# DriveLock Security Awareness

## Dokumentation 2023.1

DriveLock SE 2023

# Inhaltsverzeichnis

# 1 Willkommen bei DriveLock Security Awareness

Das Sicherheitsbewusstsein von Mitarbeitenden zu stärken, ist heute eine der wichtigsten Aufgaben eines Unternehmens. DriveLock Security Awareness unterstützt Sie dabei mit anlassbezogenen Kampagnen und Trainings, die folgenden Mehrwert bieten:

- Flexibel einsetzbare Security Awareness Trainings, die kontinuierlich online oder off-line verfügbar und komplett zentral administrierbar sind,
- Interaktive Anzeige sicherheitsrelevanter Informationen zum richtigen Zeitpunkt, z. B. beim Einstecken eines USB-Sticks,
- Anlassbezogene Kampagnen, z. B. automatisiert einmal pro Woche oder Monat,
- Ad-hoc Veröffentlichen von Verhaltensmaßnahmen bei einem Sicherheitsvorfall und
- Umsetzung von Schutzmaßnahmen im Sinne der DSGVO.

Security Awareness ist als Feature der DriveLock Zero Trust Plattform standardmäßig in DriveLock enthalten und benötigt keine separate Lizenz.

Das Security Awareness Content AddOn hingegen benötigt eine separate Lizenz und bietet Ihnen eine Vielzahl an externen Inhalten, mit denen Sie Security-Awareness-Kampagnen erstellen können.

> Hinweis: Beachten Sie bitte, dass Content-AddOn-Pakete nur dann korrekt angezeigt werden können, wenn auf den Agenten Microsoft Edge WebView2 installiert ist.

# 2 Konzepte

## 2.1 Kampagnen

Die in DriveLock verwendeten Security-Awareness-Kampagnen können sich aus Texten in unterschiedlichen Formaten (RTF, PDF, Text), Bildern, Videos, Web-Inhalte oder E-Learning-Modulen zusammensetzen. Sie werden verwendet, um Benutzern gezielt Sicherheitsinformationen zukommen zu lassen, sie auf konkrete Ereignisse hinzuweisen, Anweisungen weiterzugeben und ihnen erforderliche Trainings zuzuweisen.

Die Kampagnen können so konfiguriert werden, dass sie zu bestimmten Zeitpunkten und bei bestimmten Ereignissen angezeigt werden, beispielsweise beim Einloggen eines Benutzers an seinem Rechner oder beim Verbinden eines Smartphones, Start einer Applikation, Einstecken eines USB-Sticks oder Verbinden eines externen Laufwerks. Sie lassen sich aber auch so konfigurieren, dass sie ohne bestimmtes Ereignis bei Benutzern angezeigt werden oder selbst vom Benutzer 'ad hoc' aufgerufen werden können. Sowohl die Häufigkeit der Anzeige also auch der exakte Start- und Endzeitpunkt lassen sich einstellen.

Um sicherzustellen, dass die Sicherheitsinformationen ihr Ziel erreicht haben und die Benutzer sich mit den Inhalten auseinandergesetzt haben, kann eine Bestätigung angefordert werden.

Kampagnen können auch individuell für Laufwerke, Geräte und Applikationen innerhalb von Regeln definiert werden.

Die Erstellung von Kampagnen ist sowohl im Richtlinien-Editor als auch im Menü **Awareness** im DOC möglich.

> Hinweis: Beachten Sie bitte, dass Sie im DOC ausschließlich Kampagnen mit Content-Paketen erstellen und für diese nur eingeschränkte bzw. vereinfachte Konfigurationsmöglichkeiten zur Verfügung stehen.

## 2.2 Content-Pakete

Das lizenzierungspflichtige Content-AddOn beinhaltet multimediale Inhalte (z.B. komplette Sicherheitstrainings), mit denen Kampagnen erstellt werden können. Die Inhalte werden auf Abonnement-Basis regelmäßig und automatisch über das Internet aktualisiert und können im DOC abgerufen werden.

Es stehen Inhalte in den Sprachen **Deutsch**, **Englisch** und **Französisch** zur Verfügung.

Hinweis: Wenn Sie DriveLock On-Premise einsetzen, müssen Sie die Content-Pakete zunächst aktivieren, bevor Sie diese in Kampagnen verwenden können.

### 2.3 Auswertungen

Im Kontext von Kampagnen werden verschiedene Auswertungen angeboten, die beispielsweise bei einem Audit herangezogen werden können. Somit lassen sich Mitarbeiterschulungen, Trainings oder Tests und sonstige Maßnahmen zu sicherheitsrelevanten Themen exakt nachvollziehen und nachweisen.

Für die Auswertung lassen sich die Kampagnen in sogenannte Sessions (Ausführungseinheit oder Sitzung) herunterbrechen. Sobald eine Kampagne einer Benutzergruppe zugewiesen und dieser auf den Endgeräten präsentiert worden ist, kann jede einzelne Session ausgewertet werden. So können Sie leicht verfolgen, ob eine Session nicht beendet oder nicht bestanden wurde, oder ob es Fehler bei der Ausführung gab.

### 2.4 Ereignisse

Im DOC werden auf dem Tab **Ereignisse** die wichtigsten Security-Awareness-Ereignisse aufgelistet. Sie ermöglichen eine exakte Auswertung der Kampagnenausführung und geben Auskunft über aufgetretene Fehler und Warnungen. Rückschlüsse auf die zum Ereignis zugehörigen Objekte sind hier auch möglich.

Im Richtlinien-Editor sehen Sie im Unterknoten **Security Awareness** unter **DriveLock-Ereignisse** im Knoten **Ereignisse und Alerts** eine Liste aller Security-Awareness-Ereignisse. Einige Ereignisse müssen erst aktiviert werden, damit Sie vom DriveLock Agenten auf den DriveLock Enterprise Service (DES) übertragen und somit für die Auswertung herangezogen werden können.

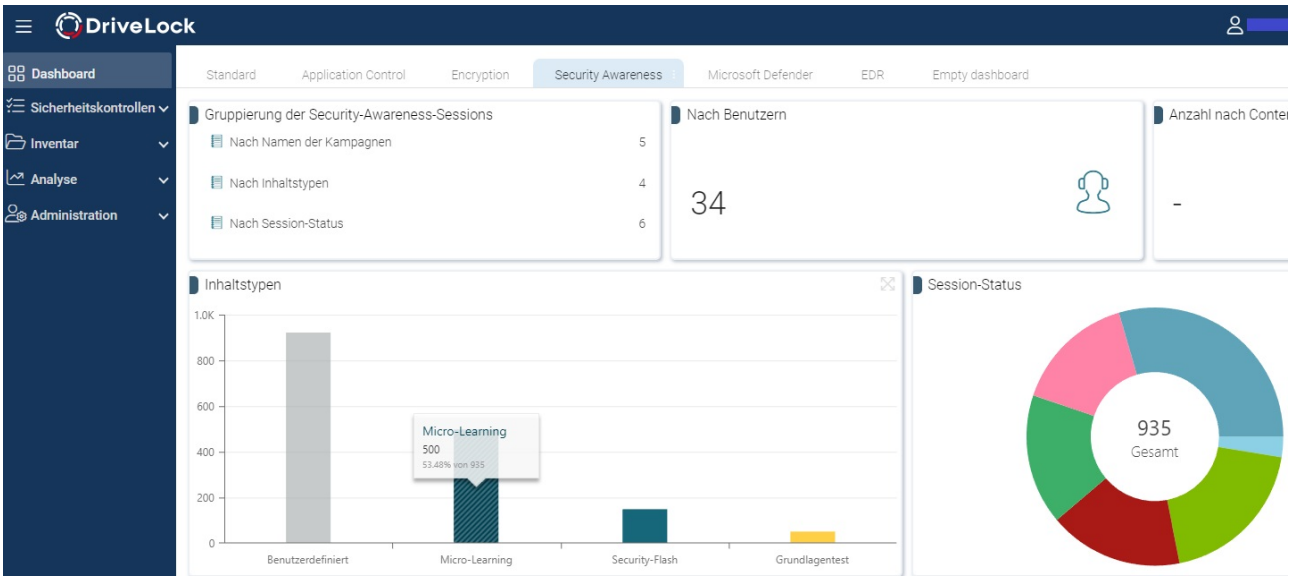
Hinweis: Die wichtigsten Security-Awareness-Ereignisse für die Auswertung im DOC sind standardmäßig aktiviert.

# 3 Konfiguration im DOC (DriveLock Operations Center)

## 3.1 Security Awareness Dashboard

Im DOC bekommen Sie im **Security Awareness-Dashboard** einen Überblick über Ihre laufenden Security-Awareness-Kampagnen (siehe Abbildung). Der Ablauf einer Kampagne wird als 'Session' bezeichnet.

Jede Ansicht ist individuell und hängt von verschiedenen Faktoren ab, z.B. von der Anzahl und vom Typ der Kampagnen, die Sie bereits erstellt haben.




Die Sessions sind nach bestimmten Filtern gruppiert:

- Wenn Sie sich z.B. anzeigen lassen wollen, wie viele Benutzer gerade an einer Kampagne mit einem bestimmten Inhaltstyp arbeiten, wählen Sie im Widget **Gruppierung der Sessions** die Option **Nach Inhaltstypen**. Auf dem Reiter **Auswertungen** erscheinen dann alle Inhaltstypen mit der jeweiligen Anzahl der Sessions. Markieren Sie eine Session und dann sehen Sie die Details: Start- und Enddatum, Computer- und Benutzername und den jeweiligen Status.
- Im Widget **Inhaltstyp** können Sie nach einem bestimmten Kampagnen-Inhaltstyp filtern.
- Der **Session-Status** zeigt Ihnen in einem Kreisdiagramm die verschiedenen Status der Sessions an. Durch Klicken auf das Segment **Nicht bestanden** können Sie beispielsweise sehen, welcher Benutzer welche Sessions nicht bestanden hat.

**Damit Kampagnen bzw. deren Sessions im DOC angezeigt werden können, müssen folgende Voraussetzungen erfüllt sein:**

1. Eine oder mehrere Security-Awareness-Kampagnen sind schon angelegt worden. Welchen Inhalt diese Kampagnen haben, spielt dabei keine Rolle.
2. Die Richtlinien mit den Kampagnen sind an die entsprechenden DriveLock Agenten zugewiesen worden. Angezeigt werden hierbei nur Kampagnen, die auf dem Agenten bereits gestartet, gerade aktiv oder schon beendet sind.

   Hinweis: Die Kampagnen, die Sie im DOC erstellen, werden automatisch zugewiesen.

3. Die Security-Awareness-Ereignisse müssen auf dem DriveLock Enterprise Service aktiviert sein.

### 3.2 Schritt für Schritt zur Kampagne

Wenn Sie zum ersten Mal eine Kampagne anlegen, diese einem Agenten zuweisen und dann auswerten wollen, können Sie folgendermaßen vorgehen.

1. Öffnen Sie in den **Sicherheitskontrollen** das Menü **Awareness**.
2. Sofern Sie das Content AddOn lizenziert haben, erscheinen automatisch sämtliche Pakete auf dem Tab **Content-Pakete**. Um herauszufinden, welchen Inhalt eine Kampagne hat, markieren Sie diese und lesen Sie sich die Beschreibung rechts in der Detailansicht unter **Eigenschaften** durch. Sie können die Pakete nach Inhaltstyp oder nach Namen gruppieren. Als Beispiel wird hier das Trainingspaket "Working in the cloud" verwendet.

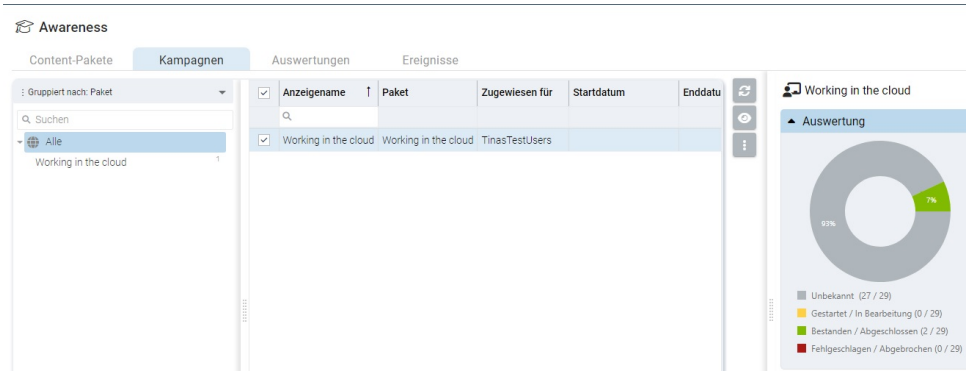
   Hinweis: Beachten Sie, dass die Pakete bei On-Premise Installationen zuerst synchronisiert werden müssen, bevor sie Kampagnen zugewiesen werden. Der Server lädt diese dann herunter, damit sie an die Agenten weiterverteilt werden können.

3. Um eine Kampagne mit diesem Paket zu erstellen, markieren Sie **Working in the cloud**. Klicken Sie rechts, um das Kontextmenü zu öffnen oder wählen Sie die Schaltfläche  . Wählen Sie **Kampagne erstellen**.
4. Geben Sie einen **Namen** und eine Beschreibung für die Kampagne an oder übernehmen Sie die Eingaben. Stellen Sie dann die **Priorität** für die Ausführungsreihenfolge der Kampagnen ein (Einstellungen von 1 - 10, Reihenfolge

absteigend). Kampagnen gleicher Priorität werden in zufälliger Reihenfolge angezeigt.

5. Auf der nächsten Seite wählen Sie ein **Zuweisungsziel** aus. Hier fügen Sie eine **Benutzergruppe** hinzu, die Sie zuvor definiert haben müssen. Falls gewünscht, definieren Sie auch einen **Start- und Endzeitpunkt** für die Kampagne.
6. Sobald Sie auf **Fertigstellen** geklickt haben, erscheint die neue Kampagne auf dem Tab **Kampagnen**.
7. Hier können Sie die Kampagne bearbeiten, löschen, deaktivieren oder die Priorität verringern bzw. erhöhen. Sobald die Kampagne ausgeführt wurde, sehen Sie den Status bereits in der **Detailansicht** unter **Auswertung**. Im Beispiel haben 2 von 29 Benutzern das Training bestanden (7%).

> Hinweis: Beachten Sie, dass sich die Gesamtzahl erhöhen kann, wenn zusätzliche Benutzer sich an ihren DriveLock Agenten anmelden, die bisher noch nicht als Mitglieder registriert sind.



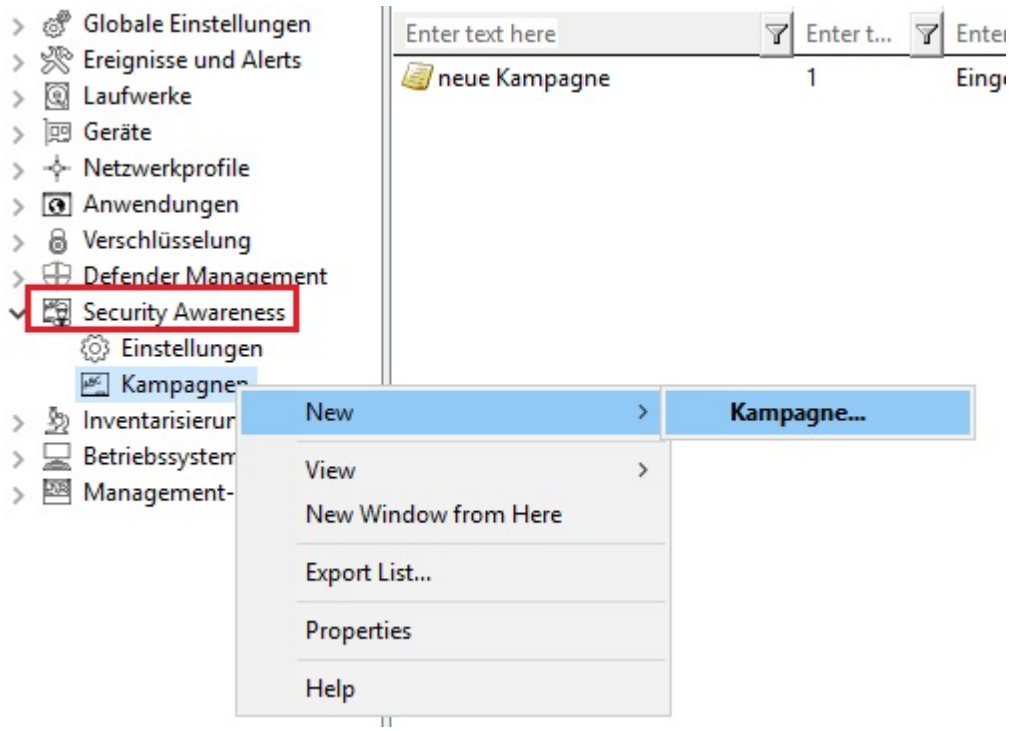

> Hinweis: In der Anzeige können die Kampagnen unterschiedliche Textfarben annehmen. Dunkelgrau, wenn das aktuelle Datum außerhalb des Start- und Endbereichs liegt. Hellgrau, wenn die Kampagne deaktiviert ist. Schwarz ist die normale Textfarbe.

8. Wenn Sie auf den grünen Bereich klicken, öffnet sich automatisch der Tab **Auswertungen** mit weiteren Informationen
   Hier können Sie mit verschiedenen Filtern und Gruppierungen einzelne Sessions von Kampagnen genauer betrachten.
9. Auf dem Tab **Ereignisse** werden die relevanten Security-Awareness-Ereignisse angezeigt.

# 4 Konfiguration im Richtlinien-Editor

## 4.1 Kampagnen anlegen

Im Knoten **Security Awareness** in Ihrer Richtlinie können Sie unter **Kampagnen** neue Kampagnen anlegen , indem Sie wie in der Abbildung gezeigt vorgehen:



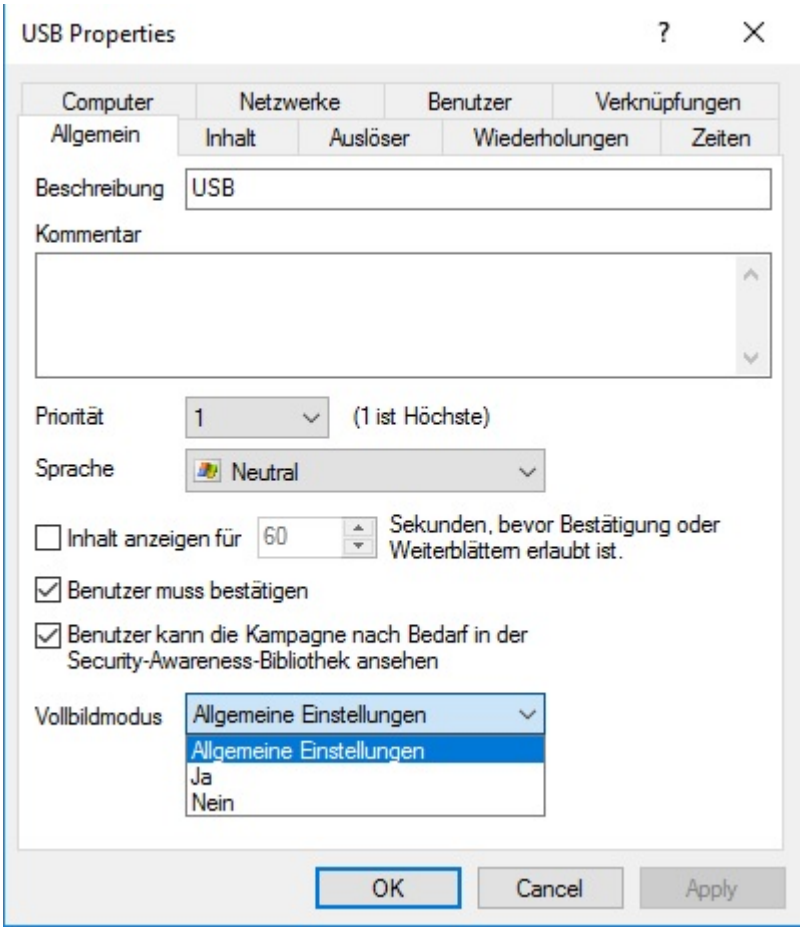

Über das Kontextmenü von **Kampagne** wählen Sie **Neu** und dann **Kampagne...**. Der Assistent zur Erstellung einer **Neuen Kampagne** wird geöffnet und Sie durchlaufen folgende Dialogseiten:

1. Inhalt einer neuen Kampagne
2. Auslöser für eine neue Kampagne
3. Wiederholungen einer neuen Kampagne
4. Allgemeine Einstellungen

> Hinweis: Um die neue Kampagne bestimmten Computern, Benutzern und Netzwerkverbindungen zuzuweisen, öffnen Sie die Eigenschaften der Security-Awareness-Kampagne. Hier können Sie auch alle Einstellungen ändern, die Sie im **Neue Kampagne** Assistent vorgenommen haben.

### 4.1.1 Allgemein

Auf der vierten Seite **Allgemein** geben Sie folgendes ein:




- **Beschreibung** Ihrer Kampagne und optional einen **Kommentar**. Die Beschreibung ist erforderlich, damit Sie Ihre Kampagne in der Kampagnenauflistung wiederfinden. Außerdem wird diese später auch für das Reporting verwendet.
- **Priorität**, nach der die Ausführungsreihenfolge der Kampagnen eingestellt wird (Einstellungen von 1 - 10, Reihenfolge absteigend). Kampagnen gleicher Priorität werden in zufälliger Reihenfolge angezeigt.
- Wählen Sie, für welche **Sprache** die Kampagne angezeigt werden soll. Wenn Sie z.B. Brasilianisch auswählen, dann wird Ihre Kampagne nur auf Agent-Rechnern angezeigt, deren Betriebssystemsprache Brasilianisch ist. Die Sprache auf Neutral zu belassen, schließt also alle Betriebssystemsprachen ein.

> Hinweis: Wenn Sie ein Security-Awareness-Paket aus dem Security-Awareness Content AddOn auswählen, wird die Sprache bereits durch diese Auswahl voreingestellt (nur Deutsch, Englisch oder Französisch).

- Geben Sie an, wie lange die Kampagne angezeigt bleibt, bevor der Benutzer bestätigen muss bzw. die Kampagne schließen kann.

- Geben Sie an, ob der Benutzer das Lesen des Kampagneninhalts bestätigen muss. In den allgemeinen Security-Awareness-Einstellungen können Sie einen entsprechenden Bestätigungstext für alle Kampagnen eingeben.
- Die Option **Benutzer kann die Kampagne nach Bedarf in der Security-Awareness-Bibliothek ansehen** ist standardmäßig aktiviert. Der Benutzer kann die Kampagnen aus der Security-Awareness-Bibliothek auswählen und zu einem passenden Zeitpunkt ansehen oder durcharbeiten.
- Vollbildmodus:
  Wählen Sie hier **Ja**, wenn Sie wollen, dass diese Kampagne dem Benutzer im Vollbildmodus angezeigt wird.
  Wählen Sie die Option **Allgemeine Einstellungen**, um die Vollbildmodus-Einstellungen in den allgemeinen Security-Awareness-Einstellungen für diese Kampagne zu übernehmen.
  Wählen Sie **Nein**, wenn Sie keinen Vollbildmodus wollen.

  Hinweis: Diese Option ist nicht verfügbar, wenn für alle Kampagnen die Option **Einstellungen zum Vollbildmodus auf Kampagnebene ignorieren** gesetzt wurde.

### 4.1.2 Inhalt

Auf der ersten Dialogseite **Inhalt** bestimmen Sie, welche Inhalte (Elemente) Ihre Kampagne enthalten soll:

- **Bild**
  Wählen Sie hier ein beliebiges Bild aus Ihrem Dateisystem oder aus Ihrem Richtliniendateispeicher. Die üblichen Bildformate (*.png, *.jpg, *.bmp) werden unterstützt.
- **Content-AddOn-Paket**
  Wählen Sie hier ein Paket aus, das für Ihre Zwecke geeignet ist. Dies kann beispielsweise ein Training, ein Security Flash oder Wissenstest sein.

  Hinweis: Beachten Sie bitte, dass Content-AddOn-Pakete nur dann in dieser Liste angezeigt werden, wenn Sie die Lizenz für das DriveLock Security Awareness Content AddOn erworben haben. Ansonsten erscheinen lediglich die Demo-Pakete.

- **Eingebautes Bild**

Wählen Sie hier eines der von DriveLock zur Verfügung gestellten Bilder aus.

- **PDF-Datei**
  Wählen Sie hier eine PDF-Datei, deren Inhalt dem Benutzer angezeigt wird. Überprüfen Sie bitte, ob der Inhalt korrekt angezeigt wird, da nicht alle PDF-Funktionalitäten unterstützt werden.
- **RTF-Datei**
  Wählen Sie hier eine RTF-Datei, deren Inhalt dem Benutzer angezeigt wird. Dies kann auch nur Text oder Unicode oder ANSI-Zeichencode sein.
- **Text**
  Geben Sie einen beliebigen Text für Ihre Kampagne ein.
- **URL (Web-Inhalt)**
  Geben Sie hier eine URL an, die auf Web-Inhalte verweist, die Sie für Ihre Kampagne einsetzen wollen.
- **Videodatei**
  Wählen Sie hier eine Videodatei aus (im Format *.mp4 oder *.avi), die dem Benutzer im Windows Media Player angezeigt wird.

> Hinweis: Die Fenstergröße wird bei der Anzeige immer dem Inhalt angepasst, außer bei Content-AddOn-Paketen und bei URL, wo die Fenstergröße 1280x1024 beträgt.

### 4.1.3 Auslöser

Auf der zweiten Seite **Auslöser** geben Sie an, bei welchem Ereignis Ihre Kampagne angezeigt werden soll.

> Hinweis: Ein **Ereignis** ist beispielsweise das Einloggen eines Benutzers an seinem Rechner, das Einstecken eines externen Laufwerks, das Verbinden eines Geräts, z.B. eines Smartphones, oder auch die Aktualiserung einer Richtlinie, die über Regeln das Anzeigen einer Kampagne steuert.

Folgende Optionen stehen zur Auswahl:

- **Unabhängig von einem Ereignis**
  Wählen Sie diese Option, um eine Kampagne zum nächstmöglichen Zeitpunkt direkt bei Benutzern anzeigen zu lassen, unabhängig von den üblichen Ereignissen, die die Anzeige einer Kampagne auslösen. In diesem Fall prüft der DriveLock Agent in

bestimmten Intervallen (alle 30 Minuten), ob unabhängige Kampagnen anstehen und zeigt diese dann entsprechend beim Benutzer an.

> Hinweis: Wenn Sie Benutzern möglichst schnell eine Security-Awareness-Kampagne, z.B. wichtige firmeninterne Informationen oder Warnungen, zukommen lassen ( 'pushen') wollen, wählen Sie diese Option.

- **Bei Anmeldung des Benutzers**
  Wählen Sie diese Option, um dem Benutzer eine Kampagne anzeigen zu lassen, sobald dieser sich an seinem Rechner anmeldet.
- **Bei Verwendung in Regeln**
  Wählen Sie diese Option, wenn Sie eine Kampagne in einer Regel verwenden wollen. Die Kampagne wird dem Benutzer angezeigt wie in der entsprechenden Regel für Laufwerke, Geräte oder Applikationen im Reiter **Awareness** definiert.

> Hinweis: Diese Option ist nur dann aktiv, wenn Sie sämtliche DriveLock-Funktionalitäten aktiviert haben.

Die beiden letzten Optionen sind nur aktiviert, wenn Sie nur DriveLock Security Awareness (ohne Device Control) einsetzen:

- **Beim Anschliessen eines Geräts**
  Wählen Sie diese Option, um dem Benutzer eine Kampagne anzeigen zu lassen, sobald dieser ein Gerät an seinem Rechner ansteckt.
- **Beim Anschliessen eines Laufwerks**
  Wählen Sie diese Option, um dem Benutzer eine Kampagne anzeigen zu lassen, sobald dieser ein Laufwerk mit seinem Rechner verbindet.

### 4.1.4 Wiederholungen

Auf der dritten Seite **Wiederholungen** geben Sie an, wie oft Ihre Kampagne angezeigt bzw. wiederholt werden soll.

Sie können hier folgendes einstellen:

- **Kampagne x mal anzeigen**
  Grenzen Sie hier die Kampagnenanzeige ein, indem Sie eine bestimmte Zahl angeben oder wählen Sie von der Dropdown-Liste **niemals** oder **unendlich oft** aus.

Die Auswahl **niemals** ist dann sinnvoll, wenn Sie Ihre Kampagne zunächst noch nicht anzeigen lassen wollen. Sie können dies dann später in den Eigenschaften der Kampagne ändern.

- **Bei jedem Auftreten des Ereignisses**
- **Einmal pro Tag/Woche/Monat/Jahr**
- Sie können auch angeben, ob Ihre Kampagne **einmal alle paar Tage** (z.B. jeden dritten Tag) angezeigt wird.
- Falls eine Kampagne nur unvollständig angezeigt wurde oder ein Fehler aufgetreten ist, können Sie angeben, dass diese nach einer bestimmten Zeit wieder angezeigt wird.

### 4.1.5 Kampagne an Benutzer verteilen

Um eine neue Security-Awareness-Kampagne an die entsprechenden Benutzer (Computer mit DriveLock Agenten) zu verteilen, müssen Sie die Richtlinie zunächst veröffentlichen.

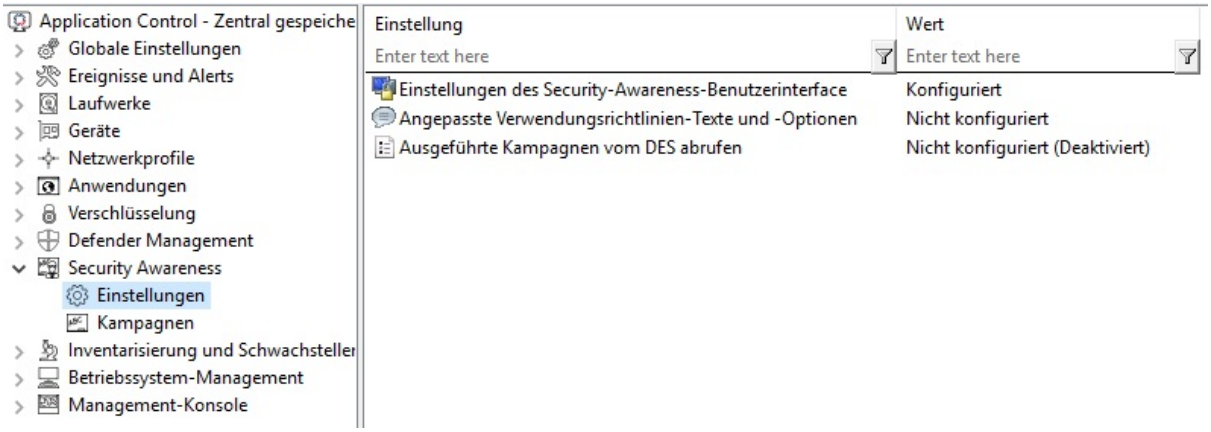
1. Öffnen Sie das Kontextmenü der Richtlinie und wählen Sie den Menüpunkt **Veröffentlichen**. Oder wählen Sie die Schaltfläche **Veröffentlichen** aus der Menüleiste.
2. Optional können Sie einen Kommentar eingeben.
3. Wenn Sie die Richtlinie signieren wollen, aktivieren Sie die entsprechende Option und wählen das Zertifikat aus.
4. Die Richtlinie ist nun veröffentlicht und wird von den DriveLock Agenten verwendet

## 4.2 Allgemeine Einstellungen

Im Knoten **Security Awareness** in Ihrer Richtlinie können Sie unter **Einstellungen** allgemeine Angaben für alle Kampagnen konfigurieren.

**Gehen Sie folgendermaßen vor:**

1. Wählen Sie unter **Security-Awareness** den Menüpunkt **Einstellungen**.




2. Klicken Sie auf die Option **Einstellungen des Security-Awareness-Benutzerinterface**, um folgende Einstellungen festzulegen:

   - **Alle Kampagnen**
     Auf diesem Reiter nehmen Sie allgemeine Einstellungen vor, die **alle** Kampagnen betreffen.
     - Hier können Sie bestimmen, ob das Fenster, in dem Security-Awareness-Kampagnen angezeigt werden, beim Benutzer immer sichtbar ist.
     - Wenn Sie wollen, dass alle Kampagnen im Vollbildmodus angezeigt werden, setzen Sie ein Häkchen bei der entsprechenden Option.

       Hinweis: Im Vollbildmodus kommen Ihre Kampagnen besonders gut zur Geltung.

     - Wählen Sie die Option **Einstellungen zum Vollbildmodus auf Kampagnenebene ignorieren**, wenn Sie die Einstellungen in einzelnen Kampagnen hierzu außer Kraft setzen wollen (der Vollbildmodus kann in den Kampagneneigenschaften gesetzt werden).
     - Wenn Sie noch keine mehrsprachigen Benachrichtigungstexte für Ihre Richtlinie erstellt haben, können Sie in diesem Dialog speziell auf Ihre Firma angepasste Überschriften und Texte für Ihre Kampagnen eingeben.
     - Alternativ können Sie im DMC-Knoten **Globale Einstellungen** unter **Mehrsprachige Benachrichtigungstexte** Sprachen festlegen und an dieser Stelle entsprechende Benachrichtigungstexte definieren.

> Hinweis: Weitere Informationen zur Erstellung von mehrsprachigen Benachrichtigungstexten finden Sie in der Admin Dokumentation unter DriveLock OnlineHelp.

3. Klicken Sie auf die Option **Angepasste Verwendungsrichtlinien-Texte und -Optionen**, um benutzerdefinierte Inhalte beim Zugriff auf ein Laufwerk und/oder Gerät anzeigen zu lassen. Diese Option betrifft ausschließlich die Anzeige von Verwendungsrichtlinien. Sie können folgende Einstellungen im Dialog vornehmen:

   - Text aus einer Datei laden oder Text selbst formulieren
   - Text für die Schaltflächen angeben (z.B. Zustimmen statt Akzeptieren)
   - Überschrift festlegen
   - Video laden und Einstellungen für dieses Video vornehmen

   > Hinweis: Sie können DriveLock so konfigurieren, dass der Zugriffe auf ein externes Laufwerk oder Gerät erst dann erfolgen kann, nachdem der Anwender durch einen Klick auf die Schaltfläche „Zustimmen“ das Lesen einer sog. Verwendungsrichtlinie nachvollziehbar bestätigt hat.

4. Klicken Sie auf die Option **Ausgeführte Kampagnen vom DES abrufen**, um festzulegen, dass Benutzer ihre bereits durchgeführten Kampagnen auch bei Anmeldung an einem anderen Rechner "mitnehmen" können, d.h. die erledigten Kampagnen werden dort nicht mehr angezeigt. Hierzu wird ein Anfrage an den DriveLock Enterprise Service (DES) geschickt.
   Die Standardeinstellung ist **Deaktiviert**, da Benutzer in der Regel an einem festen Arbeitsplatz arbeiten.

### 4.2.1 Angepasste Verwendungsrichtlinien-Texte und Optionen

Verwendungsrichtlinien dienen dazu, den Benutzer vor dem eigentlichen Zugriff auf ein Laufwerk oder ein Gerät über sicherheitsrelevante Verhaltensmaßnahmen oder Unternehmensrichtlinien zu informieren.

Sie können DriveLock so konfigurieren, dass der Zugriffe auf ein externes Laufwerk oder Gerät erst dann erfolgen kann, nachdem der Anwender durch einen Klick auf die Schaltfläche „Zustimmen“ das Lesen einer sog. Verwendungsrichtlinie nachvollziehbar bestätigt hat.

Sie können sowohl eine Überschrift, die Texte für die beiden Schaltflächen, als auch den Text selbst frei über diesen Konfigurationspunkt definieren. Dazu setzen Sie ein Häkchen bei **Benutzerdefinierten Inhalt verwenden**.

Geben Sie den Nachrichtentext entweder direkt in das Eingabefeld ein, oder wählen Sie eine RTF-formatierte Datei von der lokalen Festplatte bzw. aus dem Richtlinienspeicher aus. Eine Datei aus dem Richtlinienspeicher ist mit einem „*“ markiert.

> Achtung: Wenn Sie eine Datei auswählen, müssen Sie sicherstellen, dass diese sich im angegebenen Pfad auf der lokalen Festplatte des Client-Rechners befindet und von dort geladen werden kann. Über den Richtlinienspeicher können Sie diese Datei zusammen mit der DriveLock Konfiguration verteilen.

Als besondere Option lässt sich innerhalb der Verwendungsrichtlinie auch ein AVI-Video abspielen, welches ebenfalls über diesen Dialog konfiguriert werden kann. Sie können dabei festlegen, welche Möglichkeiten der Benutzer während der Anzeige des Videos hat.

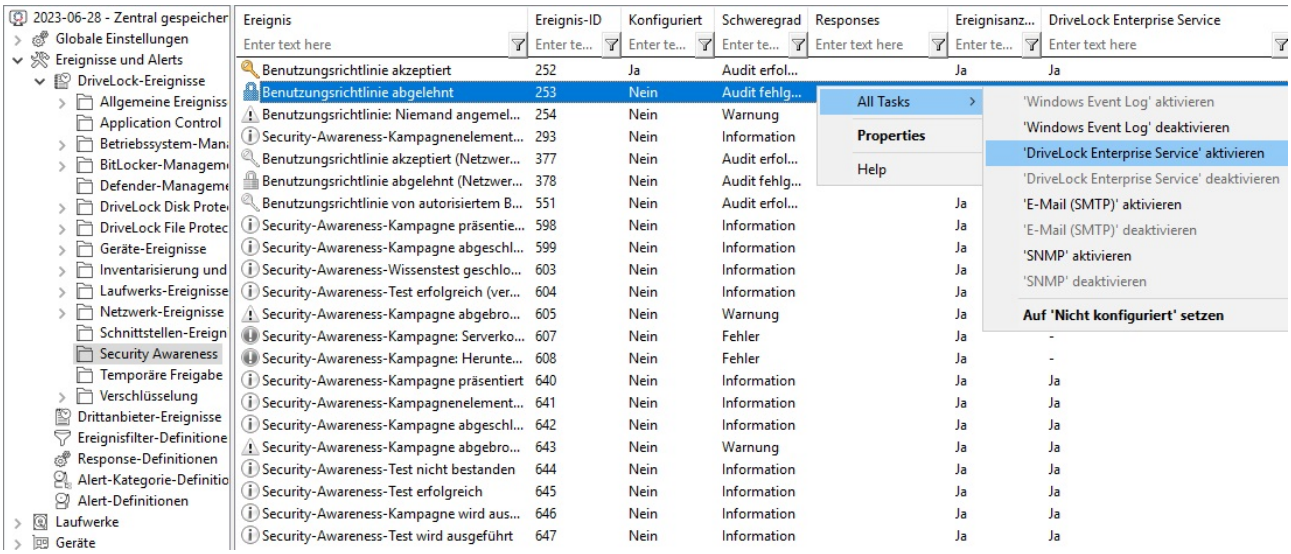
Über die Option **Pro Benutzer und Session x Mal anzeigen** wird die Nachricht nicht öfter als die angegebene Anzahl angezeigt.

Legen Sie außerdem fest, wann die und wie lange es dauert, bis die Akzeptieren-Schaltfläche für den Benutzer verfügbar gemacht wird.

### 4.3 Security-Awareness-Ereignisse im Richtlinien-Editor aktivieren

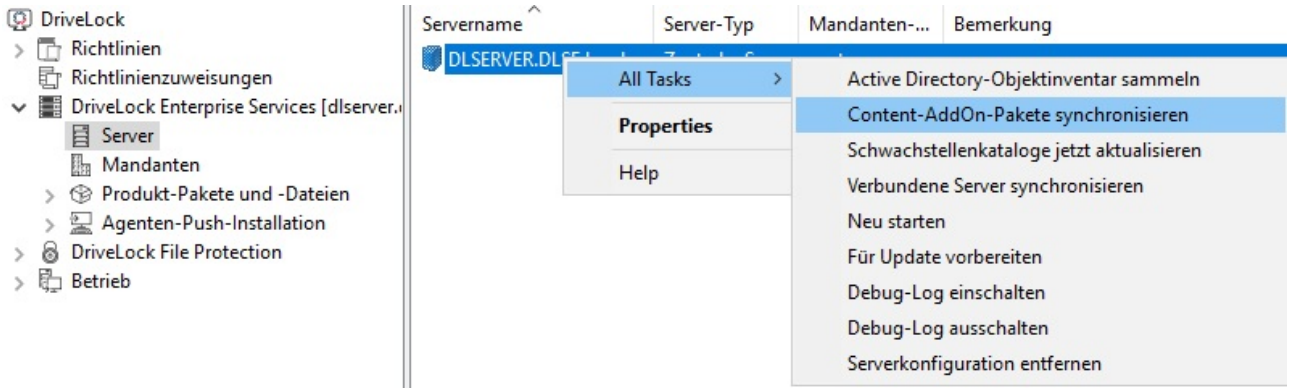
**Im Richtlinien-Editor werden Security-Awareness-Ereignisse folgendermaßen aktiviert:**

1. Öffnen Sie im Knoten **Ereignisse und Alerts** unter **Ereignisse** den Unterknoten **Security Awareness**.
2. Markieren Sie alle Ereignisse, die Sie im DOC angezeigt haben wollen und öffnen Sie das Kontextmenü.
3. Wählen Sie **'DriveLock Enterprise Service' aktivieren**, damit die Ereignisse zum DES hochgeladen werden können.


2023-06-28 - Zentral gespeicher
Globale Einstellungen
Ereignisse und Alerts
DriveLock-Ereignisse
Allgemeine Ereigniss
Application Control
Betriebssystem-Mana
BitLocker-Managem
Defender-Manageme
DriveLock Disk Protec
DriveLock File Protec
Geräte-Ereignisse
Inventarisierung und
Laufwerks-Ereignisse
Netzwerk-Ereignisse
Schnittstellen-Ereign
Security Awareness
Temporäre Freigabe
Verschlüsselung
Drittanbieter-Ereignisse
Ereignisfilter-Definitione
Response-Definitionen
Alert-Kategorie-Definitio
Alert-Definitionen
Laufwerke
Geräte
Ereignis
Ereignis-ID
Konfiguriert
Schweregrad
Responses
Ereignisanz...
DriveLock Enterprise Service
Benutzungsrichtlinie akzeptiert 252 Ja Audit erfol... Ja Ja
Benutzungsrichtlinie abgelehnt 253 Nein Audit fehlg...
Benutzungsrichtlinie: Niemand angemel... 254 Nein Warnung
Security-Awareness-Kampagnenelement... 293 Nein Information
Benutzungsrichtlinie akzeptiert (Netzwer... 377 Nein Audit erfol...
Benutzungsrichtlinie abgelehnt (Netzwer... 378 Nein Audit fehlg...
Benutzungsrichtlinie von autorisiertem B... 551 Nein Audit erfol... Ja
Security-Awareness-Kampagne präsentie... 598 Nein Information Ja
Security-Awareness-Kampagne abgeschl... 599 Nein Information Ja
Security-Awareness-Wissenstest geschlo... 603 Nein Information Ja
Security-Awareness-Test erfolgreich (ver... 604 Nein Information Ja
Security-Awareness-Kampagne abgebro... 605 Nein Warnung Ja
Security-Awareness-Kampagne: Serverko... 607 Nein Fehler Ja -
Security-Awareness-Kampagne: Herunte... 608 Nein Fehler Ja -
Security-Awareness-Kampagne präsentiert 640 Nein Information Ja Ja
Security-Awareness-Kampagnenelement... 641 Nein Information Ja Ja
Security-Awareness-Kampagne abgeschl... 642 Nein Information Ja Ja
Security-Awareness-Kampagne abgebro... 643 Nein Warnung Ja Ja
Security-Awareness-Test nicht bestanden 644 Nein Information Ja Ja
Security-Awareness-Test erfolgreich 645 Nein Information Ja Ja
Security-Awareness-Kampagne wird aus... 646 Nein Information Ja Ja
Security-Awareness-Test wird ausgeführt 647 Nein Information Ja Ja
All Tasks
Properties
Help
'Windows Event Log' aktivieren
'Windows Event Log' deaktivieren
'DriveLock Enterprise Service' aktivieren
'DriveLock Enterprise Service' deaktivieren
'E-Mail (SMTP)' aktivieren
'E-Mail (SMTP)' deaktivieren
'SNMP' aktivieren
'SNMP' deaktivieren
Auf 'Nicht konfiguriert' setzen

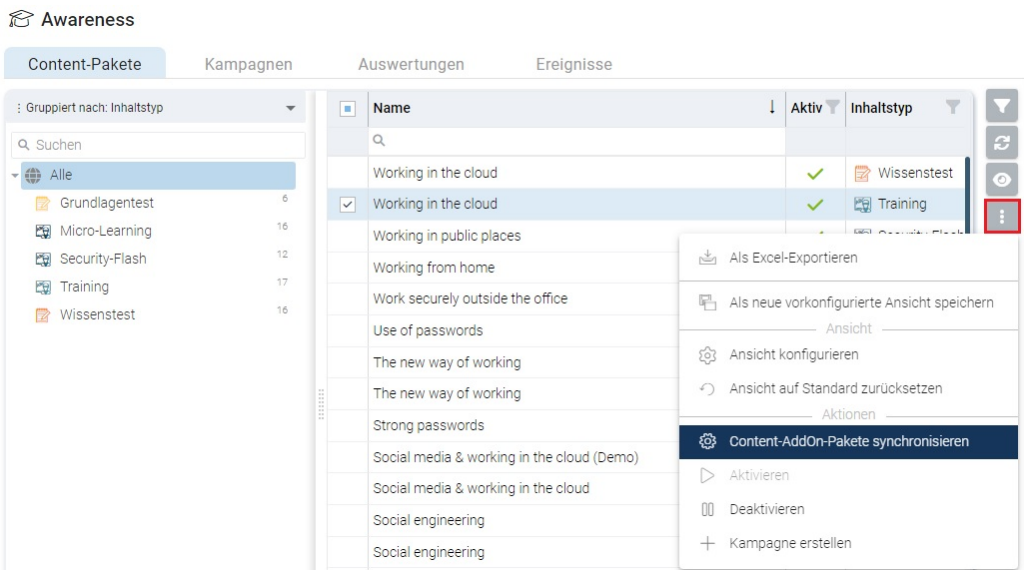
# 5 Content-AddOn-Pakete synchronisieren

Wenn Sie DriveLock On-Premise einsetzen, können Sie Ihre Content-AddOn-Pakete auch manuell vom DriveLock Enterprise Service (DES) synchronisieren, indem Sie wie abgebildet vorgehen:

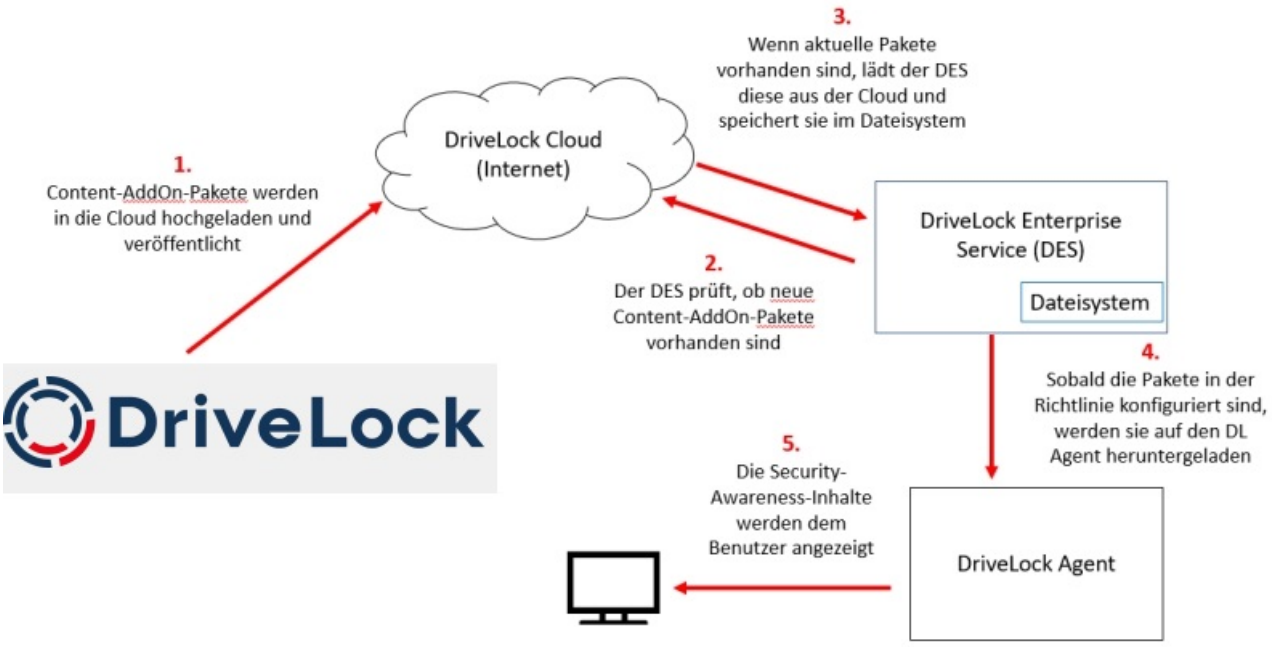



1. Öffnen Sie in der DriveLock Management Konsole (DMC) den Knoten **DriveLock Enterprise Services**.
2. Wählen Sie den **Server** aus, der für Ihre Content-AddOn-Pakete 'zuständig' ist.
3. Öffnen Sie das Kontextmenü und dann den Menübefehl **Alle Aufgaben**.
4. Klicken Sie den Menübefehl **Content-AddOn-Pakete synchronisieren**.
5. Alle Content-AddOn-Pakete sind nun auf dem neuesten Stand.

Wenn Sie das DOC mit DriveLock Managed Services einsetzen, können Sie die Content-AddOn-Pakete auch manuell synchronisieren, indem Sie im Menü Awareness auf dem Tab **Content-Pakete** den Menübefehl **Content-AddOn-Pakete synchronisieren** wie in der Abbildung gezeigt verwenden.



## 5.1 Überblick über die Synchronisierung



# 6 Verwendung von Security-Awareness-Kampagnen

Die im DriveLock Operations Center (DOC) erstellten Kampagnen können nur Content-Pakete verwenden. Sie sind automatisch so konfiguriert, dass sie beim Einloggen eines Benutzers angezeigt oder über die Security Awareness-Bibliothek abgerufen werden können. Die Konfiguration im DOC ist schneller und leichter, bietet aber weniger Konfigurationsmöglichkeiten.

## 6.1 Bei Aufruf einer Anwendung

Um Security-Awareness-Kampagnen beim Aufrufen von Anwendungen zu konfigurieren, gehen Sie wie unten beschrieben vor. Diese Vorgehensweise gilt für alle Anwendungs-Regeln.

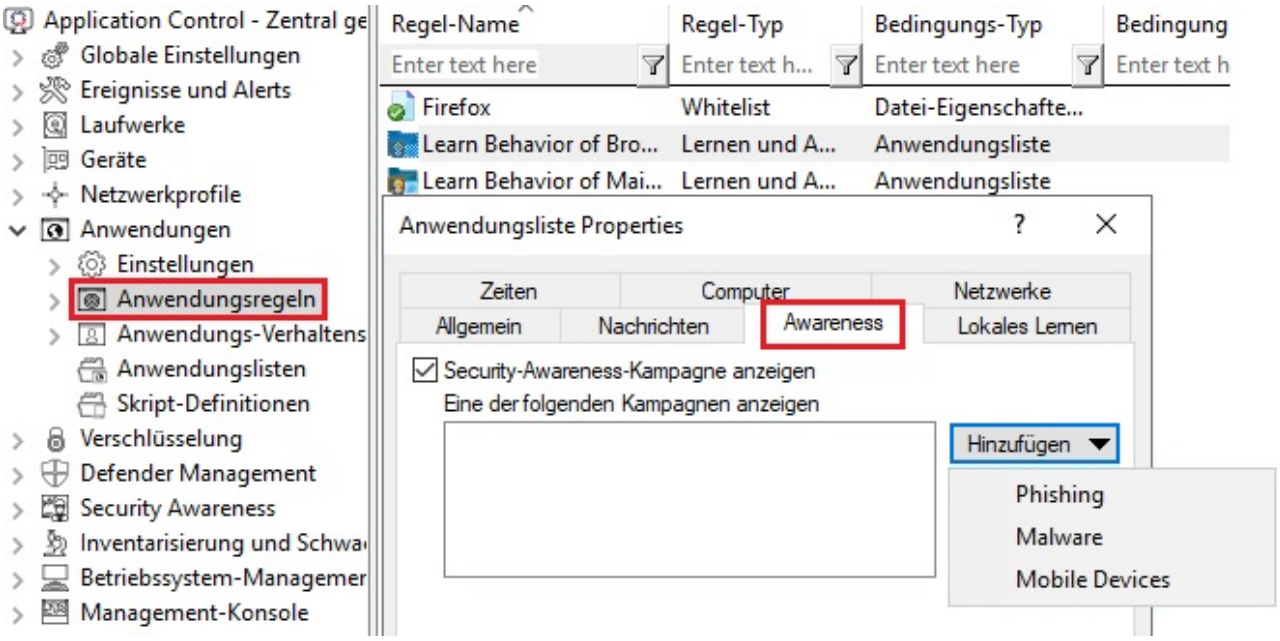
Hinweis: DriveLock Application Control unterliegt einer gesonderten Lizensierung und gehört nicht zum Standardumfang von DriveLock.

Hinweis: Wichtig zu beachten ist, dass die Anzeige einer Security-Awareness-Kampagne vom übergeordneten **Scan- und Blockier-Modus** abhängig ist, den Sie für die Anwendungsausführung definiert haben. So gibt im Whitelist-Modus die übergeordnete Regel eine bestimmte Anwendung frei, während im Blacklist-Modus die übergeordnete Regel die Anwendung sperrt. Erst wenn das System die bereits konfigurierte Regel geprüft und angewendet hat, wird die Regel zur Anzeige der Security-Awareness-Kampagne angewendet. Dieser Mechanismus ist im Administrationshandbuch unter Kapitel Applikationskontrolle beschrieben.

1. Wählen Sie in der Richtlinienkonfiguration den Knoten **Anwendungen**.
2. Wählen Sie die **Anwendungs-Regel** aus (Beispiel siehe Abbildung), für die Sie Security-Awareness einstellen wollen und öffnen das jeweilige Kontextmenü.
3. Klicken Sie den Menübefehl **Neu**, dann die jeweilige Regel und öffnen den Reiter **Awareness** im Eigenschaftendialog.
4. Wählen Sie **Security-Awareness-Kampagne anzeigen** und fügen eine zuvor erstellte Kampagne hinzu.

   Hinweis: Entsprechend der Einstellungen, die Sie bei Erstellung der Kampagne angegeben haben (z.B. wie oft und zu welchen Zeiten diese angezeigt bzw. wiederholt werden soll), wird die Kampagne auf dem DriveLock Agenten angezeigt. Kampagnen gleicher Priorität werden nach dem Zufallsprinzip angezeigt.

5. Bestätigen Sie Ihre Einstellungen.




## 6.2 Beim Verbinden eines Laufwerks

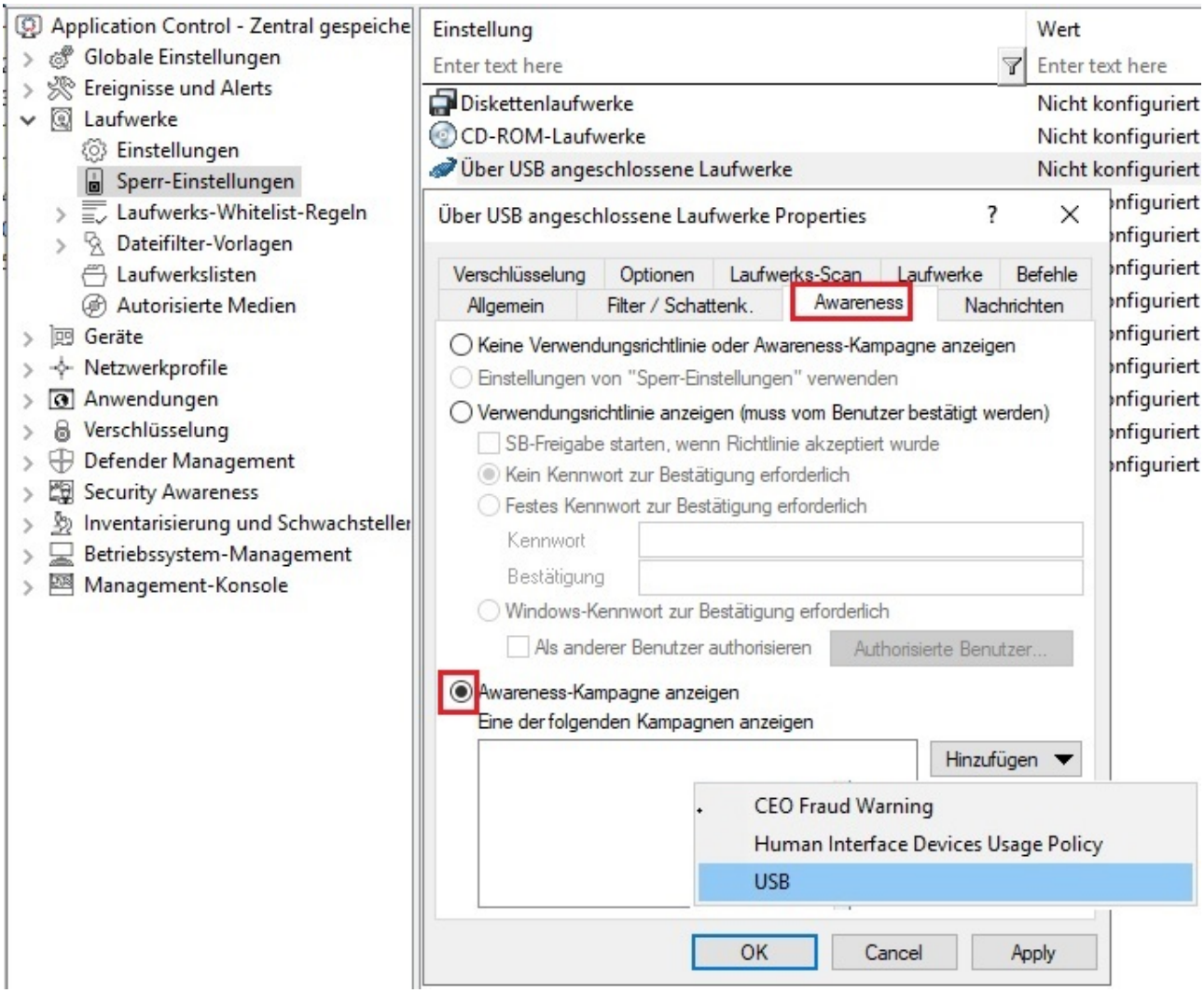
Um Security Awareness zu konfigurieren, so dass eine Kampagne bei der Verbindung eines Laufwerks angezeigt wird, gehen Sie wie in der Abbildung gezeigt vor. Diese Vorgehensweise gilt für alle Arten von Laufwerken.

1. Wählen Sie in der Richtlinienkonfiguration den Knoten **Laufwerke**.
2. Wählen Sie unter **Sperr-Einstellungen** das Laufwerk, für das Sie eine Security-Awareness-Kampagne anzeigen lassen wollen. Im Beispiel ein USB-Laufwerk.
3. Doppelklicken Sie das Laufwerk, um den Eigenschaftendialog zu öffnen.
4. Auf dem Reiter **Awareness** können Sie folgende Einstellungen machen:
   - Wenn Sie eine **Verwendungsrichtline anzeigen** lassen wollen, wählen Sie diese Option. Hierzu können Sie auch Passwörter vergeben, die bei der Bestätigung eingegeben werden müssen oder Sie haken die Option **SB-Freigabe starten, wenn Richtlinie akzeptiert wurde** an, damit ein Benutzer das Gerät verwenden kann, sobald die Richtlinie bestätigt wurde.
   - Wenn ein anderer Benutzer als der in Windows angemeldete die Richtlinie bestätigen soll, markieren Sie **Windows-Kennwort zur Bestätigung erforderlich** und **Als anderer Benutzer authorisieren**. Klicken Sie **Authorisierte Benutzer**, um diesen Benutzer in die Liste einzutragen und markieren Sie die **Option "Als Benutzer anmelden" standardmäßig aktivieren**. Der SB-Freigabe-Assistent wird dann unter dem autorisierten Benutzer ausgeführt.

Hinweis: Wie Sie eine Verwendungsrichtlinie erstellen, erfahren Sie hier.

- Beim Verbinden mit dem Gerät wollen Sie eine **Awareness-Kampagne anzeigen** lassen. Jetzt können Sie hier eine zuvor erstellte Kampagne hinzufügen. Wählen Sie diese aus der Liste aus, die nach Klick auf **Hinzufügen** geöffnet wird.

5. Bestätigen Sie Ihre Einstellungen.



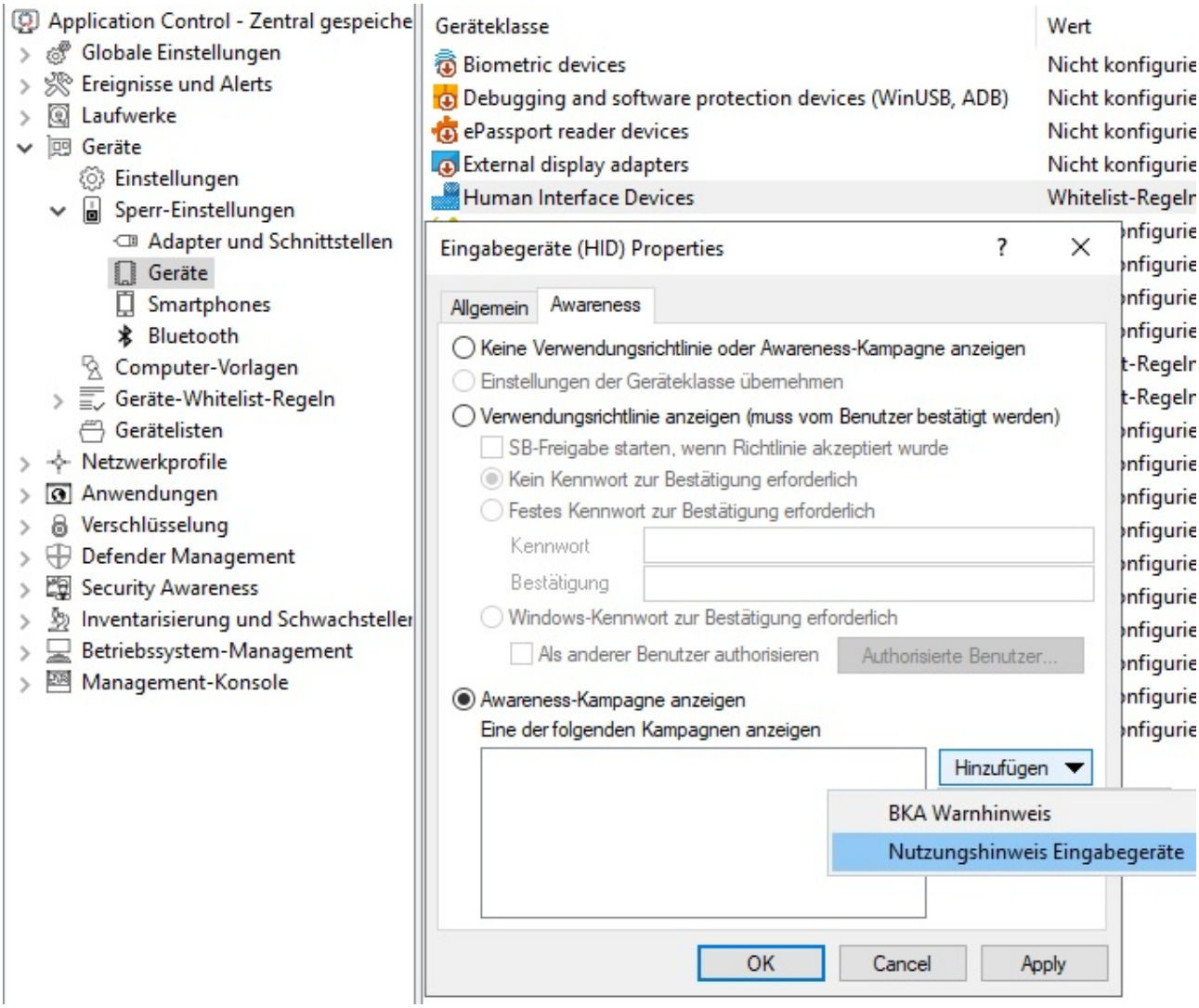

Bei **Laufwerk-Whitelist-Regeln** lassen sich Security-Awareness-Kampagnen bei allen Regeln außer den folgenden einbinden: Netzwerklaufwerk-Regeln, WebDAV-Netzwerklaufwerk-Regel und Terminaldienste-Regeln.

### 6.3 Beim Verbinden von Geräten

Um Security-Awareness bei der Verwendung von Geräten zu konfigurieren, gehen Sie wie in der Abbildung gezeigt vor. Diese Vorgehensweise gilt für alle Geräte und alle Smartphones,

sowie alle Adapter und Schnittstellen, außer COM und LPT, ebenso wie für alle Geräte-Whitelist-Regeln.

Im Beispiel unten soll eine Awareness-Kampagne angezeigt werden, sobald ein Benutzer versucht, ein Eingabegerät (HID) mit seinem Arbeitsrechner zu verbinden.



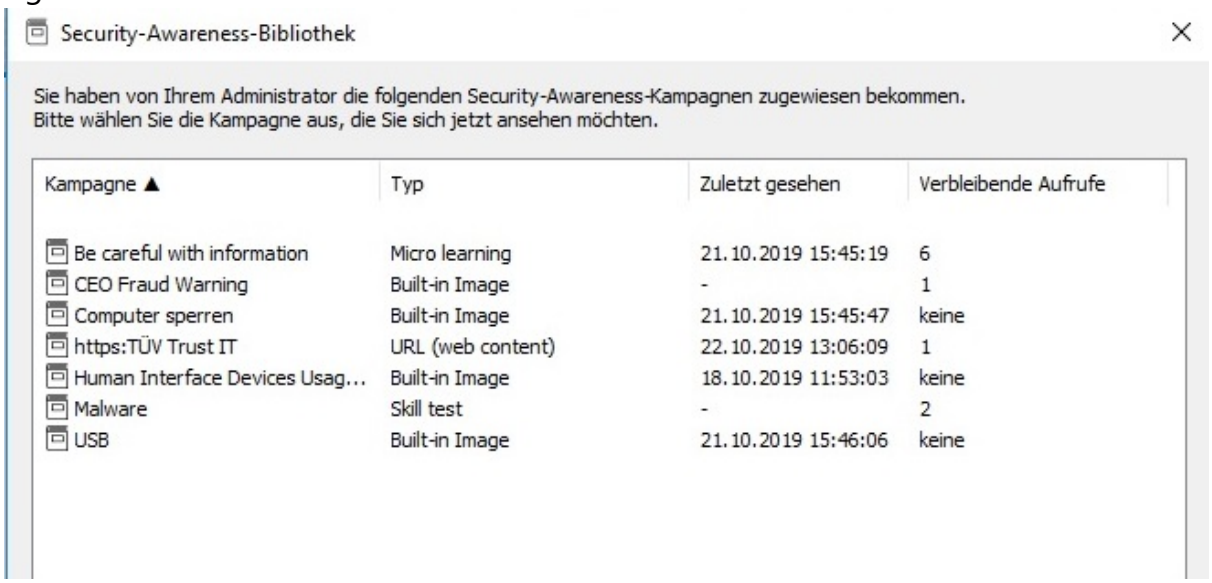

1. Wählen Sie in der Richtlinienkonfiguration den Knoten **Geräte**.
2. Wählen Sie unter **Sperr-Einstellungen** die Geräteklasse aus, bei der Sie Security-Awareness-Einstellungen vornehmen möchten.
3. Auf dem Reiter **Awareness** können Sie dieselben Einstellungen setzen wie bei den Laufwerken.
4. Bestätigen Sie Ihre Einstellungen.

# 7 DriveLock Agent

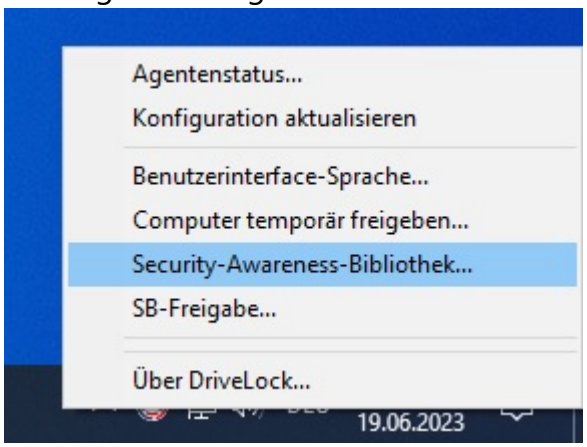
## 7.1 Anzeige auf dem DriveLock Agenten

Auf Agentenseite werden Kampagnen gemäß den Einstellungen in der Richtlinie angezeigt.

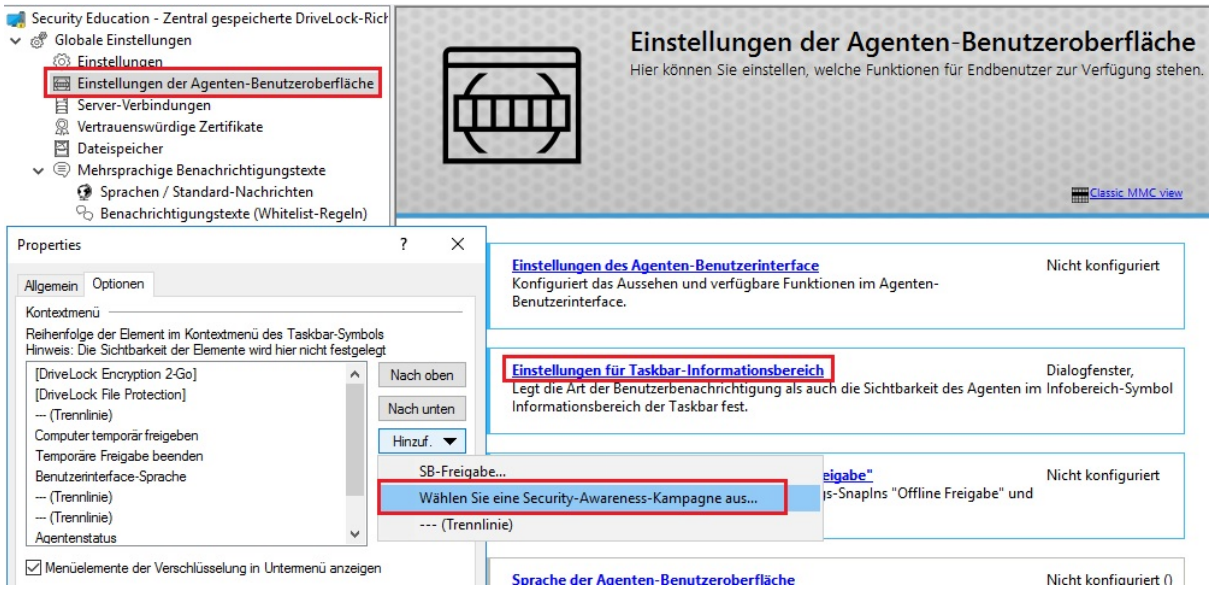
- Benutzer können die Security-Awareness-Bibiliothek in der Benutzeroberfläche des Agenten öffnen:




- Die Security-Awareness-Bibliothek kann alternativ über das Taskleistensymbol auf dem Agenten aufgerufen werden:




Hierzu müssen Sie vorher in der Richtlinie unter **Einstellungen der Agenten-Benutzeroberfläche** die Option **Einstellungen für Taskbar-Informationsbereich** auswählen.
Auf dem Reiter **Optionen** muss der Eintrag **Wählen Sie eine Security-Awareness-Kampagne ...** hinzugefügt werden (siehe Abbildung).
Dann erst kann der Benutzer auf dem Agenten eine Kampagne auswählen.


Security Education - Zentral gespeicherte DriveLock-Rich
Globale Einstellungen
Einstellungen
Einstellungen der Agenten-Benutzeroberfläche
Server-Verbindungen
Vertrauenswürdige Zertifikate
Dateispeicher
Mehrsprachige Benachrichtigungstexte
Sprachen / Standard-Nachrichten
Benachrichtigungstexte (Whitelist-Regeln)
Einstellungen der Agenten-Benutzeroberfläche
Hier können Sie einstellen, welche Funktionen für Endbenutzer zur Verfügung stehen.
Classic MMC view
Properties
Allgemein
Optionen
Kontextmenü
Reihenfolge der Element im Kontextmenü des Taskbar-Symbols
Hinweis: Die Sichtbarkeit der Elemente wird hier nicht festgelegt
[DriveLock Encryption 2-Go]
[DriveLock File Protection]
--- (Trennlinie)
Computer temporär freigeben
Temporäre Freigabe beenden
Benutzerinterface-Sprache
--- (Trennlinie)
--- (Trennlinie)
Agentenstatus
Nach oben
Nach unten
Hinzuf.
SB-Freigabe...
Wählen Sie eine Security-Awareness-Kampagne aus...
--- (Trennlinie)
Menüelemente der Verschlüsselung in Untermenü anzeigen
Einstellungen des Agenten-Benutzerinterface
Konfiguriert das Aussehen und verfügbare Funktionen im Agenten-Benutzerinterface.
Nicht konfiguriert
Einstellungen für Taskbar-Informationsbereich
Legt die Art der Benutzerbenachrichtigung als auch die Sichtbarkeit des Agenten im Informationsbereich der Taskbar fest.
Dialogfenster, Infobereich-Symbol
Nicht konfiguriert
Sprache der Agenten-Benutzeroberfläche
Nicht konfiguriert

# Copyright