DriveLock Security Awareness

Documentation 2023.1

DriveLock SE 2023

Table of Contents

1 Welcome to DriveLock Security Awareness

Raising employee security awareness is one of the most important tasks of a company today. With DriveLock Security Awareness, you can deliver event-driven campaigns and trainings with the following added value:

- Flexible security awareness trainings that are available online or offline continuously and can be administrated centrally,
- Interactive presentation of security-relevant information when needed, for example, when a USB flash drive is inserted,
- Event-driven campaigns, for example once a week or once a month automatically,
- Adaptive posting of actions to be taken following a security incident, and
- Implementation of security measures in line with the GDPR.

As part of the DriveLock Zero Trust platform, Security Awareness is a standard feature of DriveLock and does not require a separate license.

However, the Security Awareness Content AddOn does require a separate license and will provide you with a variety of external content you can use to create security awareness campaigns.

Note: The Content AddOn packages can only be displayed correctly if Microsoft Edge WebView2 is installed on the agents.

2 Concepts

2.1 Campaigns

The security awareness campaigns used in DriveLock consist of texts in various formats (RTF, PDF, text), images, videos, web content, or e-learning modules. Campaigns provide users with targeted safety information, alert them to specific events, give instructions and assign the training they need.

You can configure security awareness campaigns so that they appear at specific times and events, for example when users log on to their computer or when connecting a smartphone, starting an application, plugging in a USB stick or connecting an external drive. You can also configure them to be displayed to users without any particular event or let the users decide when they want to watch the campaigns. The frequency of the display is also adjustable.

To ensure that the security information has reached its destination and the user has dealt with the content, a confirmation can be requested.

Campaigns can also be defined individually for drives, devices and applications within rules.

You can create campaigns in the Policy Editor and in the **Awareness** menu in the DOC.

Note: The DOC only allows you to create campaigns with content packages, and only limited or reduced configuration options are available for these campaigns.

2.2 Content packages

The Content AddOn, which requires a license, contains multimedia content (for example, complete security trainings) and can be used to create campaigns. The content is updated regularly and automatically via the Internet on a subscription basis and can be accessed in the DOC.

Content is available in **English**, **French** and **German**.

Note: If you are using DriveLock On-Premise, you will need to activate the content packages before you can include them in campaigns.

2.3 Evaluations

A range of evaluations are offered in the context of campaigns, and can be used in an audit, for example. Employee trainings, courses or tests and other measures relating to security-relevant issues can be precisely tracked and verified in this way.

Campaigns can be split into sessions for evaluation purposes. Once a campaign has been assigned to a user group and presented to them on their respective endpoints, every single session can be evaluated. This makes it easy to track whether a session failed to complete or was not passed, or whether there were any errors during completion.

2.4 Events

The DOC lists the main security awareness events on the **Events** tab. They allow for a precise evaluation of how the campaign was executed and provide information about errors and warnings that occurred. It is also possible to trace back the objects associated with the event here.

In the Policy Editor, you can see a list of all security awareness events in the **Security Awareness** subnode under **DriveLock events** in the **Events and Alerts** node. Some of the events need to be activated before they can be transmitted from the DriveLock Agent to the DriveLock Enterprise Service (DES) and used for evaluation.

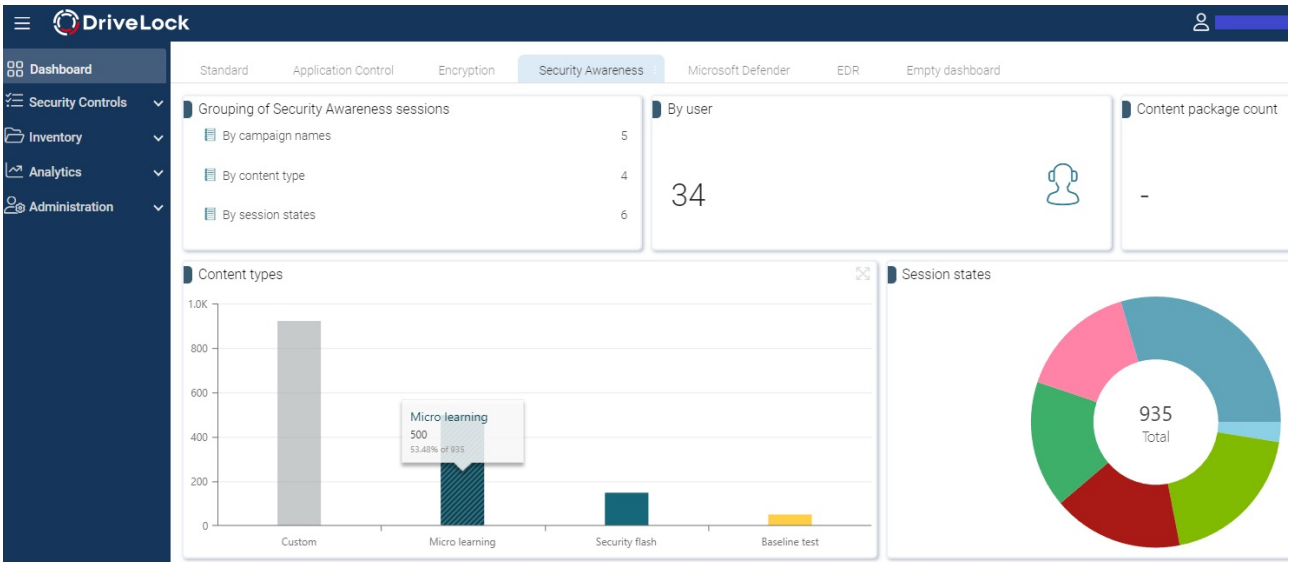
> Note: By default, the most important security awareness events are enabled for evaluation in the DOC.

3 Configuration in the DOC (DriveLock Operations Center)

3.1 Security awareness dashboard

In the DOC, you get an overview of your ongoing security awareness campaigns in the **Security Awareness** dashboard (see figure). The course of a campaign is referred to as a 'session'.

Each view is individual and depends on various factors, such as the number and type of campaigns you have already created.



The sessions are grouped according to certain filters:

- For example, if you want to see how many users are currently working on a campaign with a specific content type, select the **By content type** option in the **Grouping of sessions** widget. On the **Evaluations** tab, all content types will then appear with the respective number of sessions. Highlight a session and then you will see the details: start and end dates, computer and user name and the status.
- In the **Content type** widget, you can filter by a specific campaign content type.
- The **Session states** shows you the different states of the sessions in a pie chart. If you click the **Failed** segment, you can see, for example, who failed a session.

The following requirements are necessary so that campaigns or their sessions can be displayed in the DOC:

1. You have already created one or more security awareness campaigns. The content is not important.

2. The policies containing the campaigns have been assigned to the applicable DriveLock Agents. Campaigns are only displayed if they have already been started, are currently active or have already been completed on the agent.

   Note: Campaigns that you create in the DOC are automatically assigned.

3. The security awareness events must be enabled on the DriveLock Enterprise Service.

3.2 How to create a campaign step by step

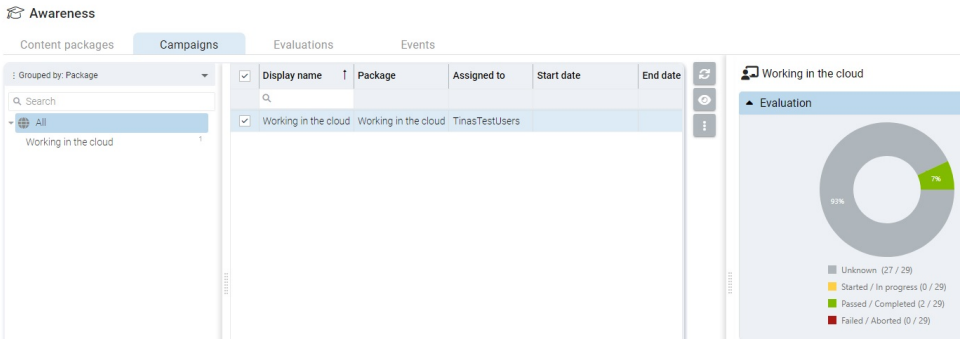
If you are creating a campaign for the first time and want to assign it to an agent followed by an evaluation, proceed as follows.

1. Open **Awareness** in the **Security Controls** menu.
2. If you have licensed the Content AddOn, all packages will automatically appear on the **Content Packages** tab. To see what kind of content a campaign has, select it and review the description on the right in the Details pane in the **Properties**. You can group the packages by content type or by name. The "Working in the cloud" training package is the example here.

   Note: Note that the packages must first be synchronized before they are assigned to campaigns if you are using DriveLock On-Premise. Then, the server downloads them so they can be redistributed to agents.

3. To create a campaign with this package, select **Working in the cloud**. Right-click to open the context menu or select the button. Select **Create campaign**.
4. Enter a **name** and description for the campaign or accept the input. Next, specify the **priority** for the campaign execution order (settings from 1 - 10, order descending). Campaigns with the same priority will be displayed in random order.
5. In the next step, select who the campaign will be **assigned to**. Add a **user group** here, which you have to define beforehand. If required, you can define a **start and end time** for the campaign.
6. Once you click **Finish** , the new campaign will appear on the **Campaigns** tab.
7. Here you can edit, delete, deactivate the campaign or reduce or increase its priority. As soon as the campaign has been executed, you can already see the status in the **Detail view** in **Evaluation**. In the example, 2 out of 29 users passed the training (7%).

Note: Note that the total number may increase as additional users log in to their DriveLock agents who are not previously registered as members.



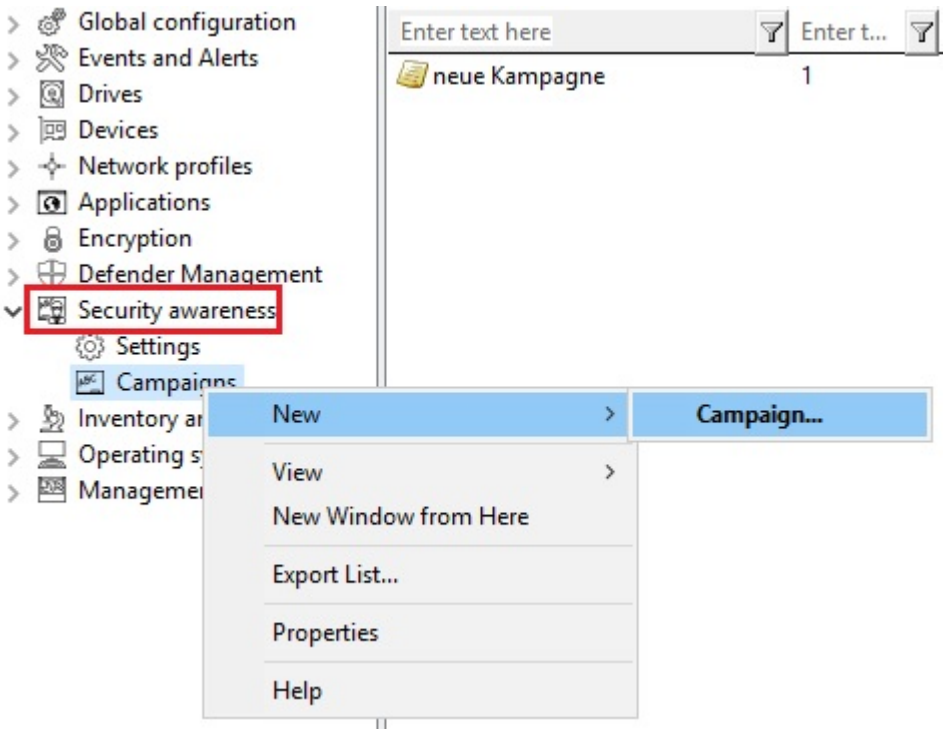
Note: In the display, the campaigns can take on different text colors. Dark gray if the current date is outside the start and end range. Light gray when the campaign is disabled. Black is the normal text color.

8. If you click on the green area, the tab **Evaluations** opens automatically with further information
   Here you can take a closer look at individual sessions of campaigns using various filters and groupings.
9. The **Events** tab displays the relevant security awareness events.

4 Configuration in the Policy Editor

4.1 Creating campaigns

In the **Security Awareness** node in your policy, you can create new campaigns in **Campaigns** as shown in the figure:



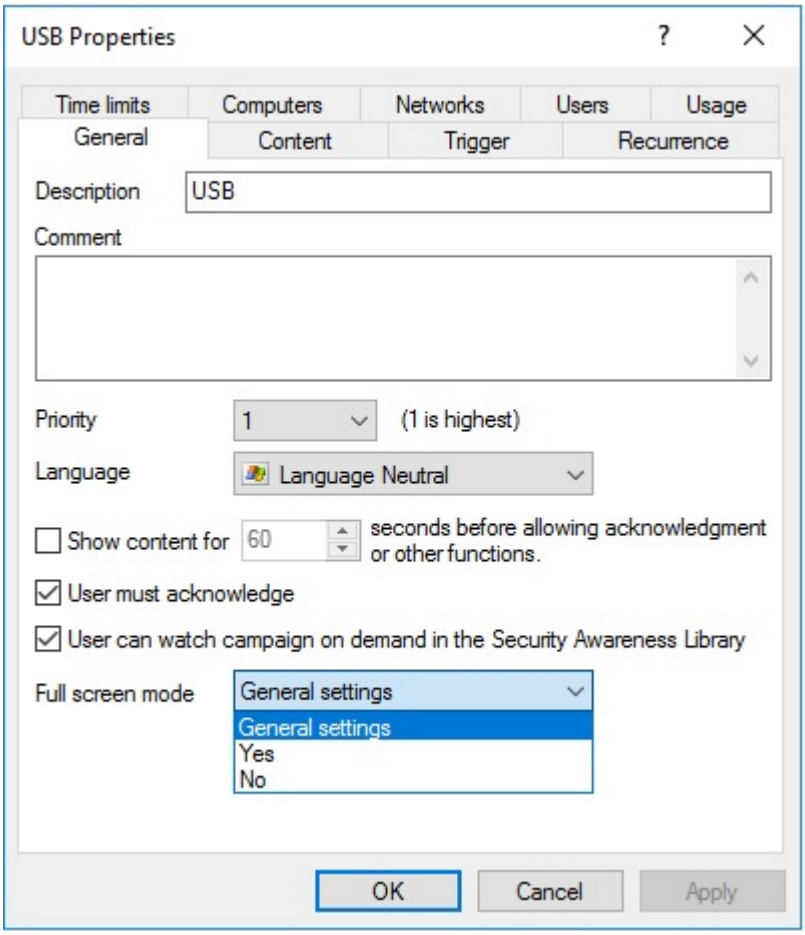
From the **campaign** context menu, select **New** and then **Campaign....** The **New Campaign** Wizard will open and you will go through the following dialog pages:

1. Content of a new campaign
2. Trigger for a new campaign
3. Recurrence of a new campaign
4. General settings

Note: To assign the new campaign to specific computers, users, and network connections, open the Security Awareness Campaign Properties. Here you can also change all the settings you made in the **New Campaign** Wizard.

4.1.1 General

The **General** tab allows you to specify the following:



- **Description** of your campaign and an optional **Comment**. A description is needed so that you can find your campaign in the campaign listing. It is also used later on for reporting.
- **Priority** according to which the execution order of the campaigns is set (settings from 1 - 10, order descending). Campaigns with the same priority will be displayed in random order.
- Select the **Language** in which the campaign is presented. For example, if you select Brazilian, your campaign will only appear on agent computers whose operating system language is Brazilian. Leaving the language on Neutral includes all operating system languages.

> Note: If you select a security awareness package from the Security Awareness Content AddOn, the language is already predefined by this selection (German, English or French only).

- Specify how long the campaign remains visible before the user has to confirm or is allowed to close the campaign.

- Specify whether the user must confirm that the campaign content has been read. You can enter a confirmation text for all of your campaigns in the general security awareness settings.
- The **User can watch the campaign on demand in the Security Awareness Library** option is enabled by default. A user can select campaigns from the Security Awareness Library and watch or complete them whenever it is convenient.
- Full screen mode:
  Select **Yes** if you want to show the campaign in full screen mode on the agent computer.
  Select **General settings** if you want to use the security awareness settings that apply to all campaigns for this specific campaign.
  Select **No** if you do not want full screen mode.

> Note: This option is not available at all if you selected the **Ignore full screen mode settings on campaign level** option earlier for all campaigns.

4.1.2 Content

The **Contents** dialog page allows you to determine which contents (elements) your campaign should contain.

- **Image**
  Select any image from your file system or policy file storage. DriveLock supports the usual image formats (*.png, *.jpg, *.bmp).
- **Content AddOn Package**
  Choose a package that suits your needs. This could be a training, a security flash or a knowledge test.

> Note: Please note that Content AddOn packages are only displayed in this list if you have purchased the license for the DriveLock Content AddOn. If not, only the demo packages will appear.

- **Built-in image:**
  Select one of the images DriveLock provides.
- **PDF file:**

Select a PDF file here that will be displayed to the user. Please make sure that the content is displayed correctly, as not all PDF features are supported.

- **RTF file**
  Select an RTF file here that will be displayed to the user. This may be plain text only, Unicode or ANSI character code.
- **Text**
  Enter any text for your campaign.
- **URL (web content):**
  Enter a URL here that points to Web content you want to use for your campaign.
- **Video file**
  Select a video file (in *.mp4 or *.avi format) which will be displayed to the user in Windows Media Player.

> Note: The window size always adjusts to the content, except for Content AddOn packages and URLs where the window size is 1280x1024.

4.1.3 Trigger

The **Trigger** dialog page allows you to specify in which event your campaign will appear.

> Note: Examples of **events** include users logging in to their computer, plugging in an external drive, connecting a device, such as a smartphone, or updating a policy that uses rules to control the display of a campaign.

The following options are available:

- **Independent of an event**
  Choose this option to display a campaign directly to users at the nearest possible time, regardless of the usual events that trigger the display of a campaign. In this case, the DriveLock Agent checks at certain intervals (every 30 minutes) whether independent campaigns are pending and then displays them to the user accordingly.

> Note: Select this option if you want to send ('push') users a security awareness campaign as quickly as possible, for example important company-internal information or warnings.

- **When a user logs on**

Select this option to display a campaign to users as soon as they log on to their computer.

- **If used in rules**
  Select this option if you want to use a campaign in a rule. The campaign is displayed to users as defined in the corresponding rule for drives, devices or applications on the **Awareness** tab.

> Note: This option is only available if you are using the full range of DriveLock features.

The last two options are only available if you are using DriveLock Security Awareness alone (without Device Control):

- **When connecting a device**
  Select this option to show a campaign to users as soon as they plug a device into their computer.
- **When connecting a drive**
  Select this option to show a campaign to users as soon as they connect a drive to their computer.

4.1.4 Recurrence

On the **Recurrence** tab, you specify how often you want your campaign to be displayed or repeated.

You can set the following here:

- **Show campaign x times**
  Here, you can define how often you want your campaign to be displayed by specifying a certain number of times, or you can select **Never** or **Indefinitely** from the drop-down list.
  Selecting **Never** makes sense if you do not want to display your campaign at first. At a later time, you can change this in the campaign's properties.
- **Every time the event occurs**
- **Once per day/week/month/year**
- You can also specify that your campaign is displayed **once every few days** (e.g. every third day).

- In case a campaign was displayed partially or an error occurred, you can specify that it will be displayed again after a certain time.

4.1.5 Deploy the campaign to users

To deploy a new security awareness campaign to the target users (computers running DriveLock Agents), you must first publish the policy.

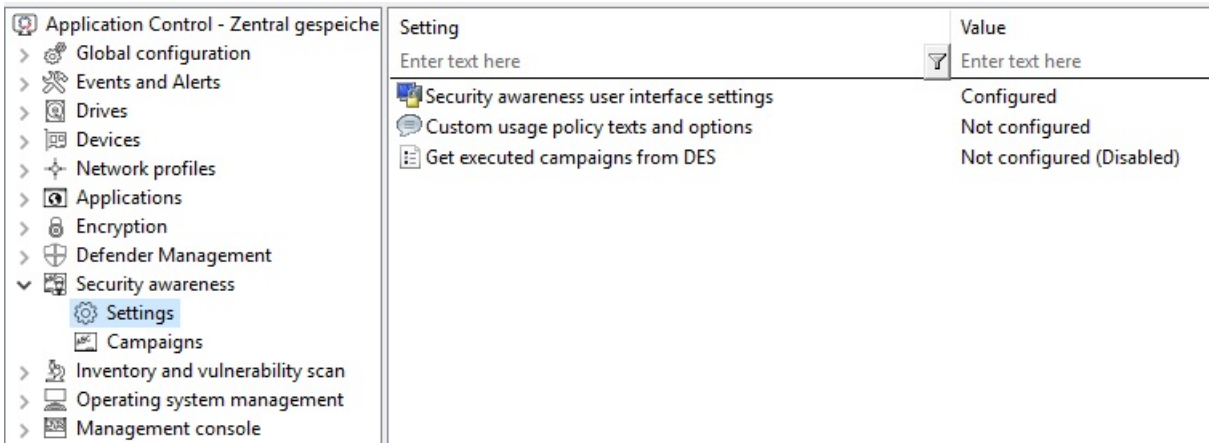
1. Open the policy's context menu and select the **Publish** menu item. Or select the **Publish** button from the menu bar.
2. Optionally, you can enter a comment.
3. If you want to sign the policy, enable the corresponding option and select the certificate.
4. The policy is now published and used by DriveLock Agents

4.2 General settings

In the **Security Awareness** node in your policy, you can configure general details for all campaigns in **Settings**.

Please do the following:

1. Under **Security Awareness**, select the **Settings** menu item.



2. Click the **Security awareness user interface settings** option to specify the following settings:

   - **All campaigns**
     On this tab you make general settings that affect **all** campaigns.
     - Here you can determine whether the window in which security awareness campaigns are displayed is always visible to the user.

- If you want all campaigns to be displayed in full-screen mode, check the corresponding option.

> Note: In full-screen mode, your campaigns come out especially well.

- Select the **Ignore full-screen mode settings on campaign level** option if you want to override the settings in individual campaigns (full-screen mode can be set in the campaign properties).
- If you have not yet created multilingual notification texts for your policy, you can use this dialog to enter headings and texts for your campaigns that are specifically tailored to your company.
- Alternatively, you can specify languages in the **Multilingual notification messages** section of the **Global configuration** node and define corresponding notification texts here.

> Note: For more information on how to create multilingual notification texts, see the Admin documentation in DriveLock OnlineHelp.

3. Select **Custom usage policy texts and options** to show customized content when a user attempts to access a drive and/or a device. The option only applies to a usage policies. In the Properties dialog, specify the following:

- Select the file that contains the usage policy or enter text for the usage policy
- Enter text for the buttons (if you don’t want to use Accept or Decline)
- Enter a caption
- Select a video to show the users and specify settings for this video

> Note: You can configure DriveLock in such a way that an external drive or device can only be accessed after the user has confirmed reading a usage policy by clicking the "Agree" button.

4. Select **Get executed campaigns from DES** to specify that users can "take" their completed campaigns with them when they log on to another computer, i.e. the completed campaigns are no longer displayed there. A request is sent to the DriveLock

Enterprise Service (DES).
The default setting is **Disable** because most users work at their own computer.

4.2.1 Custom usage policy texts and options

Usage policies are used to inform the user of security-related behavioral measures or corporate policies before actually accessing a drive or device.

You can configure DriveLock in such a way that an external drive or device can only be accessed after the user has confirmed reading a usage policy by clicking the "Agree" button.

You can freely define a heading, the texts for the two buttons, as well as the text itself via this configuration item. To do so, check the **Display custom content** option.

Either type the message text directly into the input field, or select an RTF-formatted file from the local disk or policy store. A file from the policy store is marked with an "*".

Warning: When you select a file, you must make sure that it is located in the specified path on the local hard disk of the client computer and can be loaded from there. You can use the policy store to distribute this file along with the DriveLock configuration.

An AVI video can also be played within the usage policy which can also be configured via this dialog as a special option. You can define the options the user has while the video is displayed.

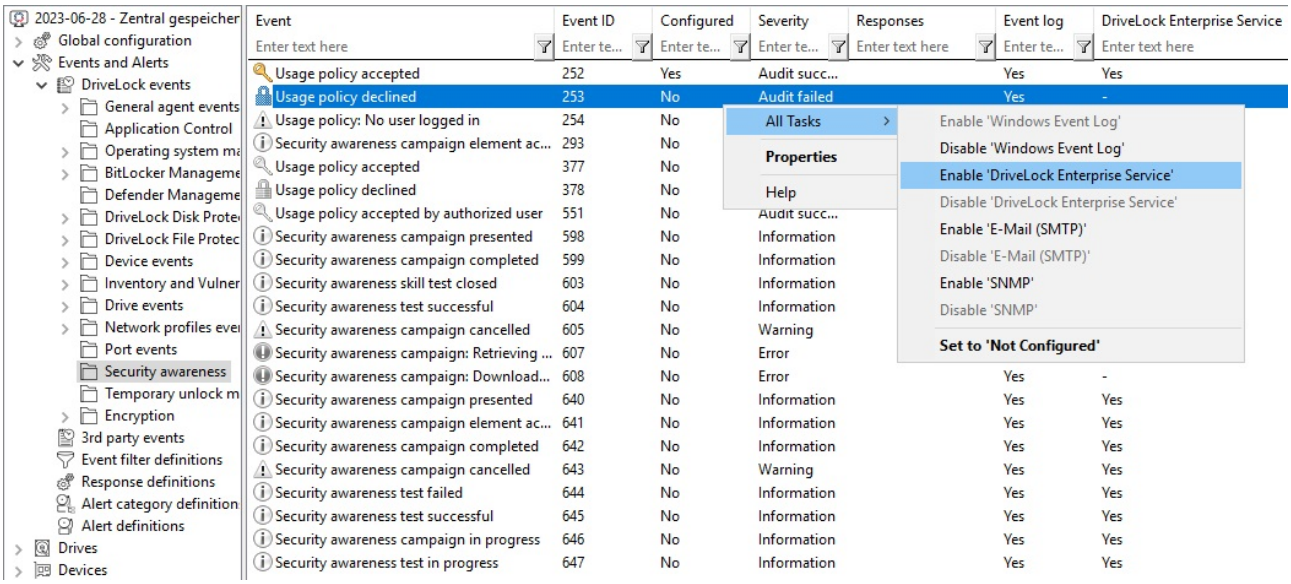
The option **Show x times per user and session** will not display the message more than the specified number of times.

You can also define when and how long it takes for the Accept button to become available to the user.

4.3 Enabling security awareness events in the Policy Editor

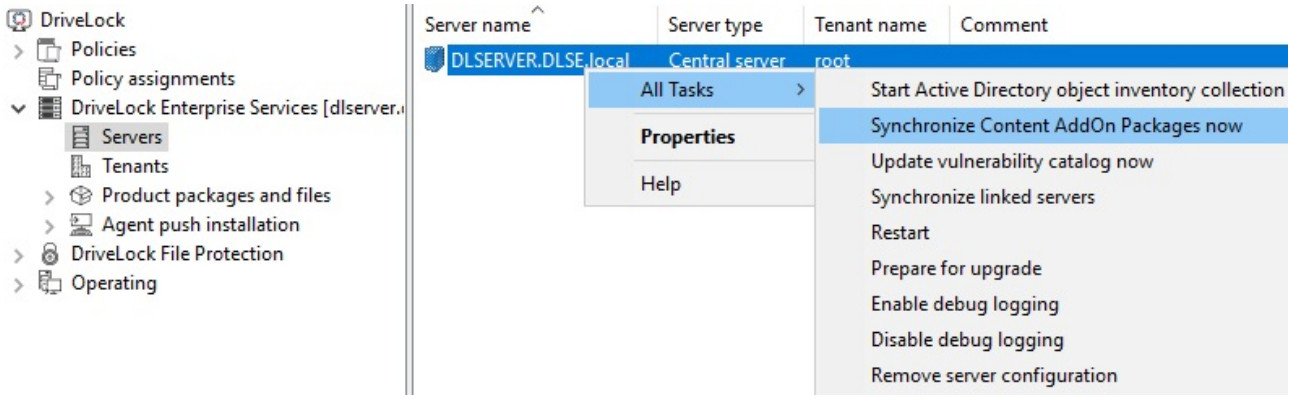
In the Policy Editor, security awareness events are enabled as follows:

1. In the **Events and Alerts** node, under **Events**, open the **Security Awareness** subnode.
2. Select all the events you want to have displayed in the DOC and open the context menu.
3. Select **'Enable DriveLock Enterprise Service'** to allow events to be uploaded to DES.


2023-06-28 - Zentral gespeicher
Global configuration
Events and Alerts
DriveLock events
General agent events
Application Control
Operating system ma
BitLocker Manageme
Defender Manageme
DriveLock Disk Prote
DriveLock File Protec
Device events
Inventory and Vulner
Drive events
Network profiles eve
Port events
Security awareness
Temporary unlock m
Encryption
3rd party events
Event filter definitions
Response definitions
Alert category definition
Alert definitions
Drives
Devices
Event
Event ID
Configured
Severity
Responses
Event log
DriveLock Enterprise Service
Enter text here
Usage policy accepted 252 Yes Audit succ... Yes Yes
Usage policy declined 253 No Audit failed Yes -
Usage policy: No user logged in 254 No
Security awareness campaign element ac... 293 No
Usage policy accepted 377 No
Usage policy declined 378 No
Usage policy accepted by authorized user 551 No
Security awareness campaign presented 598 No Information
Security awareness campaign completed 599 No Information
Security awareness skill test closed 603 No Information
Security awareness test successful 604 No Information
Security awareness campaign cancelled 605 No Warning
Security awareness campaign: Retrieving ... 607 No Error
Security awareness campaign: Download... 608 No Error Yes -
Security awareness campaign presented 640 No Information Yes Yes
Security awareness campaign element ac... 641 No Information Yes Yes
Security awareness campaign completed 642 No Information Yes Yes
Security awareness campaign cancelled 643 No Warning Yes Yes
Security awareness test failed 644 No Information Yes Yes
Security awareness test successful 645 No Information Yes Yes
Security awareness campaign in progress 646 No Information Yes Yes
Security awareness test in progress 647 No Information Yes Yes
All Tasks
Properties
Help
Enable 'Windows Event Log'
Disable 'Windows Event Log'
Enable 'DriveLock Enterprise Service'
Disable 'DriveLock Enterprise Service'
Enable 'E-Mail (SMTP)'
Disable 'E-Mail (SMTP)'
Enable 'SNMP'
Disable 'SNMP'
Set to 'Not Configured'

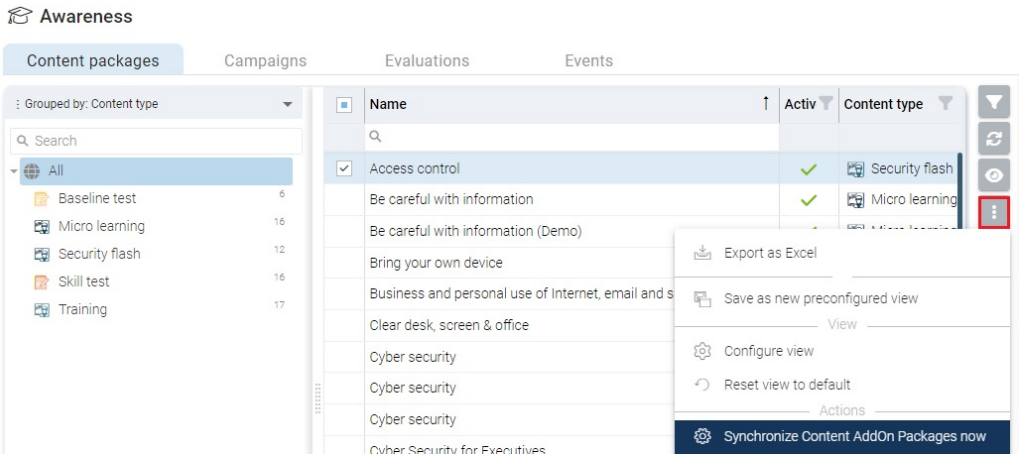
5 Synchronize Content AddOn packages

If you are using DriveLock On-Premise, your Content AddOn packages can also be manually synchronized from DriveLock Enterprise Service (DES) by proceeding as illustrated:

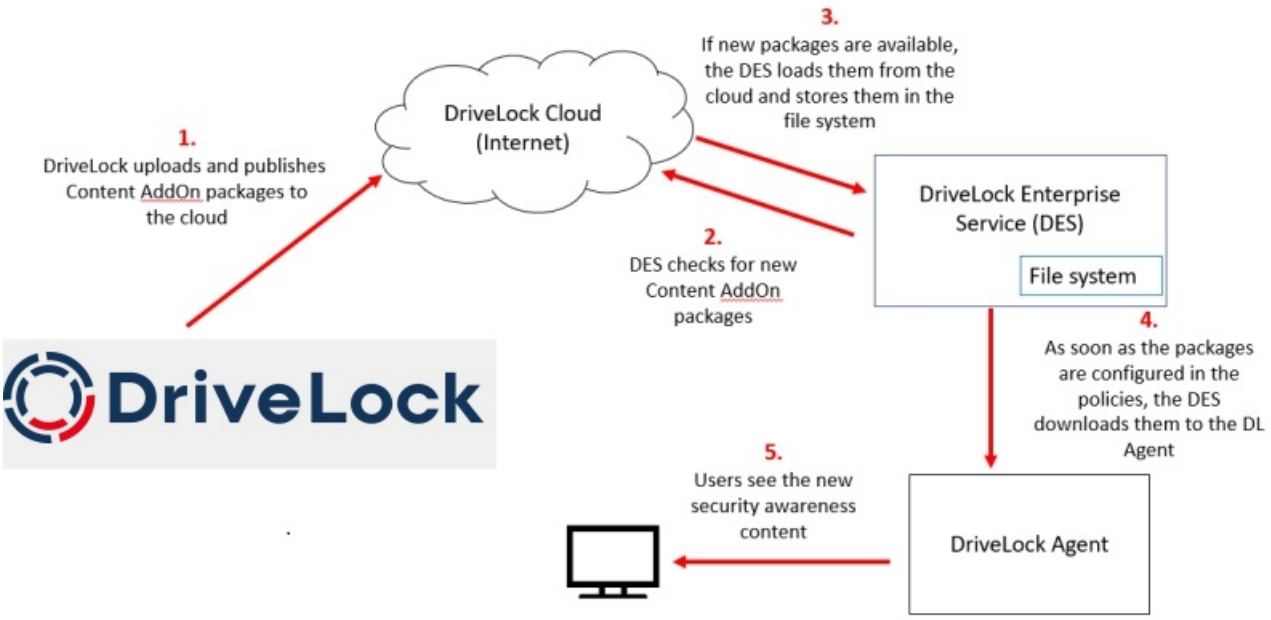


1. In the DriveLock Management Console (DMC), open the **DriveLock Enterprise Services** node.
2. Select the **server** that is 'responsible' for your Content AddOn packages.
3. Open the context menu and then the **All Tasks** menu command.
4. Click **Synchronize Content AddOn packages**.
5. All Content AddOn packages are now up to date.

If you are using the DOC with DriveLock Managed Services, you can also synchronize the Content AddOn packages manually by clicking the **Synchronize Content AddOn packages** menu command on the **Content Packages** tab in the Awareness menu as illustrated.



5.1 Synchronization overview



6 Usage of security awareness campaigns

Campaigns created in DriveLock Operations Center (DOC) can only use content packages. They are automatically configured so that they are shown when a user logs in or they can be accessed from the Security Awareness library. Configuring in the DOC is faster and easier, but offers fewer configuration options.

6.1 When starting an application

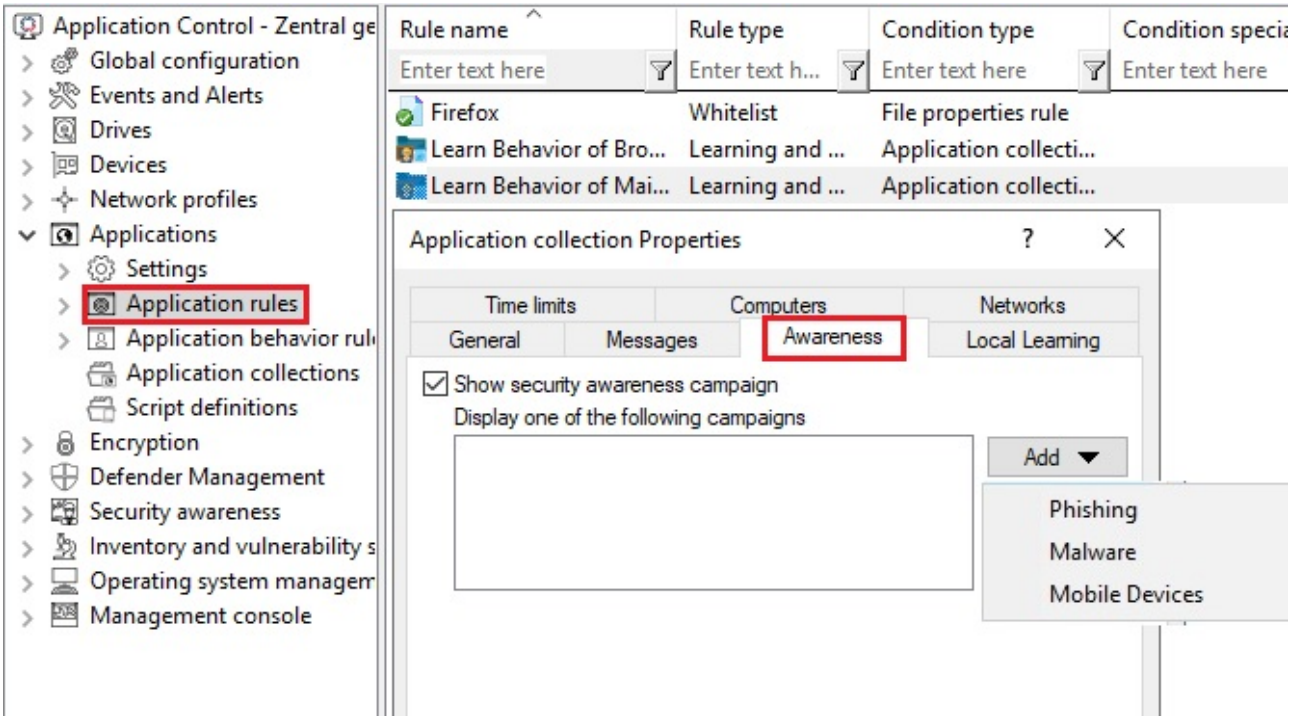
To trigger security awareness campaigns when users start an application, follow the steps below. This procedure applies to all application rules.

> Note: DriveLock Application Control requires a separate license and is not part of the standard DriveLock product range. The display of a security awareness campaign as a consequence of starting an application depends on the **Scanning and blocking mode**. Please refer to the Application Control documentation for more information.

1. Select the **Applications** node in the policy configuration.
2. Select the **Application rule** (see figure below) where you want to set security awareness and open the context menu.
3. Click **New**, then the rule and open the **Awareness** tab in the Properties dialog.
4. Select **Show security awareness campaign** and add the campaign you created earlier.

   > Note: The DriveLock agent will show the campaign according to the settings you specified when creating the campaign (e.g. how often and at what times it should be displayed or repeated). Campaigns with the same priority appear in random order.

5. Confirm your settings.



6.2 When connecting a drive

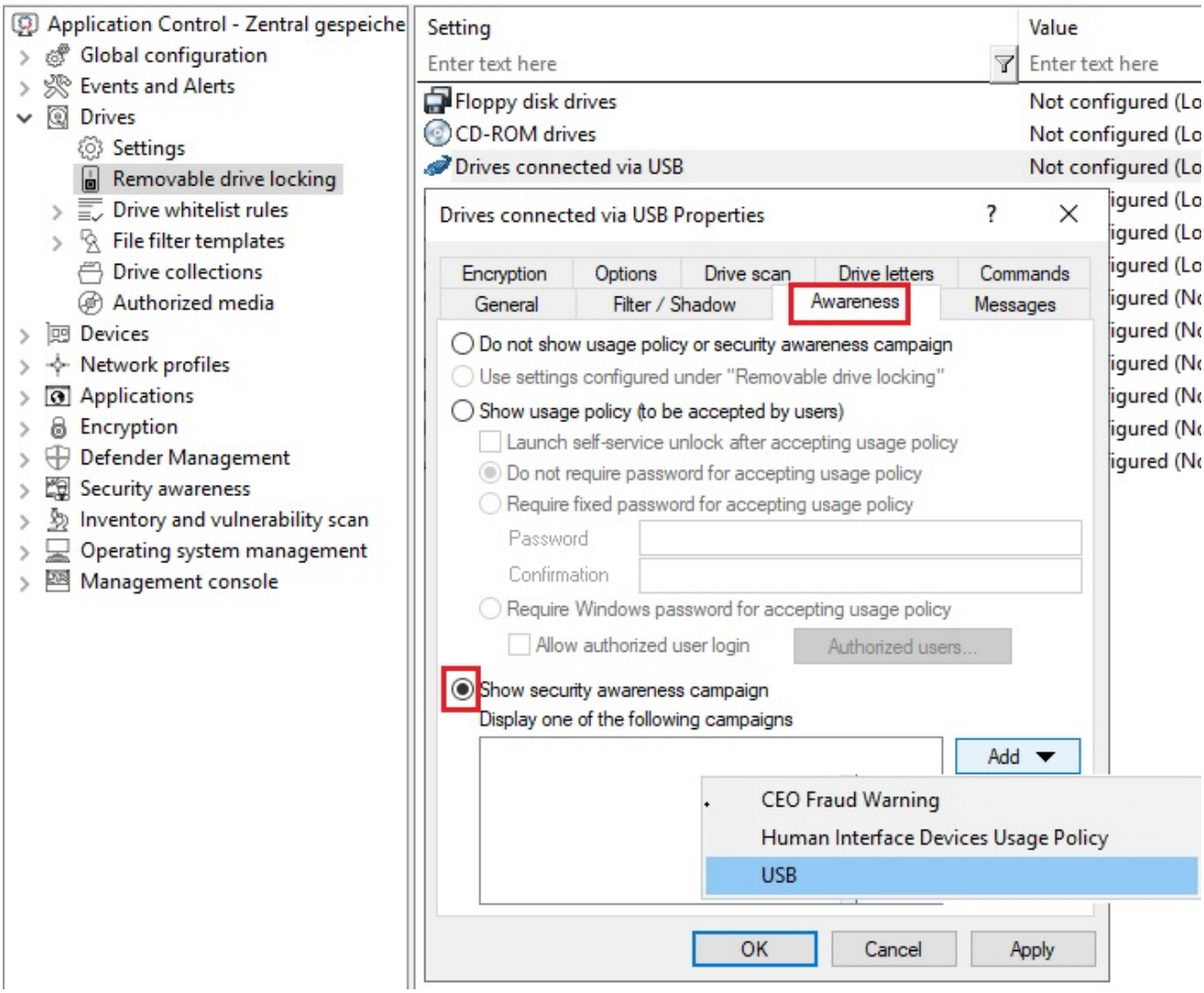
To configure security awareness to display a campaign when connecting a drive, proceed as indicated in the figure. This procedure applies to all types of drives.

1. Select the **Drives** node in the policy configuration.
2. Select the drive type you want to make security awareness settings for in the **Removable drive locking** section. In the example below, this is a USB bus connected drive.
3. Double-click the drive to open the Properties dialog.
4. On the **Awareness** tab, you can specify the following:
   - If you want to **Show a usage policy**, select this option. You can also specify passwords that must be entered when accepting the policy or check the **Launch self-service unlock after accepting usage policy** option so that the user can use the device after having confirmed the policy.
   - If you want other users than the user logged on to Windows to confirm the policy, select **Require Windows password for accepting usage policy** and **Allow authorized user login**. Click **Authorized users** to enter these users in a list and check **Enable "login as user" option by default**. The self-service wizard will "run as" the authorized user.

> Note: Click here to find out how you can create a usage policy.

- You want to **display an awareness campaign** when a user attempts to connect to the device. Now you can add a campaign you created earlier.
  Select it from the list that opens after you click **Add**.

5. Confirm your settings.

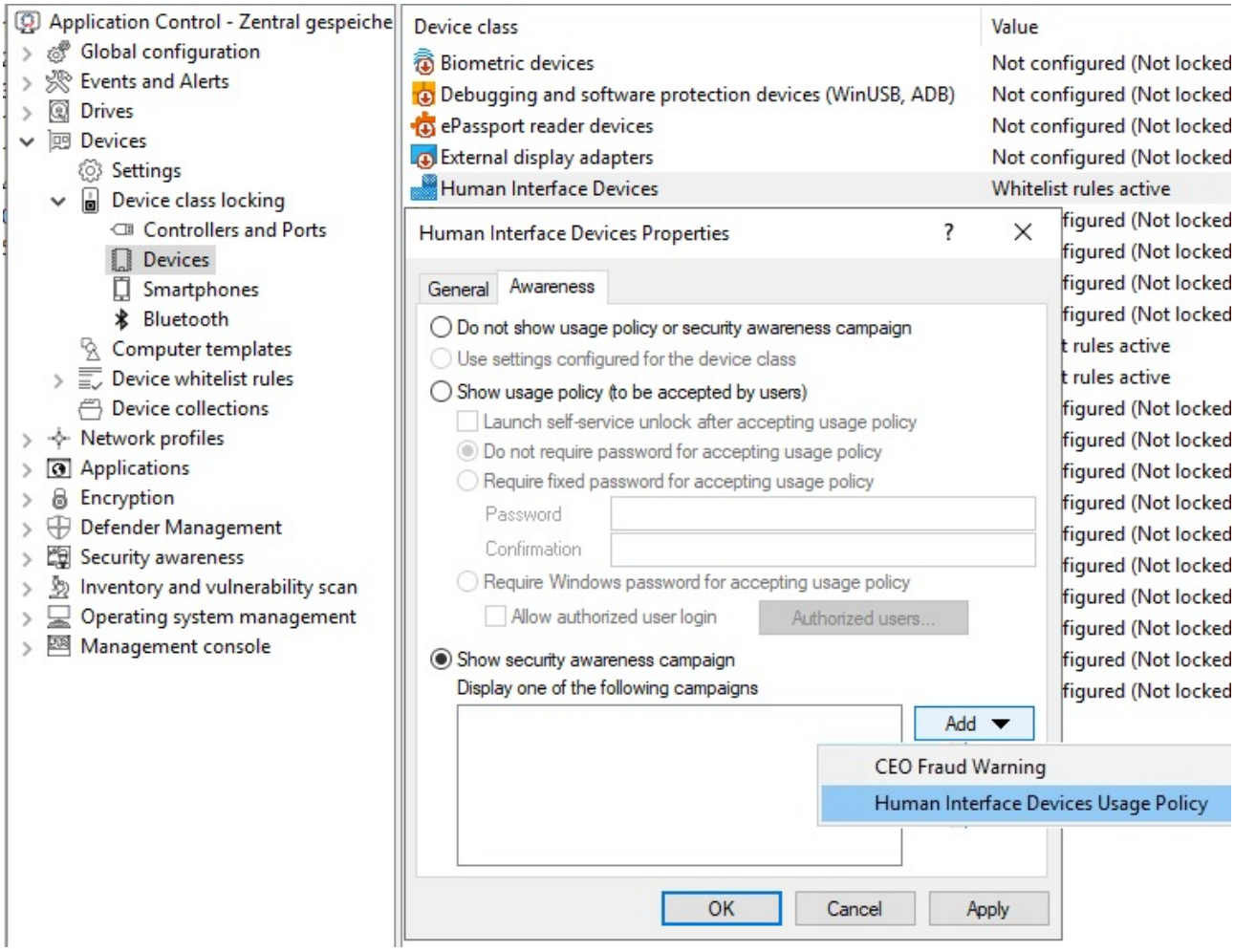


For **drive whitelist rules**, security awareness campaigns can be included with all rules except the following: network drive rules, WebDAV network drive rule, and terminal services rules.

6.3 When connecting devices

To configure security awareness when a device is being used, follow the steps illustrated below. This procedure applies to all devices and all smartphones, plus all adapters and interfaces except COM and LPT, and also to all device whitelist rules.

The example below shows how an awareness campaign will be displayed once a user tries to connect an input device (HID) to their computer at work.



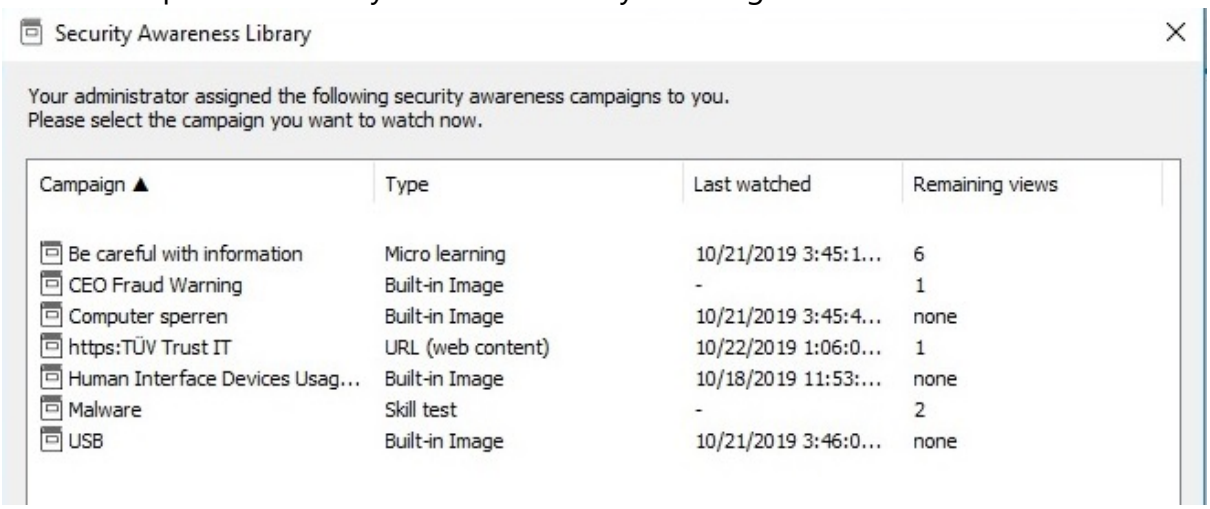
1. In the policy configuration, select the **Devices** node.
2. In the **Device class locking** section, select the device class you want to specify security awareness settings for.
3. On the **Awareness** tab you can configure the same settings as for the drives.
4. Confirm your configuration.

7 DriveLock Agent

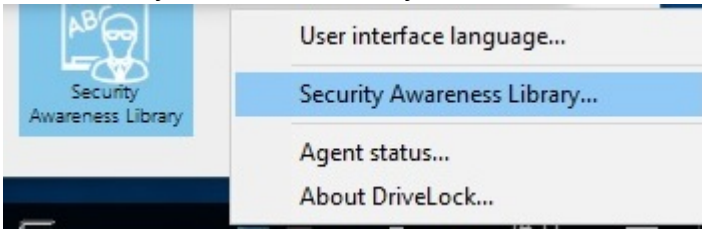
7.1 Display on the DriveLock Agent

Campaigns are displayed on the DriveLock Agent according to the settings in the policy.

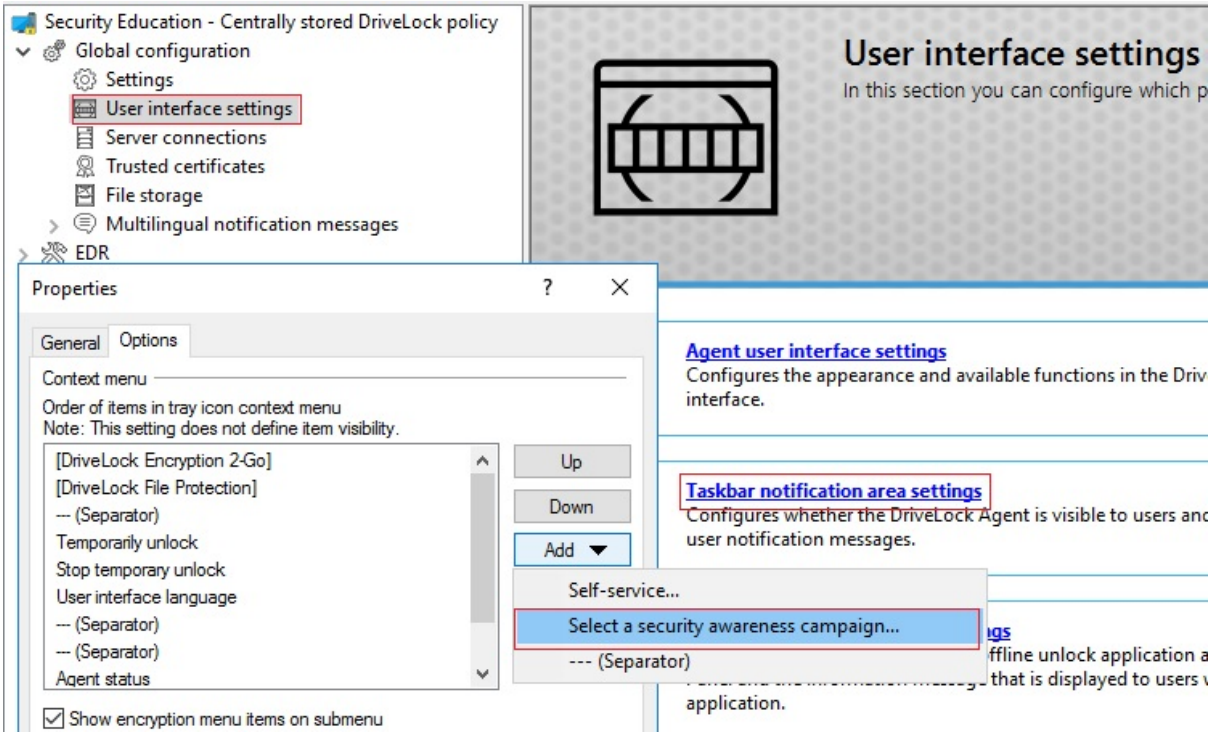
- Users can open the security awareness library in the agent user interface:



- The security awareness library can also be accessed via the tray icon on the agent:



In order for this to work, select **Taskbar notification area settings** in the policy in **Agent user interface settings** beforehand.
On the **Options** tab, add the option **Select a security awareness campaign...**(see figure).
Then the user can select a campaign on the agent.


Security Education - Centrally stored DriveLock policy
Global configuration
Settings
User interface settings
Server connections
Trusted certificates
File storage
Multilingual notification messages
EDR
User interface settings
In this section you can configure which p
Properties
General
Options
Context menu
Order of items in tray icon context menu
Note: This setting does not define item visibility.
[DriveLock Encryption 2-Go]
[DriveLock File Protection]
--- (Separator)
Temporarily unlock
Stop temporary unlock
User interface language
--- (Separator)
--- (Separator)
Agent status
Up
Down
Add
Self-service...
Select a security awareness campaign...
--- (Separator)
Show encryption menu items on submenu
Agent user interface settings
Configures the appearance and available functions in the Driv
interface.
Taskbar notification area settings
Configures whether the DriveLock Agent is visible to users and
user notification messages.
application.

Copyright