




# DriveLock Security Awareness

Documentation 2022.1 SP1

---

DriveLock SE 2022



---

# Table of Contents

<b>1 WELCOME TO DRIVELOCK SECURITY AWARENESS</b> .....	<b>4</b>
<b>2 BASICS</b> .....	<b>5</b>
2.1 DriveLock Security Awareness .....	5
2.2 The Security Awareness Content AddOn .....	5
<b>3 CONTENT ADDON PACKAGES</b> .....	<b>6</b>
3.1 Available languages .....	7
3.2 The principle behind Content AddOn packages on the DriveLock Enterprise Service (DES) .....	7
3.3 Specify security awareness settings in the server properties .....	8
3.4 Synchronizing Content AddOn packages .....	8
<b>4 CONFIGURE SECURITY AWARENESS</b> .....	<b>10</b>
4.1 General security awareness settings .....	10
4.2 Create campaigns .....	12
4.2.1 Creating security awareness campaigns .....	12
4.2.1.1 Contents of a new campaign .....	12
4.2.1.2 Trigger for a new campaign .....	13
4.2.1.3 Recurrence of a new campaign .....	14
4.2.1.4 General settings for the new campaign .....	15
4.2.2 Deploying security awareness campaigns to users .....	16
<b>5 HOW TO USE DRIVELOCK SECURITY AWARENESS</b> .....	<b>18</b>
5.1 Security awareness when launching an application .....	18
5.2 Security awareness when connecting a drive .....	19
5.3 Security awareness when using a device .....	21
<b>6 SECURITY AWARENESS EVENTS</b> .....	<b>23</b>
6.1 Activate security awareness events on the DES .....	23
<b>7 DRIVELOCK AGENT</b> .....	<b>24</b>

7.1 Security awareness campaigns on the DriveLock Agent .....	24
<b>8 SECURITY AWARENESS IN THE DRIVELOCK OPERATIONS CENTER (DOC) .....</b>	<b>26</b>
8.1 The Security Awareness view .....	27
<b>COPYRIGHT .....</b>	<b>29</b>

# 1 Welcome to DriveLock Security Awareness

Security awareness is a feature of the DriveLock Endpoint Protection Platform and is included in the standard DriveLock products.

[Security Awareness Content](#) focuses entirely on the security awareness feature. The DriveLock functionalities for drive, device or application control are not available.

So whether you want to use security awareness within your familiar DriveLock environment or just distribute security-related campaigns with Smart SecurityEducation, you are well equipped to raise your team's awareness of security-related topics and increase their level of security awareness.

Minimize the risks to your IT security by using our security awareness feature!

## 2 Basics

### 2.1 DriveLock Security Awareness

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.

 Note: When using the complete DriveLock functionality, you can define campaigns individually for [drives](#), [devices](#) and [applications](#) within rules.

For more information on how to create campaigns, see [Creating security awareness campaigns](#).

### 2.2 The Security Awareness Content AddOn

This AddOn requires a license and contains additional multimedia content (as complete security training), you can use to create campaigns. The content is updated regularly and automatically via the Internet on a subscription basis.


 Note: Please make sure that the version of your DriveLock agents is suitable for the content add-on packages. For example, version 22.1 packages will only work on version 22.1. agents with SP1, but not on older agent versions. Also, with this version, you will need Microsoft WebView2 to display the content correctly on agent computers. For the latest information, see the corresponding version's Release Notes auf [DriveLock Online Help](#).

See how security awareness packages are updated via DriveLock Enterprise Service (DES) [here](#).

### 3 Content AddOn packages

You can find the Content Addon packages in the following location in the DriveLock Management Console:

In the **DriveLock Enterprise Services** node in **Product packages and files** you can see the available **Content Addon packages**.

 **Note:** You will only receive a detailed overview of all available packages if you subscribed to the **Security Awareness Content AddOn**. If the AddOn is not licensed yet, you only see a selection of demo packages.

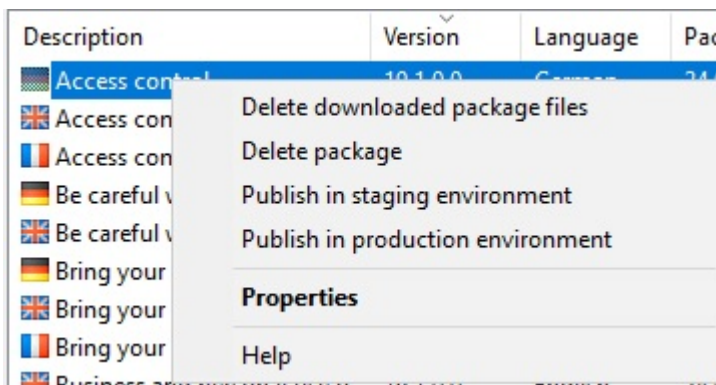
<ul style="list-style-type: none"> <li>&gt; Policies</li> <li>&gt; Policy assignments</li> <li>&gt; DriveLock Enterprise Services [dlservice/root]             <ul style="list-style-type: none"> <li>Servers</li> <li>Tenants</li> <li>&gt; Product packages and files                 <ul style="list-style-type: none"> <li>Software packages</li> <li>Content AddOn Packages (SecAware)</li> </ul> </li> </ul> </li> </ul>	<table border="1"> <tr> <td></td> <td>Cyber Security for Executives</td> <td>19.1.0.0</td> <td>English</td> <td>24.06.2019 13:23:47</td> <td>46,3 MB</td> <td>Training</td> <td>root</td> <td>Unpublished</td> <td>Published</td> <td>DES</td> </tr> <tr> <td></td> <td>Risk Management</td> <td>19.1.0.0</td> <td>English</td> <td>24.06.2019 13:23:40</td> <td>23,8 MB</td> <td>Skill test</td> <td>root</td> <td>Unpublished</td> <td>Published</td> <td>DES</td> </tr> <tr> <td></td> <td>Cyber security</td> <td>19.1.0.0</td> <td>English</td> <td>24.06.2019 13:23:45</td> <td>56,9 MB</td> <td>Training</td> <td>root</td> <td>Unpublished</td> <td>Published</td> <td>DES</td> </tr> <tr> <td></td> <td>Working in the cloud</td> <td>19.1.0.0</td> <td>English</td> <td>24.06.2019 13:24:13</td> <td>64,8 MB</td> <td>Training</td> <td>root</td> <td>Unpublished</td> <td>Published</td> <td>DES</td> </tr> <tr> <td></td> <td>Strong passwords</td> <td>19.1.0.0</td> <td>English</td> <td>24.06.2019 13:58:20</td> <td>44,1 MB</td> <td>Security flash</td> <td>root</td> <td>Unpublished</td> <td>Published</td> <td>DES</td> </tr> <tr> <td></td> <td>Work securely outside the o...</td> <td>19.1.0.0</td> <td>English</td> <td>24.06.2019 13:21:15</td> <td>30,8 MB</td> <td>Micro learning</td> <td>root</td> <td>Unpublished</td> <td>Published</td> <td>DES</td> </tr> <tr> <td></td> <td>EU General Data Protection ...</td> <td>19.1.0.0</td> <td>English</td> <td>24.06.2019 13:23:33</td> <td>23,8 MB</td> <td>Skill test</td> <td>root</td> <td>Unpublished</td> <td>Published</td> <td>DES</td> </tr> <tr> <td></td> <td>Use of passwords</td> <td>19.1.0.0</td> <td>English</td> <td>24.06.2019 13:21:13</td> <td>37,3 MB</td> <td>Micro learning</td> <td>root</td> <td>Unpublished</td> <td>Published</td> <td>DES</td> </tr> </table>		Cyber Security for Executives	19.1.0.0	English	24.06.2019 13:23:47	46,3 MB	Training	root	Unpublished	Published	DES		Risk Management	19.1.0.0	English	24.06.2019 13:23:40	23,8 MB	Skill test	root	Unpublished	Published	DES		Cyber security	19.1.0.0	English	24.06.2019 13:23:45	56,9 MB	Training	root	Unpublished	Published	DES		Working in the cloud	19.1.0.0	English	24.06.2019 13:24:13	64,8 MB	Training	root	Unpublished	Published	DES		Strong passwords	19.1.0.0	English	24.06.2019 13:58:20	44,1 MB	Security flash	root	Unpublished	Published	DES		Work securely outside the o...	19.1.0.0	English	24.06.2019 13:21:15	30,8 MB	Micro learning	root	Unpublished	Published	DES		EU General Data Protection ...	19.1.0.0	English	24.06.2019 13:23:33	23,8 MB	Skill test	root	Unpublished	Published	DES		Use of passwords	19.1.0.0	English	24.06.2019 13:21:13	37,3 MB	Micro learning	root	Unpublished	Published	DES
	Cyber Security for Executives	19.1.0.0	English	24.06.2019 13:23:47	46,3 MB	Training	root	Unpublished	Published	DES																																																																															
	Risk Management	19.1.0.0	English	24.06.2019 13:23:40	23,8 MB	Skill test	root	Unpublished	Published	DES																																																																															
	Cyber security	19.1.0.0	English	24.06.2019 13:23:45	56,9 MB	Training	root	Unpublished	Published	DES																																																																															
	Working in the cloud	19.1.0.0	English	24.06.2019 13:24:13	64,8 MB	Training	root	Unpublished	Published	DES																																																																															
	Strong passwords	19.1.0.0	English	24.06.2019 13:58:20	44,1 MB	Security flash	root	Unpublished	Published	DES																																																																															
	Work securely outside the o...	19.1.0.0	English	24.06.2019 13:21:15	30,8 MB	Micro learning	root	Unpublished	Published	DES																																																																															
	EU General Data Protection ...	19.1.0.0	English	24.06.2019 13:23:33	23,8 MB	Skill test	root	Unpublished	Published	DES																																																																															
	Use of passwords	19.1.0.0	English	24.06.2019 13:21:13	37,3 MB	Micro learning	root	Unpublished	Published	DES																																																																															

In addition to general information, such as version, language, timestamp, size or content type, note the following properties, since they can also be changed in the context menu of the respective package:

- **Staging status and Production status:**

The status can be either **Published** or **Unpublished**, depending on whether you have already published the package in the staging or production environment.

You can change this from the context menu or from the settings in the server properties.



- **Source:**

- **Not specified yet:** The package is available in the cloud but not yet on the DES. Select the context menu command **Download to DES** to make the package available on the DES.

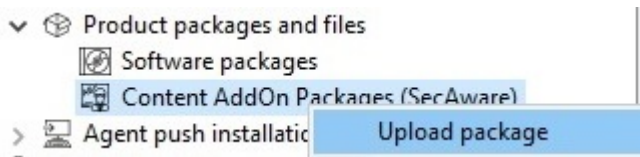
- **DES:** The package is available on the DES..

Note: The settings for updating and publishing are defined in the [server properties](#).

Note: Please note that an Internet connection is mandatory to keep the Content AddOn packages up to date.

Note that you can only use the **Upload Package** command to upload your own training content in a standardized format.

Please contact our Consulting Service for further information.

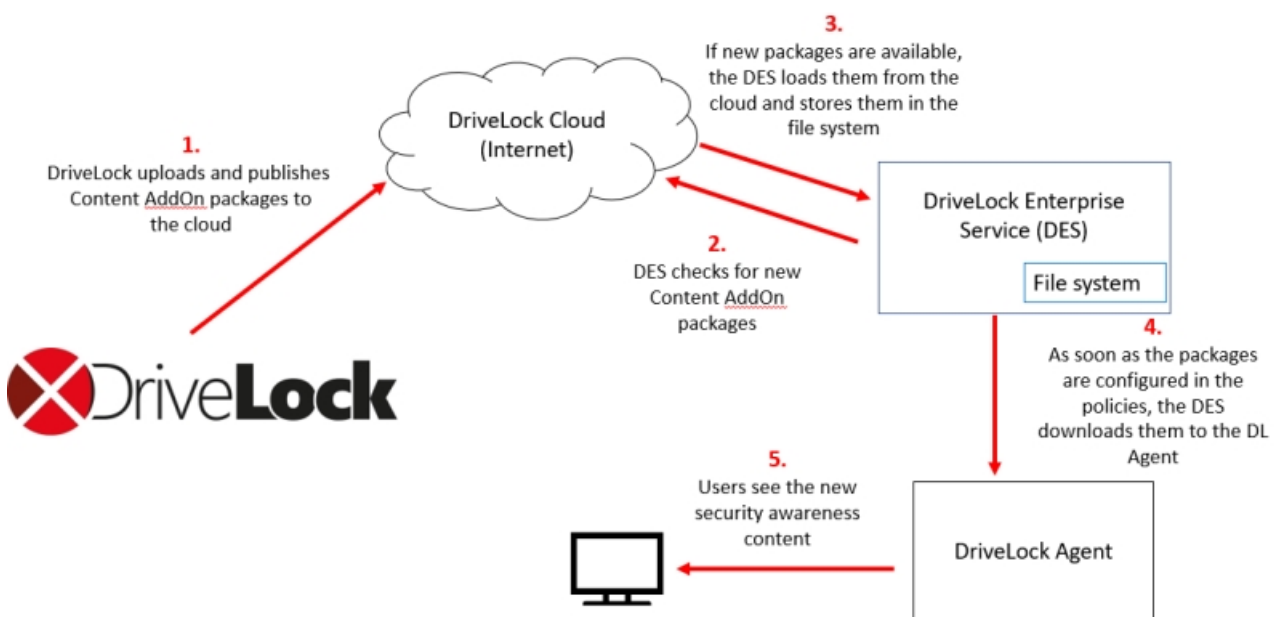


### 3.1 Available languages

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

Warning: Dutch is no longer supported, which means that these packages are automatically deleted when the DES is updated to this version.

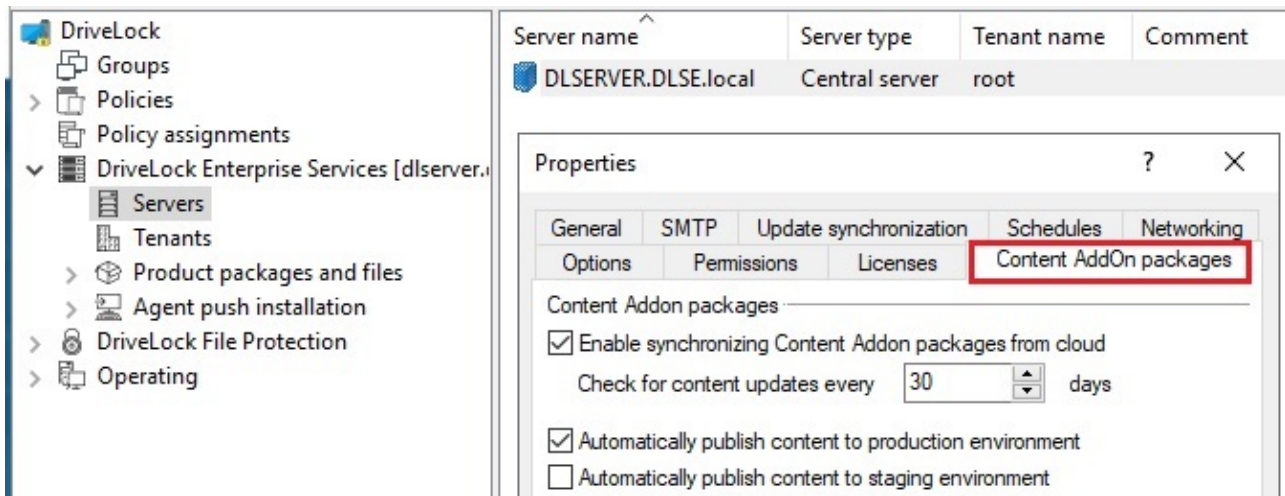
### 3.2 The principle behind Content AddOn packages on the DriveLock Enterprise Service (DES)






### 3.3 Specify security awareness settings in the server properties

To keep your Content AddOn packages up to date, you can have your server check for updates automatically. Proceed as illustrated:



1. Open the **DriveLock Enterprise Services** node in the DriveLock Management Console.
2. Select the **server** handling your Content AddOn packages.
3. Open the server properties from the context menu and go to the **Content AddOn packages** tab.
4. Select the **Enable synchronizing Content AddOn packages from cloud** option and then specify how often you want the server to check for updates. We recommend 30 days, which is sufficient. Click [here](#) to find out how that works.
5. You can also specify whether the updates will be automatically published in the production and/or staging environment.

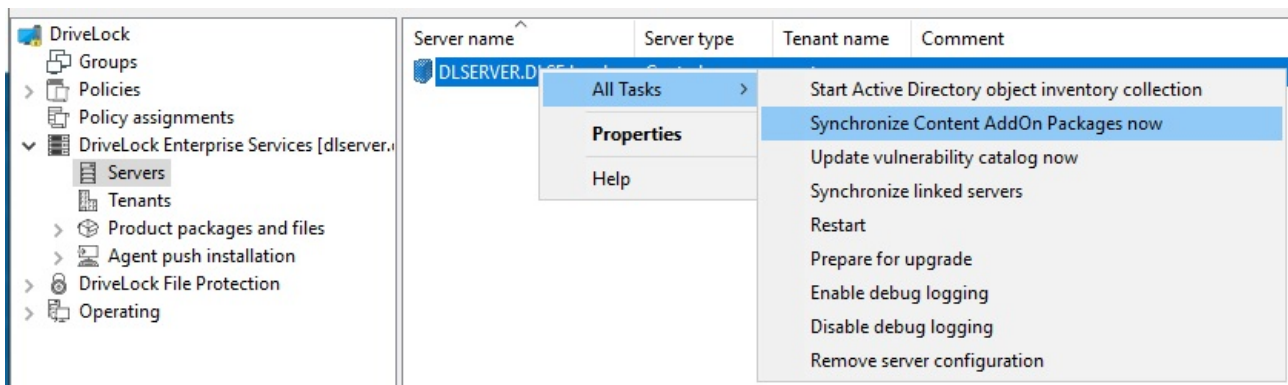
 Note: Only after a package is published, the agents can download it. If you set either (or both) of these options, the content is published automatically after downloading the packages, depending on your selection for production and/or staging environment.

6. Confirm your settings.

### 3.4 Synchronizing Content AddOn packages

You can also synchronize your Content AddOn packages manually by proceeding as illustrated below:





1. Open the **DriveLock Enterprise Services** node in the DriveLock Management Console (MMC).
2. Select the **server** handling your Content AddOn packages.
3. Open the context menu and select **All Tasks**.
4. Click **Synchronize Content AddOn packages now**.
5. All Content AddOn packages are up to date now.

## 4 Configure security awareness

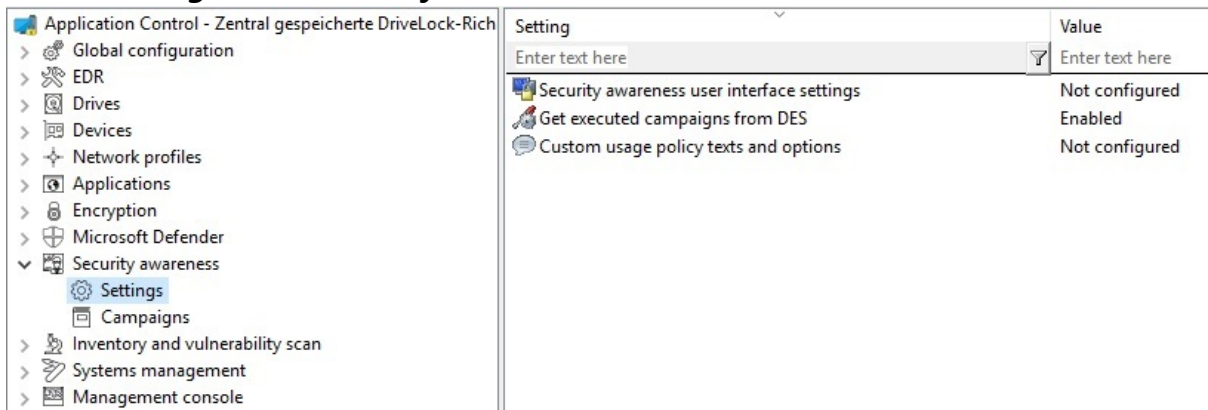
To configure security awareness, please proceed as follows:

1. Select the **Policies** node in the DriveLock Management Console.
2. Double-click any policy.
3. You can start with the configuration in the **Security awareness** node.
  - In the **Settings** section you can enter general settings for all campaigns.
  - Select **Campaigns** to create new campaigns. For more information, refer to chapter [Creating campaigns](#).

### 4.1 General security awareness settings

Please do the following:

1. Select **Settings** in the **Security awareness** node.




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


- **All campaigns**

On this tab you can define settings that affect **all** campaigns.

- Here you can determine whether the window displaying the security awareness campaign remains visible to the user at all times.
- If you want to show the campaign on the agent computers in full screen mode, select the respective option.


 Note: In full-screen mode, you can display your campaigns most effectively.

- 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 Settings** node and define corresponding notification texts here.

 Note: For more information on how to create multilingual notification messages, please refer to the [Administration Guide](https://drivelock.help) on our website <https://drivelock.help>.

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.

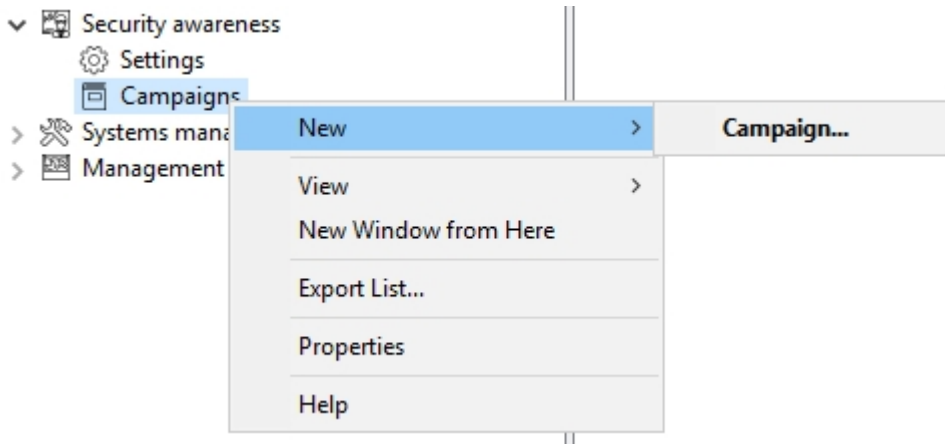
4. Select **Get executed campaigns from DES** to specify that users can "take" their completed campaigns with them when they log on to another computer, i.e. the completed campaigns are no longer displayed there. A request is sent to the DriveLock Enterprise Service (DES).

The default setting is **Disable** because most users work at their own workstation.

## 4.2 Create campaigns


### 4.2.1 Creating security awareness campaigns

To create a new campaign, proceed as illustrated below:



In the context menu for **Campaigns**, choose **New** and then **Campaign...**. The **New campaign** wizard starts and you proceed through the following dialog pages:

1. [Contents 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 [properties of the security awareness campaign](#). Here you can also change all settings you have made in the **New campaign** wizard.

#### 4.2.1.1 Contents of a new campaign


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.

#### 4.2.1.2 Trigger for a new campaign

The **Trigger** dialog page allows you to specify the event for which 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 activated in DriveLock Smart SecurityEducation:

- **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.

#### 4.2.1.3 Recurrence of a new campaign

The **Recurrence** dialog page allows you to specify how often your campaign is displayed or repeated.

You can configure the following here:

- **Show campaign x times**

Limit the campaign display by specifying a certain number or select **never** or **indefinitely** from the drop-down list.

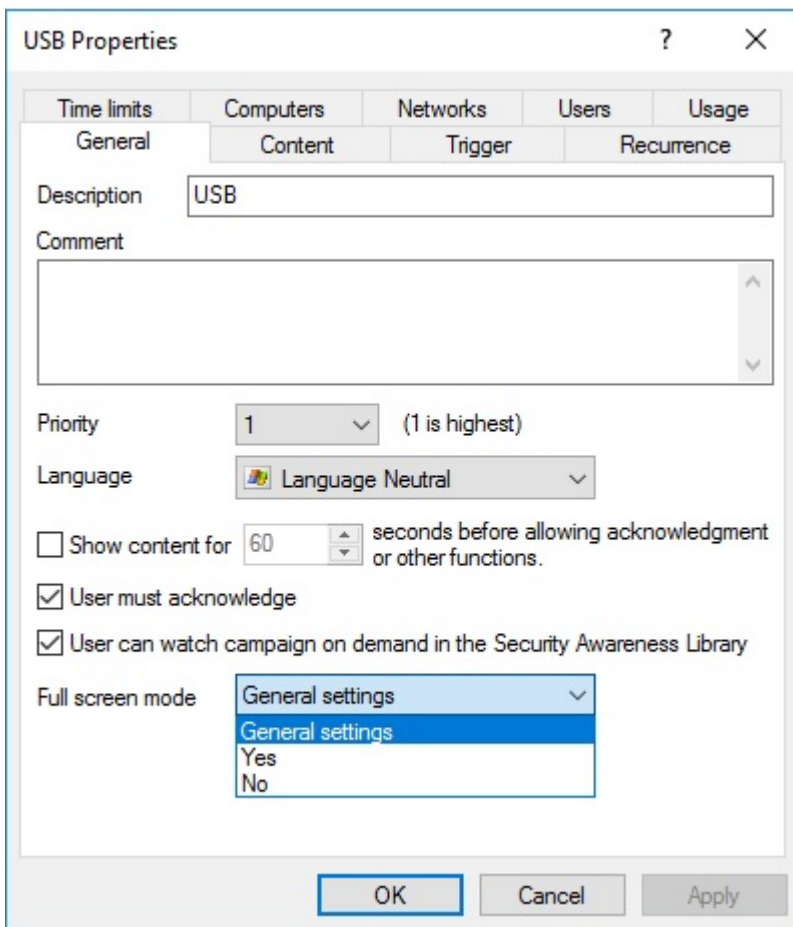
Choosing **never** makes sense if you do not want to display your campaign at first. You can change this later in the campaign's Properties dialog.

- **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).
- If the campaign was only partially displayed or an error occurred, you can specify that it is displayed again after a certain time.

#### 4.2.1.4 General settings for the new campaign

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




The screenshot shows the 'USB 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: 'Time limits', 'Computers', 'Networks', 'Users', and 'Usage'. Under the 'Computers' tab, there are four sub-tabs: 'General', 'Content', 'Trigger', and 'Recurrence'. The 'General' sub-tab is active. The 'Description' field contains the text 'USB'. The 'Comment' field is empty. The 'Priority' is set to '1' with a dropdown arrow and the text '(1 is highest)'. The 'Language' is set to 'Language Neutral' with a dropdown arrow. There are three checkboxes: 'Show content for 60 seconds before allowing acknowledgment or other functions.' (unchecked), 'User must acknowledge' (checked), and 'User can watch campaign on demand in the Security Awareness Library' (checked). The 'Full screen mode' dropdown menu is open, showing 'General settings' (selected), 'Yes', and 'No'. At the bottom are 'OK', 'Cancel', and 'Apply' buttons.


- **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 appear 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.

 Note: Once you have updated DriveLock to version 2019.2, this option is pre-set for all existing campaigns. Please note that the DriveLock Agents must also be updated to this version.

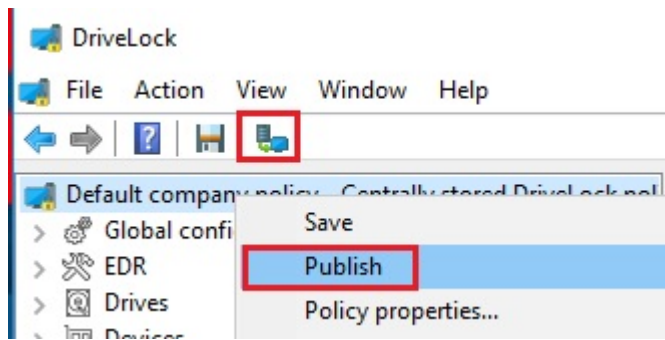
- Full screen mode:  
Select **Yes** if you want to show the campaign in full screen mode on the agent computer.  
Select **General settings** if you want to use the [security awareness settings](#) that apply to all campaigns for this specific campaign.  
Select **No** if you do not want full screen 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.

#### 4.2.2 Deploying security awareness campaigns to users

To deploy a new security awareness campaign to the appropriate users (computers with DriveLock agents), you must first publish the policy.

1. Open the context menu of the policy and select **Publish**. Or click the **Publish** button on the menu bar.




2. You can enter an optional comment.
3. If you want to sign the policy, check the appropriate option and select the certificate.
4. The policy is now published and will be used by DriveLock agents.


For more information on publishing policies and selecting signing certificates, see the **DriveLock Administration Guide**, available at <https://drivelock.help/>.

## 5 How to use DriveLock Security Awareness


### 5.1 Security awareness when launching an application

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

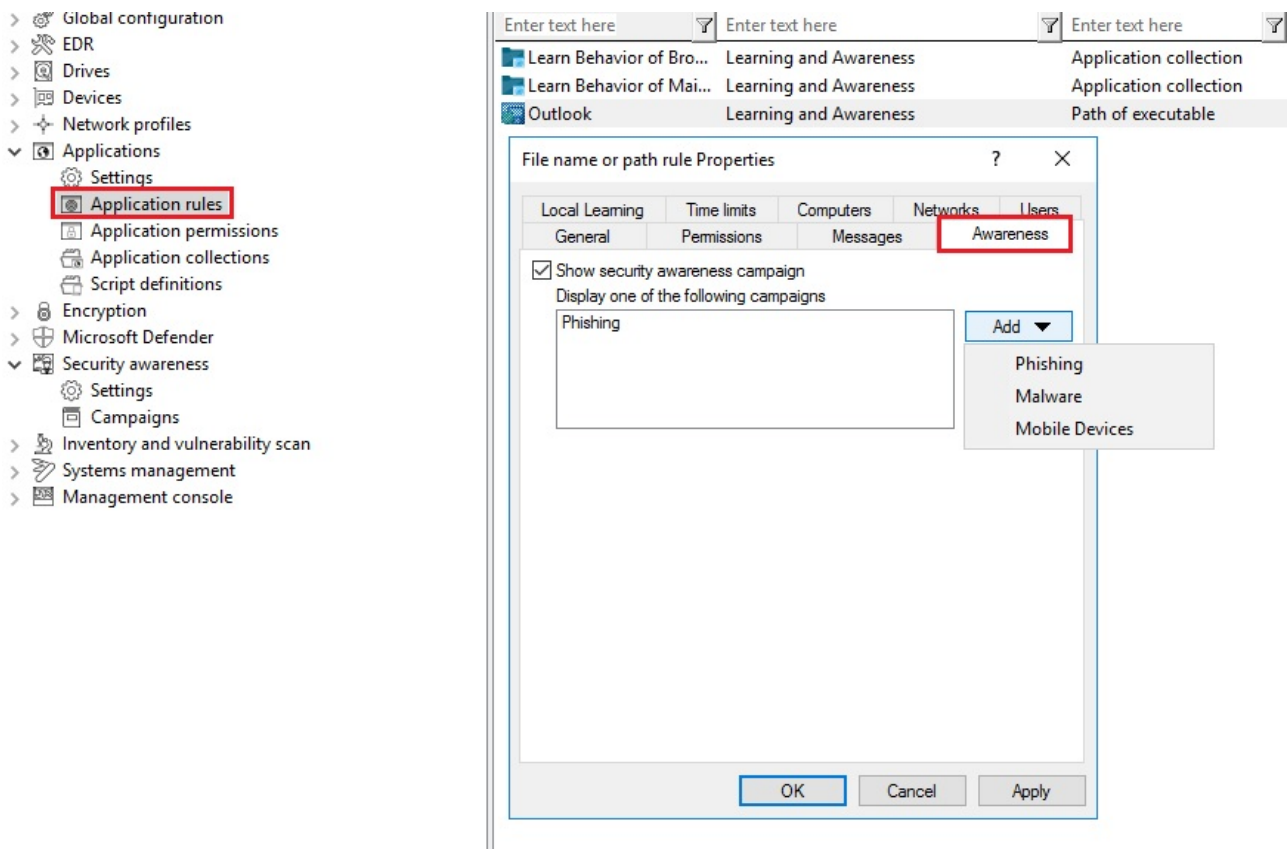
 Note: DriveLock Application Control requires a separate license and is not part of the standard DriveLock product range.

 Note: Please note that the display of a security awareness campaign depends on the higher-level **Scanning and blocking mode** that you have defined for your application launch. For example, in whitelist mode, the parent rule unblocks a particular application, while in blacklist mode, the parent rule blocks the application. Only if the system has checked and applied the rule already configured, the rule for displaying the security awareness campaign is applied. See Application Control in the Administration Guide for a full description of this procedure.

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.




## 5.2 Security awareness 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.

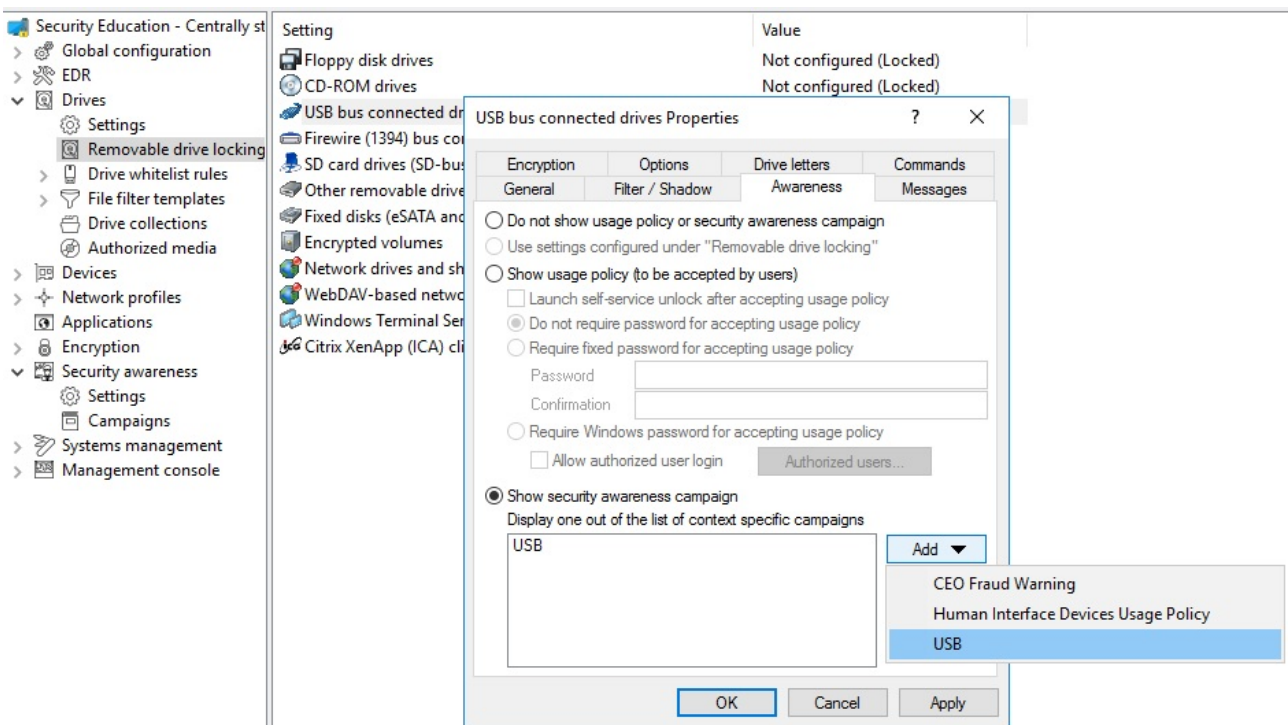
1. Select the **Drives** node in the policy configuration.
2. Select the drive type you want to make security awareness settings for in the **Removable drive locking** section. In the example below, this is a USB bus connected drive.
3. Double-click the drive to open the Properties dialog.
4. On the **Awareness** tab, you can specify the following:
  - You don't want to show a usage policy or a security awareness campaign. This is the default setting.
  - 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.



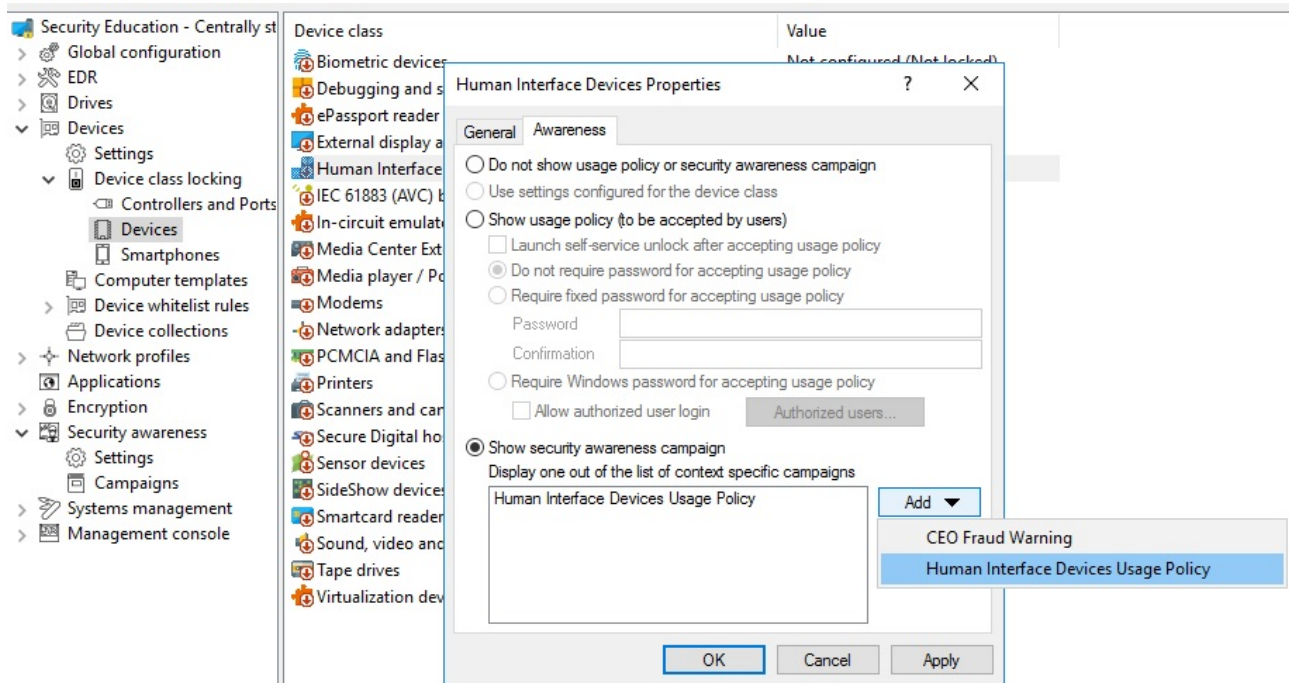
You can set security awareness for the following **Drive whitelist rules**:

- Vendor/Product ID rule
- Drive size rule
- Encrypted media rule
- Base rule

In these cases, you can make more detailed settings for each drive and specify whether a parent setting is applied or overridden. Check the **Use settings configured under "Removable drive locking"** option on the **Awareness** tab.

### 5.3 Security awareness when using a device

To trigger security awareness campaigns when users attempt to connect devices, follow the steps below. This procedure applies to all devices and all smartphones, all adapters and interfaces, except COM and LPT, and to all device whitelist rules.



1. Select the **Devices** node in the policy configuration.
2. Select the device type you want to make security awareness settings for in the **Device class locking** section.

In the example above, an awareness campaign or usage policy will appear when a user attempts to connect a Human Interface Device (HID) to their workstation.

3. Select **Devices** and double-click **Human Interface Devices** to open the Properties dialog.
4. On the **Awareness** tab, you can specify the following:
  - You don't want to show a usage policy or a security awareness campaign. This is the default setting.
  - To display 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.



## 6 Security awareness events

All events that occur on each DriveLock agent are automatically displayed by feature in the DriveLock Management Console in the **EDR** node.

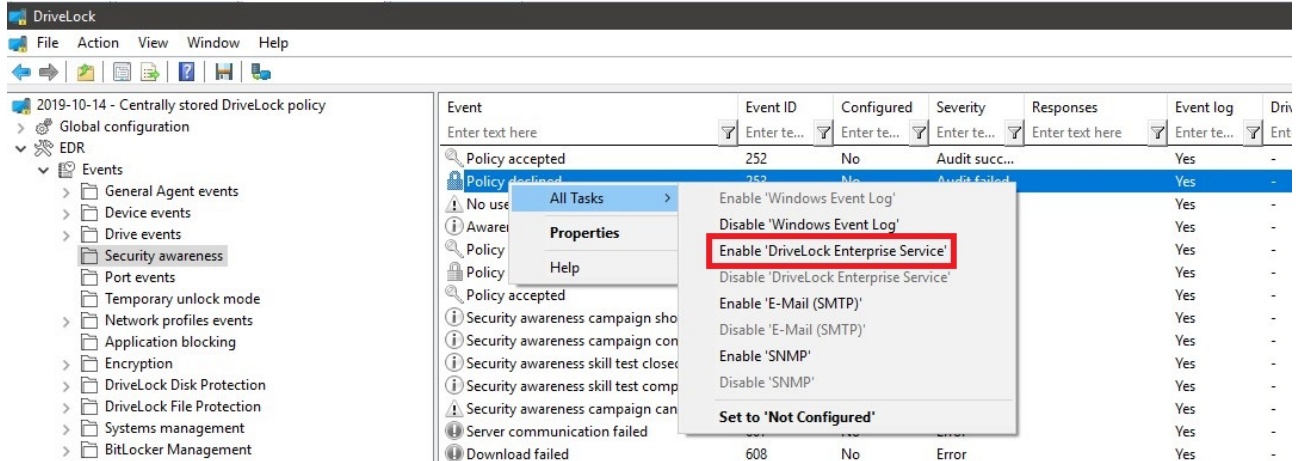
In the **Events** section of the **Security Awareness** sub-node, you can see a list of all security awareness events.

**Warning:** Before you can monitor security awareness events in the DriveLock Control Center (DCC) and DriveLock Operations Center (DOC), they must first be loaded (and thus activated) from the DriveLock Agent to the DriveLock Enterprise Service (DES).

### 6.1 Activate security awareness events on the DES

**Please do the following:**

1. Open the **Security awareness** subnode in the **Events** section of the **EDR** node.
2. Select all events that you want to display in the DCC or DOC and open the context menu.
3. Select **Enable 'DriveLock Enterprise Service'** to upload the events to the DES.

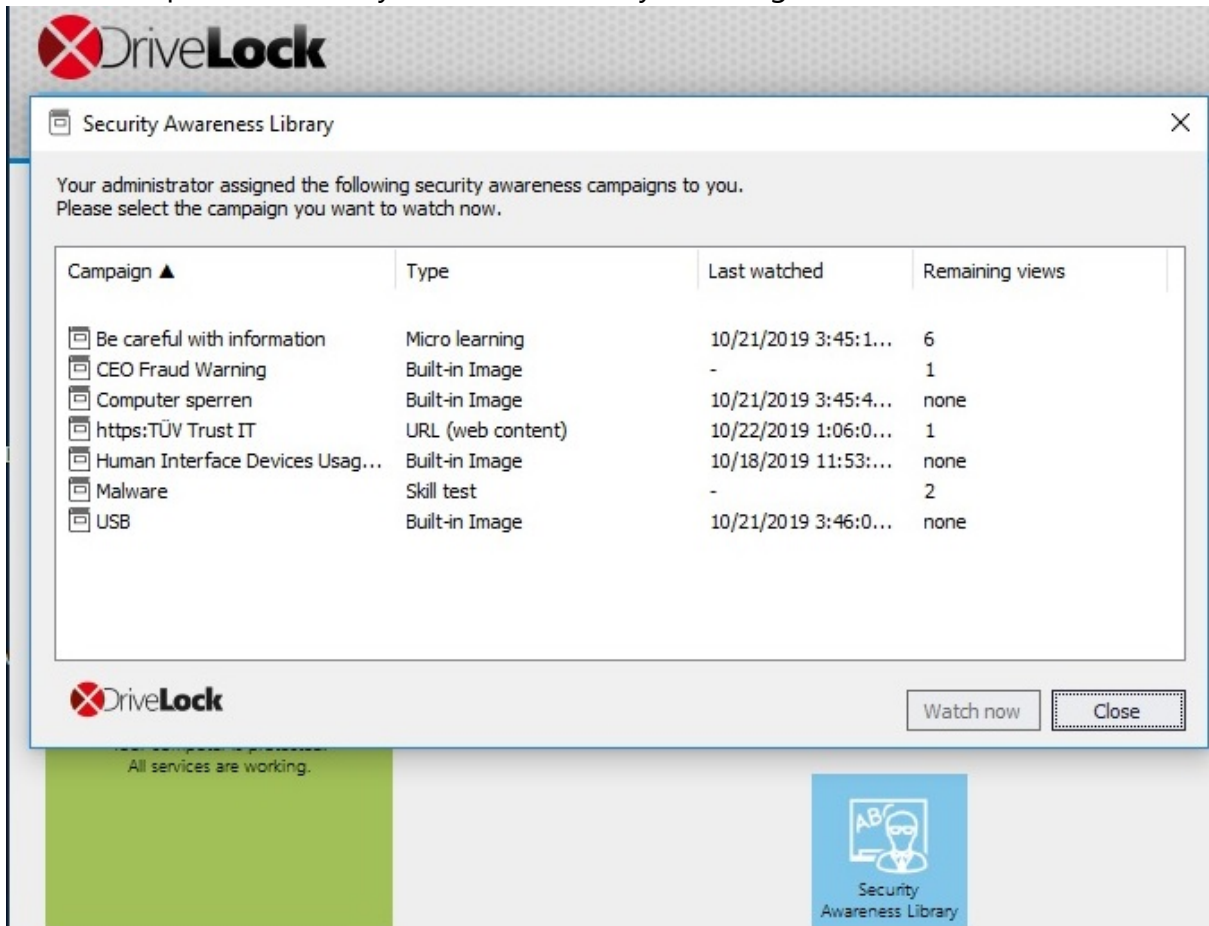


## 7 DriveLock Agent

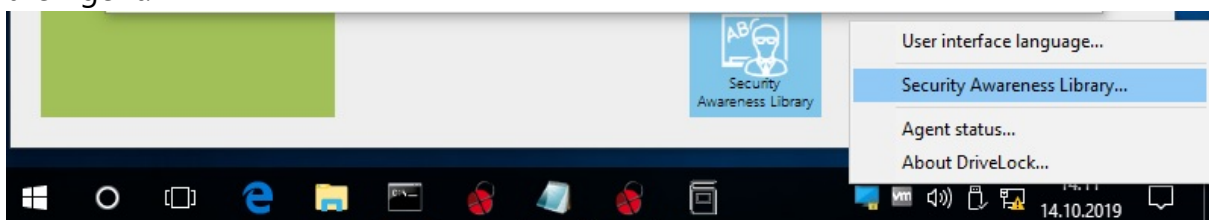
### 7.1 Security awareness campaigns on the DriveLock Agent

Campaigns are displayed to users on the Agent depending on the settings in the policy.

- Users can open the Security Awareness Library in the Agent's user interface:



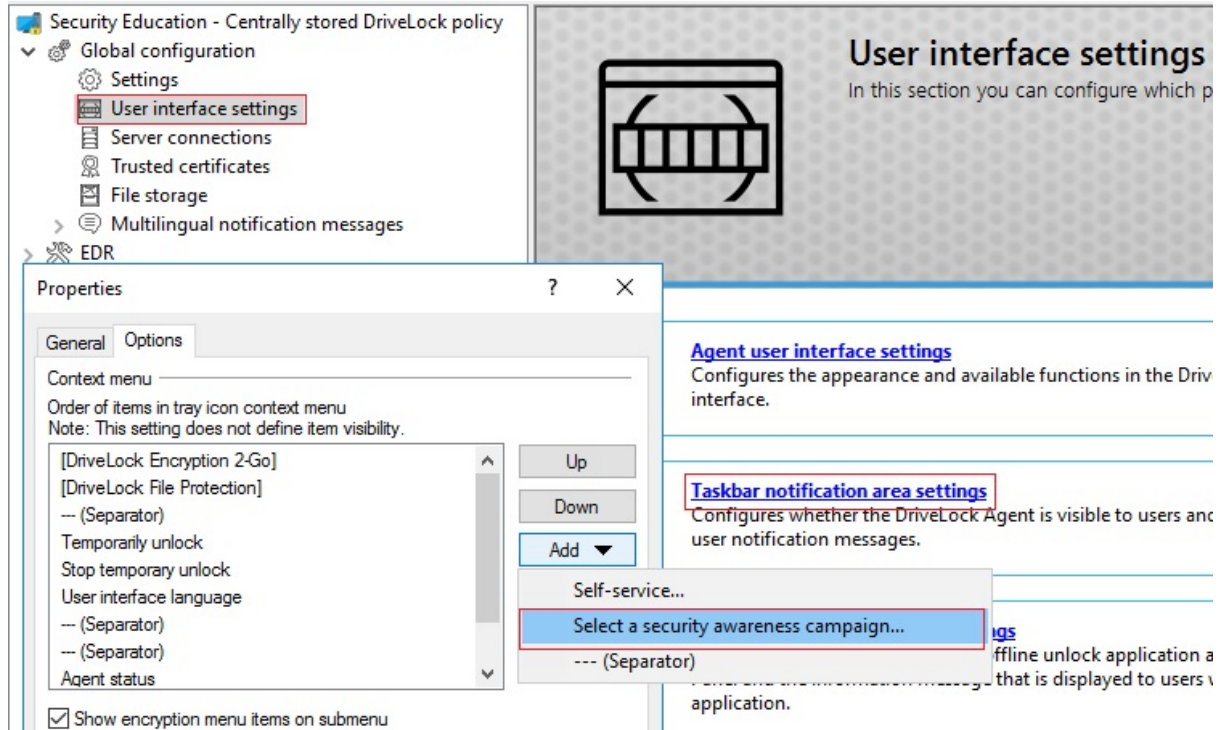
- Alternatively, the Security Awareness Library can be accessed via the taskbar icon on the Agent:



For this, you must first select the **Taskbar notification area settings** option in the policy in the **User interface settings** section (for more information, refer to chapter 6.5.2 in the Administration Manual at [DriveLock Online Help](#)).

Then, add the **Select a security awareness campaign...** entry on the **Options** tab (see figure below).

After that the user can select a campaign from the taskbar on the Agent.

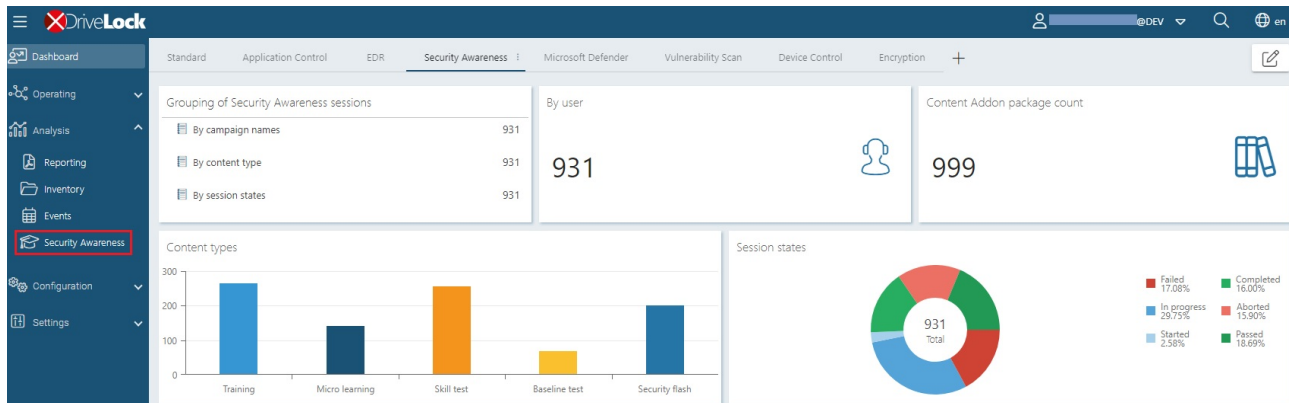


## 8 Security Awareness in the DriveLock Operations Center (DOC)

In the DOC, the Security Awareness Dashboard gives you an overview of your ongoing security awareness campaigns. The course of a campaign is referred to as a 'session'.

The figure shows an example of a security awareness dashboard.

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 **All campaigns** tab, all content types appear with the corresponding number of users. Select a user and you will immediately see all details of the session: start and end date, computer and user name and 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 preconditions must be met before campaigns and their sessions can be displayed in the DOC:**

1. You have already created one or multiple security awareness campaigns. The content of these campaigns is irrelevant.
2. You have assigned the policies with the campaigns to the appropriate DriveLock agents. Only campaigns that have already been started, are currently active or have already ended on the agent are displayed.



Warning: Agents must have at least DriveLock version 2019.2 or higher installed. Execution of security awareness campaigns on agents with older DriveLock versions cannot be visualized in the DOC.

3. You must activate the [security awareness events](#) on the DriveLock Enterprise Service.

## 8.1 The Security Awareness view

Filter options are displayed under **All campaigns**.

You can also filter by **Content add-on packages**, but only the packages that require a license are displayed here (without a license, only the demo packages). You can only see the number of started or passed/failed sessions from the status, but you do not get further information e.g. about users or computers.





## Copyright

Information in this document, including URL and other Internet Web site references, is subject to change without notice. Unless otherwise noted, the example companies, organizations, products, domain names, e-mail addresses, logos, people, places, and events depicted herein are fictitious, and no association with any real company, organization, product, domain name, e-mail address, logo, person, place, or event is intended or should be inferred. Complying with all applicable copyright laws is the responsibility of the user.

© 2022 DriveLock SE. All rights reserved.

DriveLock and others are either registered trademarks or trademarks of 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.