How to use DriveLock with Igel Thin-Clients

Table of Contents

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.

2 Securing Your Data with DriveLock

DriveLock is a lightweight software solution that helps you secure your desktop computers. It has a Multilingual User Interface (MUI), allowing you to select the desired language during installation or when running the program.

DriveLock offers dynamic, configurable access control for mobile drives (floppy disk drives, CD-ROM drives, USB memory sticks, etc.). DriveLock also lets you control the use of most other device types, such as bluetooth transmitters, printers, cameras, smart phones, media devices and many more. By configuring whitelist rules based on device type and hardware ID you can define exactly who can access which device at which time. Removable drives can be controlled based on the drive's manufacturer, model and even serial number. This lets you define and enforce very granular access control policies. Additional features let you unlock specific authorized media and define time limits or computers for whitelist rules. Authorized administrators can even temporarily suspend device blocking on a computer, if required, even when the computer is offline and not connected to a network.

Installation of the client software (the DriveLock Agent) and policy deployment can be achieved easily by using existing software deployment mechanisms or by using the Group Policy feature of Active Directory. Alternatively, you can distribute policies using configuration files for standalone computers or in environments without Active Directory (for example Novell).

The auditing capabilities of DriveLock, coupled with its file shadowing functionality, give you the information you need to monitor and enforce policy compliance. By using the DriveLock Device Scanner you can detect any drive or device that has been used in your network, even if it is no longer connected to the computer. The DriveLock Agent doesn't need to be installed on the target computers to use the Device Scanner.

Encryption is another main feature of DriveLock. DriveLock can help you secure sensitive information by enforcing encryption when data is copied to removable drives. You can use the DriveLock Full Disk

Encryption option to encrypt hard disks, including the system partition and to perform pre-boot authentication with single sign-on to Windows. DriveLock can also erase sensitive data permanently and securely by overwriting data multiple times using one of several industry-standard algorithms.

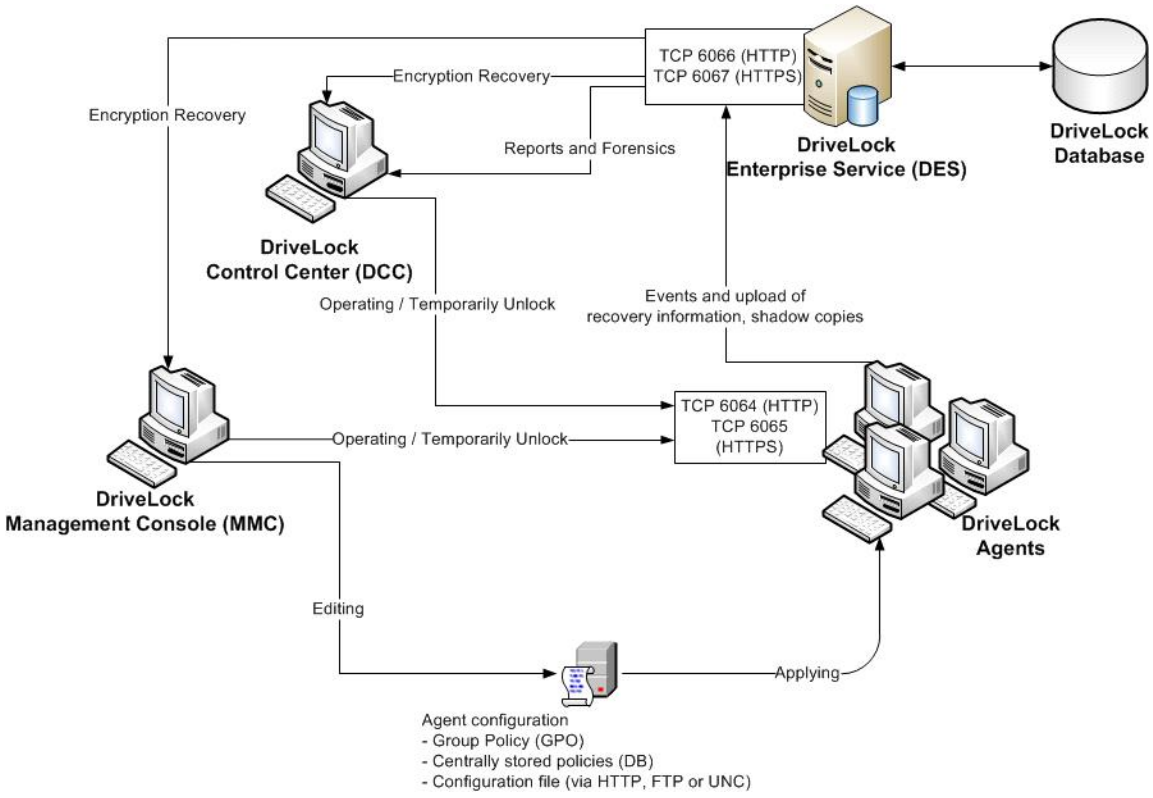
DriveLock's application control enables easy control over which applications run on a computer. You can allow or deny the starting of applications based on several criteria, such as the current user, network connection or computer.

The DriveLock Enterprise Service (DES) is a central component that consolidates all DriveLock events and Device Scanner results in a central database. Administrators can then use this data to create dynamic reports for auditing and management purposes.

A single, unified DriveLock Management Console is used to configure all DriveLock components, which simplifies administration tasks.

2.1 The DriveLock Components

This section describes the DriveLock components and how they communicate with each other.



2.1.1 DriveLock Agent

The DriveLock Agent is the most important component of the DriveLock infrastructure. It implements and enforces your policy settings and must be installed on every computer where you want to control removable drives, devices or other settings. The Agent is a lightweight Windows service that runs in the background and maintains control over hardware ports and interfaces and enforces your security policy. To prevent unauthorized access or bypassing of the security settings, regular users can't stop the service; only users who are specifically authorized by you can access and control the service.

Using DriveLock in IGEL thin client environments the DriveLock Agent must be installed and configured on the terminal server, the Citrix XenApp server respectively.

2.1.2 DriveLock Management Console

You use the DriveLock Management Console to configure the security settings for your clients, manage your environment and access other DriveLock components. This console is a Microsoft Management Console (MMC) snap-in so you can easily integrate it into existing MMC console files that administrators may have already configured.

The DriveLock Management Console lets you create central stored configurations. that will be assigned to computers or groups. Or you may define configurations by creating and changing Active Directory Group Policy settings.

You can also monitor the status of clients or access the DriveLock Agent on clients. You can use the Management Console to remotely unlock an Agent by accessing it remotely, or - if the Agent is not connected to a network - by creating an offline access code that a user can enter on the client computer. In addition, the Device Scanner is integrated into the DriveLock Management Console.

2.1.3 DriveLock Control Center

The DriveLock Control Center (DCC) lets you create dynamic reports and forensic analysis reports from events that were reported by DriveLock Agents data to a central server running the DriveLock Enterprise Service (DES). You can use the DCC to monitor the use of mobile drives, devices and data transfers in aggregate or in detail. The DCC includes the option to assign granular permissions for data queries and report creation.

For example, you can create reports about the use of removable media and device connection attempts (both allowed and blocked). In addition, you can create reports about which files have been written to or read from removable media and execute a forensic analysis by using the data drill-down capabilities of the DCC. The settings in your DriveLock policy determine what types of data are recorded.

The DCC also lets you monitor your current DriveLock Agent environment and view the status of clients. For example, you can identify computers that don’t have the Agent installed or that have not recently reported their status. If you use the Full Disk Encryption option, you can view the current status of the drive encryption (for example, “Not installed” or “Currently encrypting”). You can also easily group and filter the list of Agents. All of these functions and the ability to view statistics as graphs make the DCC a very powerful monitoring and reporting tool.

2.1.4 DriveLock Enterprise Service

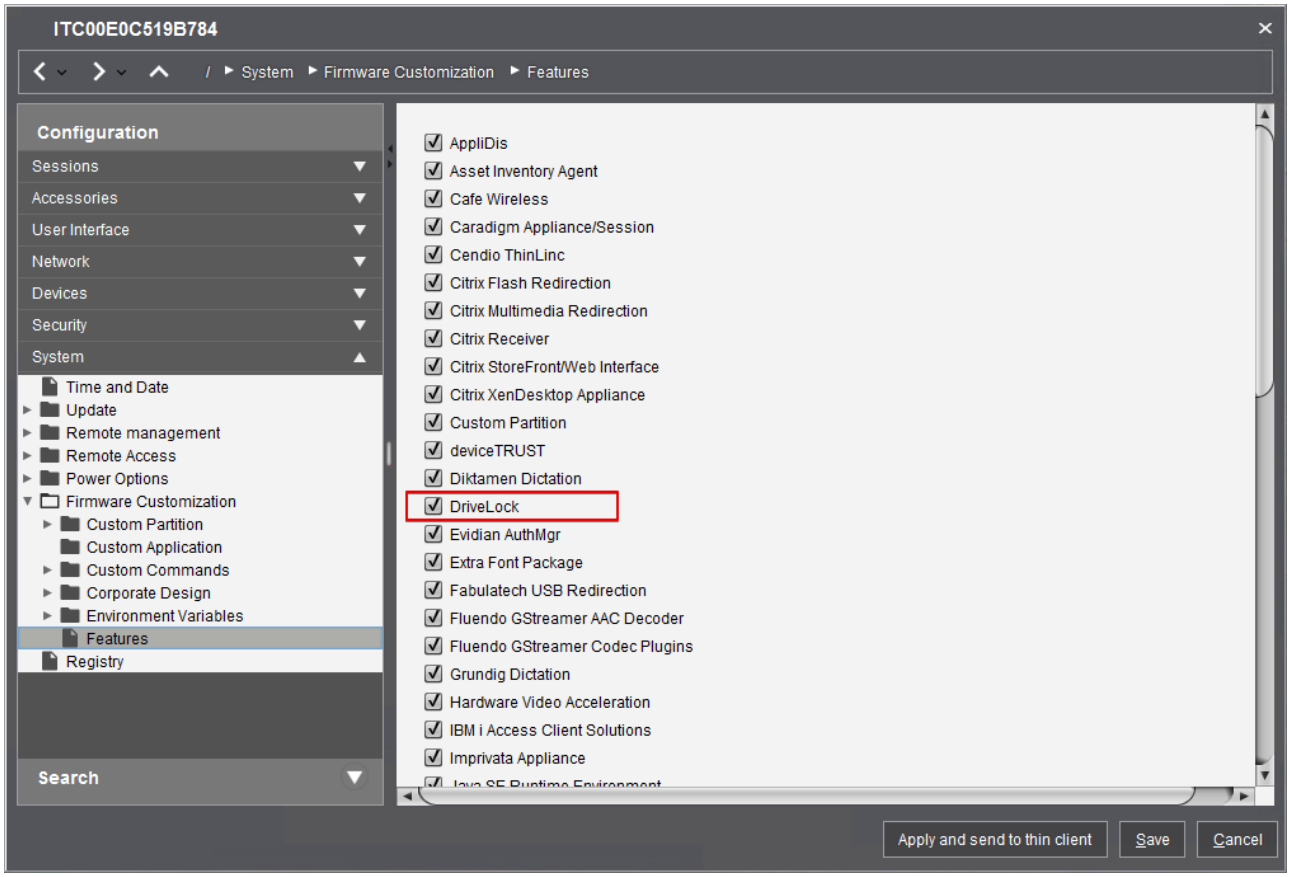
The DriveLock Enterprise Service (DES) centrally stores events from all DriveLock Agents. This service is not required for DriveLock to operate, but it lets administrators easily monitor all DriveLock operations and user activities in the entire organization. The DES replaces the Security Reporting Centers (SRC), which performed similar functions in DriveLock 5. The DES uses a new architecture and database structure to improve performance and add new functionality. The DriveLock Control Center (DCC) is the reporting console that enables administrators to view events that are stored in the DES and create reports from the event data.

Organizations that use one or both encryption modules (Encryption 2-Go or Full Disk Encryption) can use the DES to centrally store recovery data to simplify and streamline data recovery operations.

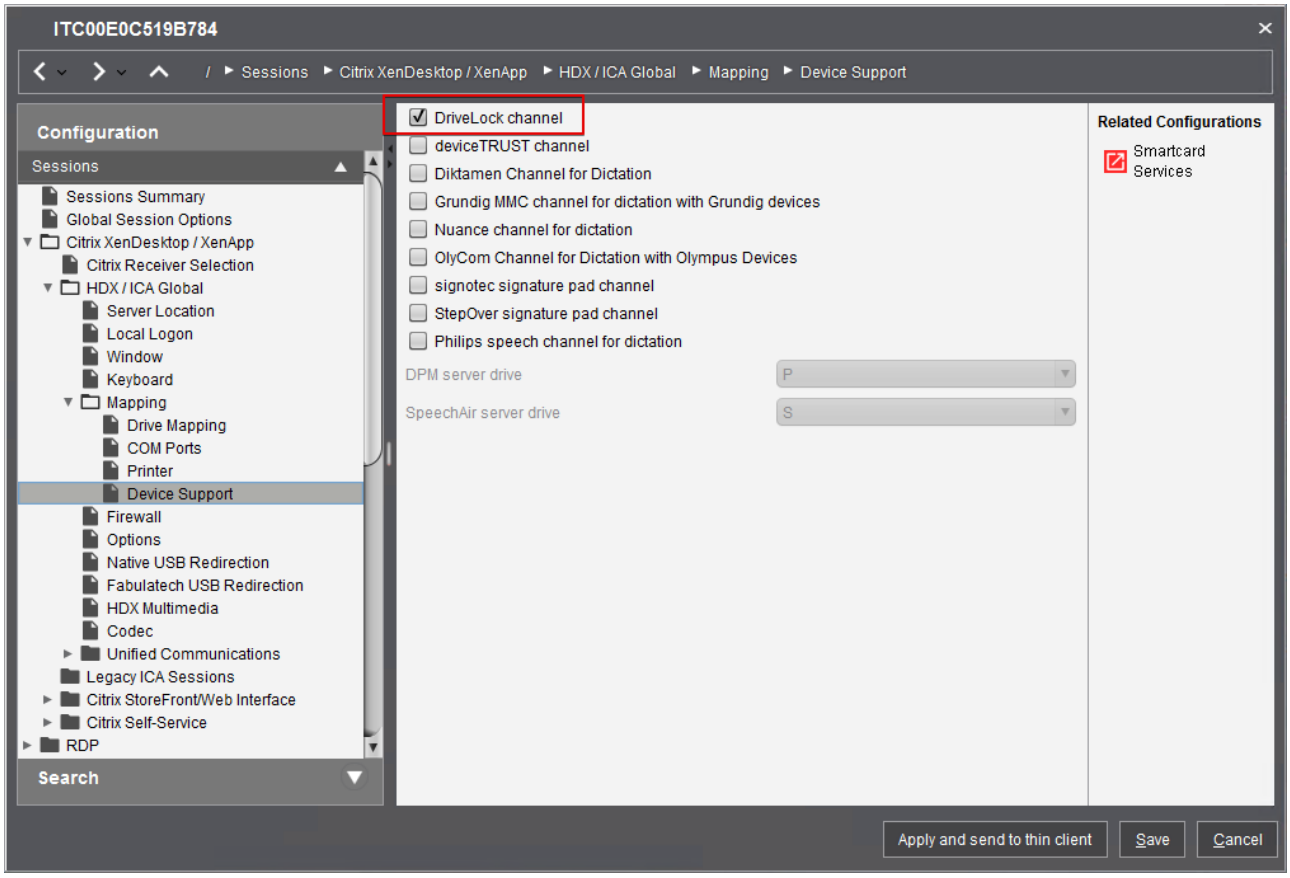
3 Configuring your IGEL Thin Client

The DriveLock Virtual Channel has been directly implemented into Igel's Linux Universal Desktop and can be activated within the Universal Desktop setup.

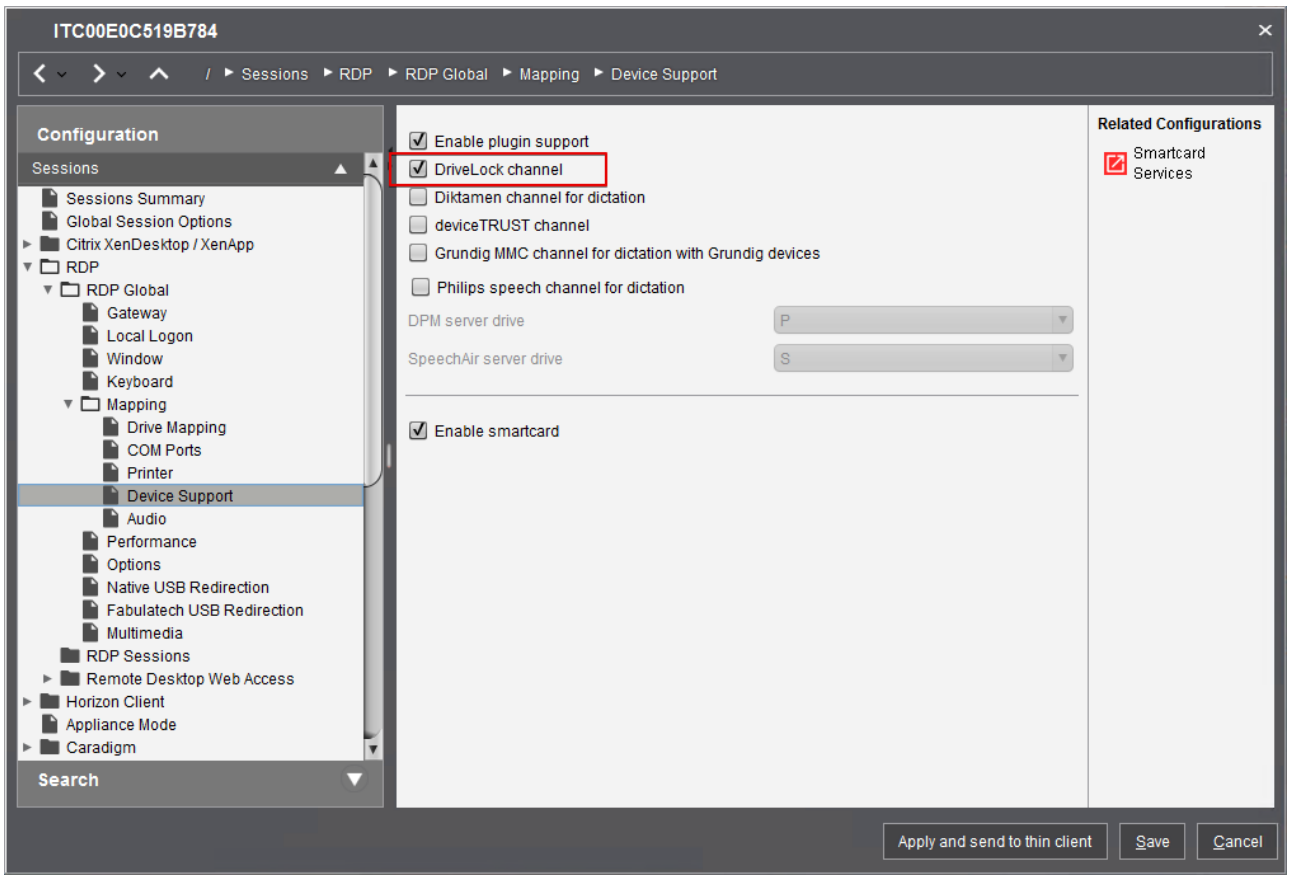
First, check if the DriveLock feature is enabled on your system:



Next, make sure the DriveLock channel is enabled under **Device Support**:

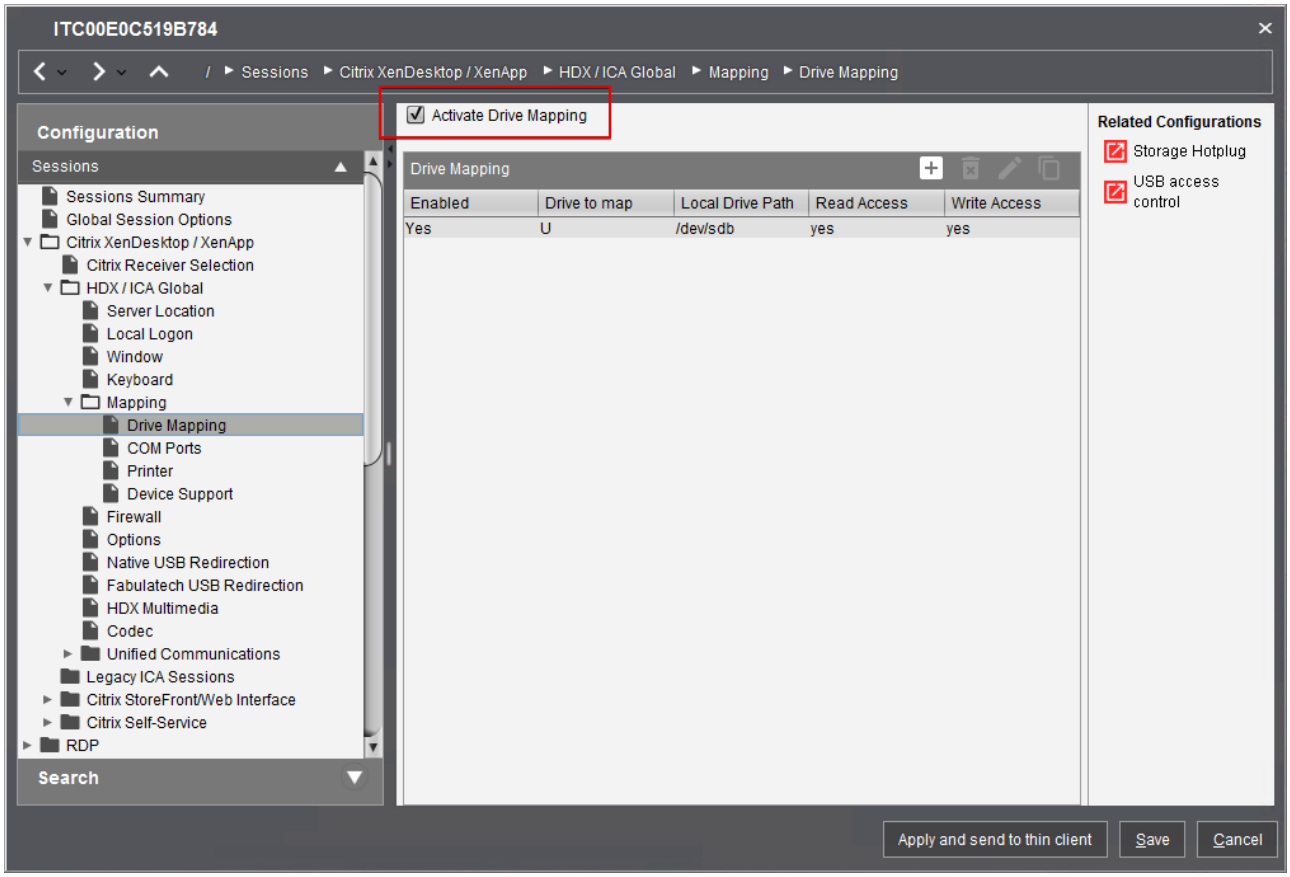


The same setting needs to be activated, in case you use RDP as protocol:

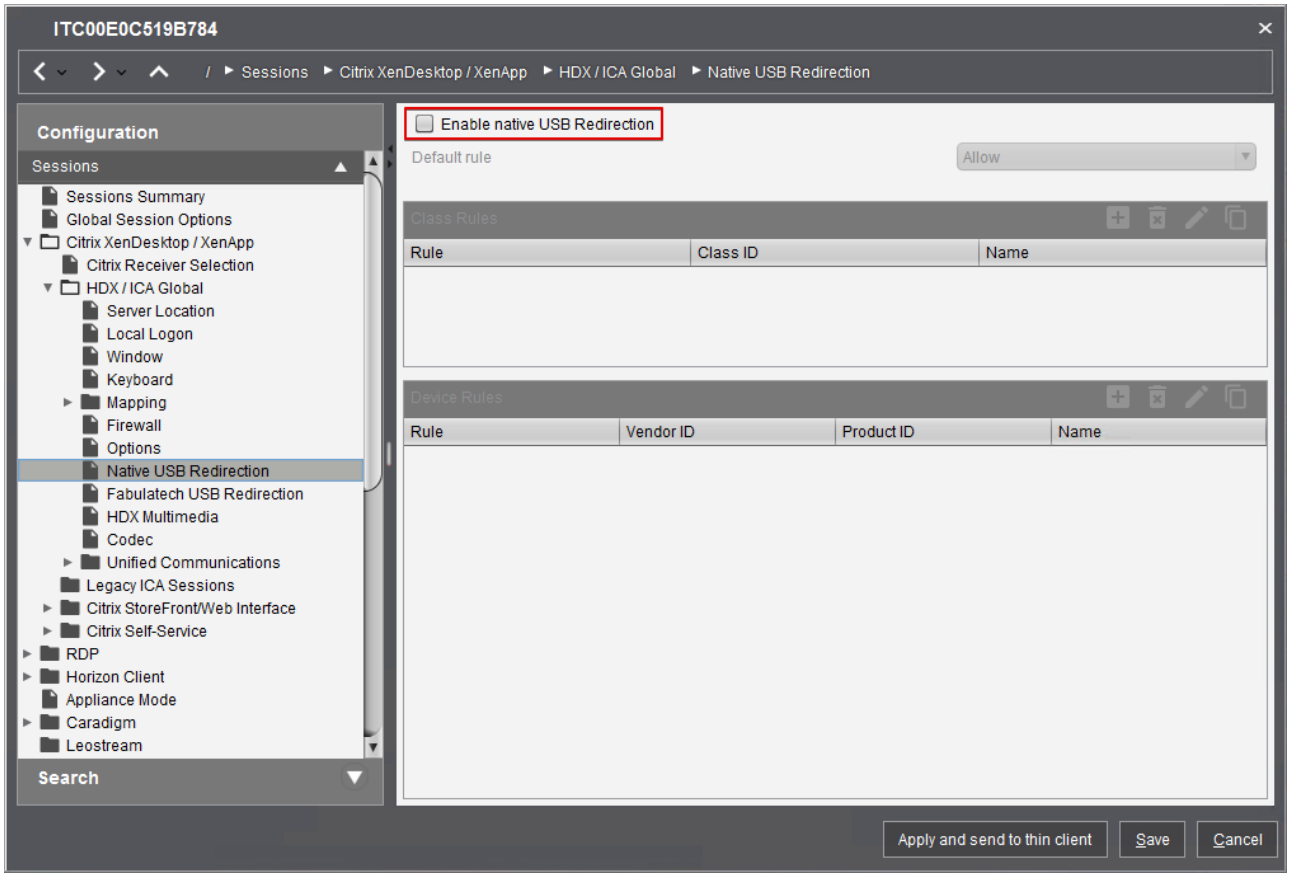


> Please notice: If you use Igel Universal Management Suite (UMS) for central configuration of your Igel Thin Clients, you need to use the latest version of UMS to activate the DriveLock Virtual Channel. If you use Profiles in USM, please optimize the existing profiles for the latest Firmware to activate the Virtual Channel for your existing Profiles. (The configuration point is not visible, if the profile is optimized for an older Firmware).

You also need to activate the drive mapping, so any attached USB device will be available as a drive within your terminal session:

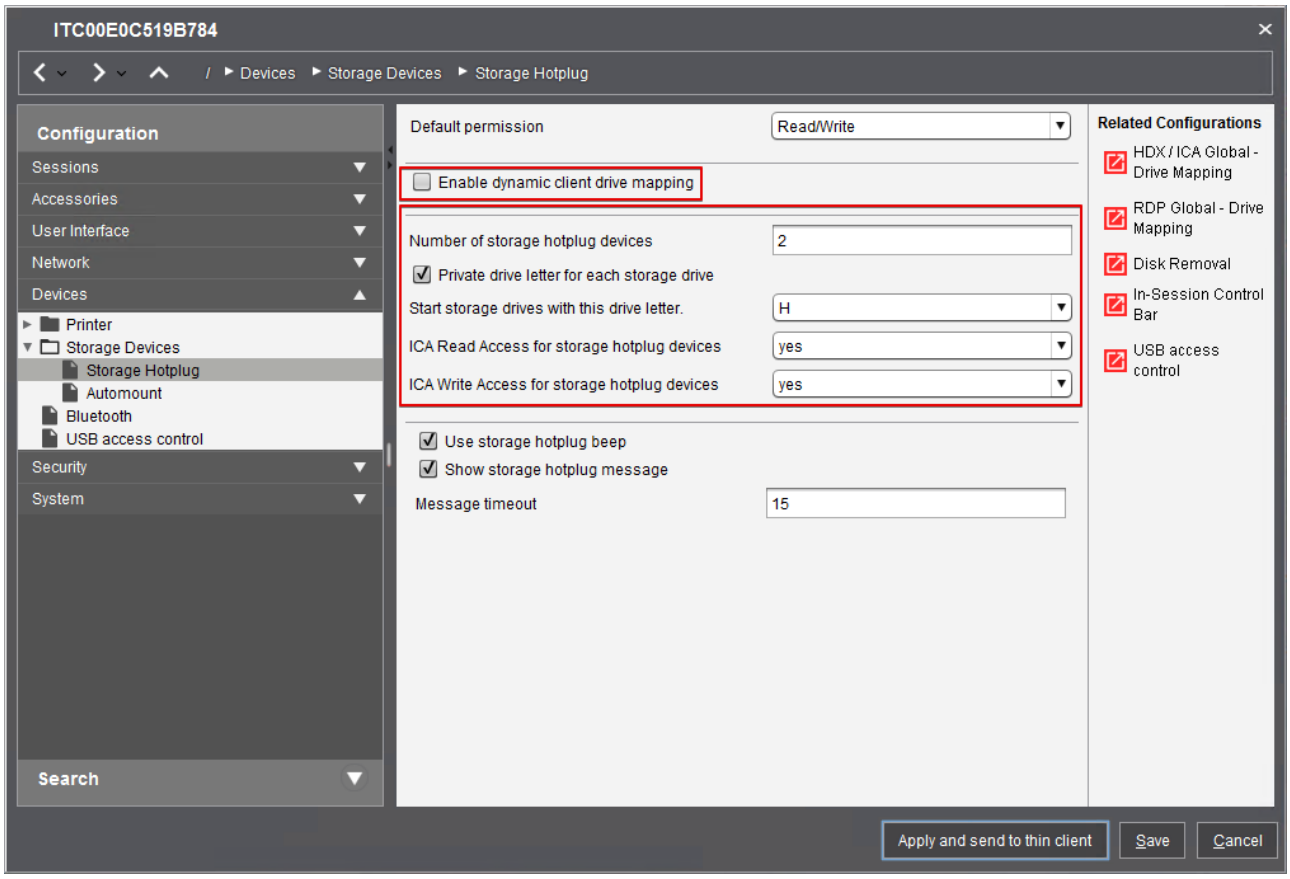


Next, check the USB Redirection Settings:



Please make sure that Citrix Native USB Redirection is disabled as this will interfere with the drive mapping recognized by DriveLock. Other USB redirection needs to be carefully tested to ensure that drives can be properly controlled by DriveLock.

At last, have a look at the **Device Storage Hotplug** settings:



At least one drive letter must be assigned and read and write access should be allowed.

Please note, that the DriveLock Virtual Channel doesn't work as expected if you have enabled dynamic client drive mapping.

4 Evaluating DriveLock

You can install DriveLock from compact disc or using files downloaded from the DriveLock website. All DriveLock components are available as separate 32-bit and 64-bit Microsoft Installer (MSI) packages. A separate installation package is available for the DriveLock documentation.

The easiest way to install DriveLock components is by using the DriveLock Installer (*DLSetup.exe*). This program can check whether the most current installation packages for all components are already present and download missing packages from the Internet. The DriveLock Installer runs both on 32-bit and 64-bit computers.

As an alternative you can download an ISO image containing the DriveLock Installer, all installation packages, documentation and additional information from www.drivelock.com. You can burn a CD from this ISO image.

> When using DriveLock for the first time, it is recommended to use a local configuration to become familiar with DriveLock before deploying configuration settings to multiple clients across your network.

When using a local configuration, policy settings are only applied to the computer where you configure settings using the DriveLock Management Console. A local configuration is appropriate for evaluating

DriveLock or testing a policy before deploying it. The advantage of using a local configuration is that all changes take effect immediately on the local computer.

Other policy types you can use later are:

- *Group Policy*: You can store DriveLock configuration settings in a Group Policy Object in Active Directory. Policy settings are deployed to client computers using the native Group Policy mechanism in Windows.
- *Centrally Stored Policies*: Centrally Stored Policy (CSP). CSPs are similar to configuration files, but they are stored by the DriveLock Enterprise Service (DES) and retrieved from there by Agents. Unlike other types of policies, CSPs also automatically support versioning and change tracking and support Quick Configuration for effortless deployment.

The DriveLock deployment described in here consists of two steps:

1. Installing the DriveLock Management Console and the DriveLock Agent on a Citrix XenApp Server
2. Creating an initial DriveLock policy (for example, an initial policy that blocks no access until further testing is complete)

> Additional information on how to install the other components can be found in the DriveLock Installation Guide or DriveLock Quick Start Guide.

Please refer to the DriveLock installation Guide and the DriveLock Release Notes for the system requirements. We recommend to use XenApp 6 or higher.

4.1 Installing DriveLock

In this document we describe the installation of the Management Console and the DriveLock Agent on one Citrix XenApp server. This is the recommended installation type for evaluating DriveLock with IGEL thin clients. Additional components are not required in this scenario.

To start the installation, run the DriveLock Installer (*DLSetup.exe*) to first download all installation packages from the Internet and then install them on the local computer. Select the Management Console and the Agent.

> If you want to create a local DriveLock policy first, without previously installing a DriveLock Agent, just select Management Console. After you have completed this installation you can configure a local policy allowing all drives to be used without limitations, thus preventing the DriveLock Agent to apply default configuration settings and blocking access to connected devices.

The Installer will check whether any of the components are already present and whether newer versions of these components are available.

To only download the selected components but not install them select the checkbox *Download files only*.

To use local versions of the selected components without downloading newer versions, select the checkbox *Do not download files*.

Click **Next** to start the download or installation. When the process has complete, a notification is displayed.

Click **Finish** to complete the installation or download.

4.2 Configuring DriveLock

When using IGEL thin clients, DriveLock must be installed on the Citrix XenApp server. The DriveLock configuration on the server determines which drives a user can access.

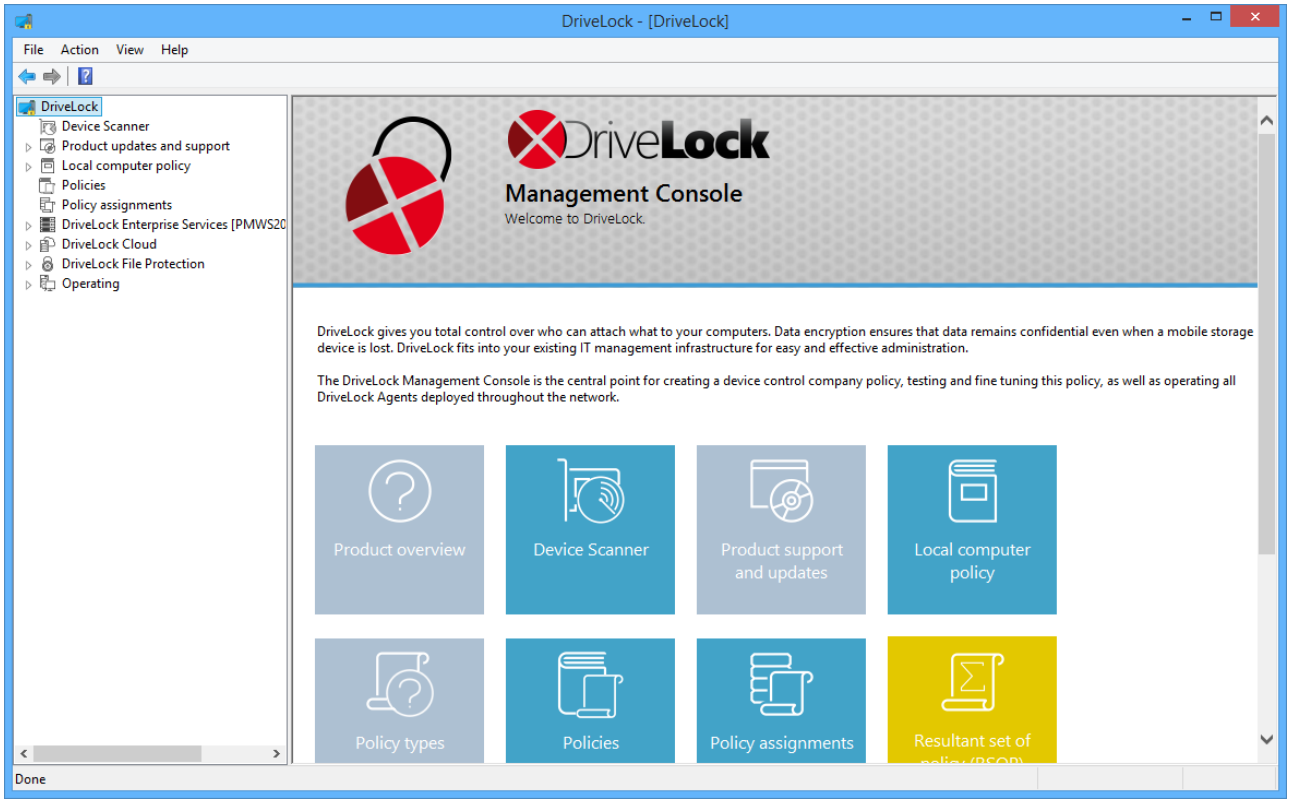
DriveLock SE has developed a DriveLock Virtual Channel (ICA/RDP protocol) that can read hardware data from local USB devices and transmit them to the XenApp/Microsoft Terminal server using a Virtual Channel Extension. This allows for the use of whitelist rules that are based on a USB-connected drive's hardware characteristics, such as manufacturer, model and serial number.

> The DriveLock Virtual Channel is included in IGEL's Universal Desktop Linux since release 4.11.100.

If the XenApp server belongs to a domain, the configuration settings can be applied using Group Policy. For test purposes, a local policy is recommended and used here.

The DriveLock Management Console is a Microsoft Management Console (MMC) snap-in that can be used on its own or in conjunction with other MMC snap-ins. Use the Management Console to configure DriveLock and DriveLock policies.

After you have installed the DriveLock Management Console you can start it from the Windows Start menu by selecting **DriveLock Management-Console**.



> After starting the console for the first time a wizard appears. You can skip all steps for this scenario here.

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.

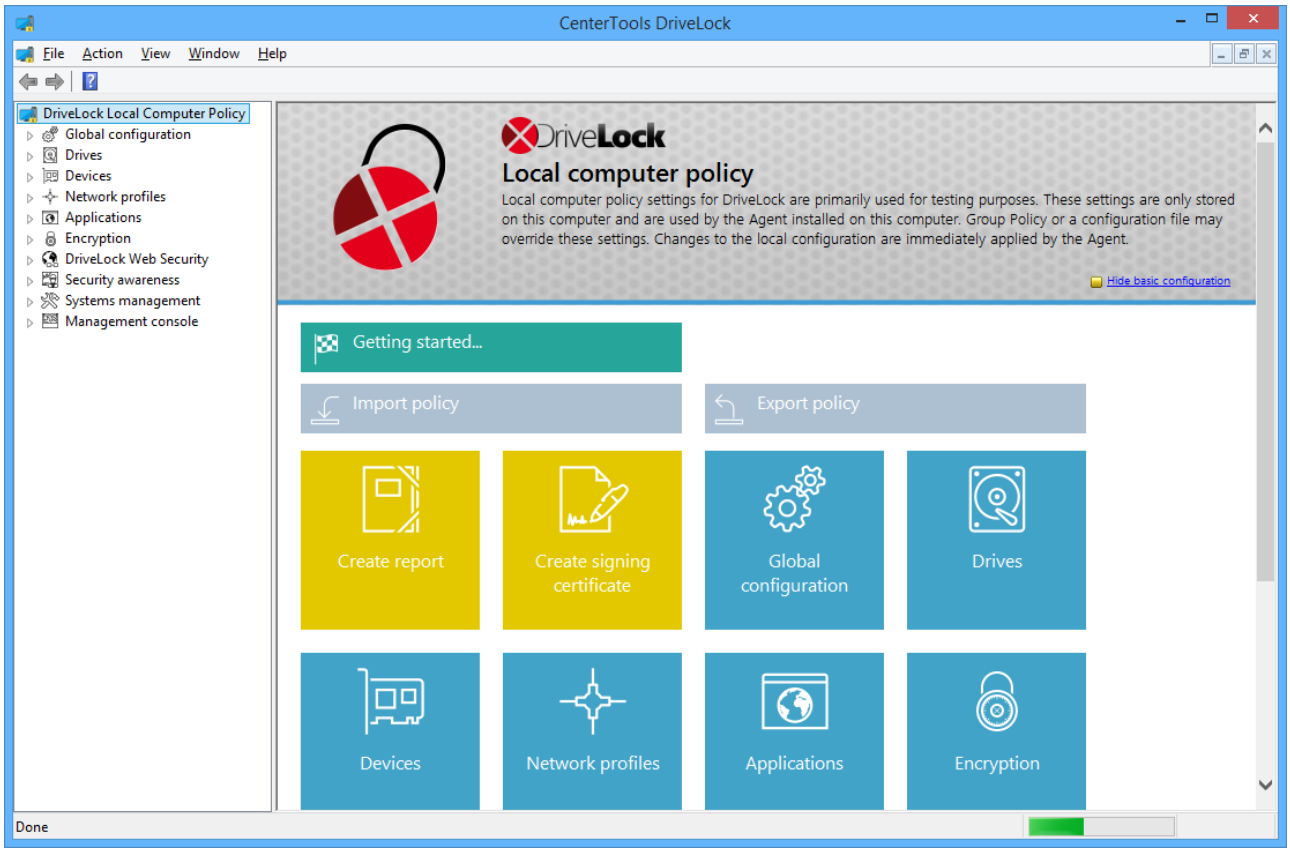
The right section of the Management Console displays taskpad views. Depending on the node you select in the console tree, taskpads contain links subnodes or configuration elements. You can navigate taskpad views by clicking the links in it. If you prefer the classic MMC view without taskpads you can optionally switch to that view in several areas of the Management Console.

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.

4.2.1 Using a Local Policy

To configure the XenApp server 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 **Policies**. Right-click on *Local computer policy* and click **Edit**. After a few seconds a new windows opens.



To clear all configuration settings from an existing DriveLock policy, right-click **DriveLock Local Computer Policy** 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 computer policy" in root console.** The next time you start the Management Console, the new entry appears in the console tree.

For the first 30 days you don't need to provide a license, so we can skip this step here.

Any of the following configurations will be done within this local policy in this window.

4.2.2 Configuring Locking of Mapped Drives

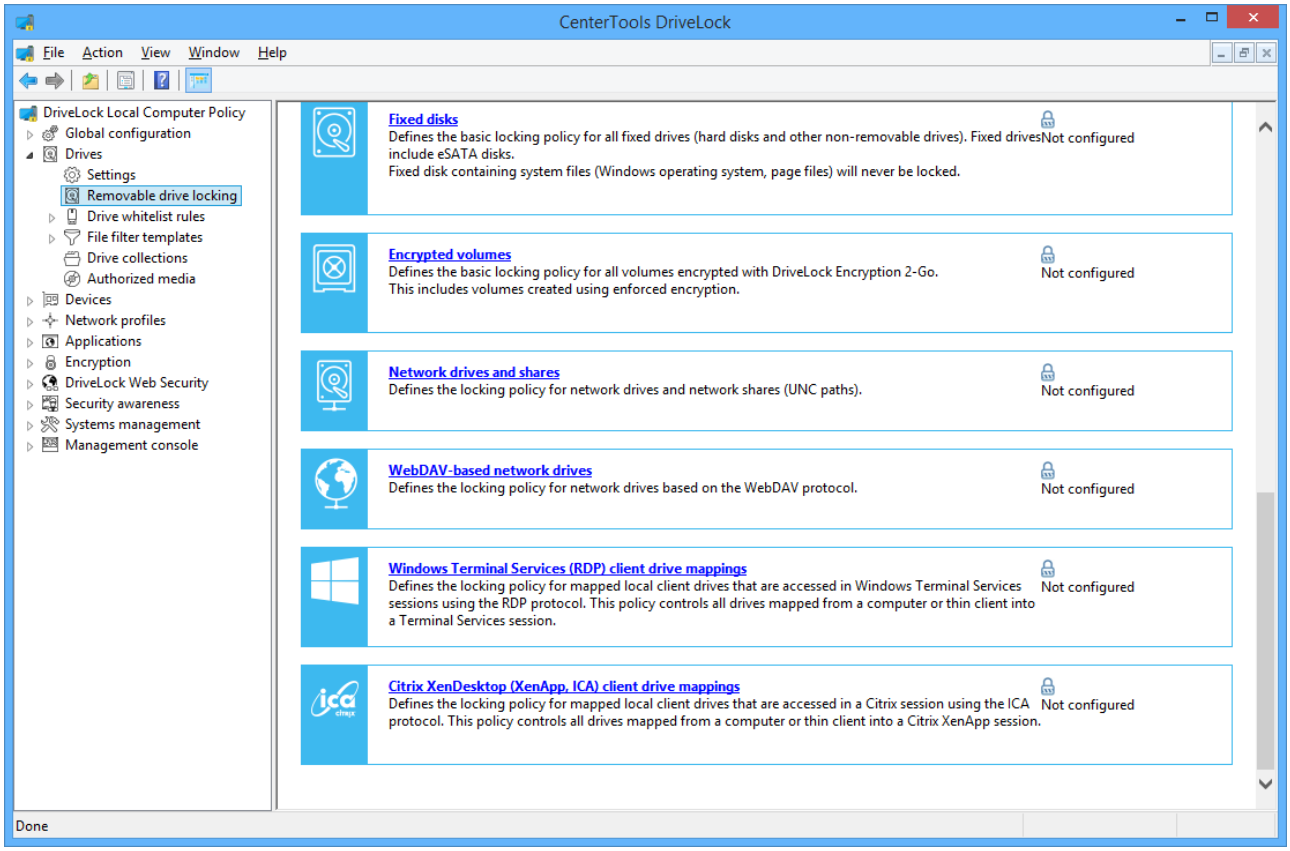
When designing your access control rules you need to identify which types of drives to lock and which exceptions are required. This includes how detailed the rules and exceptions need to be and whether drives need to be locked based on users and groups, hardware characteristics or a combination of these factors.

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:

- Citrix XenDesktop (XenApp, ICA) client drive mappings are drives in client sessions using Independent Computer Architecture (ICA)
- Windows Terminal Services (RDP) instead are using the Remote Desktop Protocol (RDP).

This protocols are used by the DriveLock Virtual Channel.

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 ICA/RDP drives, in the right pane click the appropriate "**... (XenApp, ICA/RDP) client drive mappings**".

Use the tabs in this configuration dialog box to configure settings that apply to all USB drives (mapped devices) connected to the thin client.

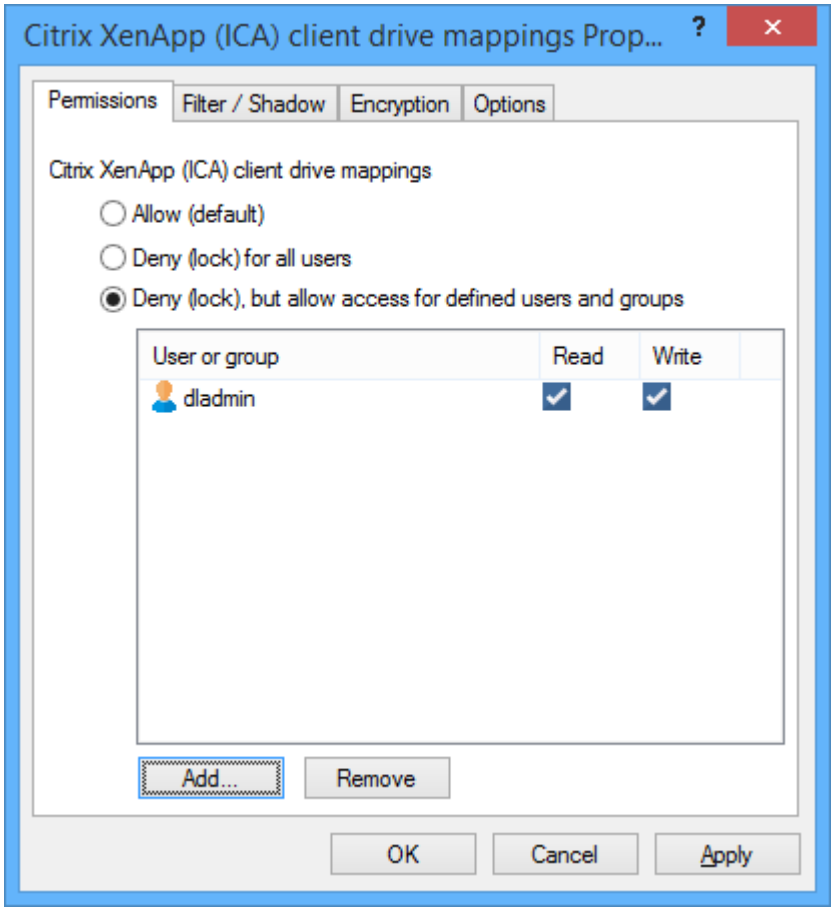
The configuration dialog is almost identical for all other drive types, but not all features are available for some drive types or look slightly different from the options you might see here.

To enable locking of all USB drives on the thin client, select "**Deny (lock) for all users (default)**" and then click **OK**.

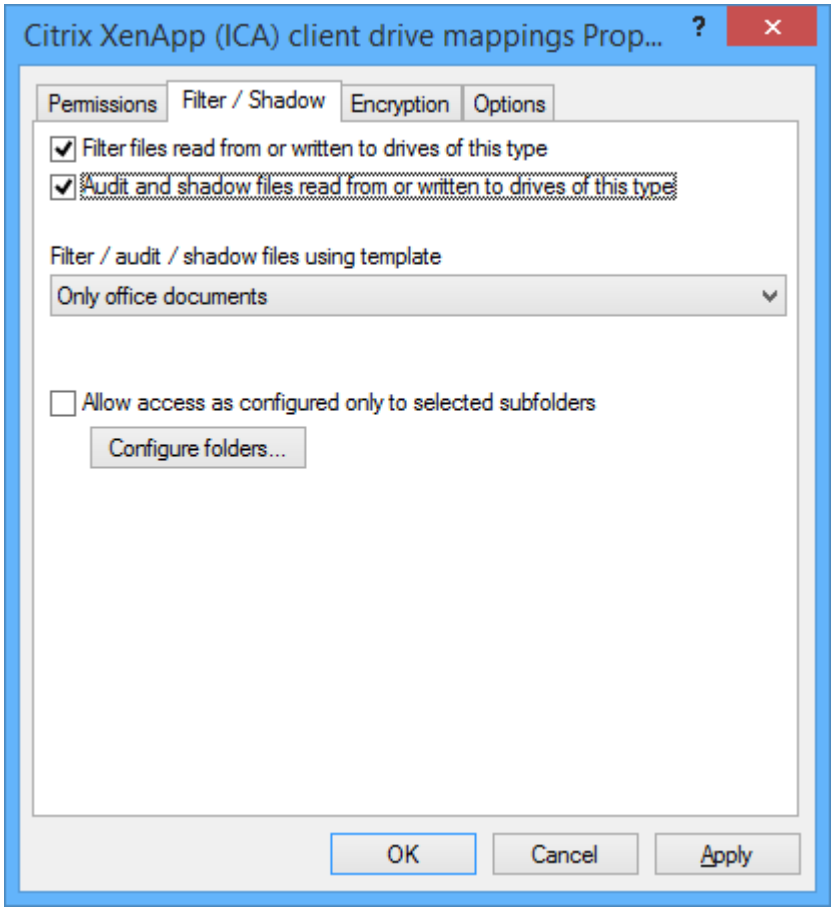
Now, if you insert a USB stick within your desktop session, when double clicking on the mapped drive within the explorer (for example, letter H:) you should get a message, that you don't have access to this drive.

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.

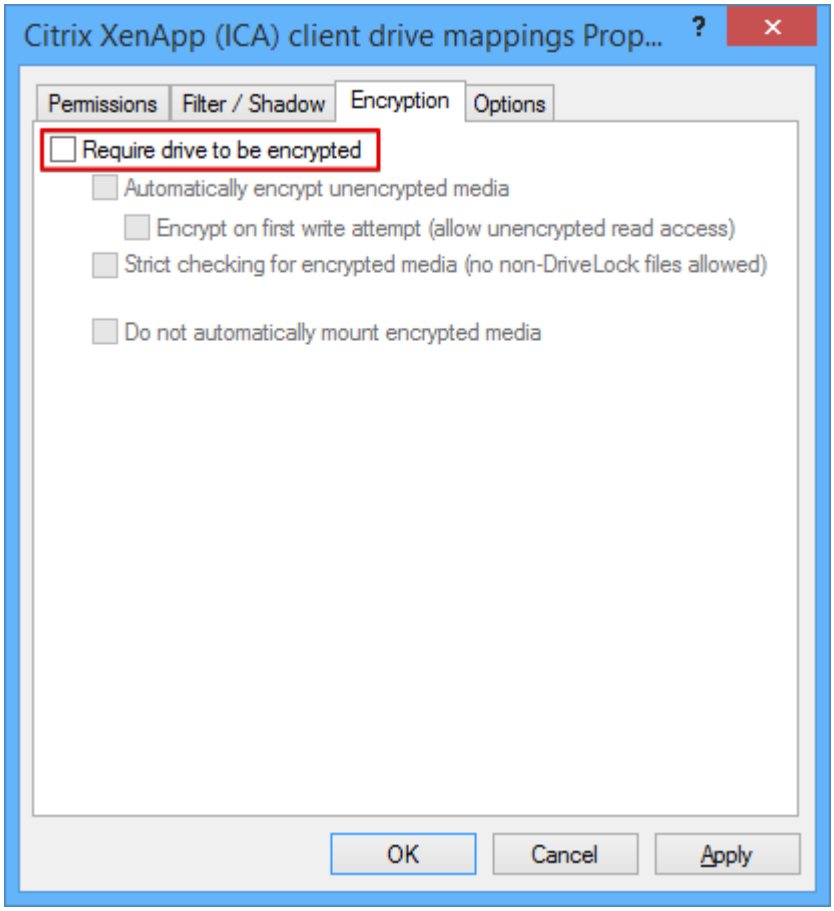


The DriveLock Agent includes a file filter component that can control and audit access to files based on the file type, such as DOC or PDF. You can configure any rule to use the file filter and apply file filter templates. You can enable file filtering and auditing under on the *Filter/Shadow* tab.



More about these settings can be found in chapter "Controlling and Auditing File Access".

If you need to configure encryption, select the *Encryption* tab:

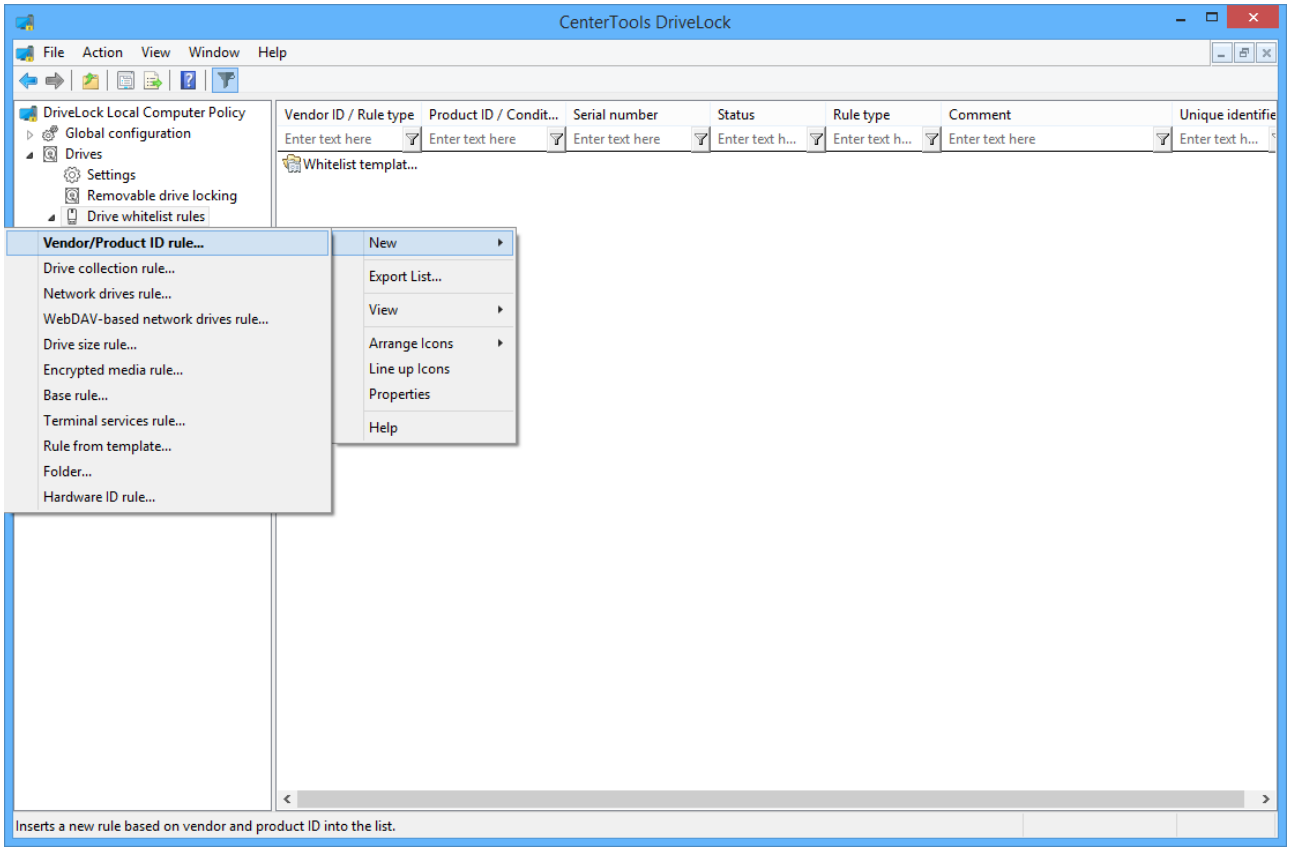


These settings are described in detail in chapter "Enforce Encryption"

After you have locked access to all types of ICA/RDP drive mappings, you can create hardware-dependent whitelist rules under *-> Removable drive locking -> Drive whitelist rules -> Vendor/Product ID rule*.

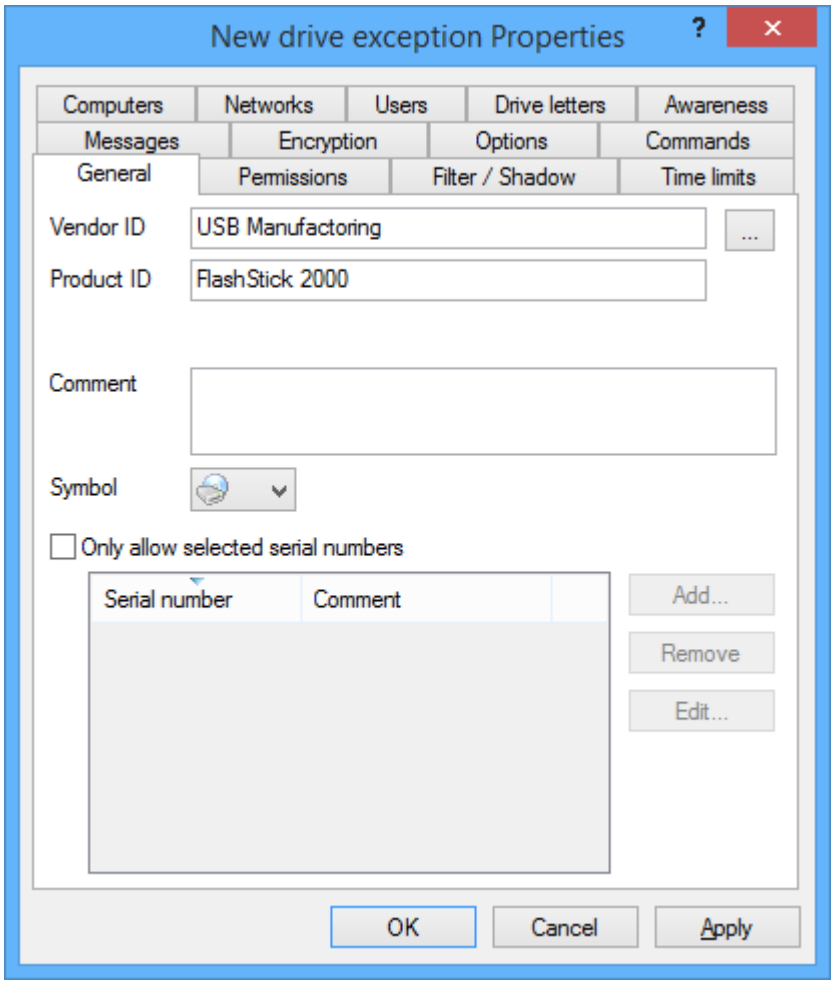
4.2.3 Configuring a Vendor/Product ID Rule

After you have disabled all mapped drives you need to configure one or more whitelist rules to allow access to connected devices.



Right-click **Drive whitelist rules** 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.

DriveLock will display a dialog box that you can use to select a drive that is currently attached to the server or to a thin client respectively, 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 thin client attached drive, select **on agent** and then type the name of your XenApp server you want to connect to and click **Connect**. Select the drive and then click **OK**.

> Mapped drives usually show *TS* as bus type.

If you need information about other drives, you can connect to a remote server and select one of the drives listed. Select **on agent** and then type the name of the server you want to connect to. This requires that the DriveLock Agent is installed and running on the remote server.

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 Server 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*".

A more convenient way to get drive information is to use the results from a Device Scanner scan that has been completed in advance. Please refer to the *DriveLock Administration Guide* to learn more about the Device Scanner.

After you have configured how DriveLock recognizes a specific device you can configure other additional parameters.

4.2.3.1 Other 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 are described in this section.

4.2.3.1.1 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**.

4.2.3.1.2 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 "*Filer 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 on the up and down arrows 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.

4.2.3.1.3 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.

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**“.

4.2.3.1.4 Settings for Computers

On the *Computers* tab you specify the computers on which a whitelist rule is applied.

> This feature usually will not be used in thin client environments unless you want to distinguish between different XenApp servers within one single policy.

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.

4.2.3.1.5 Network Settings

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

> This feature usually will not be used in thin client environments.

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.

4.2.3.1.6 User and Group Validation

On the *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.

4.2.3.1.7 Assigning Drive Letters

Assigning Drive letters might interfere with the drive mapping within your thin client setting. Therefor activating this feature is not recommended when using thin client drive mappings.

4.2.3.1.8 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.

4.2.3.1.9 Enforce 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.

DriveLock utilizes two different ways of encryption: container based and file & folder based encryption. In Terminal Service environments, only container based enforced encryption can be used, due to technical limitations.

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.

Due to technical limitations, the option "**Require drive to be encrypted**" is not available for CD drives, network drives and WebDAV drives.

> 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 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.

Click **OK** to save the action.

4.2.3.1.10 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.

> 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.

5 More Information

You have completed the first steps to secure your thin client environment using DriveLock and it's comprehensive device control and encryption capabilities.

Please refer to the DriveLock manuals to get detailed information about all the features included in DriveLock. The following manuals are available for download (http://drivelock.help) or included in the DriveLock ISO image:

- DriveLock Installation Guide
- DriveLock User Guide
- DriveLock Administration Guide
- DriveLock Control Center User Guide
- DriveLock Quick Start Guide

If you need to test the DriveLock Virtual Channel within a terminal session, you can download our test tool here: http://download.drivelock.com/web/VirtualChannelTest.zip.

DriveLock and Igel Thin-Clients