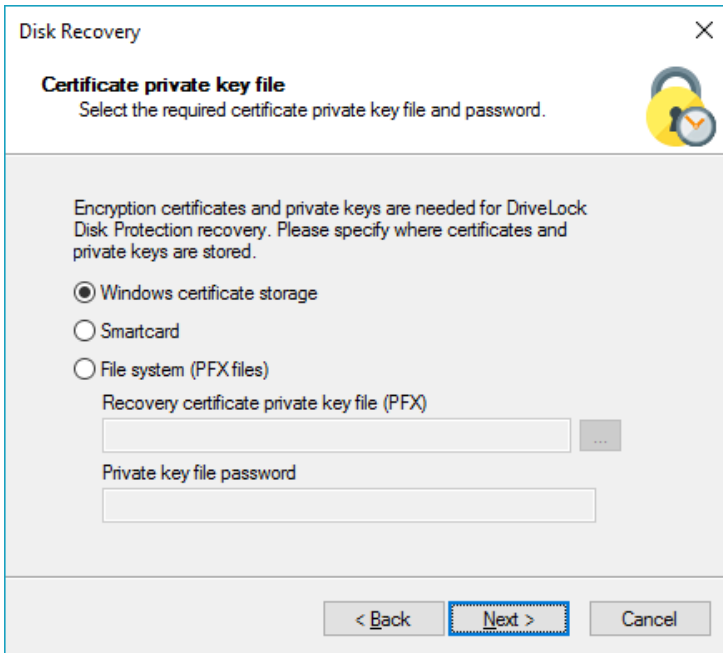
12.4.3.1 Creating the Files Required for Decryption



Select **Disk key recovery** as the recovery type.

If you configured DriveLock FDE to send the client's recovery disk keys to the DriveLock database, select **DriveLock Enterprise service connection (DES)**. To specify a file as the location of the required recovery disk keys, select **Recovery files (copied from the agent computer)**.

Click **Next** to continue.



For disk recovery procedures you need to access the private key of the recovery certificate. If the private key was stored in a file, specify the path where the file **DLFDEMaster.pfx** file is located and type the password that is used to protect the private key. To access a private key that was stored on a smartcard, select **"Smart card"**.

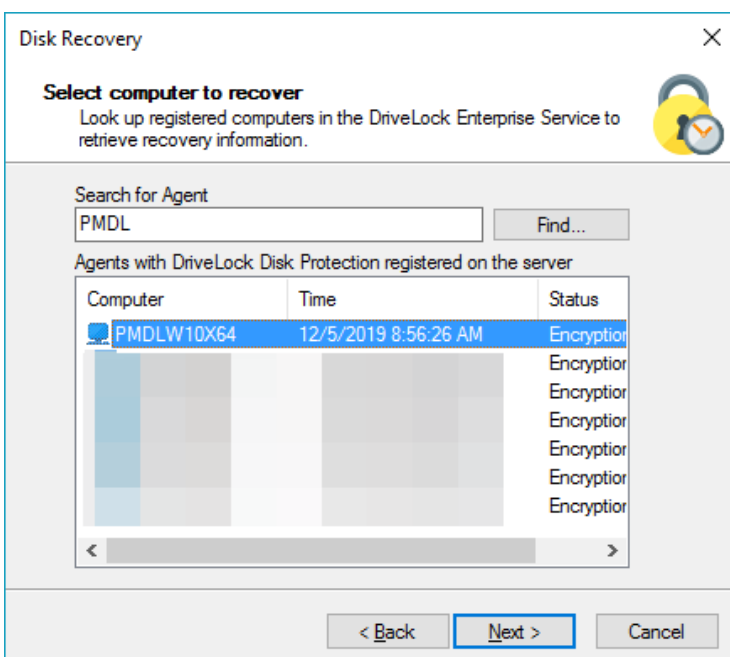
If you previously imported the certificate and private key into your local certificate store, select the option **"Windows certificate storage"**

If you lost access to the private key, recovery is no longer possible.

Click **Next** to continue.

If you selected a smartcard, you will be prompted to insert the smartcard. Details depend on the smartcard you are using.

If you selected the option to retrieve recovery information from the DriveLock Enterprise Service, the following dialog box appears.



To search for registered Agents on the DriveLock Enterprise Service, type the computer name or part of the name and then click **Find**. DriveLock Disk Protection displays all registered computers that contain the text you typed as part of their names. To view a list of all registered computers, don't type any text and the click **Find**.

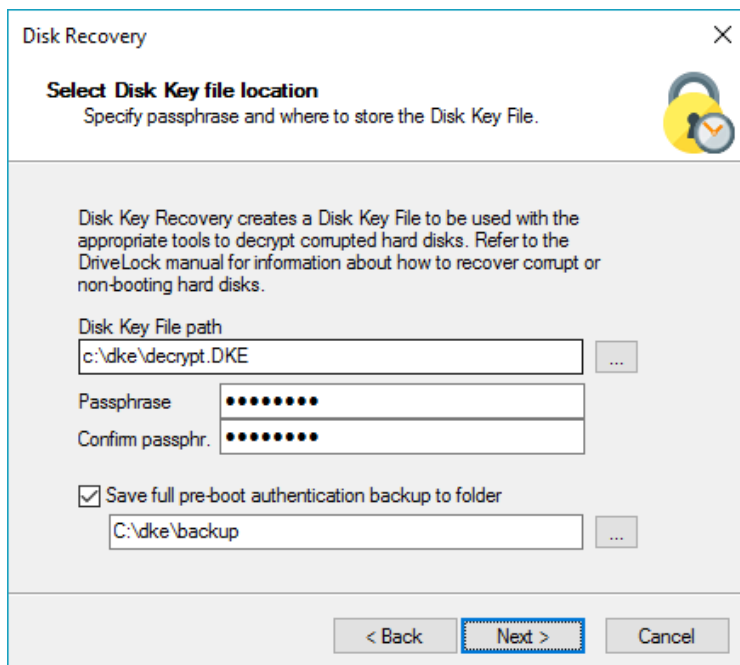
Select the appropriate computer from the list and then click **Next** to continue.

If you selected to retrieve recovery information from a file, type the path for the location of the recovery file or click the "...” button to open the file selection dialog box.

Each client computer has its own disk recovery file, which must be used for emergency recovery logon procedures. If you configured DriveLock FDE to upload this file automatically to a central shared folder, the file name is prefixed with the name of the client computer (for example: *DE2319WX_Backup.zip*).

The EFS disk recovery files are automatically generated by the DriveLock Agent when it starts encrypting hard disks.

Click **Next** to continue.



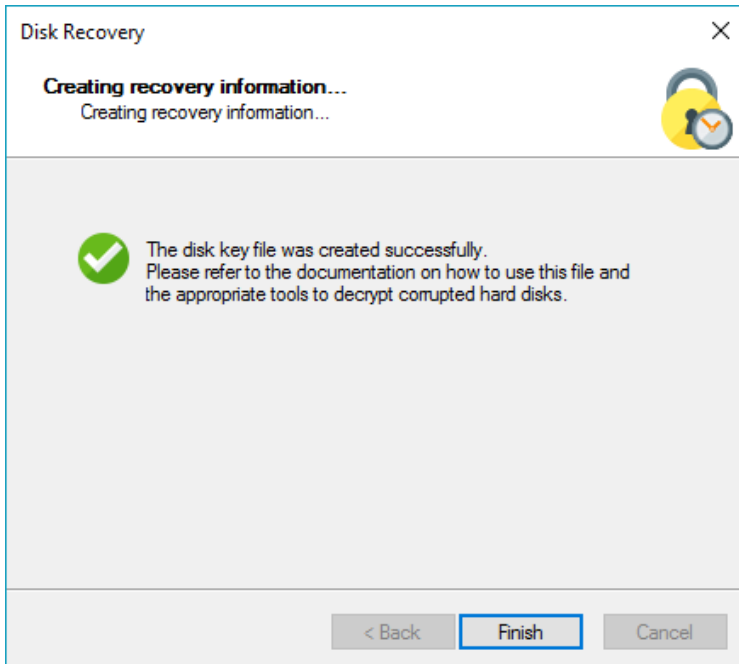
To allow for recovery, DriveLock Disk Protection must generate a Disk Key File. To specify a file name and path, click the "...” button, or type the path and file name, including the file extension (**.dke**).

Type a password or passphrase to secure access to this file and confirm this password by typing it again. The password must at least contain 6 characters. You will need to provide this password during the disk recovery operation.

Select the **“Save full pre-boot authentication backup to folder”** checkbox and type the path for the location of the Backup.zip file that contains all recovery data stored in the DriveLock database for this computer.

Click **Next** to generate the Disk Key File.

If you selected a smartcard, you will be prompted for the PIN that is required to access the smartcard.



If the procedure was successful and a Disk Key File has been created, DriveLock displays a completion message.

Click **Finish** to close the wizard.

Copy the Disk Key files you created to a floppy disk, USB drive or the Recovery CD image. You will need access to the files during the recovery operations described in the following sections.

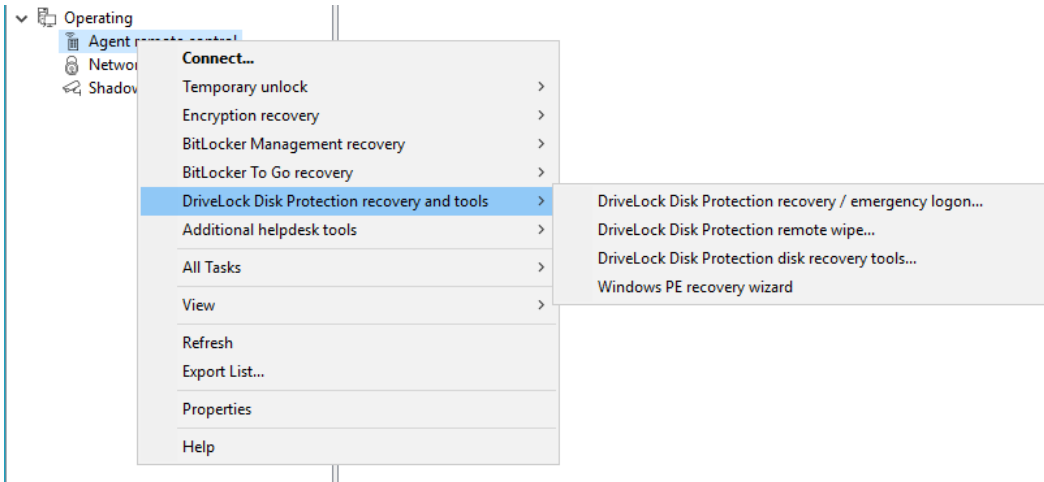
12.4.3.2 Creating Recovery Media

To recover data from a disk that has become inaccessible due to disk failure or failure of the operating system to start, you need to start the computer from bootable media, such as a Recovery CD.

You only need one recovery medium for your system environment, because the individual recovery file is copied to another USB stick.

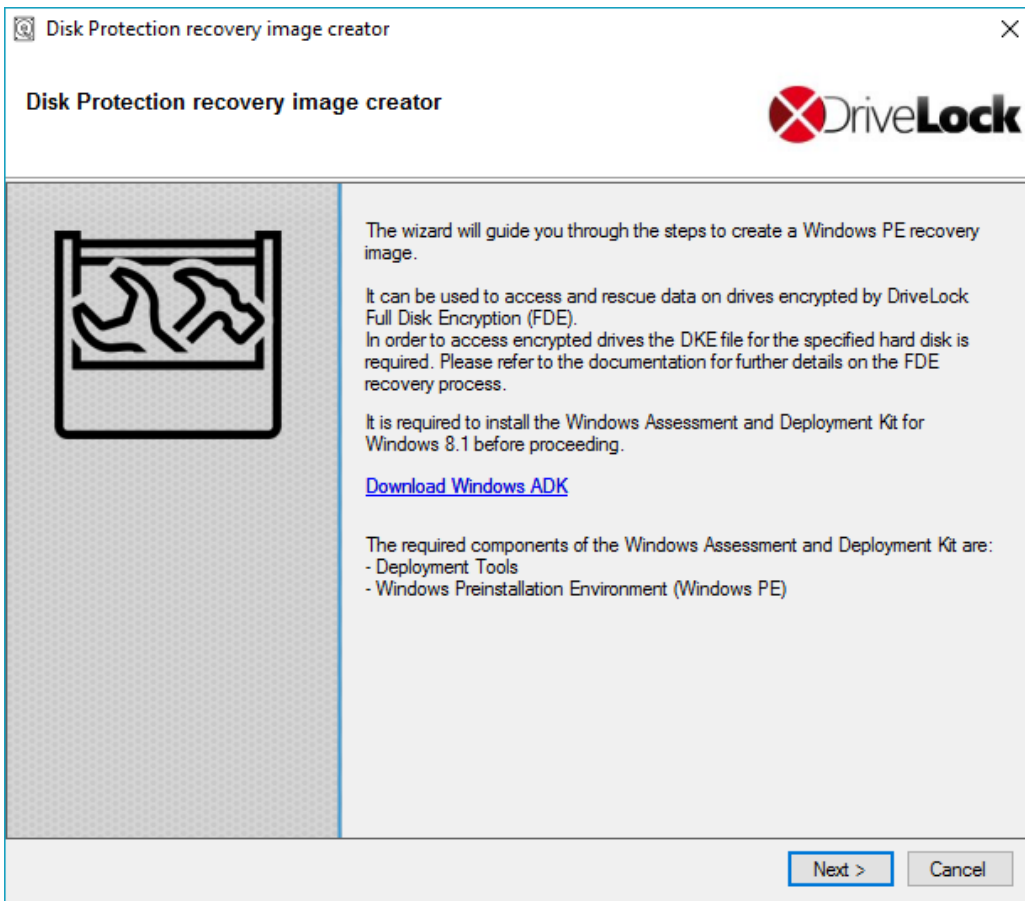
Before you start the wizard, make sure you meet the following requirements:

- You have administrative privileges on your computer to install the *Windows Assessment and Deployment Kit (ADK)* (if not already installed).
- The current DriveLock Management Console is installed on your computer.
- A USB stick (min. 1GB) or a writable CD for the Windows PE recovery medium is ready.



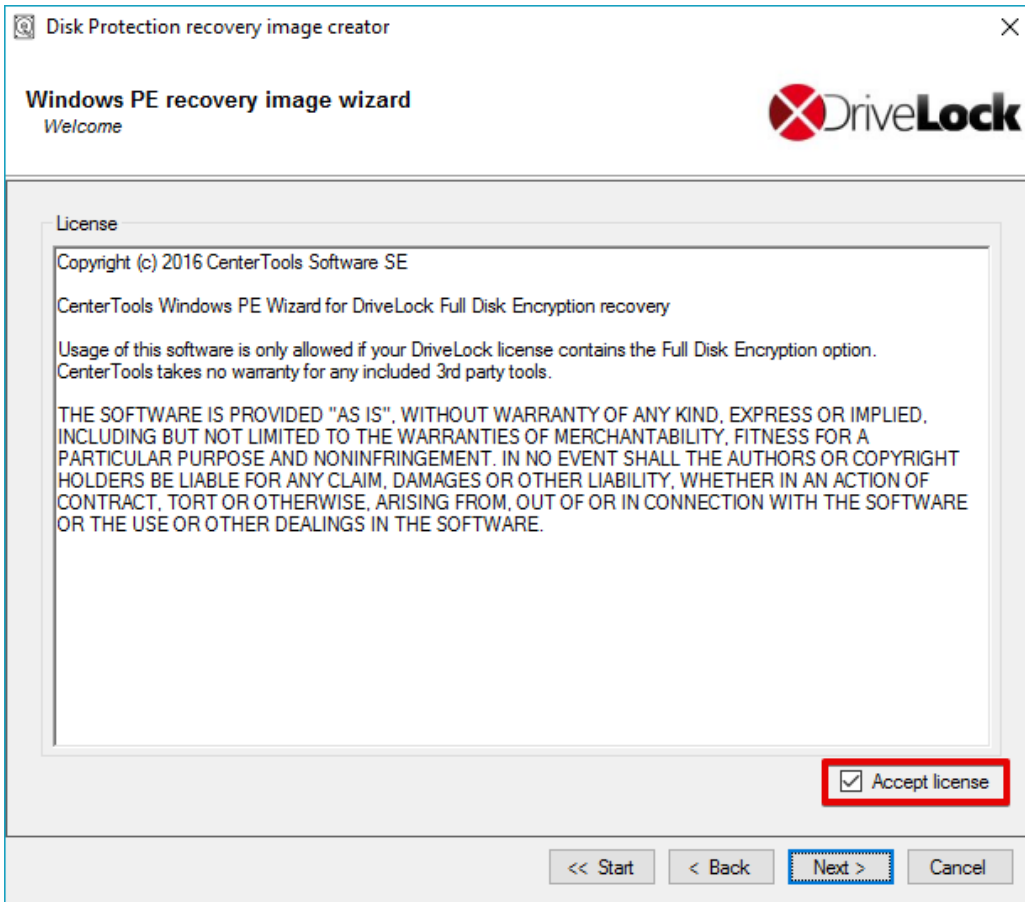
To create a Windows PE CD, in the DriveLock Management Console, right-click *Operating* -> *Agent remote control* and then click **Disk Protection disk recovery and tools**.

Select *Windows PE-based recovery wizard*.

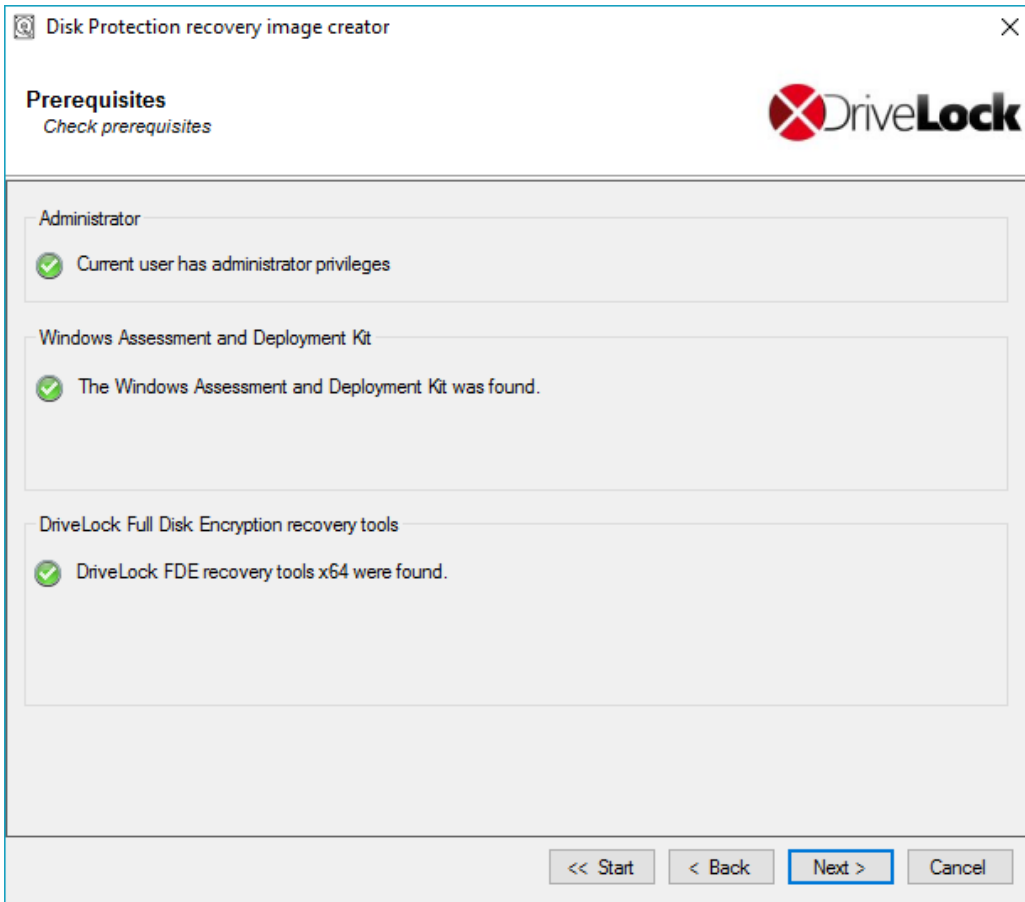


If you have not yet installed or downloaded Windows ADK, you can do so using the link displayed. The Windows ADK must be installed for the next steps.

Click **Next**.

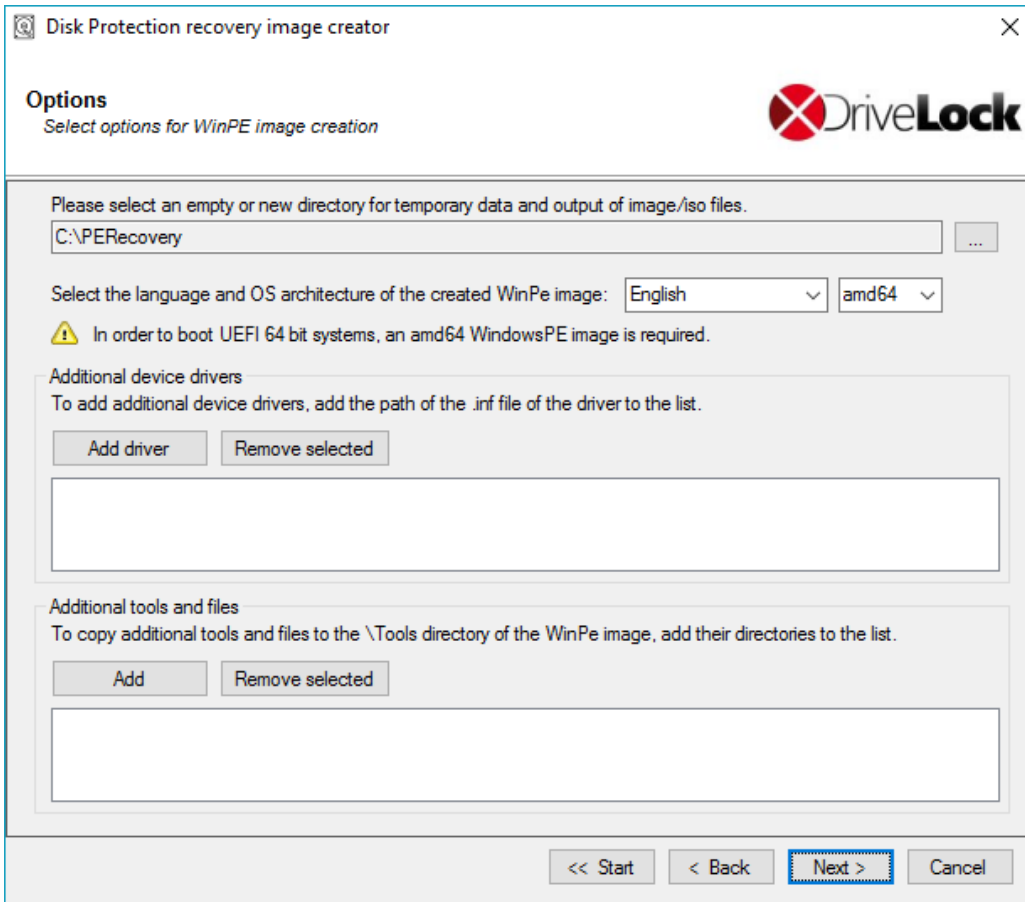


Enable "Accept license" and click **Next**.



Check that all prerequisites are met and that they have a green checkmark.

Click **Next**.

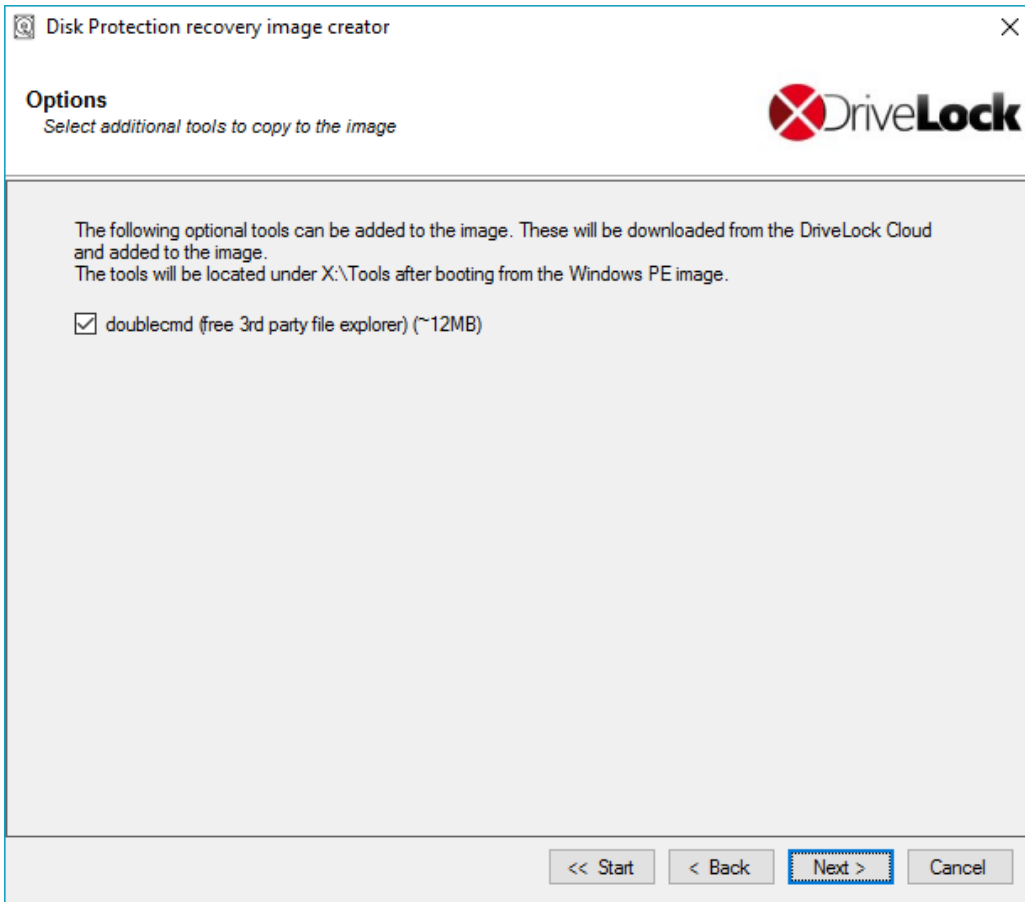


Enter the directory where the output files will be written to. Also select the language and the target architecture of the Windows PE environment you want to use.

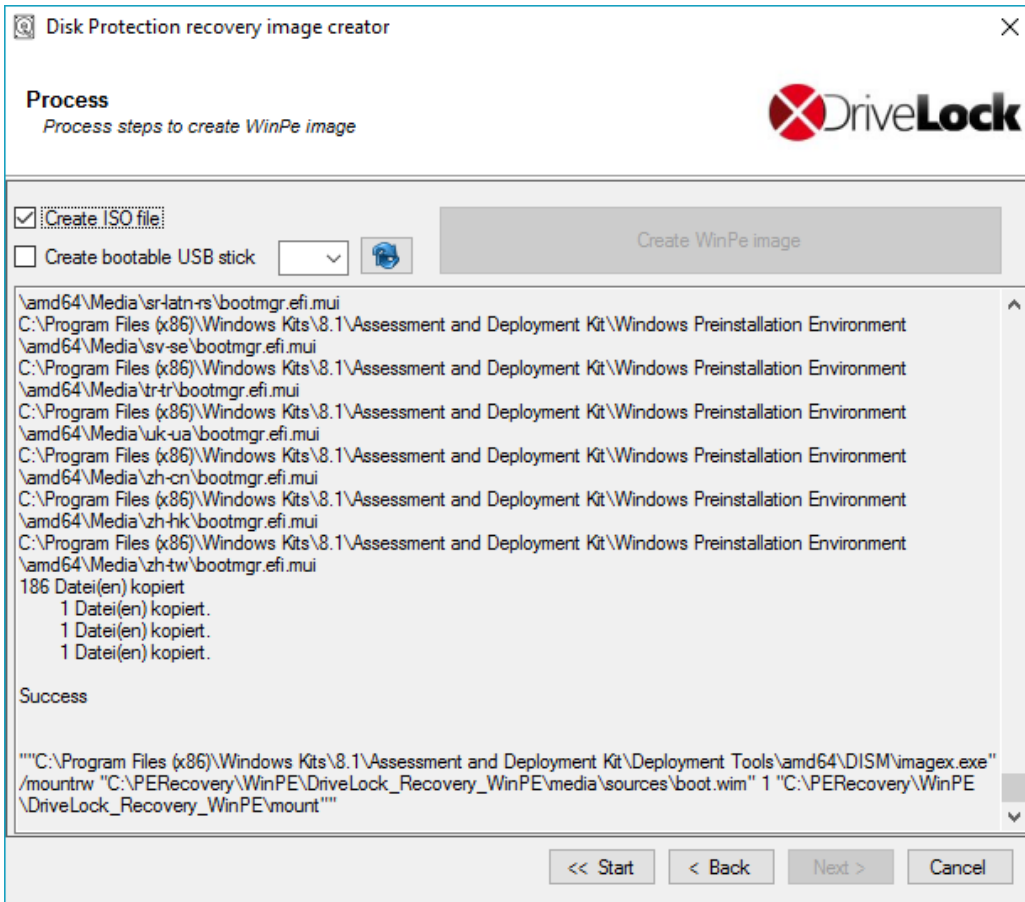
On UEFI systems it is mandatory to select the architecture "amd64".

You can specify additional drivers and tools you want to add to the Windows PE environment. This may be additional hard disk drivers or any other tools that can be run without an installation (e.g. antivirus scanners, backup tools, other third-party tools, etc.).

When you are done making changes, click **Next**.

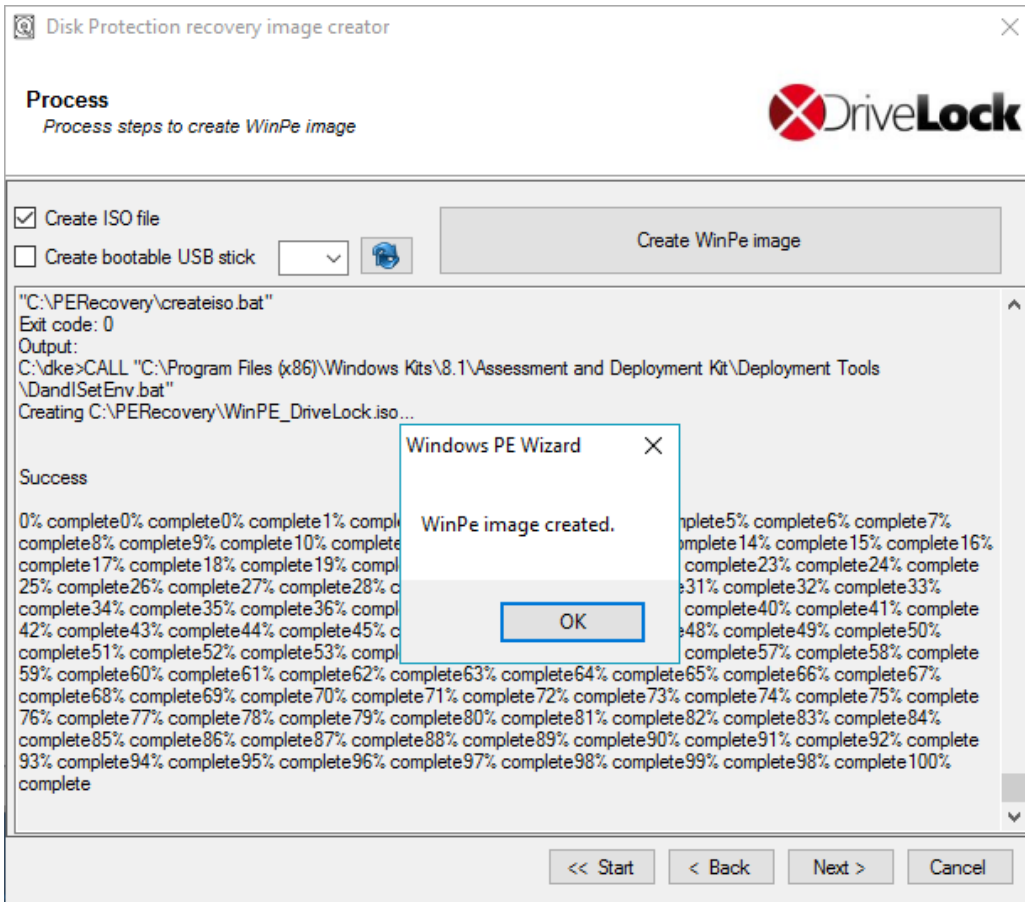


In addition, you can now add a freely available file explorer available from our Cloud CDN.
Click **Next**.



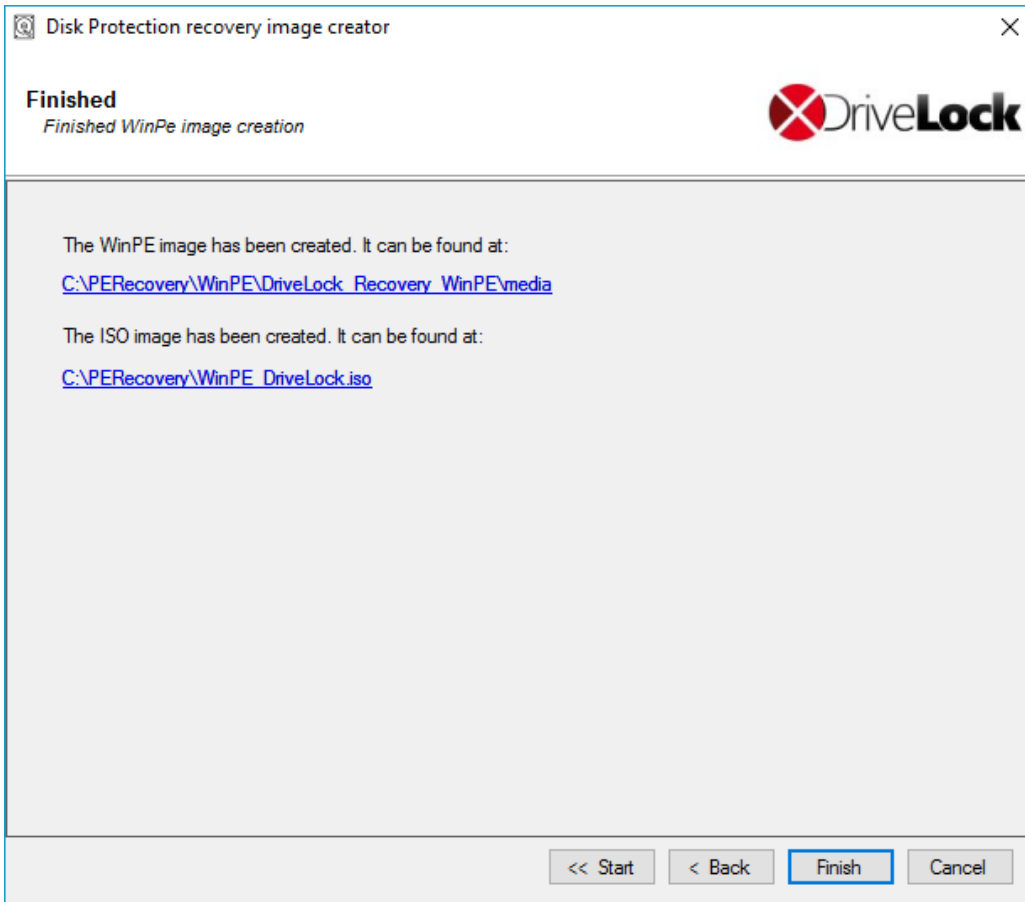
Next, select whether you want to create a bootable ISO file or a bootable USB stick. If you do not select any, only a file structure will be created, which you have to copy manually to a bootable medium.

Start the automatic process by clicking Create WinPe image.



As soon as the process is completed, you will get a notification.

Click **Ok** and then **Next**.



When the process is finished, you will see the links to the respective directory.

Click **Finish** to complete the wizard.

The Recovery CD contains all tools and drivers that are required to perform a disk recovery.

12.4.3.3 Recovering Disks

Before you can start the recovery, make sure you meet the following requirements:

- The *.pke file required for the computer was created and copied to a USB stick.
- You have created a bootable Windows PE recovery media.

Now boot the computer from the recovery medium. Then you will see a command line window with a list of available disks (volumes). To display this list again, use this command: `echo lis vol | diskpart`

```

Administrator: X:\windows\system32\cmd.exe - diskpart
X:\windows\system32>wpeinit
X:\windows\system32>cd ..\..\DriveLock
X:\DriveLock>peprep.exe /usb
SafeNet ProtectDrive peprep.exe Version: 9.4.8.33
USB support installed.
X:\DriveLock>diskpart
Microsoft DiskPart version 6.2.9200
Copyright (C) 1999-2012 Microsoft Corporation.
On computer: MININT-KN5DIRF
DISKPART> lis vol

   Volume ###  Ltr  Label          Fs          Type          Size      Status       Info
   -----
   Volume 0     F    DUD_ROM        UDF         DUD-ROM       177 MB    Healthy
   Volume 1     C    System Rese    NTFS        Partition     350 MB    Healthy
   Volume 2     E                    NTFS        Partition     59 GB     Healthy
   Volume 3     D                    RAW         Partition     2045 MB   Healthy
   Volume 4     G    DRIVELOCK     FAT         Removable     955 MB    Healthy

DISKPART> _
    
```

Encrypted volumes are displayed in the *Fs* column as *RAW*. Memorize the drive letter of the USB stick that contains the recovery file (if necessary, insert the stick and display the list again).

Enter the command `cd X:\DriveLock`.

Use the following command to introduce the recovery key for decryption to the system:

```
peprep -inj <USB drive letter>:\<path to disk key file>
```

The command in this example is `peprep -inj G:\PMDLW8X84.DKE`. Now enter the password that you used to create the DKE file.

Run the command `echo lis vol | diskpart` again to see if the recovery key was successfully added.


```

Administrator: X:\windows\system32\cmd.exe - diskpart
1 Dir(s) 1,000,521,728 bytes free

X:\DriveLock>peprep -inj g:\PMDLW8X64.DKE
SafeNet ProtectDrive peprep.exe Version: 9.4.8.33
Determining data for encrypted drive D:\ succeeded.
Injecting disk key
Please enter the pass-phrase for file g:\PMDLW8X64.DKE
*****
Disk key successfully injected.

X:\DriveLock>diskpart

Microsoft DiskPart version 6.2.9200

Copyright (C) 1999-2012 Microsoft Corporation.
On computer: MININT-KN5DIRF

DISKPART> lis vol

   Volume ###  Ltr  Label          Fs          Type          Size      Status       Info
   -----
   Volume 0    F    DUD_ROM        UDF          DUD-ROM       177 MB     Healthy
   Volume 1    C    System Rese    NTFS         Partition     350 MB     Healthy
   Volume 2    E    Data           NTFS         Partition     59 GB      Healthy
   Volume 3    D    Data           NTFS         Partition     2045 MB    Healthy
   Volume 4    G    DRIVELOCK      FAT           Removable     955 MB     Healthy

DISKPART>
    
```

The drive is no longer displayed as *RAW* if successful.

Enter `Exit` to leave DISKPART.

You can now access the drive (provided there is no other critical issue) and copy important files or try to repair the hard drive.

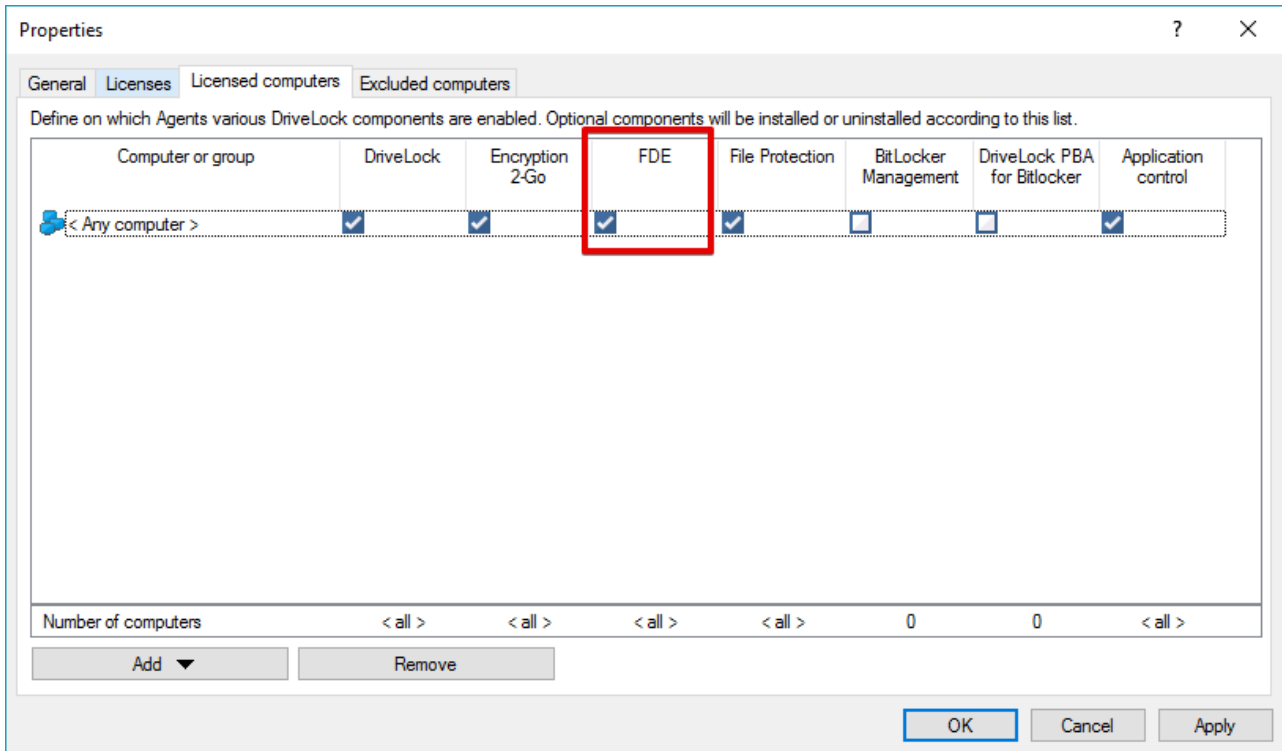
12.5 Uninstalling DriveLock Disk Protection

You can configure DriveLock Disk Protection to decrypt previously encrypted hard disks on client computers, to remove pre-boot authentication and to completely uninstall DriveLock Disk Protection.

Changes to the configuration settings in a DriveLock policy typically apply to all computers the policy is assigned to. To remove Disk Protection from a single computer, follow the steps in the section “Uninstalling or Reconfiguring Disk Protection on a Single Computer”.

12.5.1 Uninstalling DriveLock Disk Protection Completely

To completely uninstall DriveLock Disk Protection from a computer, remove this computer from the list of computers that have the FDE license. Simply remove the checkmark in the FDE column.



In contrast with previous versions of DriveLock, Disk Protection installation is entirely determined by a computer's license status.

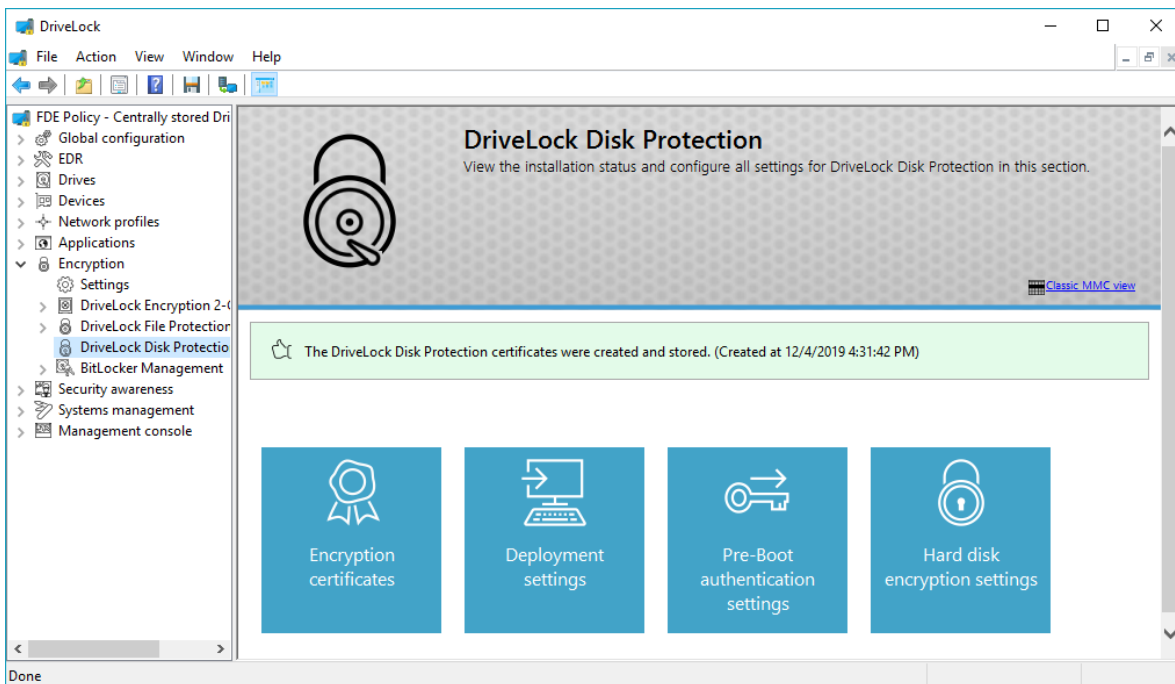
When the Agent receives the new configuration settings, it performs the following steps:

1. The Agent decrypts all encrypted hard disks
2. The Agent removes pre-boot authentication from the system
3. The Agent uninstalls DriveLock FDE

If you installed the DriveLock Disk Protection installation package *DLFde_<Version>.pkg* locally on the client and it is no longer required, you must delete it manually.

12.5.2 Decrypting Hard Disks

You can configure DriveLock Disk Protection to decrypt encrypted disk drives.



To disable encryption on client computers, click **Hard disk encryption settings**.

Clear the “**Encrypt local hard disk on Agent computers**” checkbox and then click **OK**.

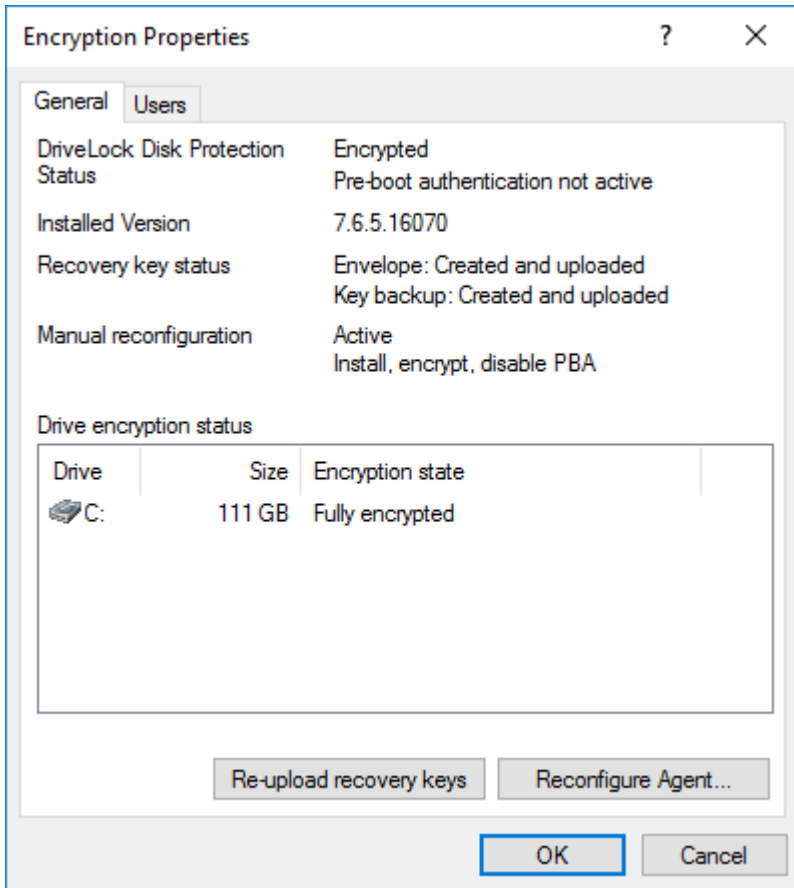
When the Agent receives the new configuration settings, it starts decrypting all encrypted hard disks.

|| Disk Protection and pre-boot authentication are not removed from the client computers. ||

12.5.3 Uninstalling or Reconfiguring Disk Protection on a Single Computer

To make changes to the DriveLock Disk Protection configuration on a single computer, such as uninstalling Disk Protection or decrypting a disk, you make this configuration change for that computer without having to change a policy that also applies to other computers. This is done using the Agent remote control function in the DriveLock Management Console.

First connect to the computer and then select **DriveLock Disk Protection Properties** from the context menu.



Click **Reconfigure Agent**.

This option is currently not available for the DriveLock PBA for BitLocker or the BitLocker hard disk encryption.

Reconfigure DriveLock Disk Protection

You can override DriveLock Disk Protection settings in your company policy on Agents. This replaces the settings configured here with the company policy that is applied to the Agent computer.

Override policy settings

Override general deployment settings

- Install DriveLock Disk Protection
- Enable pre-boot authentication
- Encrypt local hard disks

Pre-boot authentication settings

- Disable 32-bit pre-boot authentication
- Enable On-Screen-Keyboard in pre-boot authentication
- Disable USB support in pre-boot authentication

Override authentication methods

	Windows	Preboot
Local user access	<input type="checkbox"/>	<input type="checkbox"/>
Domain user access (with password)	<input type="checkbox"/>	<input type="checkbox"/>
Domain user access (with token)	<input type="checkbox"/>	<input type="checkbox"/>

Enable logon using "password tokens"

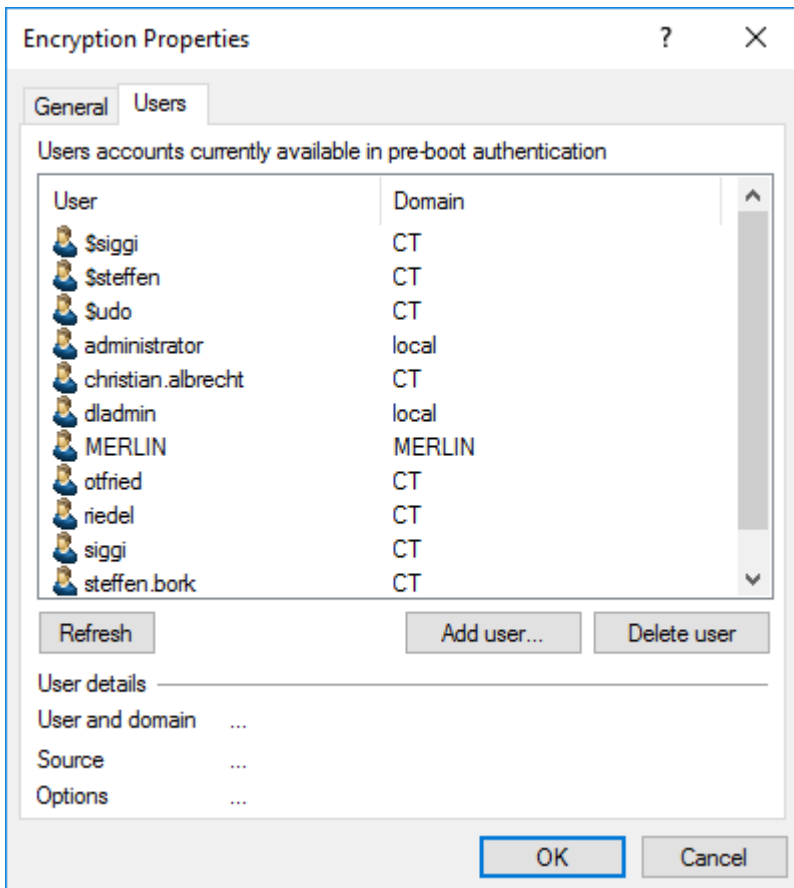
Require token PIN on Windows logon

Override emergency access methods

- Allow emergency logon with user name
 - Single Sign-on after emergency logon
- Allow emergency logon without user name
- Allow emergency logon for token users

OK Cancel

Check **Override policy settings** - variant to the central policy you now may configure computer specific settings. Open tab **Users** to see the users locally stored in the PBA. You may add or delete single users here.



12.6 User Logon

If you disabled pre-boot authentication in the System Policy settings, this section does not apply. Without pre-boot authentication the standard Windows authentication dialog box is displayed and normal Windows logon procedures apply.

12.6.1 UEFI Pre-Boot Authentication

The sections below provide information on system behavior when the DriveLock PBA is installed on a UEFI system.

Unlike earlier versions, you can no longer use function keys.

After starting a computer with activated PBA, you will see a message "DriveLock Pre-Boot Authentication" followed by the start screen:



Press any key or click with the mouse to go to the login screen as in Windows 10.

By pressing the following keys (hot keys) after the text display and before the start screen, you can prevent certain drivers from loading to avoid issues when starting the PBA on certain systems:

Key	Function
k	Default keyboard driver is not loaded
l	The PBA does not provide keyboard layouts other than English.
s	No smartcard support
a	Selects all of the above functions

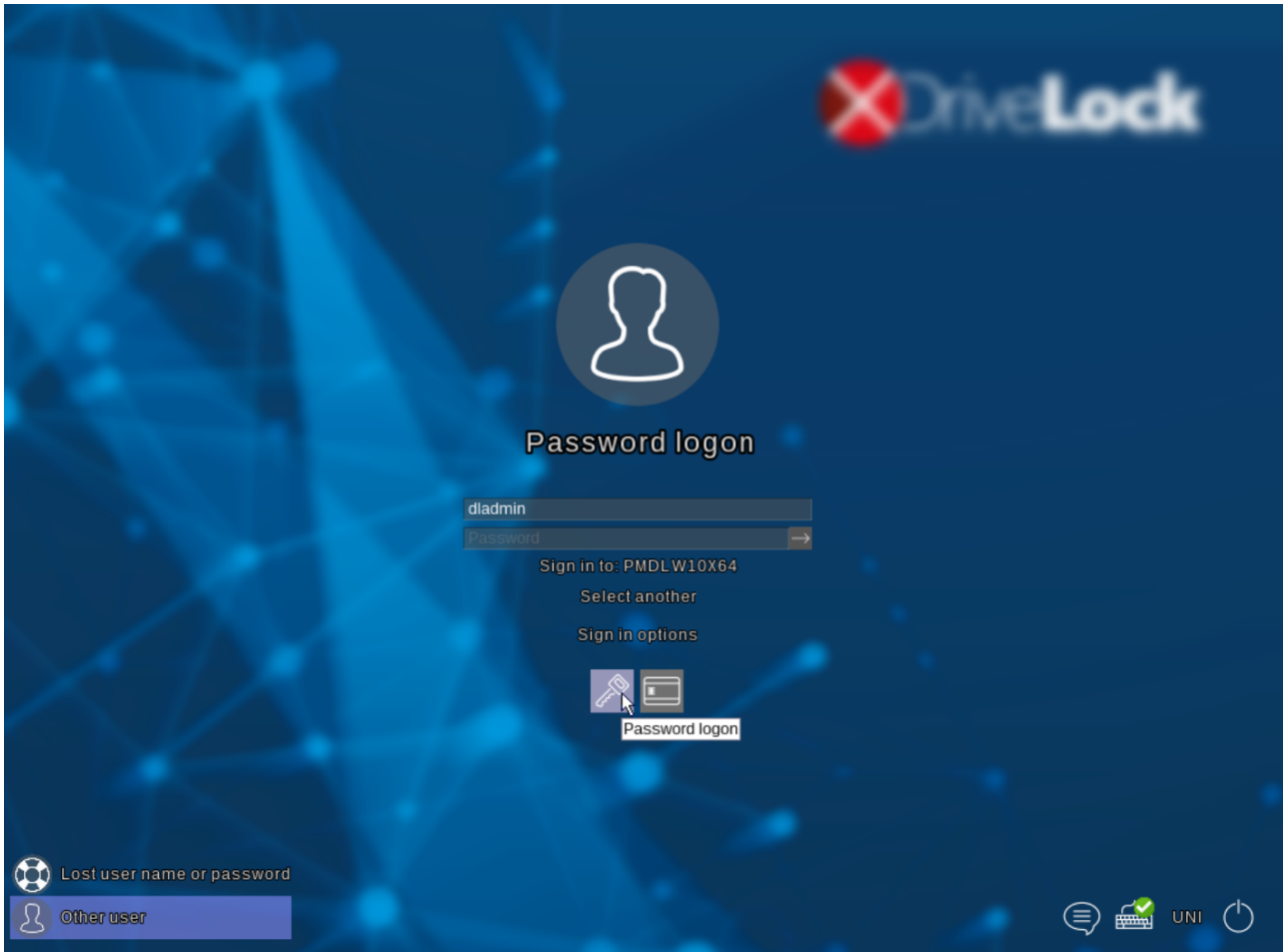
Then the system briefly displays the current status before loading the PBA:

```
DriveLock Pre-Boot Authentication

Toggle Keyboard Drivers
Result:
SmartCard Drivers: Y
Keyboard Drivers: N
Keyboard Layouts: Y
```

Hotkeys can be used to disable or enable one of these functions if it has been permanently activated or deactivated via the command line.

12.6.1.1 Authentication with User Name and Password

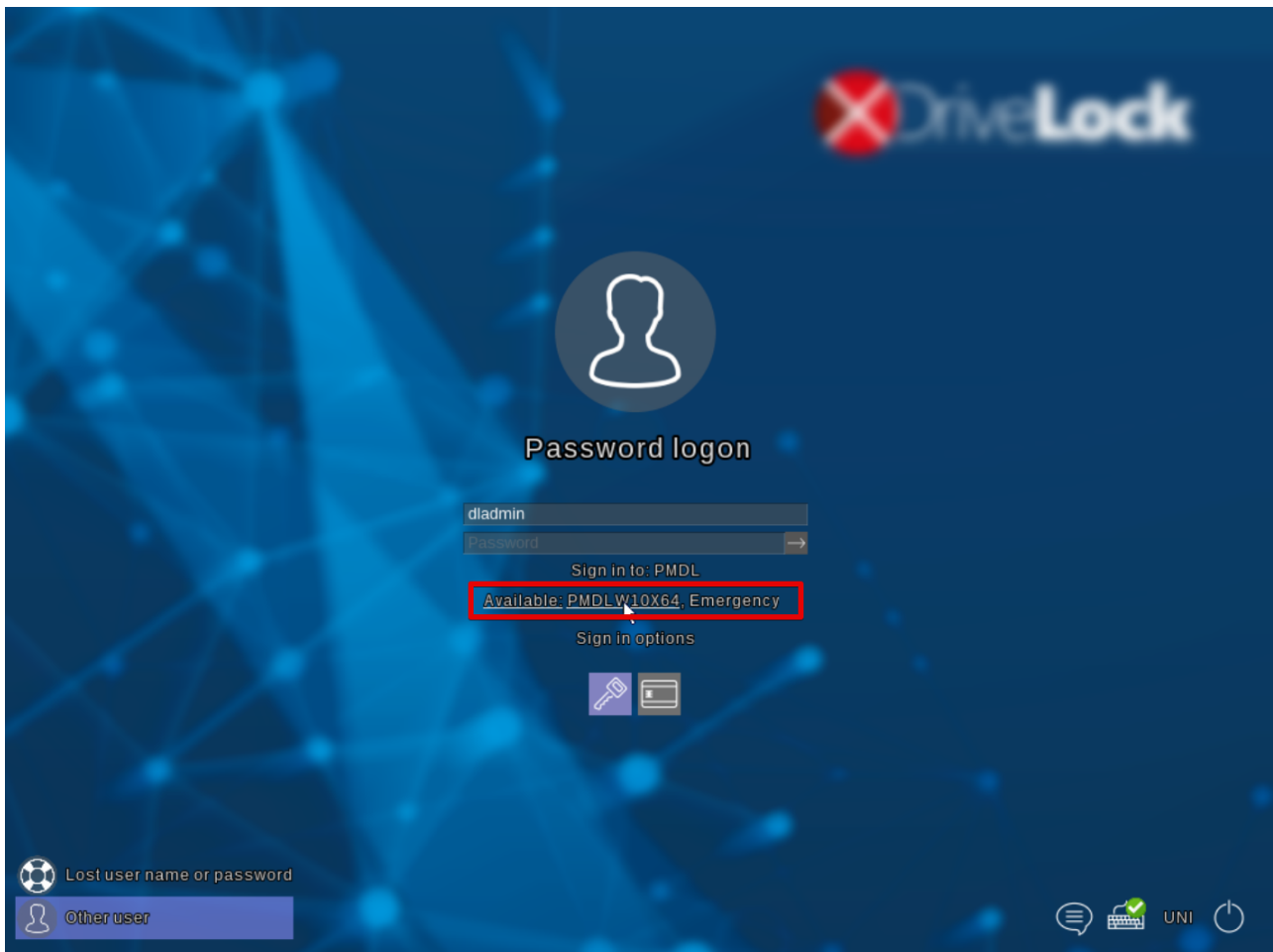


The DriveLock PBA supports both mouse selection and keyboard navigation.

If you prefer to use the keyboard only, move to the next element using the TAB key. Press ENTER or the space bar to select the active element. Press ESC to close the help text display.

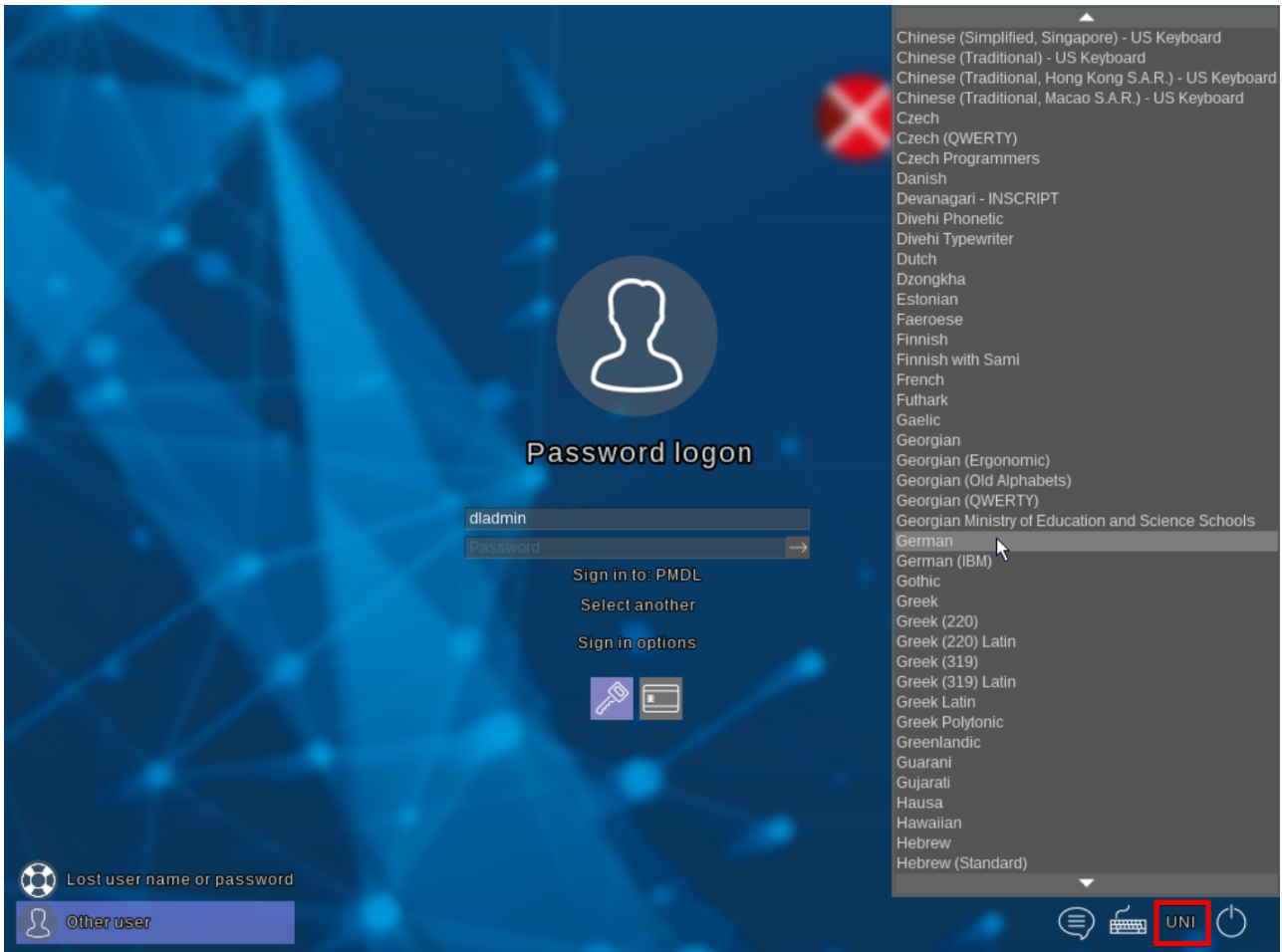
Enter the Windows user name and password in the appropriate fields to log in. The active domain is displayed after "Sign in to:".

If you click **Select another**, a list of all known domains appears, including the local computer and any manually created domains:



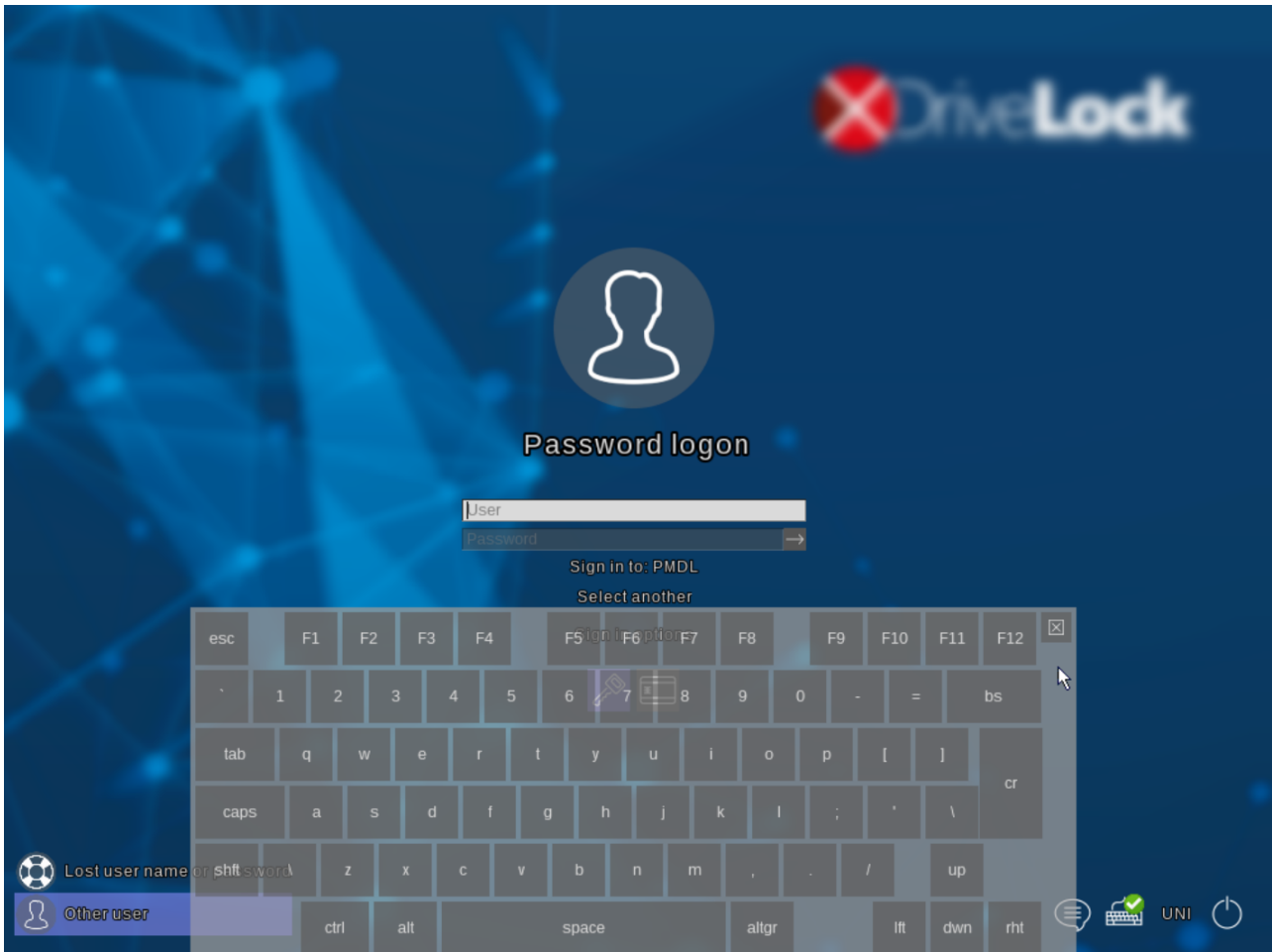
After having entered the correct password, the login starts as soon as you press the Enter key or click on the arrow symbol to the right of the password field.

The DriveLock PBA allows you to select other keyboard layouts. You can access the list of available layouts by clicking on the language icon in the lower right corner:



Select the keyboard layout you want. The next time you start the program, the previously selected layout is preset.

If you have enabled the virtual keyboard option (On-Screen Keyboard) in the policy, you can use the keyboard icon to control whether or not the virtual keyboard is displayed when you select an input field:

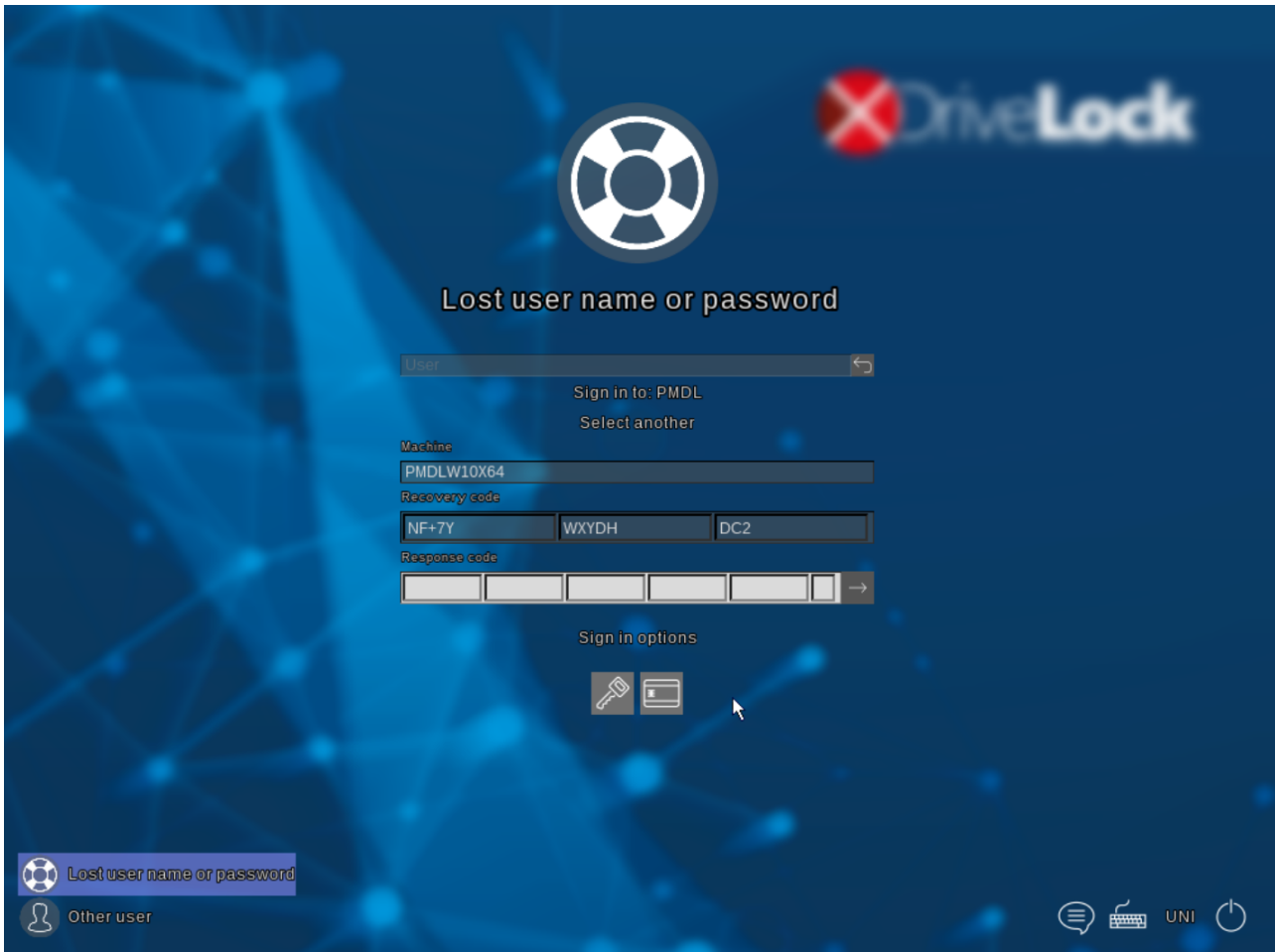


This allows you to log on to DriveLock PBA even on tablets that only have a touch screen and no physical keyboard.

The user or password input field must be activated so that the keyboard appears.

The keyboard layout you set will determine which keys the virtual keyboard will display.

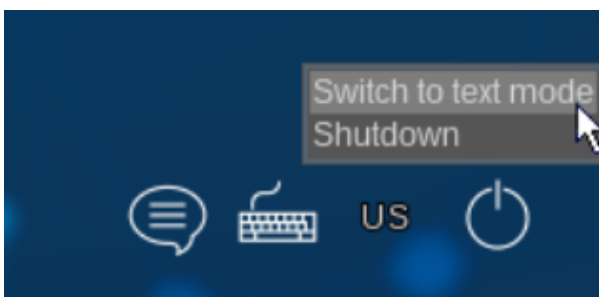
If you've forgotten your Windows password, click **Lost user name or password** in the lower left corner. The emergency logon dialog will then appear:



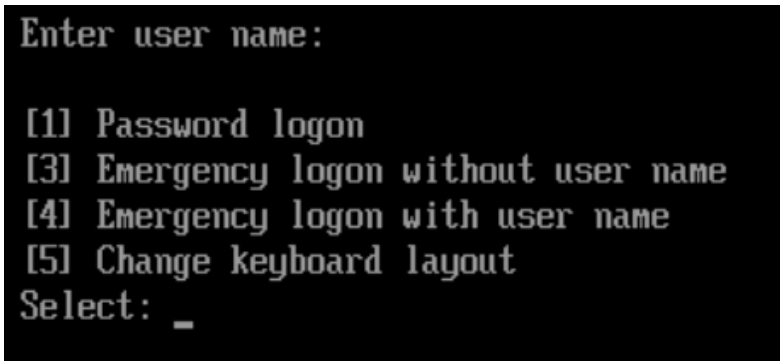
First, please make sure that you have selected the correct domain (usually not local).

See the chapter [Emergency logon procedure](#) for further steps on emergency logon.

By clicking the button in the bottom right corner you can either shut down the system or switch to text mode without graphical display.



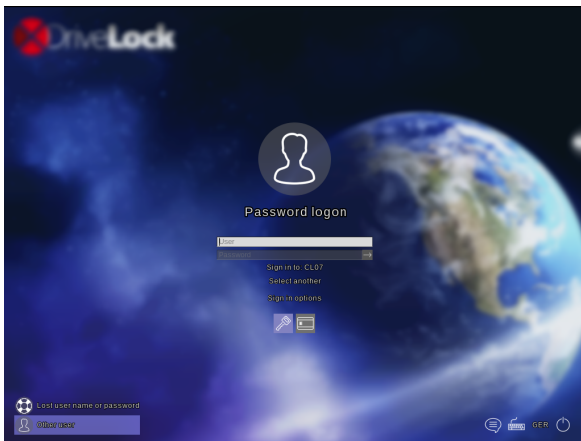
In text mode, only a simple console is available for logon or emergency logon:



Select the option you want by entering the displayed number and type in the required data.

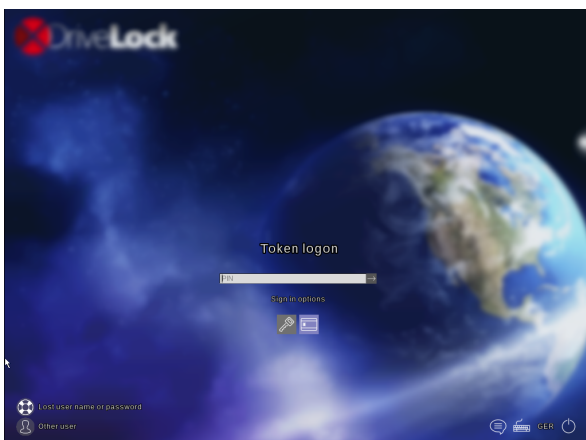
12.6.1.2 Smartcard Authentifizierung

The DriveLock PBA also allows authentication via smartcards or specific eTokens.



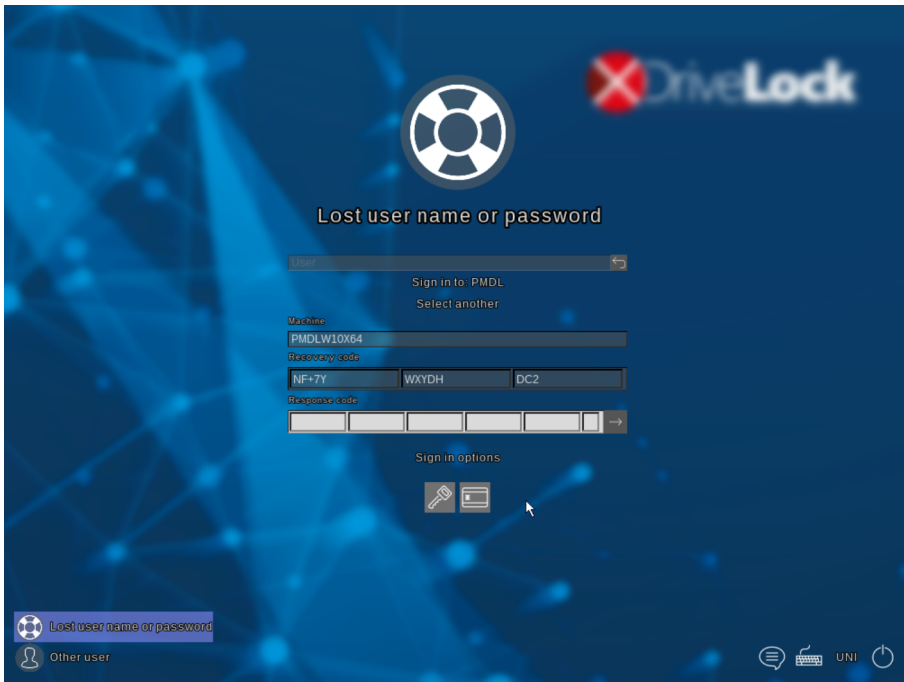
See the technical article "TA - Supported Smart Cards and Tokens in PBA.pdf", available also on the DriveLock ISO disk, for a list of currently supported smart cards and tokens.

Once the appropriate logon options have been enabled in the DriveLock policy, you can select them using the displayed icons just as you would for Windows logon.



Now enter the PIN for the smartcard or the token and press ENTER to log in.

If you forgot your PIN, click **Lost user name or password** in the lower left corner. The dialog for emergency logon will then appear:



First, please make sure that you have selected the correct domain (usually no local login) and that you have not entered a user name.

See chapter [Emergency logon procedure](#) for further steps.






12.6.2 BIOS Pre-Boot Authentication

The chapters below provide information on system behavior when Disk Protection PBA is installed on a legacy BIOS system.

Users can switch to the respective views/functions using the on-screen function keys.

12.6.2.1 Authenticating With User Name, Password and Domain Name

If the **Local user access** or the **Domain user access (password)** options are selected, the following logon screen is shown.

 Password [F1]	 Smartcard [F2]	 Emergency [F3]	 Settings [F4]	 Help [F5]
---	--	--	---	---

Login using user name, domain name and password.

User name:

Password: Show

Domain name:

If both authentication options *Local login* and/or *Domain user (with password)* are enabled, you can switch to the smartcard login screen by pressing the **F2** key.






The domain field lists all available domains if **Domain user access (password)** is allowed. If logon using local accounts is allowed, the local computer name is also listed in the Domain field. Use the *[Up-Arrow]* and *[Down-Arrow]* keys to scroll through the list of available domains.

To prevent password guessing, you can define a lockout policy to lock the computer after a configurable number of consecutive failed authentication attempts. To view details of failed logon attempts and other events use the Windows **Event Viewer**.

If a user can no longer log on to the system (for example, the user does not remember the correct password), it is possible to start the *emergency logon procedure with a user name*. For more information about this procedure, see chapter "[Emergency Logon Procedure](#)".

12.6.2.2 Authenticating With Smartcard or Token and PIN

If you selected the DriveLock FDE **Domain user access (token)** or **Shared Key Access** authentication checkboxes, the following logon screen is shown.

 Password [F1]	 Smartcard [F2]	 Emergency [F3]	 Settings [F4]	 Help [F5]
--	---	---	--	--

Login using smart card (token) and PIN.

Pin:

If both authentication options *Local login* and/or *Domain user (with password)* are enabled, you can switch to the Username/Password/Domain name screen by pressing the **F1** key.

If the **Local user access** or **Domain user access (password)** authentication options are also enabled, pressing the function keys to switch between the Username/Password/Domain Name logon screen and the Token/PIN logon screen.

To authenticate from this screen a user must insert a smart card or token and type the corresponding PIN. To prevent PIN guessing, you can define a lockout policy to lock the computer after a configurable number of consecutive failed authentication attempts. To view details of failed logon attempts and other events use the Windows **Event Viewer**.

If a user doesn't remember the correct PIN and therefore cannot logon to the system, the user can start the **emergency logon for token user procedure**. For details about this procedure, refer to the section "[Emergency Logon Procedure](#)".

12.6.3 Windows Authentication

Every time a user successfully logs on to Windows or changes the password in Windows, the user's current Windows password is synchronized with the pre-boot authentication database. The same happens when a user changes their personal password under Windows.

The login behavior depends on the setting in the DriveLock policy:

- *Automatic – Single Sign-On Mode Is Enabled*: users are automatically signed-on to Windows.
- *Manual – Single Sign-On Mode Is Disabled*: the Windows authentication dialog box appears and users enter their credentials to log in.



Part XIII

BitLocker Management and BitLocker To Go



13 BitLocker Management and BitLocker To Go

You can find the description for the DriveLock modules BitLocker Management and BitLocker To Go in a separate documentation on [DriveLock Online Help](#).



Part XIV

DriveLock Encryption 2-Go



14 DriveLock Encryption 2-Go

DriveLock has advanced encryption capabilities that allow you to encrypt sensitive information easily, quickly and securely.

DriveLock Disk Protection (FDE) encrypts entire hard drives in computers and also includes preboot authentication. DriveLock FDE is covered in detail in a separate chapter of this manual.

DriveLock Encryption 2-Go lets you securely encrypt external drives or storage media, such as USB flash drives or SD cards. You can also use DriveLock Encryption 2-Go to securely and irreversibly delete sensitive data using one of several standard methods.

This chapter describes how to configure settings that determine how DriveLock Encryption 2-Go functions, including the encryption parameters it uses. The use of encrypted external drives and media is described in the DriveLock User Guide.

With DriveLock 7.5.8 or higher you may either

- use the **Container based (DriveLock Encryption 2-Go)** as it was default in former DriveLock versions or
- use the **File based (DriveLock File Protection)** encryption as it was possible only with the DriveLock File Protection add-on or
- use **Container based and File based** in parallel and let the user decide.

In the DriveLock policy open **Encryption / Settings / Available encryption** methods and select the desired option.

To use DriveLock File Protection with network shares, you still need a DriveLock File Protection license.

For more information about DriveLock File Protection see chapter [DriveLock File Protection](#).

14.1 How DriveLock Encryption 2-Go Works

You can create and manage encrypted drives that consist of container files (encrypted archives). Access to encrypted drives is secured by passwords. Each encrypted drive can be accessed by typing a user password that is unique to the drive. In addition, a centrally configured administrative password enables data recovery, providing access to the data when a user's password is not available. An alternative password recovery procedure enables offline password recovery.

Encryption converts data to a format that makes it appear like random data to anyone who does not have the password that's required to decrypt the data. When you create an encrypted drive, all files and all empty space on that drive is encrypted. The encryption algorithm you select when you create the drive determines how data on it is encrypted.

On computers with modern processors that include hardware-based encryption (AES NI), DriveLock File Protection takes advantage of this functionality for approximately 4 times better performance.

14.1.1 DriveLock Encryption Algorithms

DriveLock supports the following encryption algorithms:

- *AES (recommended)* - The Advanced Encryption Standard (AES) is a symmetric encryption mechanism that was chosen by the National Institute of Standards (NIST) as successor to DES and 3DES in October 2000. It is also called the Rijndael algorithm for its developers Joan Daemen and Vincent Rijmen. DriveLock uses a 256-bit key (AES-256), which is considered sufficient also for top secret information (U.S. CNSS (Committee on National Security Systems)).
- *Triple DES* - Triple DES (3DES) is a symmetric encryption method based on the older DES (Data Encryption Standard) but works with twice the key length (112 bit) of its predecessor. Data is encrypted using three

successive DES operations. Because of the key length, 3DES is regarded as a relatively safe method for encrypting most data, unlike DES, which is more susceptible to brute-force attacks.

- *Blowfish* - This is a fast algorithm offering exceptional performance, especially on 32-bit-systems. One advantage of Blowfish is its variable key length (32 to 448 bits). Blowfish was first introduced in 1994 and is considered very secure.
- *Twofish* - Twofish is the entry in the AES competition by Counterpane Systems (the company of renowned cryptography expert Bruce Schneier). This algorithm uses a block size of 128 bits and can utilize key lengths from 128 to 256 bits. Twofish is extremely fast: on a Pentium-class CPU each byte is encrypted using only 18 CPU cycles. Twofish has been tested extensively without finding any weaknesses.
- *CAST 5* - CAST is a symmetric block cipher with a block length of 64 bits and a key length from 40 to 128 bits. The CAST algorithm is named after its developers and a patent application for it was filed in 1996. Because of its higher speed compared to DES, CAST is well-suited for real time applications. When used with key lengths from 80 to 128 bit, the algorithm is referred to as CAST 5.
- *Serpent* - Serpent is a symmetric key block cipher that was a finalist in the Advanced Encryption Standard (AES) contest, where it came in second to Rijndael. Serpent was designed by Ross Anderson, Eli Biham, and Lars Knudsen. Like other AES submissions, Serpent has a block size of 128 bits and supports a key size of 128, 192 or 256 bits. Serpent was widely viewed as taking a more conservative approach to security than the other AES finalists, opting for a larger security margin. The Serpent cipher has not been patented. It is completely in the public domain and can be freely used by anyone without restrictions.

DriveLock doesn't store passwords. Instead it calculates a unique value (hash) that allows it to determine whether the password you type to access an encrypted drive is correct. DriveLock can use the following hash algorithms to perform this calculation:

- *SHA-1* - This algorithm was developed by NIST (National Institute of Standards and Technology) in cooperation with the NSA (National Security Agency) as the secure signing hash function of the digital signature algorithm (DSA) for the Digital Signature Standard (DSS). Published in 1994, Secure Hash Standard (SHS) specifies a secure hash-algorithm (SHA) with a hash value of 160 bits for messages with a size of up to 264 bits. SHA is similar to the MD4 algorithm developed by Ronald L. Rivest. There are three SHA versions, SHA-0, SHA-1 and SHA-2. The SHA-2 family uses an identical algorithm with a variable digest size. that Depending on this digest size, the algorithm is called SHA-224, SHA-256, SHA-384 or SHA-512.
- *RIPEMD-160* - RIPEMD-160 was developed by Hans Dobbertin, Antoon Bosselaers and Bart Preneel and published 1996. It is an improved version of RIPEMD (based on MD4) and comparable to SHA-1 in security and speed. This algorithm is less likely to contain security holes because its development process was more open than that of SHA-1.
- *WHIRLPOOL* - Whirlpool is a cryptographic hash function designed by Vincent Rijmen (co-creator of the Advanced Encryption Standard) and Paulo S. L. M. Barreto. The hash has been recommended by the NESSIE project. It has also been adopted by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) as part of the joint ISO/IEC 10118-3 international standard.

To perform encryption operations DriveLock uses an embedded FIPS 140-2 validated cryptographic module (Certificate #1051) running on a Windows platform per FIPS 140-2 Implementation Guidance section G.5 guidelines.

14.1.2 DriveLock Encryption Modes

With DriveLock you can create two types of encrypted drives:

- Drives that are physically represented as a container file.
- Drives that map to an entire existing drive partition.

A DriveLock container file has a DLV extension. You can save a container file on any type of storage device or on a network share. To use a container, DriveLock mounts it and assigns it a pre-defined or user-selected drive letter, so you can use it like any other drive in Windows.

A DriveLock partition is a normal drive partition that has been completely encrypted by DriveLock. You can encrypt any partition, including floppy disks, ZIP drives, USB or Firewire-connected hard disks, USB flash drives and other mass storage devices.

Some types of storage media don't allow the creation of an encrypted partition. If you encounter such a drive, contact the manufacturer for more information.

Local drives cannot be encrypted using the methods described here. To encrypt a local drive, use DriveLock Disk Protection instead.

14.2 Configuring DriveLock Encryption

Before you can use DriveLock container-based encryption, an administrator must configure some general encryption parameters.

14.2.1 Configuring Encryption Using Basic Configuration Mode

When DriveLock Basic configuration mode is enabled, you can configure all basic encryption setting in the Basic configuration mode encryption task view. Click **Encryption** to open the encryption setting page.



Use the four sections to configure the following types of settings:

- General settings for encryption of removable media
- Settings that will be used when enforcing encryption of removable media
- Generation of a password recovery certificate and settings to enable password recovery for removable media.

- Settings for DriveLock Disk Protection. (These settings are described in the chapter “*DriveLock Disk Protection*” of the DriveLock Administration Guide.)

14.2.1.1 Configuring General Encryption Settings

General encryption settings control the options that are available to users when they manually encrypt a drive, burn an encrypted CD or DVD or create an encrypted container file.



Click **Configure general settings** to configure all basic settings for encrypting removable drives and media. The *General encryption settings* wizard starts.

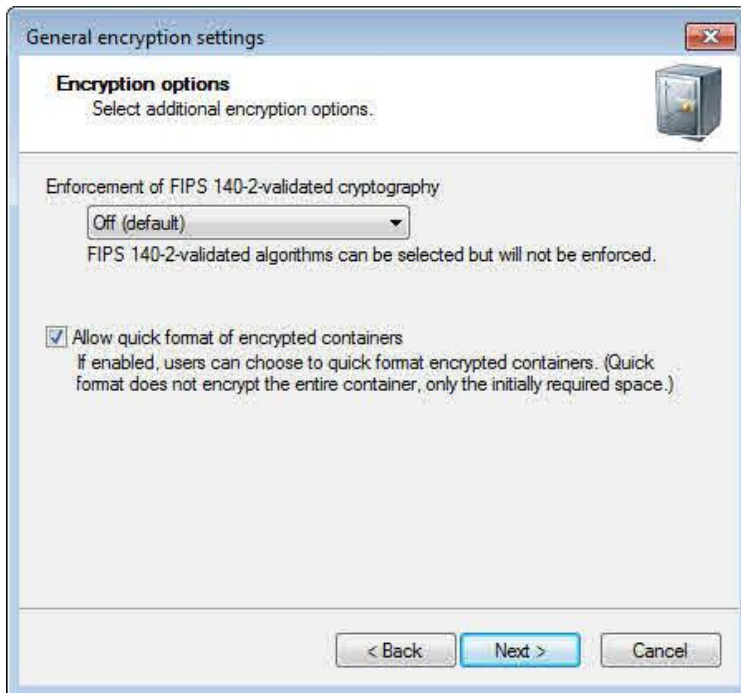


On the *Encryption algorithms* page you select the encryption algorithm, the password hash algorithm and the algorithm used to securely delete files.

Select each algorithm by using the drop down lists.

For a description of the available algorithms, refer to the section "[DriveLock Encryption Algorithms](#)".

Click **Next** to continue.



If your organization requires the use of FIPS 140-2 validated algorithms for encryption operations, you can configure the use of these algorithms on the *Encryption options* page.

By default FIPS-mode is disabled (**Off**). Users can select to use the FIPS 140-2-validated algorithms for encryption or select to use non-FIPS 140-2-validated algorithms.

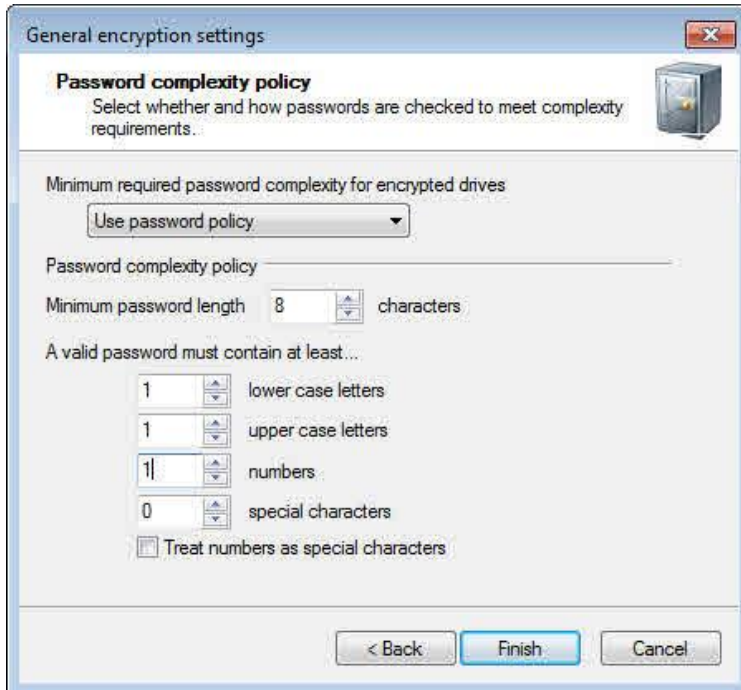
When you enable FIPS-mode, select from the following two settings:

- *On*: Use this setting if you need to access encrypted media (or container files) that were encrypted using non-FIPS algorithms. When you encrypt a new container, only FIPS validated algorithms are used.
- *On (disable non-FIPS cryptography)*: Use this setting to ensure that DriveLock only use FIPS 140-2-validated algorithms for both reading existing and creating new encrypted drives (and container files). Any container that was encrypted using a non-FIPS-validated algorithm cannot be accessed.

To speed up the process of creating an encrypted volume, select the "**Allow quick-format of encrypted containers**" checkbox. This prevents the DriveLock Agent from pre-initializing and encrypting all space in newly created encrypted volumes. Instead, only the required space is initially encrypted. Selecting this option can significantly reduce the time required for initial encryption, but some existing unencrypted data may remain accessible until it is overwritten by files that are added to the encrypted device at a later time.

Quick format results in a noticeable decrease of the encryption time only on computers running Windows 7.

Click **Next** to continue.



To ensure that users select secure passwords, on the **Password complexity page** you can define the minimum complexity required for these passwords. This complexity requirement should match your organization’s guidelines for data security. The password complexity is dynamically calculated based on the characters used in the password and the password length.

To configure a custom password complexity policy instead, select “**Use password policy**” and then complete the appropriate settings.

A password complexity policy contains all requirements an encryption password must meet when a drive (or container file) is created or when an encryption password is changed. This includes the minimum number of characters, special characters and numbers the password must contain.

If your password policy requires the use of characters that are either a number or a special character, select the “**Treat numbers as special characters**” checkbox and then select the number of special characters. When you select to treat numbers as special characters, any value specified for numbers is ignored.

Click **Finish** to complete the wizard.

To configure additional encryption settings, in the Encryption task view, click **Advanced configuration**.

14.2.1.2 Configuring Enforced Encryption

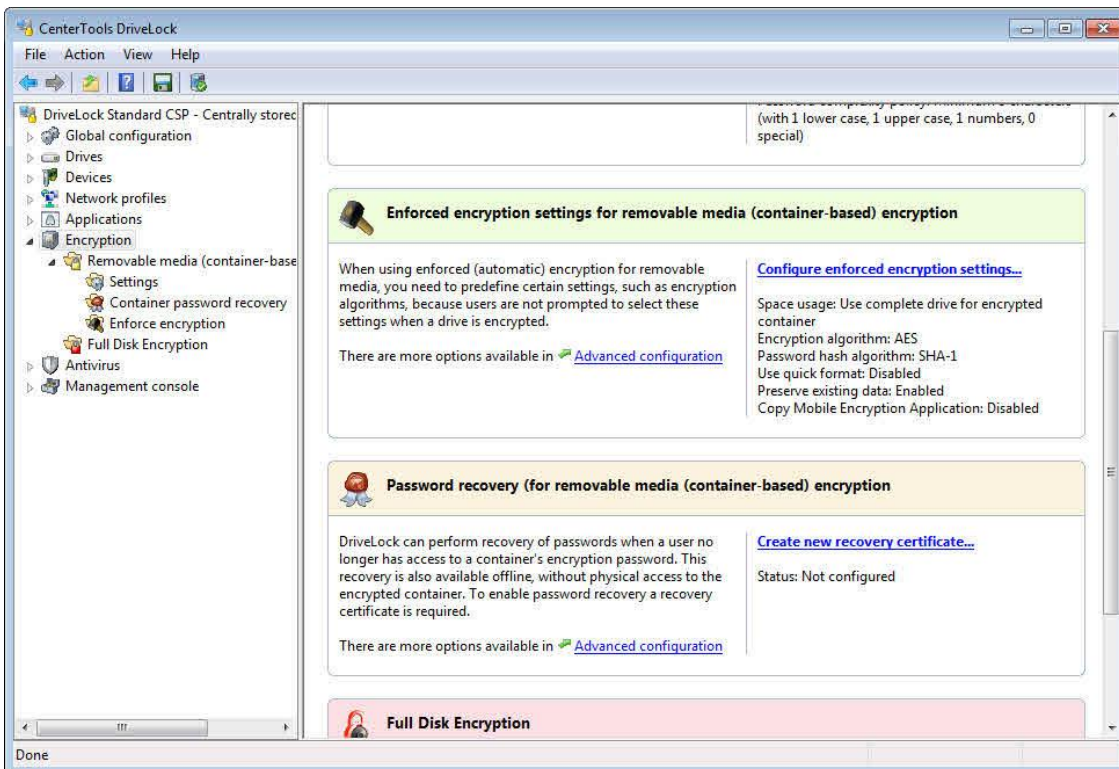
Activate enforced encryption with *DriveLock Encryption 2-Go* in the policy at:

Encryption / Settings / Enforced Encryption Method

Check **DriveLock Encryption 2-Go**.

You also may use *DriveLock File Protection* to enforce encryption (see [Configuring Enforced Encryption with File Protection](#)).

Enforced encryption settings control how removable drives and media are encrypted when your policy enforces encryption of devices.



Click **Configure enforced encryption settings** to configure all basic settings for enforced encryption.



Select the encryption algorithm and the password hash algorithm by using the drop down lists.

To speed up the process of creating an encrypted volume, select the **“Allow quick-format of encrypted containers”** checkbox. This prevents the DriveLock Agent from pre-initializing and encrypting all space in newly created encrypted volumes. Instead, only the required space is initially encrypted. Selecting this option can significantly reduce the time required for initial encryption, but some existing unencrypted data may remain accessible until it is overwritten by files that are added to the encrypted device at a later time.

Quick format results in a noticeable decrease of the encryption time only on computers running Windows 7.

Select the checkbox **Preserve existing data** to encrypt a removable drive without deleting the data that's currently stored on it. Instead, DriveLock creates a temporary container in the user's profile on the computer's hard drive, copies all existing files from the drive to this container and then moves this container to the removable drive.

Select the checkbox **Copy Mobile Encryption Application to unencrypted portion** to have DriveLock copy the Mobile Encryption Application to a removable drive that is encrypted using enforced encryption. The Mobile Encryption Application provides access to encrypted media on computers where DriveLock is not installed, such as an employee's home computer.

Select one of the following options to determine whether some unencrypted space will remain available on the disk:

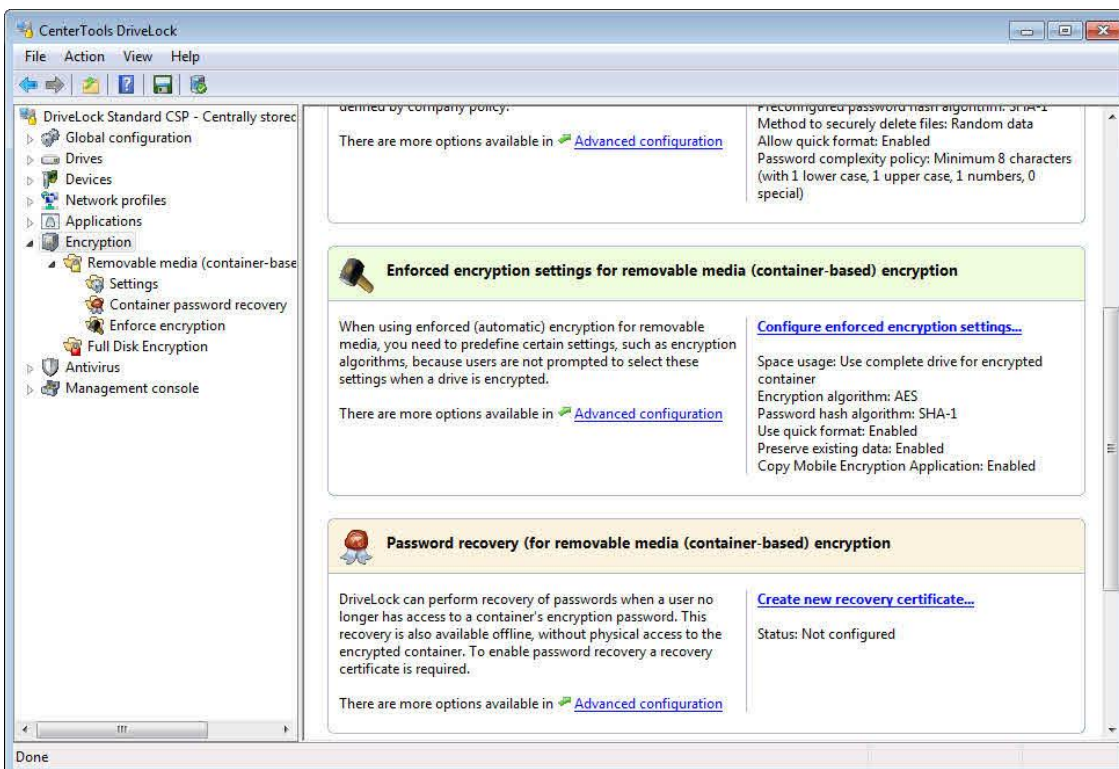
- *Use complete drive for encrypted container:* No unencrypted space remains available on the drive after encryption. By default, when enforcing encryption, DriveLock attempts to use all available disk space to create an encrypted container. However, due to file system limitations, often a small amount of disk space remains unencrypted. DriveLock fills this space by creating a hidden system file to ensure that no unencrypted data can be saved to the drive.
- *Leave unencrypted space on drives:* To allow users to save some unencrypted data on the drive when it is connected to a computer where DriveLock is not running, select this option and then specify the size of the unencrypted space in megabytes or as a percentage of the drive's size.

Click **Finish** to close the window.

To configure additional encryption settings, in the Encryption task view, click **Advanced configuration**.

14.2.1.3 Configuring Password Recovery

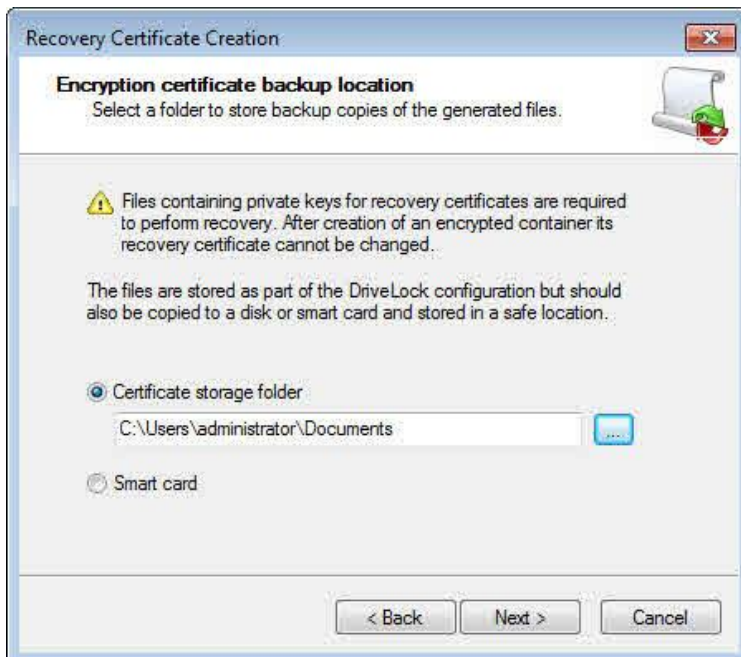
If you configure password recovery, you can enable users who forgot an encryption password to reset the password. If password recovery is configured you can also reset a password to gain access to a drive that was encrypted by a user who has left your organization.



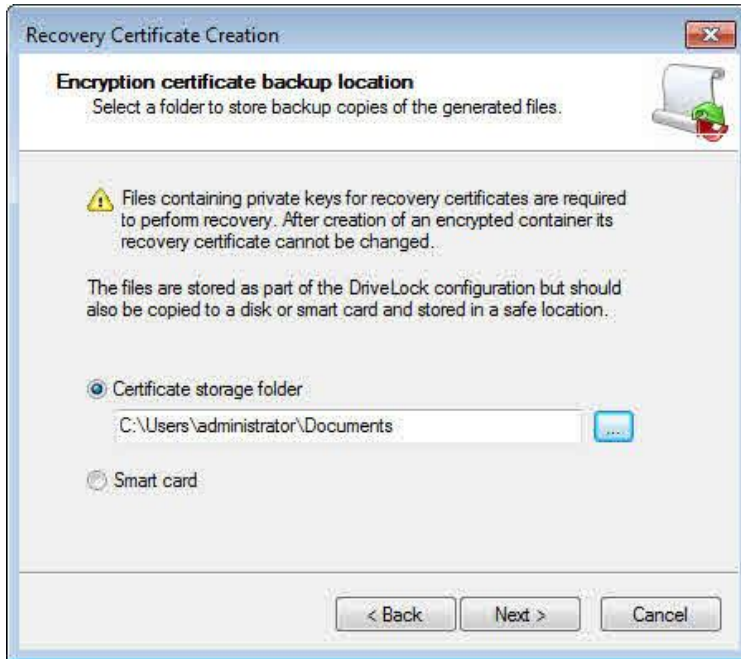
To perform offline recovery of encryption passwords you have to create a master certificate and the corresponding public/private key pair before the first encrypted container is created. Click **Create new certificate** to create a new certificate. This starts the Recovery Certificate Creation wizard.



Click Next.



Specify the folder where to save the certificate and associated private key as a file or select the option to them on a smart card.



Click Next.

If you selected to store the certificate on a smart card, further steps are required. Details depend on the smart card used.

Store the file containing the private key of the master certificate in a secure location. The private key is required to perform all password recovery operations.



Type the password that will be required to access the certificate's private key. To ensure that you typed the password correctly, you have to type it twice. To continue, click Next.

If you forget the password for accessing the private key you will no longer be able to recover passwords for encrypted containers. To prevent this from happening, store a copy of this password in a secure location, such as a safe.

DriveLock creates the certificate. The wizard notifies you when the process is complete and the certificate and associated keys have been stored in the selected location.

If you selected to store the certificate and keys on a smart card, Windows prompts you to enter the PIN for the smart card.

Click **Finish**.

When the master certificate has been created, the taskpad reflects the new state (**Configured**).

Once encrypted drives and containers have been created using a certificate, you must not create a new certificate. Doing so would replace the existing certificate, making it impossible to recover previously encrypted containers.

DriveLock also stores the certificate in the local certificate store of the user who created the certificate.

To configure additional encryption settings, in the Encryption task view, click **Advanced configuration**.

14.2.2 Configuring Encryption Using Extended Configuration Mode

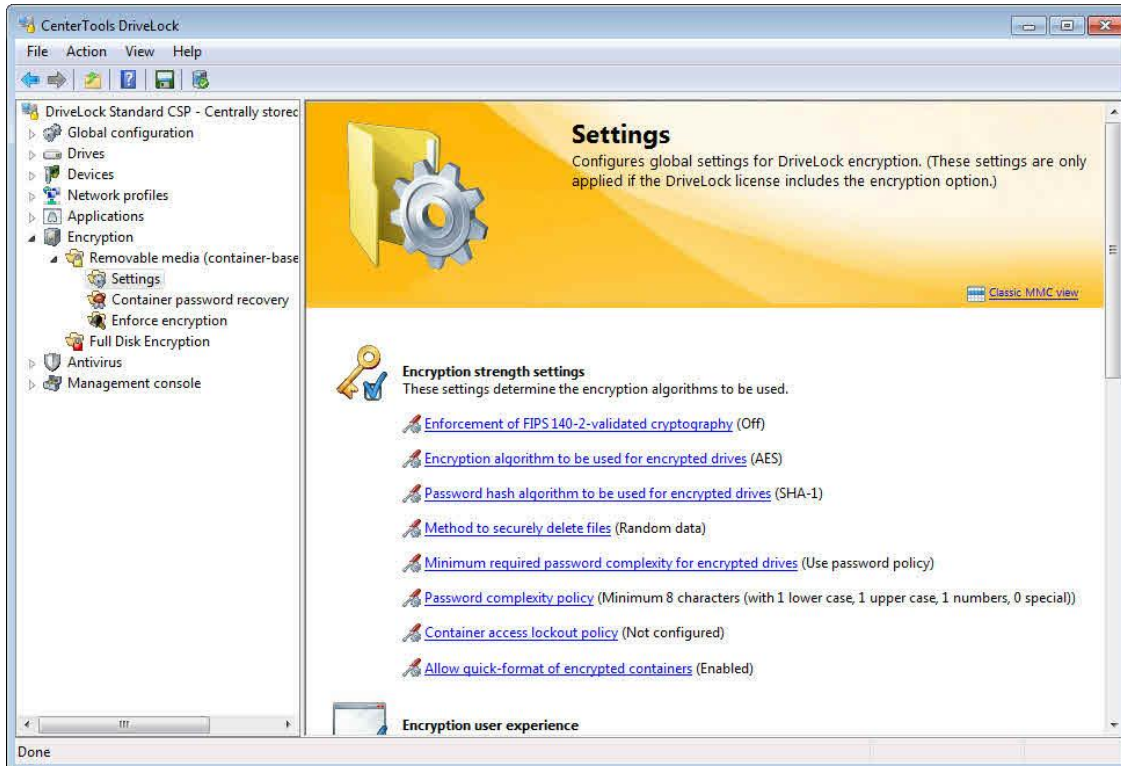
Click **Encryption** and then click **Removable media (container based) encryption** to display the encryption configuration page.



14.2.2.1 Configuring Global Parameters

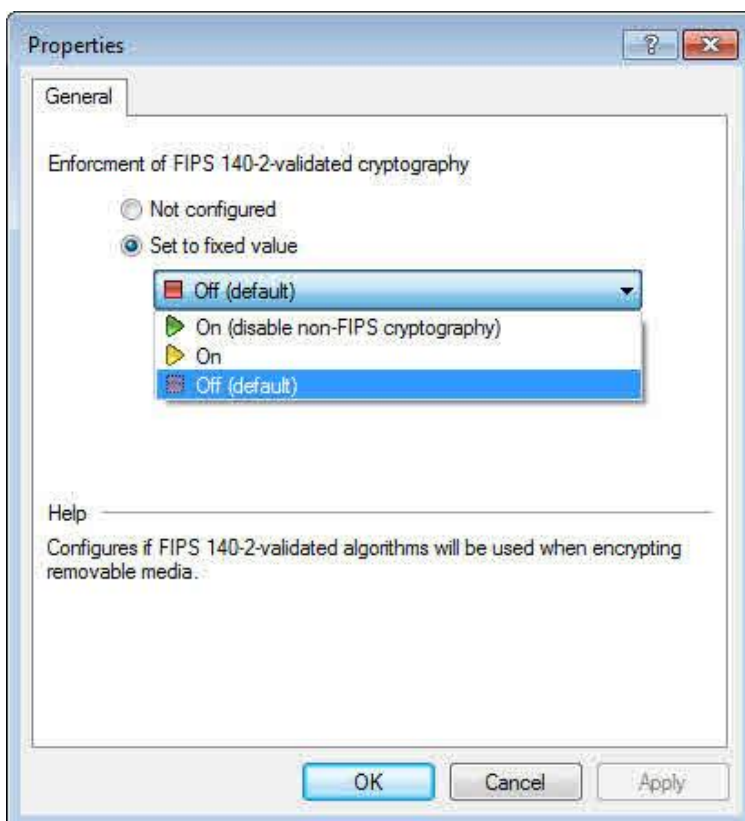
Global settings control the options that are available to users when they manually encrypt a drive, burn an encrypted CD or DVD or create an encrypted container file.

Click **Settings** to configure the global parameters for encryption.



14.2.2.1.1 Encryption Strength Settings

Enforcement of FIPS 140-2 validated cryptography



If your organization requires the use of FIPS 140-2 validated algorithms for encryption operations, you can configure the enforcement of this requirement on the *Encryption options* page.

By default FIPS-mode is disabled (**Off**). Users can select to use the FIPS 140-2-validated algorithms for encryption or select to use non-FIPS 140-2-validated algorithms.

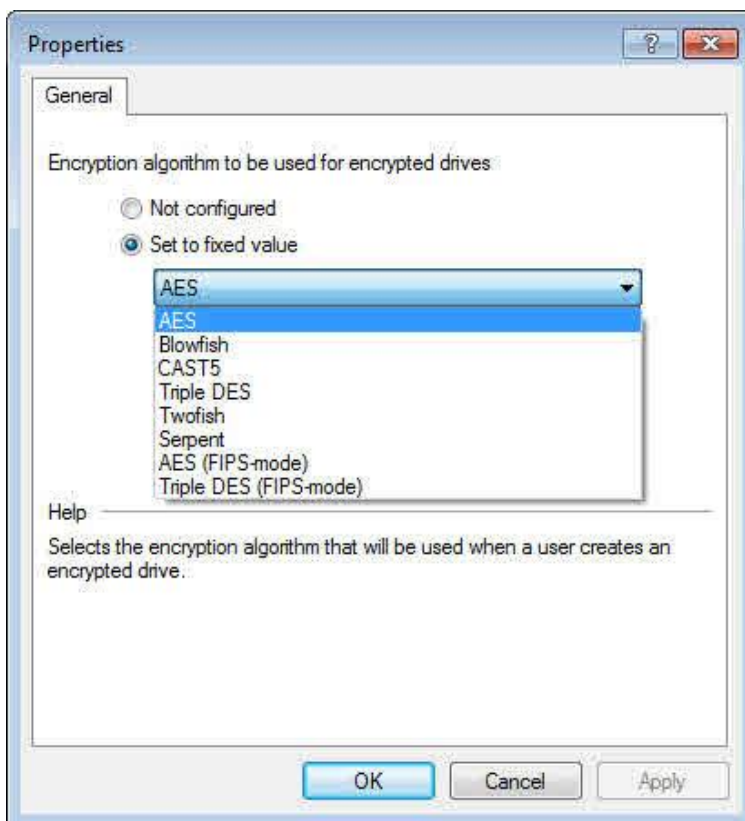
When you enable FIPS-mode, select from the following two settings:

- *On*: Use this setting if you need to access encrypted media (or container files) that were encrypted using non-FIPS algorithms. When you encrypt a new removable drive (or container file), only FIPS validated algorithms are used.
- *On (disable non-FIPS cryptography)*: Use this setting to ensure that DriveLock only use FIPS 140-2-validated algorithms for both reading existing and creating new encrypted drives (and container files). Any container that was encrypted using a non-FIPS-validated algorithm cannot be accessed.

Click **OK** when finished.

Encryption algorithms

Select the encryption algorithm to be used. The available algorithms are described in the section "[DriveLock Encryption Algorithms](#)".



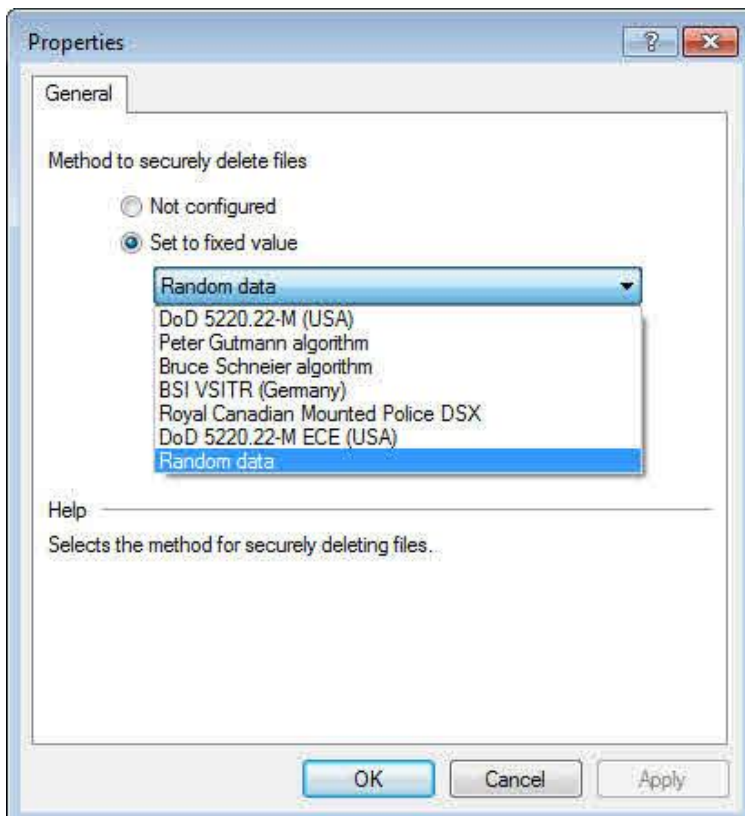
Hash algorithms

Select the hash algorithm to be used. The available algorithms are described in the section "[DriveLock Encryption Algorithms](#)".



Method to securely delete files

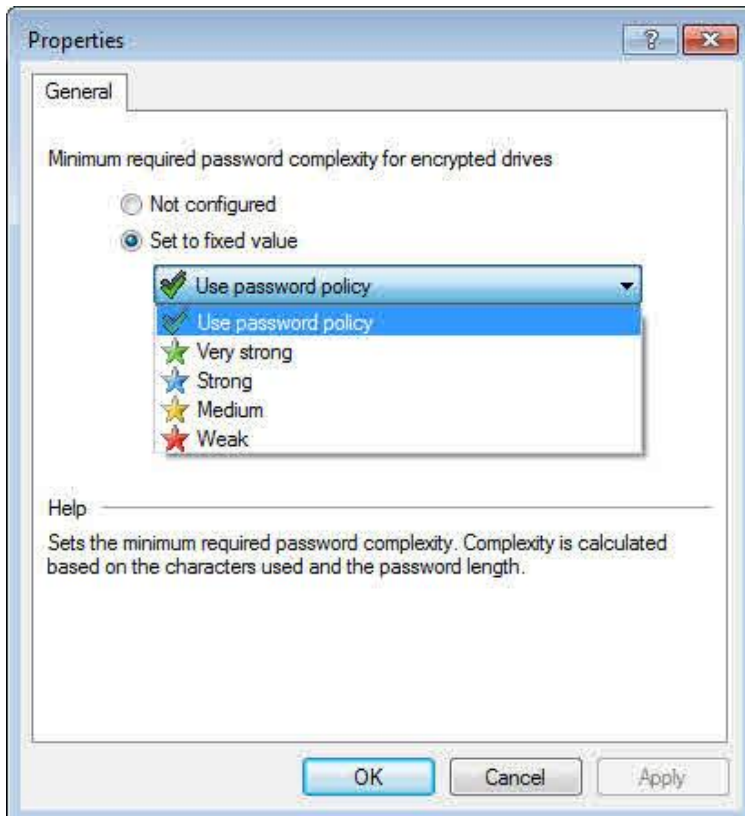
Select the algorithm to be used for securely deleting files. The available algorithms are described in the section [“DriveLock Encryption Algorithms”](#).



Minimum required password complexity for encrypted drives

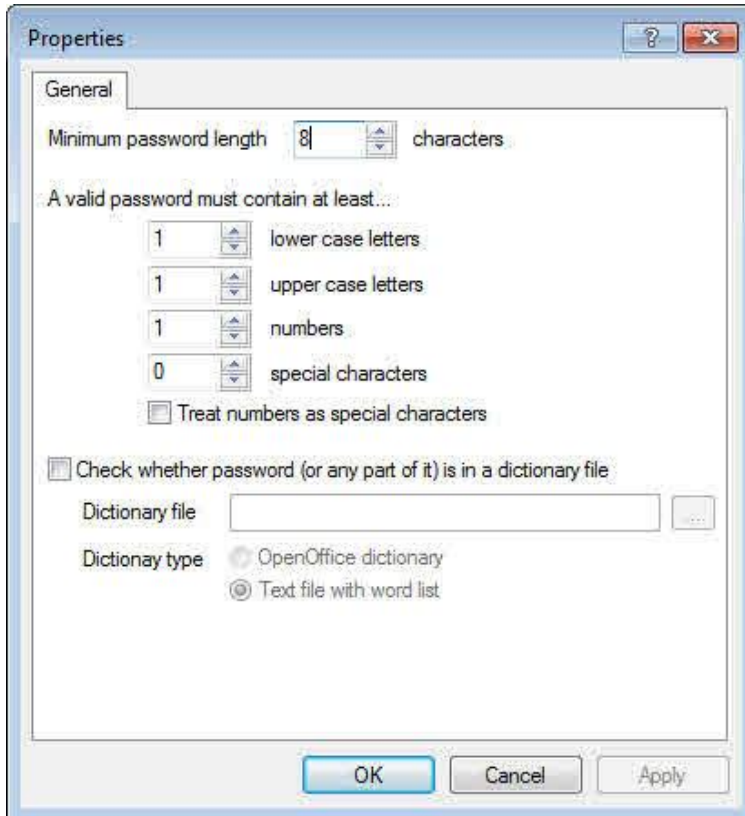
To ensure that users select secure passwords, you should define the minimum complexity that is required for these passwords. This complexity requirement should match your organization's guidelines for data security. The password complexity is dynamically calculated based on the characters used in the password and the password length.

To configure a custom password complexity policy instead, select **"Use password policy"** and then configure a custom policy (for more information, refer to the following section).



Password complexity policy

A password complexity policy contains all requirements an encryption password must meet when a drive (or container file) is created or when an encryption password is changed. This includes the minimum number of characters, special characters and numbers the password must contain. DriveLock can also prevent users from creating a password that exists in a dictionary you specify (password dictionary validation).



If your password policy requires the use of characters that are either a number or a special character, select the **“Treat numbers as special characters”** checkbox and then select the number of special characters. When you select to treat numbers as special characters, any value specified for numbers is ignored.

A dictionary can be a dictionary file in the OpenOffice format or a text file that contains a single word on each line. DriveLock includes OpenOffice dictionaries for English, German, Dutch and French. You can find these .diz-files in the DriveLock installation folder on the administration computer where you installed the DriveLock Management Console (for example **“DictEnglish.diz”**).

If you specify a custom file, ensure that this file exists on all Agent computers in exactly the same location, as the Agents looks for this file in the location you specify.

You can also place dictionary files into the policy file storage and select **“Policy file storage...”** as the dictionary location. Files located in the policy file storage are identified by an asterisk (“*”) in front of the file name and are copied to the client automatically. For more information about the policy file storage, see the corresponding chapter in the document **“DriveLock Administration Guide”**

When you use a dictionary to validate your passwords, keep in mind that passwords containing any part of a word contained in the dictionary are not allowed (for example if the dictionary contains “it”, passwords such as “hit”, “with” or “glitter” are not allowed).

Configuring Lockout Settings

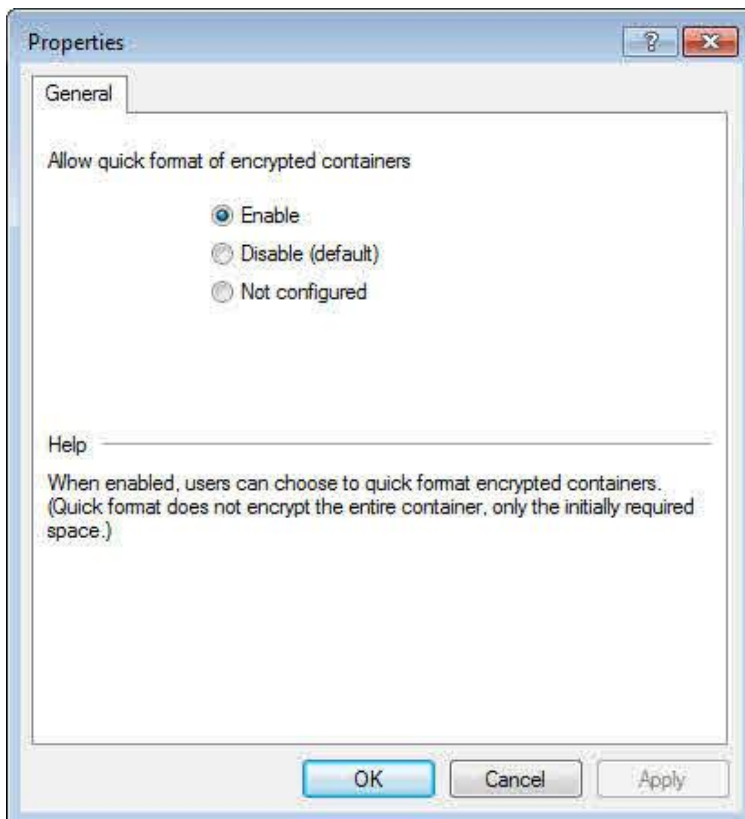
To prevent attempts to determine the password of an encrypted container by attempting to open it using a large number of character combinations (brute force attack), you can prevent a container from being opened after a configurable number of invalid attempts. The lockout can be for a period that you configure or DriveLock can lock the drive indefinitely. The following settings are available:

- *Prevent access to container (lock out) after access attempts with invalid password:* Select this checkbox to enable lockout.
 - *Number of invalid attempts:* Specify the number of invalid access attempts after which a container will be locked.
 - *Lock access for x minutes:* Specify the number of minutes for which the container will be locked.
 - *Lock access indefinitely:* Select this checkbox to lock all access to the container after the maximum number of invalid access attempts has been reached. To gain access to the container again, you need to perform a password recovery operation.

The lockout functionality requires the use of container files (.DLV) that were created or updated by a client running the DriveLock 7.0 Agent (or higher). DriveLock automatically updates the settings for a container file created by an earlier version of the Agent after it is mounted for the first time using the DriveLock 7.0 Agent (or higher).

The current version of the Mobile Encryption Application (MEA) is required to access encrypted containers for which lockout has been configured. To enable automatic updating of the MEA on existing encrypted drives, change the following setting to *Disable (default): Extended configuration -> Encryption -> Removable media encryption -> Settings -> Do not automatically upgrade Mobile Encryption Application to newer version during enforced encryption.*

Allow quick-format of encrypted containers



To speed up the process of creating an encrypted volume, select **“Enable”**. This prevents the DriveLock Agent from pre-initializing and encrypting all space in newly created encrypted volumes. Instead, only the required space is initially encrypted. Selecting this option can significantly reduce the time required for initial encryption, but some existing

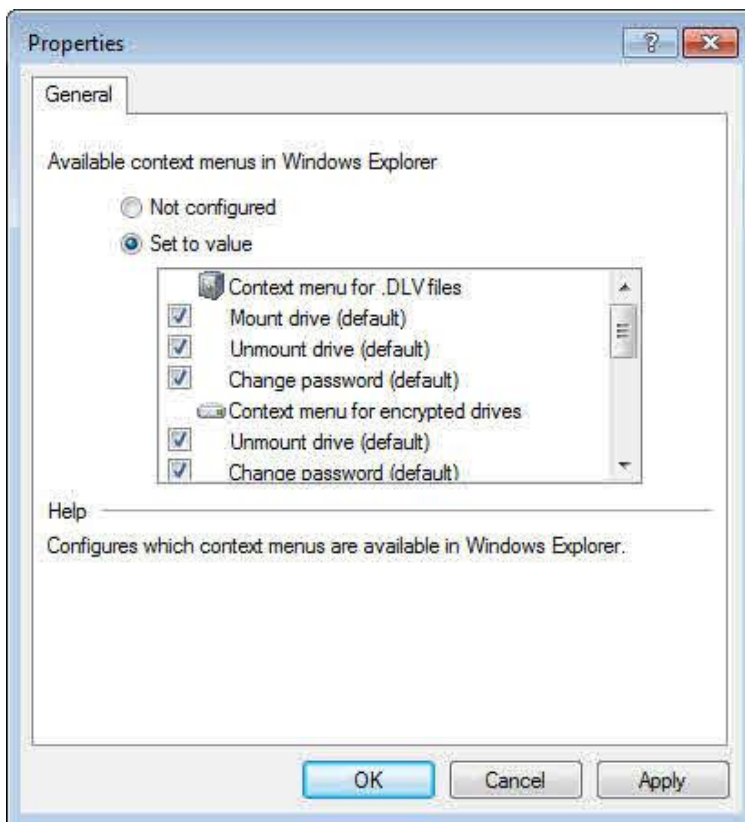
unencrypted data may remain accessible until it is overwritten by files that are added to the encrypted device at a later time.

Quick format results in a noticeable decrease of the encryption time only on computers running Windows 7.

14.2.2.1.2 Encryption End User Appearance

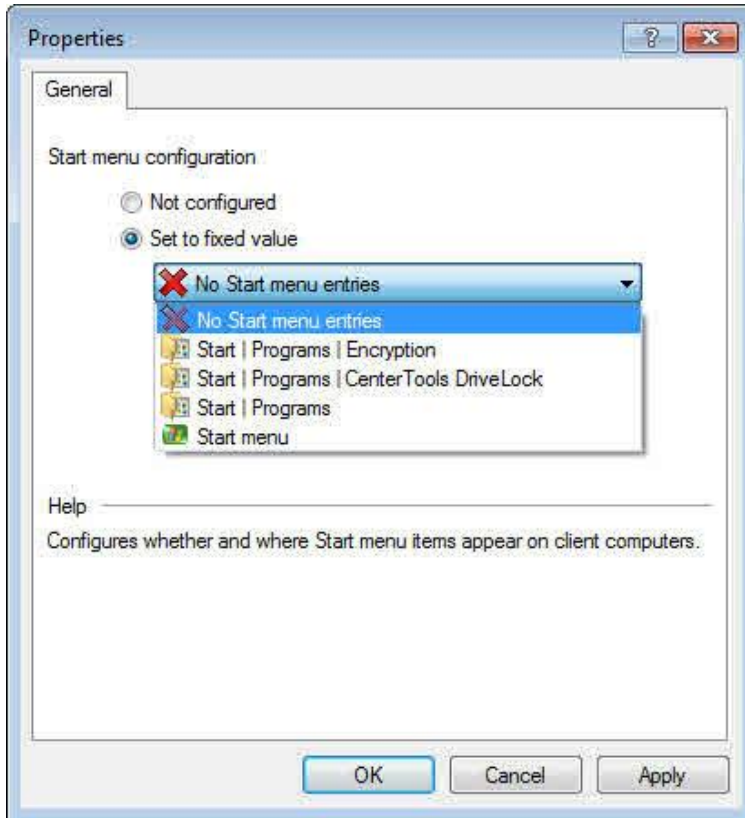
Context menus available in Windows Explorer

You can configure which commands are displayed in the context menus that appear when a user right-clicks an encrypted drive or container file in Windows Explorer. When this option is set to “Not configured”, all available commands are displayed.



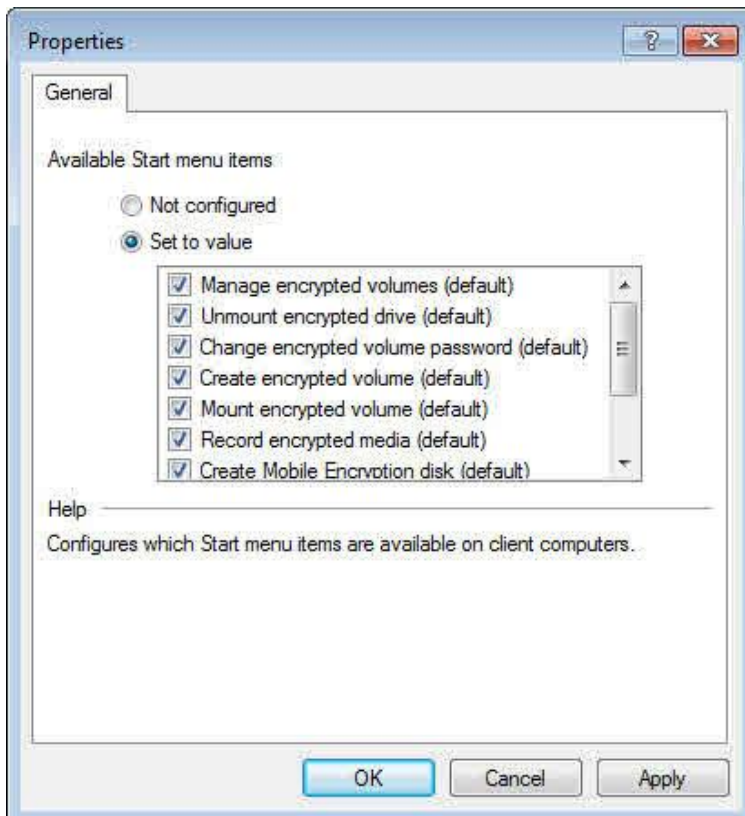
Start menu configuration

You can configure whether DriveLock commands are available from the Start menu and how they are arranged. When this option is set to “Not configured”, the commands can be accessed from the default location “Start – All Programs – DriveLock”.



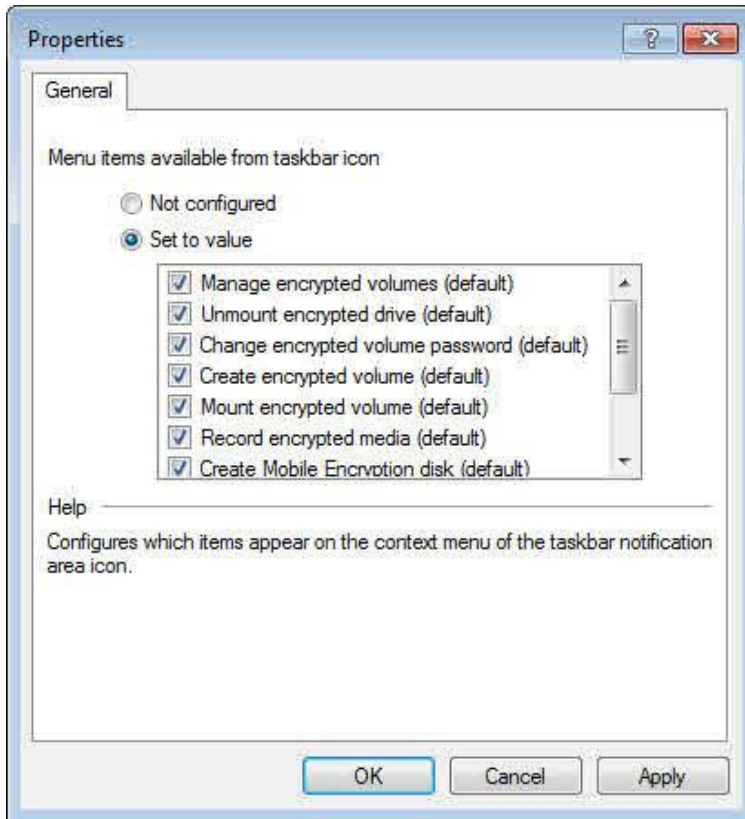
Available Start menu items

This option defines which commands are available from the Start menu. When this option is set to “Not configured”, all commands appear in the Start menu.



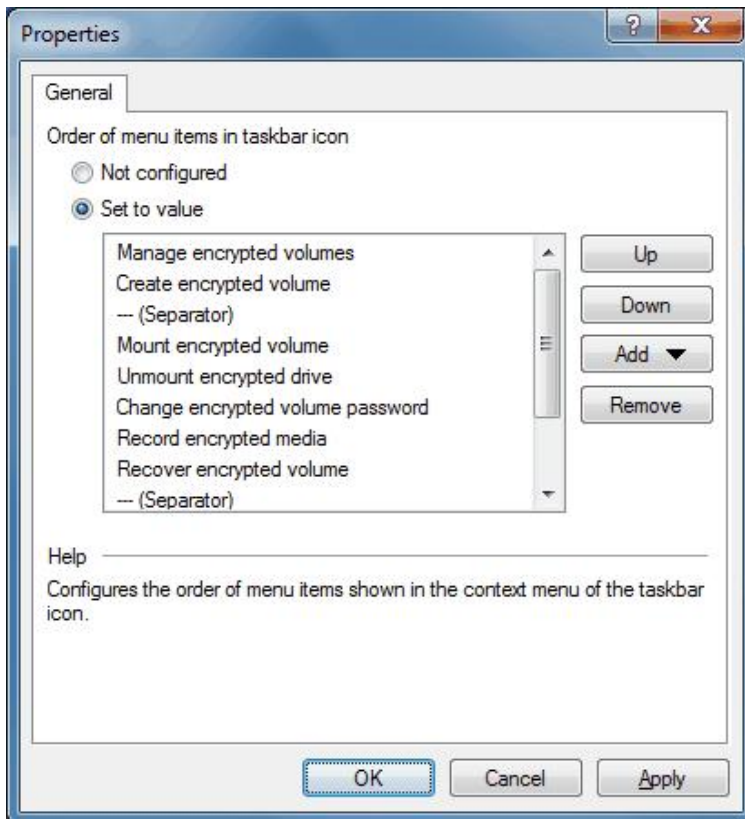
Menu items available from the taskbar icon

This option defines which commands are available when right-clicking the DriveLock taskbar icon. When this option is set to “**Not configured**”, all commands can be accessed from the taskbar icon.



Order of menu items in taskbar icon

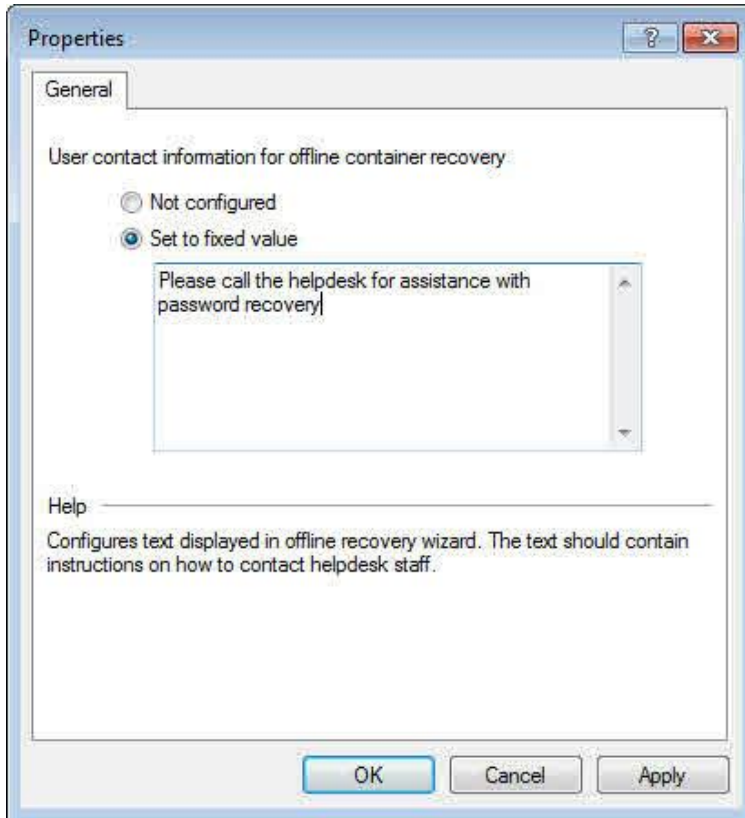
You can configure which items are displayed when you right-click the DriveLock taskbar icon and the order in which they appear.



To change the order of a menu item, select the item and then click **Up** or **Down**. To remove an element, click **Remove**. To add a divider, click **Add**. To restore the default settings, select **Not configured**.

User contact information for offline password recovery

A user who has forgotten or misplaced the password for an encrypted volume can initiate a recovery process by starting the password recovery wizard from the Start menu or the taskbar. Because the recovery process requires assistance from an administrator or helpdesk employee, the user may need contact information, such as the helpdesk telephone number. Use this menu item to add any contact information to be displayed when a user initiates a password recovery.

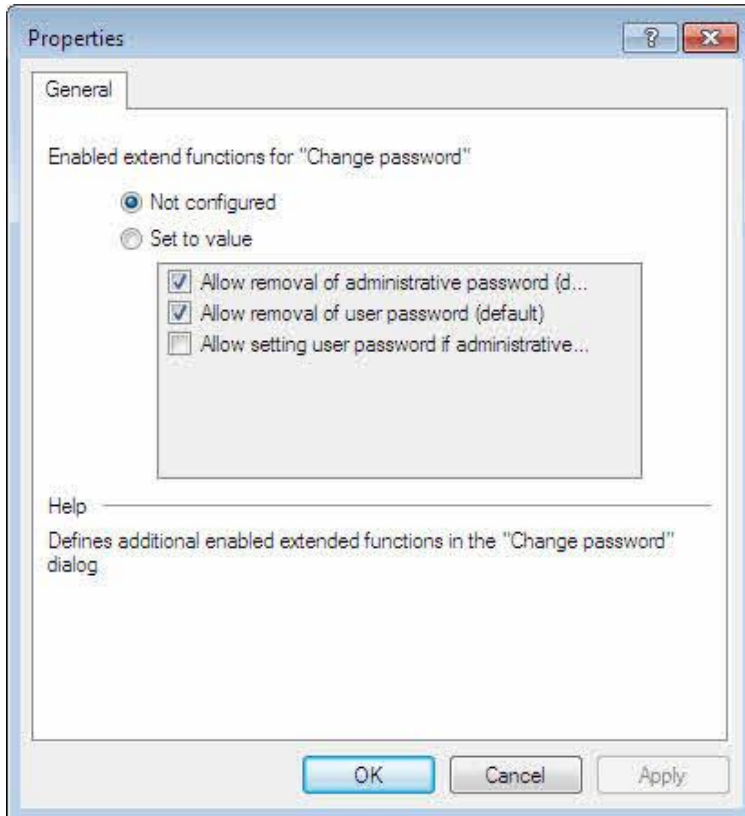


Select **Set to fixed value** and then type the text to be displayed.

Enabling extended functionality for „Change password“

When a user no longer remembers the personal password for accessing an encrypted container or drive, the user can start a wizard that allows the changing of the personal container password. You can also configure DriveLock to let the user perform any of the following additional actions:

- *Allow removal of administrative password:* When the user sets a personal password, the user can remove the administrative password. The result is an encrypted container that can only be accessed by providing the personal password.
- *Allow removal of user password:* When administrative password has been configured, the user can remove personal password. The result is an encrypted container that can only be accessed by providing the administrative password. When removing the personal password, the user has to enter the existing personal password for authorization.
- *Allow setting user password when an administrative password is defined:* When an administrative password has been set, a user can add an additional personal password without needing to know an existing password.



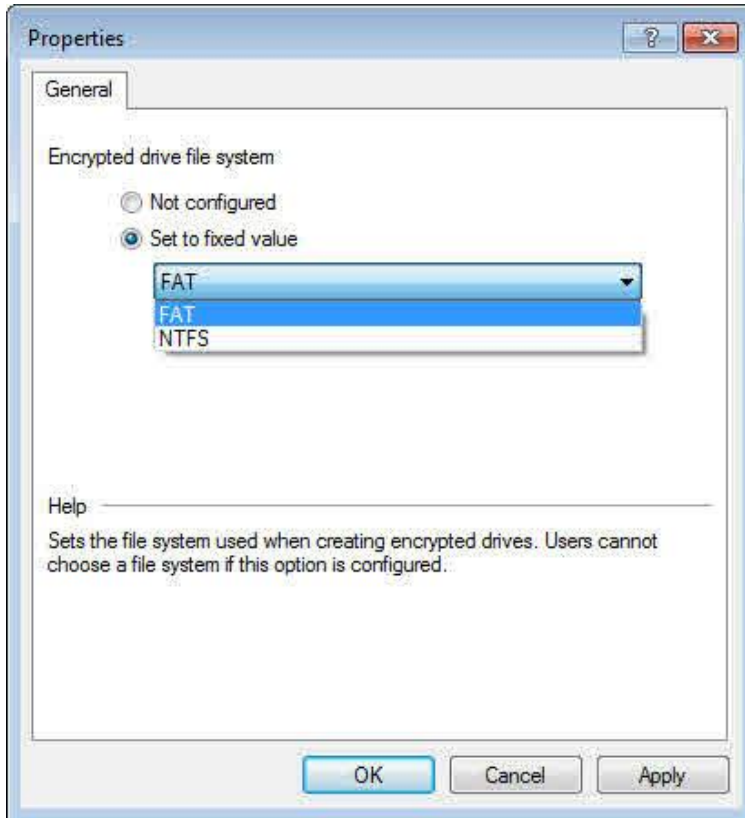
Select **Set to fixed value** and then select the checkboxes for the options you want to enable.

14.2.2.1.3 Encrypted Drive Settings

Encrypted drive file system

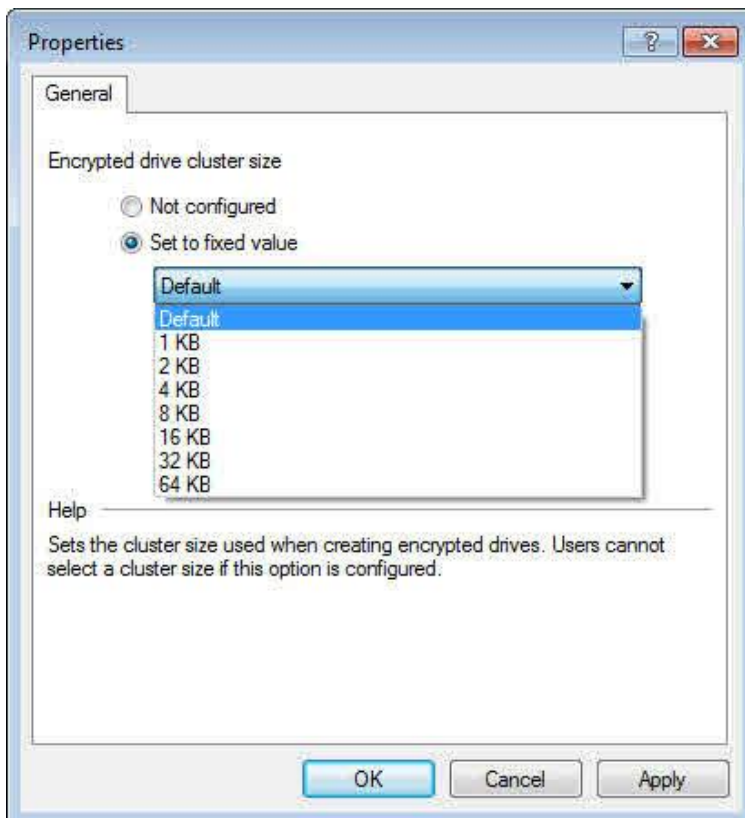
Configure this option to set the file system for new encrypted drives to **FAT** or **NTFS**.

When you select **FAT**, DriveLock automatically uses **FAT32** when the size of the drive is larger than 40 MB. For smaller drives DriveLock uses **FAT**.



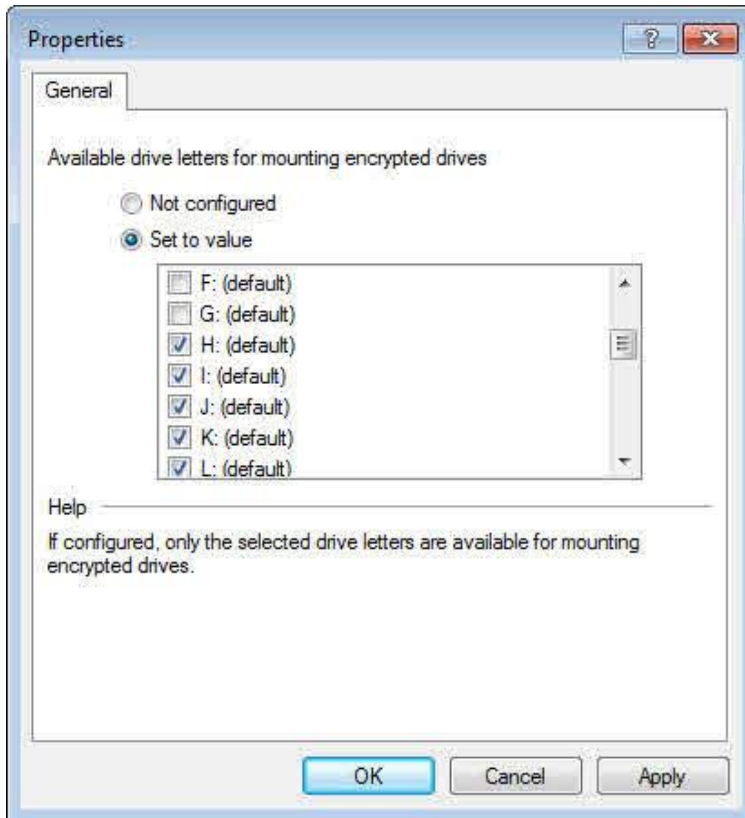
Encrypted drive cluster size

Configure this option to set the cluster size that is used for new encrypted drives.



Available drive letters for mounting encrypted drives

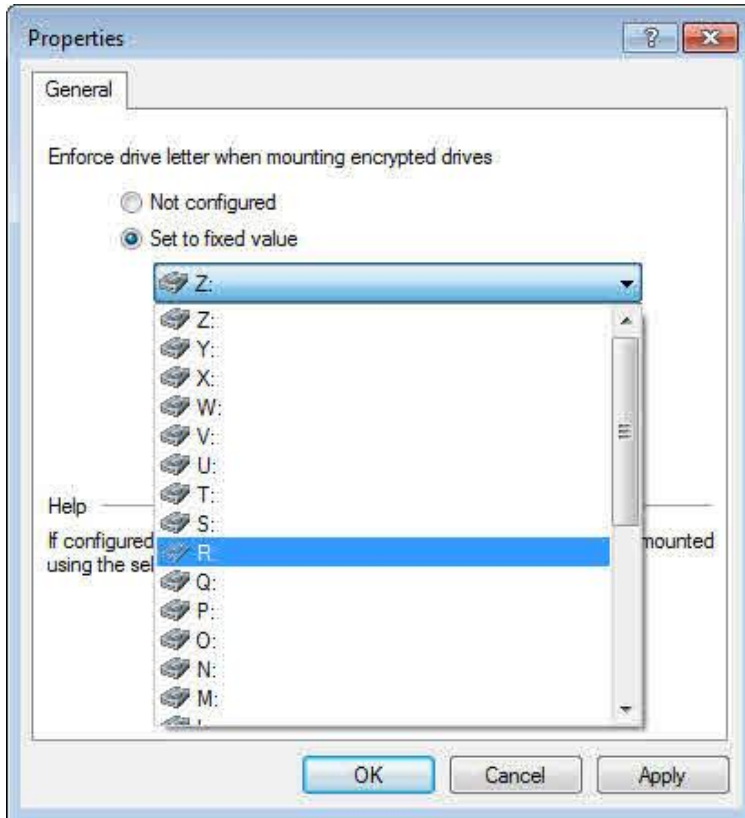
Configure this option to select the drive letters that can be assigned to encrypted volumes when they are mounted on a computer. If you don't configure this option, a user can assign any available drive letter to an encrypted volume and DriveLock offers the next available drive letter as the default choice.



This setting is especially useful to prevent problems when network drive letters conflict with those that Windows previously assigned to removable drives.

Enforce drive letter when mounting encrypted drives

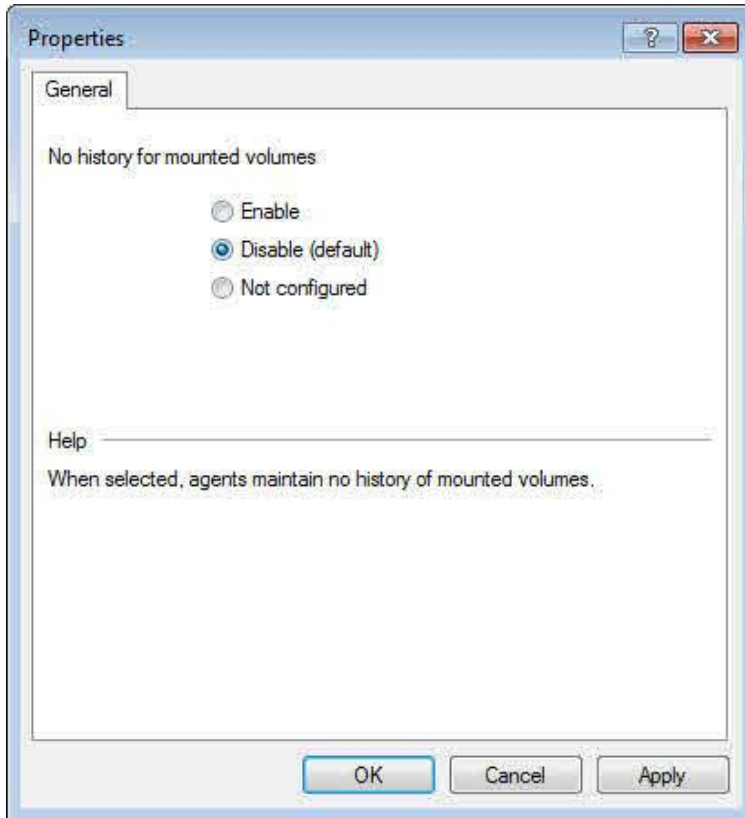
Configure this option to always assign a single drive letter to encrypted volumes when they are mounted on a computer. When you configure this option, only one encrypted drive can be connected at a time and the drive letter you selected is assigned.



14.2.2.1.4 End user restrictions

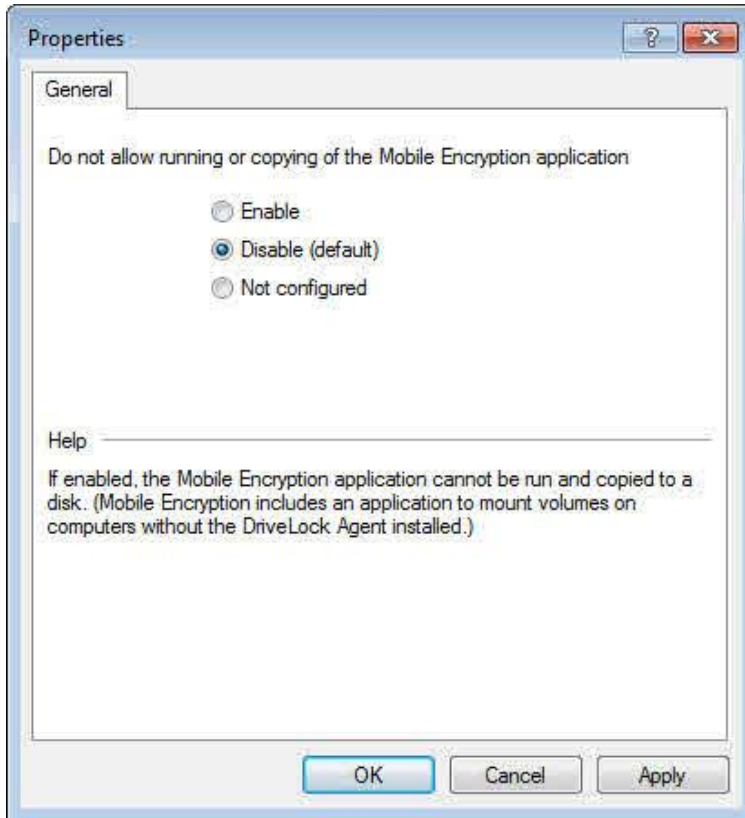
No history for mounted volumes

Configure this option to prevent client computers from storing information about which encrypted volumes users mount.



Do not allow creation of Mobile Encryption disks

The Mobile Encryption Application (MEA) is a standalone program that lets you access encrypted drives on a computer without the DriveLock Agent. When a user creates a Mobile Encryption disk by selecting the corresponding option on the DriveLock menu, DriveLock copies the MEA and an auto-start file (Autorun.inf) to the drive. Enable this option to prevent the copying of the MEA and Autorun.inf to drives.



Password recovery methods for encrypted volumes

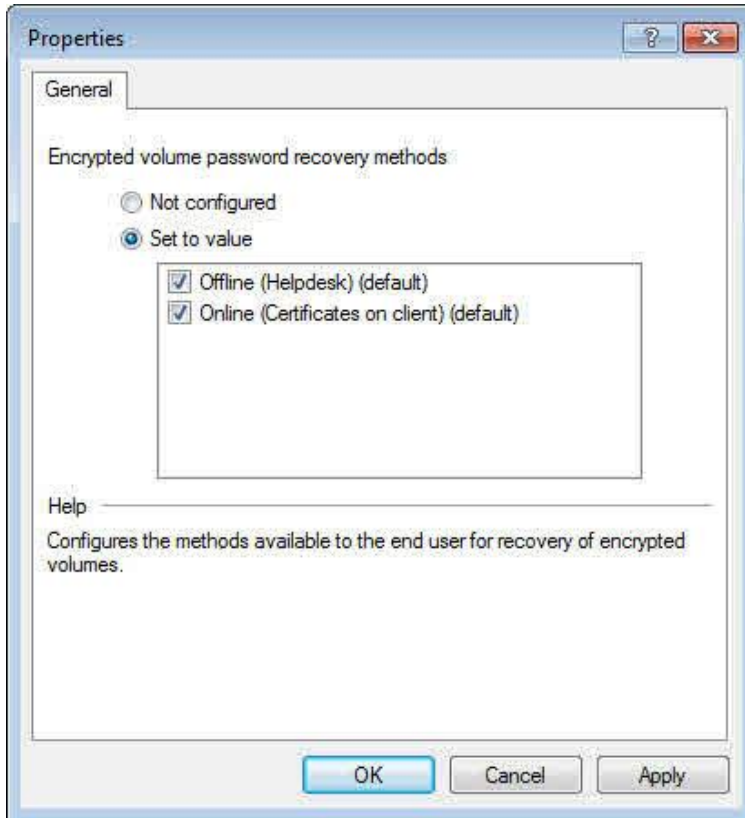
DriveLock offers two methods for gaining access to an encrypted container when the user password for the container is no longer available:

- *Offline recovery using a challenge/response mechanism:*

A user can start a wizard to reset the password using a recovery code that is provided by an administrator or helpdesk personnel. The recovery code can be provided over the telephone and a connection to the corporate network is not required.

- *Online recovery using a locally installed certificate:*

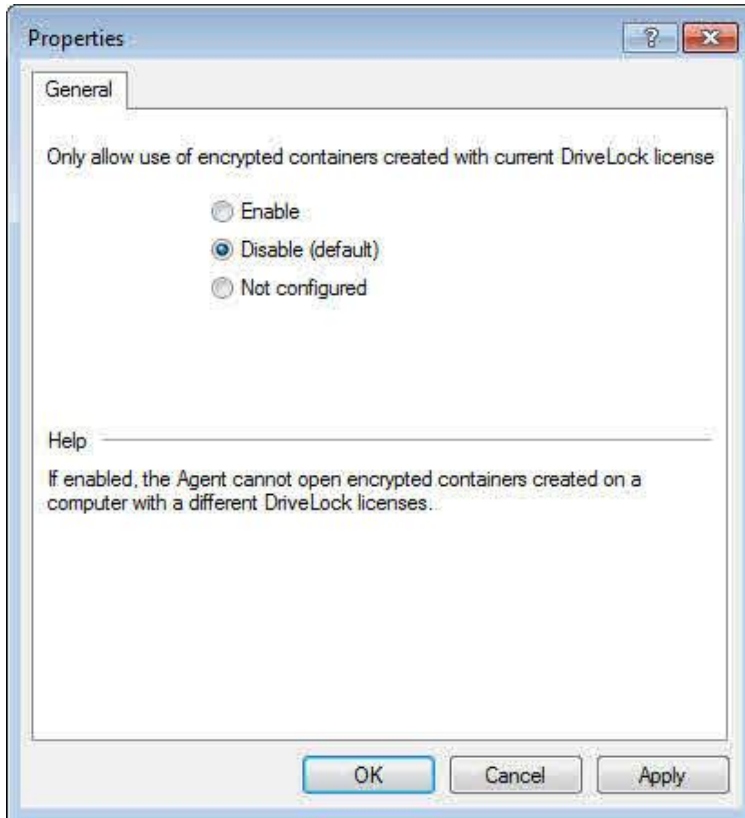
If you activate this option you can reset the password without the challenge/response procedure. To perform such a password reset, the appropriate recovery certificate and private key must be available on the computer where the recovery procedure is performed.



To configure the recovery method to be used, select **Set to value** and then select one or both checkboxes indicating recovery methods to be used.

Only allow encrypted containers created with current DriveLock licenses

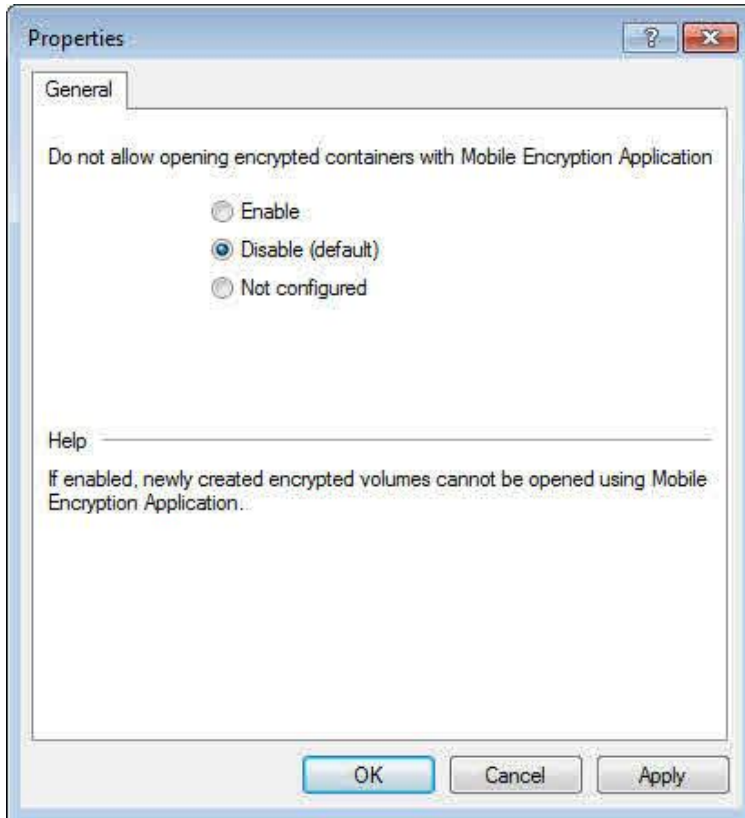
Usually an Agent can open any volume that was encrypted by using DriveLock, regardless of where the volume was created. For example, a DriveLock Agent at a company's headquarters using one DriveLock license can open an encrypted volume that was created at a subsidiary using its own DriveLock license.



Select *Enable* to only allow the use of encrypted volumes that were created by Agents using the same license as the one in the current configuration. If enabled, a volume encrypted with a different license can't be opened and decrypted.

Do not allow opening encrypted containers with Mobile Encryption Application

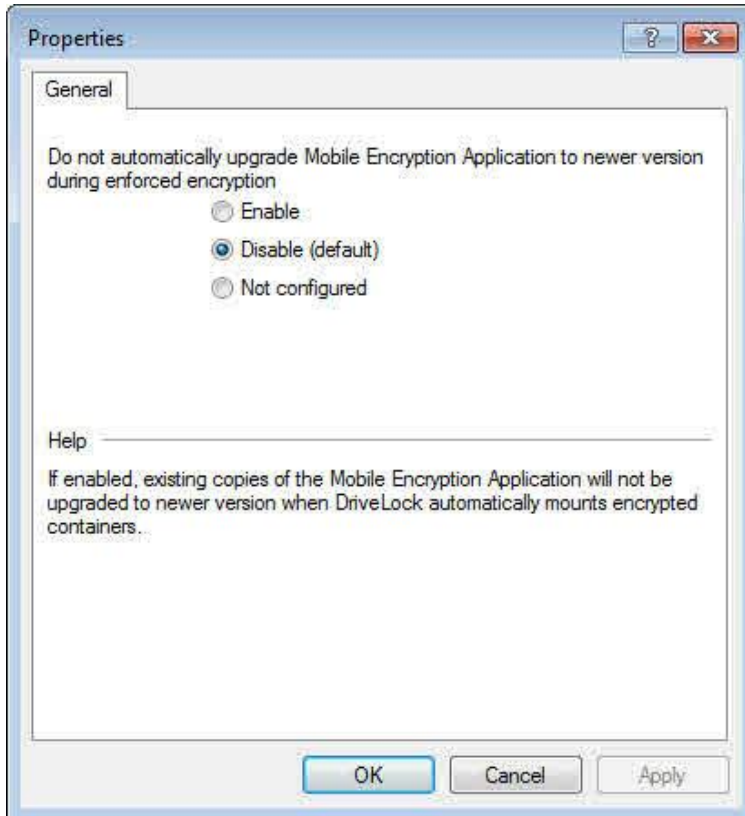
The DriveLock Mobile Encryption Application is used to access encrypted drives or container files on computers without the DriveLock Agent installed.



To prevent any access to encrypted volumes using the DriveLock Mobile Encryption Application, select **Enable**. Volumes that are created after you activate this setting can't be opened by the DriveLock Mobile Encryption Application.

Do not automatically upgrade MEA to newer version during enforced encryption

DriveLock automatically checks whether the Mobile Encryption Application (MEA) on a removable disk is up-to-date. By default DriveLock automatically updates MEA on a removable drive to most recent version.



To prevent automatic updating of the MEA, select **Enable**.

14.2.2.2 Configuring Password Recovery

You can configure DriveLock to use one or two password recovery mechanisms: an administrative password used for online recovery of encryption passwords and a recovery certificate for offline recovery. This section describes how to configure each of these mechanisms.

To be access an encrypted volume when the encryption password is no longer available, you must have configured password recovery before the encrypted volumes was created.

If you don't configure at least one of the recovery methods you will not be able to get access to the data on an encrypted volume if the encryption password for the volume is not available, for example, if a user forgets the password. Having no recovery mechanism may be a desired configuration in certain high-security environments, but using encryption without enabling password recovery significantly increases the risk of losing access to the data

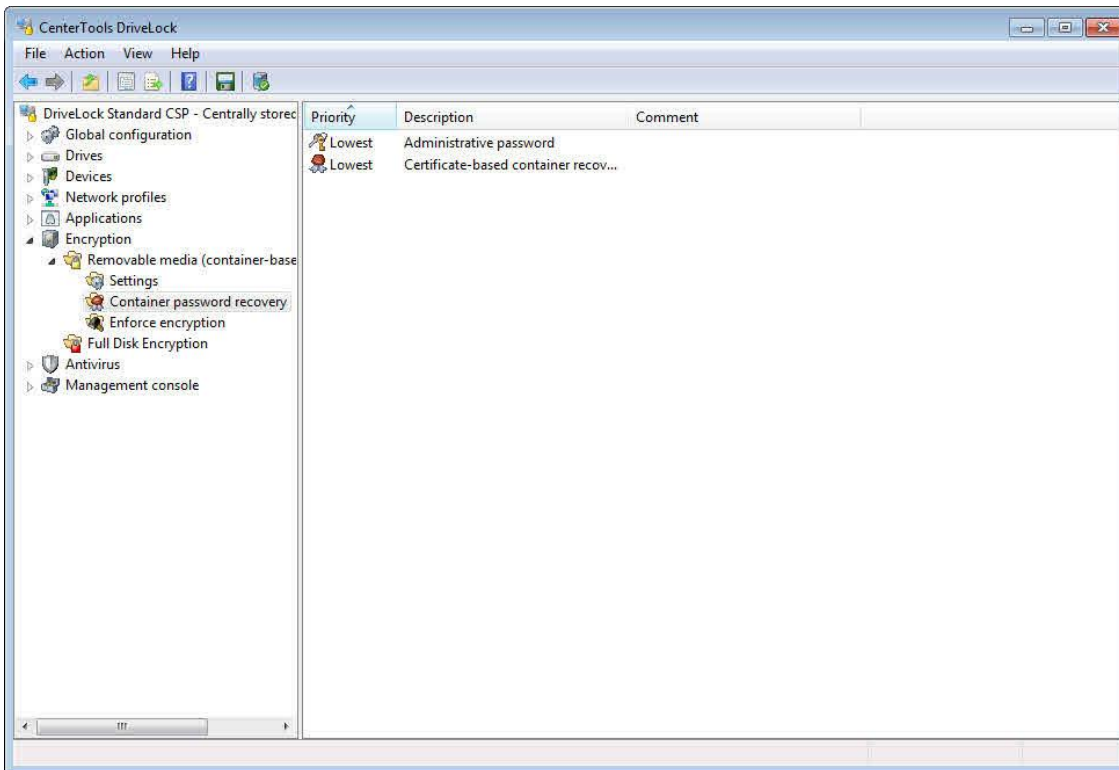
To use a challenge/response mechanism for offline password recovery, the DriveLock Enterprise Service (DES) must have been installed and configured.


When an encrypted container is created, for example when you enforce encryption of USB-connected drives, the DriveLock Agent creates the recovery data locally and then sends it to the DES. An administrator can later access the recovery data from the DES. The recovery procedures are described in detail in the section "[Recovering Passwords for Encrypted Containers](#)".

If the DES is offline, recovery information will be uploaded as soon as the server becomes available again. It may take up to 30 minutes until all recovery data has been completely synchronized.

14.2.2.2.1 Configuring an Administrative Password

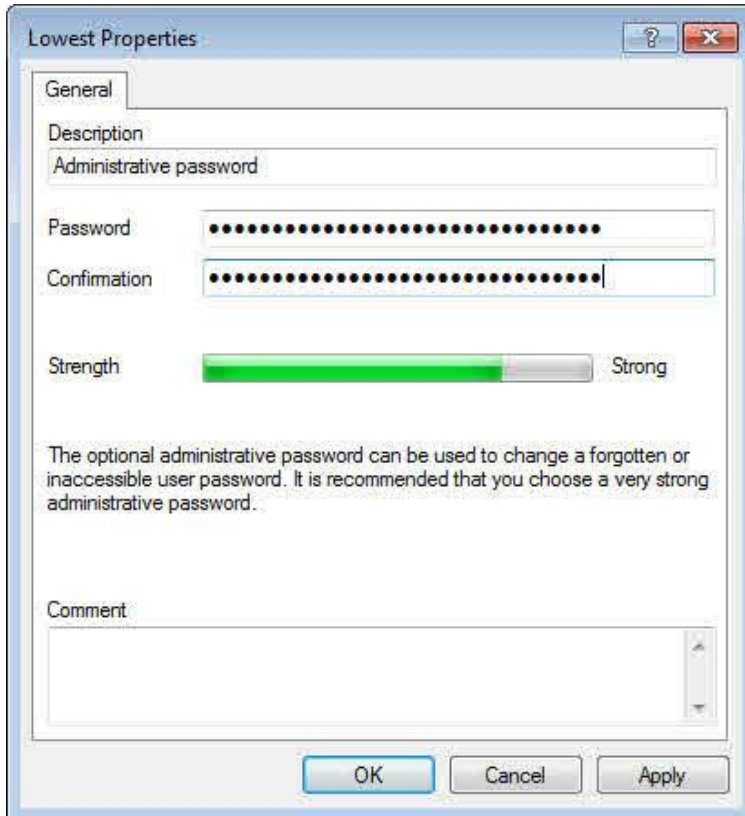
In addition to the encryption password, which is unique to each encrypted volume, you can configure a central administrative password. You use the administrative password to access an encrypted drive if a user cannot remember his or her password or if the password is not available for any other reason. You can use the administrative password to access the encrypted drive or reset the existing user password. DriveLock recommends that you use a very strong password or passphrase as the administrative password.



Navigate to Container password recovery in the console tree. **Administrative passwords** are identified by the symbol .

By default a single administrative password exists. This password is used for all encrypted containers that are configured for administrative password recovery. This password has the lowest priority and cannot be deleted.

Double-click **Administrative password** to configure the password.



Type the password, and then click **OK**.

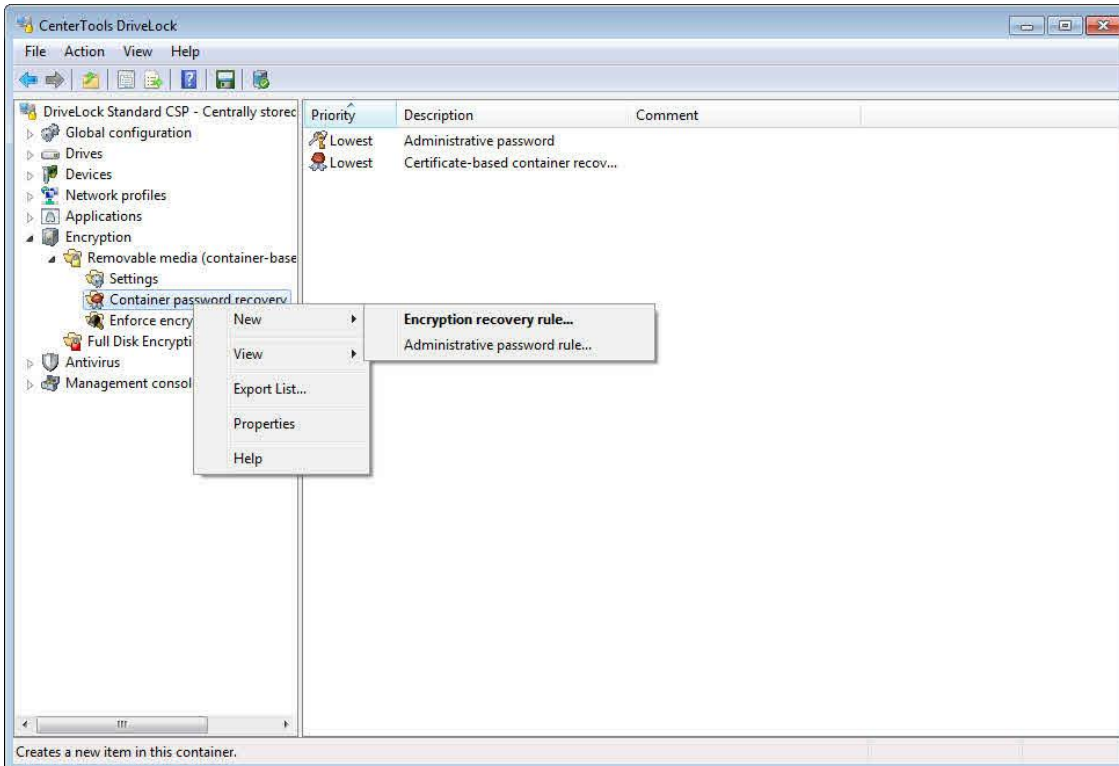
Consider using the following guidelines when choosing an administrative password:

- Use a combination of characters from the at least three of the following categories: Numbers (0 to 9), uppercase letters (A to Z), lowercase letters (a to z) and special characters (+"*ç%&/()=?è!éà£;:_.-\$``^# etc.)
- The password cannot be guessed by anyone.
- The password or parts of it don't appear in any dictionary
- The password should be as long as feasible. Passwords that are shorter than 15 characters generally don't provide sufficient long-term protection for stored data. If you find it too difficult to remember a long, complex password, consider using a passphrase instead.

For maximum security it is strongly recommended that you use a very strong password or passphrase as the administrative password. Use the strength indicator in the password dialog box to determine whether the password is strong enough to meet your requirements.

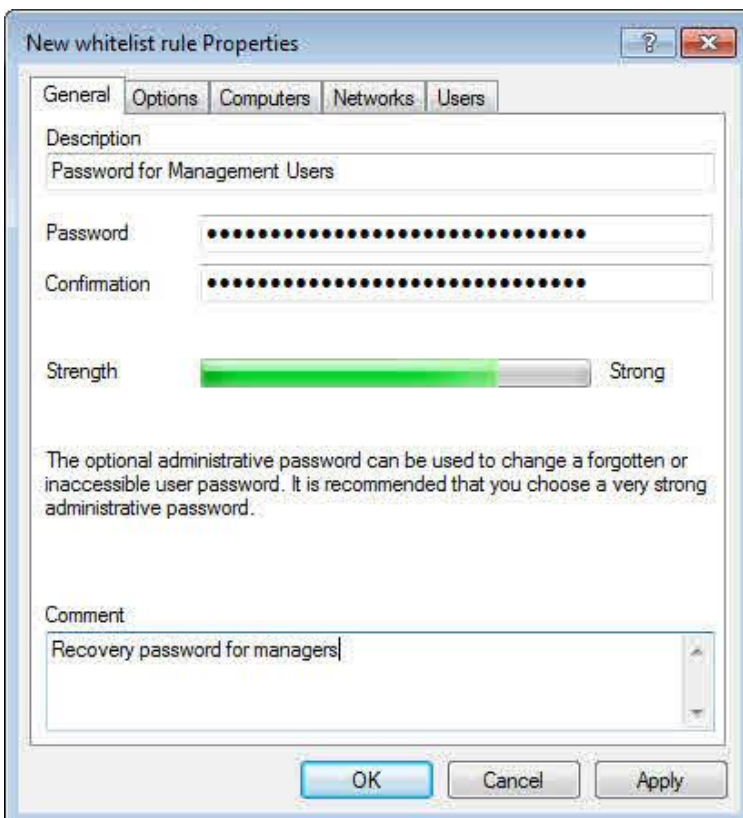
If you forget the administrative password you will no longer be able to recover passwords for encrypted containers. To prevent this from happening, store a copy of the administrative password in a secure location, such as a safe.

You can create additional administrative passwords to be used for specific users, computers or network profiles. For example, you can use a different password for encrypted containers created by management than for those created by other users. You can also utilize multiple administrative passwords to enable various scenarios for mounting encrypted drives without prompting the user for a personal password. For example, you could enable automatic mounting of managers' flash drives without prompting for the drive's password, while administrative assistants will be required to provide the drive's password.



To create an additional administrative password rule, right-click **Container password recovery**, point to **New** and then click **Administrative password rule**.

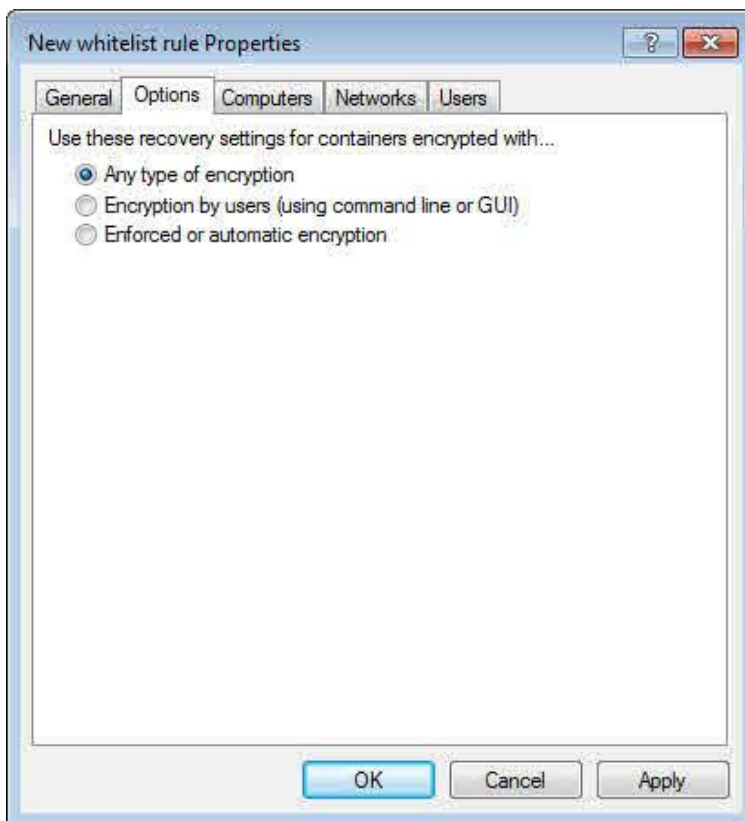
Type a strong password.



On the Options tab, select which when the rule will be used:

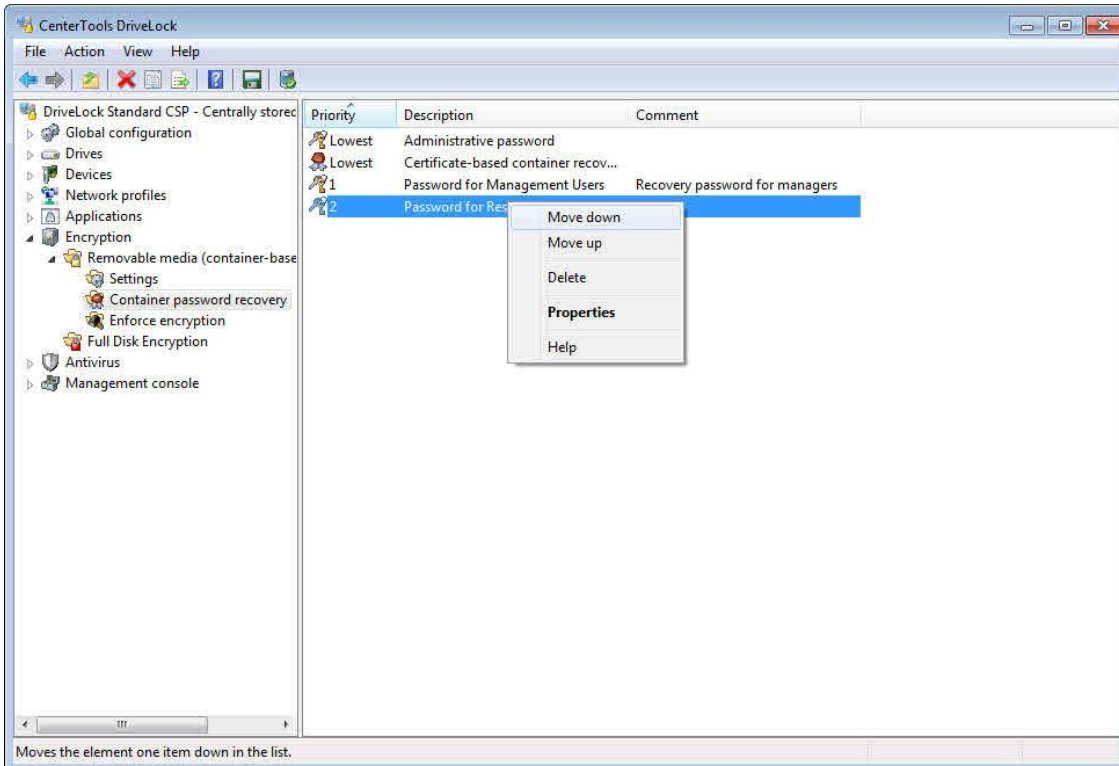
- Any type of encryption

- Encryption by users (using command line or GUI)
- Enforced or automatic encryption



On the tabs *Computers*, *Networks* and *Users*, select which of these entities the rule will be used for.

Click **OK** to save the rule. The new rule is displayed in the right pane. The first rule you create is assigned the priority of 1. The initial priority of additional rules is always one higher than the highest existing priority.



To change the priority of a rule, right-click it and then click **Move down** or **Move up**.

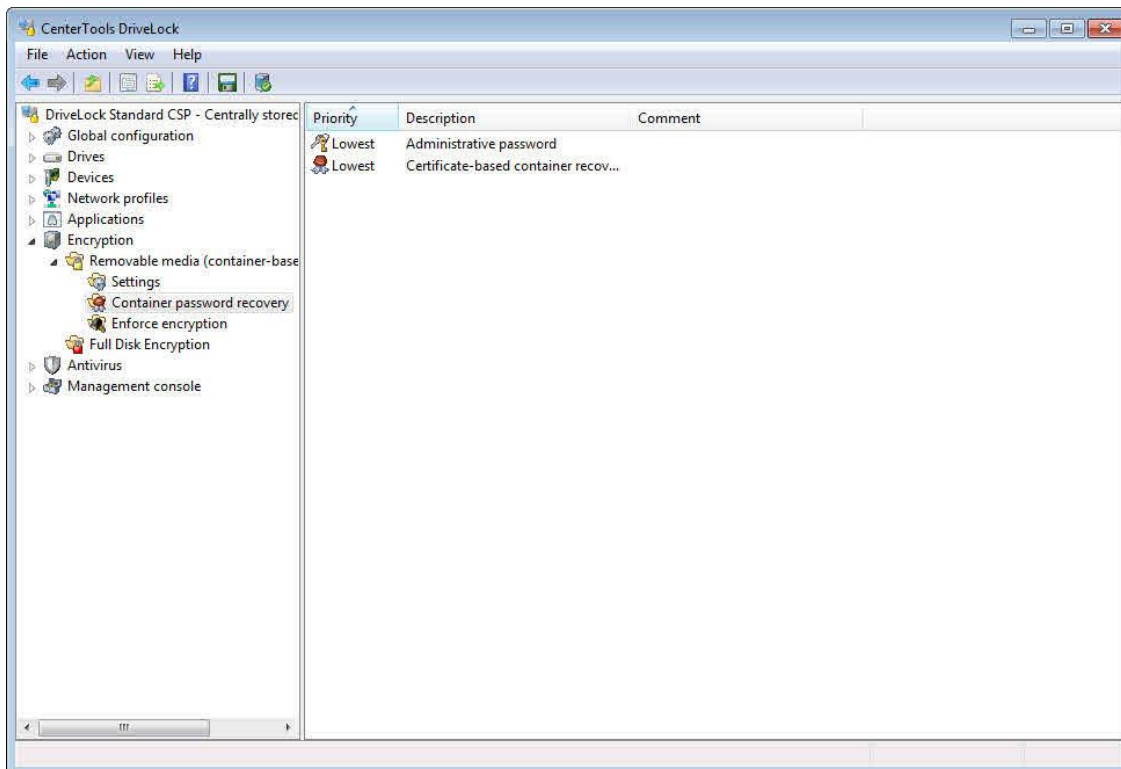
If you delete an administrative password that was used for encrypting containers, password reset or automatic mounting will no longer be possible using this password.

14.2.2.2.2 Creating an Offline Recovery Certificate


To use offline recovery you have to create a master certificate and the corresponding public/private key pair before creating the first encrypted container.

To enable advanced recovery scenarios you can create multiple recovery key pairs and use different recovery keys for certain users, computers or networks. This lets you authorize different administrators or helpdesk personnel to only recover encryption passwords for certain encrypted containers but not for others. For example, you could use one encryption certificate for encrypted containers used by management and a different certificate for containers created by all other users. You would then provide the private key for the first certificate only to enterprise administrators, enabling them to recover passwords for management. The second private key would be shared with helpdesk personnel, enabling them to recover passwords for all other users.

Before users encrypt containers, ensure that you have at least created one set of recovery key with the priority *Lowest* to enable password recovery.



When you recover the password of an encrypted container you have to provide the private key of the recovery certificate that was specified in the policy when the container was encrypted.

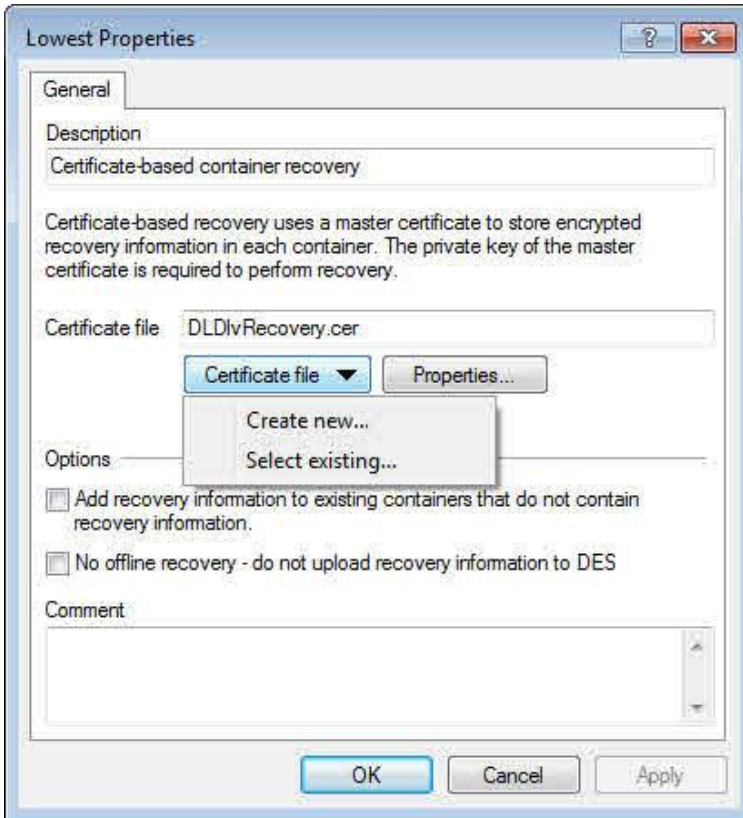
Recovery certificates are identified by the symbol .

By default a single certificate-based recovery policy exists. This policy is used for all encrypted containers that are configured for certificate-based password recovery. This certificate has the lowest priority and cannot be deleted.

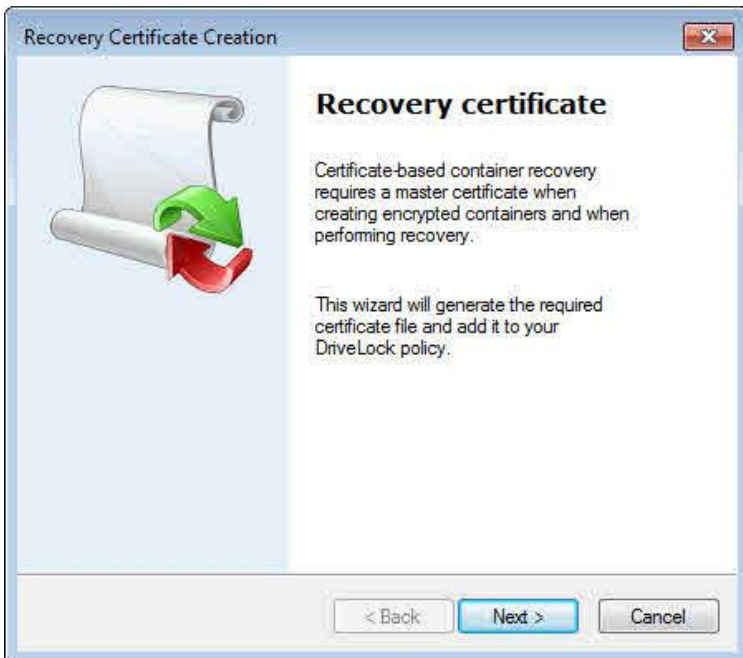
Double-click **Administrative password** to configure the password.

To create a master certificate, double-click **Certificate-based container recovery**,

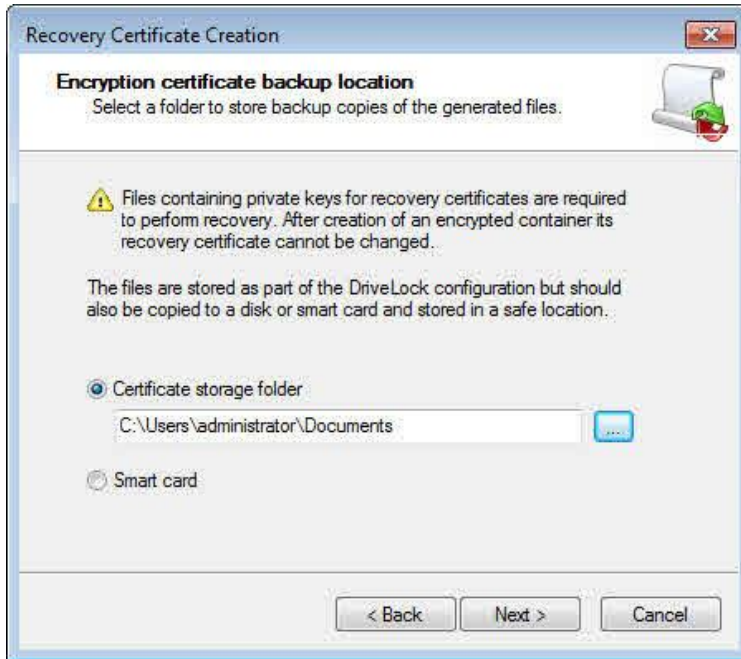
If you have not previously created a recovery certificate, no certificate information is displayed.



To create the certificate, click **Certificate file** and then click **Create new**. This starts the Recovery Certificate Creation wizard.



Click **Next**.



Specify the folder where to save the certificate file to or select the option to save the certificate and associated private key on a smart card.

Click **Next**.

If you selected to store the certificate on a smart card, further steps are required. Details depend on the smart card used.

Ensure to back up the certificate file in a secure location, such as a safe. The certificate and private key are required to recover access to encrypted volumes when a user password is no longer available.



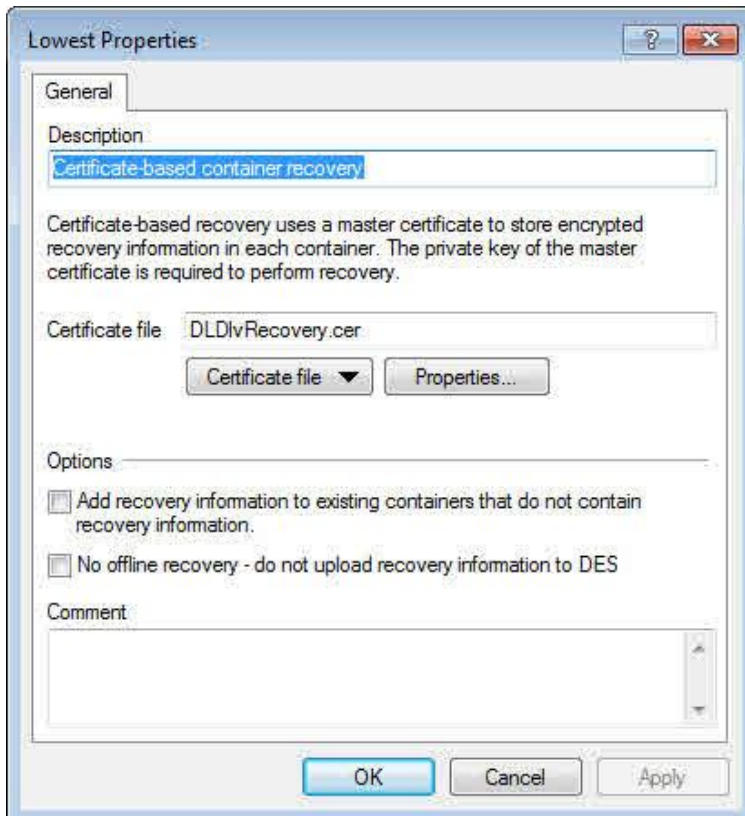
Type the password that will be required to access the private key that is stored with the certificate. To ensure that you typed the password correctly, you have to type it twice. To continue, click **Next**.

If you forget the password for accessing the private key you will no longer be able to recover passwords for encrypted containers. To prevent this from happening, store a copy of this password in a secure location, such as a safe.

DriveLock creates the certificate. When the process is complete and the certificate and associated keys have been stored in the selected location, the wizard notifies you that this has happened.

If you selected to store the certificate and keys on a smart card, Windows prompts you to enter the PIN for the smart card.

Click **Finish**.



DriveLock displays the file name of the certificate you created.

Once you have created the certificate and the first encrypted container using this certificate was created, you must not create a new certificate. Doing so would replace the existing certificate and you would not be able to recover previously encrypted containers.

To view the details of the certificate, click **Properties**.

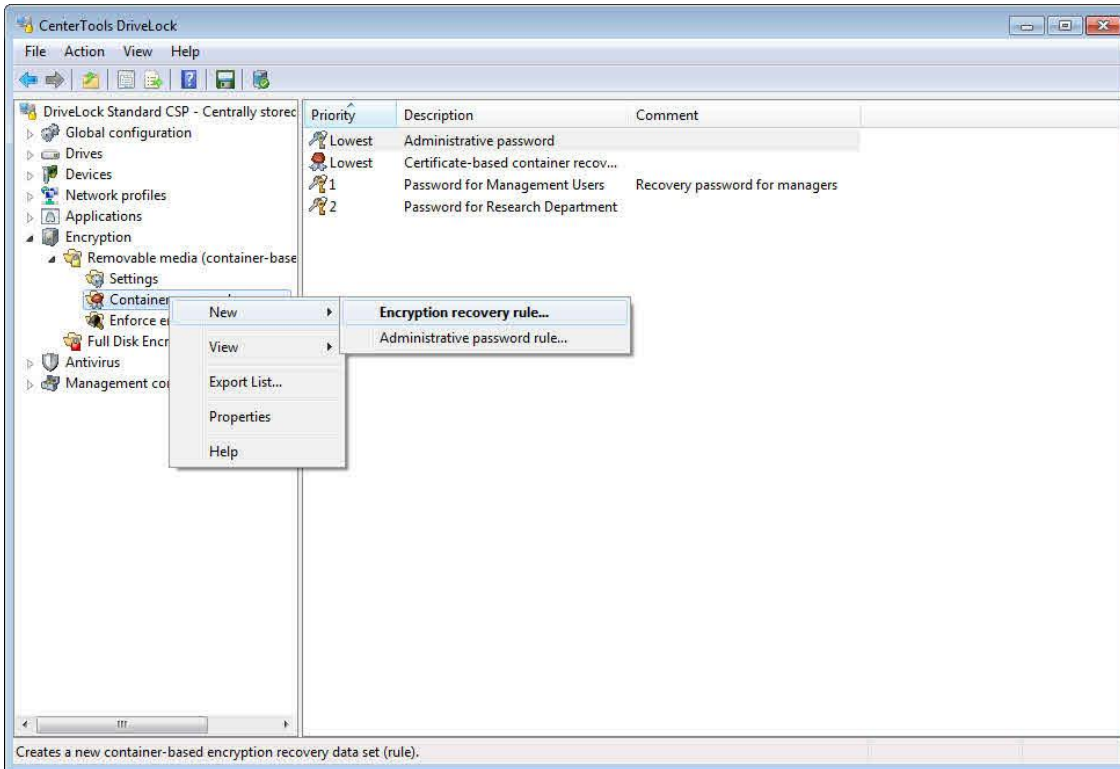
DriveLock also stores the certificate in local certificate store of the user who created the certificate.

The certificate's public key is also stored in the file storage of the local DriveLock policy.

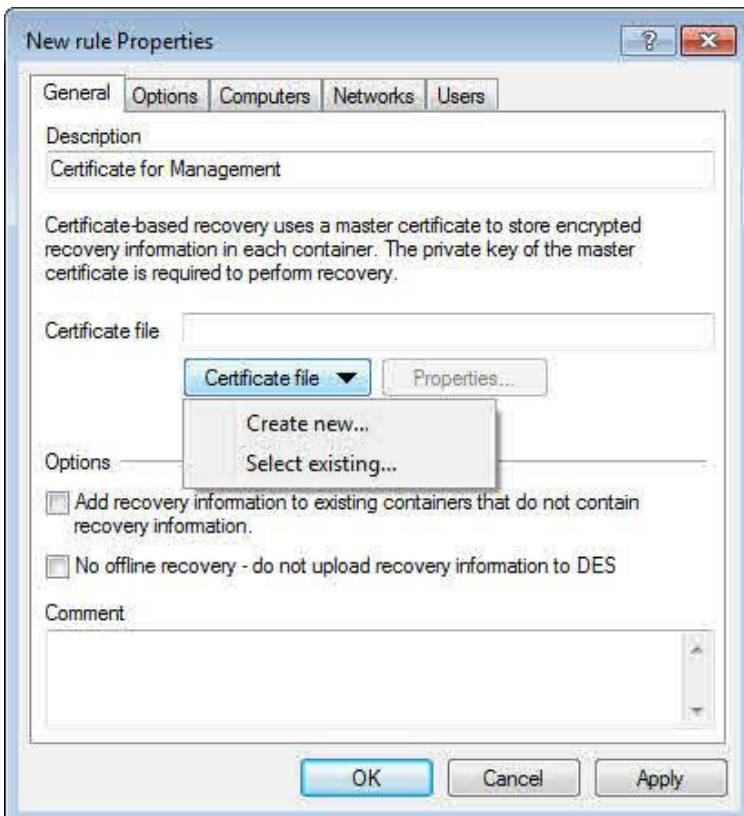
If you stop the wizard before the certificate has been created or if an error occurred while running the wizard, DriveLock displays an error message and you need to run the wizard again to create the certificate.

If you created encrypted containers using a previous version of DriveLock, you can add certificate-based recovery data to these containers. To do this, select the **Add recovery information to existing containers that do not contain recovery information** checkbox. If this checkbox is selected, each time a container is mounted, DriveLock checks whether the container already contains recovery data. If no recovery data exists, DriveLock creates this data, adds it to the container and sends it to the DriveLock Enterprise Service.

If you are not using the DriveLock Enterprise Service or if you don't want to store recovery data in the DriveLock database, select the **No offline recovery** checkbox. If you disable offline recovery, you must have physical access to a container to recover the data stored in it.



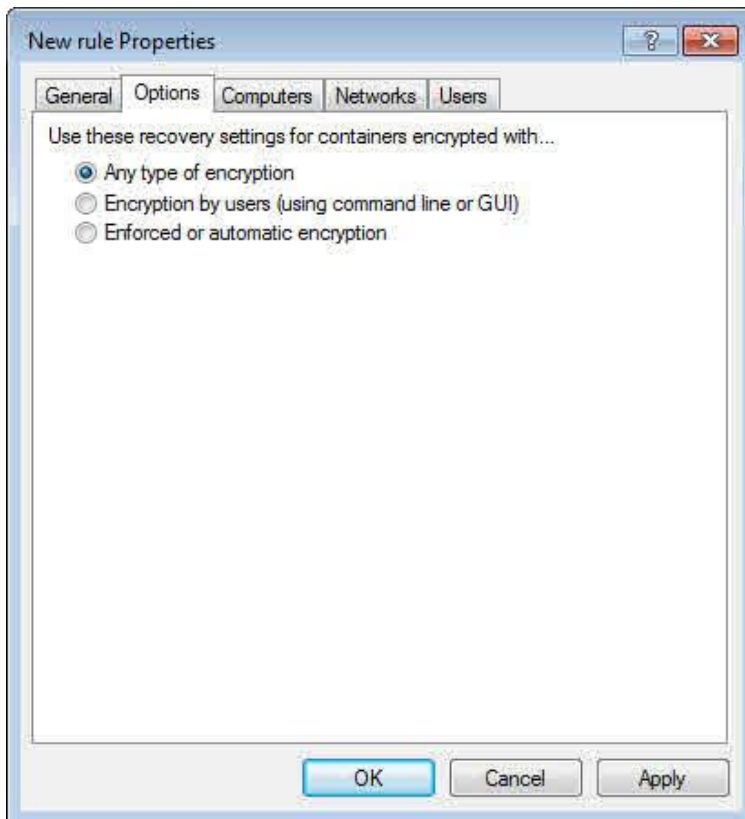
To create an additional recovery rule, right-click **Container password recovery**, point to **New** and then click **Encryption recovery rule**.



Because you have not yet created a recovery certificate, no certificate information is displayed. Create a new certificate.

On the Options tab, select which when the rule will be used:

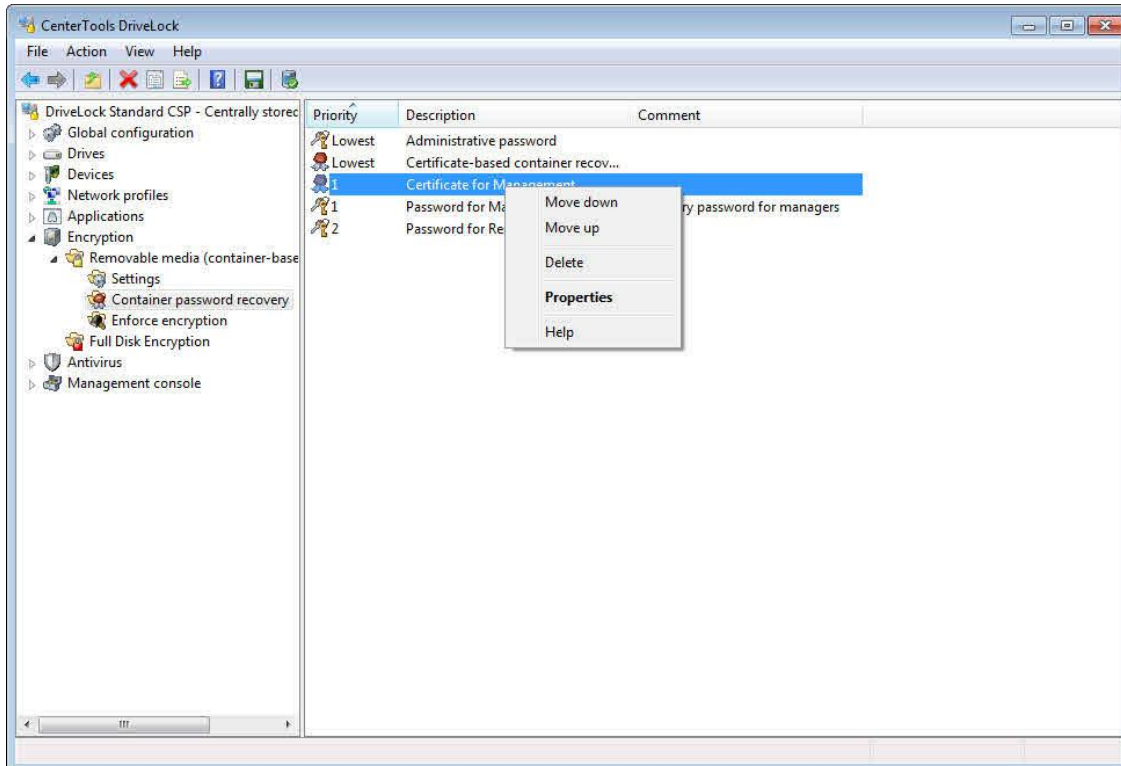
- Any type of encryption
- Encryption by users (using command line or GUI)
- Enforced or automatic encryption



On the tabs *Computers*, *Networks* and *Users*, select which of these entities the rule will be used for.

Click **OK** to save the rule. The new rule is displayed in the right pane. The first rule you create is assigned the priority of 1. The initial priority of additional rules is always one higher than the highest existing priority.

To change the priority of a rule, right-click it and then click **Move down** or **Move up**.



If you delete a certificate that was used for encrypting containers, password reset or automatic mounting will no longer be possible using this certificate.

14.2.2.3 Configuring Enforced Encryption

Activate enforced encryption with *DriveLock Encryption 2-Go* in the policy at:

Encryption / Settings / Enforced Encryption Method

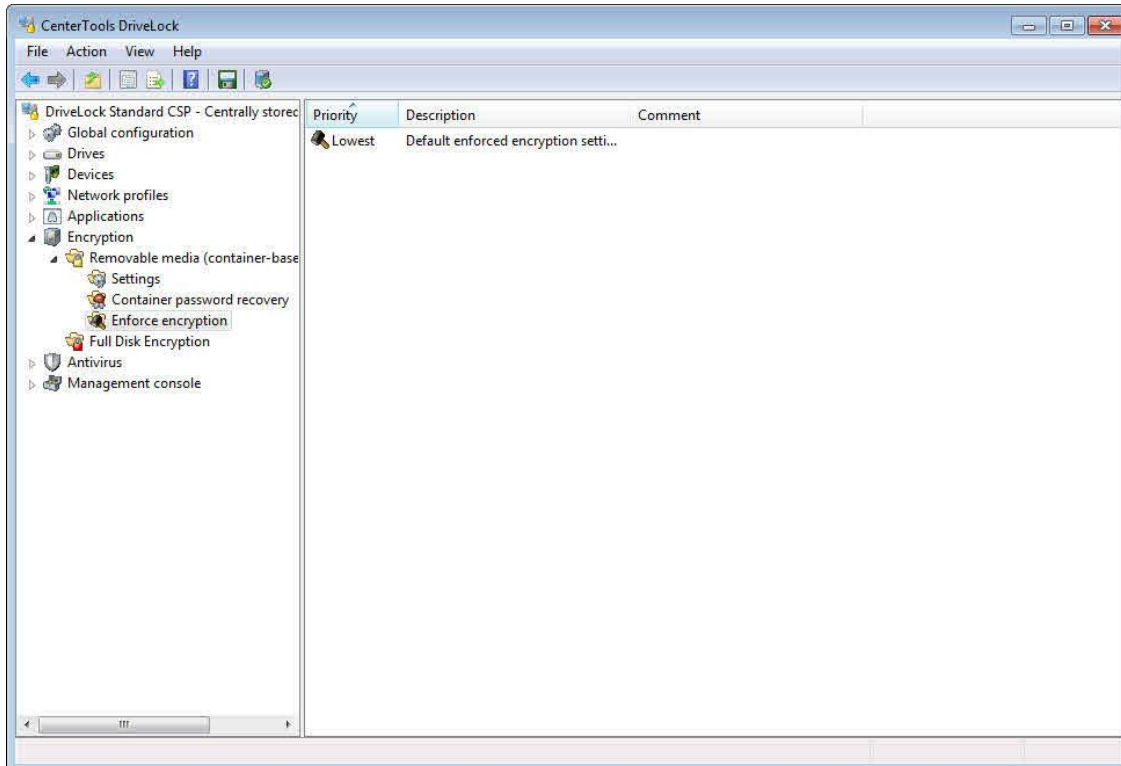
Check **DriveLock Encryption 2-Go**.

You also may use *DriveLock File Protection* to enforce encryption (see [Configuring Enforced Encryption with File Protection](#)).

Before USB-connected drives are automatically encrypted using DriveLock enforced removable media encryption, you have to configure some general settings, including the encryption algorithms to be used, whether existing data will be preserved when a drive is encrypted and some other settings. You can configure multiple sets of encryption settings and then assign different settings for certain users, computers or networks. This may be desirable when you need to use different encryption algorithms for certain groups of users. For example, you could enforce the use of AES (FIPS mode) to encrypt drives used by management and use AES for drives encrypted by all other users. To do this, first create one enforced encryption rule that specifies AES with the *Lowest* priority. Then create another enforced encryption rule specifying AES (FIPS mode) and filter the second rule to only apply to the user group Management.

To enable Encryption 2-Go, at least one set of enforced encryption settings with the priority *Lowest* must have been created. Once you have created one or more enforced encryption rules you also need to specify the option *Enforce encryption* in any drive rules for drives you want to encrypt automatically.

To enable automatic encryption of removable drives you must configure the settings that are used to automatically encrypt removable drives that users connect to a computer.

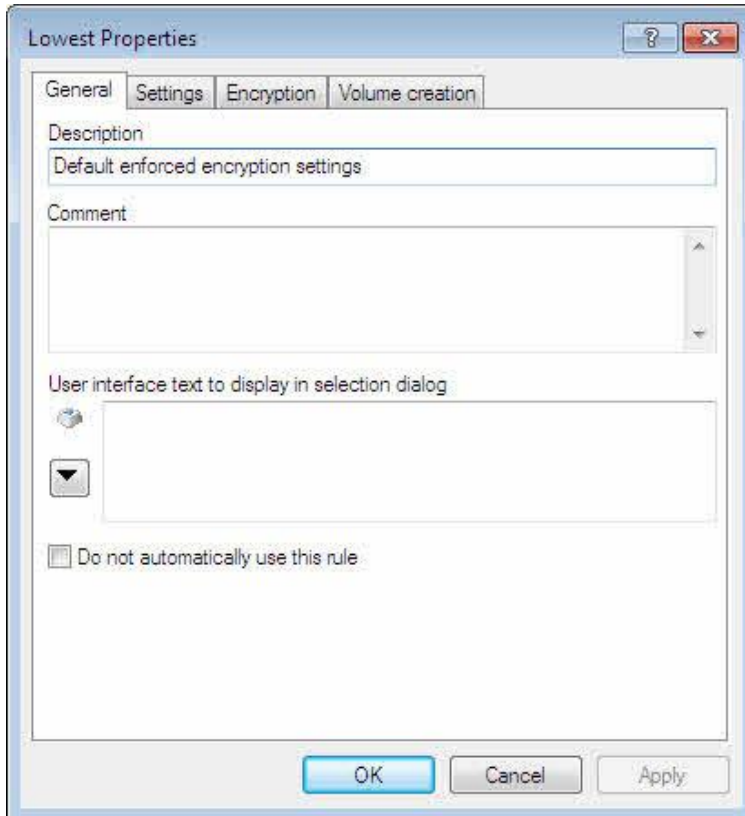


14.2.2.3.1 Settings Available for All Automatic Encryption Rules

Click **Enforce encryption** and then double-click **Default enforced encryption settings**.


A default set of enforced encryption settings that is assigned the lowest priority is always available and cannot be deleted. Before you can use enforced encryption you need configure the default settings or create a custom encryption rule.

Configure the following settings that DriveLock will use when automatically encrypting a removable drive.



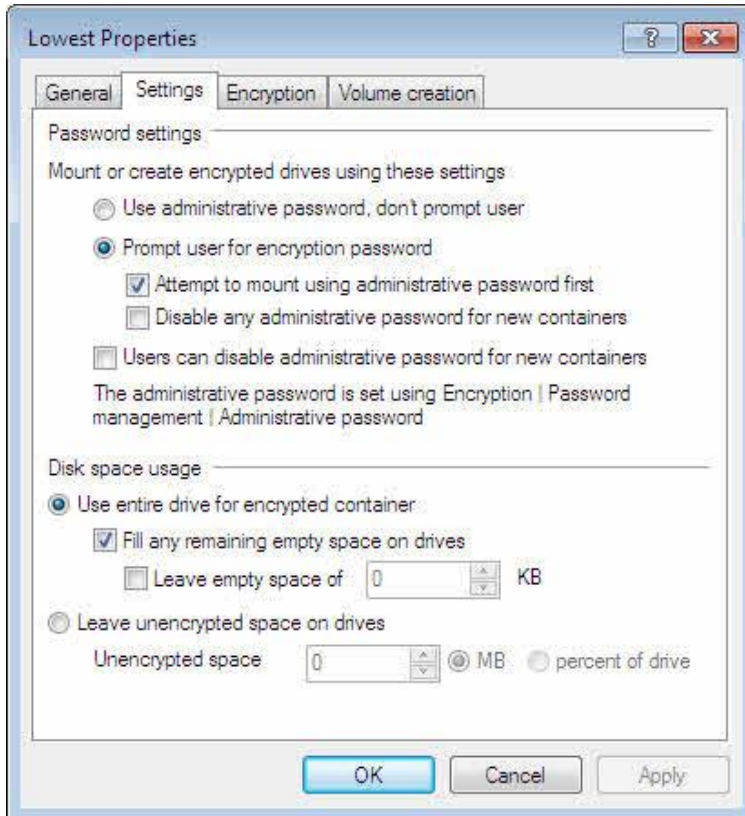
The description is displayed in the DriveLock management Console and helps you distinguish between different rules. The Comment field is also used to identify encryption rules.

The next two settings are only used if you also enable users to select an encryption rule and the current rule is one of the choices to be offered.

In the field “*User interface text to display in selection dialog*” type the text that is displayed on the button in the policy selection dialog box. (For more information about selecting an encryption policy, refer to the section “[Creating User Selection Rules](#)”.) If you have preconfigured multilingual notification texts you can select these texts by clicking the  button.

If you want to use the encryption rule in a User Selection Rule, you need to select the “*Do not automatically use this rule*” checkbox. Selecting this option ensures that the encryption settings are not immediately enforced when a drive is connected. Instead a user is presented with a dialog box for selecting an encryption rule. Only after the user has selected an encryption rule will the settings in this rule be enforced.

Configure the following on the *Settings* tab:



- *Use administrative password, don't prompt user*

Select this option if you want DriveLock to mount and create encrypted drives without prompting users for a password. To use this setting, you must first configure an administrative password. Users do not have the option to specify their own password. If you select this option, you can use encrypted drives on all computers that are configured with the same administrative password, but you are not able to access any encrypted drive using the Mobile Encryption Application.

- *Prompt user for personal password*

Select this option if you want DriveLock to prompt for the password of the encrypted drive when the computer detects an encrypted drive or when initially encrypting a drive. If you select this option, you can use encrypted drives using the Mobile Encryption Application.

- *Attempt to mount administrative password first:* If you have configured an administrative password, you can also select the option to try mounting drives using the administrative password first. If you select this option, users are not prompted for a password when using an encrypted drive on any computer that is configured with the same administrative password. Users are still prompted for the password when accessing an encrypted drive by using the Mobile Encryption Application.
- *Disable any administrative password for new containers:* As soon as a user sets a personal password, DriveLock deletes the administrative password. Once the administrative password has been deleted, access to the encrypted data is only possible by providing the personal password.

- *Users can disable administrative password for new container*

Select this option to allow users to create “private” encrypted containers with no access using the administrative password. If you also select the “Use administrative password, don't prompt user” setting, a user must select “**private**” when creating the container before being able to type the encryption password.

When no administrative password has been configured and offline recovery of removable drives has been disabled, recovering a forgotten password is NOT possible.

- *Use entire drive for encrypted container / Fill technically remaining empty space on drives*

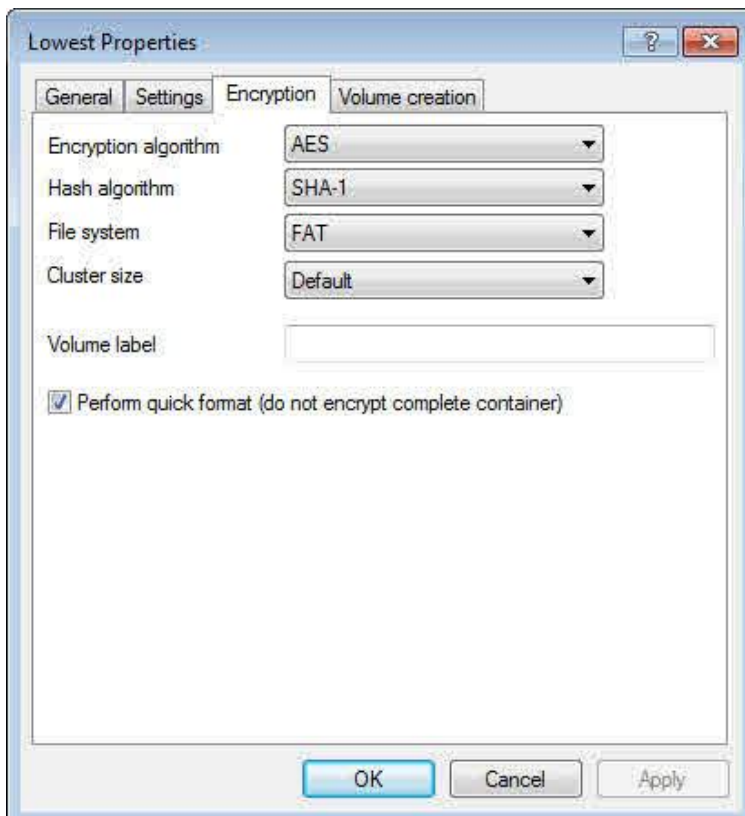
Select *Use complete drive for encrypted container* to use all available space on a drive when creating an encrypted contain. When a drive contains data that will be encrypted, DriveLock needs to estimate how much space is available for the encrypted container when it will be copied to the removable drive.

- *Fill any remaining empty space on drives:* To ensure that the container size doesn't exceed the available space, normally a small amount of unencrypted space remains available on the drive after the process completes. Select this checkbox to have DriveLock fill this remaining space with a hidden system file to ensure that users can't inadvertently copy data to the unencrypted space when using the drive on a computer where encryption is not enforced.
- *Leave empty space of x KB:* In some Windows 7 environments a few kilobytes of space must remain available for the operating system to access a drive. Select this option and specify the size of this empty space to enable access in such environments.

- *Leave unencrypted space on drives*

Select this option to leave unencrypted space on a drive that is encrypted. Enter a number and then select whether the number refers to the size of the unencrypted space in megabytes or a percentage of the total available space.

Select the "Encryption" tab.



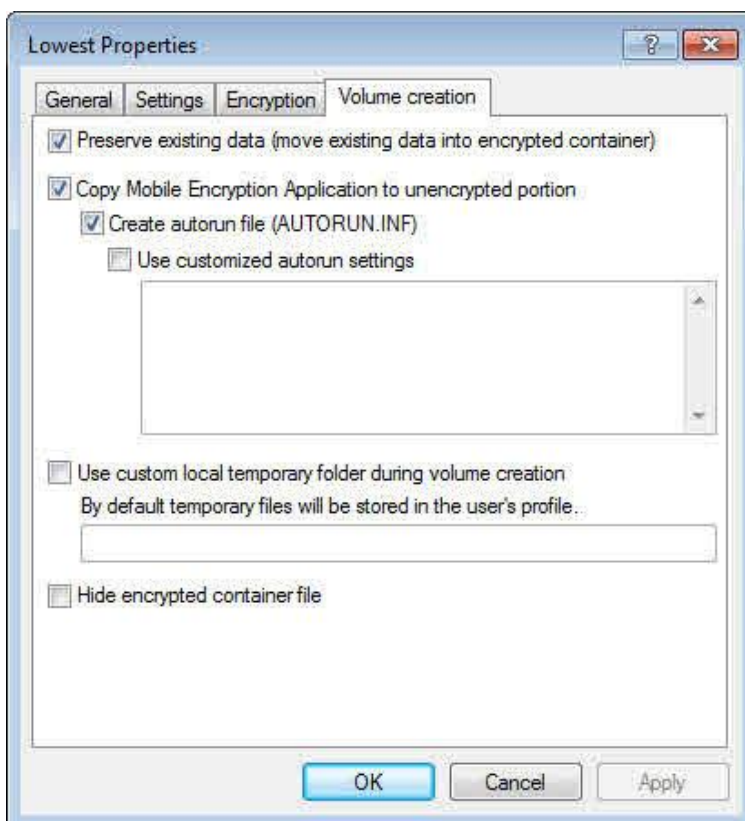
The following encryption settings are available:

- *Encryption algorithm:* Select the encryption algorithm that is used to encrypt drives when your policy enforces media encryption.

- *Hash algorithm*: Select the password hash algorithm that is used to encrypt drives when your policy enforces media encryption.
- *File system*: Select NTFS or FAT as the file system that is used on encrypted drives when your policy enforces media encryption.
- *Cluster size*: Select the cluster size that is used for the file system on encrypted drives when your policy enforces media encryption.
- *Volume label*: Type a volume label that is assigned to encrypted drives when your policy enforces media encryption.
- *Perform quick-format*: To speed up the process of creating an encrypted volume, select the “**Perform quick-format**” checkbox. This prevents the DriveLock Agent from pre-initializing and encrypting all space in newly created encrypted volumes. Instead, only the required space is initially encrypted. Selecting this option can significantly reduce the time required for initial encryption, but some existing unencrypted data that remain accessible until it is overwritten by files that are added to the encrypted device at a later time.

Quick format results in a noticeable decrease of the encryption time only on computers running Windows 7.

Select the *Volume creation* tab.



The following settings for volume creation are available:

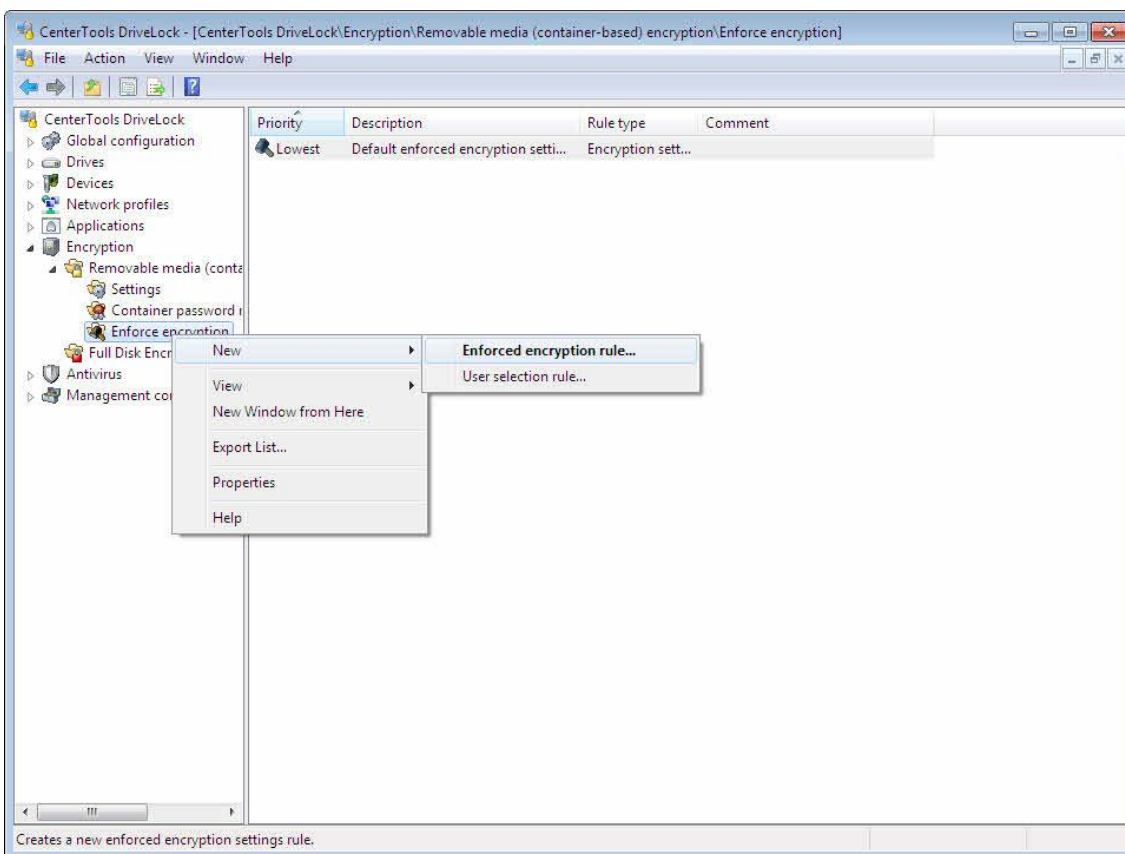
- *Preserve existing data*: Select this checkbox to create an encrypted removable drive without deleting the data that’s currently stored on it. Instead, DriveLock creates a temporary container in the user’s profile on the computer’s hard drive, copies all files from the drive to this container and then moves this container to the removable drive.
- *Copy Mobile Encryption Application to unencrypted portion*: Select this checkbox to have DriveLock copy the Mobile Encryption Application to removable drives when a drive is encrypted and your policy enforces media

encryption. You use the Mobile Encryption Application to access encrypted removable media on computers where DriveLock is not installed, such as an employee’s home computer.

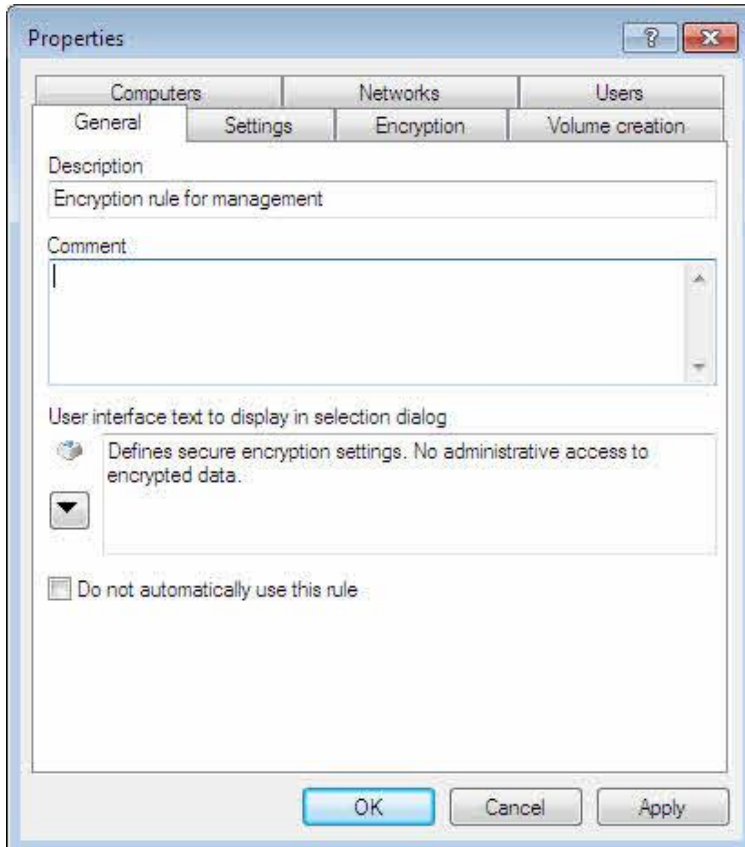
- **Create auto run file (AUTORUN.INF):** Select this checkbox to automatically copy the default **autorun.inf** to the removable drive. This file facilitates the launching of the Mobile Encryption Application when the drive is connected to a computer that is not running DriveLock.
- **Use customized auto run settings:** To change the content of the **autorun.inf** file, select the “**Use customized auto run settings**” checkbox and then type the contents of the custom file in the text box.
- **Use custom local temporary folder during volume creation:** Select this checkbox and specify a folder that exists on each client computer for DriveLock to create temporary container files in this folder. By default, temporary container files are created in the local user profile.
- **Hide encrypted container file:** When you select this option, the container file **EEDATA.DLV** is marked as hidden.

Click **OK** to accept the settings.

14.2.2.3.2 Creating Multiple Encryption Rules

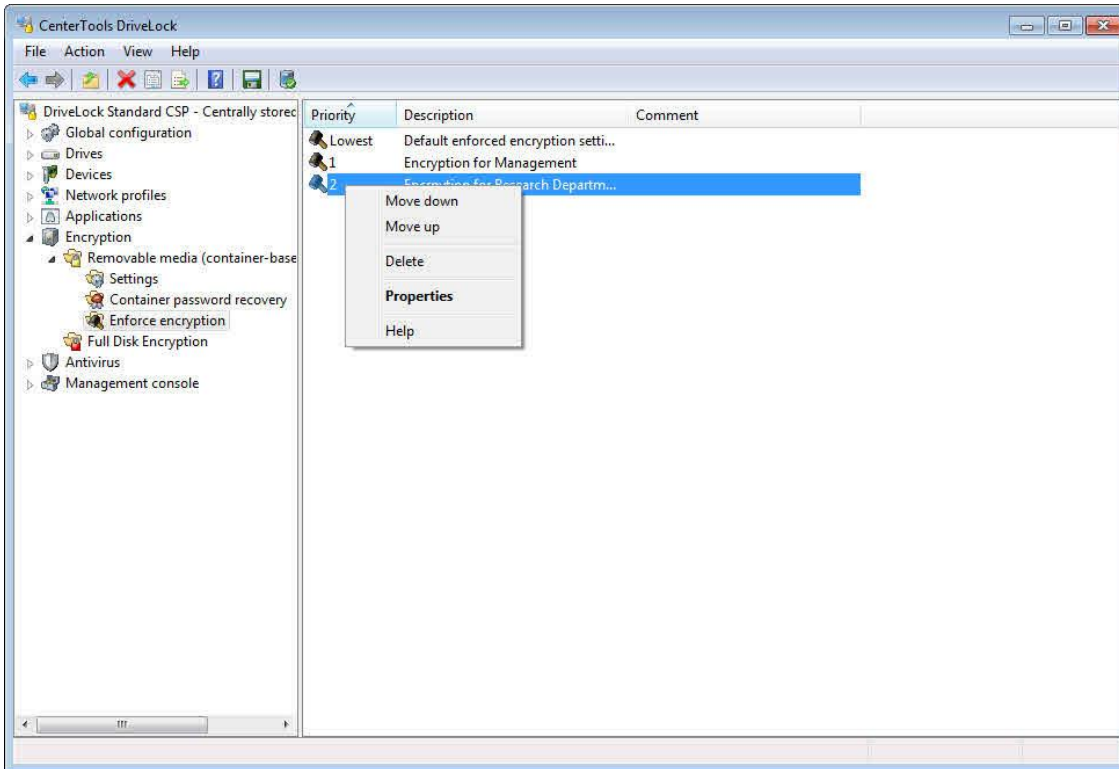


To create an additional enforced encryption rule, right-click **Enforced encryption**, point to **New** and then click **Enforced encryption rule**.



The settings on the *Settings*, *Encryption* and *Volume creation* tabs are identical to those available for the default rule. On the tabs *Computers*, *Networks* and *Users*, select which of these entities the encryption rule will be used for. Because these settings work the same way as in other DriveLock rules, such as drive locking rules, they are not described in detail here. Selecting users to whom a rule applies is most frequently used to assign different enforced encryption settings to different groups of users.

Click **OK** to save the rule. The new rule is displayed in the right pane. The first rule you create is assigned the priority of 1. The initial priority of additional rules is always one higher than the highest existing priority.



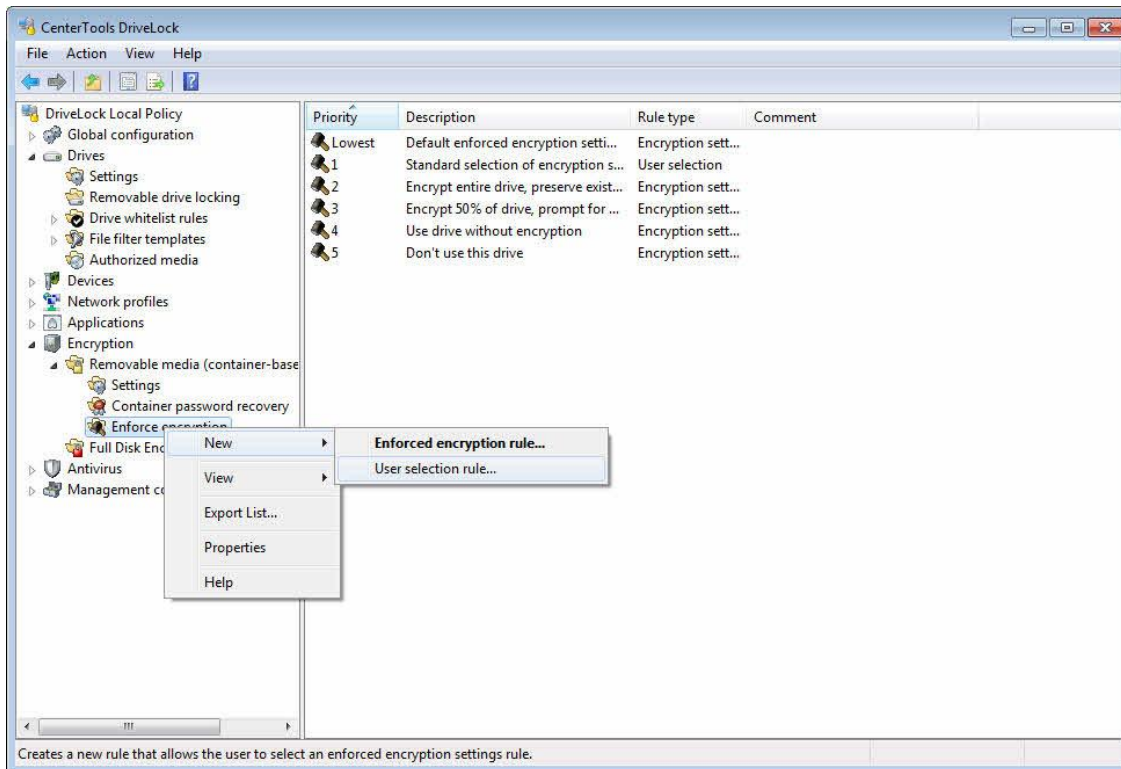
To change the priority of a rule, right-click it and then click **Move down** or **Move up**.

14.2.2.3.3 Creating User Selection Rules

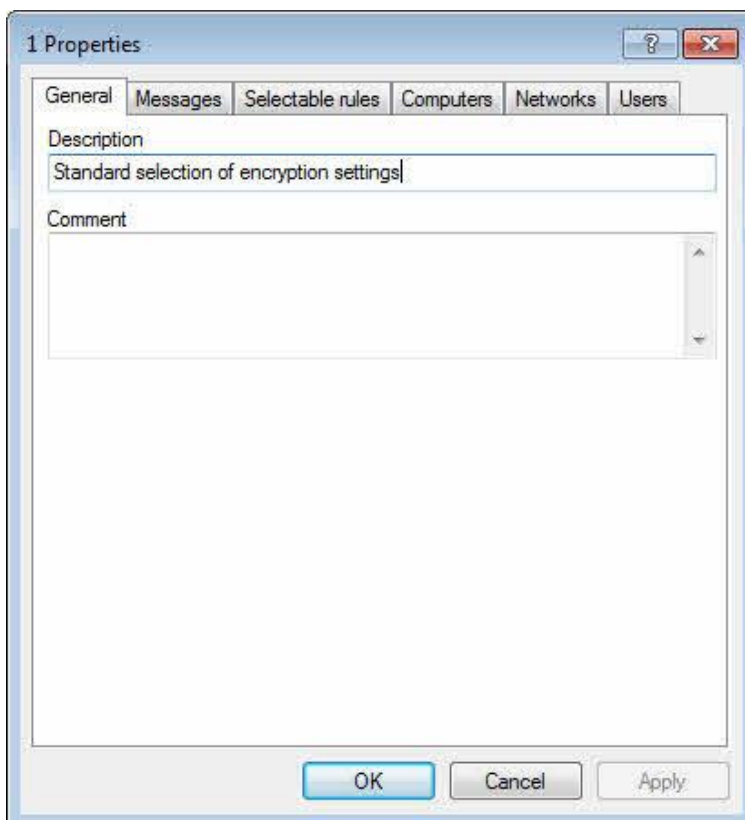
You use User Selection Rules to enable users to select the encryption and usage options for an encrypted drive. The settings in the rule determine the appearance of a dialog that is displayed when a user connects a drive and which encryption rules a user can select in this dialog box. The following graphic is an example of such a dialog box:



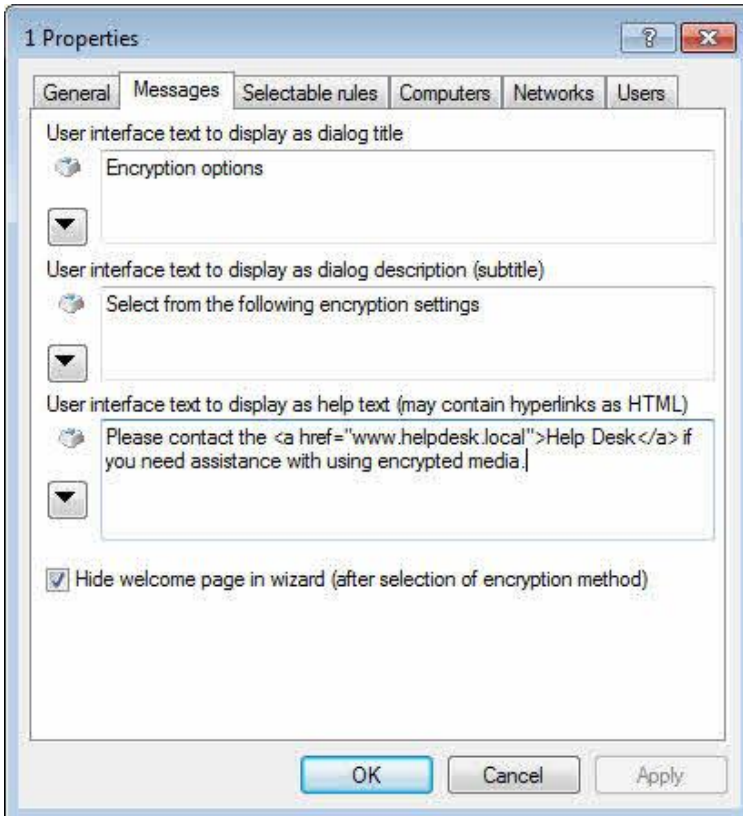
To create a user selection dialog box, perform the following steps:



To create a user selection rule, right-click **Enforce encryption** and then click **New -> User selection rule**.




Type a name and an optional comment. Next, click the **Messages** tab.



Specify the text to be displayed in the top area of the selection dialog box.



You can type each of the three text elements or click the  button to select from multilingual notification texts that you have previously created.

Select the checkbox “*Hide welcome page in wizard (after selection of encryption method)*” to not display the Welcome page of the encryption wizard if the option selected by the user causes this wizard to start.

To configure which encryption rules are available to users, click the **Selectable rules** tab.



In the top section of the dialog box you can add up to three previously created encryption rules that will be displayed to users. The order in which you add the rules determines the order in which they will be displayed in the selection dialog box.

The selection dialog box can contain a maximum of three choices of encryption rules in addition to the option "Allow selection of 'No access to volume'". The option "Allow selection of 'Access volume without encryption'" counts as one of these choices. If you select this option you can only add two custom encryption rules.

If you enable the option "Allow selection of 'Access volume without encryption'" and the user selects this option, the user will have full read and write access to the drive even if the applicable drive locking rule grants no access or only read access. When enabling this option it is recommended to also select the "Show usage policy before unlocking the volume" checkbox to display a usage guideline to the user before access to the drive is granted.

The option "Allow selection of 'No access to volume'" is essentially equivalent to a Cancel button. If the user selects this option, no automatic encryption settings are enforced and the user is granted to type of access that has been defined in the applicable whitelist rule for the drive. The same access restrictions are enforced if a user cancels the encryption wizard without completing it.

On the tabs *Computers*, *Networks* and *Users*, select which of these entities the user selection rule will be used for. Because these setting work the same way as in other DriveLock rules, such as drive locking rules, they are not described in detail here. Selecting users to whom a rule applies is most frequently used to present different encryption choices and display messages to different groups of users.

To change the priority of a rule, right-click it and then click **Move down** or **Move up**. To delete a rule, right-click it and then click **Delete**.

Always ensure that a user selection rule has a higher priority (lower number) than the first enforced encryption rule.

To display a graphic, such as a company logo, in the top right corner of the selection dialog box, create a bitmap file of 48 pixels x 48 pixels and name it DLWizardLogo.bmp. Add this file to DriveLock File Storage. When DriveLock detects the presence of this file, it automatically replaces the standard logo with it.

14.3 Recovering Encrypted Containers

If a user forgot the password for an encrypted container, or if the password is not available for another reason, you can use one of recovery mechanisms provided by DriveLock to gain access to the data stored in the encrypted container. To use the first recovery method, mount the container using the administrative password and then access the data. The second recovery method is certificate-based recovery, which has the following advantages:

- Password recovery is possible even when you don't have physical access to the encrypted container. You can create a recovery code that enables a user to change the password. This recovery code can be provided to the user by telephone.
- To recover a password you don't need to provide the administrative password to a user or helpdesk employee, and the person performing recovery does not need to have physical access to the encrypted container.
- You can manually distribute the required public/private key pair certificate into the private certificate store of the Administrator or helpdesk employee who will recover encrypted containers. For security reasons the certificate should also be marked to not be exportable from the store.

The challenge/response procedure that is used for offline password recovery is similar to the procedure that is used to give temporary access to locked drives and devices. First, the user who needs to access data in the encrypted container runs a wizard to create a challenge code. Then an administrator or helpdesk employee uses the DriveLock Management Console to create the corresponding response code. Finally, the user types the response code into the wizard. After the wizard validates the response code, the user is prompted to provide a new password.

14.3.1 User-Initiated Password Recovery

The steps a user needs to perform to recover a forgotten password are described in the *DriveLock User Guide*.

14.3.2 Recovering Encrypted Drives and Folders

The administrator's part of the recovery process is identical for encrypted drives (containers) and folders.

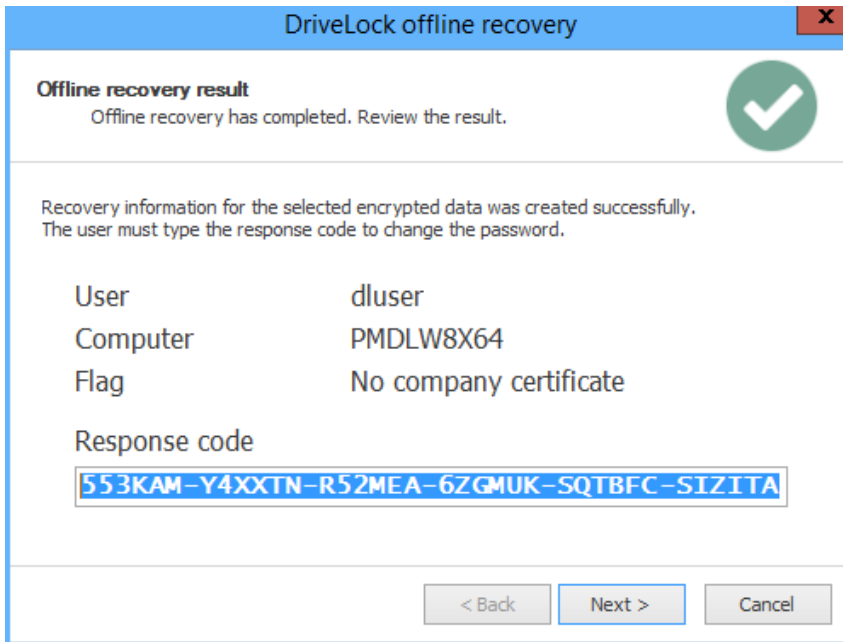
Recovery may become necessary when a user has lost access to encrypted drives or folders because of forgetting a password or losing access to a certificate's private key. Administrators or helpdesk personnel can perform an offline recovery operation in conjunction with the user that uses a challenge/response mechanism to restore access.

The challenge/response mechanism validates both the challenge (request code) that DriveLock creates for the user and the corresponding response code that is generated by the person performing the recovery. Only when both codes are valid for the drive or folder to be recovered, can access to the data be restored (for example enabling the user to select a new encryption password). The user generates the challenge code using a wizard and provides this code to an administrator. The administrator checks that the request code is valid and then generates a response code that is in turn validated by the wizard running on the client computer.

To perform offline recovery, an administrator needs to perform the following steps:

1. In the *DriveLock Management Console (MMC)* at **Operating /** section *Encryption recovery resp.* in the *DriveLock Control Center (DCC)*, functional area **Helpdesk** open **Container-based encryption recovery** or **Encrypted folder recovery**.
2. Type the challenge code that was provided by the user.

3. Click **Next** resp. **Find**. The wizard locates the challenge code in the DriveLock database. If more than one hit is shown, select the appropriate folder or container.
4. Next you have to provide the recovery certificate (from certificate file DLDlvRecover.pfx, smart card or certificate store) and where required the password.
5. Next a response code is generated and displayed. Provide this response code to the user and finish the wizard



If you lost the private key of a certificate that was used for encryption, a recovery/password reset will no longer be possible.

Part XV

DriveLock File Protection

15 DriveLock File Protection

DriveLock File Protection is a centrally managed, transparent data encryption solution that is completely integrated into the DriveLock Management Console.

To use DriveLock File Protection you need a license for all computers where you use this type of encryption.

DriveLock File Protection is a file and folder encryption product. Unlike container-based encryption (such as DriveLock 2-Go), DriveLock File Protection encrypts designated files. When a file is encrypted, its entire contents are encrypted but the file structure and file name remain unchanged. This ensures that encrypted files appear in Windows Explorer the same way as unencrypted files. Also, other programs, such as backup or defragmentation utilities, treat encrypted files the same as any other file. Only when you try to view the contents of a file, for example, if you open it in Microsoft Word, does the encryption become apparent.

15.1 How Does DriveLock File Protection Work?

The way DriveLock File Protection works is rather straightforward: First, a folder is marked as “*encrypted*”, which indicates that all data in this folder is to be encrypted. Next, authorized users are designated for whom DriveLock File Protection will automatically and transparently encrypt and decrypt files as they are read and saved.

Note:

The following folders are excluded from encryption:

- the Windows directory, typically C:\Windows
- the \Program Files and \Program Files (x86) directories

Creating encrypted subfolders is allowed below the Users directory, typically C:\Users<user name>

and in

- <user name>\Desktop
- <user name>\Documents

but not in

- All Users\Application Data and <user name>\Application Data
- <user name>\Start Menu

If a user tries to encrypt these folder, a message will appear: *"The selected folder cannot be encrypted. Certain system folders (and subfolders) cannot be encrypted for compatibility and stability reasons."*

On a computer where DriveLock File Protection is active, it checks every time a folder is accessed whether that folder is marked as encrypted. When such a folder is detected, the current user’s permissions are validated and encryption or decryption is automatically performed in the background as files in the folder are accessed.

You can exempt specific processes, such as backup programs or file synchronization operations, from the automatic encryption and decryption to prevent any impact on existing system maintenance routines.

To authenticate users, DriveLock File Protection can use the following two methods:

- Passwords: To access files in an encrypted folder, a user must provide a password.
- Certificates: Authentication uses a certificate from the user’s certificate store in Windows or from a smart card or token.

To use certificates for authentication, an existing Public Key Infrastructure (PKI) is not required. Instead you can use the certificate functionality built into DriveLock itself.

If your organization already has an existing PKI and uses it to issue user certificates, you can use this PKI to authenticate users for DriveLock File Protection.

All encryption and decryption operations take place in the background and are completely transparent to users. On a computer with modern processors that include hardware-based encryption (AES NI), DriveLock File Protection takes advantage of this functionality for approximately 4 times better performance.

Administration of the encryption of centralized file resources, such as shared folders and network-attached storage (NAS), can be performed by IT administrators using the DriveLock Management Console. Administrators can delegate the permissions to perform these tasks to others. This enables designated individuals to administer permissions for their departments and also makes it possible to remove the permission to decrypt certain sensible files even from administrators.

In addition to centrally managed folders, users can also create their own encrypted folders and securely store data in them. This can include folders on flash drives and on cloud storage providers, such as Dropbox. As with centrally managed folders, permissions to access data in such individual encrypted folders can be given to additional users.

This manual describes the administration of centrally managed folders. The DriveLock User Manual describes the use of individual encrypted folders.

15.2 Supported Encryption Mechanisms

DriveLock supports the following encryption algorithms:

- *AES (recommended)*: The Advanced Encryption Standard (AES) is a symmetric encryption mechanism that was chosen by the National Institute of Standards (NIST) as successor to DES and 3DES in October 2000. It is also called the Rijndael algorithm for its developers Joan Daemen and Vincent Rijmen. DriveLock uses a 256-bit key (AES-256), which is considered sufficient also for top secret information (U.S. CNSS (Committee on National Security Systems)).
- *Triple DES*: Triple DES (3DES) is a symmetric encryption method based on the older DES (Data Encryption Standard) but works with twice the key length (112 bit) of its predecessor. Data is encrypted using three successive DES operations. Because of the key length, 3DES is regarded as a relatively safe method for encrypting most data, unlike DES, which is more susceptible to brute-force attacks.
- *IDEA*: The IDEA algorithm (International Data Encryption Algorithm) was developed in 1990 by James L. Massey and Xuejia Lai as a joint project between ETH Zurich and Ascom Systec AG. IDEA is a symmetric key block cipher that uses 128-bit keys. During encryption, clear text is broken into 64-bit blocks and the key is divided into 16-bit fragments. Encryption is performed by combining the logical function XOR, the addition of modulo 216 and the multiplication by module 216+1. The combination of these three operations, chosen from different algebraic groups, is designed to ensure a high degree of security.

Hash algorithms are used to validate passwords or private keys without storing the passwords or key material themselves. DriveLock supports the following hash algorithms:

- *SHA-1*: This algorithm was developed by NIST (National Institute of Standards and Technology) in cooperation with the NSA (National Security Agency) as the secure signing hash function of the digital signature algorithm (DSA) for the Digital Signature Standard (DSS). Published in 1994, Secure Hash Standard (SHS) specifies a secure hash-algorithm (SHA) with a hash value of 160 bits for messages with a size of up to 264 bits. SHA is similar to the MD4 algorithm developed by Ronald L. Rivest. There are three SHA versions, SHA-0, SHA-1 and SHA-2. The SHA-2 family uses an identical algorithm with a variable digest size. Depending on this digest size, the algorithm is called SHA-224, SHA-256, SHA-384 or SHA-512.

- **RIPEMD-160:** RIPEMD-160 was developed by Hans Dobbertin, Antoon Bosselaers and Bart Preneel and published 1996. It is an improved version of RIPEMD (based on MD4) and comparable to SHA-1 in security and speed. This algorithm is less likely to contain security holes because its development process was more open than that of SHA-1.
- **WHIRLPOOL:** Whirlpool is a cryptographic hash function designed by Vincent Rijmen (co-creator of the Advanced Encryption Standard) and Paulo S. L. M. Barreto. The hash has been recommended by the NESSIE project. It has also been adopted by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) as part of the joint ISO/IEC 10118-3 international standard.

15.3 Configuring DriveLock File Protection

Before you can use DriveLock File Protection you need to determine your exact requirements and perform the configuration steps that match these requirements.

You need to determine the following requirements:

- How will you administer the user certificates that will be used for authentication?
- What settings will apply to the encryption and decryption of data?
- What functionality will be available to users on their computers?
- What will be the folder structure that you will use for storing encrypted data and files?

For administering user certificates you can use the following methods:

- Certificates are managed by the user - a personal (self signed) certificate can be created using the DriveLock Application.
- Certificates are administered using DriveLock. The Certificates (public key) are stored by DriveLock in a database.
- User certificates are administered in an existing PKI using Microsoft Active Directory without any involvement by DriveLock.
- User certificates are administered in a third-party Windows compatible-environment without any involvement by DriveLock.

Certificate management using DriveLock is described in the section "[Managing User Accounts and Certificates](#)".

How to configure the various options for encryption and decryption and the configuration of user options is described in the section "[Configuring Encryption Rules for Clients](#)".

How to create and administer centrally managed encrypted folders is described in the section "[Centrally Managing Encrypted Folders](#)".

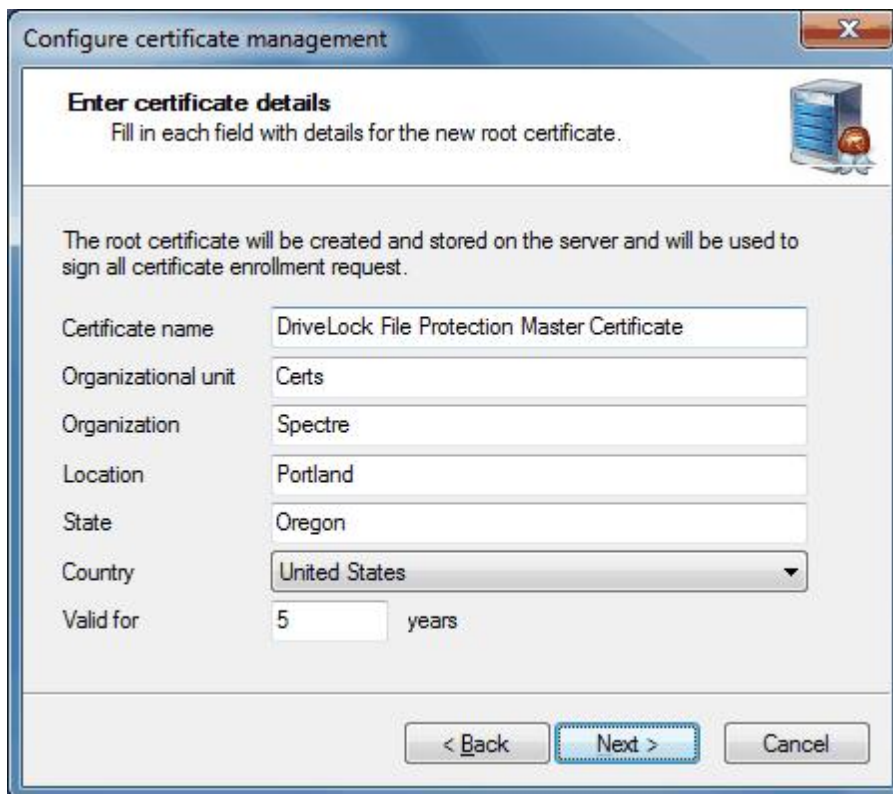
15.3.1 Creating a Master Certificate for Key Management

Before you can create and manage any user certificates using the DriveLock Enterprise Service, you need to create or import a master certificate for tenant root or per tenant. This master certificate will be used to sign all user certificates that you will issue.

You may use their master certificate of tenant root for all tenants or create a master certificate for each tenant. Open **DriveLock Enterprise Services / Server / double-click <Server Name> / Options** and check or uncheck **Enable tenant-aware certificate management**.

To create a master certificate for DriveLock File Protection:

1. Öffnen Sie **DriveLock Enterprise Services / Tenants** right-click **<tenant name> / All Tasks / Configure root certificate**. The Configure certificate management wizard appears.
2. Click **Next**.
3. To use an existing certificate, select “Existing Master Certificate” and then click “...” to select a certificate file. When prompted, type the password used to protect the private key, click **Next** and then continue with Step 5 of this procedure.
To create a new, self-signed certificate, select “Create new master certificate” and then click Next.
4. Provide all required information for the new master certificate, as shown in the following dialog box, and then click **Next**.



5. DriveLock stores the certificate in its database. When this process has completed, click **Finish**. If the process fails, review the reasons for this failure, and after eliminating the cause, run the wizard again.

When the master certificate has been created and the wizard has finished, certificate and key management is initialized on the server running the DriveLock Enterprise Service and the DriveLock Enterprise Service is restarted.

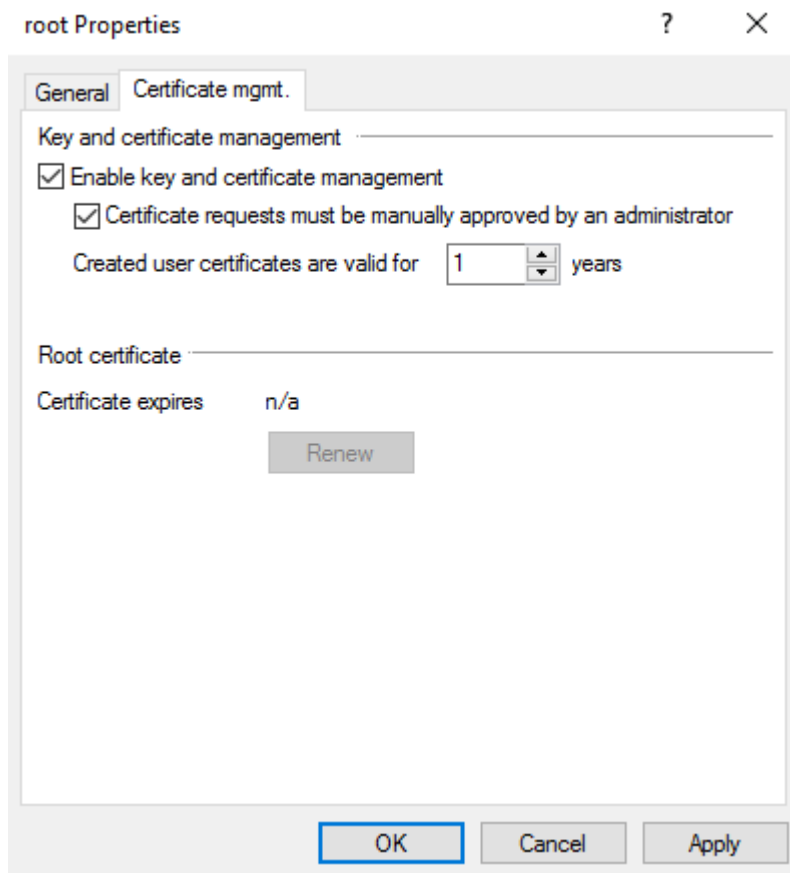
15.3.2 Configuring Certificate Management

Creating or designating a master certificate automatically activates the certificate and key management functionality of the DriveLock Enterprise Service. You can deactivate or reactivate this functionality at any time. Another setting used for certificate management is the configuration of how DriveLock File Protection issues the creation and renewal of user certificates. The following two methods are available:

- A user certificate is automatically generated and issued when a user applies for a certificate. (Default)
- An administrator must approve user certificates before they are issued to users.

To change settings for certificate management, perform the following procedure:

1. Navigate to **DriveLock Enterprise Service / double-click <tenant name> / Certificate mgmt.**



2. To activate certificate management, select the “*Enable key and certificate management*” checkbox.
3. To require an administrator to validate and approve all user certificates, select the “*Certificate requests must be manually approved by an administrator*” checkbox.
4. Enter the number of years the user certificate is valid for.
5. To save the settings, click **Apply**.

15.3.3 Configuring Encryption Rules for Clients

You configure policies for encryption and decryption of data and the behavior of DriveLock File Protection on a client computer in a DriveLock policy. The process of creating and distributing DriveLock policies is described in the chapter “Distributing DriveLock Configuration Settings”.

To open an existing policy, in the DriveLock Management Console perform the following steps:

1. In the navigation pane, click **Policies**.
2. In the details pane, right-click an existing policy and then click **Edit**.
3. After the policy opens in a new window, in the navigation pane of that window, click **Encryption -> File Protection**.

You can perform the following tasks:

- [Configuring encryption settings](#)
- [Configuring the encryption user interface](#)

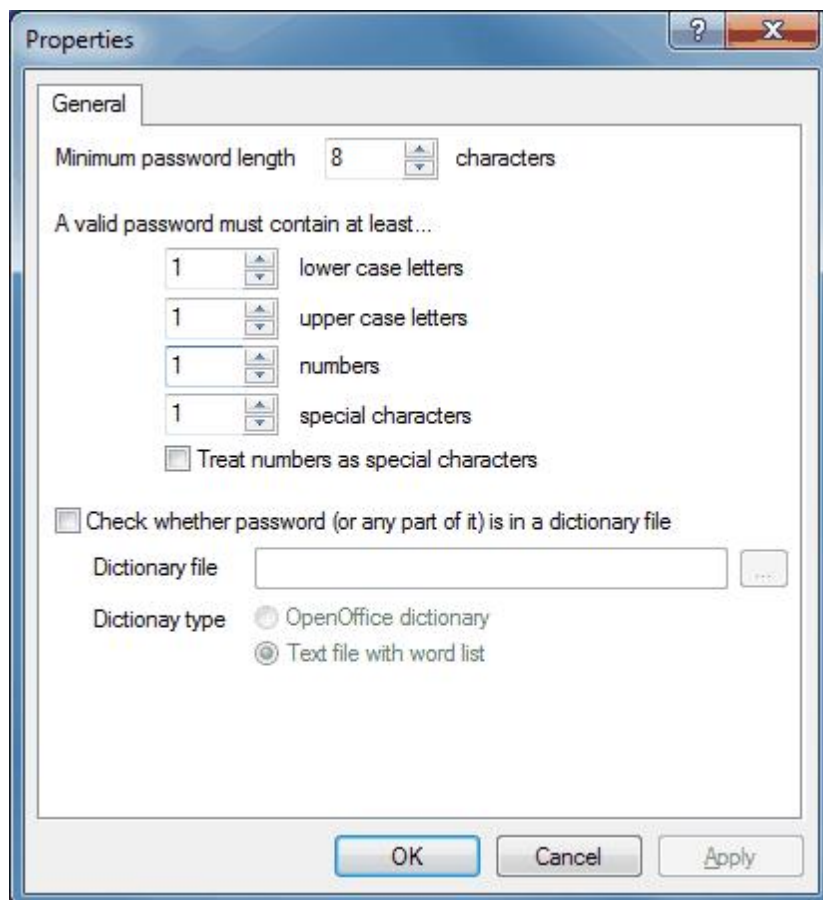
- [Configuring settings for encrypted folders](#)
- [Configuring additional settings](#)
- [Creating recovery certificates](#)
- [Configuring Enforced Encryption](#)

15.3.3.1 Configuring encryption settings

To configure encryption settings, in the navigation pane, click **File Protection** and then click **Settings**.

To configure the various settings, click the appropriate option in the details pane:

- *Encryption algorithm for encrypted folders*: Select the encryption algorithm to be used for encrypting data. (For more information about the available algorithms, refer to the section “[Supported Encryption Algorithms](#)”.)
- *Hash algorithm for passwords for encrypted folders*: Select the algorithm to be used for creating password hashes. (For more information about the available algorithms, refer to the section “[Supported Hash Algorithms](#)”.)
- *Minimum password complexity for encrypted folders*: Configure the required password complexity to match your organization’s IT policy. Password complexity is computed from the types of characters that are used and the length of the password. To define a custom requirement for password complexity, click **Password complexity policy** and then define the policy.
- *Password complexity policy*: Select the required number of characters in a password that need to be in each of the available categories. If your organization’s policy treats numbers and special characters as belonging to the same category, select the “*Treat numbers as special characters*” checkbox.



A dictionary can be a dictionary file in the OpenOffice format or a text file that contains a single word on each line. DriveLock includes OpenOffice dictionaries for English, German, Dutch and French. You can find these .diz-files in the DriveLock installation folder on the administration computer where you installed the DriveLock Management Console (for example “*DictEnglish.diz*”).

If you specify a custom file, ensure that this file exists on all Agent computers in exactly the same location, as the Agents looks for this file in the location you specify.

You can also place dictionary files into the policy file storage and select “*Policy file storage...*” as the dictionary location. Files located in the policy file storage are identified by an asterisk (“*”) in front of the file name and are copied to the client automatically. For more information about the policy file storage, refer to the chapter “[Using the DriveLock Policy File Storage](#)”.

When you use a dictionary to validate your passwords, keep in mind that passwords containing any part of a word contained in the dictionary are not allowed (for example if the dictionary contains “it”, passwords such as “hit”, “with” or “glitter” are not allowed).

15.3.3.2 Configuring the encryption user interface

To configure how the encryption interface appears to users, navigate to **File Protection** and then click **Settings**.

To configure any of the following settings, click the item and then complete the steps described for each of them:

- *Available context menus in Windows Explorer:* To configure the context menus that are available to a user who right-clicks an encrypted folder, click **Set to value** and then select from the available options. When you select *Not configured*, all menu entries are displayed.
- *Start menu configuration:* To configure where menu items that are available to users appear on the Windows Start menu, click **Set to fixed value** and then select from the available options. When you select *Not configured*, menu items are displayed under *All Programs -> DriveLock File Protection*.
- *Available Start menu entries:* To configure which commands are available from the Start menu, click **Set to value** and then select the items that will be available to users. When this option is set to “*Not configured*”, all commands appear on the Start menu.
- *Menu items available from the taskbar icon:* To configure which commands are available when right-clicking the DriveLock taskbar icon, click **Set to value** and then select the items that will be available. When this option is set to “*Not configured*”, all commands can be accessed from the taskbar icon.
- *Order of menu items in taskbar icon:* To configure the order in which commands are displayed when right-clicking the DriveLock taskbar icon, click **Set to fixed value**. To change the order of the menu items, select an item and then click **Up** or **Down**. To remove an item, select the item and then click **Remove**. To add a separator line, click **Add**. When this option is set to “*Not configured*”, the items are displayed in the default order.
- *User contact information for offline password recovery:* A user who has forgotten or misplaced the password for an encrypted volume can initiate a recovery process by starting the password recovery wizard from the Start menu or the taskbar. Because the recovery process requires assistance from an administrator or helpdesk employee, the user may require contact information, such as the helpdesk telephone number. To add any contact information to be displayed when a user initiates a password recovery, click **Set to fixed value** and then type the contact information. When this option is set to “*Not configured*”, no contact information is displayed.
- *Format for user display names:* To configure the format in which user names are displayed when administering permissions for encrypted folders, click **Set to fixed value**. When this option is set to “*Not configured*”, names are displayed in the format *[Last name], [First name]*.

- *Do not show popup messages for automatic folder mounting*: To disable the display of popup messages when connecting to encrypted folders, click **Enable**. When this option is set to “Disable” or “Not configured”, popup messages are displayed.
- *Do not allow users to save encrypted folder passwords*: To prevent users from saving passwords, click **Enable**. When this option is set to “Disable” or “Not configured”, users can select the “Save password” option to save a password and have it entered automatically the next time the users connects to the encrypted folder.
- *Encrypted folder password saving options*: Select whether and how users are allowed to save passwords of encrypted folders. Options are *deny*, *allow* or *allow - current session only*. If you select *current session only*, the password will be deleted, when the user logs off, but it will be valid for all folders secured with the same password. This eases working with multiple encrypted folders keeping security high.

15.3.3.3 Configuring Settings for Encrypted Folders

To configure encryption settings, navigate to **File Protection** and then click **Settings**.

To configure any of the following settings, click the item and then complete the steps described for each of them:

- *Encrypted volume password recovery methods*: To select which password recovery methods are available to users, click **Set to value** and then select the methods you want to be available. When this option is set to “Not configured”, all recovery methods are available to users.
- *Interval for checks for certificate revocation*: To configure the interval at which DriveLock checks whether a user certificate has been revoked, click **Set to fixed value** and then select a time interval. When this option is set to “Not configured”, DriveLock checks every 24 hours whether a certificate has been revoked.
- *Access to encrypted files in locked folders*: To configure the action DriveLock File Protection performs when a user does not have permissions to encrypt or decrypt a file, click **Set to fixed value** and then select from the following options. When this option is set to “Not configured”, access is denied.
 - *Deny*: Users without DriveLock permissions are not allowed to access encrypted folders even if the user has the required Windows permissions. The Windows “Access denied” message is displayed.
 - *Allow for administrator*: Users without DriveLock permissions can only access files if they are members of the Administrators group.

When you enable access without DriveLock permissions, the folder is treated for these users like any other Windows folder. Files are not decrypted when they are read and not encrypted when users write to them. This can cause problems when both user with and without DriveLock permissions write to the same files. When a user with DriveLock permissions accesses a file in an encrypted folder, DriveLock attempts to decrypt the file, preventing the user from reading it. When such a user writes to an unencrypted file, the file’s contents may be rendered unusable.

- *Automatic mount of encrypted folders*: To configure the behavior of DriveLock File Protection when connecting to an encrypted folder, click **Set to fixed value** and then select from the following options. When this option is set to “Not configured”, the option “On (show wizard if needed)” applies.
 - *On (show wizard if needed)*: DriveLock File Protection attempts to open the folder by using a user certificate from the local certificate store or a previously saved password. If the user does not have the required permissions or enters a wrong password, a window opens, prompting the user to select the authentication method. This option is appropriate when you don’t allow users to save their passwords or you use certificates that are not stored in the local certificate store, such as certificates on smart cards or tokens.

- *Fully automatic only, do not show wizard*: DriveLock File Protection attempts to open the folder by using a user certificate from the local certificate store or a previously saved password. If the user does not have the required permissions or enters a wrong password, the user is treated as not authorized.
- *Off*: Connections to an encrypted folder are not automatically established. The user is treated as not authorized until he or she right-clicks the folder and authenticates using the menu item *Mount encrypted folder*.

15.3.3.4 Configuring Additional Settings

To configure additional encryption settings, navigate to File Protection and then click Additional settings.

To configure any of the following settings, click the item and then complete the steps described for each of them:

- *Files and paths excepted from encrypted folder autoregistration*: To designate folders that DriveLock will never attempt to mount automatically, click **Set to configured list**. Then edit the list of folders by clicking **Add**, **Remove** or **Edit**.
- *Backup process names (access to encrypted data)*: To designate programs that need to access encrypted folders without having DriveLock permissions to decrypt data, click **Set to configured list**. Then edit the list of programs by clicking **Add**, **Remove** or **Edit**. Type program names without the path (for example, *backup.exe*). The program files for Dropbox, OneDrive and Google Drive are already automatically included.

Long filenames are not supported by the driver for recognizing backup processes. Enter the first seven characters instead. E.g. BACKUP.EXE (real 8.3 filename) but MYBACKU for MyBackupBackupAndRestore.exe.

15.3.3.5 Configuring Enforced Encryption

To force encryption of external drives, you can also use DriveLock File Protection instead of container encryption (see [DriveLock Encryption 2-Go](#)). For large drives, this will speedup the initialization, as no container has to be created first, but only the files will be encrypted while copied to the folder. Additionally you can create up to three folders with different permissions, e.g. one using an company certificate for all employees, one with user name and password for the owner and one unencrypted folder.

Use enforced encryption with DriveLock File Protection

1. Activate enforced encryption with DriveLock File Protection in the policy at:

Encryption / Settings / Enforced Encryption Method

Check **DriveLock File Protection**. Then for all new unencrypted drives, which have enforced encryption activated in a rule, the file- and folder encryption will be used instead of the container encryption.

Check **Let the user decide** if your users should have the option to use either file- and folder based or container based encryption.

2. Configure the encryption settings in *Enforce Encryption*.

With *right mouse click* you create one resp. more new encryption rules for different user groups.

- a. In the configuration dialog, tab *General*, enter a short description for the new rule
- b. In tab **Volume Creation** you check, whether to **preserve existing data** and to be copied/encrypted to the configured folder and if the *Mobile Encryption Application* shall be copied to the drive. If you don't select to **preserve existing data**, all data on the drive will be deleted, before it will be encrypted.
- c. In tab **Settings** define the permission and encryption settings and assign a name for the encrypted folder. In **extended settings**, you can name additional folders and check which folder shall receive the data to be preserved.

- d. In tabs **Computer, Networks and Users** you define for whom and where the rule shall apply.
- e. Apply a priority for the rule. The rule with the highest priority where the conditions apply, will be executed.

User selection of encryption rules (optional)

In the same manner you create new User Selection Rules and there add encryption rules, if users shall select the appropriate encryption rules by them self. Apply a proper priority to ensure, that this user selection rules are executed before encryption rules.

Did you check Let the user decide, then first the encryption method dialog will appear and afterwards the rules selection dialog. Take care to check the options, which are available in both dialogs only once.

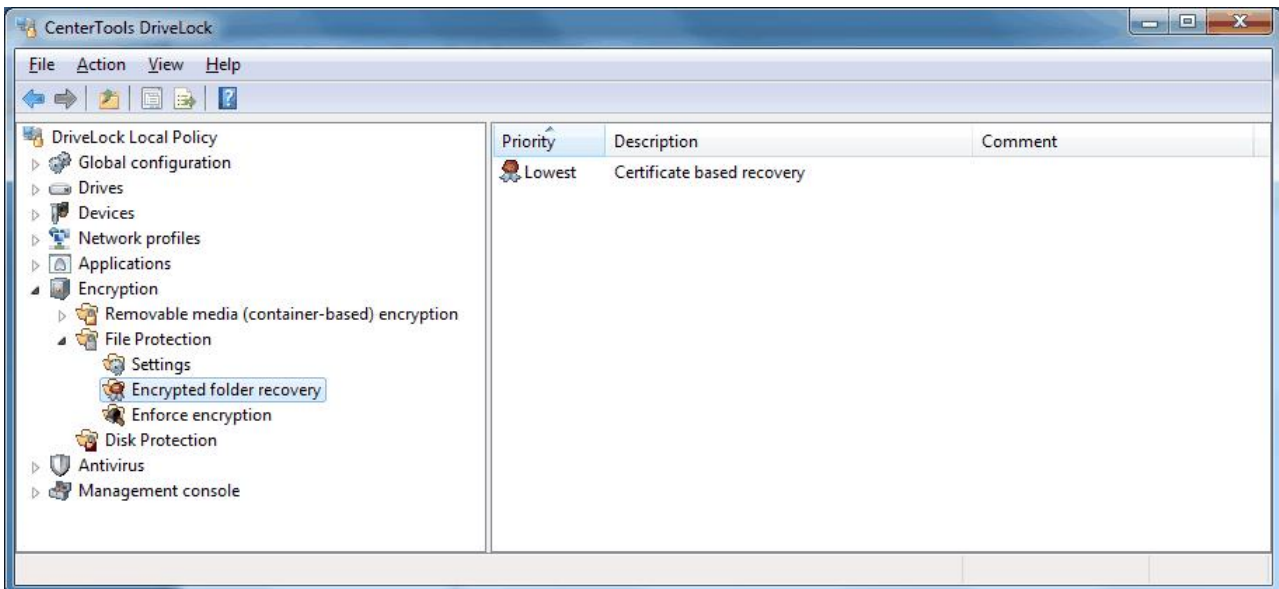
15.3.3.6 Configuring Recovery Certificates

To use offline recovery you have to first create a master certificate and the corresponding public/private key pair before creating the first encrypted container.


To enable advanced recovery scenarios you can create multiple recovery key pairs and use each of them for a different group of users, computers or networks. This lets you authorize different administrators or helpdesk personnel to only recover encryption passwords for certain encrypted containers but not for others.

Example: Especially in large IT environments you might use one encryption certificate for files encrypted by management and a different certificate for files encrypted by all other users. You would then provide the private key for the first certificate only to enterprise administrators, enabling them to recover passwords for management. The second private key would be shared with helpdesk personnel, enabling them to recover passwords for all other users.

To configure the settings for the recovery of encrypted folders, navigate to **File Protection** and then click **Encrypted folder recovery**.



If you use multiple encryption certificates and you recover an encrypted file, you have to provide the private key of the recovery certificate that was specified in the policy when the file was encrypted.

Recovery certificates are designated by the  symbol.

By default a single certificate-based folder recovery policy exists. This policy has the lowest priority and cannot be deleted.

To create a default recovery certificate, perform the following steps:

- Double-click **Certificate-based folder recovery**.
- Click **Certificate file** and then click **Create new**. This starts a wizard that creates a new recovery certificate.
- Click **Next**.
- Specify the folder where you want to store the certificate and the associated private key as files or select a smart card to store the certificate and private key on.
- Click **Next**.
- If you selected to store the certificate and private key on a smart card, further steps are required. Details depend on the smart card used.

Ensure to back up the certificate files in a secure location, such as a safe. The certificate and private key are required to recover access to encrypted folder when regular access is no longer possible.

- Type the password that will be required to access the private key that is stored with the certificate. To ensure that you typed the password correctly, you have to type it twice. To continue, click **Next**.

If you forget the password for accessing the private key you will no longer be able to recover encrypted files. To prevent this from happening, store a copy of this password in a secure location, such as a safe.

- DriveLock creates the certificate. When the process is complete and the certificate and associated keys have been stored in the selected location, the wizard notifies you that this has happened.
- If you selected to store the certificate and keys on a smart card, Windows prompts you to enter the PIN for the smart card.
- Click **Finish**.

DriveLock displays the file name of the certificate you created.

Once you have created the certificate and the first encrypted folder using this certificate was created, you must not create a new certificate. Doing so would replace the existing certificate and you would not be able to recover previously encrypted files.

To view the details of the certificate, click **Properties**.

DriveLock also stores the certificate and its private key in local certificate store of the user who created the certificate. The certificate's public key is also stored in the file storage of the local DriveLock policy.

If you stop the wizard before the certificate has been created or if an error occurred while running the wizard, DriveLock displays an error message and you need to run the wizard again to create the certificate.

If you previously created encrypted folders without a default recovery certificate, you can add certificate-based recovery data to these folders. To do this, select the *"Add recovery information to existing folders"* checkbox. If this checkbox is selected, each time a folder is mounted, DriveLock checks whether the container already contains recovery data. If no recovery data exists, DriveLock creates this data, adds it to the container and sends it to the DriveLock Enterprise Service.

If you are not using the DriveLock Enterprise Service or if you don't want to store recovery data in the DriveLock database, select the *"No offline recovery – do not upload recovery information to DES"* checkbox. If you disable offline recovery, you must have physical access to a file to recover the data stored in it.

To create an additional recovery rule, right-click **Encrypted folder recovery**, point to **New** and then click **Encryption recovery rule**.

Because you have not yet created a recovery certificate, no certificate information is displayed. To create a new certificate, follow the steps for creating a default recovery certificate.

On the tabs *Computers*, *Networks* and *Users*, select which of these entities the rule will be used for. Information on these tabs is applied in the same way as in other DriveLock rules, such as those for device control and application control and thus is not described in detail here.

Click **OK** to save the rule. The new rule is displayed in the right pane. The first rule you create is assigned the priority of 1. The initial priority of additional rules is always one higher than the highest existing priority.

To change the priority of a rule, right-click it and then click *Move down* or *Move up*.

If you delete a certificate that was used for encrypting folders, recovery will no longer be possible using this certificate.

15.3.3.7 Company certificate

Encrypted folders containing a company certificate can be mounted by any user, who has access to the corresponding private key in the windows certificate store. If so, when the user mounts an encrypted folder, DriveLock first checks, whether the folder can be decrypted using the company certificate. Then the folder will be mounted without any further user interaction. Otherwise, the user will be asked for his credentials.

DriveLock does not create company certificates but allows you to import the public key of any certificate (*.cer) you own. DriveLock does distribute the private key (*.pfx) to the windows certificate store (user account or computer account). You have

Technically a company certificate is very similar to a recovery certificate and configured in the same way (see chapter before).

Create a company certificate

To add a new company certificate in a policy open **Encryption / File Protection / Encrypted folder recovery / New / Company certificate... / General** and add a description and certificate.

Check **Enabled** to use the certificate when creating / updating encrypted folders.

Open tab **Options** and check the desired type of encryption.

For evaluation purposes you may use e.g. a DriveLock Recovery certificate as a company certificate. Import the DLFfeRecovery.cer to the policy and the DLFfeRecovery.pfx to the Windows certificate store

Update a company certificate

DriveLock does not care about the expiration date of a company certificate but still allows you to access and create encrypted folders. Nevertheless you may add new company certificates to your policy at any time and you may remove the expired certificates from your policy.

If you remove the (expired) private key from the Windows certificate store, you can no longer access the encrypted folders using this key. If this has been the only key for a folder, a new company certificate cannot be added any more.

15.4 Managing User Accounts and Certificates

Before you can administer users and their certificates you need to configure several settings. These settings are described in the sections "[Creating a Master Certificate for Key Management](#)" and "[Configuring Certificate Management](#)".

15.4.1 How User Administration Works

User administration in DriveLock File Protection allows you to issue and administer certificates for users without the need for an existing public key infrastructure (PKI).

The integrated user administration is not required if:

- You already have a Microsoft Active Directory environment and you are administering user certificates using this infrastructure
- You are already using a PKI that is compatible with Microsoft Windows
- You want to use exclusively passwords for encryption authentication. (Note that these passwords are different from Windows passwords.)

One main advantage of using user certificates for authentication with DriveLock File Protection is that encryption and decryption processes can be performed completely transparent to users and without requiring users from changing anything about how they access and use files and folders. Each time an encrypted folder is accessed, DriveLock File Protection checks whether the user's certificate store contains a user certificate and automatically uses this certificate for authentication.

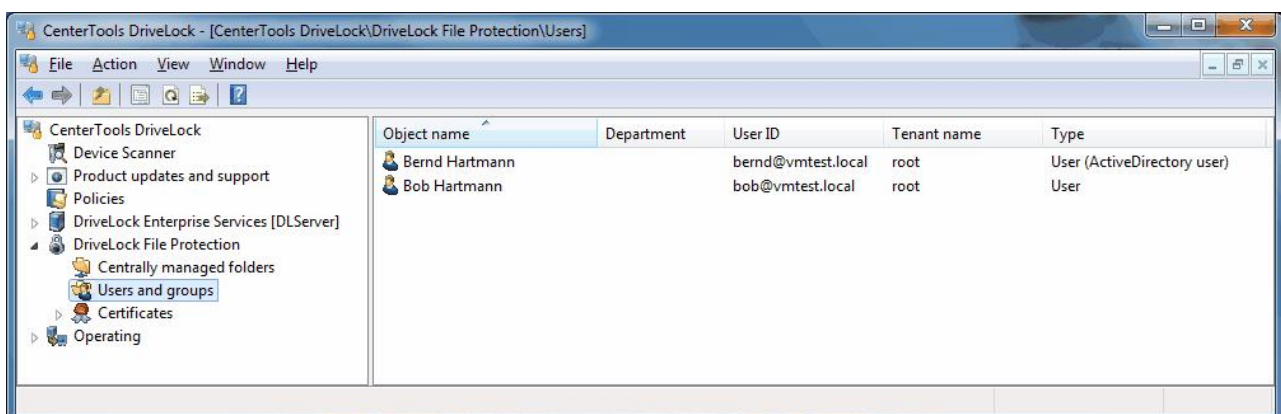
To make it easy for administrators to use certificates without having to become familiar with the details of a public key infrastructure (PKI), all functionality for quick and easy administration of users and their certificates is integrated into DriveLock File Protection. Users can apply for their own certificates, these applications can be automatically approved and stored in the user's certificate store. Administrators can add or remove users, modify, revoke and delete certificates and import existing certificates from Active Directory or other sources.

In DriveLock File Protection a user and the user's certificate are closely linked. Every DriveLock File Protection user needs a certificate and each certificate is linked to one user. When a user requests a certificate, DriveLock automatically creates a corresponding user account. Similarly, if an administrator creates a user account, DriveLock File Protection automatically creates a certificate for the user.

The DriveLock PKI does not store and manage the private key of a user's certificate. Users should export the certificate including the private key (PFX file) from the windows certificate store using the DriveLock Application and keep it in safe place. They have to import it again to the windows certificate store to access their encrypted folder from a different computer

15.4.2 Managing User Accounts

You use the DriveLock Management Console to administer user accounts. To perform user administration tasks, navigate to **DriveLock File Protection** and then click **Users and Groups**.



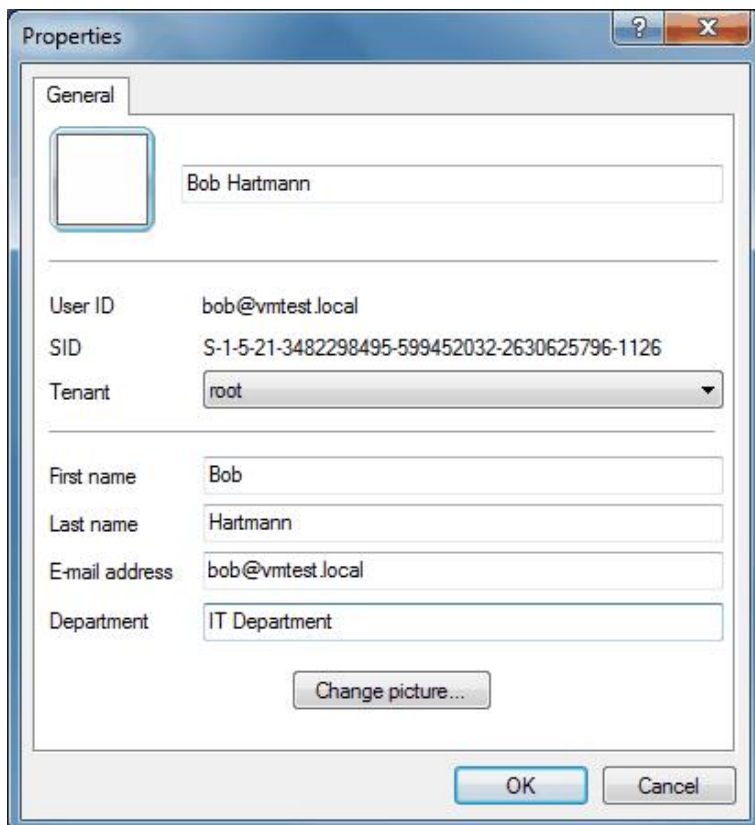
The details pane displays an overview of all user accounts that are stored in the DriveLock database.

By default, user accounts are arranged alphabetically by object name. To change the sort order, click the header of the column you want to sort by. To change between ascending and descending sorting, click the same column header again.

When administering user accounts, you cannot generate new certificates for users. Only a user can create his or her own certificate. However, you can import existing user certificates from another PKI and associate them with DriveLock File Protection users. The process for creating user certificates is described in the DriveLock User Manual.

To import an existing certificate for a user, perform the following procedure:

- In the navigation pane, right-click **User** or right-click an empty area in the details pane.
- In the context menu, point to **New** and then click one of the following:
 - *User from Active Directory*: Select this option to add a user that already has a user certificate stored in Active Directory. The standard Windows object picker dialog box appears, letting you select the Active Directory user.
 - *User from certificate*: If you have access to a user's certificate in a certificate file (*.cer), you can select this certificate file.
- When the certificate has been read from Active Directory or the file, the User account's *Properties* window opens.



- DriveLock File Protection automatically copies user information that is contained in the certificate. You can add any missing information, such as e-mail address or department.

- *Optional:* In multi-tenant environments with multiple DriveLock Enterprise Service servers you can specify the tenant that the user is associated with. To do this, select the appropriate tenant in the *Tenant* box. In all other environments, leave this setting unchanged.
- *Optional:* You can add a display picture to the user account. This picture will be displayed at various points when selecting a user. Displaying a picture can help select the correct user, especially when multiple users share the same name. To add a picture, click **Display picture**, select the appropriate image file and then click **Open**. If the file can be used as a display picture, the picture will be displayed in the top left corner of user account's *Properties* dialog box.
- Click **OK** to create the user account and save any modifications you made. The user account will be displayed in the details pane.

When a user creates or applies for a certificate, the corresponding user account is automatically created.

To view or modify a user account, double-click the account entry in the details pane.

- The *Centrally managed folders* tab displays all centrally managed folders that the user is authorized to access.
- The *Certificates* tab displays all certificates associated with the user that are stored in the DriveLock database.

To delete a user, right-click the user and then click **Delete user**.

For more information about centrally managed folders, refer to the section "[Centrally Managing Encrypted Folders](#)". For more information about managing certificates, refer to the section "[Managing Certificates](#)".

15.4.3 Managing Groups

DriveLock File Protection Groups are a set of DriveLock File Protection users. DriveLock groups can be assigned to centrally managed encrypted folders. Each time when DriveLock users are added or deleted from a DriveLock group, in the background the DriveLock Enterprise Server adds or removes the corresponding DriveLock users to/from all centrally managed folders, where the DriveLock group is assigned to.

This is a different behavior as for windows (AD) groups. While permissions of AD groups are assessed at access time, as groups cannot own certificates and cannot authenticate, DriveLock must assign the corresponding users to the folders. There might be a delay of approximately 15 minutes until this is done.

To create a new group, right click **Users and groups / New**.

You may either create a new DriveLock **Group** and then add the desired DriveLock users or you may import an existing **Group from Active Directory** (AD). If you import a group from the AD, the members from the AD group are added to the DriveLock group under the following conditions:

- the AD user already exists as DriveLock user => the user will just be added to the DriveLock group
- the AD user owns a valid certificate => a new DriveLock user will be created and then be added to the DriveLock group
- the AD user does not own a valid certificate => a notification will be shown and the user will not be added

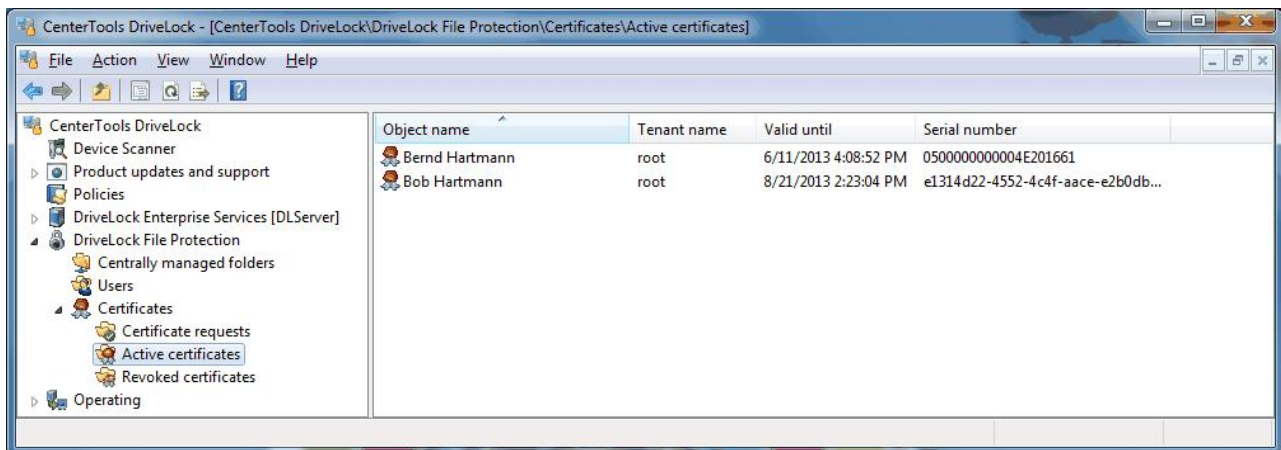
In the properties dialog of the new group on tab **General** enter or adapt the group name and select the right **Tenant**. On tab **Users** add or adapt users of the select tenant and check at least on user as **Group administrator**. Click **OK** to save the new group.

Once created, only the group administrators may add additional users and grant or revoke administrator permissions to users using the DriveLock Application. For more information see the DriveLock User Manual.

Open the properties dialog of a DriveLock group to get information about users who are members of the group and about the managed folders the group is assigned to. As DriveLock Administrator exceptionally you may remove users and managed folders from the group in case the group administrator is not available.

15.4.4 Managing Certificates

To manage certificates, in the DriveLock Management Console navigate to **DriveLock File Protection** and then click **Certificates**.



DriveLock File Protection uses three categories of certificates that are displayed separately:

- *Certificate requests*: This includes user requests for certificates or certificate renewals that an administrator has not yet approved or denied.

Approving certificates only needs to be performed if you configured the setting to require administrator approval in the DriveLock Enterprise Service. If administrator approval is not required, this list of certificate requests will always be empty. For more information about certificate approval, refer to the section [“Configuring certificate management”](#).

- *Active certificates*: This includes all certificates that are stored in the DriveLock database that have not been revoked. You can view certificates, export a certificate’s public information, delete and revoke a certificate.
- *Revoked certificates*: This list displays all certificates that have been revoked by an administrator. Certificate revocation marks a certificate as invalid, for example when a user leaves the organization or if a private key has been compromised. By retaining these certificates but marking them as revoked you can ensure that they can no longer be used to decrypt data, even if they are still within their validity period. You can view revoked certificates, export a revoked certificate’s public information and cancel a revocation marking the certificate as active again.

To administer a certificate, select on the certificate lists to view all certificates in a category. The details pane displays data about the certificates.

By default, certificates are arranged alphabetically by object name. To change the sort order, click the header of the column you want to sort by. To change between ascending and descending sorting, click the same column header again.

To manage certificate requests, perform the following procedure:

- In the navigation pane, click **Certificate requests**.

- Right-click the certificate request to manage.
- To approve the request and issue a certificate, click **All tasks -> Approve request**. The certificate is issued, the request is removed from the list and the certificate is added to the list of active certificates.
- To deny the request and not issue a certificate, click **All tasks -> Deny request**. The request is removed from the list and deleted.

To revoke an active certificate, perform the following procedure:

- In the navigation pane, click **Active certificates**.
- Right-click the certificate to revoke and then click **All tasks -> Revoke**
- Select the reason for the revocation from the list.
- *Optional:* In the *Comment* field, type a detailed description of the reason for revoking the certificate.
- Click **OK** to revoke the certificate. The certificate is moved to the *Revoked certificates* list.

To cancel a certificate revocation and re-activate the certificate, perform the following procedure:

- In the navigation pane, click **Revoked certificates**.
- Right-click the certificate to revoke and then click **All tasks -> Cancel revocation**
- Select the reason for the revocation from the list.
- Click **Yes** to re-activate the certificate. The certificate is moved to the *Active certificates* list. To stop the procedure and leave the certificate marked as revoked, instead click **No**.

To export a certificate, perform the following procedure:

- In the navigation pane, click **Active certificates** or **Revoked certificates**.
- Right-click the certificate to export and then click **Export certificate**
- Select the folder where the certificate will be stored and type the name of a file (*.cer) that will store the certificate and associated public key.

You can use a file that holds a certificate to authorize the certificate's owner to access an encrypted folder. This procedure is described in the *DriveLock User Manual*.

To delete a certificate, perform the following procedure:

- In the navigation pane, click **Active certificates**.
- Right-click the certificate to delete and then click **All tasks -> Delete certificate**
- Click **Yes** to delete the certificate. The certificate is deleted and removed from the list. To stop the procedure and keep the certificate, instead click **No**.

Deleting a user certificate does not delete the user from the DriveLock database. However, once a user's certificate has been deleted you can no longer authorize the user to access centrally managed encrypted folders. Any existing DriveLock File Protection permissions remain in place when a certificate is deleted as long as the certificate still exists in the user's certificate store. To revoke any previously granted permissions, revoke the certificate instead of deleting it.

15.5 Centrally Managing Encrypted Folders

To centrally manage encrypted folders you use the DriveLock Management Console. To manage such folders, navigate to **DriveLock File Protection -> Centrally managed folders**.

The details pane displays a list of all centrally managed folders from the DriveLock database and the status of each folder.

By default, certificates are arranged alphabetically by UNC path. To change the sort order, click the header of the column you want to sort by. To change between ascending and descending sorting, click the same column header again.

In the “*Centrally managed folders*” area you can create and delete encrypted folders and view or modify permissions for existing encrypted folders (provided that you have permissions as a folder administrator).

When creating a new centrally managed folder, consider the following points:

- Folders that already exist cannot be centrally managed and encrypted. The reason for this is that typically servers are not running the DriveLock File Protection service, which would need to encrypt any existing files. Also, possible conflicts during the encryption of existing data might not be correctly resolved (for example, if some files are already encrypted or if a large file is remotely accessed by a user at the same time it is being encrypted).

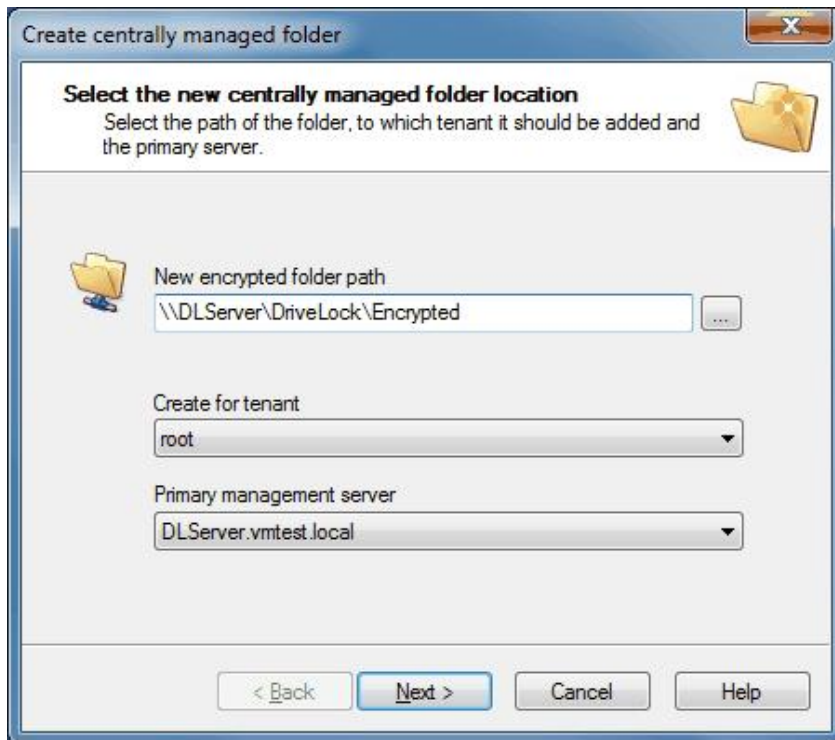
Users that are authorized for access when the folder is created are automatically given administrator permissions for this folder. Administrator permissions enable a user to grant permissions to additional users or to remove permissions. You can use this behavior delegate administration rights and responsibilities for a folder when it is created. For example, you can delegate administration of a departmental folder to a designated employee in that department.

15.5.1 Creating an Encrypted Folder

When creating a new encrypted folder you need Windows Write permissions for the parent folder.

To create a new encrypted folder, perform the following procedure:

- In the navigation pane, right-click **Centrally managed folders** or right-click an empty area in the details pane and then click **New -> Centrally managed folder**.



- Type or select the UNC path of the new encrypted folder.
- *Optional:* In multi-tenant environments with multiple DriveLock Enterprise Service servers you can specify the tenant that the encrypted folder belongs to. To do this, select the appropriate tenant in the *Tenant* box. In all other environments, leave this setting unchanged.
- Confirm that the UNC path is correct and then click **Next**.
- Select users who will be assigned administrative permissions for the folder. To search for a user, type at least three letters of the person's name in the search field. Only those users in the DriveLock database with names containing the text you typed will be displayed. Alternatively, click Search to manually search for a user.
- Click **Next**. The new folder is created and the permissions are assigned. You will be notified whether the procedure completed successfully.
- Click **Finish**.

15.5.2 Modifying Permissions

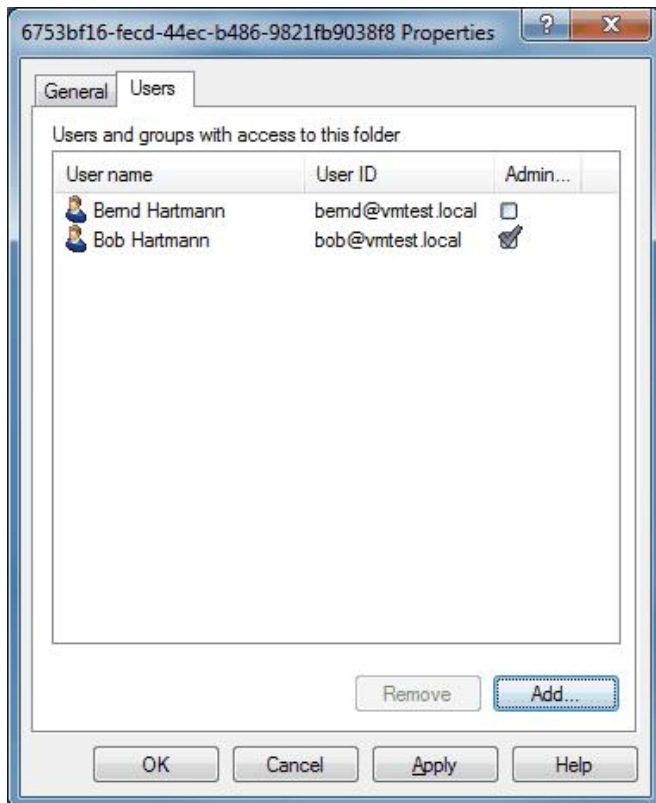
You can configure access permissions for encrypted folders from the DriveLock Management Console, the DriveLock user interface or the context menu in Windows Explorer. To change these permissions you need to have administrative permissions for the folder.

To change the access permissions as an administrator in Windows Explorer, right-click the encrypted folder and then click **Properties and users of encrypted folder**.

To change the access permissions as an administrator using the DriveLock Management Console, perform the following procedure:

- Navigate to **Centrally managed folders**.
- In the details pane, right-click the encrypted folder and then click **Manage folder** or double-click the folder, and then on the *Users* tab, click **Manage**.

- If a dialog box is displayed, prompting you to authenticate before you can view the folder's properties, click **Authenticate** and select the certificate that is required to access the folder.
- Select the *Users* tab.



- To add a user, click **Add**. To remove a user, click **Delete**.
- To add a user from Active Directory, perform the following procedure:
 - Select the option *Windows user (with certificate)*.
 - To select the user, click “...” and then select the user from Active Directory.
 - Click **Finish**. The user is added as a regular user without administrative permissions.
- To add a user from the DriveLock database, perform the following procedure:
 - Select the option *DriveLock File Protection user (with certificate)*.
 - Click **Next**.
 - Select one or more users from the DriveLock database..
 - Click **Finish**. The user is added as a regular user without administrative permissions.
- Click **OK** to close the dialog box.

15.6 Recovering Encrypted Folders

Recovery may become necessary when a user has lost access to encrypted drives or folders because of forgetting a password or losing access to a certificate's private key. Administrators or helpdesk personnel can perform an offline recovery operation in conjunction with the user that uses a challenge/response mechanism to restore access. The challenge/response mechanism validates both the challenge (request code) that DriveLock creates for the user and the corresponding response code that is generated by the person performing the recovery. Only when both codes

are valid for the drive or folder to be recovered, can access to the data be restored (for example enabling the user to select a new encryption password). The user generates the challenge code using a wizard and provides this code to an administrator. The administrator checks that the request code is valid and then generates a response code that is in turn validated by the wizard running on the client computer.

The procedure a user must complete to initiate recovery are described in the *DriveLock User Manual*.

The procedure an administrator or helpdesk employee must perform to complete recovery is identical as for drives/containers and described in [Recovering Encrypted Drives and Folders](#).

15.7 Reporting and Analysis

You can generate reports and statistics by using the *DriveLock Control Center*. For more information about these tasks, refer to the *DriveLock Control Center Manual*.



Part XVI

Defender Management



16 Defender Management

You can find the description of the DriveLock Defender Management module in a separate documentation on [DriveLock Online Help](#).



Part XVII

Security Awareness



17 Security Awareness

You can use security awareness to create campaigns that alert employees to specific security risks, for example when they want to connect their smartphone to their computer. You can also create complete training units that staff members have to complete and confirm at certain intervals. In addition, the feature also provides and evaluates feedback on completed or canceled training sessions.

This DriveLock feature is described in a separate DriveLock SecurityEducation manual.

This section only provides information on configuring usage policies.

17.1 Usage Policies

Usage policies inform users of safety-related procedures or corporate policies before they actually access a drive or device.

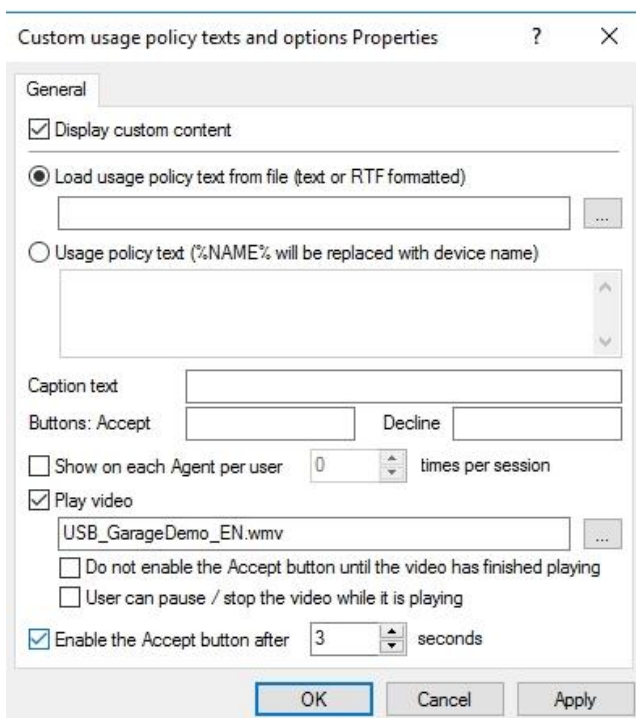
Up to version 7.7, usage policies could be configured within the drive control settings. Since version 7.8, usage policies are part of security awareness settings and can be configured there.

You can configure DriveLock so that an external drive or device can only be accessed after the user has confirmed reading the usage policy by clicking on the "Accept" button.

Creating a usage policy

Select the **Security awareness** node and then **Settings; -> Einstellungen** then, select **Custom usage policy texts and options**.

You can define a heading, the texts for the two buttons and also the text for the usage policy.



You can enter the message text either directly in the input field or select an RTF file from your local hard disk or from the policy file storage. A file from the policy file storage is marked with a „*“.

When you select a file, make sure it is in the specified path on the local hard disk of the client computer and can be accessed from there. You can distribute this file together with the DriveLock configuration via the policy file storage.

A special option within the usage policy is to play an AVI video, which can also be configured in this dialog. You can define the options the user has while watching the video.

Specify how many times per session the video will be shown with the **Show on each Agent per user x times per session** option.

You can also specify when and how long it takes until the user sees the Accept button.

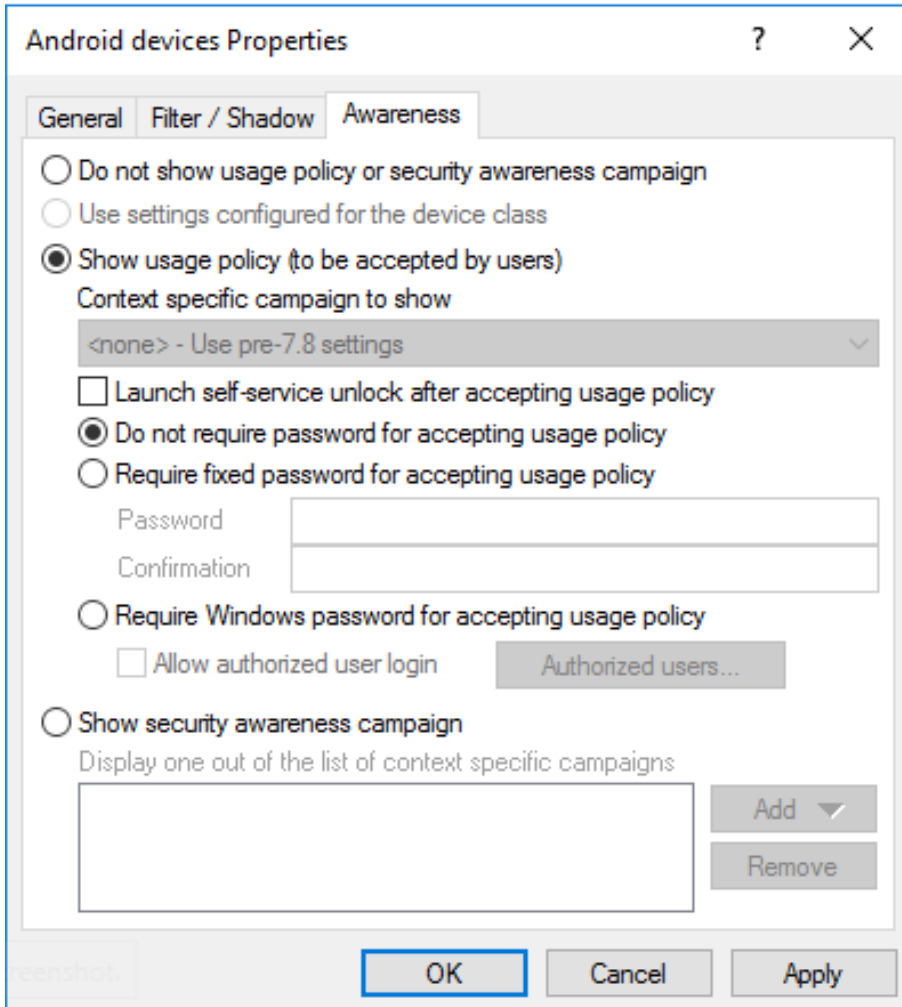
Enable the usage policy

Here you can create a usage policy which is valid globally for the complete policy. You can then activate it like a security awareness campaign from within a drive or device rule:

USB bus connected drives Properties

Encryption Options Drive letters Commands
General Filter / Shadow Awareness Messages

Do not show usage policy or security awareness campaign
 Use settings configured under "Removable drive locking"
 Show usage policy (to be accepted by users)
Context specific campaign to show
<none> - Use pre-7.8 settings
 Launch self-service unlock after accepting usage policy
 Do not require password for accepting usage policy
 Require fixed password for accepting usage policy
Password
Confirmation
 Require Windows password for accepting usage policy
 Allow authorized user login Authorized users...
 Show security awareness campaign
Display one out of the list of context specific campaigns
Add Remove
OK Cancel Apply



Select the **Show usage policy (to be accepted by users)** option on the **Awareness** tab.

The following options are available:

- **Launch self-service unlock...:** After the user confirms the usage policy, the self-service unlock wizard starts automatically.
- **Fixed password:** Specify a password the user must enter before unlocking.
- **Windows password:** In this case, the logged on user must enter their Windows password to confirm.
- **Windows password and other user:** This option allows a user other than the logged in user to unlock by entering their user name and password. Optionally you can specify authorized users by clicking the **Authorized users...** button.



Part XVIII

Inventory and Vulnerability Scan



18 Inventory and Vulnerability Scan

This chapter remains in the Administration Guide until further notice, but will not be updated. Please note that starting with version 2020.1, the latest documentation on inventory and client compliance can be found in the Vulnerability Scan manual at [DriveLock Online Help](#).

18.1 Settings

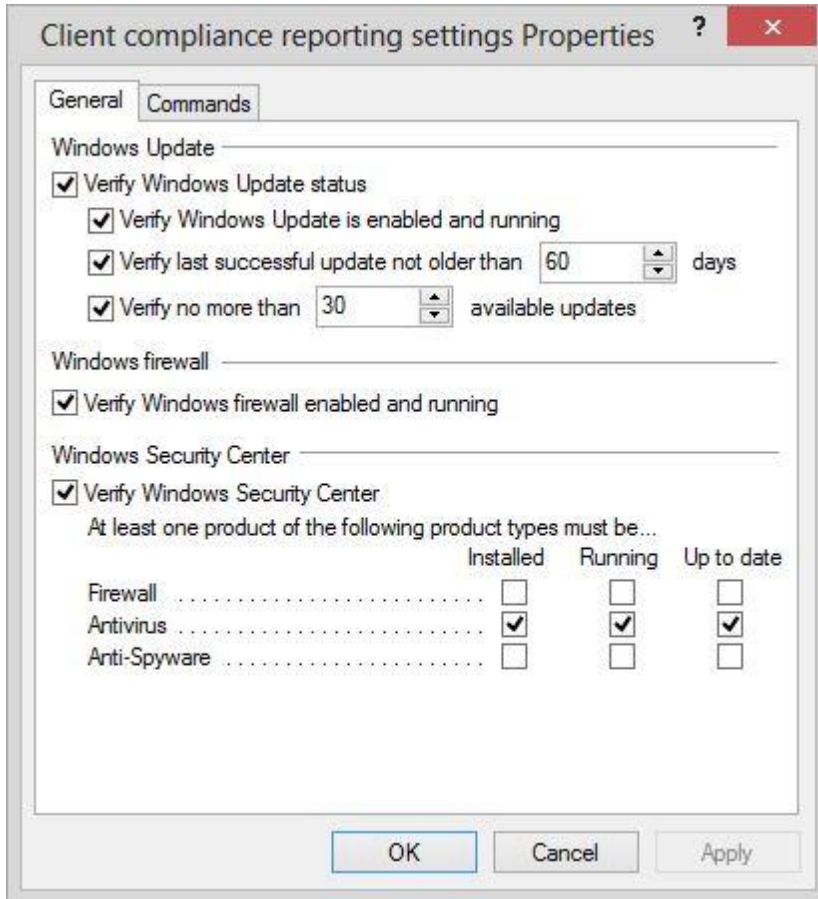
This chapter remains in the Administration Guide until further notice, but will not be updated. The Systems Management / Settings node has been moved to a different location in the DriveLock Management Console and is now called Inventory and Vulnerability Scan. Please note that starting with version 2020.1, the latest documentation on inventory and client compliance can be found in the Vulnerability Scan manual at [DriveLock Online Help](#).

18.1.1 Client Compliance

This chapter remains in the Administration Guide until further notice, but will not be updated. The Systems Management / Settings node has been moved to a different location in the DriveLock Management Console and is now called Inventory and Vulnerability Scan. Please note that starting with version 2020.1, the latest documentation on inventory and client compliance can be found in the Vulnerability Scan manual at [DriveLock Online Help](#).

This option allows you to configure, which parameters should be checked on each PC for compliance state.

If the common parameters does not fit, use Tab **Commands** to configure optional commands (executable or script). Best, you add this commands to the [policy file storage](#) before and select them from there. The commands will be executed from the Agent on any PC and must return **1** for compliant and **0** for non compliant.



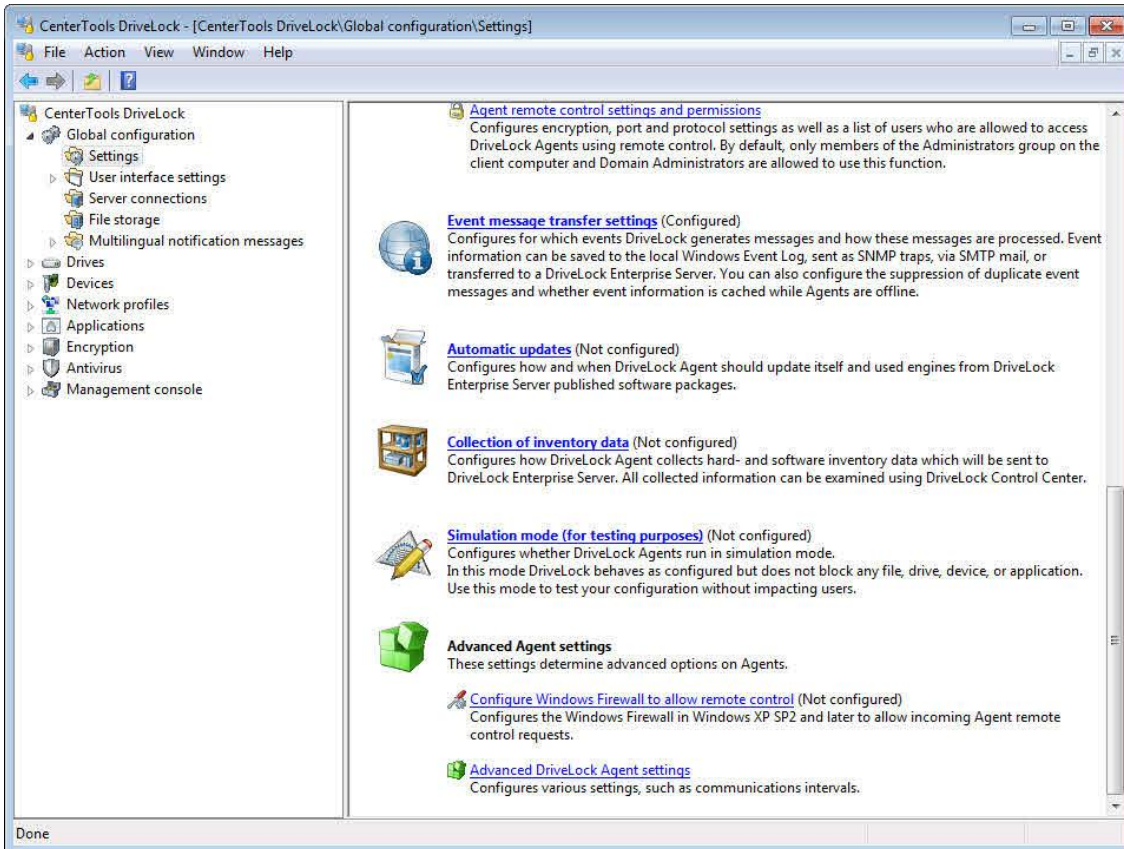
The DriveLock Control Center (*DCC / Helpdesk*) displays the compliance state of any PC in detail.

18.1.2 Configuring Hardware and Software Inventory

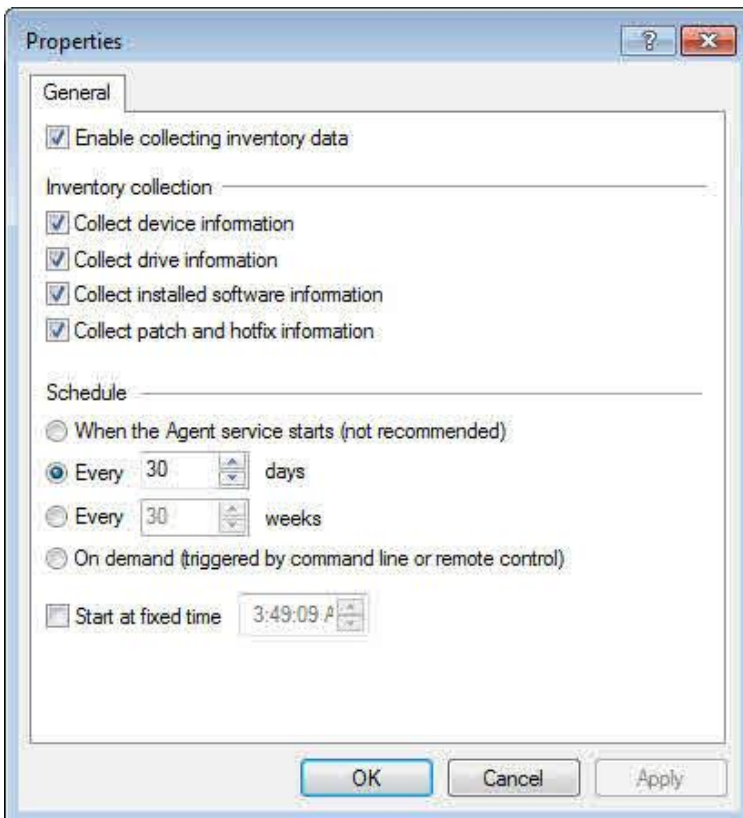
This chapter remains in the Administration Guide until further notice, but will not be updated. The Systems Management / Settings node has been moved to a different location in the DriveLock Management Console and is now called Inventory and Vulnerability Scan. Please note that starting with version 2020.1, the latest documentation on inventory and client compliance can be found in the Vulnerability Scan manual at [DriveLock Online Help](#).

The DriveLock Agent can scan the computer at regular intervals for currently connected hardware and installed software and send this data to the DriveLock Enterprise Service. You can use this information to create reports that show which software and patches are installed on computers in your organization.

The global settings for inventory collection determine whether the DriveLock Agent collects inventory data, which data to collect and when.



In the console tree, click Global configuration and then click **Settings**. In the task pane, click **Collection of inventory data**.



To enable the collection of inventory data, select the *Enable collecting inventory data* checkbox. Then select the appropriate checkboxes to configure the types of inventory data the client will collect. Finally, configure the time interval and starting time for the inventory data collection.

Collecting inventory data uses system resources. If you configure the Agent to scan each time the service starts, inventory collection may be delayed by a few minutes to prevent a slow startup experience for users.



Part XIX

Operating System Management



19 Operating System Management

In this section you can configure settings for operating and system management of DriveLock Agents.

If you do not have a Native Security license, the only option available in this node is the Power management option. The settings are based on Microsoft's Power Options and can be individually distributed to your agents via your policy.

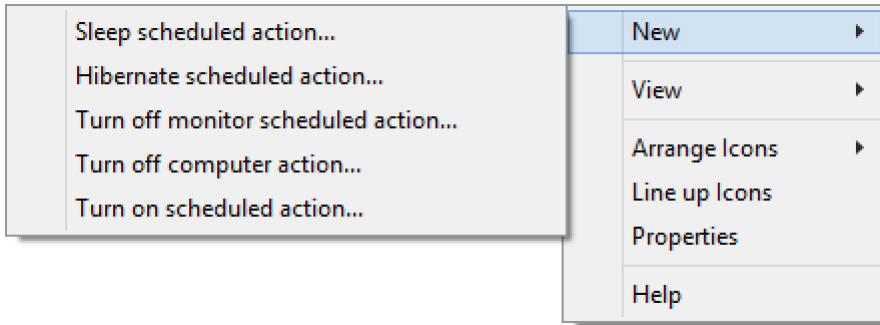


With the Native Security license, you can also manage local users and groups, and create rules to manage the firewall, in addition to the power management options. In this case, two additional nodes appear in your Management Console.



19.1 Power Management

In a DriveLock Policy you may schedule actions when to sleep, pause, power off or on the computer or schedule, when to use which windows power plan. Open **Systems management / Power management / ... / New** and select the appropriate action or plan.



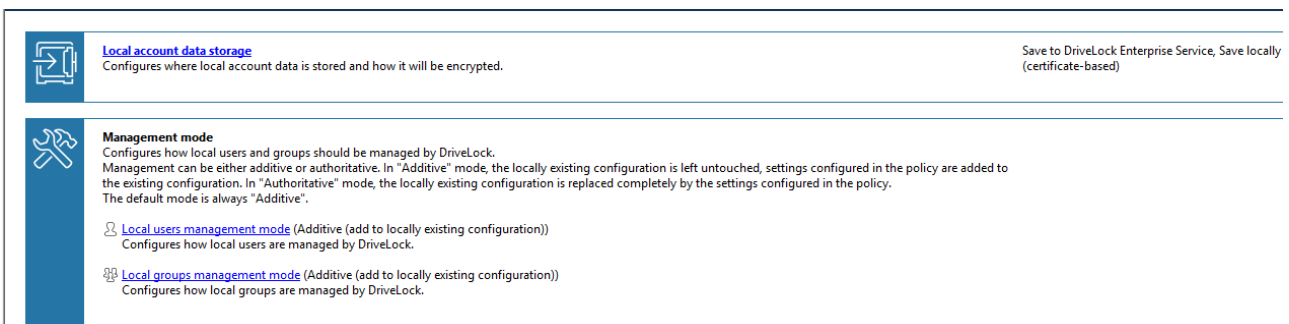
19.2 Local Users and Groups

This DriveLock functionality allows you to restrict important access rights for specific users and groups, making it easier to implement your zero-trust strategy.

For example, certain users can be added to the Local Administrators group, thus having different local administrators for a given group of computers. You then specify which user gets local admin rights on which systems.

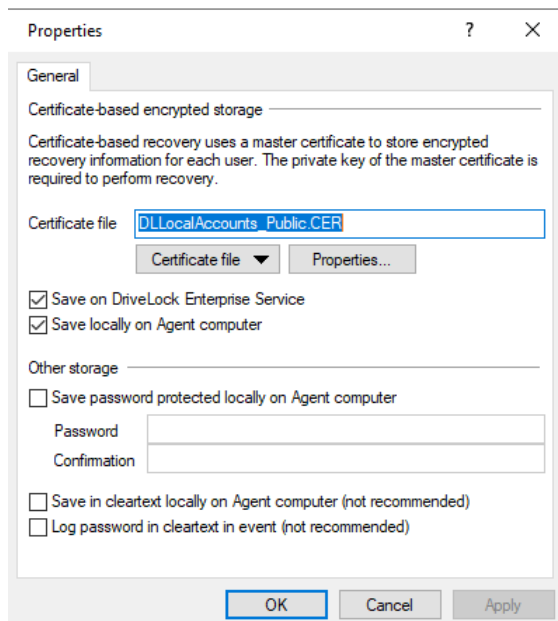
19.2.1 Settings

You can use the following settings:



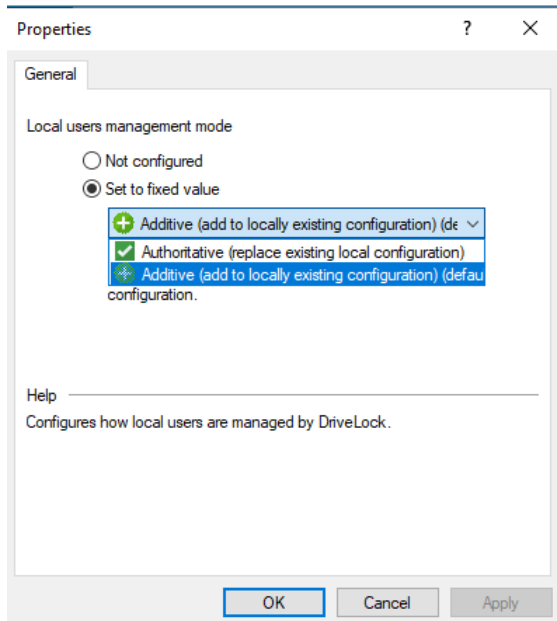
1. Local account data storage

This setting allows you to specify where user names and passwords are stored: Locally based on certificates or on the DES.



2. Settings for the management mode

- Local users management mode



- Local groups management mode

You can define how DriveLock manages users and groups via the **user and group management mode**.

In **additive** mode (default), the existing local users are not changed, except for the users defined in the policy. For example, if a user exists in the policy, this user will be added in addition to all other local users.

In **authoritative** mode, the existing local users/groups are all deleted and only the users or groups defined in the policy are created.

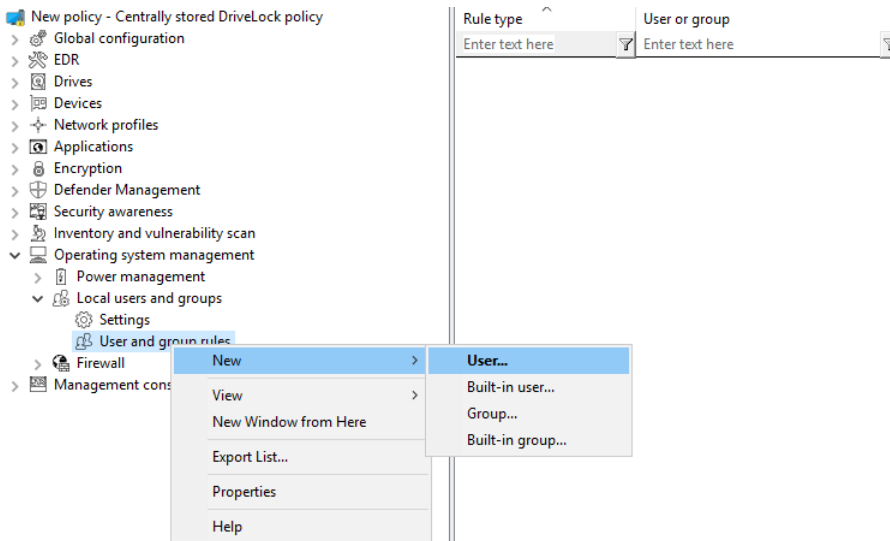
19.2.2 User and group rules

Implement user and group rules for managing local users and groups. Depending on the management mode, you can add users and groups defined in DriveLock to the local user database, or they can completely replace the users and groups in the local user database.

User rules

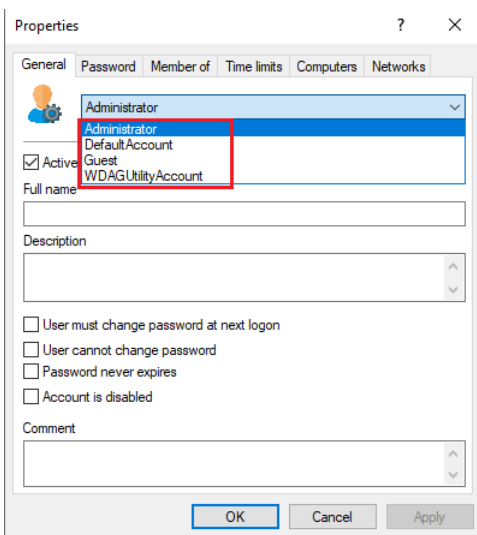
You need to create a rule for each user.

Proceed as shown in the figure:

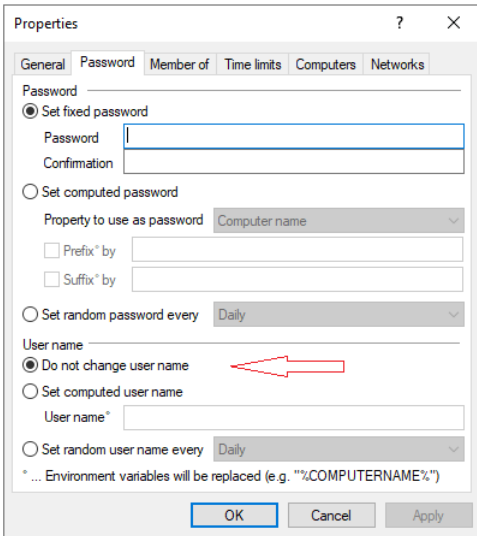


The difference between built-in and custom accounts is the username.

The built-in accounts are the four accounts that are created during Windows installation (most importantly, the "Administrator" account). These cannot be deleted, but can usually be renamed.



On the **Password** tab, you specify whether to use a fixed, a calculated, or a random password for the account. Also, for built-in users, you can specify whether to change the fixed user name:



Group rules

Here, too, the built-in groups are the predefined Windows groups. The membership is defined in the rules. You can add other users or AD users/groups (using the **Include** button) or remove them from the group (using the **Exclude** button). So, for example, if you want to remove a certain AD group from the Administrators group, create a rule for the built-in group and add an Exclude to the rule.



19.3 Firewall

These options can be used to manage the firewall settings of Windows clients. This allows you to configure rules for a specific group of computers smoothly.

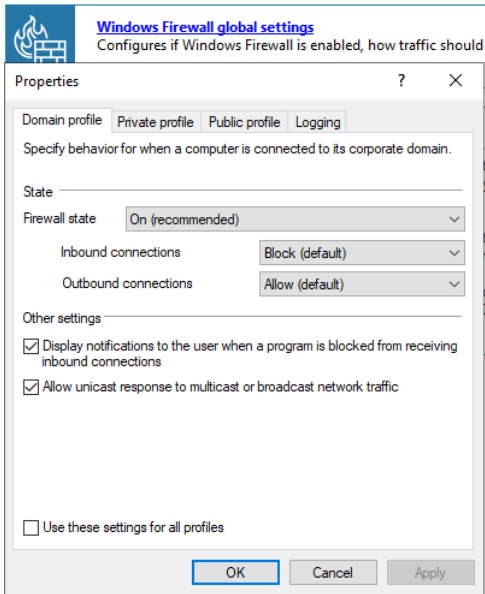
DriveLock can extend the built-in functionality of Defender Firewall by dynamically adding and removing rules based on conditional settings.

19.3.1 Settings

You can use the following settings:

	<p>Windows Firewall global settings Configures if Windows Firewall is enabled, how traffic should be handled by default and if connections should be logged.</p>	<p>Domain profile: On (recommended); Private profile: On (recommended); Public profile: On (recommended)</p>
	<p>Management mode Configures how Firewall rules should be managed by DriveLock. Management can be either additive or authoritative. In "Additive" mode, the locally existing configuration is left untouched, settings configured in the policy are added to the existing configuration. In "Authoritative" mode, the locally existing configuration is replaced completely by the settings configured in the policy. The default mode is always "Additive".</p> <ul style="list-style-type: none"> ↳ Inbound rules management mode (Not configured (Additive (add to locally existing configuration))) Configures how inbound firewall rules are managed by DriveLock. ↳ Outbound rules management mode (Not configured (Additive (add to locally existing configuration))) Configures how outbound firewall rules are managed by DriveLock. 	

The following options are available in the Windows Firewall global settings and can be used to achieve the following goals:



Blocking or allowing communication depending on

- a period of time
- computers and computer groups
- the logged in user and user groups
- the currently existing network connection

Two modes are available: additive / authoritative

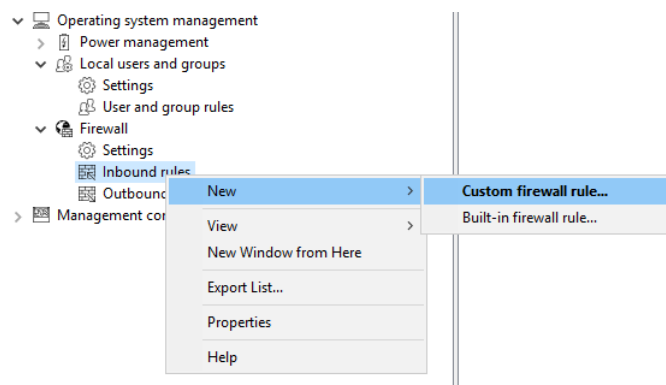
Configuration of specific settings for the Domain, Private, Public profiles

Logging of network connections to be analyzed later

19.3.2 Inbound and outbound rules

In this section, you can create custom or built-in firewall rules and manage them with DriveLock.

Proceed as shown in the figure:





Part XX

Using Agent Remote Control



20 Using Agent Remote Control

You can use the DriveLock Management Console to connect to a remote computer with the DriveLock Agent running. Available options for remote control include temporarily enabling a category of drives on a remote computer or to updating the DriveLock configuration by forcing the Agent to update its Group Policy or configuration file settings. When used in conjunction with the DriveLock Enterprise Service (DES), you can also control the Agent status. Agent Remote Control lets you display inventory data or manually start a hardware and software inventory collection.

Agent remote control requires the DriveLock Management Console and is not available for the Group Policy Object Editor you use to configure GPO-based policies. However, you can use the DriveLock Management Console to connect to DriveLock Agents that are configured via a Group Policy.

DriveLock uses the HTTP(S) protocol to connect to remote computers. To establish a connection to a remote computer, DriveLock must be installed and running on the client computer. To establish a connection to a computer with the Windows Firewall enabled, you must allow incoming connections from TCP Port 6064 (default) or 6065 (for SSL connections) and the program "DriveLock" in the firewall settings.

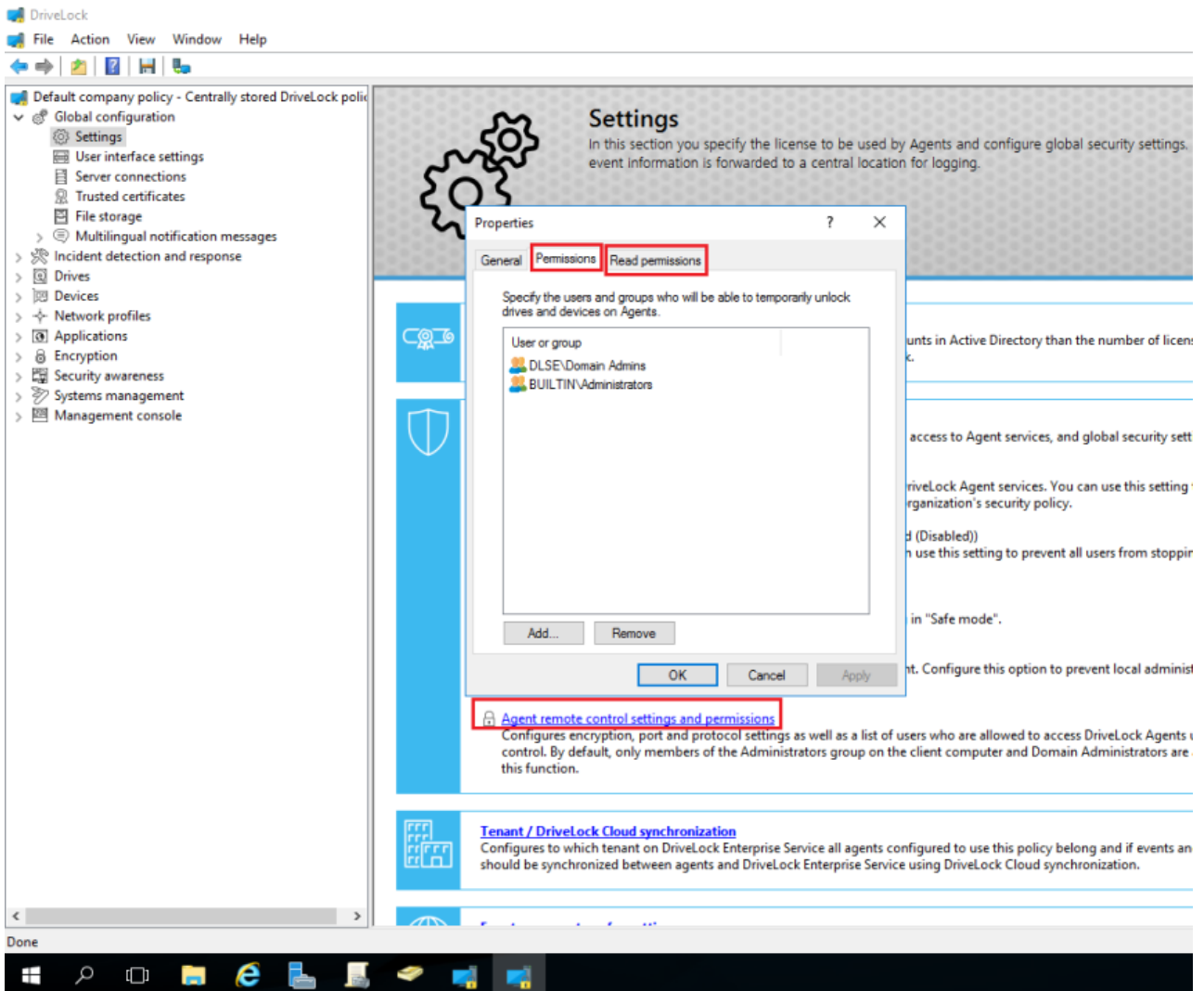
By default, the DriveLock Management Console uses Quick Configuration using DNSD-SD to discover all and display all DriveLock Agents in the same network. As an alternative, you can configure the DriveLock Management Console to get the list of all DriveLock Agents from the DriveLock Enterprise Service (DES).

20.1 Policy Settings for Agent Remote Control

To perform remote control actions on DriveLock Agents, you must define the required permissions.

In the **Agent remote control settings and permissions** section of a policy (**Global configuration - Settings**) you can specify the different permissions for users (see figure below) who can remote-control a DriveLock Agent. Also, you can specify additional communication and certificate settings.

- On the **Read permissions** tab you add users or groups who may only request (read) information from DriveLock Agents during remote actions.
- On the **Permissions** tab you add the users or groups that are explicitly allowed to perform actions on the Agent, such as temporarily unlocking an Agent or modifying the configuration.

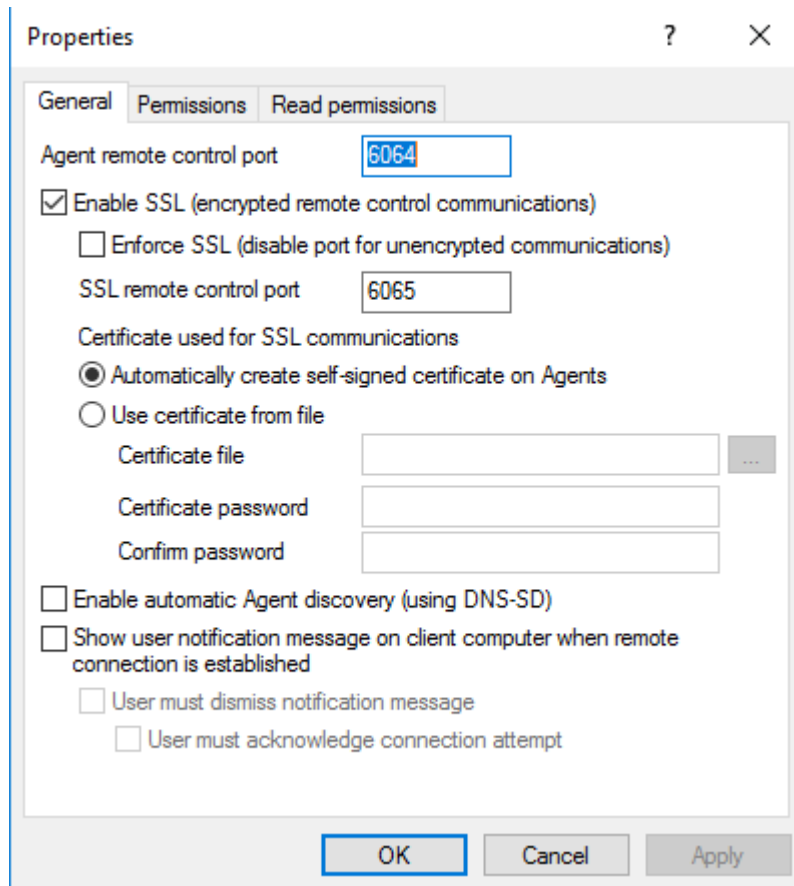


- On the **General** tab you configure all Agent settings for accepting and authenticating remote control sessions from the DriveLock Management Console (see figure below).

The default ports used for remote control are TCP port 6064 for unencrypted communications and port 6065 for encrypted communications. To use different ports, change one or both port numbers. To enable the Agent to accept encrypted remote control connections, select the **Enable SSL (...)** checkbox. Select the **Enforce SSL (...)** checkbox to prevent the Agent from accepting unencrypted remote control connections.

By default DriveLock creates and uses a self-signed certificate for SSL communications. To use a different SSL certificate instead, click **Use certificate from file**, and then click ... to select a certificate file. If the certificate's private key is protected using a password, you must also type and confirm this password.

To display a user notification message on a client computer when an administrator connects to the DriveLock Agent, select the **Show user notification messages...** checkbox.

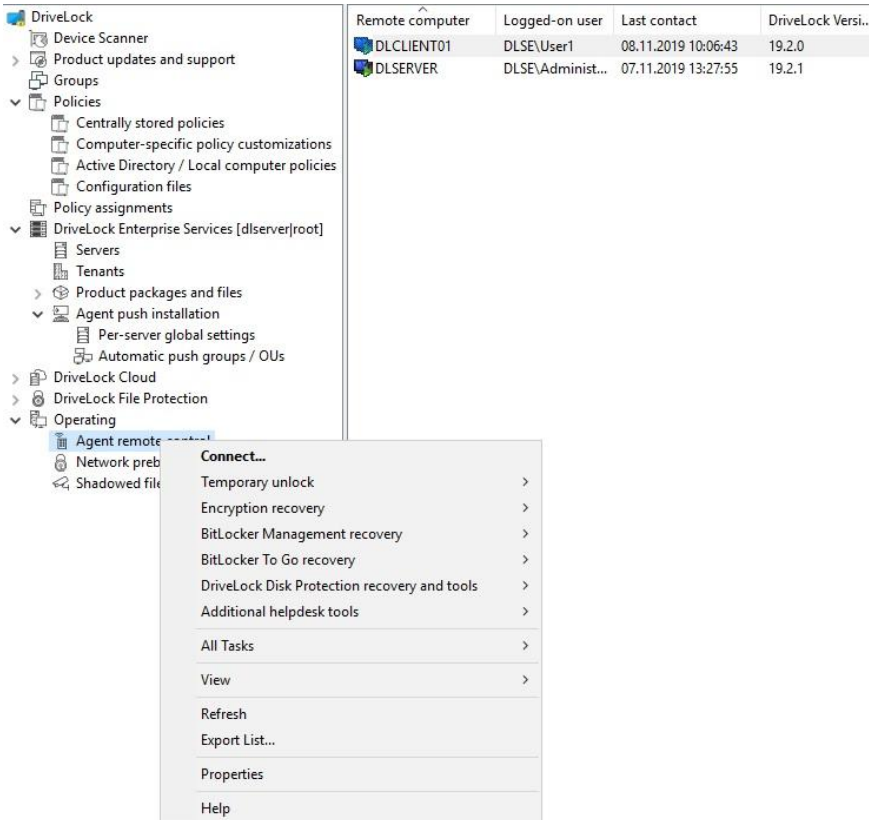


20.2 Performing Agent Tasks

You can use the DriveLock Management Console to perform a number of maintenance tasks on DriveLock Agents. You can use the Helpdesk view of the DriveLock Control Center instead of the DriveLock Management Console to perform the same tasks. The remote control procedures and dialog boxes in the DriveLock Control Center are identical to the ones described here.

20.2.1 Viewing Agents

By default, the DriveLock Management Console displays all Agents it discovers in the network under *Operating* -> *Agent remote control*. The discovery is an automatic process using DNS-SD and requires no configuration.

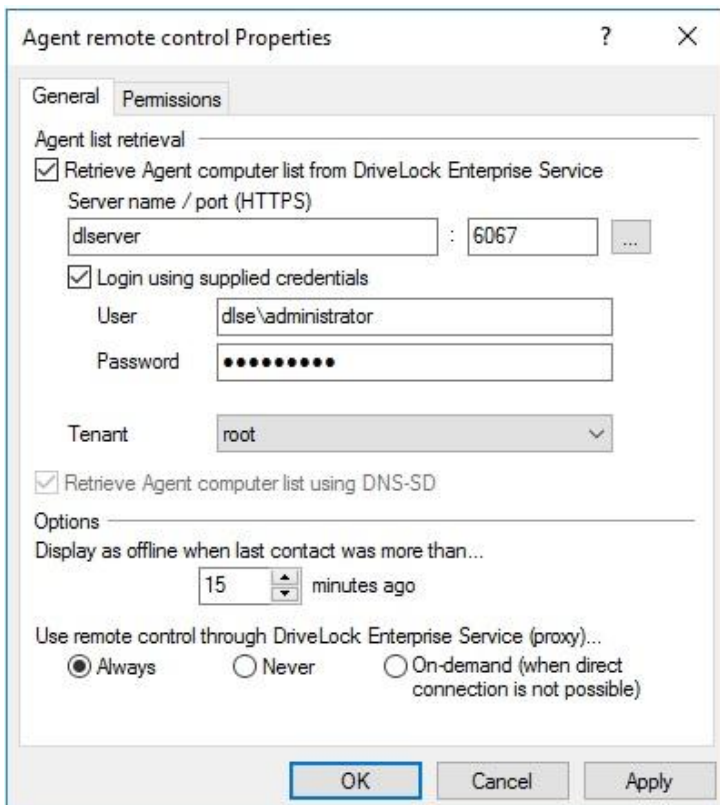


The screenshot shows the DriveLock Management Console interface. On the left is a tree view with 'Operating' expanded to 'Agent remote control'. A context menu is open over 'Agent remote control', listing various actions like 'Connect...', 'Temporary unlock', 'Encryption recovery', etc. On the right, a table displays the list of agents:

Remote computer	Logged-on user	Last contact	DriveLock Versi...
DLCLIENT01	DLSE\User1	08.11.2019 10:06:43	19.2.0
DLSERVER	DLSE\Administ...	07.11.2019 13:27:55	19.2.1

In network environments where the use of DNS-SD is not desired or in routed networks that consist of several segments you can configure the DriveLock Management Console to download a list of all Agents.

To configure how the list of Agents is obtained, in the console tree, right-click *Operating* -> *Agent remote control* and then click **Properties**.



The screenshot shows the 'Agent remote control Properties' dialog box. The 'Permissions' tab is selected. The 'Agent list retrieval' section contains the following settings:

- Retrieve Agent computer list from DriveLock Enterprise Service
 - Server name / port (HTTPS): dlserver : 6067
 - Login using supplied credentials
 - User: dlse\administrator
 - Password: [masked]
 - Tenant: root
- Retrieve Agent computer list using DNS-SD

The 'Options' section includes:

- Display as offline when last contact was more than...: 15 minutes ago
- Use remote control through DriveLock Enterprise Service (proxy)...:
 - Always
 - Never
 - On-demand (when direct connection is not possible)

Buttons at the bottom: OK, Cancel, Apply.

In the *Agent remote control Properties* dialog box, configure the following settings:

- *Retrieve Agent computer list from DriveLock Enterprise Service*: Select this checkbox to have the Console retrieve the Agent list from a DES server and then select the server connection to use for this process. The list may include Agents that are currently offline.
- *Retrieve Agent computer list using DNS-SD*: Use Quick Configuration announcements to build the list of Agents. Only Agents that are online are displayed.

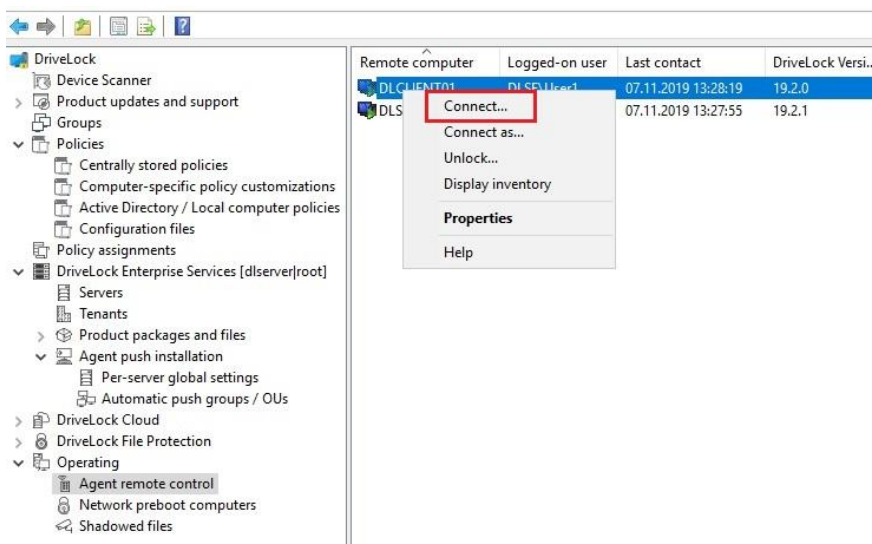
Permissions: On the *Permissions* tab, configure access to the *Remote control* node in the When viewing the Agent status in the Management Console, agents that are offline are identified by an icon containing red square.

In environments where the DriveLock Management Console is run on a computer that is not in the same network as the Agent, the DriveLock Enterprise Service can proxy this connection. For example, this can be used by a Security-As-A-Service provider to connect to an Agent in a customer's network. Change the setting *Use remote control through DriveLock Enterprise Service (proxy)* to configure how the DriveLock Management Console connects to the client for remote control:

- *Always*: The connection is always established via the DriveLock Enterprise Service.
- *Never*: The DriveLock Management Console always connects directly to the Agent without going through the DriveLock Enterprise Service.
- *On-demand*: The DriveLock Management Console attempts to connect directly to the Agent. If the connection attempt fails, a connection via the DriveLock Enterprise Service is attempted.

20.2.2 Connecting to a DriveLock Agent

Before you can connect to an Agent to perform any tasks on it, you need to connect to the Agent. To do this, right-click an Agent that is displayed in the DriveLock Management Console and then click **Connect**.



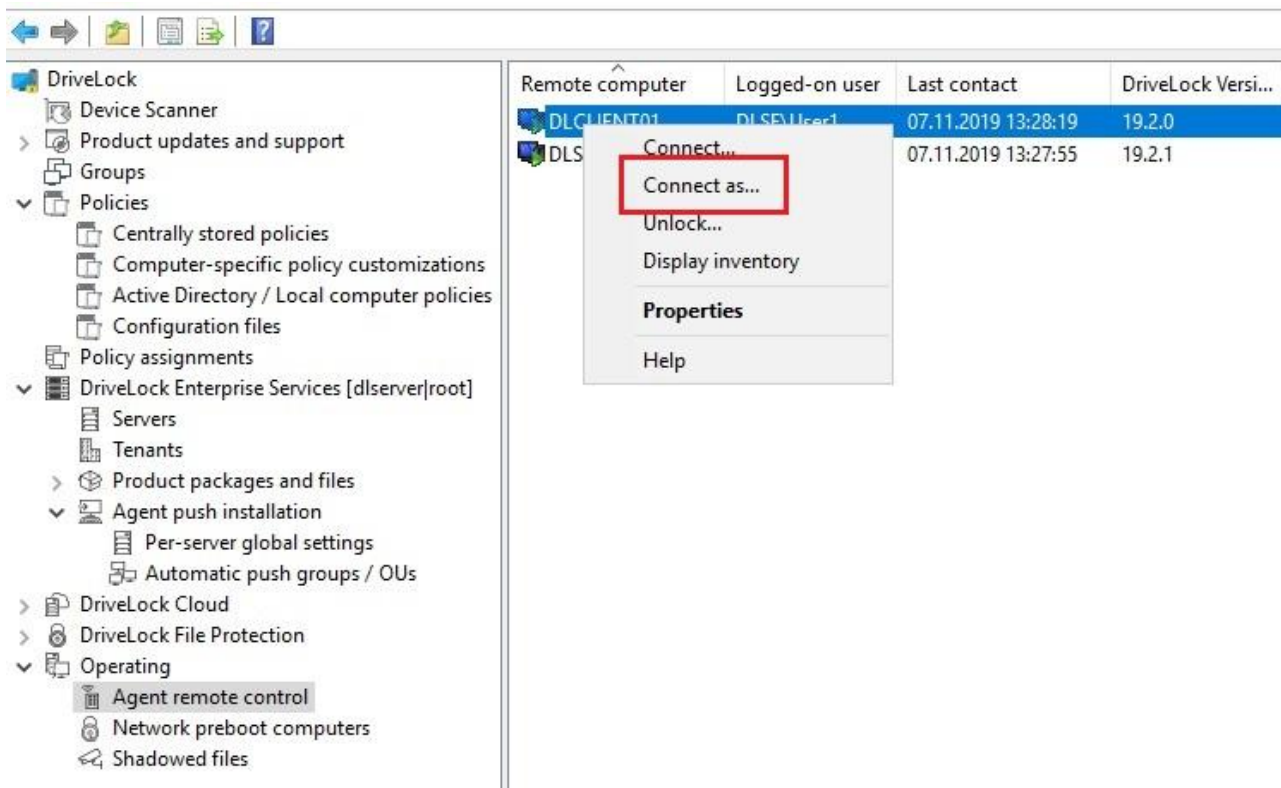
If the Agent is not currently displayed, right click **Agent remote control** and then click **Connect**. Type the name or IP address of the remote computer.

To establish a connection to a computer with the Windows Firewall enabled, you must allow incoming connections from TCP Ports 6064 and 6065 (default) and the program "DriveLock" in the firewall settings.

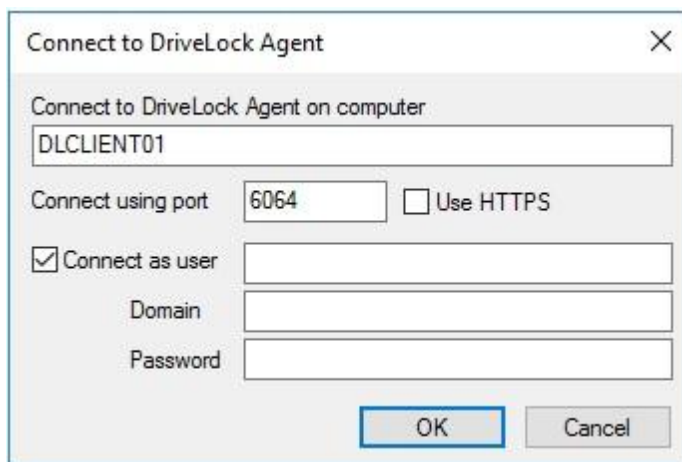
After the connection has been established, you can view the current configuration and control the DriveLock Agent.

20.2.2.1 Connect as

To use a different port for communication between the DriveLock Agent and the DES, select **Connect as** from the DriveLock Agent context menu.

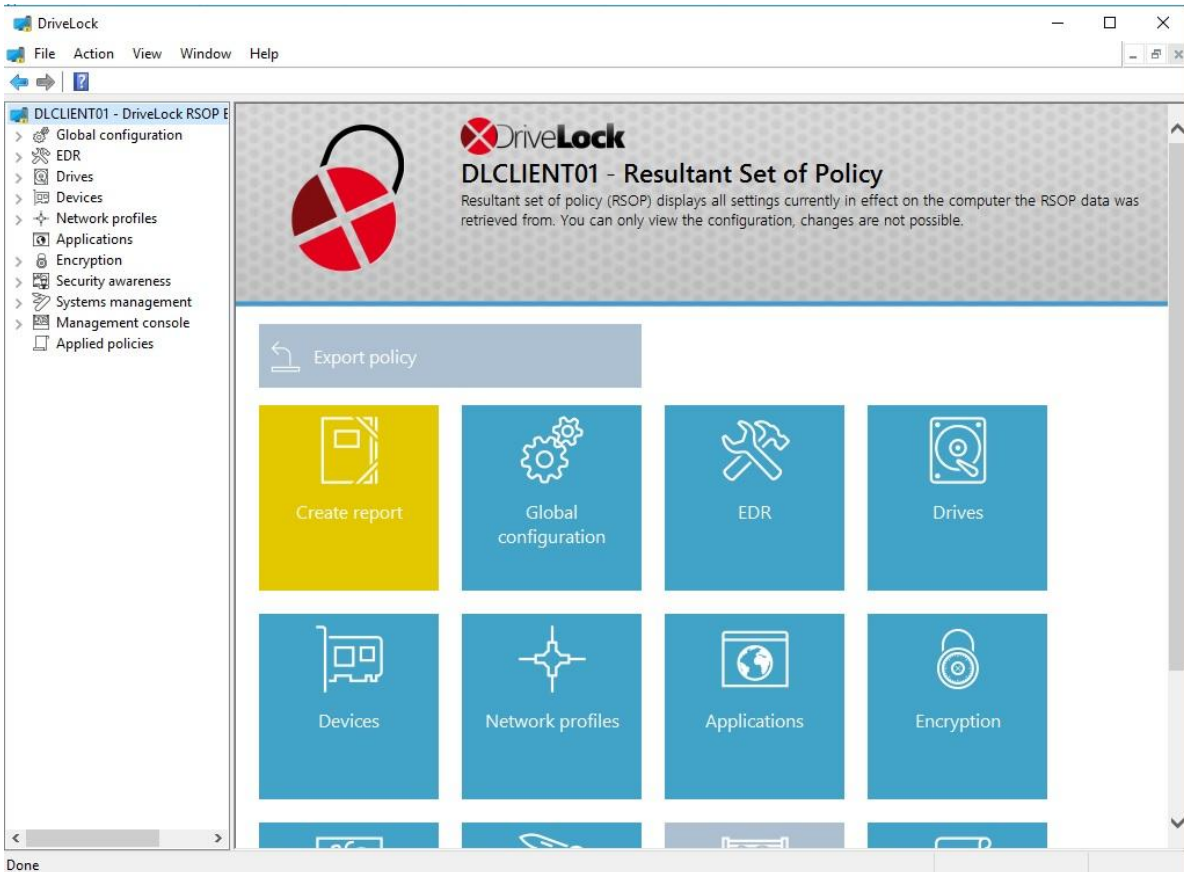


To encrypt communications with the Agent, select the **Use HTTPS** checkbox. To connect using a different user account, type the credentials for the account. Click **OK** to connect.

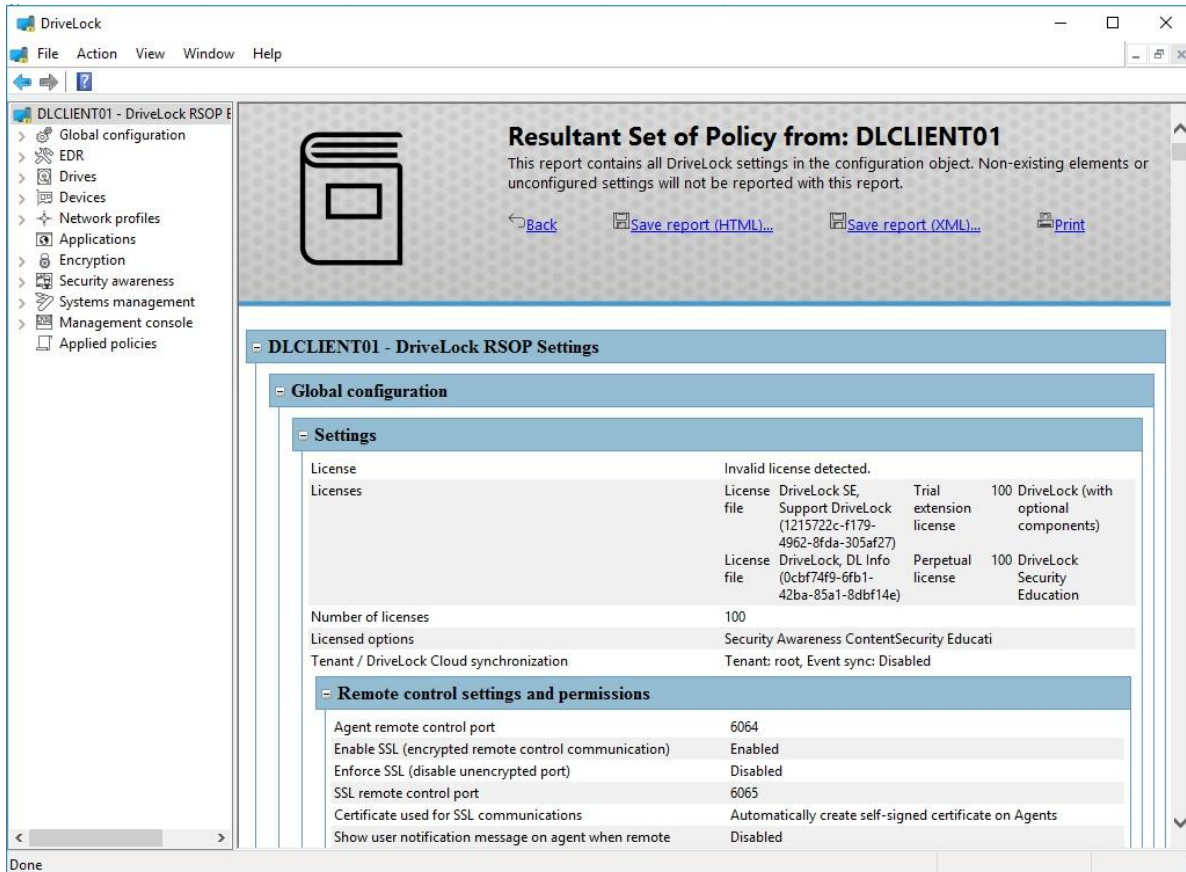


20.2.3 Viewing the Agent Configuration (RSOP)

To display the current configuration (RSOP, or Resultant Set of Policy) on a client computer, right click the computer and then click **Show RSOP**.



A new window opens that is similar to the DriveLock Management Console. To view details of the current settings that are enforced by the Agent, expand the relevant node and select the configuration settings. All settings are read-only and cannot be changed.



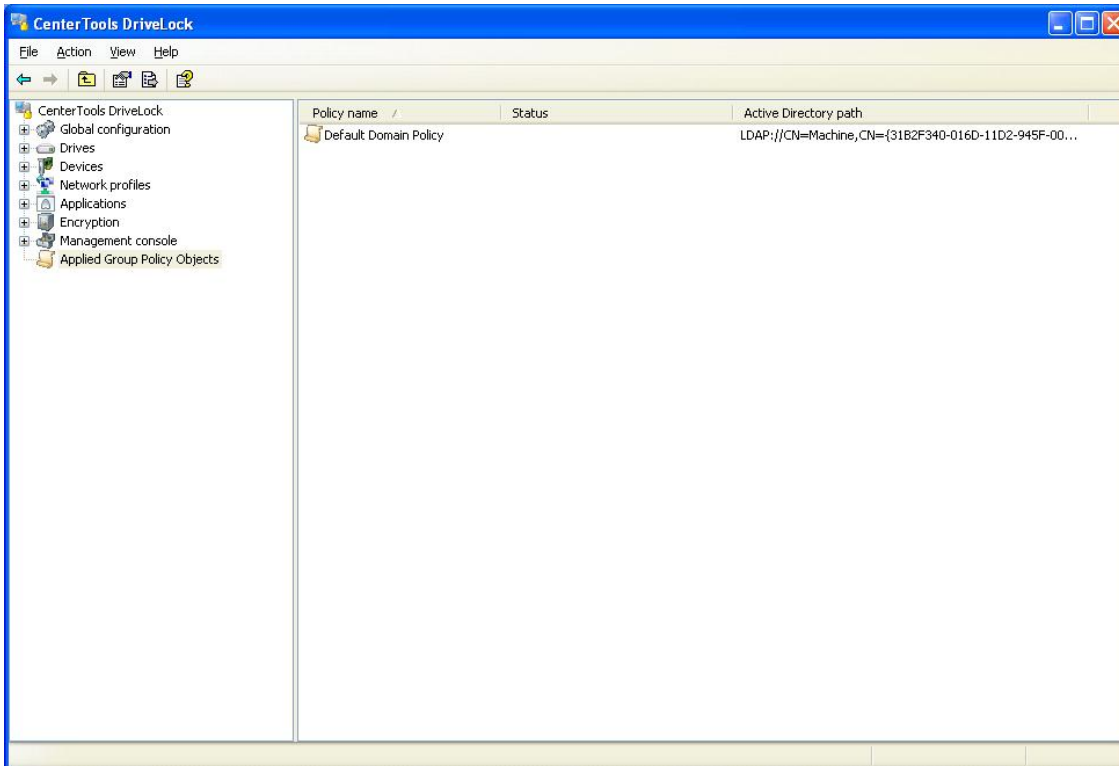
The screenshot shows the DriveLock application window with a menu bar (File, Action, View, Window, Help) and a toolbar. The main content area displays a report titled "Resultant Set of Policy from: DLCLIENT01". Below the title, there are options to "Back", "Save report (HTML)...", "Save report (XML)...", and "Print". The report is organized into sections: "DLCLIENT01 - DriveLock RSOP Settings", "Global configuration", "Settings", and "Remote control settings and permissions".

DLCLIENT01 - DriveLock RSOP Settings			
Global configuration			
Settings			
License	Invalid license detected.		
Licenses	License file	DriveLock SE, Support DriveLock (1215722c-f179-4962-8fda-305af27)	Trial extension license 100 DriveLock (with optional components)
	License file	DriveLock, DL Info (0cbf74f9-6fb1-42ba-85a1-8dbf14e)	Perpetual license 100 DriveLock Security Education
Number of licenses	100		
Licensed options	Security Awareness ContentSecurity Educati		
Tenant / DriveLock Cloud synchronization	Tenant: root, Event sync: Disabled		
Remote control settings and permissions			
Agent remote control port	6064		
Enable SSL (encrypted remote control communication)	Enabled		
Enforce SSL (disable unencrypted port)	Disabled		
SSL remote control port	6065		
Certificate used for SSL communications	Automatically create self-signed certificate on Agents		
Show user notification message on agent when remote	Disabled		

Click **Generate report** to view a configuration report that lists all current settings and all Group Policy Objects that were applied to the computer.

To search for a text string in the report. Press CTRL – F.

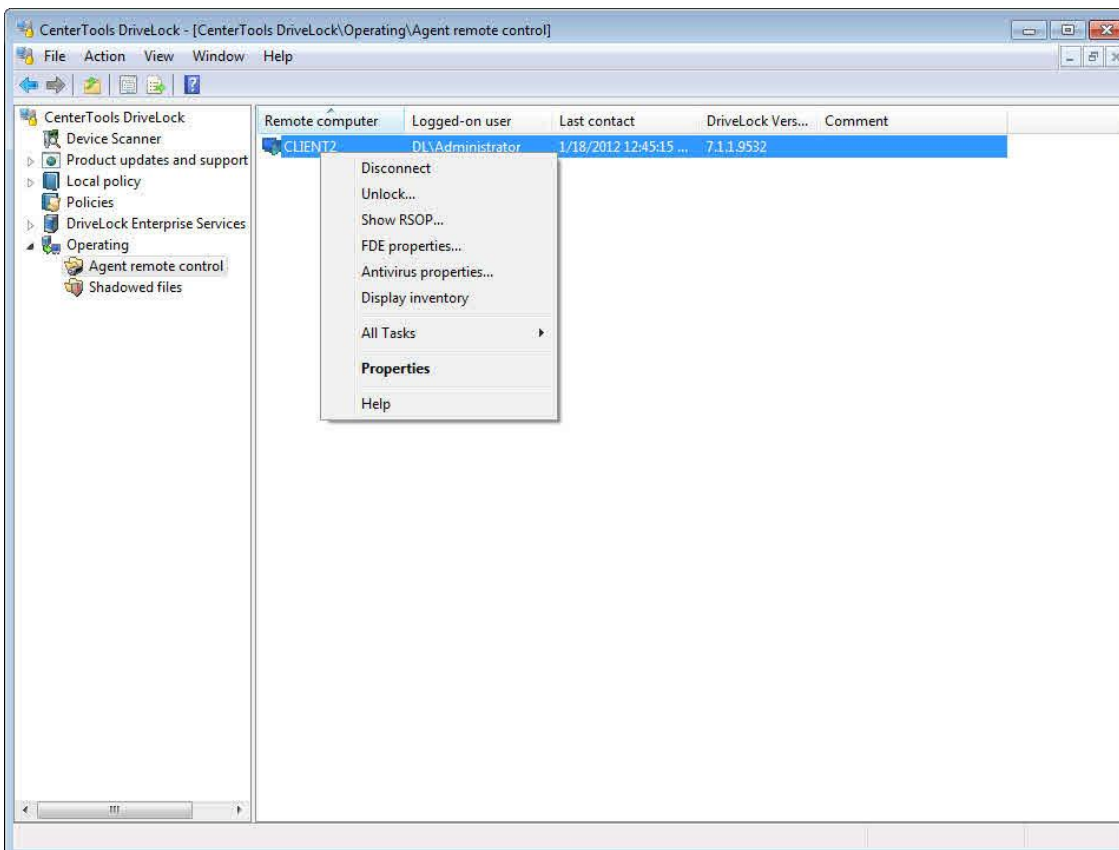
Click **Applied Group Policy Objects** to view the Group Policy Objects that have been applied to the computer by the Windows Group Policy engine.



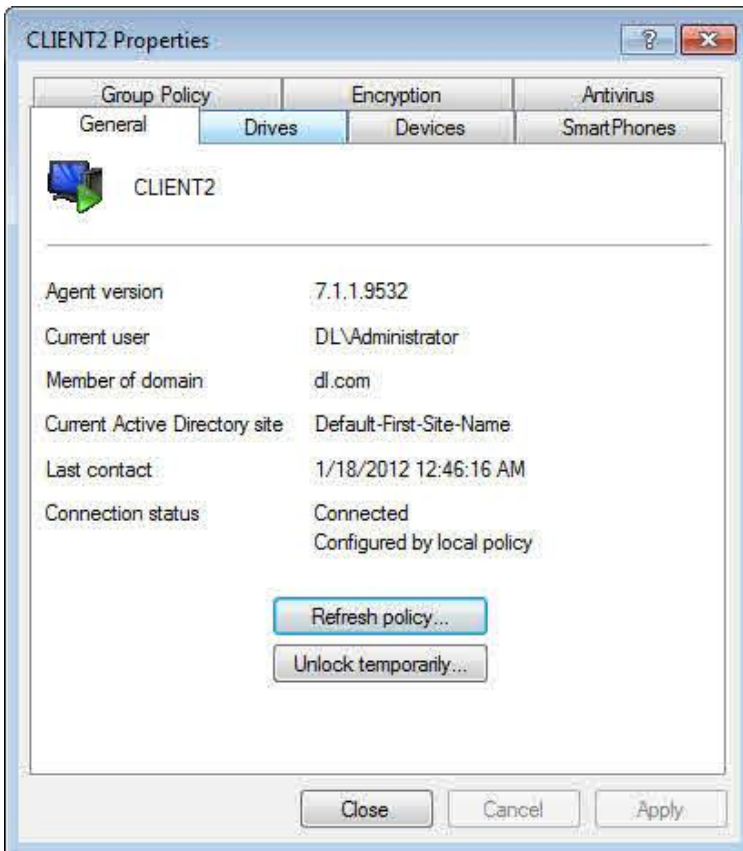
Right-click a GPO to view its properties or to edit it in the Group Policy Object Editor.

When you have finished viewing the Agent information, close the window.

20.2.4 Viewing Currently Attached Devices

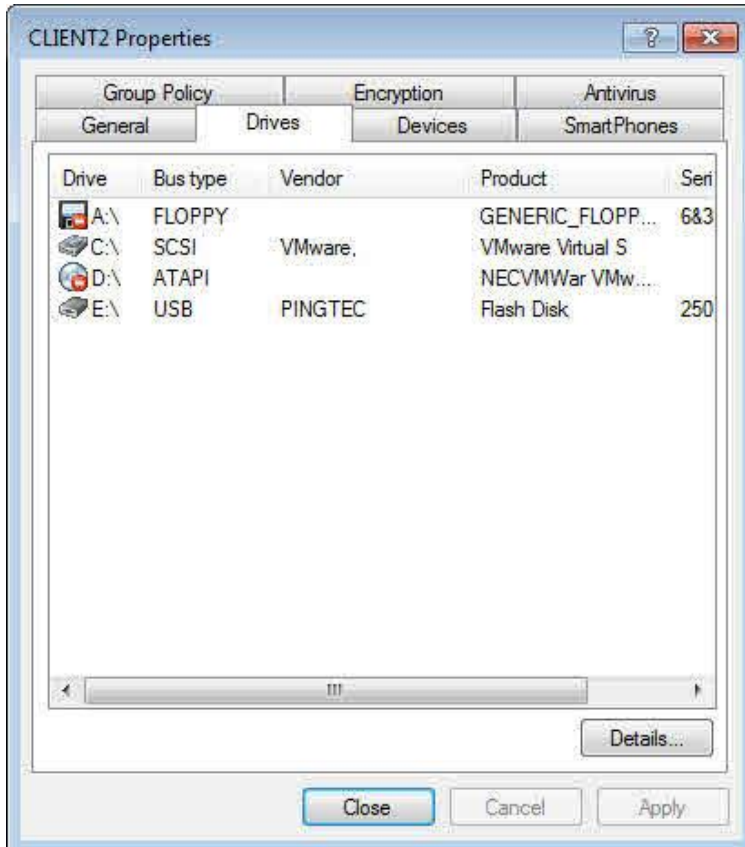


To display the drives and devices currently attached to a client computer, right click the computer and then click **Properties**, or double click the computer.

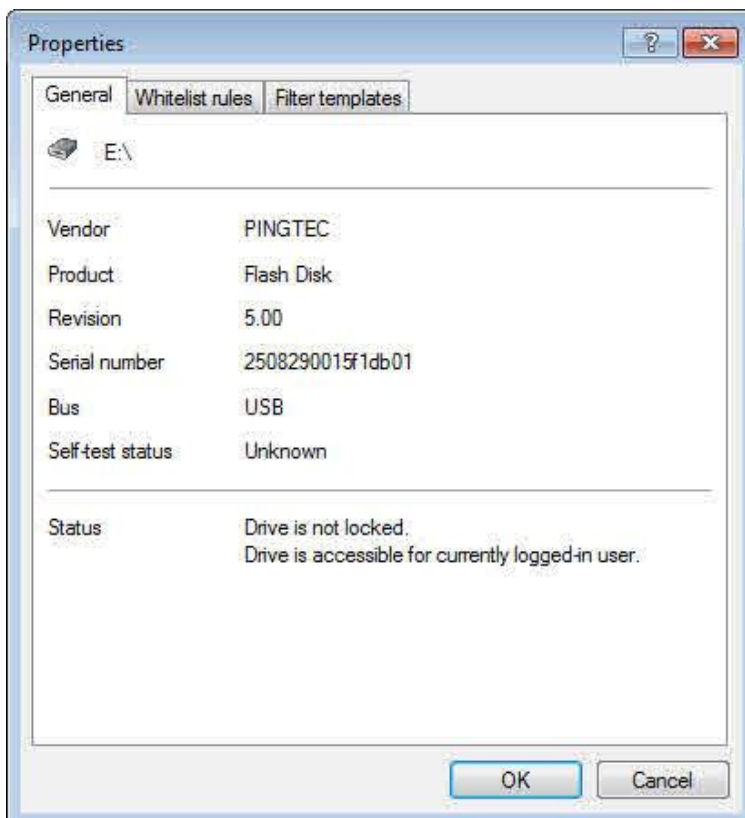


Use the buttons to force the client to refresh its Group Policy settings or to temporarily unlock devices.

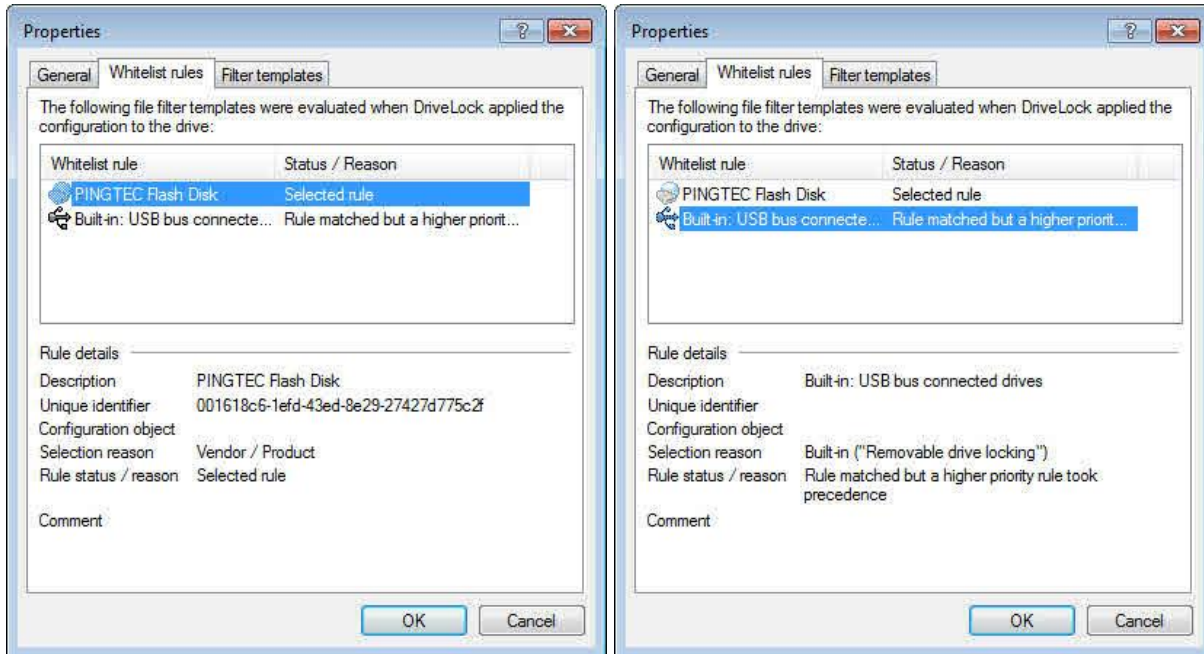
On the **Drives** tab you can view all drives that are currently connected to the computer and whether they are currently locked.



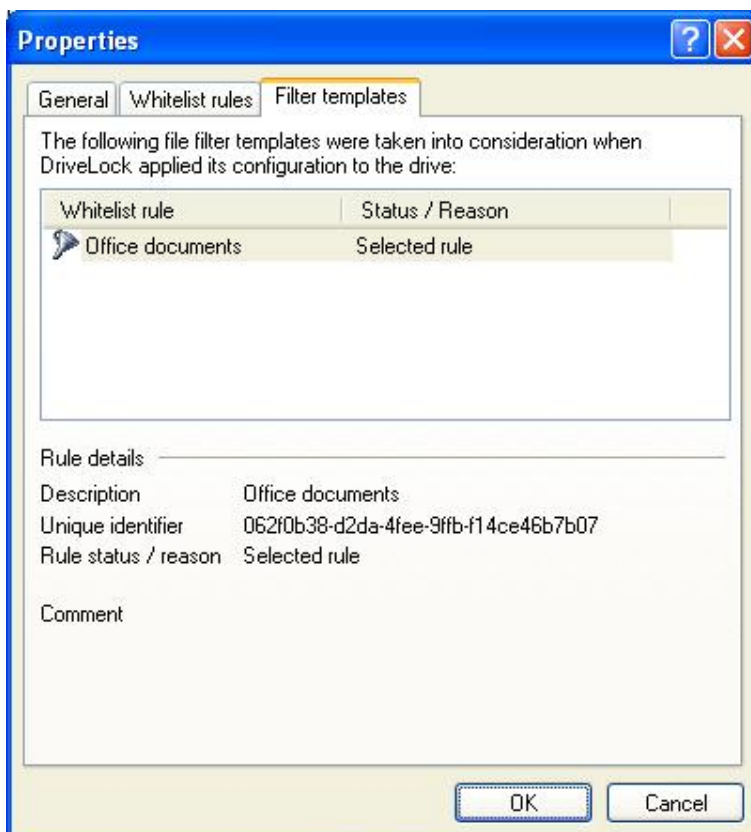
Select a drive and then click **Details** to view more information about the whitelist rules or filters that currently apply to the drive.



The status of this drive is displayed (for example, whether it is blocked or access is allowed).



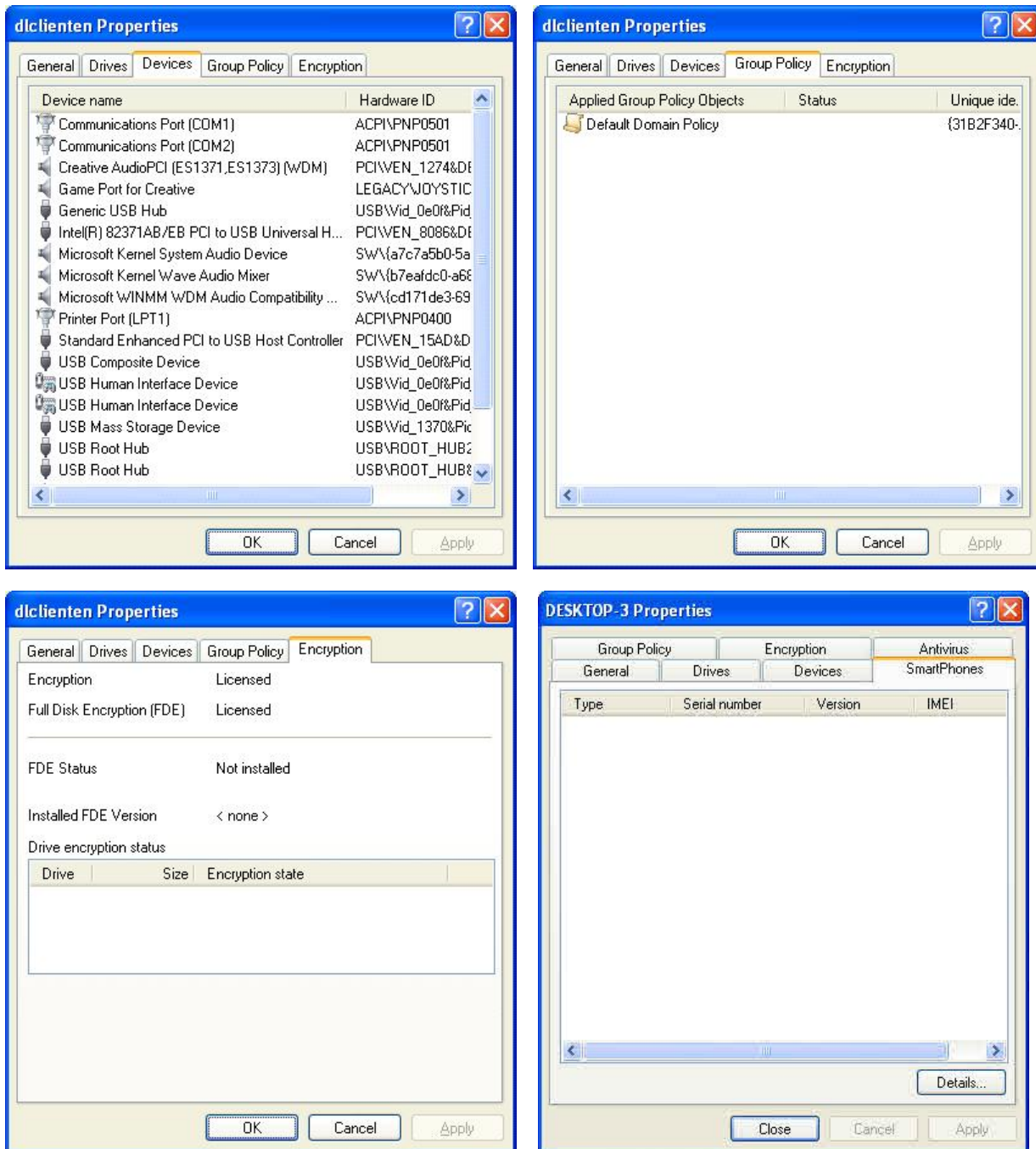
Click the **Whitelist rules** tab to view additional information about all whitelist rules that apply to this drive and which whitelist rule is enforced.



Click the **Filter templates** tab to view additional information about file filter templates that apply to this drive and which template is enforced.

You can use the list of whitelist rules and file filter templates to identify conflicts between competing rules or templates when drive locking does not work as expected.

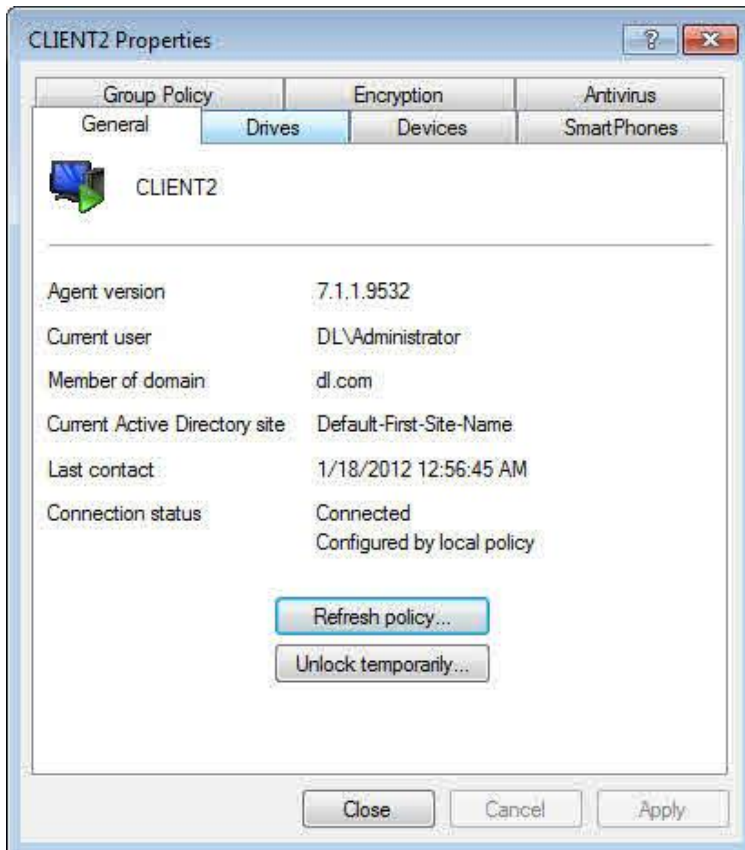
Click **OK** to close the Properties window.



Use the other tabs to view information about currently used devices, smartphones and Group Policy Objects that have been applied to the client computer and the status of Encryption 2-Go, Disk Protection and Antivirus.

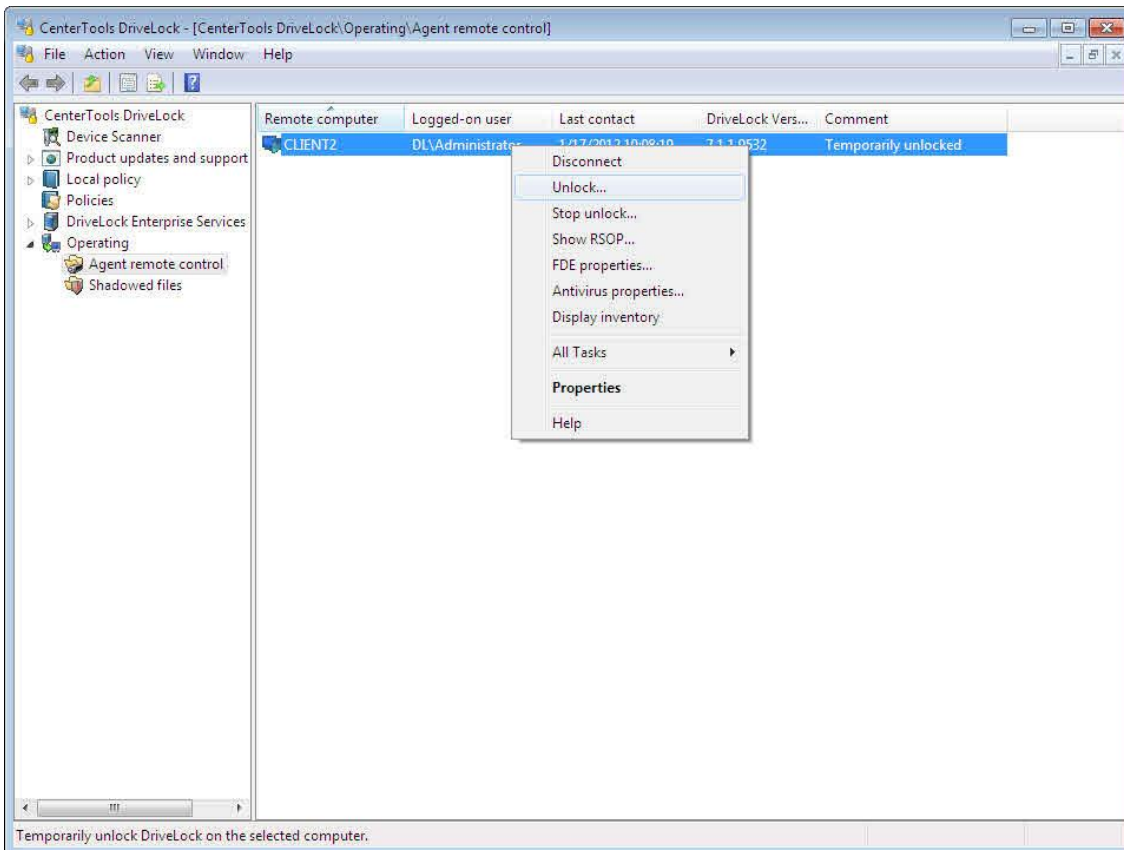
Click **OK** to close the Properties window.

20.2.5 Manually Updating the Policy

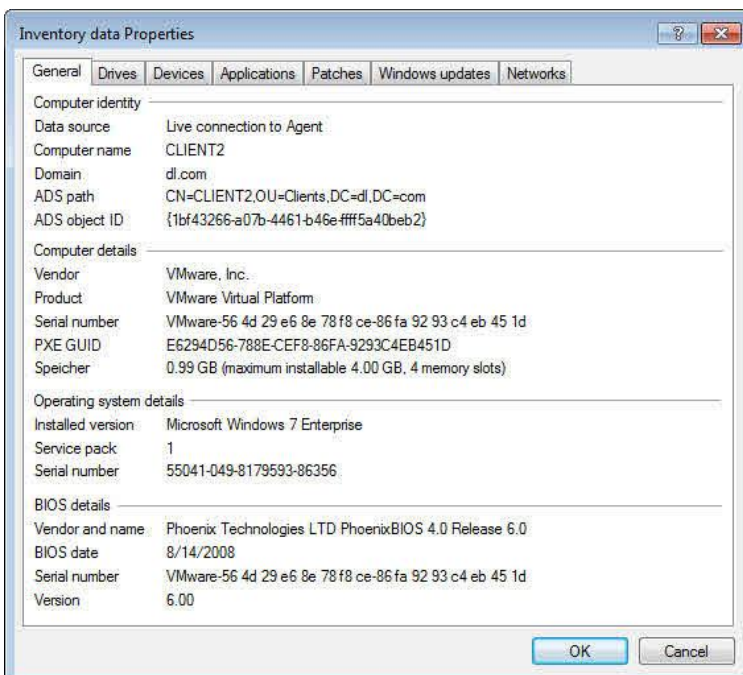


To manually initiate a policy update on an Agent, right-click the computer and then click **Properties**. In the Agent's *Properties* dialog box, on the *General* tab, click **Refresh policy**. This is equivalent to refreshing the Group Policy by using the Windows command `gpupdate /force` or re-loading settings from a configuration file or a centrally stored policy from the DriveLock Enterprise Service.

20.2.6 Displaying Inventory Data

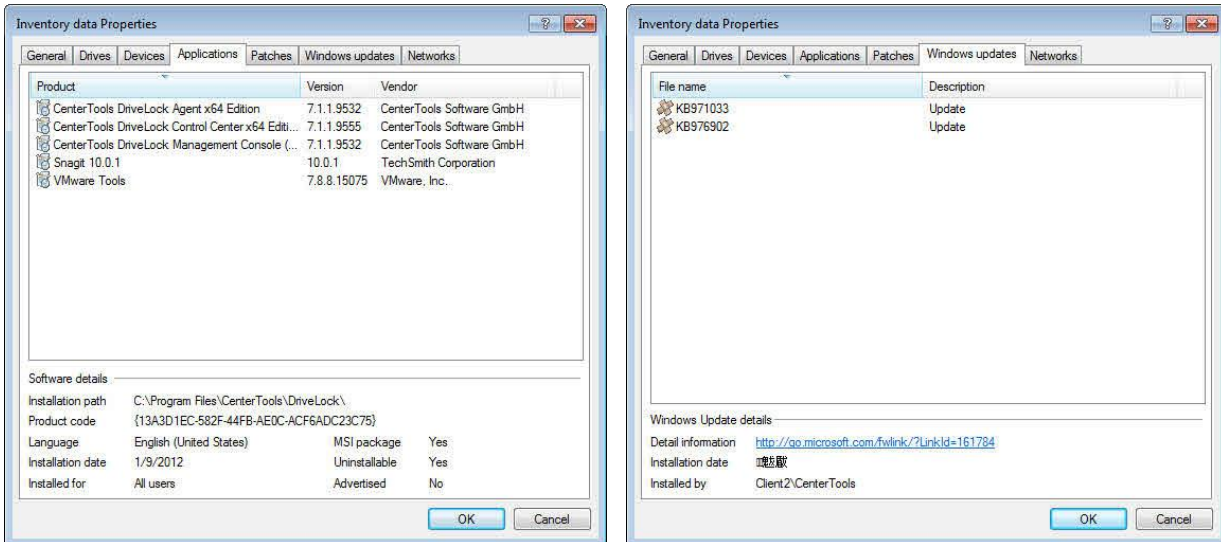


To display the inventory data of a computer, right-click the computer and then click **Display inventory**. All software and hardware inventory data is displayed.



The data source information indicates whether the data was retrieved directly from the computer (when connected using Agent Remote Control) or from the DriveLock database via DES.

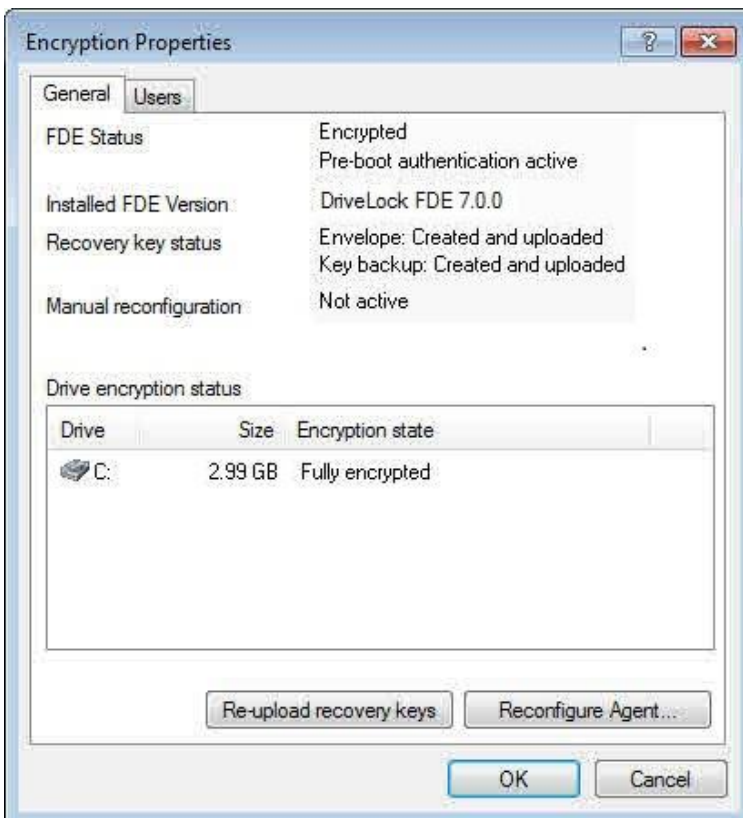
Click the appropriate tabs to view information about drives, devices, networks, installed applications and updates.



Click **OK** to close the window.

20.2.7 Viewing the disk encryption status

To view a computer's disk encryption status, including the status of recovery keys, right-click the computer and then click **Disk Protection properties**.



In the Encryption Properties dialog box, on the General tab, you can perform the following tasks (only DriveLock Disk Protection, not BitLocker Management):

- *Re-upload recovery keys*: If the recovery key status indicates that the keys have not been uploaded to a central location (DES or file share) or if you need to upload they keys again for any reason, click **Re-upload recovery keys**.

- **Reconfigure Agent:** You can temporarily change the Disk Protection settings for a single Agent. Most often this is used when you perform disk recovery to prevent the Agent to immediately start encrypting the disk again. Click **Reconfigure Agent** to change the following settings for the computer:

- **Override policy settings:** Change the selected settings.
 - **Install Disk Protection:** Clear the checkbox to uninstall Disk Protection from the computer. Before Disk Protection is removed, all disks are decrypted and pre-boot authentication is disabled. This process can take several hours.
 - **Enable pre-boot authentication:** Clear this checkbox to disable pre-boot authentication on the computer.
 - **Encrypt local disks:** Clear this checkbox to decrypt all local disks. This process can take several hours.

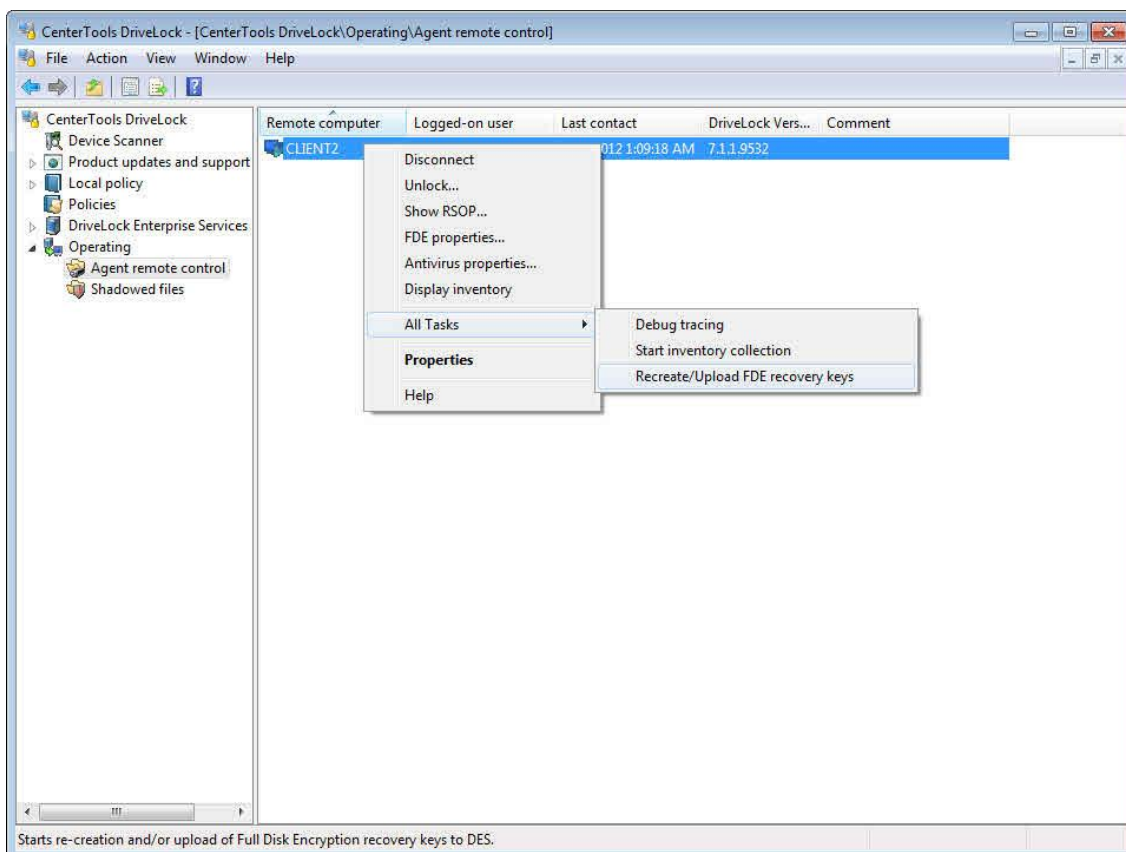
For the following options there are three settings :

- keep the policy value , ✓ switch on, □ switch off.

On the *Users* tab you can view all user accounts that are currently in the pre-boot authentication database and that can be used to authenticate when the computer starts (currently only for DriveLock Disk Protection).

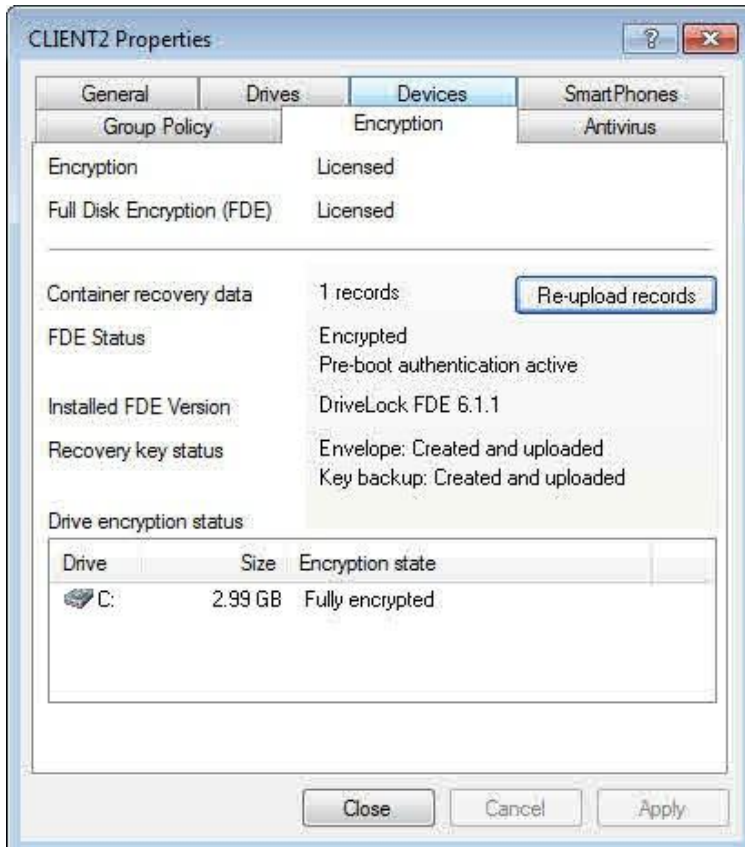
20.2.8 Manually Uploading Disk Protection Recovery Data

If the uploading of Disk Protection recovery data to the DES or a file share has been enabled in your policy, this data is automatically backed up to the specified location. If you have not configured this setting or if you notice that the recovery data is missing for any reason (for example, when monitoring Agents using the DriveLock Control Center), you can manually upload this data to the configured location. To do this, right-click the computer, point to *All Tasks* and then click **Recreate/Upload Disk Protection recovery keys**.



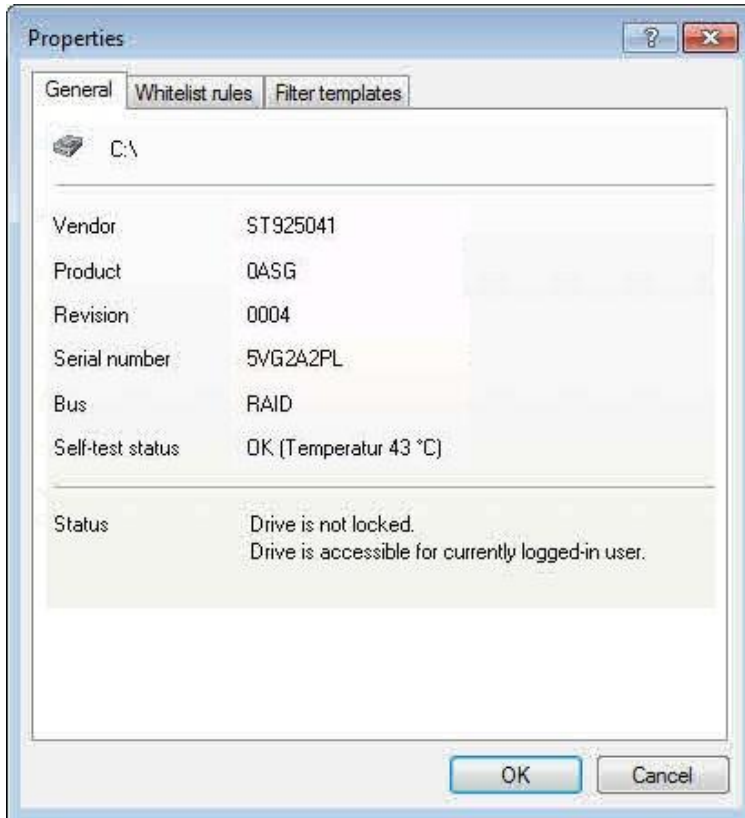
20.2.9 Manually Uploading Encryption 2-Go Recovery Data

If the uploading of Encryption 2-Go (removable media encryption) recovery data to the DES or a file share has been enabled in your policy, this data is automatically backed up to the specified location. If you have not configured this setting or if you notice that the recovery data is missing for any reason (for example, when monitoring Agents using the DriveLock Control Center), you can manually upload this data to the configured location. To do this, right-click the computer and then click **Properties**. On the *Encryption* tab the number of container recovery sets is displayed. Click **Recreate/Upload Encryption 2-Go recovery keys**.



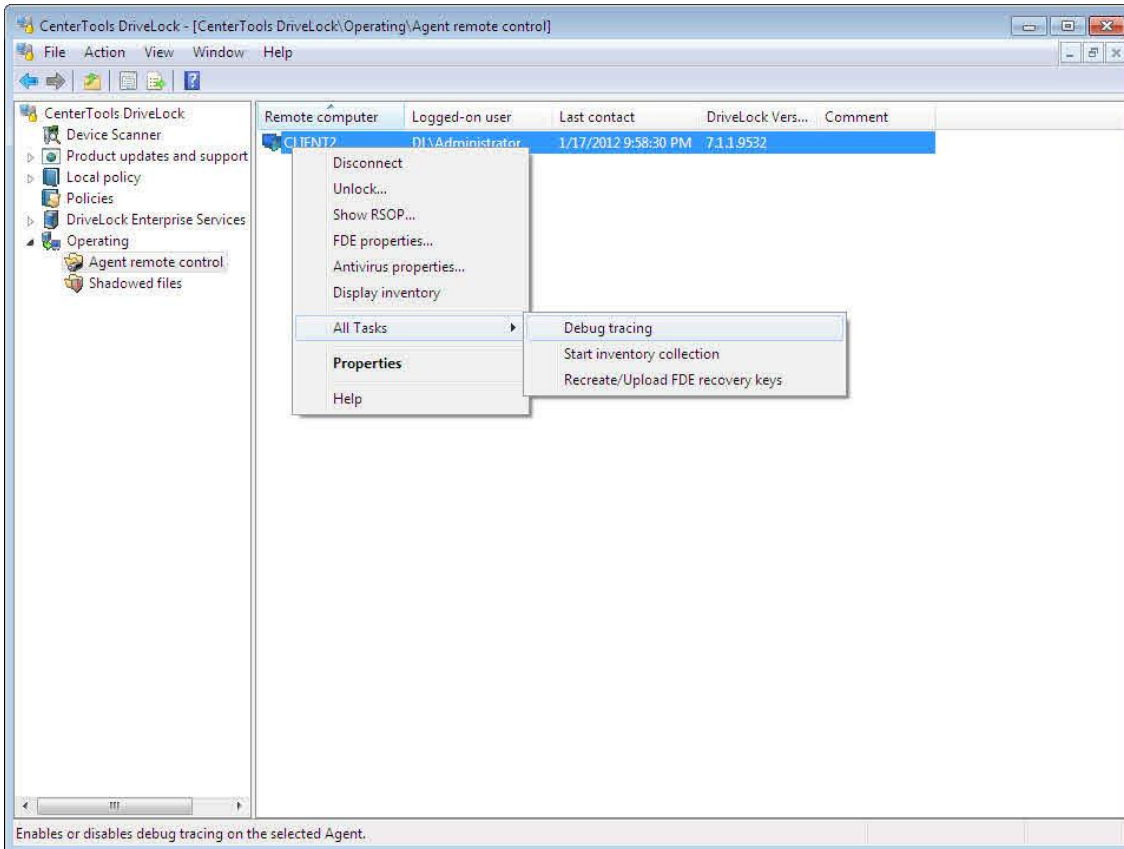
20.2.10 Viewing Disk Health Information (S.M.A.R.T.)

If you enabled the monitoring of Self-Monitoring, Analysis and Reporting Technology (S.M.A.R.T.) data in your policy, you can view the health status of hard disks on a client computer. To view this information, in the Agent's *Properties* dialog box, on the *Drives* page, select a drive and then click **Properties**. The disk's current status is displayed under *Self-test status*.



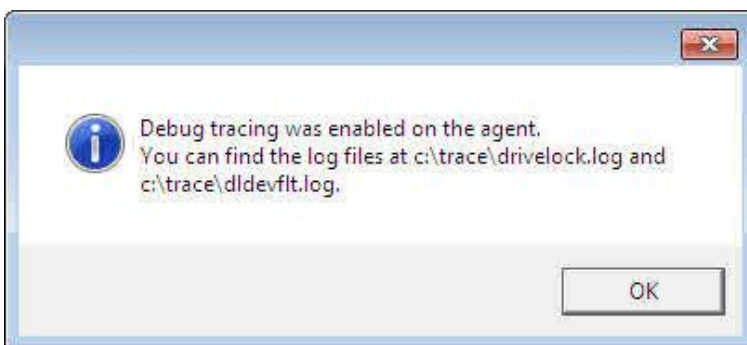
20.2.11 Activating Tracing

For troubleshooting you can configure the DriveLock Agent to record detailed diagnostics information about all operations. This is called Tracing. Tracing creates files that can help DriveLock technical support to identify the source of problems you may encounter, such as policy settings not being applied as expected. You should activate tracing on an Agent only for troubleshooting and de-activate it when the required data has been collected.



To activate tracing on an Agent, right-click the computer and then click **All Tasks -> Debug tracing**.

A message appears, confirming that tracing has been activated.

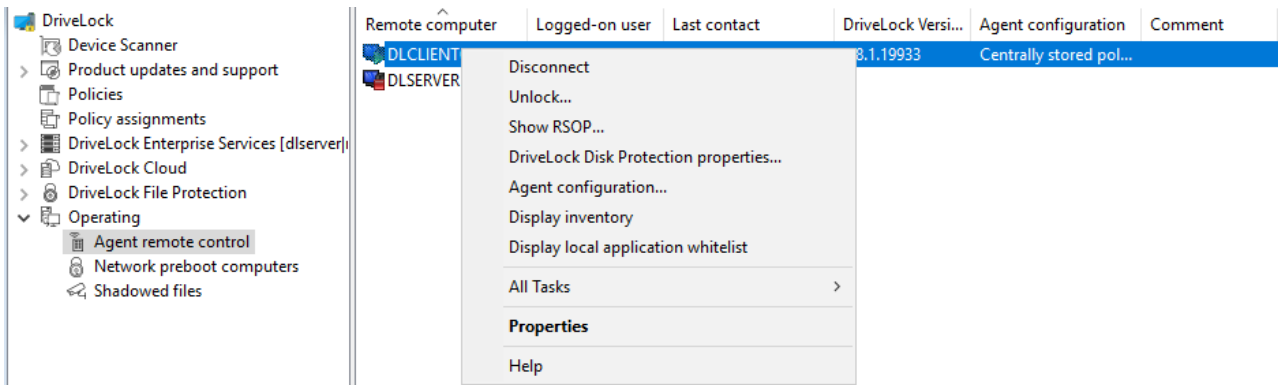


To de-activate tracing on an Agent, right-click the computer and then click **All Tasks -> Debug tracing**.

20.2.12 Displaying and Deleting Locally Learned Applications

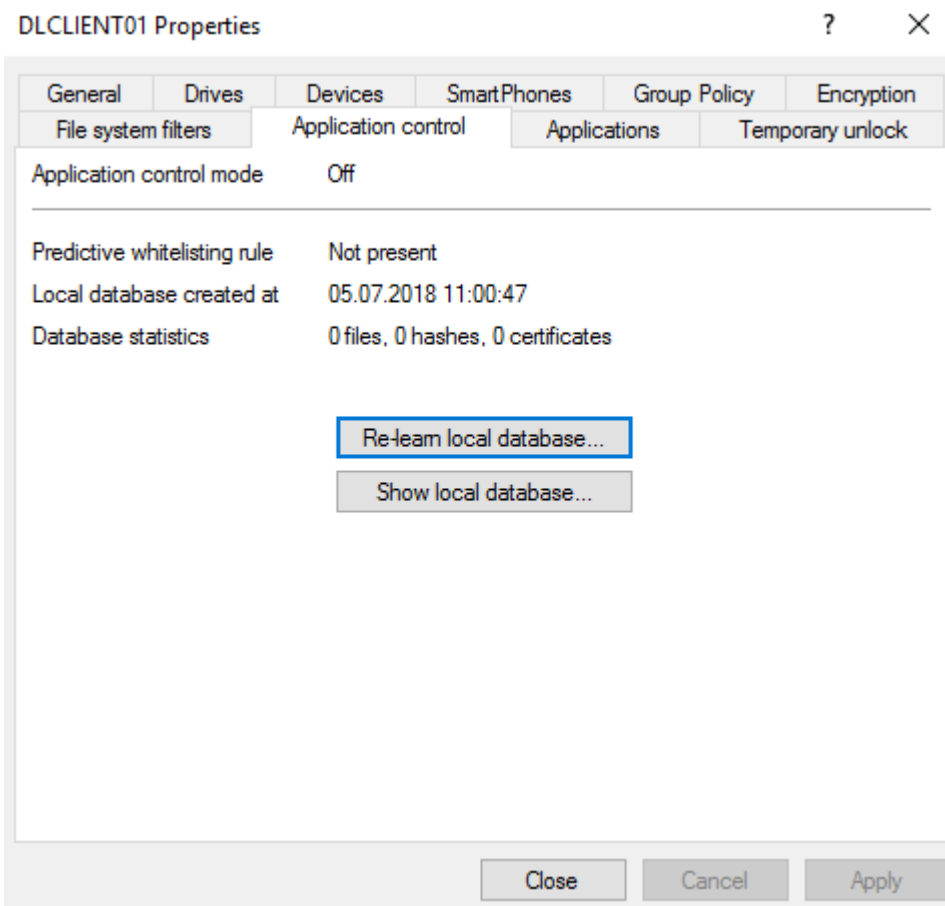
This chapter remains in the Administration Guide until further notice, but it will not be updated. Please note that the current documentation on application control can be found in a separate manual available at [DriveLock Online Help](#) starting with version 2020.1.

If you use application control in combination with machine learning, a database with the application shared with this computer is created on the client (local whitelist database). You can connect to an agent and view the contents of this database.

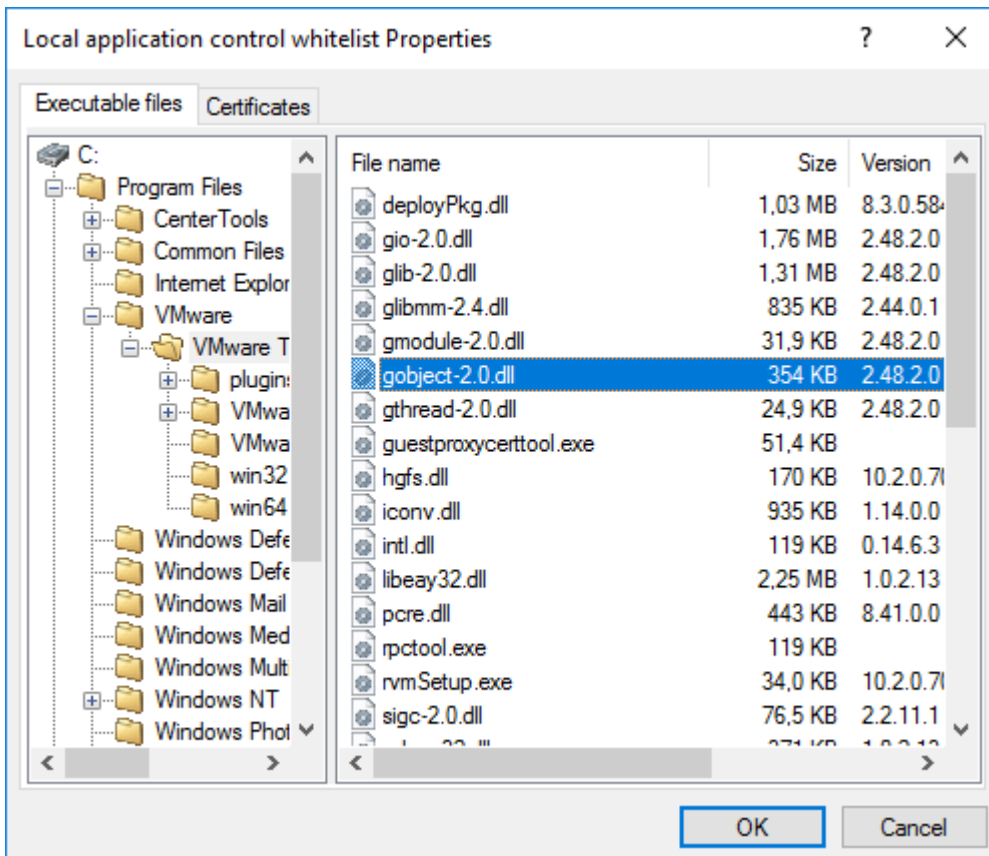


Select the computer where the agent is running, open the context menu and then click **Display local application whitelist**, after having connected to the computer.

On computer's Properties dialog, you can also open the **Application control** tab and click **Show local database**:



A window with a structure similar to Windows Explorer opens. Depending on the size of the database, it may take some time to open.



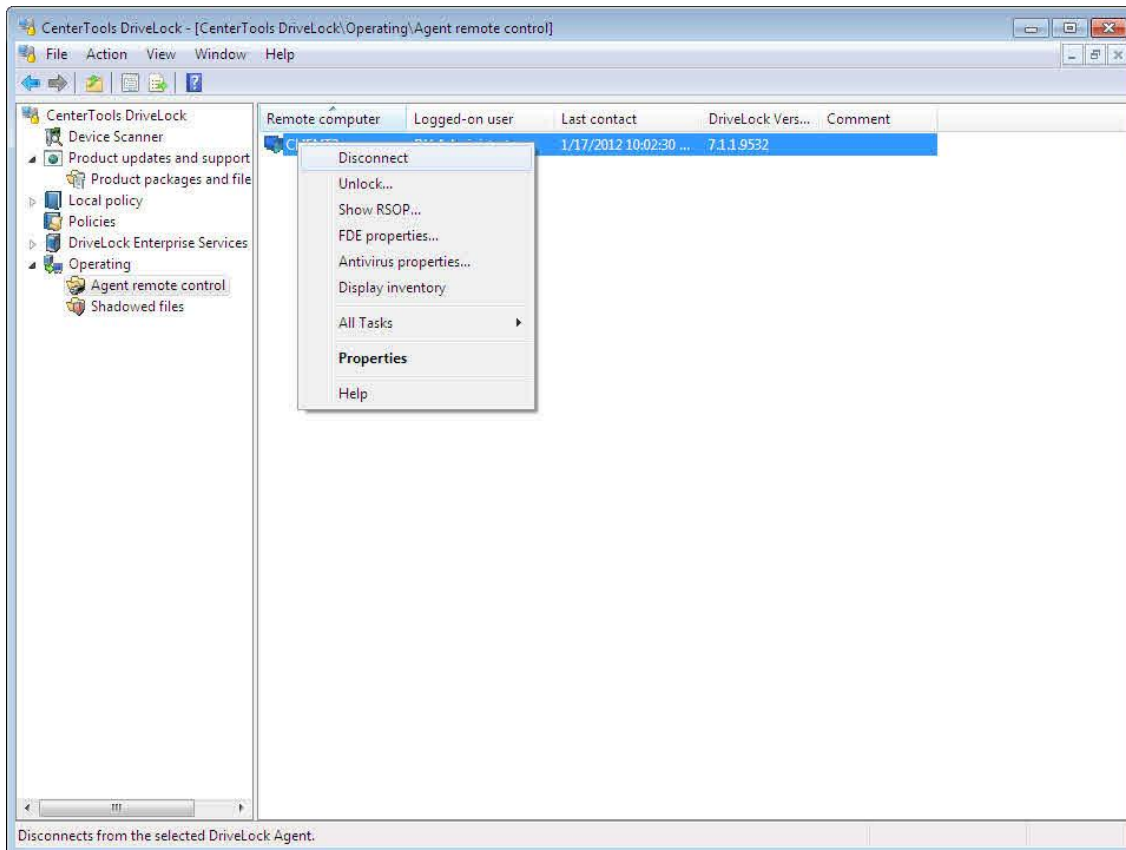
Here you can see the applications contained in the database. You cannot add new applications in the MMC, but you can remove applications that have been unintentionally unlocked (learned) from the database. Select the application you want to remove and click the **Delete** button.

20.2.13 Checking the Defender Status

On the **Defender** tab you can check the status of the last Microsoft Defender scan on the agent, update it and start a new scan if necessary.

For more information about DriveLock Defender Management, see the related manual on [DriveLock Online Help](#).

20.2.14 Disconnecting from an Agent



To close the connection to an Agent, right-click the Agent and then click **Disconnect**.

20.3 Unlocking Agents

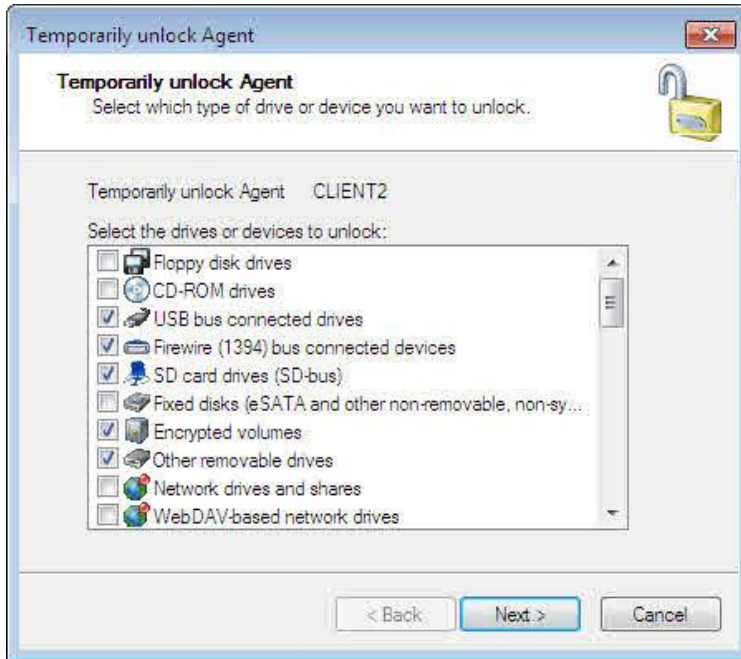
You can temporarily unlock Agents to temporarily disable restrictions that are configured in your policy. This lets you respond quickly and flexibly to users who require access to a locked drive or device. For example, even though you disable access to all USB flash drives, a user has a legitimate need to copy a presentation to such a drive. Unlocking lets you temporarily give the user the required access without having to reconfigure your policy.

20.3.1 Configuring General Unlocking Settings

Different steps are required to initiate the process, depending on whether you unlock a single Agent or multiple Agents, and whether you perform online or offline unlocking. The actions that are available for each of these methods are identical and are described in the following sections.

20.3.1.1 Unlocking Drives, Devices and Smartphones

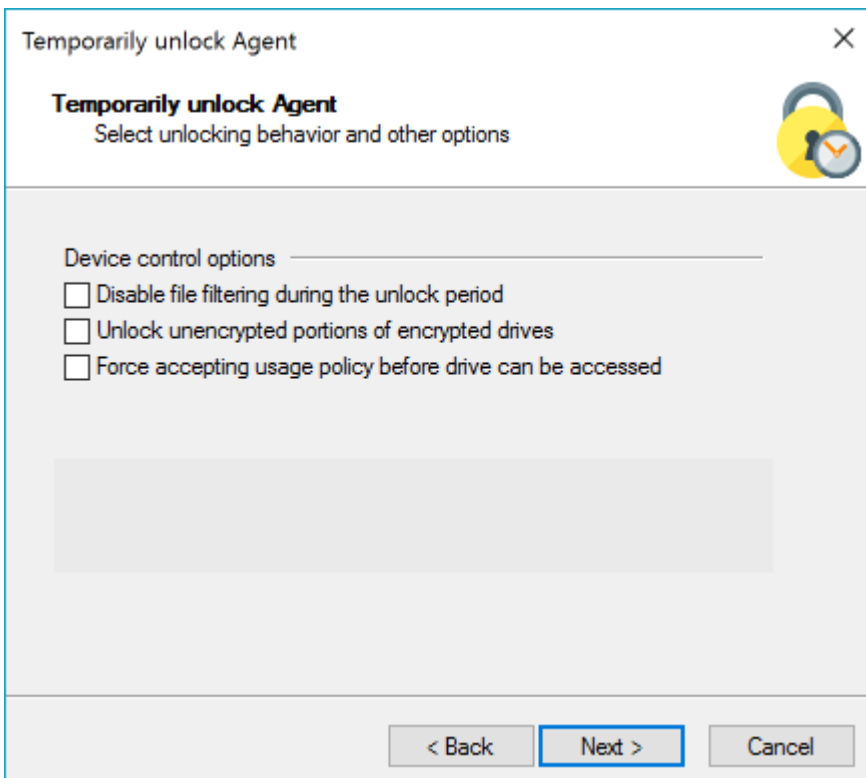
Select the type of drive, device or smartphone to temporarily unlock. For example, to unlock USB-connected drives, select the *USB bus connected drives* checkbox.



When you select a class of drives or devices, such as USB-connected drives, access to all drives of this class will be enabled. Unlocking a specific drive or device is not possible using temporary unlocking. If you need this functionality, you need to create a whitelist rule instead.

20.3.1.2 Setting Time Limits and Suspending Restrictions

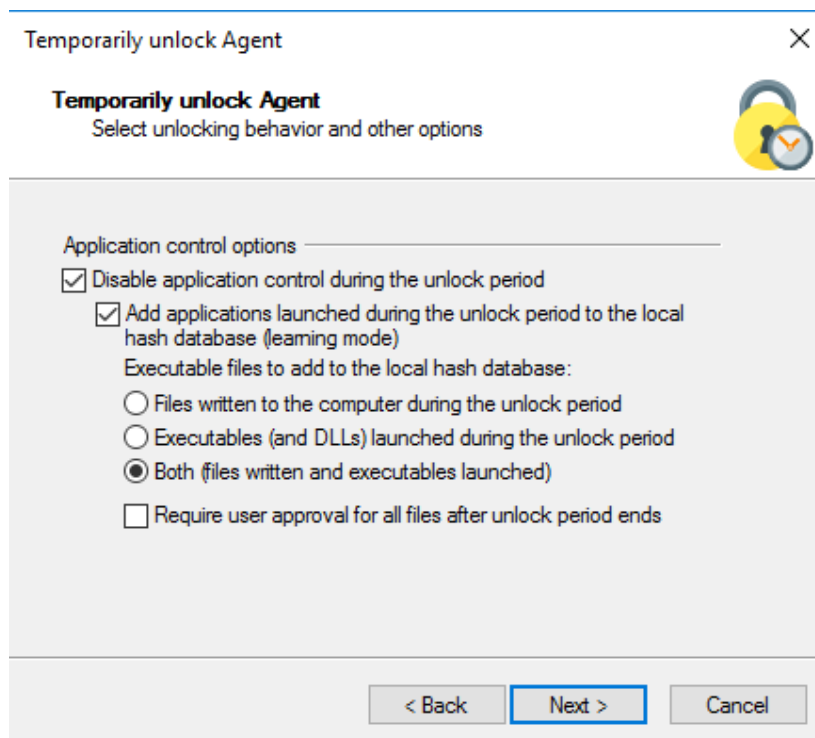
In this step, you determine the period or time until which this temporary unlock is valid. The unlock is even maintained during a computer restart, e.g. if you temporarily unlock USB drives for the next three days, the computer can be rebooted in between.



When you unlock drives, you can select the following options to temporarily additional restrictions:

- *Disable file filtering and auditing during unlock period:* Users can read and copy files that would normally be blocked based on file filtering rules. No auditing of file access is performed.
- *Unlock encrypted portions of encrypted drives:* Allow access to unencrypted portions of drives that are encrypted using Encryption 2-Go. Commonly the Mobile Encryption Application (MEA) is stored on an unencrypted portion of such a drive.
- *Force accepting usage policy before drive can be accessed :* The user must agree to a configured usage policy before the drive is unlocked.

Click **Next**.



If you are using application control, you can specify settings here, so that applications can be disabled during unlock. You also specify whether and which application files are added to the local hash database during this unlock period.

Use the *Require user approval for all files after unlock period ends* option to check the "learned" applications manually after the unlock is finished before they are added to the local application database and thus unlocked.

If you have Defender Management licensed and are running Defender scans on your agents, you can disable Microsoft Defender control in the Unlock wizard. For more information, refer to the Defender Management documentation at [DriveLock Online Help](#).

Click **Next**.

Temporarily unlock Agent

**Temporarily unlock Agent**

Select for how long policy settings are disabled.



Select for how long the target computer will be unlocked

 Time span min (ends with reboot) Until date

Reason for unlocking (for reporting purposes)

< Back

Finish

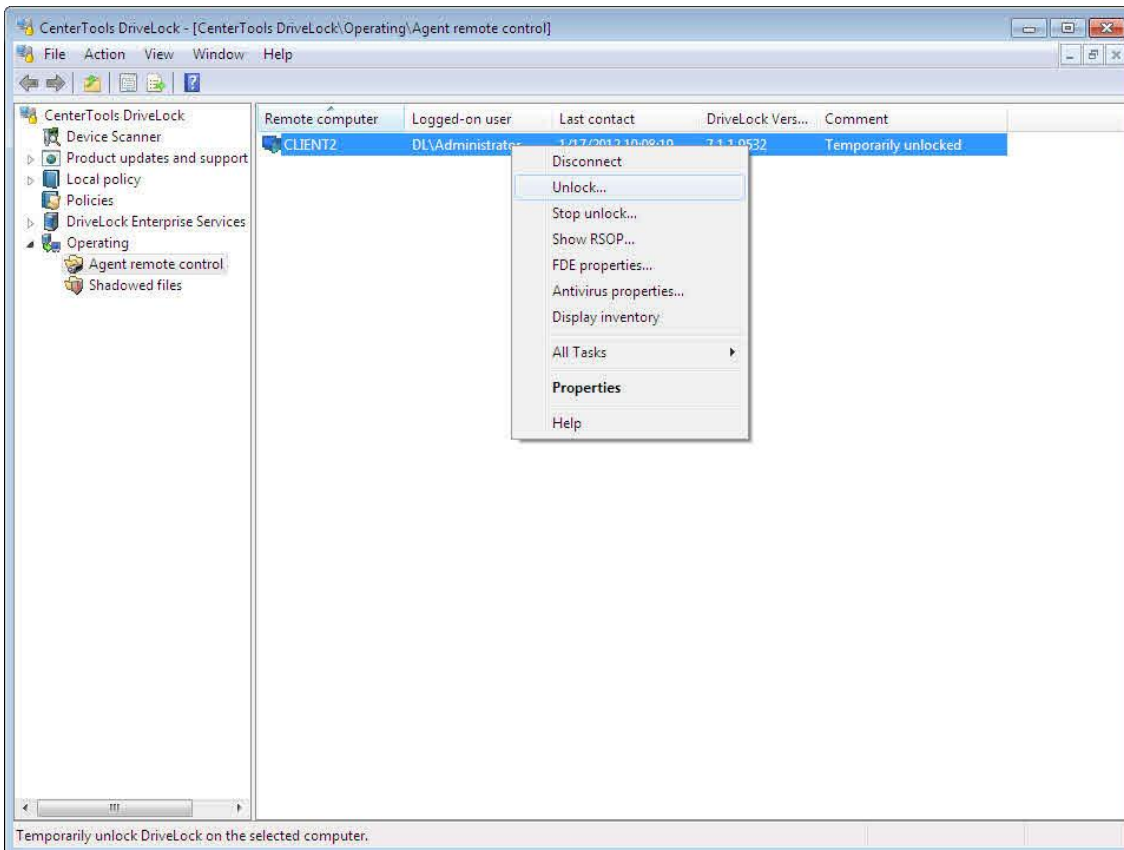
Cancel

Finally, select the required unlock period, either in minutes or up to a specific date and time.

As administrator, you can also enter a text (for example, the reason for unlocking) at this point. This text is also stored in the event and can be evaluated via reporting.

Unlocking starts as soon as you click **Finish**.

20.3.2 Temporarily Unlocking a Single Online Agent



To temporarily suspend drive or device controls on a client computer, click **Agent remote control**, right click the remote computer and then click **“Unlock”**. (For more information about how to connect to Agents remotely, see the section [“Connecting to a DriveLock Agent”](#))

Configure the unlocking settings as described in the section ["Configuring General Unlocking Settings"](#).

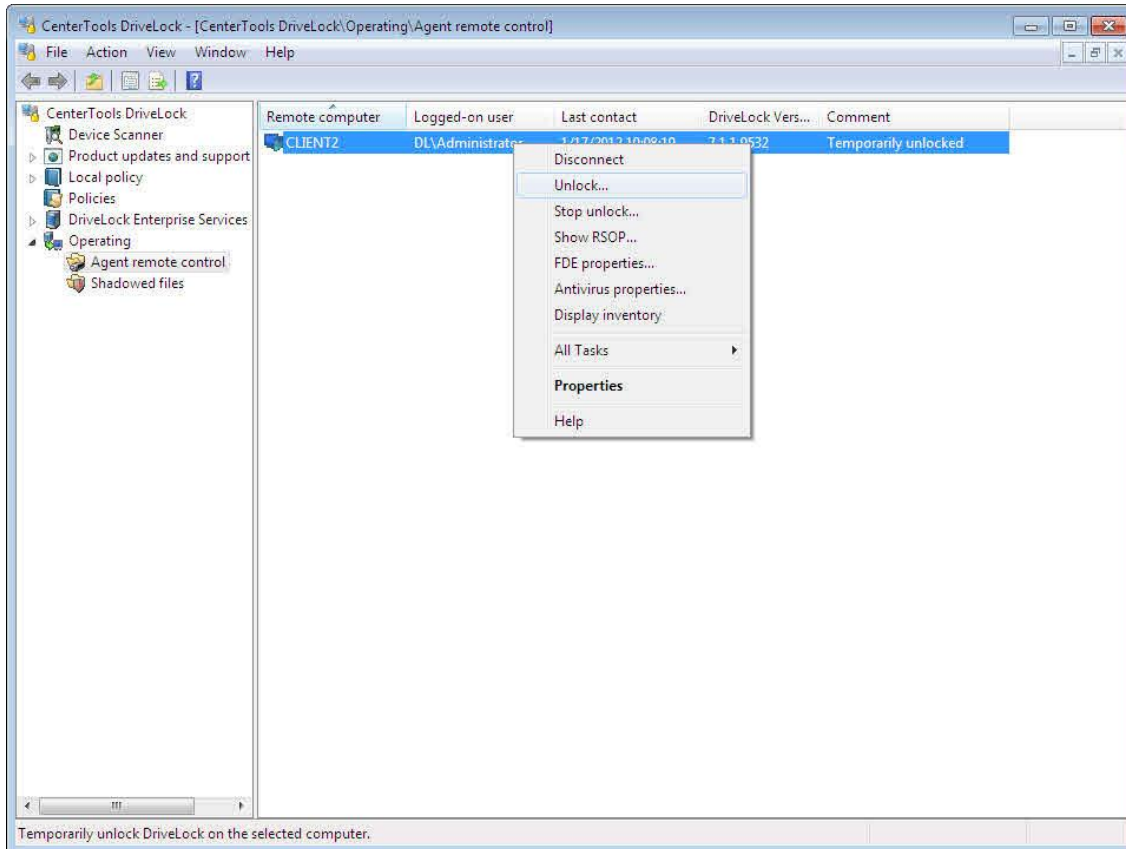
When you have configured all settings, click **Finish** to unlock the Agent. A confirmation dialog box appears.

Click **OK** to acknowledge the message.

If your policy is configured to notify users when an Agent is unlocked, a popup message appears on the computer where you unlock drives or devices:



You can cancel unlocking, for example if you temporarily unlocked an online Agent by mistake.



Right click the remote computer and then click **Stop unlock**. A confirmation dialog box appears:
Click **OK** to acknowledge the message.

20.3.3 Temporarily Unlocking an Offline Agent

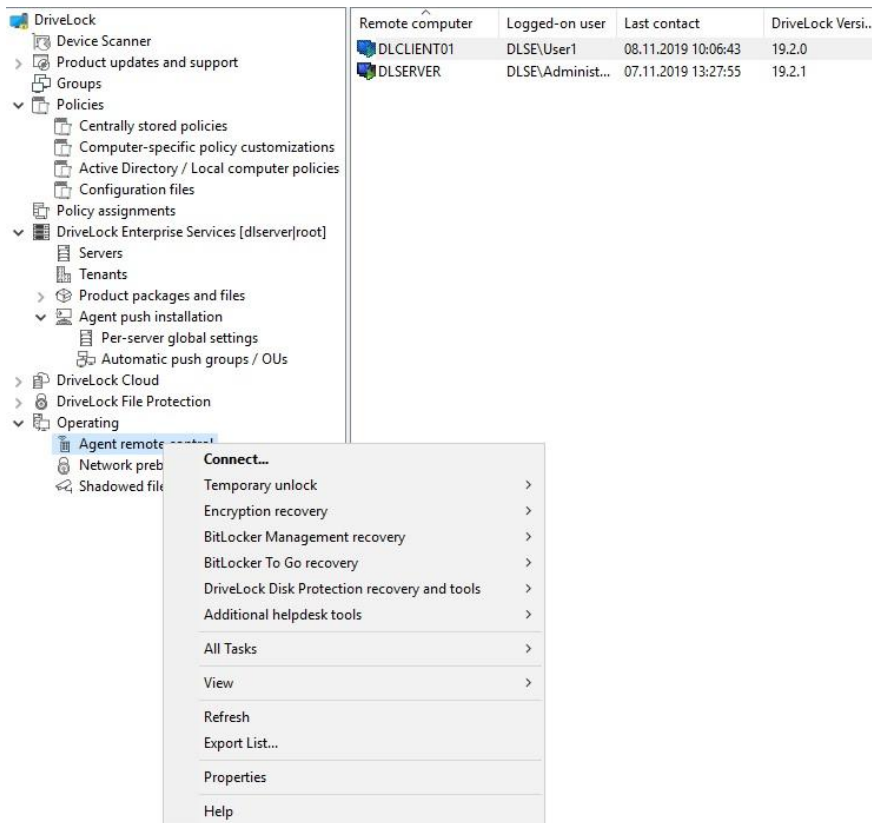
To unlock Agents that you cannot connect to over the network, use the following procedure. The process requires both the user and the administrator to complete separate tasks. The user must start the “Unlock computer” wizard by selecting “**Control Panel (classic view) -> DriveLock**” from the Start menu. The administrator must use the DriveLock Management Console.

The procedure for unlocking offline Agents is described below. The first part consists of the steps that a user must complete. The second part describes the steps an administrator must complete.

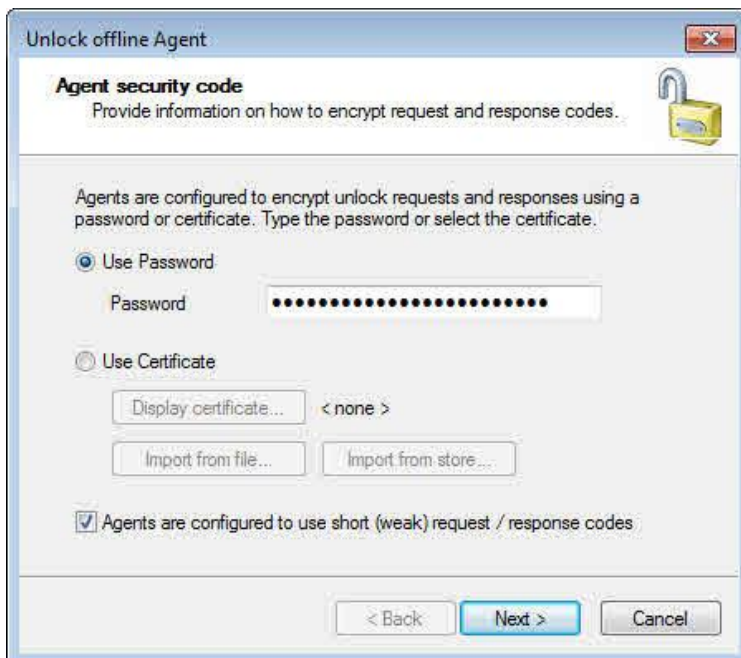
20.3.3.1 User Procedure to Unlock an Offline Agent

The user procedure is described in the *DriveLock User Guide*.

20.3.3.2 Administrator Procedure to Unlock an Offline Agent



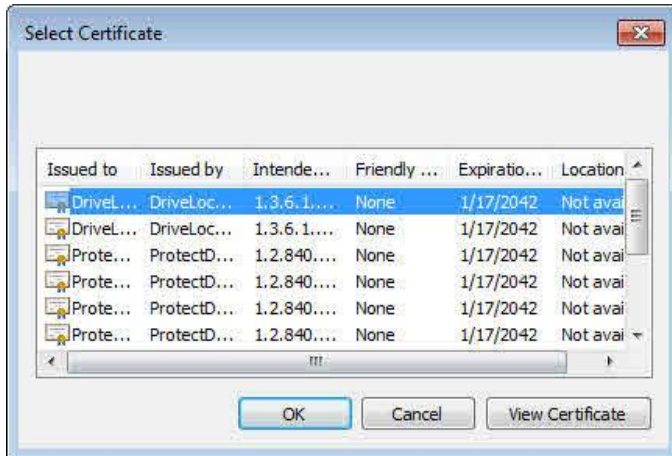
In the DriveLock Management Console, right-click **Agent remote control** and then click “**Unlock offline Agent**”.



Type the offline unlocking password or provide the certificate that is specified in your policy.

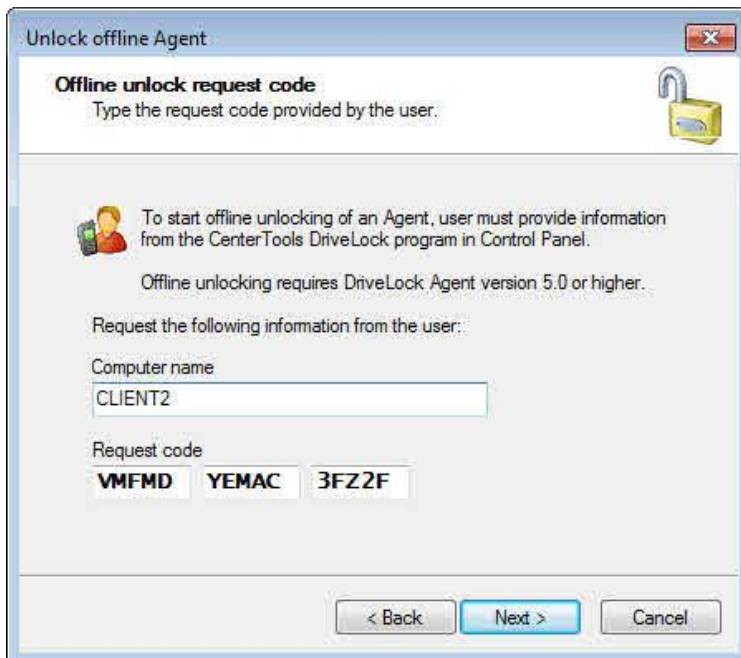
You can import the certificate from a file or use a certificate from the Windows certificate store on the local computer. To import a certificate from a file, click **Import from file** and then select the certificate file.

To use a certificate from the certificate store, click **Import from store**.



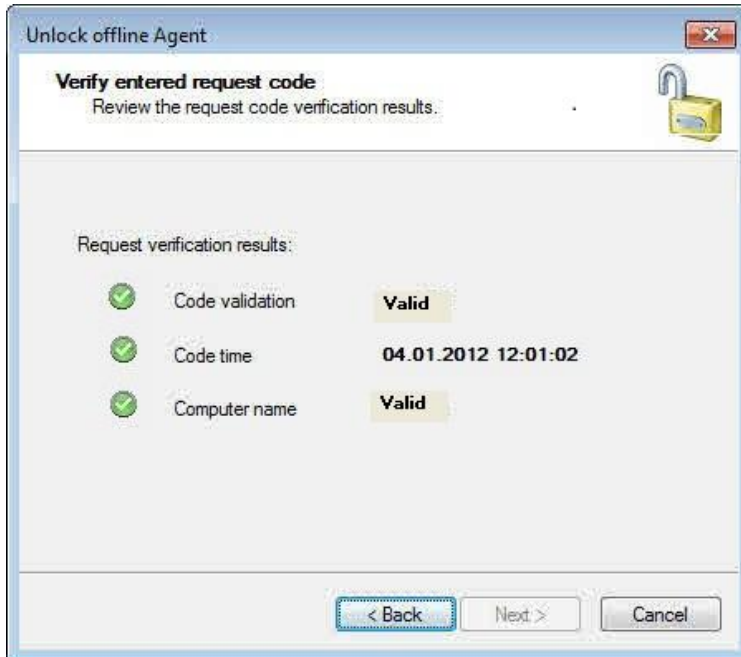
Select the certificate and then click **OK**.

Click **Next** to proceed.



Type the computer name and the request code provided by the user, and then click **Next**.

Depending on the configuration, the length of the request code may vary.



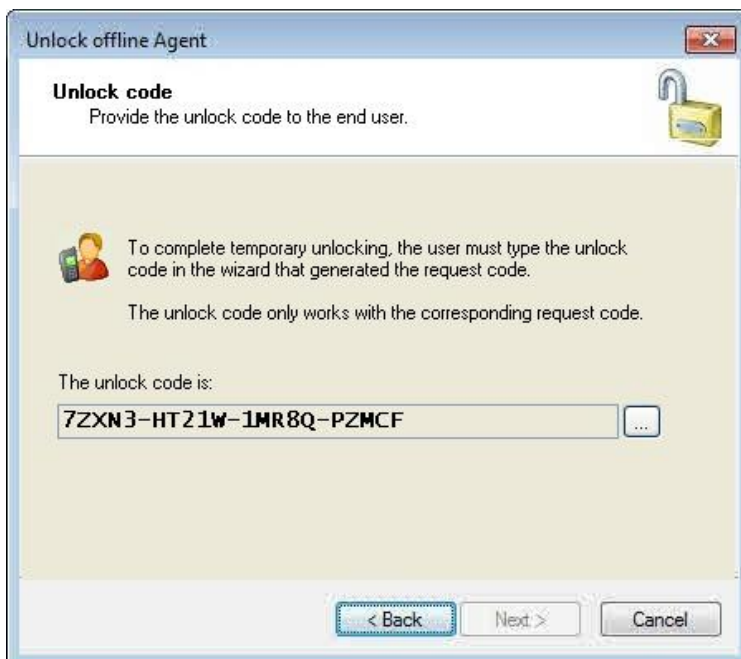
DriveLock verifies the data. If the activation code was generated more than one hour ago, this is indicated under "Code age".

The code provided by the user for unlocking the DriveLock Agent is only valid for one hour. If this time has been exceeded, the user has to start the "Unlock computer" wizard again.

Click **Next** to continue.

Configure the unlocking settings as described in the section "[Configuring General Unlocking Settings](#)".

Click **Next** to display an unlock code.

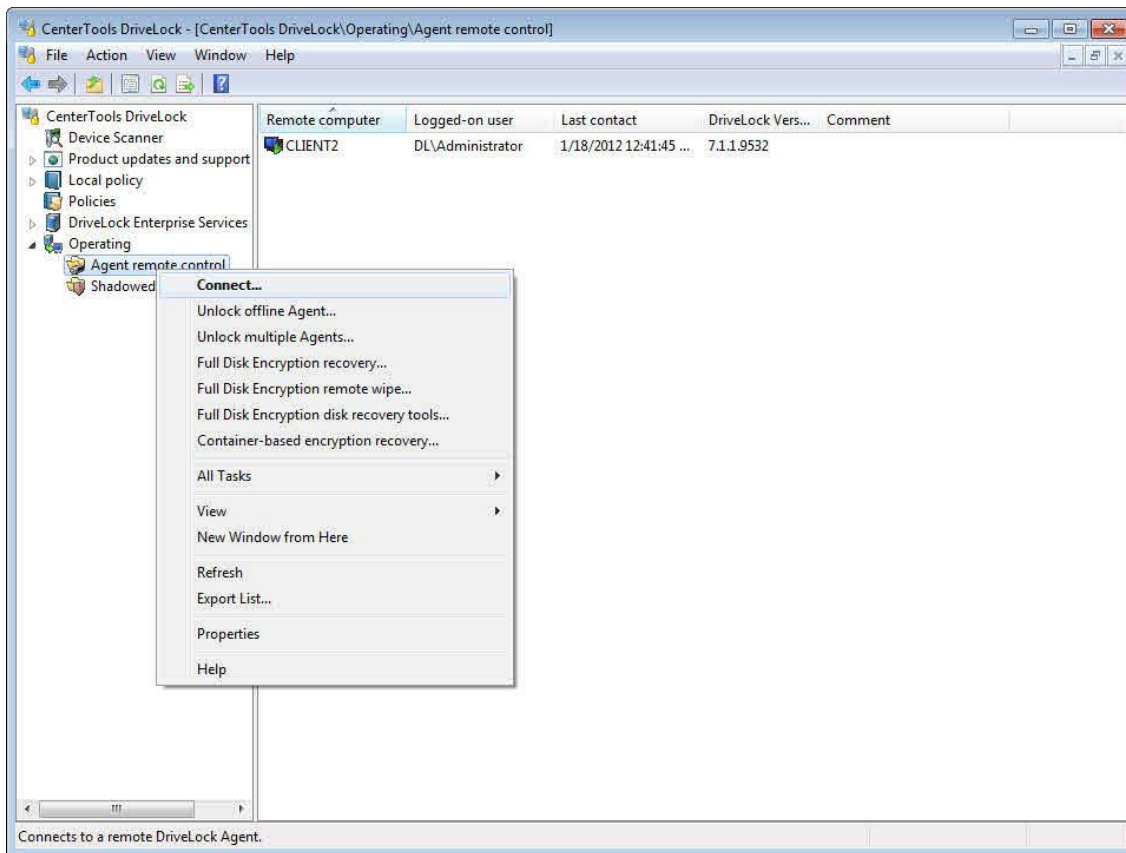


Provide the unlock code to the user. The user will type the code in the wizard on the client computer.

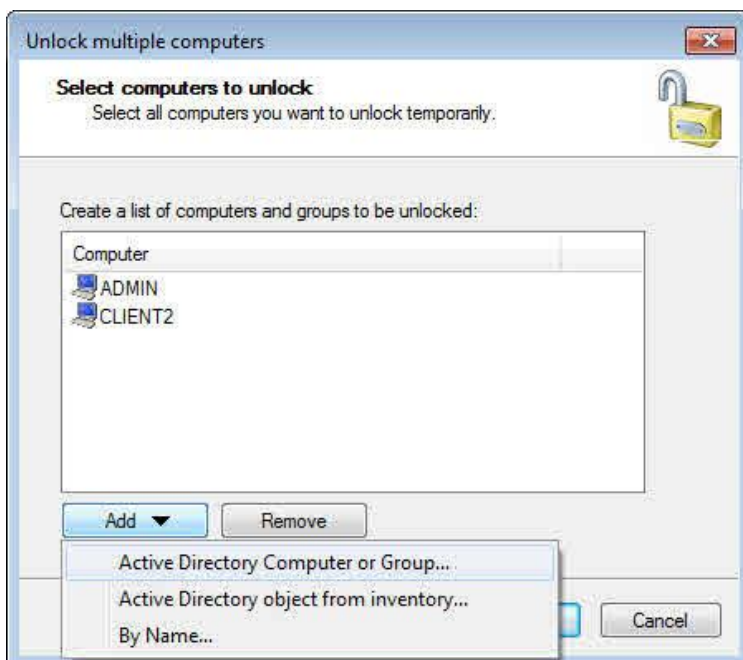
Depending on the configuration, the length of the response code may vary.

Click **Finish** to close the wizard.

20.3.4 Temporarily Unlocking Multiple Agents

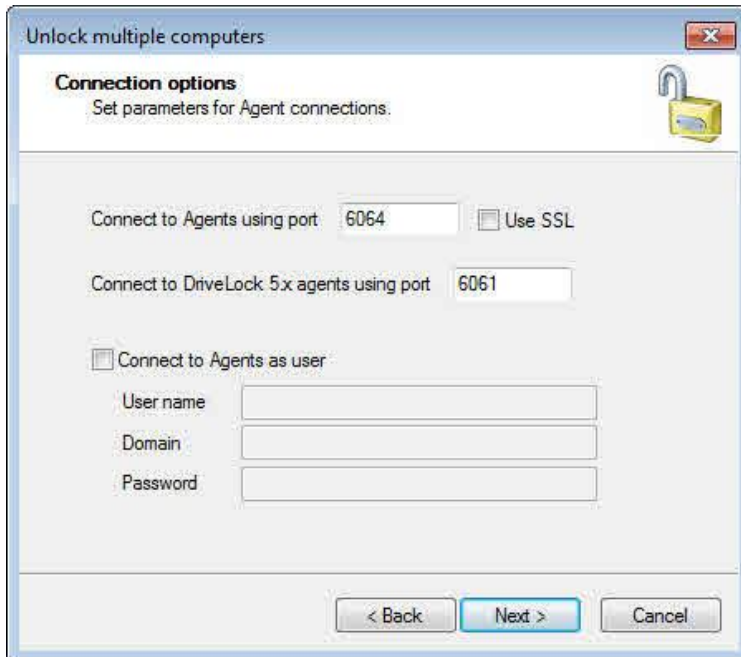


To temporarily suspend drive or device controls on multiple client computers, right-click **Agent remote control** and then select “**Unlock multiple Agents**”.



Click **Add** and then click “**Active Directory Computer or Group**” to select computers from Active Directory or click “**By Name**” to type computer names. The computers you select will be added to the list.

To remove a computer from the list, click the computer and then click **Remove**.
Click **Next** once you have selected all computers to unlock.



The screenshot shows the 'Unlock multiple computers' dialog box with the 'Connection options' tab selected. The dialog has a title bar with a close button. Below the title bar is a sub-header 'Connection options' with a sub-instruction 'Set parameters for Agent connections.' and a yellow padlock icon. The main area contains several input fields and checkboxes: 'Connect to Agents using port' with a text box containing '6064' and a 'Use SSL' checkbox; 'Connect to DriveLock 5.x agents using port' with a text box containing '6061'; and a 'Connect to Agents as user' checkbox. Below this checkbox are three text boxes labeled 'User name', 'Domain', and 'Password'. At the bottom of the dialog are three buttons: '< Back', 'Next >', and 'Cancel'.

Type the port used to connect to the Agent if you configured a non-standard port for Agent communications. To encrypt communications with the Agent, select the **Use SSL** checkbox.

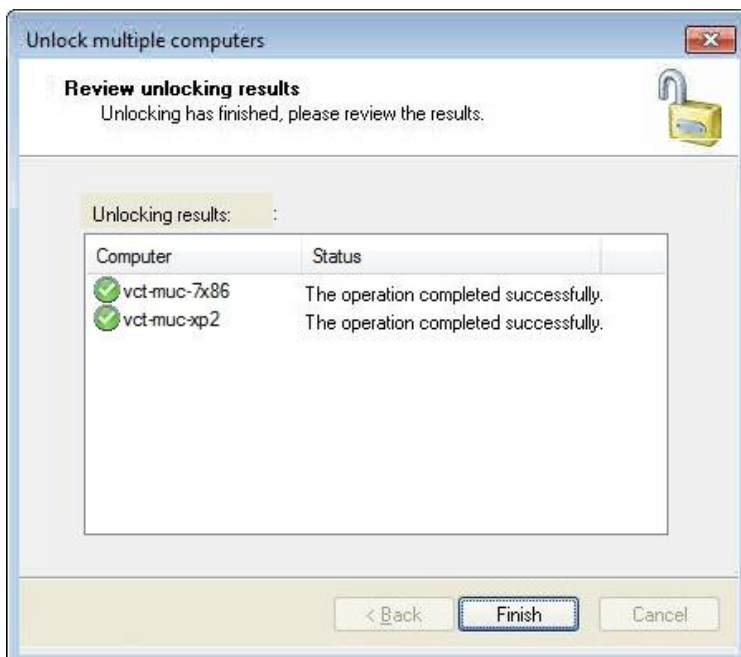
To connect to an Agent by using a different user account, select the **“Connect to Agent as user”** checkbox and type the user name, domain and password.

Click **Next** to continue.

Configure the unlocking settings as described in the section "[Configuring General Unlocking Settings](#)".

Click **Next** to unlock the computers.

After all computers have been unlocked, the results of the operation are displayed.



The screenshot shows the 'Unlock multiple computers' dialog box with the 'Review unlocking results' tab selected. The dialog has a title bar with a close button. Below the title bar is a sub-header 'Review unlocking results' with a sub-instruction 'Unlocking has finished, please review the results.' and a yellow padlock icon. The main area contains a table with the following data:

Computer	Status
✔ vct-muc-7x86	The operation completed successfully.
✔ vct-muc-xp2	The operation completed successfully.

At the bottom of the dialog are three buttons: '< Back', 'Finish', and 'Cancel'.

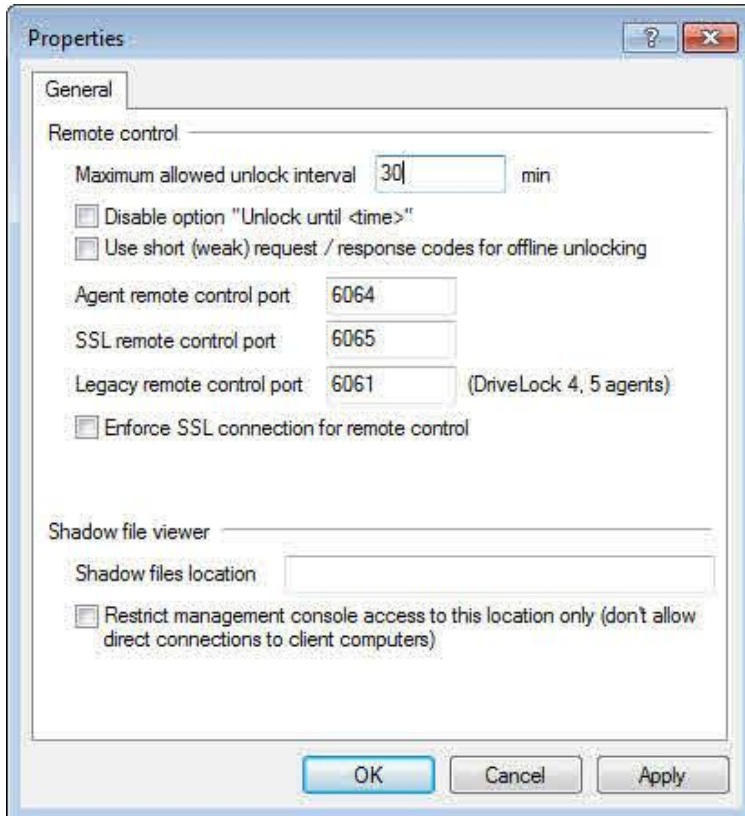
Click **Finish** to close the wizard.

20.3.5 Configuring Default Settings for Agent Remote Control

You can define the requirements and default settings for remote unlocking of Agents, either online or offline. To configure these settings, in the DriveLock Management Console, go to *Extended configuration -> Management console -> Settings*.



Click **Remote control / Operating settings**.



Enter the maximum duration for which an administrator can temporarily unlock a DriveLock Agent remotely. To not restrict the unlocking duration, enter 0.

Select, whether to make the option “**unlock an Agent until a certain point in time**” available for to administrators.

To enable shorter request and response codes used for offline unlocking, select the appropriate checkbox.

Using shorter request / response codes may prevent user errors, such as typing a wrong code, but they are weaker and more vulnerable to brute force attacks.

Select the “**Enforce SSL connection for remote control**” checkbox to always encrypt any remote connections between the Agent and the DriveLock MMC. To use non-default ports for communicating with Agents, type the port numbers in the appropriate fields.



Part XXI

Software Deployment and Update



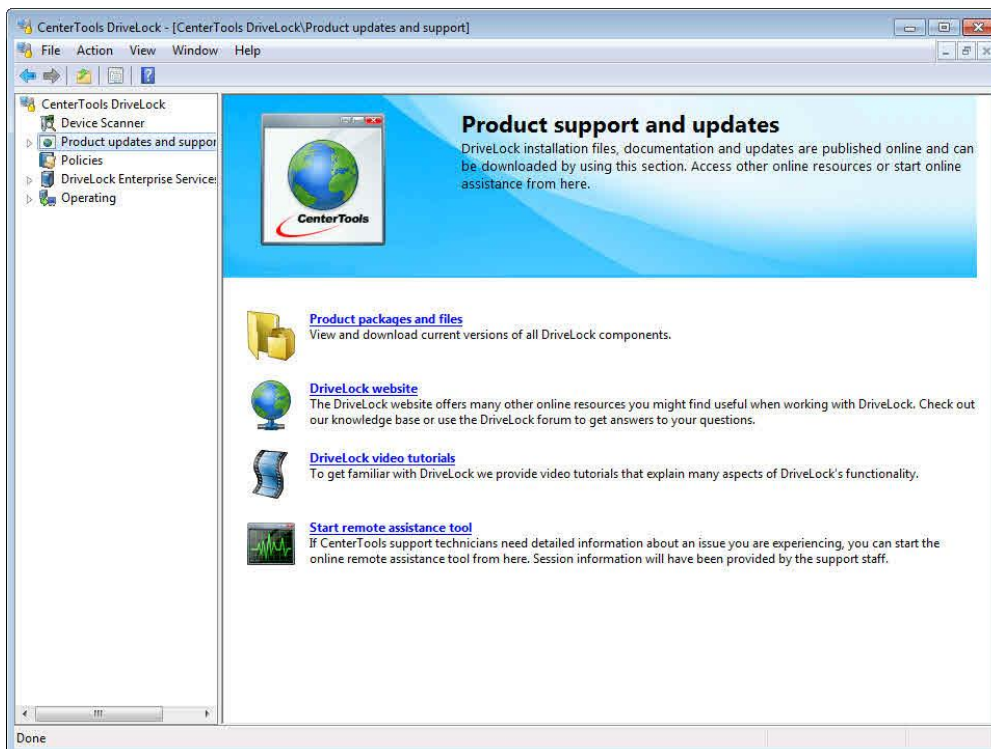
21 Software Deployment and Update

With the [push installation of DriveLock](#) the Agent can be installed on all designated PCs. For a manual push installation, you enter the names of the desired PCs manually in the *DCC / Helpdesk*. or, if you, in the *MMC*, determine appropriate *computer groups / OUs* in the AD, you select the PCs for installation from the PC list in the *DCC / Helpdesk*. If you, in the *MMC*, decide to use the automatic push installation, the configured PCs will be installed fully automatic, synchronized with the determined groups.

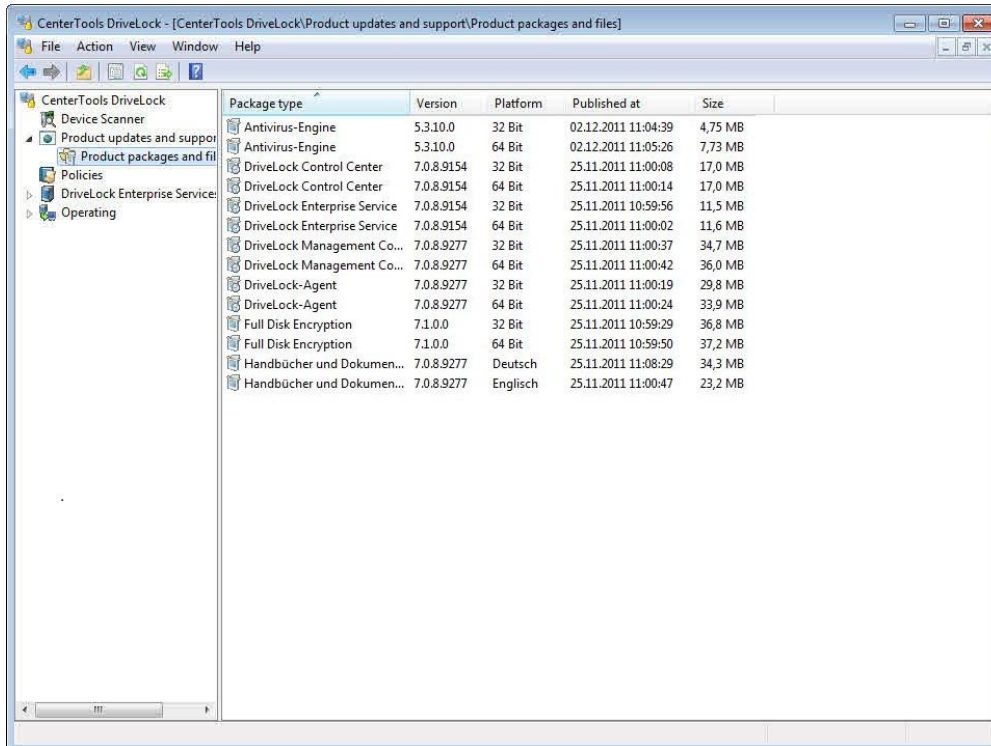
Once DriveLock is installed on a client computer, automatic updates ensure that the DriveLock Agent on client computers is automatically updated as newer versions become available. Once you enable automatic updates, the DriveLock Enterprise Service (*DES*) regularly checks whether Agent updates exist and downloads them as they become available. Client computers then download updates from the *DES* and install them. For more details about this process, refer to the section "[Fully Automatic Updates](#)".

21.1 Manually Updating DriveLock

In the DriveLock Management Console, in the console tree, select **Product updates and support** to view or change settings for updates and other online content.



To directly access available DriveLock installation files without visiting the DriveLock Web site, click **Product packages and files**.

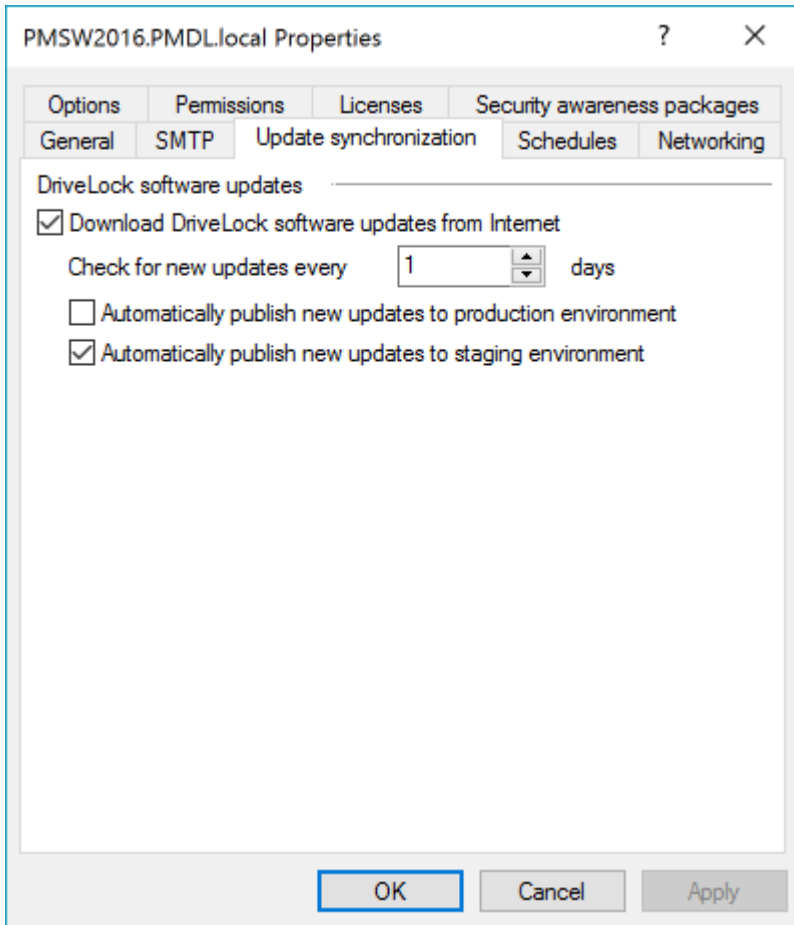


DriveLock packages are Microsoft Installer (MSI) files that install a specific DriveLock component, such as the DriveLock Agent or the DriveLock Control Center. To download one of the available software packages, right-click it and then click **Download**. Once you have downloaded a package, you can install it on a computer manually or by using any automatic software deployment mechanism your organization employs. To view the details of a software package, right-click the package and then click **Properties**.

21.2 Publishing Software Packages

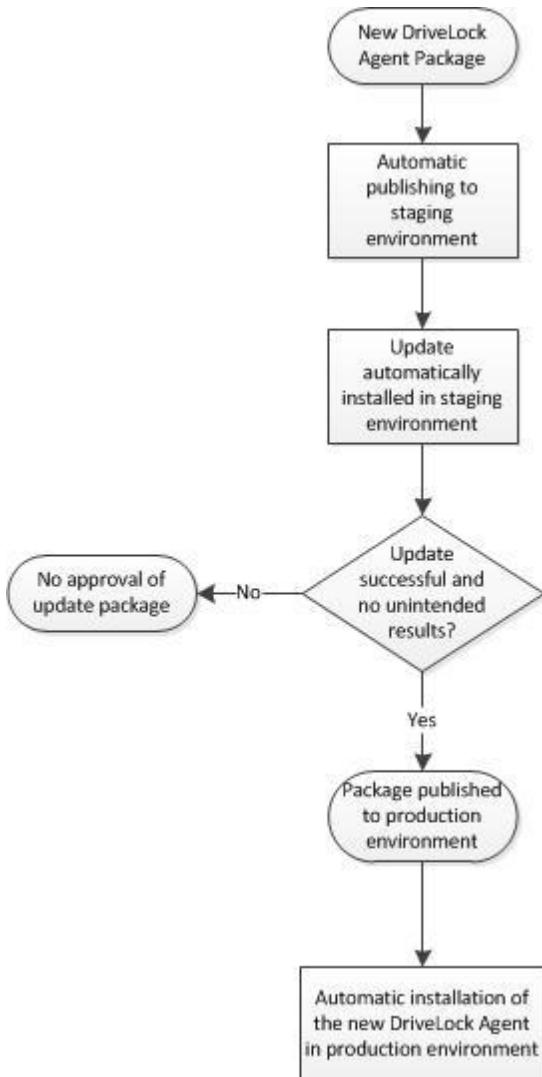
To simplify the deployment of DriveLock packages in organizations that use the DriveLock Enterprise Service (DES), DES servers can automatically download new software packages as they become available and make them available to computers running the DriveLock Agent or other DriveLock components.

By default, DES servers download all new update packages and then make them immediately available to computers that are in a staging network. Some organizations may prefer to have more control over the deployment process. To enable or disable the automatic publishing of product updates, in the DriveLock Management Console right-click **DriveLock Enterprise Services -> Servers -> <server name>** and then click **Properties**. On the *Update* synchronization tab, select or deselect the following checkboxes:



- Automatically publish new updates to production environment (default: not selected)
- Automatically publish new updates to staging environment (default: selected)
- By default, the Download Disk Protection updates checkbox is not selected. Select this checkbox to automatically download updates to the DriveLock Disk Protection (FDE) component. Downloaded FDE updates are used for new installations but the FDE component on DriveLock Agents is not automatically updated.

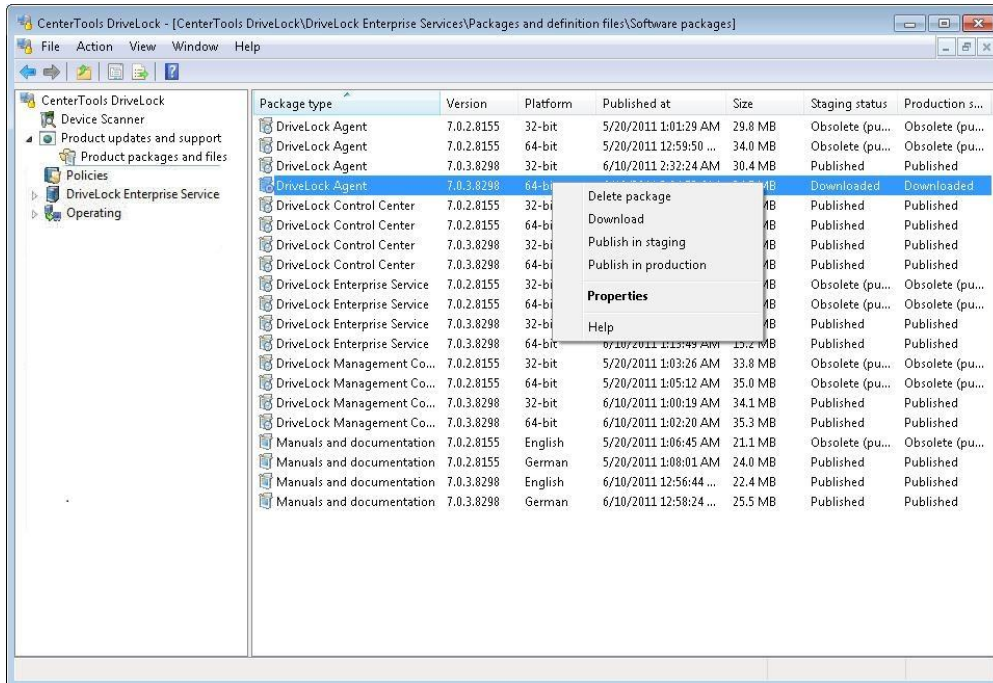
The following diagram illustrates the typical process for updating software in a managed environment where updates are tested in a staging environment before they are rolled out to the production network:



To assign a client computer to the staging or production environment, run one of the following commands on the client computer:

- `drivelock.exe -setstaging ->` Assigns the client to the staging environment
- `drivelock.exe -setproduction ->` Assigns the client to the production environment (default setting)

To determine which updates are distributed to client computers, you configure the staging or production status of a software package. When you change the status of a package, the change takes effect on all DES servers.



The staging and production status can be one of the following:

- **Published:** Clients will download the package and install the update.
- **Downloaded:** Package has been downloaded to the DriveLock Enterprise Service but is not available to clients.
- **Obsolete (downloaded):** Package has been downloaded to the DES but is superseded by a newer package. The package is not available to clients.
- **Obsolete (published):** Package has been downloaded to the DES but is superseded by a newer package. The package is still available to clients until the newer version is published.

DriveLock installs a package only if the status is Published and a previous version of the same package is already installed on the computer. For example, a published DriveLock Control Center (DCC) 7.0.9 package will be installed on a client where version 7.0.8 of the DCC is installed but not on a client where the DCC is not installed.

To change the status of a package, right-click the package and then click one of the following:

- **Delete package:** Remove the package from the DES. You can only delete packages that are not currently published.
- **Download:** Download the package to the DES. Once the package has been downloaded, you need to publish it to make it available to clients.
- **Publish in staging / production:** Make the package available to the staging or production environment.
- **Unpublish from staging / production:** Make the package unavailable to clients in the staging or production environment.

21.3 Push Installation of DriveLock

The push installation of DriveLock supports you, to deploy the DriveLock Agent on your user's PCs.

For the push installation, the DriveLock Enterprise Server regularly checks, if all PCs from the configured AD groups / OUs have an agent installed. If not, the administrator can select this PCs in the DriveLock Control Center DCC /

Helpdesk and initiate the installation. Alternatively he can configure in the *MMC*, that the installations will be started fully automatic

The manual push installation also can be started by the administrator in the *DCC* for particular PCs independent of AD groups / OUs.

The push installation uses an administrative account to push a DriveLock update service (*DIUpdSvc*) to the PC and start it. The *DIUpdSvc* downloads the published DriveLock Agent package from DES executes the installation.

The push installation only starts, if there are both, a 32-bit as well as a 64-bit agent package published for staging and for production.

21.3.1 Per-Server Global Settings

The global settings for the push installation will be configured in the *MMC* independent for each DES. So the settings for several organization can be easily separated.

Open **MMC / DriveLock Enterprise Services / Agent push installation / Per-server global settings / <server name>**

General

Enable synchronization with Active Directory: if checked DES identifies the designated PCs from the configured AD groups / OUs. The PCs without a DriveLock agent can be selected and installed from DCC / Helpdesk.

Enable automatic push deployment: if checked, identified PCs without a DriveLock agent will be installed fully automatic.

Default Settings: this settings will be used for the automatic push installation and also as default for the execution of the push installation from the DCC.

Account for installation: this account requires administrative permissions on the local PC.

Install in staging environment: if enabled, the PCs to be installed will be set to staging environment.

Force reboot after installation: if enabled, the PCs will be rebooted after agent installation without user interaction.

Configuration type: select the type of policy and the policy to be used for the PCs.

21.3.2 Automatic Push Groups / OUs

Open **MMC / DriveLock Enterprise Service / Agent push installation / Automatic push groups / OUs**

Select the computer groups or OUs from the AD to be used for automatic push installation

Right click / New opens the dialog window.

21.3.3 Execute Push Installation

DriveLock Control Center / Helpdesk

Open **DCC / Helpdesk** to start a manual push installation.

If you want to install one or more PCs, which are not listed as known PC, open **Install agent**, select the appropriate *DES* and enter the names of the PCs in *Computer* or use the Computer Selection dialog to add Computers, Groups or OUs from the Active Directory, from an IP-Network scan or from the Network Neighborhood to the list.

If you have configured **Enable synchronization with Active Directory** and **Automatic push groups / OUs** in the *MMC*, all PCs without an agent installation will be listed in *Helpdesk* with status *not installed* or *installation failed*. You can

filter and select this PCs. **Right click / Install** opens the same dialog as for **Install agent** with the names of the PCs already filled in.

Install agent

Published Agent Version: shows the published versions to be installed in staging and production environment.

Advanced: The values configured in **MMC / DriveLock Enterprise Services / Agent push installation / Per-server global settings** are set as default. To change this values, open the *Advanced* settings.

Account for installation: this account requires administrative permissions on the local PC.

Install in staging environment: if enabled, the PCs to be installed will be set to staging environment.

Force reboot after installation: if enabled, the PCs will be rebooted after agent installation without user interaction.

Configuration type: select the type of policy and the policy to be used for the PCs.

Repair Settings: use only, e.g. on request of the DriveLock support, if a former installation failed and a regular update or de-installation does not work.

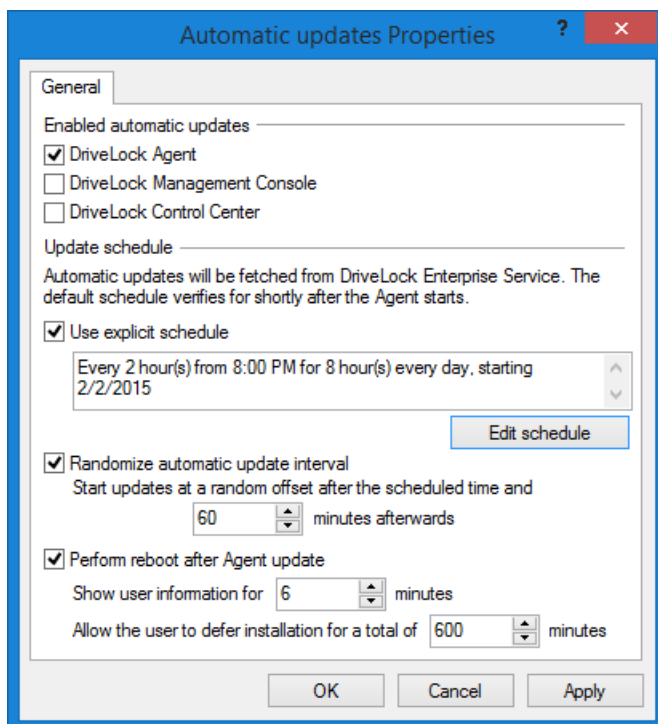
Force removal of installed DriveLock Agents: the DriveLock installation directory, the registry and Microsoft Installer entries we directly deleted.

Ignore other running installations: possibly still running installations will be ignored, installation will be tried anyhow.

21.4 Configuring Automatic Updates

The DriveLock Agents can automatically update themselves and other components to newer versions:

Open **Global configuration / Settings / Automatic updates**.



Check **Enable automatic updates** for the components you want to be updated.

By default, a DriveLock Agent then checks the DES for newer versions of installed components within the first 60 minutes after the Agent service starts and every 60 minutes after the initial check. If a new update is available, the client will immediately download it. To distribute downloads from multiple clients over time, by default clients wait for a random time interval before starting the initial update check.

You can also create your own schedule and select to use your random offset for the initial update.

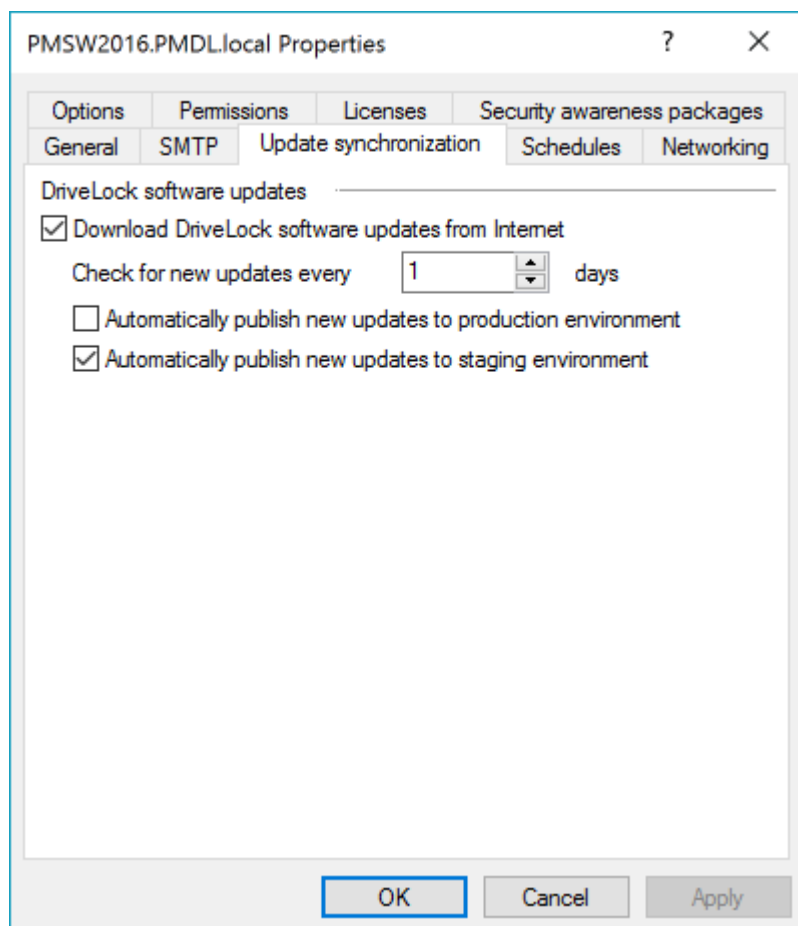
During the update process, DriveLock is inactive for a short period. If you want to assure that the update runs while the system is not in use, check **Perform reboot to update**. Then the user can delay the update for a maximum of N minutes. If they accept or the time is over they will be logged off and the update will be performed before the reboot.

21.4.1 Configuring Fully Automatic Updates

When you configure DriveLock for fully automatic updates, DriveLock components are automatically updated without an administrator's intervention when a new version is made available by DriveLock.

To ensure that fully automatic updates can work correctly, ensure that the DES is configured to automatically download and publish software packages and that clients are configured to automatically download updates from a DES server.

By default, DES servers automatically download all new packages from the Internet. This is configured in the *Properties* dialog box of the DES server on Update synchronization tab by selecting the Download DriveLock software updates from the Internet checkbox.



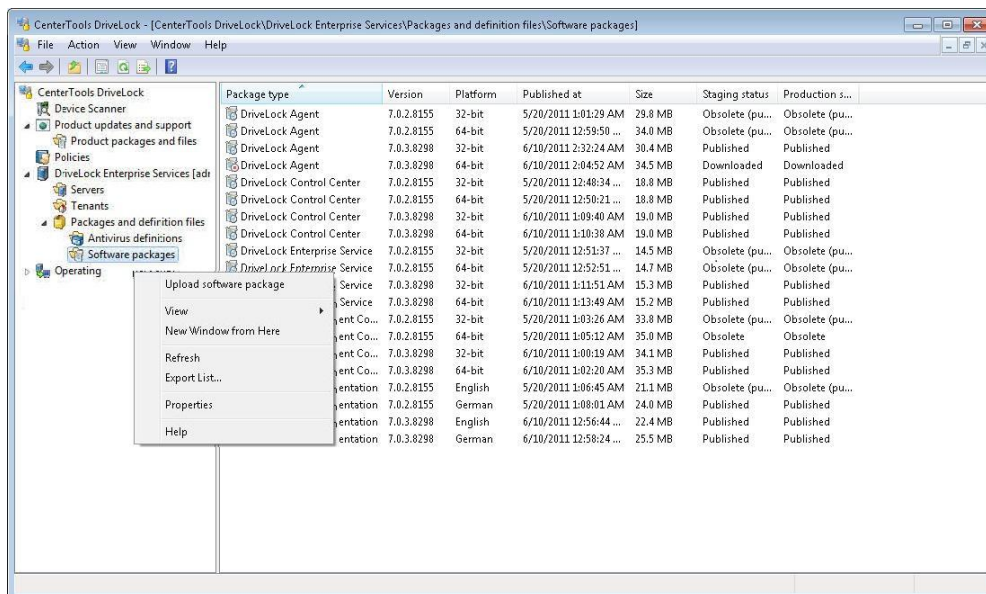
21.4.2 Configuring Semi-Automatic Updates

If you need more control over which packages are downloaded and made available to clients, you can disable automatic publishing, as described in the section [Publishing Software Packages](#), and instead manually publish the

packages and antivirus definitions you want to make available to clients.

An alternative method to configure semi-automatic updates is to configure the DES server to not check for updates. You can then manually download updates or definition files and add only the ones you want to the DES server. To do this, perform the following steps:

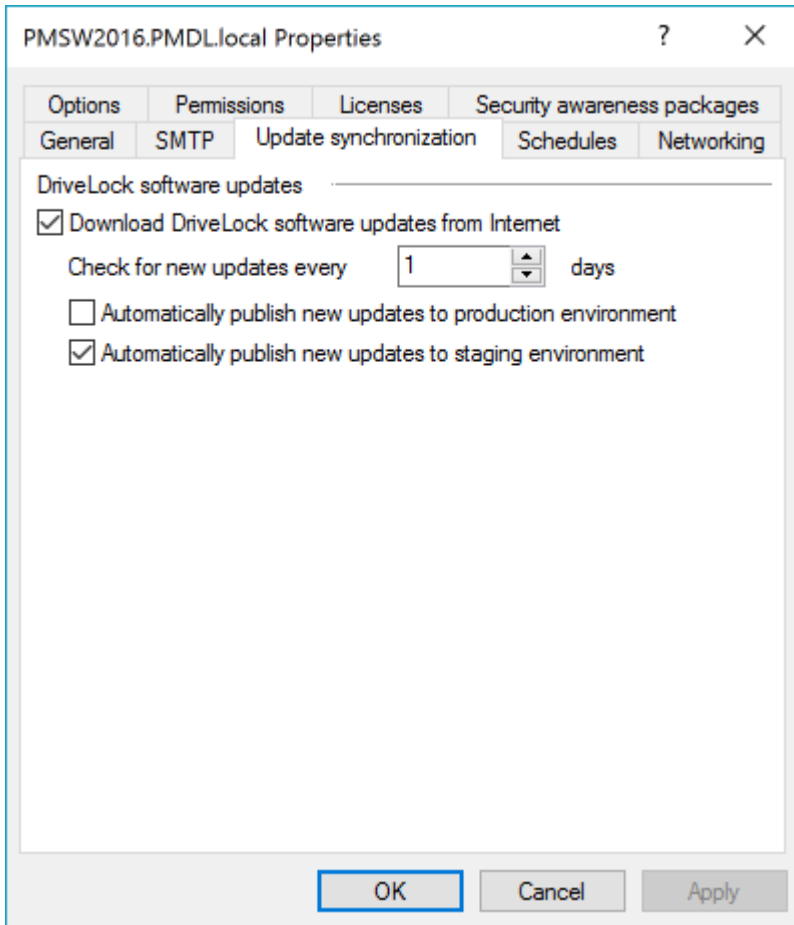
1. Disable the automatic downloading of software packages, as described in the section [Disabling Automatic Package Downloading](#).
2. Check for available packages and download them, as described in the section [Manually Updating DriveLock](#).
3. Go to **DriveLock Enterprise Services -> Packages and definition files -> Software packages**. Right-click **Software packages** and then click **Upload software package**. Select the package you have manually downloaded and then click **Open**.



4. The package status **Downloaded** is displayed for the package. You need to publish the package before it becomes available to clients.

21.4.3 Disabling Automatic Package Downloading

By default, DES servers automatically download all new packages from the Internet and make them available to clients based on your publishing configuration. To disable automatic downloads, in the *Properties* dialog box of the DES server on the *Update* synchronization tab, deselect the *Download DriveLock software updates from the Internet* checkbox.





Part XXII

Using DriveLock in Terminal Server Environments



22 Using DriveLock in Terminal Server Environments

DriveLock can be used in terminal server environments. The drive locking and application control components are available in such configurations. Because terminal server sessions may allow access to drives that are connected to USB ports on the client, DriveLock was designed to control the access to such drives inside a terminal server session.

Terminal server environments may include various forms of client connectivity. The following sections cover each of these environments and explain various scenarios and differences between them, including any limitations of DriveLock's functionality.

22.1 Terminal Server Connections

The following table illustrates which drive control functionality DriveLock provides for different connection types:

Function	Fat Clients	Windows Embedded clients	Virtual-clients	Thin clients by Wyse running Linux V6	Thin clients by other vendors
Access control based on users and groups	Yes	Yes	Yes	Yes	Yes
Access control based on drive letter	Yes	Yes	Yes	Yes	Yes
Access control based on hardware data, incl. serial number	Yes	Yes	Yes	Yes	No
File filter	Yes	Yes	Yes	Yes	Yes
File filter incl. Header inspection	Yes	Yes	Yes	Yes	Yes
File auditing	Yes	Yes	Yes	Yes	Yes
Shadow copies	Yes	Yes	Yes	Yes	Yes
Requires local DriveLock Agent	Yes	Yes	Yes	Plugin for Wyse Linux V6	No
Requires DriveLock Agent on terminal server	No	No	Virtual client used instead of terminal server	Yes	Yes

When using application control on a terminal server, the DriveLock Agent must be installed on the terminal server itself in all environments.

22.1.1 Fat Clients / Desktop Clients

A fat client or desktop client is a regular computer running Windows XP or higher from where you initiate a terminal server client session. When you install the DriveLock Agent on such a computer, device control is enforced at the point where a device is connected, i.e. the client computer. Only the drives and devices that can be accessed according to the computer's DriveLock policy can be used inside a terminal server session.

If the client computer belongs to a domain, the configuration settings can be applied using Group Policy. In other environments, centrally stored policies are recommended.

22.1.2 Windows Embedded Clients

A Windows Embedded client is a client running Windows Embedded XP, Windows Embedded Vista or Windows Embedded 7 that establishes a connection to a terminal server. To enable drive control, the DriveLock Agent must be included in the Windows Embedded image or installed on the client. The local DriveLock Agent controls access to drives and devices and policy settings that are applied to it also apply inside a terminal server session.

If the client computer belongs to a domain, the configuration settings can be applied using Group Policy. In other environments, centrally stored policies are recommended.

22.1.3 Virtual Clients

A virtual client is a virtual machine running Windows XP or higher that is running on a virtual server and is accessed using a thin client or client software. Using a USB-mapping driver, locally attached USB devices can be made available inside the virtual machine.

The DriveLock Agent must be installed on the virtual client. The DriveLock configuration on the virtual client determines which drives a user can access.

If the client computer belongs to a domain, the configuration settings can be applied using Group Policy. In other environments, centrally stored policies are recommended.

22.1.4 Thin Clients

A thin client is a specialized computer running a minimal operating system that lets users establish client sessions to terminal servers. To use DriveLock with thin clients you need to install the DriveLock Agent on the terminal server. The DriveLock configuration on the terminal determines which drives a user can access inside a terminal server session, including any mapped local USB drives.

If the terminal server belongs to a domain, the configuration settings can be applied using Group Policy. In other environments, centrally stored policies are recommended.

22.1.5 Thin Clients by Wyse Running Linux V6

Wyse is a manufacturer of thin clients. Several models of these thin clients are running a hardened version of the Linux V6 operating system. Drives connected to local USB ports on the thin client can be made available inside a terminal server session.

When using such clients, DriveLock must be installed on the terminal server. The DriveLock configuration on the terminal server determines which drives a user can access.

DriveLock has developed a plugin for Wyse Linux V6 (ICA channel only!) that can read hardware data from local USB devices and transmit them to the terminal server using a Virtual ICA-Channel Extension. This allows for the use of whitelist rules that are based on a USB-connected drive's hardware characteristics, such as manufacturer, model and serial number.

To obtain the DriveLock plugin for Wyse clients (for ICA only!), contact DriveLock technical support at support@drivelock.com.

If the terminal server belongs to a domain, the configuration settings can be applied using Group Policy. In other environments, centrally stored policies are recommended.

22.2 Configuring Drive Control

Once you have identified your client environment and connections, you can configure the rules that are required to control access to drives. Based on the type of connection, these rules need to be configured for the client or the terminal server.

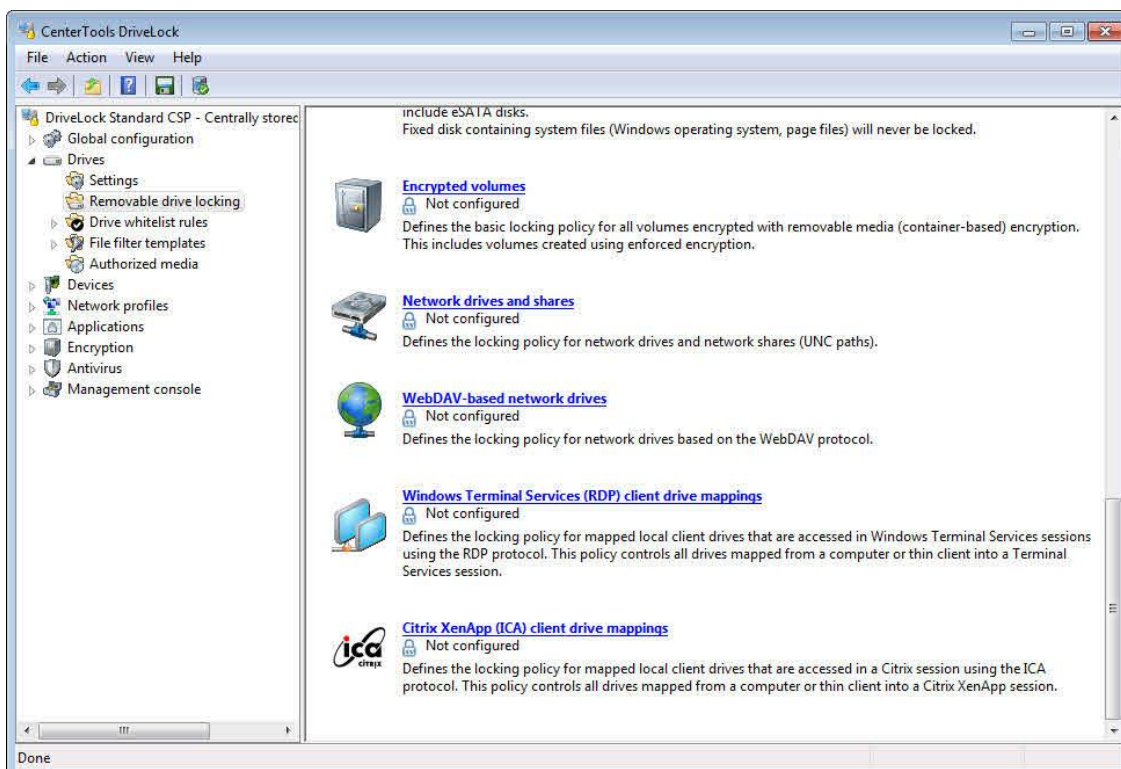
When designing your access control rules you need to identify which types of drives to lock and which exceptions are required. This includes how detailed the rules and exceptions need to be and whether drives need to be locked based on users and groups, drive letter, hardware characteristics or a combination of these factors. When designing these rules you also need to account for any client limitations. For example, rules that include hardware characteristics (such as allowing only Kingston Data Traveler drivers) are not available for all types of clients.

In general, it is recommended to maintain separate DriveLock policies for terminal servers and clients that connect to terminal servers, for example by using separate Group Policy settings.

22.2.1 Global Permissions

The easiest way to assign permissions to locally connected drives is to assign them to all drives, regardless of whether they are CD-ROM drives, hard drives or USB flash drives. You can assign these permissions for each of the following terminal server environments under *Extended configuration* -> *Removable drive locking*:

- *Windows Terminal Services (RDP) client drive mappings*: All drives in client sessions using Remote Desktop Protocol (RDP). This protocol is used by Windows Terminal Services.
- *Citrix Presentation Server (ICA) client drive mappings*: drives in client sessions using Independent Computer Architecture (ICA). This protocol is used by Citrix. This requires Citrix Presentation Server 4.5 (64-Bit) or XEN 5 or higher.



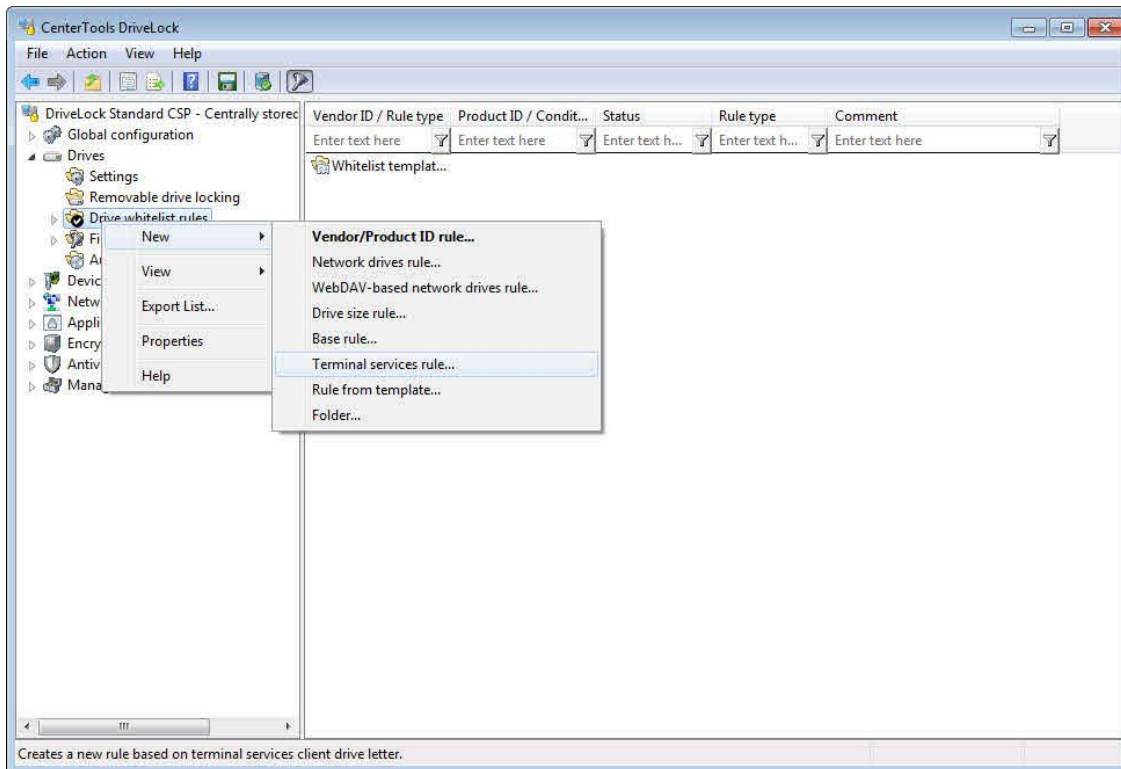
22.2.2 Rules Based on Mapped Drive Letter

To control drives by type (for example, USB-connected drives), you need to configure the terminal server client session so that each drive type is always assigned the same drive letter. Depending on your environment, you may

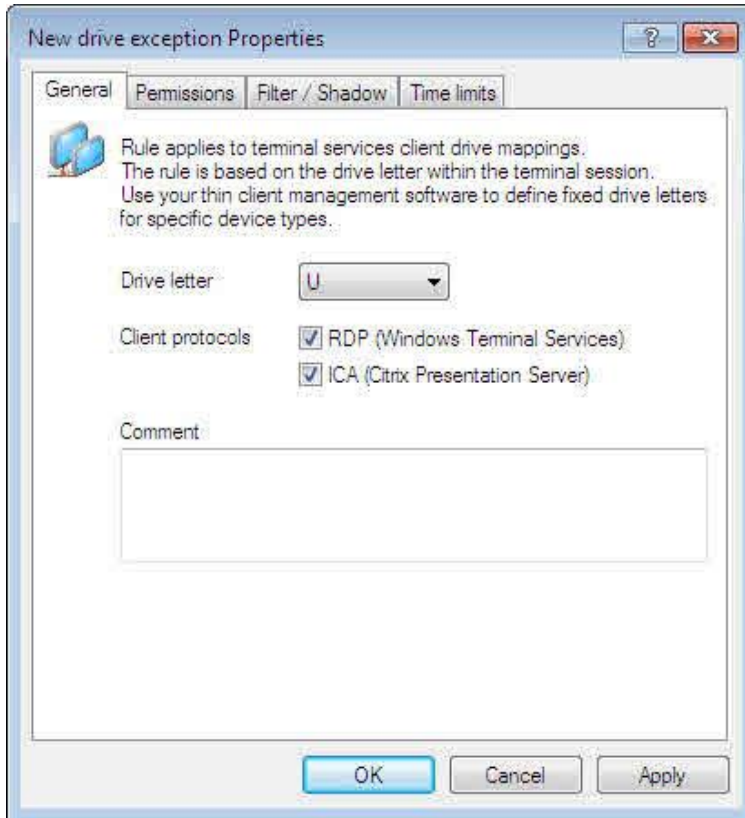
need to configure this on the thin client or in a central session configuration. Once you have ensured that drive letters in client sessions always point to the same types of local drives you can create terminal services rules that apply to these drive letters. Each of these rules can allow or deny access for users and groups or enforce time restrictions.

For example, if a thin client is configured to always make locally connected USB flash drives available using the drive letter U:, you can create a terminal services rule that only lets helpdesk personnel access drive U:. In effect, this restricts the use of all USB flash drives to helpdesk personnel.

To create a new whitelist rule that is based on drive letters, under *Removable drive locking* -> *Drive whitelist rules*, right-click, point to **New** and then click **Terminal services rule**.



Select the appropriate drive letter and then select the protocol or protocols used in your network. You can configure access permissions on the *Permissions* tab.



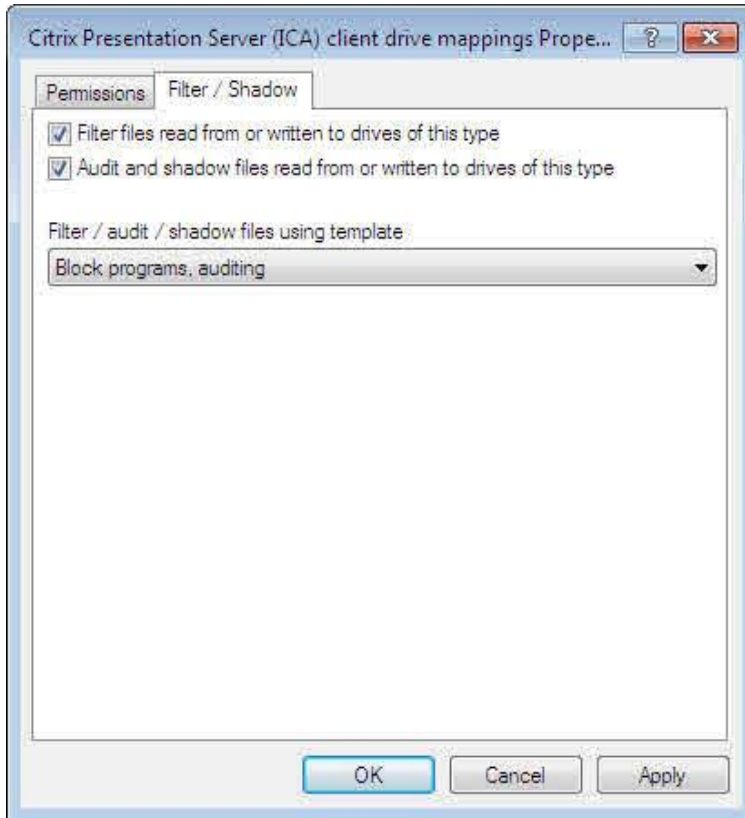
22.2.3 Rules Based on Hardware Characteristics

If the type of client connection supports rules based on hardware characteristics, such as device model or serial number, you can create hardware-dependent whitelist rules as you would for any other DriveLock client under -> *Removable drive locking* -> *Drive whitelist rules* -> *Vendor/Product ID rule*. When specifying the device that the rule will apply to, connect to the client or terminal server (depending on the connection type) and then select the desired drive. You can configure access permissions on the *Permissions* tab.

22.2.4 Using the File Filter

The DriveLock Agent includes a file filter component that can control and audit access to files based on the file type, such as DOC or PDF. You can configure any rule to use the file filter and apply file filter templates. In general, if the terminal server connection type allows for a local installation of the DriveLock Agent, such a configuration is preferable because it provides better file filtering capabilities than a DriveLock Agent running on a terminal server. For more detail about limitations, refer to the table in the section "[Terminal Server Connections](#)".

If the type of client connection supports use of the file filter, you can enable file filtering and auditing under *Drives* -> *Removable Drive locking* -> *Windows Terminal Services client drive mappings* or *Citrix ZenApp (ICA) client drive mappings* on the *Filter/Shadow* tab.



22.3 Using Application Control

Because terminal servers are designed for multiple users to run applications concurrently, using DriveLock Application Control is an important component of a terminal server security strategy. For example, you can use Application Control to block even system programs, such as `cmd.exe`, `wscript.exe`, `cscript.exe` and `mmc.exe` for regular users but allow administrators to access these programs.

Configuring Application Control on a terminal server is identical to the configuring it for other DriveLock clients. For more information about this configuration, refer to the chapter *DriveLock Application Control*.



Part XXIII

Troubleshooting and Tools



23 Troubleshooting and Tools

The complete DriveLock installation includes a command-line based diagnostic tool. Use this tool to diagnose the devices and drives on a computer.

The command line tool “**dlicmd.exe**” is installed in the DriveLock installation folder. DICmd.exe can display various types of diagnostic information, as described in this chapter.

23.1 Viewing Information about Drives and Containers

You have two options for obtaining information on the current status of the agent and its configuration, both for administrators and users:

- Command line
- Agent Tray Icon

Command line

Open the Command Prompt and enter **drivelock -showstatus**:

```
Component licensing status
=====
Device control:      No
Application control: No
Security awareness:  No
Encryption 2-Go:    No
File Protection:     No
Disk Protection:     No
Legacy OS option:    No

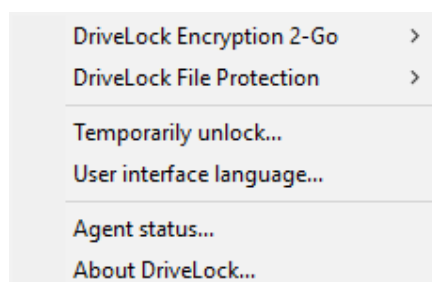
Current agent status
=====
Environment:         Production
FDE special config:  No
Appl. terminal srv.: No
Reboot pending:     No
Temporary unlock:    Not active
Policy config source: Not available (NoStore)
Local config source: Database
  Database file:     C:\ProgramData\CenterTools DriveLock\Config\RSOPCSP_20180704_152151304.db3
  Object ID:         0
  Version:           0
Configuration type:  CSP assignments

Agent configuration
=====
Configuration type:  Policy assignments
```

You get detailed information about the licenses, the configuration and the status of the individual components.

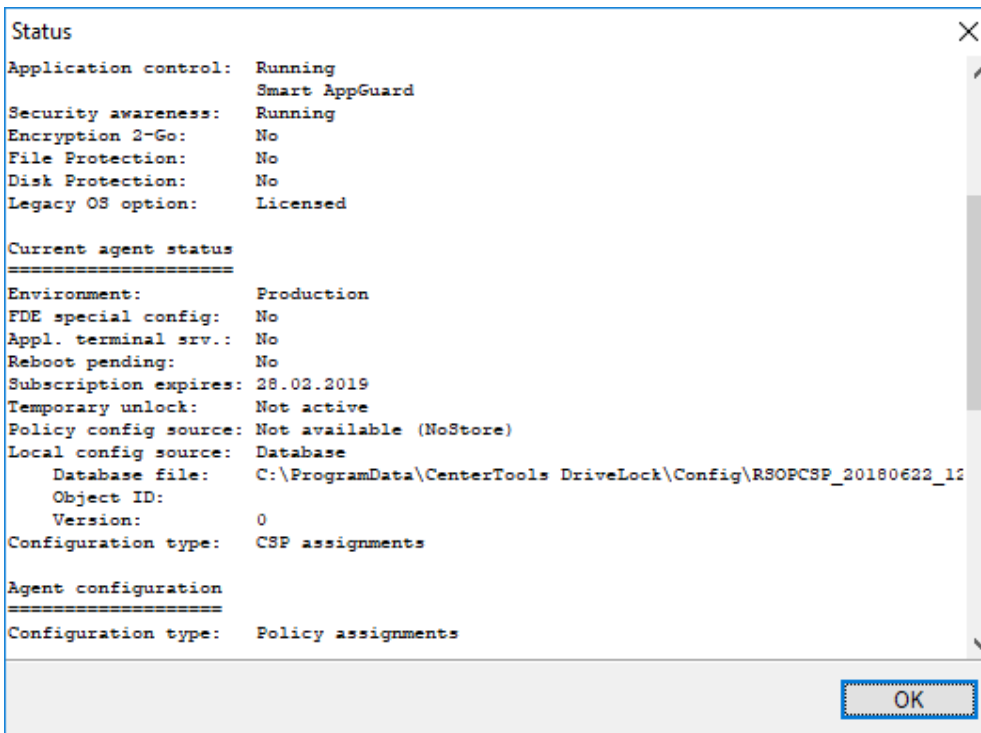
Tray Icon

Right-click the DriveLock Tray Icon to open the context menu:



Select **Agent status**....

This opens a new window where you get the same information as above:



```

Status
Application control: Running
                    Smart AppGuard
Security awareness: Running
Encryption 2-Go:    No
File Protection:   No
Disk Protection:   No
Legacy OS option:  Licensed

Current agent status
=====
Environment:       Production
FDE special config: No
Appl. terminal srv.: No
Reboot pending:   No
Subscription expires: 28.02.2019
Temporary unlock:  Not active
Policy config source: Not available (NoStore)
Local config source: Database
    Database file:  C:\ProgramData\CenterTools DriveLock\Config\RSOPCSP_20180622_12
    Object ID:
    Version:        0
Configuration type: CSP assignments

Agent configuration
=====
Configuration type: Policy assignments
    
```

You can select the text in this window and copy & paste it, if you need to.

23.2 Commands for Troubleshooting

To install DriveLock Event Log message sources, use the command `dlcmd -r`. Use this command if you encounter *"The description for Event ID (0) in Source (DriveLock) cannot be found..."* messages in the Event Viewer.

To run the DriveLock service from a command prompt, use the command `dlcmd -l`. This starts the DriveLock service, but allows you to stop the program by pressing Ctrl-C.

To release all devices, use the command `dlcmd -x`

23.3 Troubleshooting Network Adapters

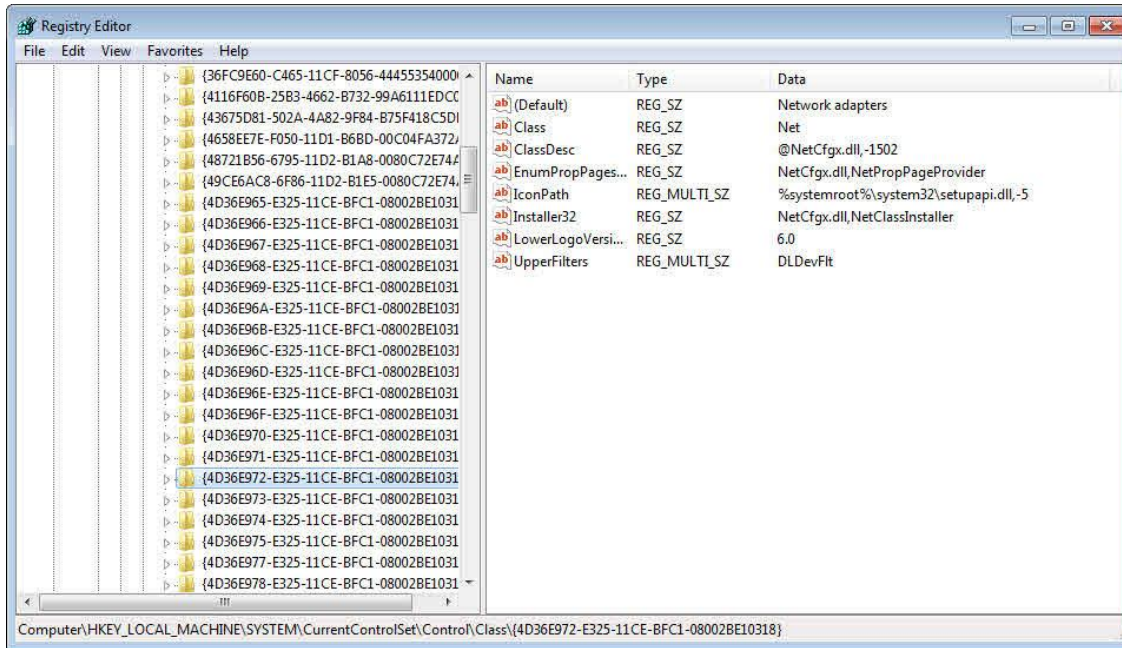
If you configured a policy that blocks all network adapters, the client can no longer receive updates to its configuration over the network. To recover from such a configuration mistake, modify the Windows registry and remove the network adapter configuration.

Before modifying the registry, ensure you have a working backup in case a problem occurs. For information about how to back up, restore and edit the registry, in Windows online help refer to "Restoring Windows registry". If you use Registry Editor incorrectly, you may cause serious problems that may require you to reinstall your operating system. Use Registry Editor at your own risk. DriveLock is not responsible for any consequences of modifying the Windows registry and does not provide support for editing the registry.

Open the Windows registry and navigate to the following registry key:

HKEY_Local_Machine\SYSTEM\CurrentControlSet\Control\Class\{4D36E972-E325-11CE-BFC1-08002BE

To unlock all network adapters, delete the value **"UpperFilters"** and then restart the computer.



23.4 Creating a Trace File

DriveLock support staff may ask you to create a trace file, which contains detailed information about the internal processing of DriveLock. DriveLock can generate several trace files, including the following:

- *DriveLock trace file*. This file helps in analyzing general problems.
- *DriveLock driver trace file*. This file helps in analyzing device driver-related problems.

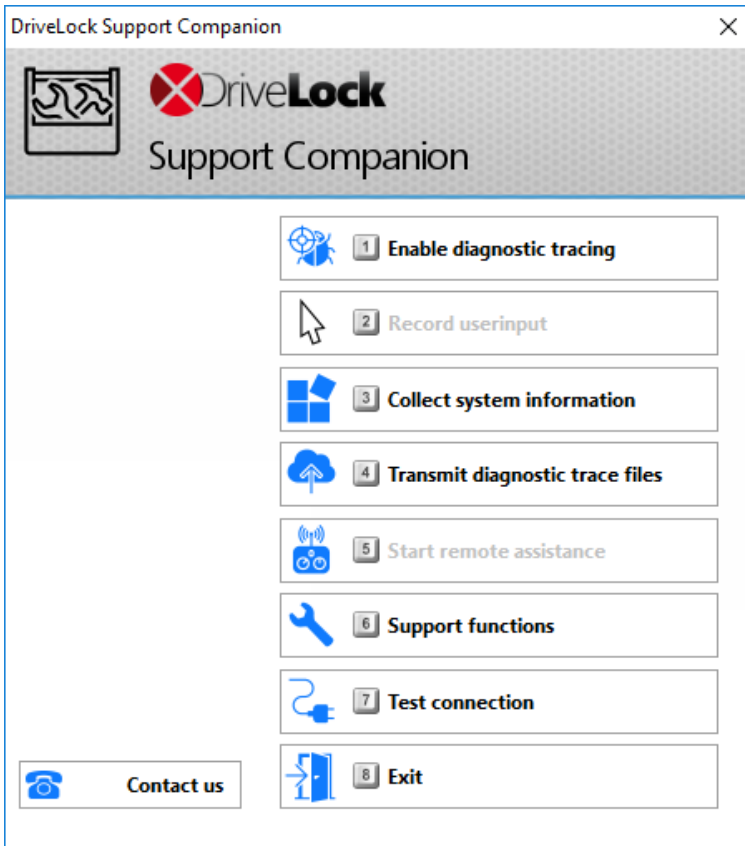
You can create a trace file by using a command line or the DriveLock Management Console. You can also activate tracing by using the DriveLock Support Tool, **DLSupport.exe**, which is located in the folder where you installed the DriveLock Management console.

Trace files are created in the root ("C:\trace") of the connected computer. If needed, you can create your own trace path with the following registry key: HKEY_LOCAL_MACHINE\Software\CenterTools\TraceLog - value: GlobalLogPath (REG_SZ)

23.4.1 Creating a DriveLock Driver Trace File by Using the Support Tool

The easiest method for creating a trace file is by running the DriveLock Support Companion on the computer that is experiencing a problem. To start this program, run one of the following files:

- *DISupport.exe*: Installed with the DriveLock Management Console. Contains the Team Viewer component for remote access by DriveLock support.
- *DISupportAgent.exe*: Installed with the DriveLock Agent. Contains no remote access component. In most cases you will use this program



Once you have located the DriveLock Support Companion, perform the following steps:

1. Start the DriveLock Support Companion as a local administrator and then click **Enable diagnostics tracing**.
2. Restart the computer.
3. Reproduce the problem you are experiencing. This may require you to log on using the account of an affected user.
4. Start the DriveLock Support Companion as a local administrator and then click **Collect system information**. The DriveLock Support Companion collects data to help analyze the problem, stores it in the folder C:\Trace and transfers it to the DriveLock support server.

Trace data contains the following information:

- All tracing files, which include detailed information about DriveLock operations
- Several registry files and hardware details
- Group Policy settings (GPresult.log)
- System information (Sysinfo.csv)
- Windows Application Log events
- Contents of the DriveLock working directory and cache

23.4.2 Creating a DriveLock Driver Trace File by Using the Command Line

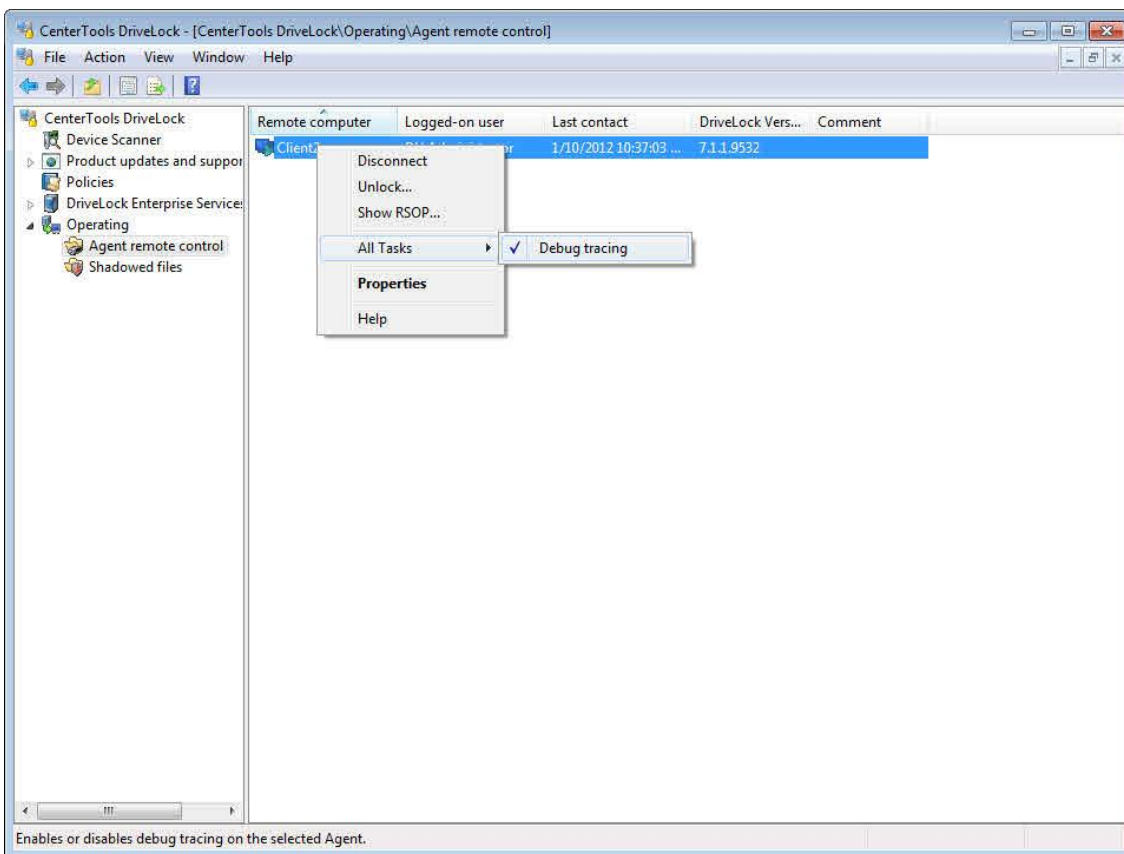
To create a driver trace file, perform the following steps:

- Stop the DriveLock service.
- Open a command prompt window.

- Navigate to the DriveLock installation folder (default installation path for an administrative installation: “C:\Program Files\CenterTools\DriveLock”, default installation path for a client-only installation: “C:\Program Files\CenterTools\DriveLock”)
- Type the command `drivelock.exe -enabledrivertracing`
- Start the “DriveLock” service
- Perform the steps required to re-create any problems
- Tracing creates the file “c:\dldevft.log” .
- Send this file to DriveLock support.
- To disable tracing, stop the “DriveLock” service and then type the command `drivelock.exe -disabledrivertracing`
- Start the “DriveLock” service again

23.4.3 Creating a DriveLock Trace File by Using the Management Console

To enable trace file creation by using the DriveLock Management Console, connect to the remote PC using “**Agent remote control**”.



Right click the connected computer and then click “**All Tasks -> Debug tracing**”.

This option creates the DriveLock trace file and the DriveLock driver trace file. Trace files are created in the root directory of the remote client computer. To disable creation of trace files, deselect “**Debug tracing**”.

23.4.4 Generating BitLocker-specific system information

DLSupportAgent.exe collects additional information about customer systems to help diagnose errors with BitLocker Management, DriveLock PBA and Disk Protection. The following commands are evaluated:

BitLocker Management:

- manage-bde -status
- echo list vol | diskpart
- echo list disk | diskpart
- bdehdcfg -driveinfo

Disk Protection / DriveLock PBA:

- dlfduser /l
- dldispefs /all

BitLocker Management, Disk Protection / DriveLock PBA:

- bcdedit /enum all

23.5 Manually Refreshing the Policy

You can force a refresh of the Group Policy on a remote client computer or instruct it to re-load its configuration file by using the DriveLock Management Console. To perform this task you must be connected to the remote computer. For more information about this task, refer to the section "[Using Agent Remote Control](#)".

Administration Guide

Die in diesen Unterlagen enthaltenen Angaben und Daten, einschließlich URLs und anderen Verweisen auf Internetwebsites, können ohne vorherige Ankündigung geändert werden. Die in den Beispielen verwendeten Firmen, Organisationen, Produkte, Personen und Ereignisse sind frei erfunden. Jede Ähnlichkeit mit bestehenden Firmen, Organisationen, Produkten, Personen oder Ereignissen ist rein zufällig. Die Verantwortung für die Beachtung aller geltenden Urheberrechte liegt allein beim Benutzer. Unabhängig von der Anwendbarkeit der entsprechenden Urheberrechtsgesetze darf ohne ausdrückliche schriftliche Erlaubnis der DriveLock SE kein Teil dieser Unterlagen für irgendwelche Zwecke vervielfältigt oder übertragen werden, unabhängig davon, auf welche Art und Weise oder mit welchen Mitteln, elektronisch oder mechanisch, dies geschieht. Es ist möglich, dass DriveLock SE Rechte an Patenten bzw. angemeldeten Patenten, an Marken, Urheberrechten oder sonstigem geistigen Eigentum besitzt, die sich auf den fachlichen Inhalt dieses Dokuments beziehen. Das Bereitstellen dieses Dokuments gibt Ihnen jedoch keinen Anspruch auf diese Patente, Marken, Urheberrechte oder auf sonstiges geistiges Eigentum, es sei denn, dies wird ausdrücklich in den schriftlichen Lizenzverträgen von DriveLock SE eingeräumt. Weitere in diesem Dokument aufgeführte tatsächliche Produkt- und Firmennamen können geschützte Marken ihrer jeweiligen Inhaber sein.

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.

DriveLock and others are either registered trademarks or trademarks of DriveLock SE 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.