



# DriveLock Control Center Benutzerhandbuch 2020.2

14.01.2021

# Inhaltsverzeichnis

Teil I	Konventionen	4
Teil II	DriveLock Control Center	6
	1 Anmeldung am DCC	7
	2 Übersicht	7
	3 Funktionsbereiche	8
	4 Arbeitsbereich	9
	Menüband	9
	Ergebnisansichten	10
	Filtereditor	11
	Ergebnisse drucken und exportieren	13
	Automatisierte Berichte	14
	Anonyme Daten	15
Teil III	Helpdesk	19
	1 Wartungsaufgaben	21
	2 Supportdateien übermitteln	22
Teil IV	Statistikreporte	24
	1 Statistikreporte erstellen	25
Teil V	Ereignisreporte	27
Teil VI	Forensische Analysen	29
	1 Forensische Analysen durchführen	30
Teil VII	Inventar	33
	1 Inventar anzeigen	34
	2 Garantie- und Wartungslaufzeit eingeben	35
Teil VIII	DOC öffnen	36
	1 Anmeldung am DOC	37
	Hinweise zur Verwendung von Zertifikaten	37
	2 Überblick über das DOC	42
	DOC Dashboard	42
	Computer	43
	Gruppen	45
	SecAware	45
	Ereignisse	45
	EDR	45
	Microsoft Defender	46
	Aufgaben	46
	Konten	46
Teil IX	Einstellungen	49





# Teil I

## Konventionen



## 1 Konventionen

In diesem Dokument werden durchgängig folgende Konventionen und Symbole verwendet, um wichtige Aspekte hervorzuheben oder Objekte zu visualisieren.

**Achtung: Roter Text weist auf Risiken hin, die beispielsweise zu Datenverlust führen können.**

Hinweise und Tipps enthalten nützliche Zusatzinformationen.

**Menüeinträge** oder die Namen von **Schaltflächen** sind fett dargestellt. Kursive Schrift repräsentiert Felder, Menüpunkte und Querverweise.

*System*schrift stellt Nachrichten oder Befehle auf Basis der Kommandozeile dar.

Ein Pluszeichen zwischen zwei Tasten bedeutet, dass diese gleichzeitig gedrückt werden müssen: „ALT + R“ beispielsweise signalisiert das Halten der ALT-Taste, während R gedrückt wird. Ein Komma zwischen mehreren Tasten fordert ein nacheinanderdrücken der jeweiligen Tasten. „ALT, R, U“ bedeutet, dass zunächst die ALT-Taste, dann die R- und zuletzt die U-Taste betätigt werden muss.



# Teil II

## DriveLock Control Center



## 2 DriveLock Control Center

Mit Hilfe des DriveLock Control Center (DCC) überwachen Sie den Status der DriveLock Agenten, werten Ereignisse und Vorfälle aus und erzeugen Berichte und Statistiken. Das DCC kommuniziert direkt mit dem DriveLock Enterprise Service (DES) und liest darüber die in der DriveLock Datenbank gespeicherten Informationen und Ereignisdaten aus.

Installieren Sie das DriveLock Control Center direkt auf dem Server, auf dem der DriveLock Enterprise Service ausgeführt wird und/oder auf den Workstations der Administratoren und Helpdesk-Mitarbeiter.

**Eine vollständige Auflistung aller DriveLock Ereignisse finden Sie im Dokument [DriveLock Ereignisse auf DriveLock Online Help](#)**

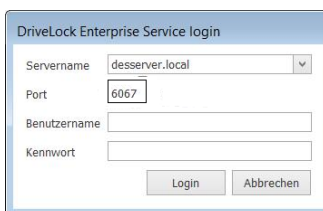
### 2.1 Anmeldung am DCC

Wenn Sie das DriveLock Control Center über das Startmenü oder das Programmsymbol aus starten, wird für die Anmeldung automatisch der aktuell am Betriebssystem angemeldete Benutzer für die Autorisierung verwendet.

Wenn bereits eine Serververbindung konfiguriert wurde, wird diese beim Starten wiederverwendet. Ansonsten können Sie beim ersten Start eine Verbindung angeben bzw. falls DNS-Multicast aktiviert ist eine gefundene Verbindung ausgewählt werden.



#### Anmeldung über Benutzernamen und Passwort

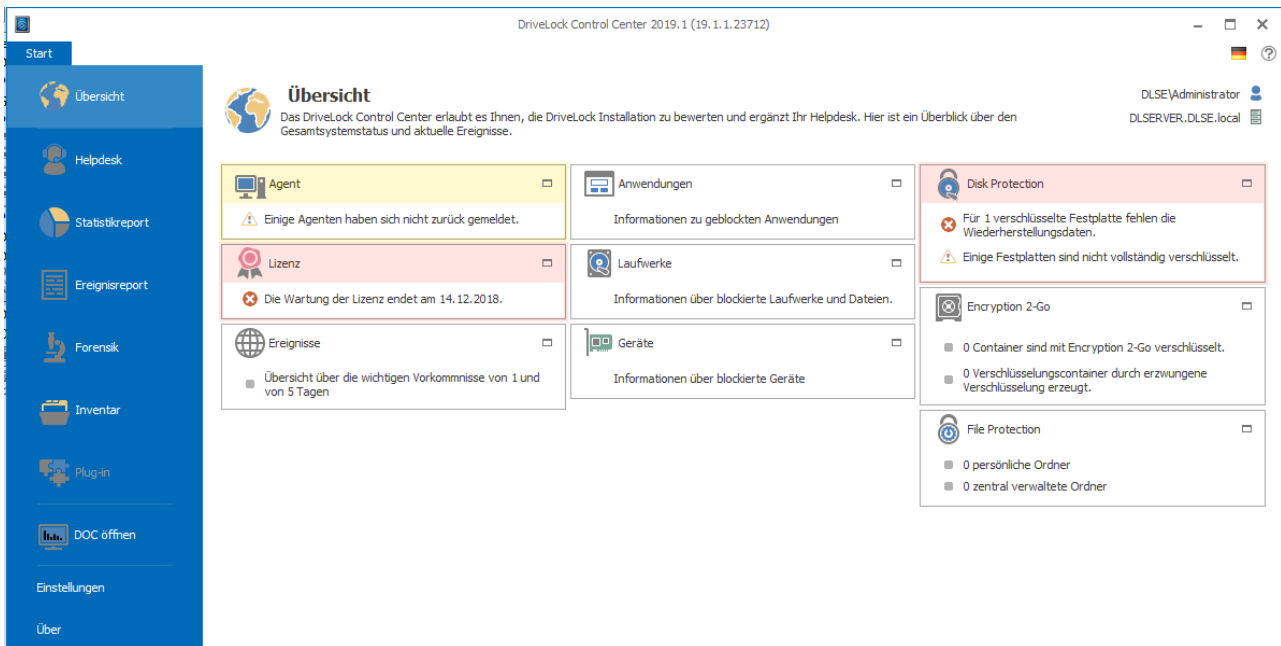
Starten Sie das DCC per Kommandozeile mit dem Parameter `-LoginDlg`, damit ein Login-Dialog erscheint.



Geben Sie hier einen anderen Benutzernamen und das dazugehörige Passwort ein, um sich mit diesem Konto am DCC zu authentifizieren. Ebenfalls können Sie hier eine andere Serververbindung auswählen oder eingeben.

### 2.2 Übersicht

Die DriveLock Control Center Startseite zeigt eine Übersicht wichtiger Informationen zu den unterschiedlichen DriveLock Funktionsbereichen an. Um sich Details anzeigen zu lassen, maximieren Sie einen Bereich durch Klick auf das Symbol  und schließen den Bereich wieder durch Klick auf das Symbol .



## 2.3 Funktionsbereiche

Die Darstellung und Bedienung im DCC ist für alle Funktionsbereiche gleichartig aufgebaut. In der Seitenleiste links wählen Sie zunächst eine Funktion aus. Der zugehörige Arbeitsbereich rechts gliedert sich in folgende Zonen:

### Aktionsschalter

Hier starten Sie bestimmte Aufgaben oder öffnen vordefinierte Ansichten.

### Zuletzt verwendet

Hier sehen Sie die zuletzt verwendeten Ansichten oder Reporte.

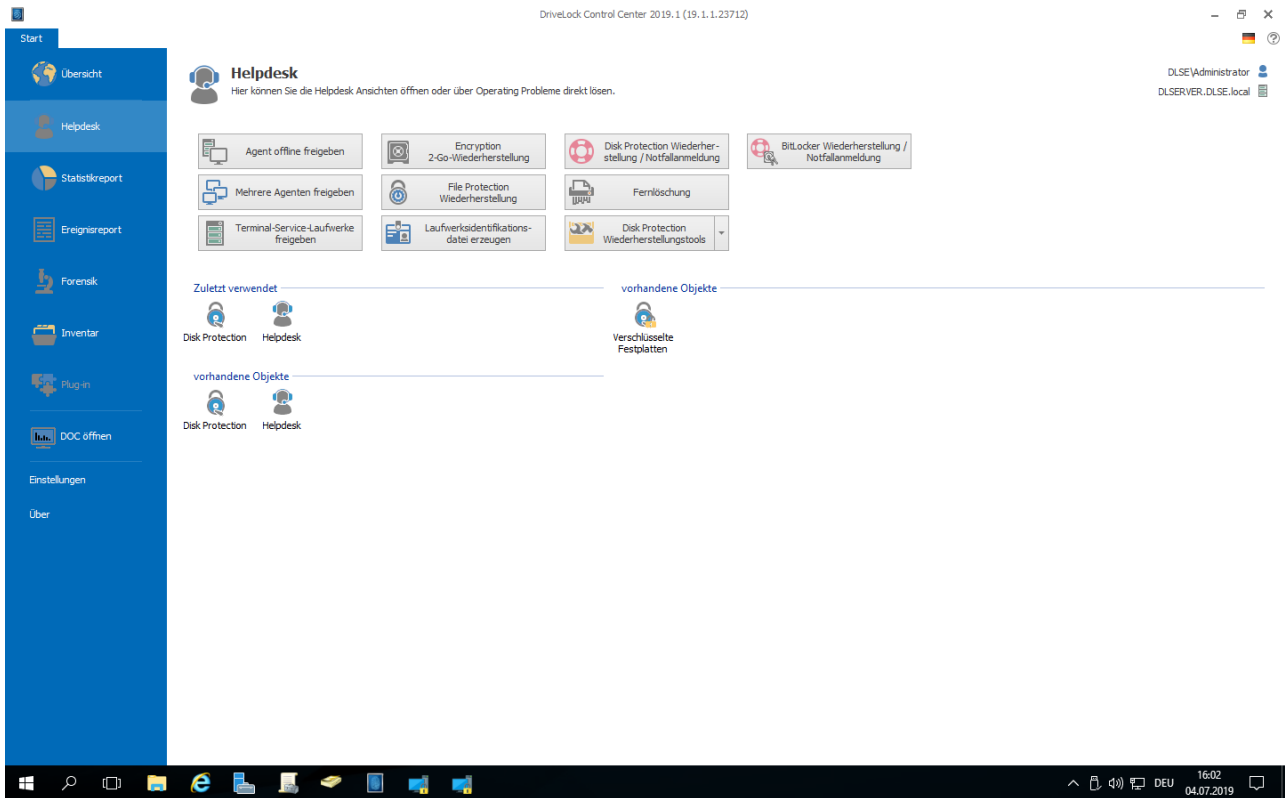
### Installiert

Hier finden Sie alle mit dem DCC installierten Ansichten und Reporte.

### Persönlich / Veröffentlicht

Zeigt, sofern vorhanden, die Ansichten und Reporte, die Sie für sich gespeichert haben bzw. die jemand veröffentlicht hat.

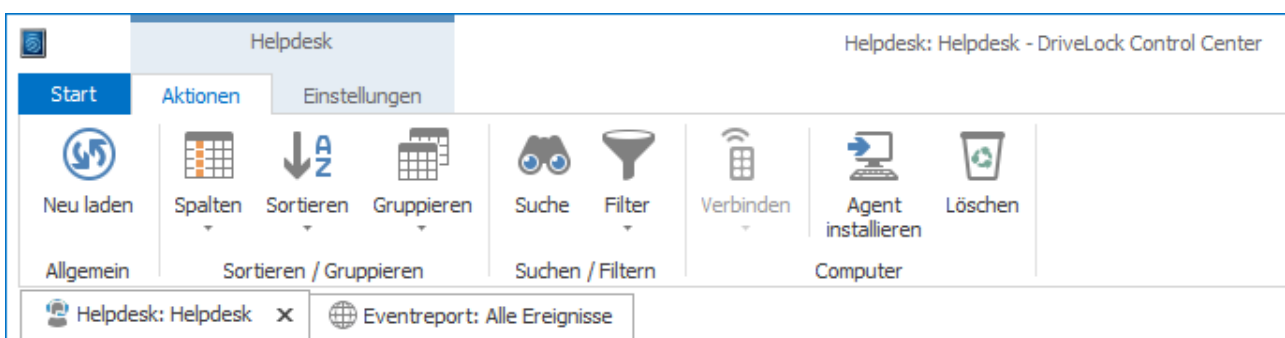


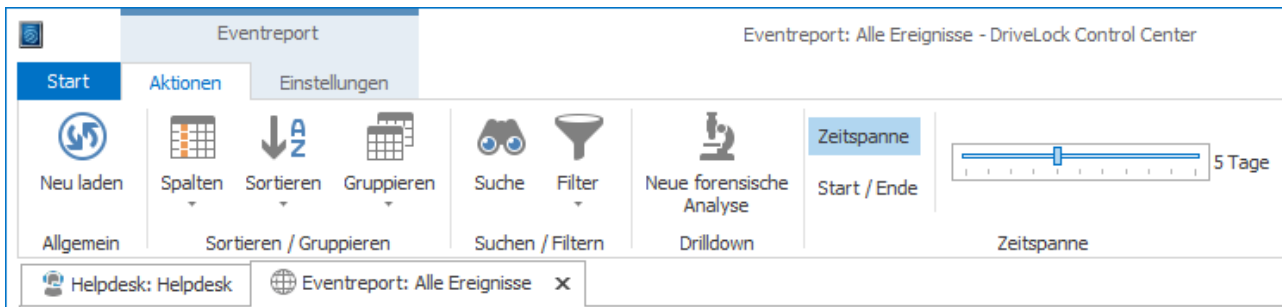


## 2.4 Arbeitsbereich

### 2.4.1 Menüband

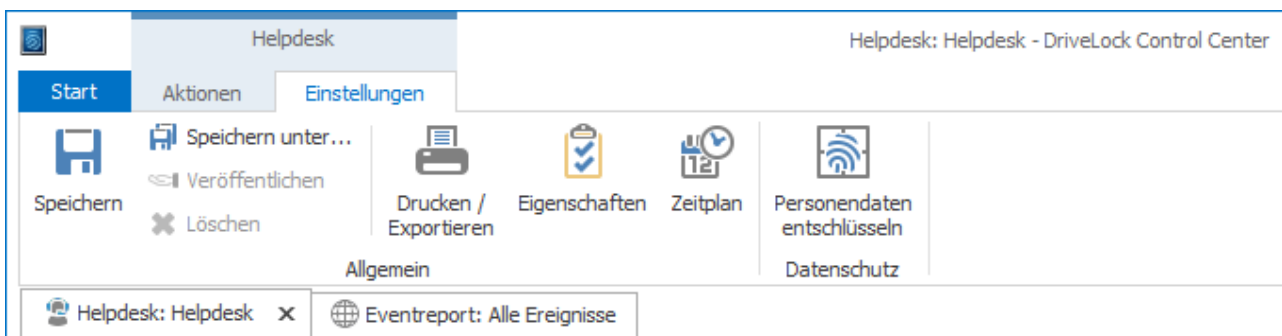
Sobald Sie eine Aktion (Ansicht, Report) öffnen, erhalten Sie neben dem Reiter **Start** zwei weitere Reiter **Aktionen** und **Einstellungen**. Der Text darüber zeigt, auf welche Aktion sich die beiden Reiter beziehen. Im Menüband darunter können Sie die für die gewählte Aktion verfügbaren Aufgaben starten oder Einstellungen vornehmen. In den beiden folgenden Abbildungen sehen Sie die Ansicht bei einem offenen Helpdesk und einem offenen Eventreport.





Mit den Reitern unter dem Menüband schalten Sie schnell zwischen den verschiedenen geöffneten Funktionen um. Zum Schließen klicken Sie auf das **X** rechts auf dem geöffneten Reiter oder klicken mit der mittleren Maustaste auf einen Reiter.

Im Menüband unter Aktionen können Sie die Ansichten und Tabellen nach ihren Wünschen anpassen, sortieren oder gruppieren, in Ergebnissen suchen oder filtern, die Zeitspanne auswählen und zum Funktionsbereich passende Aufgaben starten.



Im Menüband unter Einstellungen speichern und veröffentlichen Sie ihre Anpassungen, bereiten die Ergebnisse für den Druck auf und erstellen Zeitpläne, um sich Berichte automatisiert regelmäßig aufbereiten und zuschicken zu lassen.

## 2.4.2 Ergebnisansichten

Passen Sie die Ansicht der Helpdesks und Reporte nach ihren Wünschen an. Manche der folgenden Anpassungen sind nicht in allen Funktionsbereichen vorhanden.

- **Aktualisieren** - Ereignisdaten können sich ändern, während man die Ergebnisse untersucht. Klicken Sie im Menüband auf **Neu laden**, um die aktuellsten Daten zu sehen.
- **Anpassungsdialog** - rechtsklicken Sie auf eine **Spaltenüberschrift**.
- **Spalten hinzufügen oder entfernen** - klicken Sie im Menüband auf **Spalten** und wählen die Spaltennamen aus oder öffnen Sie im Anpassungsdialog die **Spaltenauswahl** und ziehen Spalten in die Tabelle oder in die Spaltenauswahl zurück.
- **Spalten entfernen** - ziehen Sie eine Spalte mit der Maus an der Spaltenüberschrift aus der Tabelle.
- **Spalten verschieben** - ziehen Sie eine Spalte an die gewünschte Position.
- **Spaltenbreite anpassen** - ziehen Sie am rechten Rand der Spaltenüberschrift oder wählen im Anpassungsdialog **Optimale Breite**.
- **Spalten sortieren** - klicken Sie in eine **Spaltenüberschrift**, um nach dieser Spalte zu sortieren oder die Sortierung umzukehren oder wählen Sie im Anpassungsdialog **Sortierung entfernen**.

- **Daten gruppieren** - wählen Sie im Anpassungsdialog **Gruppierungsfeld anzeigen** und ziehen Sie eine oder mehrere Spalten in das Gruppierungsfeld über den Spaltenüberschriften oder zurück in die Tabelle oder wählen Sie im Menüband **Gruppieren** die gewünschten Spalten aus. In der Tabelle können Sie auf der Schaltfläche ganz links die Inhalte der Gruppen ein- (>) oder ausblenden (v).
- **Zeitspanne festlegen** - Standardmäßig werden die Ereignisse der letzten fünf Tage angezeigt. Klicken Sie im Menüband auf **Zeitspanne** und bewegen den **Schieber** oder klicken Sie auf **Start/Ende** und geben die gewünschten Daten ein.
- **Daten filtern** - doppelklicken Sie auf einen Wert in der Tabelle, um die Ergebnisse schnell nach diesem Wert zu filtern. Der Filter wird unter der Tabelle angezeigt. Klicken Sie auf **X**, um den Filter wieder zu entfernen. Die letzten fünf Filter verbleiben in der Historie.
- **Vordefinierte Filter und Historie** - öffnen Sie im Menüband **Filter** und einen beliebigen vorhandenen Filter.
- **Autofilter** - öffnen Sie im Menüband mit **Filter** die **Auto Filterzeile**. Nun können Sie unter den Spaltenüberschriften Werte eingeben, nach denen die Ergebnisse sofort gefiltert werden. Beginnt der Suchtext mit \*, ändert sich der Filter in *Enthält* anstelle von *Beginnt mit*.
- **Filtereditor** - das DCC hat umfangreiche Filtermöglichkeiten, um zu steuern, welche Daten in einem Bericht angezeigt werden. Sie können einfache Filterbedingungen und detaillierte logische Ausdrücke verwenden. Genaueres erfahren Sie im Kapitel [Filtereditor](#).

Nachdem Sie nun eine angepasste Ansicht erstellt haben, öffnen Sie das Menüband **Einstellungen**, **speichern** Sie die Ansicht für sich ab und geben Sie sie ggf. mit **Veröffentlichen** für andere Administratoren frei.

Gespeicherte Ansichten sind immer nur für den Mandanten sichtbar, mit/für den sie erstellt wurden. Die installierten Ansichten sind für alle Mandanten sichtbar.

## Berechtigungen

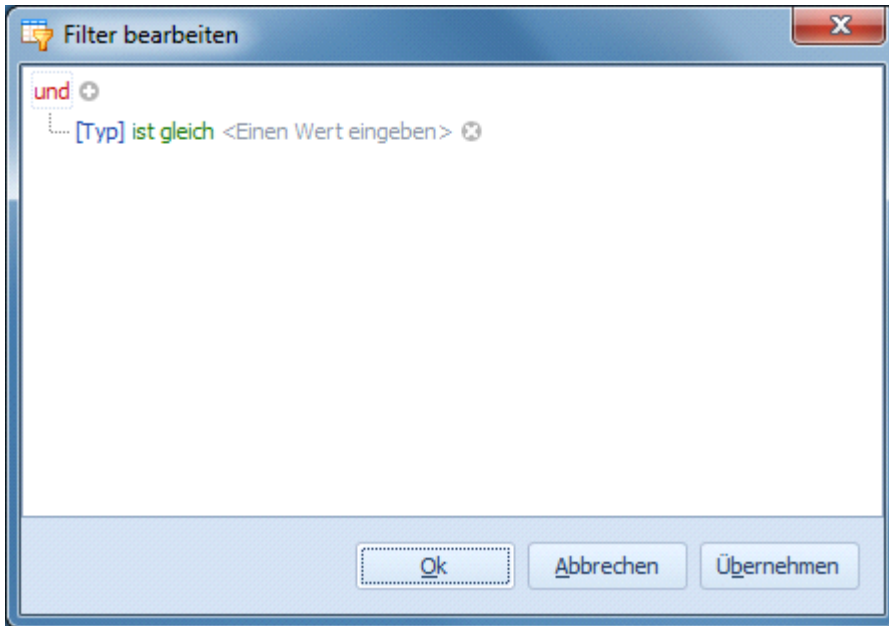
Veröffentlichte Ansichten können in der Voreinstellung durch andere Administratoren geöffnet und eingesehen werden (Leseberechtigung). Allen Benutzern und Gruppen eines Mandanten, die zum DCC hinzugefügt wurden, können Sie weitere Berechtigungen erteilen oder Berechtigungen verweigern. Öffnen Sie eine Ansicht und klicken im Menüband **Einstellungen** auf **Eigenschaften** und dann auf **Sicherheit**. Fügen Sie die Benutzer oder Gruppen hinzu, deren Berechtigungen Sie anpassen wollen und ändern die Rechte.

- **Voll** - Kann die Definition und Berechtigungen ändern.
- **Ändern** - Kann die Definition ändern.
- **Lesen** - Kann die Ansicht öffnen.

### 2.4.3 Filtereditor

Um eigene Filter zu erzeugen, öffnen Sie im Menüband **Filter** und wählen **Editor**.

Sie können Filter dazu verwenden, um eine oder mehrere Bedingungen anhand von standardmäßigen logischen Ausdrücken zu filtern. Entsprechend der Filterkriterien werden die Ereignisse angezeigt.



Um einen Filter zu erstellen, führen Sie die folgenden Schritte in der Filtertafel aus:

- Klicken Sie auf (+).
- In der neuen Filterbedingung klicken Sie auf **[Typ]** und klicken dann auf den Namen der Spalte, die von dem Filter verwendet werden soll.
- Klicken Sie auf **ist gleich** und wählen dann einen der Ausdrücke aus. Welche Ausdrücke verfügbar sind, hängt von dem Datentyp der jeweiligen Spalte ab. Sie enthalten *ist gleich, ist ungleich, ist größer als, ist kleiner als, enthält, beginnt mit* und *endet mit*.
- Klicken Sie auf **<Einen Wert eingeben>** und wählen einen Wert aus oder geben Sie einen ein, der in dem Ausdruck enthalten sein soll. Abhängig von dem Datentyp der Spalte können Sie aus einer Liste oder aus einem Kalender auswählen oder einen eigenen Wert eintragen.

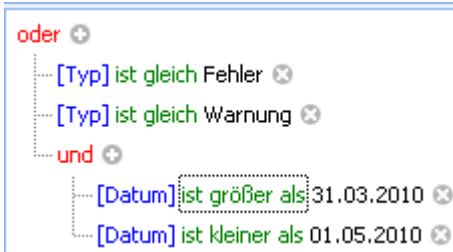
Standardmäßig werden mehrere Bedingungen in der Filtertafel über einen **und** Operator miteinander kombiniert, d.h. es werden nur Ereignisse angezeigt, die alle Bedingungen erfüllen. Um den Operatortyp zu ändern, klicken Sie auf **und** und wählen einen der folgenden Operatoren aus:

- *und*: Es werden nur Ereignisse angezeigt, die alle Bedingungen erfüllen.
- *oder*: Es werden Ereignisse angezeigt, die eine der Bedingungen erfüllen.
- *nicht und*: Es werden nur Ereignisse angezeigt, die keine der Bedingungen erfüllen.
- *nicht oder*: Es werden nur Ereignisse angezeigt, die nicht eine der Bedingungen erfüllen.

Um weitere Bedingungen zu einem Filterausdruck hinzuzufügen, klicken Sie auf den Operator und wählen **Bedingung hinzufügen**.

Um eine komplexe Filterung zu ermöglichen, können Sie Filterbedingungen gruppieren und verschachteln. Um z.B. einen Filter zu erstellen, der alle Warnungen und Fehler im April 2010 anzeigt, muss man die folgenden Bedingungen verwenden:

- Typ gleich Warnung oder Typ gleich Fehler.
- Datum ist größer als der 31.3.2010 und Datum ist kleiner als 1.5.2010.
- Kombinieren Sie beide vorherigen Gruppen-Filter mit einem **und** Operator.



Um einem bestehenden Operator eine neue Gruppe wie ein **und** oder **oder** hinzuzufügen, klicken Sie auf **Gruppe hinzufügen**. Eine neue Gruppe wird unterhalb des aktuellen Operators eingerückt angezeigt. Die neue Gruppe enthält zu Beginn eine leere Filterbedingung. Sie können den Operator ändern, die Filterbedingungen bearbeiten oder weitere Bedingungen der Gruppe hinzufügen.

Das DriveLock Control Center behandelt die Bedingungen jeder einzelnen Gruppe auf der kleinsten gemeinsamen Menge. Das Ergebnis aus jeder Gruppe wird dann mit dem jeweils höheren Operator verglichen. Im Ergebnis werden nur Ereignisse angezeigt, die den kompletten logischen Ausdruck erfüllen.

Eine einzelne Bedingung zu entfernen, funktioniert über einen Klick auf die (x) Schaltfläche an der rechten Seite der jeweiligen Bedingung. Alternativ dazu können Sie auch auf den Gruppen Operator und auf **Gruppen entfernen** klicken. Um alle Bedingungen zu entfernen, klicken Sie auf den obersten Operator und wählen **Alles leeren** aus.

Um einen Filter von einem Report zu entfernen, klicken Sie auf **Kein Filter** im Bereich **Filter**.

## 2.4.4 Ergebnisse drucken und exportieren

Wählen Sie im **Einstellungen** Menüband **Drucken / Exportieren**, um die Vorschau zu öffnen.

The screenshot shows the 'Drucken und Exportieren' (Print and Export) window in DriveLock Control Center. The main content is a preview of a helpdesk report titled 'Helpdesk' dated 12.01.2015. The report includes a table with the following data:

Status	Computer Name	Domäne	Letzter Benutzer	Letzter Standort	Agenten Version	Letzter Kontakt	Encryption 2-Go Lizenz	FDE Lizenz	Antivirus Lizenz	File Protection Lizenz	FDE Status	FDE Version	Notfallmeldung	Festplattenwiederherstellung	Antivirus Software Version	Antivirusignaturversion	Antivirusignatur letzte Aktualisierung
Ausgeschaltet	BAHAMAS	my-domain.org	my-domain\carver	my-site	7.3.9	07.01.2015 13:35:38	gewährt	nicht gewährt	gewährt	nicht gewährt	FDE: Status unbekannt		nicht gewährt	nicht gewährt	0.0.0		
Ausgeschaltet	BEIJING	my-domain.org	my-domain\LeChiffre	my-site	7.3.9	07.01.2015 13:35:38	nicht gewährt	nicht gewährt	nicht gewährt	nicht gewährt	FDE: Nicht installiert		nicht gewährt	nicht gewährt	0.0.0		
Ausgeschaltet	DL-FDE-01	my-domain.org	my-domain\goIdfinger	my-site	7.3.9	07.01.2015 13:35:38	nicht gewährt	nicht gewährt	nicht gewährt	nicht gewährt	FDE: Vollständig verschlüsselt		nicht gewährt	nicht gewährt	0.0.0		
Ausgeschaltet	DL-FDE-02	my-domain.org	my-domain\carver	my-site	7.3.9	07.01.2015 13:35:38	nicht gewährt	nicht gewährt	nicht gewährt	nicht gewährt	FDE: Vollständig verschlüsselt		nicht gewährt	nicht gewährt	0.0.0		
Ausgeschaltet	DL-FDE-03	my-domain.org	my-domain\larigo	my-site	7.3.9	07.01.2015 13:35:38	nicht gewährt	nicht gewährt	nicht gewährt	nicht gewährt	FDE: Wird installiert		nicht gewährt	nicht gewährt	0.0.0		

## Zoom

Nutzen Sie im Menüband den Bereich **Zoom**, um die Darstellung nach ihren Vorstellungen anzupassen und sich einen Überblick über die Ergebnisse zu verschaffen

## Wasserzeichen

Konfigurieren Sie Wasserzeichen, um die Seiten mit Text (z.B. VERTRAULICH) oder Bildern (z.B. ihr Firmendesign) zu hinterlegen.

## Drucken

Klicken sie **Sofortdruck**, um die Ergebnisse auf dem voreingestellten Drucker mit den Standardeinstellungen auszugeben oder klicken Sie **Drucken**, um einen Drucker auszuwählen oder Druckeinstellungen zu tätigen.

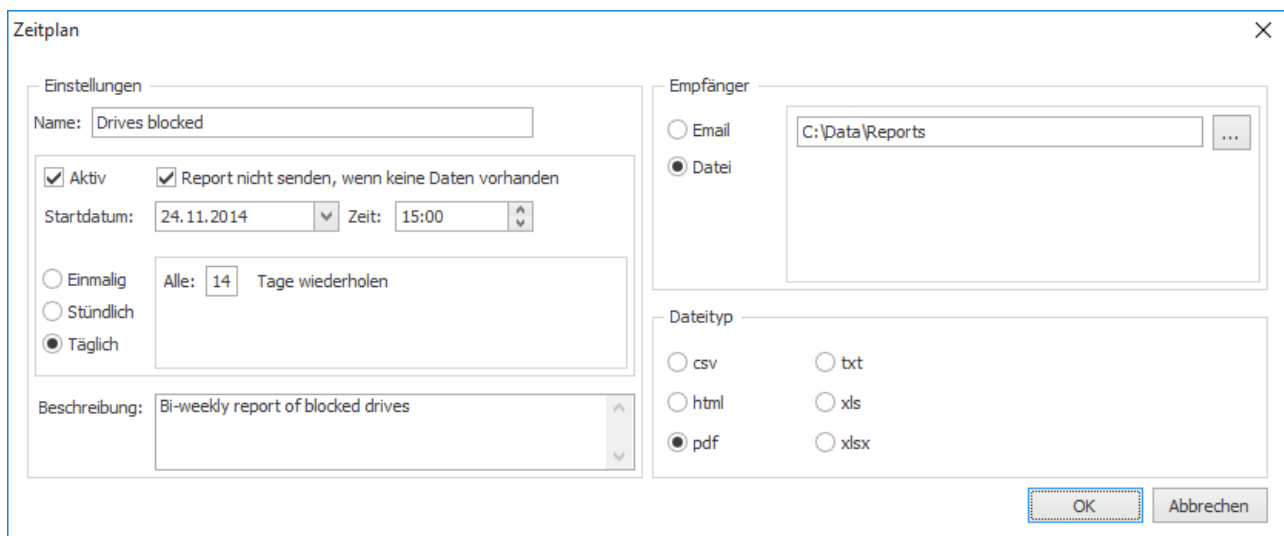
## Exportieren

Sie können die Ergebnisse auch in verschiedensten Ausgabeformaten speichern, z.B. als PDF, um sie zu archivieren, als EXCEL, um weitere Auswertungen zu erstellen oder als HTML, um die Ergebnisse im Intranet zu veröffentlichen.

### 2.4.5 Automatisierte Berichte

Jede gespeicherte Ergebnisansicht kann nach Zeitplan erstellt und per Email versendet oder in einem Verzeichnis (z.B. auf einem Netzlaufwerk) bereitgestellt werden. So können Personen regelmäßig Berichte erhalten, ohne Zugriff auf das DCC zu benötigen. Vordefinierten Ansichten können nicht für einen Zeitplan verwendet werden.

Um zum Beispiel einen automatisierten Bericht für gesperrte Laufwerke zu erstellen, öffnen Sie den vordefinierten Bericht **Laufwerks-Ereignisse**, filtern **Ereignis ID = 115** und speichern den Bericht, z.B. als **Drives blocked** ab. Nun öffnen Sie im **Einstellungen** Menüband mit **Zeitplan / Neu** einen neuen Zeitplan.



Vergeben Sie einen Namen, legen Sie fest, wann, in welchen Intervallen und mit welchem Format der Bericht erstellt werden soll und hinterlegen Sie eine aussagekräftige Beschreibung, welchen Zweck der Bericht verfolgt.

Die Anzahl der in einer Datei enthaltenen Ereignisse ist aus technischen Gründen auf 100.000 Ereignisse limitiert.

## Per Email versenden

Im Bereich Empfänger aktivieren Sie **Email** und fügen eine oder mehrere E-mail-Adressen hinzu. Mit **Test Email** können Sie prüfen, ob der Email-Versand funktioniert.

Damit automatische Berichte versendet werden können, muss am DriveLock Enterprise Service ein SMTP-Server eingestellt werden. Weitere Informationen hierzu finden Sie im DriveLock Administrationshandbuch.

### Als Datei bereitstellen

Um den automatisch generierten Bericht in einem Ordner abzuspeichern, aktivieren Sie im Bereich Empfänger Datei und wählen dann das Verzeichnis aus, in dem die Datei abgelegt werden soll.





Damit in dem angegebenen Verzeichnis ein Bericht abgespeichert werden kann, muss das Verzeichnis vom DriveLock Enterprise Service erreichbar sein und das Konto, unter dem der DriveLock Enterprise Service läuft, muss dort Schreibrechte besitzen.

Sie können einen bestehenden Zeitplan deaktivieren, ohne die Einstellungen zu löschen. Dazu deselektieren Sie im Zeitplan die Option **Aktiv**.

### 2.4.6 Anonyme Daten

In verschiedenen Ländern (z.B. in Deutschland) ist der Schutz personenbezogener Daten durch gesetzliche Anforderungen sehr genau geregelt. Gleiches gilt für die Speicherung von Daten mit personenbezogenen Inhalten, wenn diese zur Auswertung bzw. Überwachung von Tätigkeiten verwendet werden können.

Durch die umfangreichen Auswertungsmöglichkeiten, die das DriveLock Control Center zur Verfügung stellt, muss insbesondere in diesen Ländern diese Problematik beachtet werden. Daher bietet das DriveLock Control Center die Möglichkeit, den Zugriff auf Reporte oder den Forensik-Bereich nur für zuvor berechnete Personen zu gestatten. Darüber hinaus ist der DriveLock Agent in der Lage, in jedem Ereignis, das an den DriveLock Enterprise Service gesendet wird, den Computernamen und/oder den Benutzernamen per Verschlüsselung zu anonymisieren. Im DriveLock Control Center werden dann die Informationen in diesen beiden Spalten anonymisiert dargestellt:

Startseite Alle Ereignisse Report				
Ziehen Sie eine Spaltenüberschrift in diesen Bereich, um nach dieser zu gruppieren				
Typ	Beschreibung	Ereignis-ID	Benutzer	Computername
 Überwachung erfolgreich	Laufwerk getrennt	113	Verschlüsselt	Verschlüsselt
 Überwachung gescheit...	Benutzungsrichtlinie abgelehnt	253	Verschlüsselt	Verschlüsselt
 Überwachung erfolgreich	Laufwerk verbunden und gesperrt	111	Verschlüsselt	Verschlüsselt
 Überwachung gescheit...	Dateizugriff	133	Verschlüsselt	Verschlüsselt

Dadurch ist eine Auswertung und Überwachung der Systemumgebung weiterhin ohne Einschränkungen möglich, ein direkter Bezug zwischen Ereignissen und einer bestimmten Person lässt sich aber ohne weiteres nicht herstellen.

Damit im speziellen Fall dennoch eine detaillierte Nachvollziehbarkeit möglich ist, kann mit Hilfe eines Assistenten die Anonymisierung dieser Daten temporär aufgehoben werden.



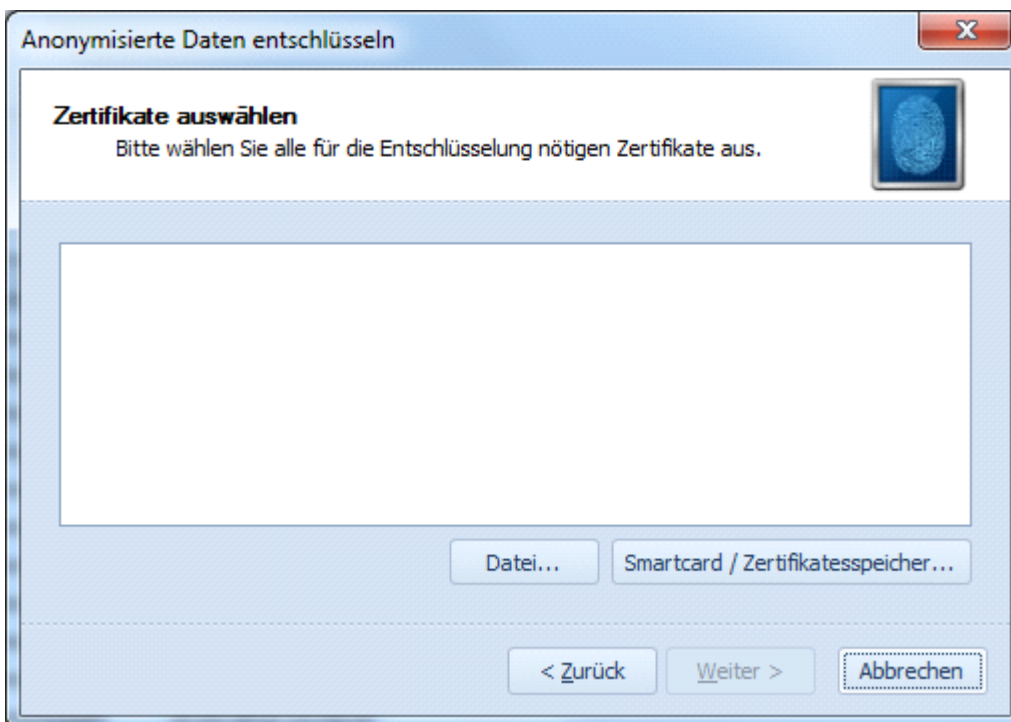
Personendaten  
entschlüsseln

Datenschutz

Klicken Sie dazu auf die Schaltfläche **Personendaten entschlüsseln** im Menüband Einstellungen.



Klicken Sie auf **Weiter**.



Nun müssen Sie alle Zertifikate angeben, die bei der Konfiguration der Verschlüsselung innerhalb der DriveLock Richtlinie erzeugt bzw. geladen wurden. Die Reihenfolge spielt dabei keine Rolle.

Zertifikate können entweder als Datei (\*.pfx / \*.p12) vorliegen, von einer Smartcard / einem Token eingelesen oder aus dem Zertifikatsspeicher des aktuellen Benutzers ausgewählt werden.

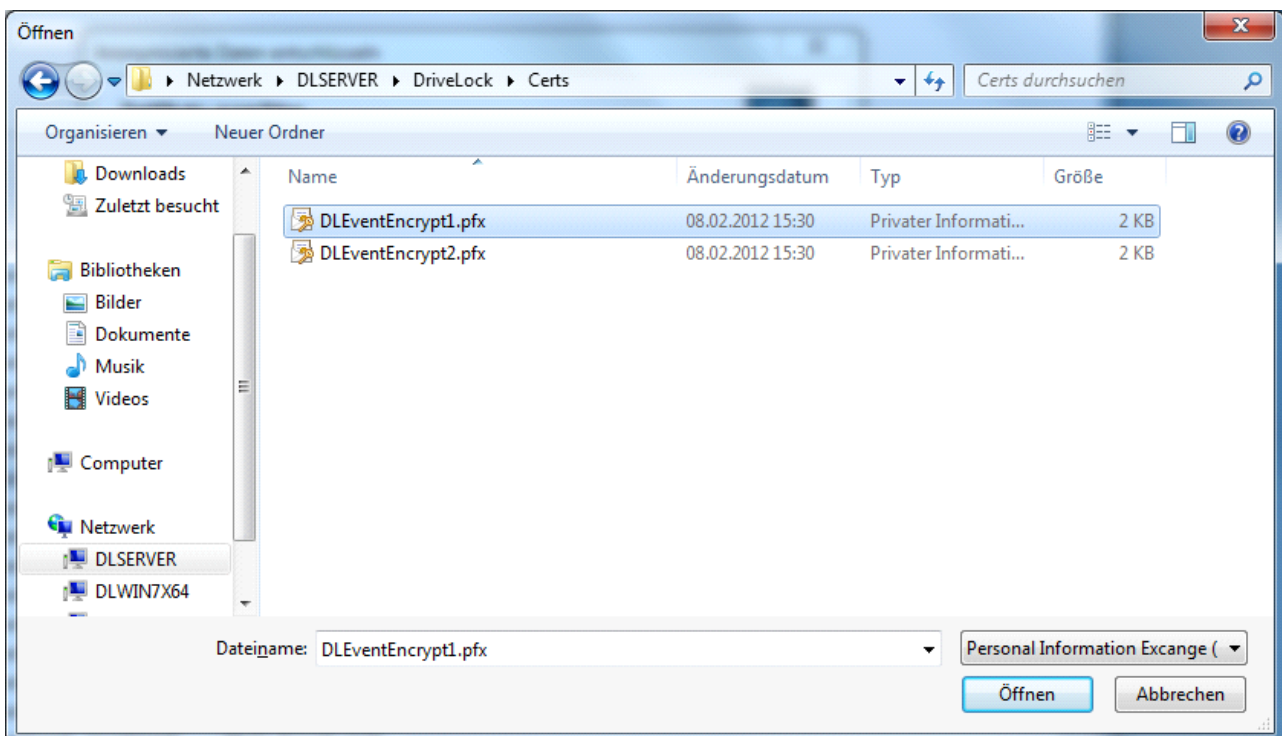
Stecken Sie eine Smartcard in das Lesegerät bzw. ein Token an Ihren Computer an, bevor Sie auf **Smartcard / Zertifikatsspeicher** klicken.





Wählen Sie dann ein Zertifikat aus.

Liegt das Zertifikat als Datei vor, klicken Sie auf **Datei**.



Wählen Sie nun die gewünschte Datei aus und geben Sie das Passwort für den privaten Schlüssel ein und bestätigen Sie diese Zertifikat, indem Sie auf OK klicken.

Wurden in der DriveLock Richtlinie mehrere Zertifikate konfiguriert, so wiederholen Sie diesen Vorgang, bis Sie alle benötigten Zertifikate angegeben haben. Klicken Sie anschließend auf **Weiter**.

Nun wird die Entschlüsselung mit den angegebenen Zertifikaten überprüft. Konnten keine oder nicht alle der testweise ausgewählten Daten mit den angegebenen Zertifikaten entschlüsselt werden, so erscheint ein entsprechender Hinweis. In diesem Fall können Sie den Assistenten entweder beenden, oder zurück zur Zertifikatsauswahl gehen, um Änderungen vorzunehmen.

Wurde der Assistent erfolgreich beendet, werden nun anstelle der anonymisierten Daten die originalen personenbezogenen Daten angezeigt. Zusätzlich ändert sich die Schaltfläche im Reiter **Einstellungen**:



Die Entschlüsselung bleibt nun für alle Bereiche des DriveLock Control Center bestehen, bis Sie entweder über diese Schaltfläche die Anonymisierung wieder aktivieren oder das DriveLock Control Center schließen.



# Teil III

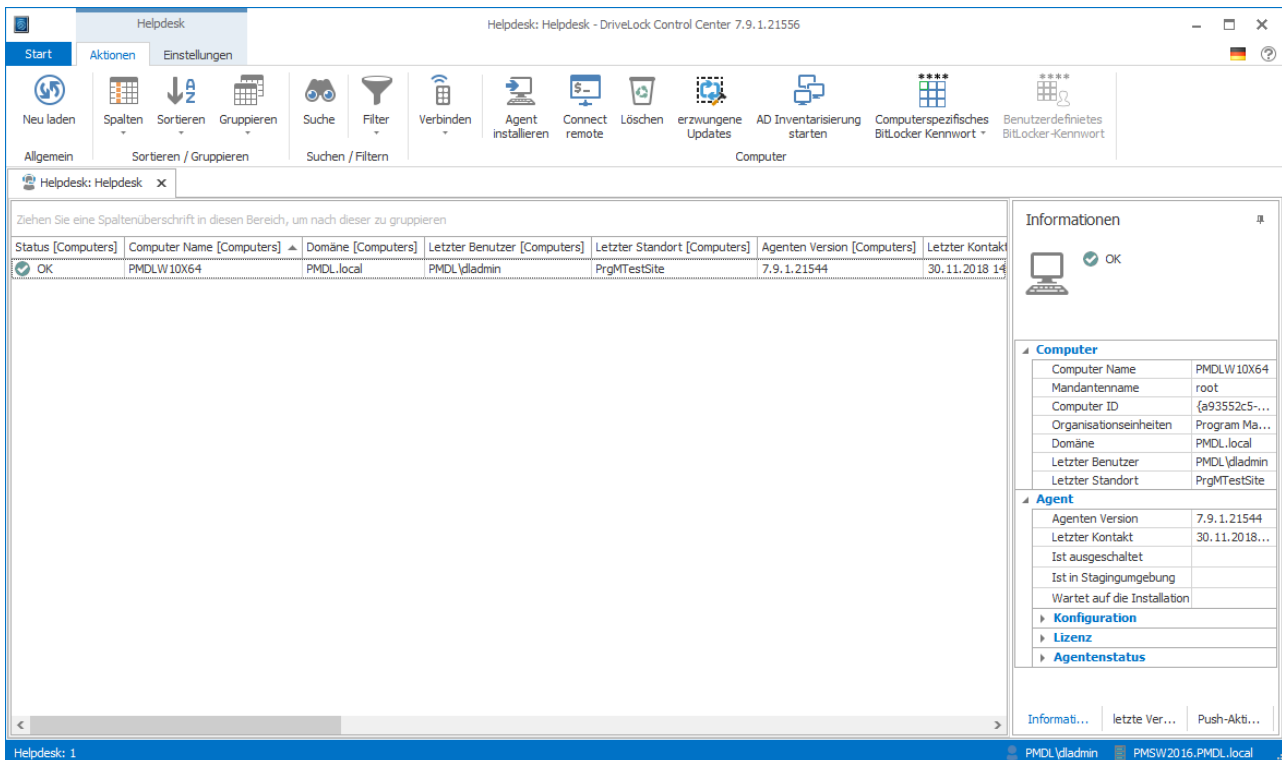
## Helpdesk



### 3 Helpdesk

Der Helpdesk-Bereich des DriveLock Control Center stellt Funktionen für verschiedene allgemeine Helpdesk-Aufgaben bereit.

Öffnen Sie im Funktionsbereich **Helpdesk** eine der Ansichten. Sie können verschiedene Sichten auf ihre installierten Computern definieren, filtern, gruppieren und nach den unterschiedlichsten Kriterien auswerten, um wiederkehrende Monitoring- und Helpdesk-Aufgaben schnell und effizient zu erledigen. Wie Sie die Helpdesk-Ansichten an ihre Bedürfnisse anpassen, speichern, freigeben, ausdrucken, exportieren und automatisiert bereitstellen, ist im Kapitel [Arbeitsbereich](#) beschrieben. Im Detailbereich rechts können Sie entweder Einzelheiten zum ausgewählten Computer oder eine Liste der zuletzt verbundenen Computer anzeigen oder Richtlinien Updates erzwingen .



The screenshot shows the 'Helpdesk' window in DriveLock Control Center. The main area contains a table with the following columns: Status [Computers], Computer Name [Computers], Domäne [Computers], Letzter Benutzer [Computers], Letzter Standort [Computers], Agenten Version [Computers], and Letzter Kontakt. The table contains one entry for computer 'PMDLW10X64' with status 'OK', domain 'PMDL.local', user 'PMDL\jladmin', location 'PrgMTestSite', and agent version '7.9.1.21544'. The last contact was on '30.11.2018 14:...'.

On the right side, there is an 'Informationen' panel for the selected computer, showing details for the 'Computer' and 'Agent' sections.

Status [Computers]	Computer Name [Computers]	Domäne [Computers]	Letzter Benutzer [Computers]	Letzter Standort [Computers]	Agenten Version [Computers]	Letzter Kontakt
OK	PMDLW10X64	PMDL.local	PMDL\jladmin	PrgMTestSite	7.9.1.21544	30.11.2018 14:...

**Informationen**

**Computer**

Computer Name	PMDLW10X64
Mandantenname	root
Computer ID	{a93552c5-...
Organisationseinheiten	Program Ma...
Domäne	PMDL.local
Letzter Benutzer	PMDL\jladmin
Letzter Standort	PrgMTestSite

**Agent**

Agenten Version	7.9.1.21544
Letzter Kontakt	30.11.2018...
Ist ausgeschaltet	
Ist in Stagingumgebung	
Wartet auf die Installation	

Buttons: Informati..., letzte Ver..., Push-Akti...

#### Statusinformationen

In der ersten Spalte wird der aktuelle Status des DriveLock Agenten bzw. des Computers angezeigt. Der Status wird vom Agenten in regelmäßigen Abständen, welchen Sie in der DriveLock Richtlinie konfigurieren können, an den DES übertragen (Standardwert: alle 10 Minuten).

Ab der Version 7.8 sehen Sie hier auch, ob eine temporäre Freigabe zum Zeitpunkt der letzten Datenübertragung aktiv war. Zusätzlich zeigt eine neue Spalte diesen speziellen Zustand separat an.

#### Vordefinierte Filter

Im Menüband öffnen Sie **Filter** und sehen im Untermenü - im Vergleich zu den Ereignisreporten - weitere Filtermöglichkeiten auf eine Helpdesk-Ansicht. Diese vordefinierten Filter können Sie verwenden, um schnell nach häufig verwendeten Kriterien zu filtern.

#### Computer löschen

Unter bestimmten Umständen kann es notwendig werden, angezeigte Computer aus der Liste zu löschen, z.B. weil Sie nicht mehr in der Systemumgebung vorhanden sind. Um einen Computer aus der Helpdesk-Ansicht zu entfernen, wählen Sie den Computer in der Liste aus und klicken im Menüband auf **Löschen**. Bestätigen Sie einmal, und falls

Wiederherstellungsdaten vorhanden sind ein zweites Mal, dass Sie den Computer wirklich löschen wollen. Der Computer wird jetzt einschließlich aller Ereignisse und Wiederherstellungsdaten aus der DriveLock-Datenbank gelöscht und im Helpdesk nicht mehr angezeigt.

### Agenten installieren

Mit **Agenten installieren** können Sie eine manuelle Push-Installation (Erst- oder Reparaturinstallation) des DriveLock Agenten auf einem oder mehreren PCs in ihrem Netzwerk starten.

Wenn die *automatisierte Push-Installation* konfiguriert ist, werden auch die dafür vorgesehenen PCs ohne installierten Agenten in der Rechnerliste angezeigt und können dort selektiert und per Rechter-Mausklick installiert werden.

Die Administration und Durchführung der Push-Installation ist im DriveLock Administrationshandbuch im Kapitel „*Push-Installation von DriveLock*“ beschrieben.

### Mit Computer verbinden

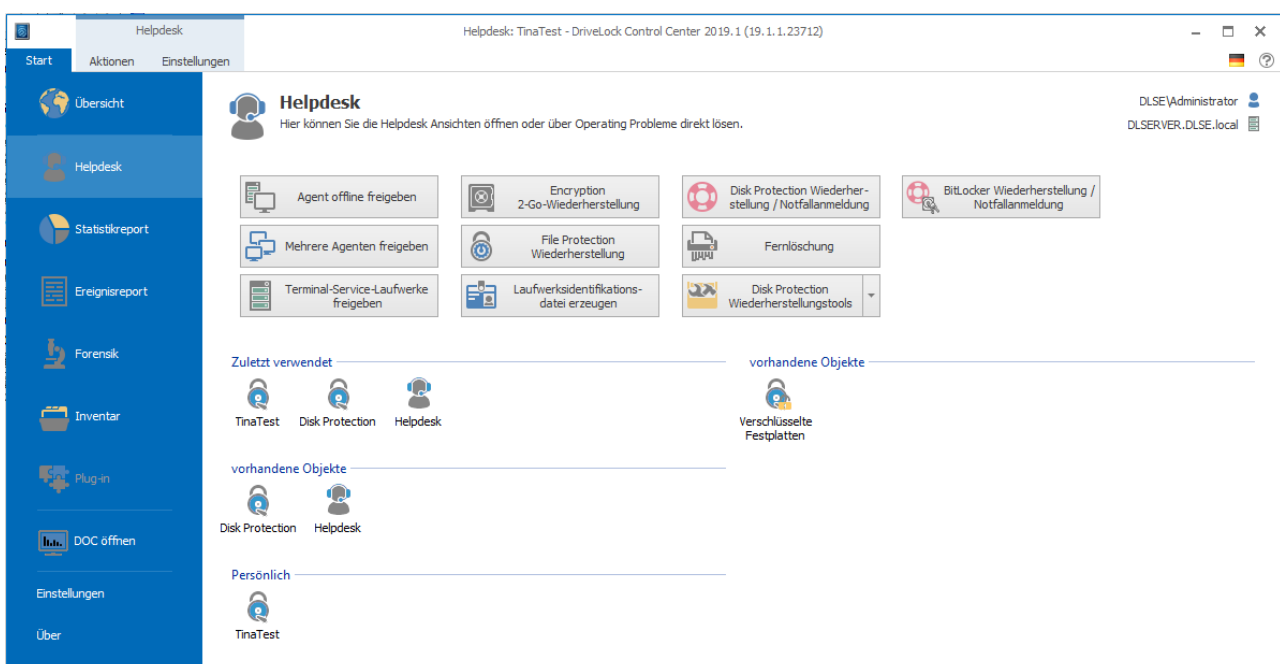
Um sich per *Agenten-Fernkontrolle* mit einem Computer zu verbinden, wählen Sie diesen in einer Helpdesk-Ansicht aus und klicken im Menüband auf das Icon über **Verbinden** oder klicken auf **Verbinden** und tippen den Namen eines Computers ein. Im Arbeitsbereich öffnet sich ein weiterer Reiter mit Aktionen für den verbundenen Computer..

Klicken Sie auf **Trennen** um die Verbindung wieder zu beenden. Wie Sie die *Agenten-Fernkontrolle* verwenden, um Wartungs- und Monitoring-Aufgaben direkt auf einem verbundenen Computer durchzuführen, ist im DriveLock Administrationshandbuch im Kapitel *Agenten-Fernkontrolle verwenden* beschrieben.

Für die Agenten-Fernkontrolle und die weiteren Wartungsaufgaben muss die DriveLock Management Konsole auf dem selben Computer installiert sein wie das DCC. Ansonsten sind entsprechenden Schaltflächen ausgegraut dargestellt und können nicht verwendet werden.

## 3.1 Wartungsaufgaben

Über die Aktionsschalter können Sie die selben Wartungsaufgaben durchführen, die auch in der DriveLock Management Konsole unter **Betrieb** zur Verfügung stehen.



The screenshot shows the DriveLock Helpdesk interface. The title bar reads 'Helpdesk: TinaTest - DriveLock Control Center 2019.1 (19.1.1.23712)'. The interface includes a left sidebar with navigation options: Start, Aktionen, and Einstellungen. The main content area is titled 'Helpdesk' and contains several action buttons for maintenance tasks:

- Agent offline freigeben
- Encryption 2-Go-Wiederherstellung
- Disk Protection Wiederherstellung / Notfallanmeldung
- BitLocker Wiederherstellung / Notfallanmeldung
- Mehrere Agenten freigeben
- File Protection Wiederherstellung
- Fernlöschung
- Terminal-Service-Laufwerke freigeben
- Laufwerksidentifikationsdatei erzeugen
- Disk Protection Wiederherstellungstools

Below the action buttons, there are sections for 'Zuletzt verwendet' (TinaTest, Disk Protection, Helpdesk) and 'vorhandene Objekte' (Verschlüsselte Festplatten). A 'Persönlich' section shows TinaTest.

Diese Aufgaben sind den in den im folgenden angegebenen Kapiteln im DriveLock Administrationshandbuch beschrieben.

- **Agenten offline freigeben, Mehrere Agenten freigeben, Terminal-Service-Laufwerke freigeben** - um durch DriveLock gesperrte Geräte oder Laufwerke temporär zu entsperren  
Kapitel *Agenten-Fernkontrolle verwenden / Temporäre Zugriffsrechte/Freigabe erteilen*
- **Container Kennwort Wiederherstellung, Wiederherstellung verschlüsselter Ordner** - die *Offline-Wiederherstellung* von verschlüsselten Ordnern oder verschlüsselten Containern starten  
Kapitel *DriveLock Encryption 2-Go / Wiederherstellung verschlüsselter Containerdateien*  
Kapitel *DriveLock File Protection / Wiederherstellung verschlüsselter Verzeichnisse*
- **Disk-Wiederherstellung/Notfallanmeldung, Datenwiederherstellung** - für die Festplattenverschlüsselung eine *Wiederherstellung verschlüsselter Laufwerke* anstoßen oder eine *Notfall-Anmeldung* bearbeiten, bzw. Boot-Medien zur Datenwiederherstellung erzeugen  
Kapitel *DriveLock Full Disk Encryption / Wiederherstellungsverfahren* bzw. *BitLocker Management Handbuch*
- **Laufwerks-Identifikations-Datei erzeugen**  
Kapitel *Laufwerke und Geräte kontrollieren / ... / Laufwerks-Identifikations-Dateien*
- **Fernlöschung** - verschlüsselte Festplatten bzw. deren Benutzerdatenbank fernlöschen  
Kapitel *DriveLock Full Disk Encryption / .. / Fernlöschung initiieren*

## 3.2 Supportdateien übermitteln

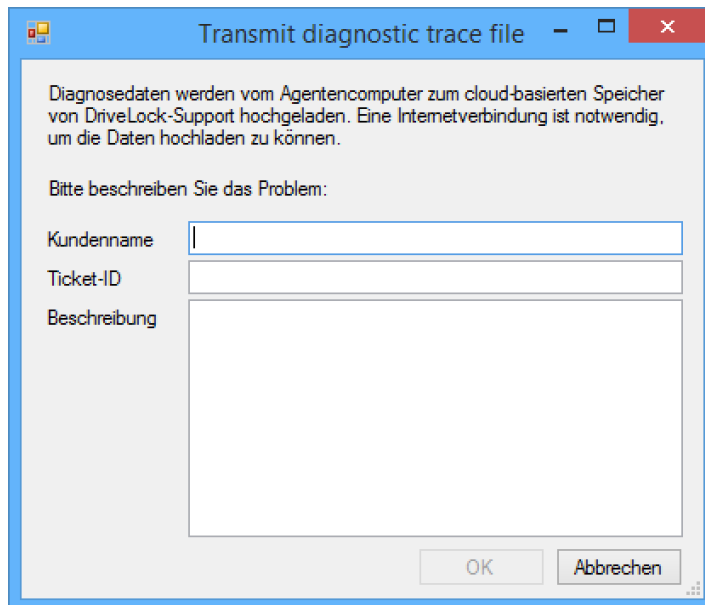
Ab der Version 7.8 können Sie über das Helpdesk ganz einfach alle benötigten Supportinformationen zu einem bereits geöffneten Supportticket übermitteln.

**Bitte wenden Sie sich zuvor an den DriveLock Support und eröffnen ein Ticket. Sie erhalten dann eine Ticket-ID, die Sie im Folgenden eingeben und dadurch die korrekte Zuordnung Ihrer Supportdaten zu Ihrem Anliegen ermöglichen.**

Mit folgenden Schritten übertragen Sie die Supportinformationen / Logdateien:

1. Starten Sie die **Helpdesk** Ansicht.
2. Verbinden Sie sich mit dem Computer, von dem Sie die Logdateien und Supportinformationen übermitteln möchten.

3. Klicken Sie auf **Upload trace logs** im oberen Menüband.



4. Bitte geben Sie jetzt Ihren Firmennamen, die zuvor erhaltene Ticket-ID und eine kurze Beschreibung ein.
5. Klicken Sie auf **OK**, um die Daten zu übertragen.

# Teil IV

## Statistikreporte



## 4 Statistikreporte

Statistikreporte ermöglichen die Analyse von DriveLock-Ereignissen über einen bestimmten Zeitraum und/oder bezogen auf die Anzahl von Ereignissen. Dabei ist es auch möglich, Zeiträume miteinander zu vergleichen und Veränderungen zu erkennen.

Verwenden Sie Statistikreporte, um zum Beispiel folgende Fragestellungen zu beantworten:

- Welches Datenvolumen wurde in der letzten Zeit übertragen?
- Wie viele Benutzer haben in den letzten beiden Monaten die Verwendungsrichtlinie akzeptiert oder abgelehnt?
- Wie viele USB-Sticks wurden in den vergangenen 6 Monaten blockiert?

Statistikreporte ähneln den Pivot-Tabellen in Microsoft Excel. Basierend auf den ermittelten Werten können Sie Grafiken in unterschiedlichen Darstellungsweisen erstellen, um den Sachverhalt in grafischer Form zu visualisieren. Dabei stehen Ihnen im DCC alle Möglichkeiten zur Verfügung, ohne dass Sie sich mit der Erstellung von Pivot-Tabellen im Detail auseinandersetzen müssen.

Statistikreporte können für folgende Einsatzzwecke verwendet werden:

- Analyse von Veränderungen über einen vorgegebenen Zeitraum
- Erkennen von Trends
- Erkennen von Abweichungen innerhalb eines Zeitraumes
- Vergleichen von zwei oder mehreren Zeiträumen, wie zum Beispiel Jahr, Quartal, Monat oder Woche

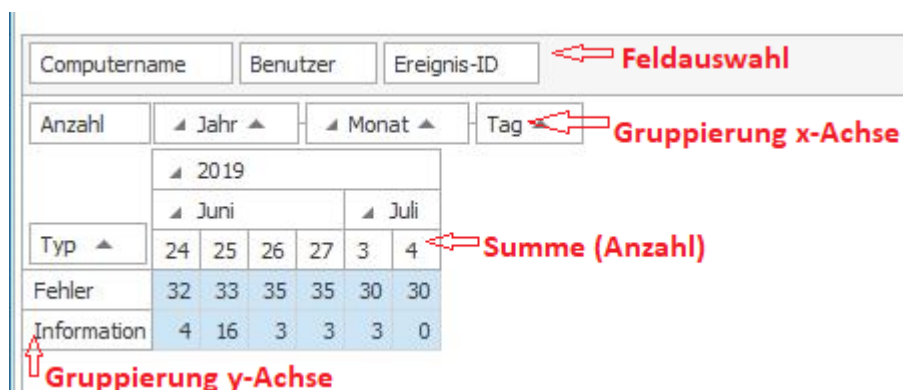
Wie Sie Statistikreporte an ihre Bedürfnisse anpassen, speichern, freigeben, ausdrucken, exportieren und automatisiert bereitstellen, ist im Kapitel [Arbeitsbereich](#) beschrieben. Im Folgenden werden nur die Besonderheiten erläutert.

Statistikreporte werden in der Regel nicht direkt aus den Ereignisdaten gefüllt, sondern erhalten ihre Werte aus Statistiktabellen, in denen die Ereignisdaten regelmäßig automatisiert für die Statistiken aufbereitet werden. Deshalb können Daten der letzten 24 Stunden nicht enthalten sein.

### 4.1 Statistikreporte erstellen

Um eigene statistische Auswertung zu erstellen, öffnen Sie eine passende vordefinierte Statistik. Statistikreporte werden als Pivot-Tabelle (unterer Bereich) und der dazu passenden grafischen Darstellung (oberer Bereich) angezeigt.

Die Pivot-Tabelle enthält die folgenden vier Bereiche:



Computername	Benutzer	Ereignis-ID	Feldauswahl					
Anzahl	Jahr	Monat	Tag	Gruppierung x-Achse				
Typ	2019		Summe (Anzahl)					
	Juni		Juli					
Fehler	24	25	26	27	3	4		
Information	32	33	35	35	30	30		
	4	16	3	3	3	0		

Gruppierung y-Achse

- Felddauswahl: Diese Felder können für die Gruppierung auf der X- oder Y-Achse verwendet werden.
- Gruppierung X-Achse: Die angegebenen Felder werden als Spalten gruppiert. In den vordefinierten Statistiken wird hier meistens die Zeit verwendet (Stunde, Tag, Monat, Jahr).
- Gruppierung Y-Achse: Die angegebenen Felder werden als Zeilen verwendet. Jede der vordefinierten Statistiken hat hier ein passendes Feld als Standardkriterium.
- Summe: Die einzelnen Zellen enthalten die aufsummierte Anzahl der jeweiligen Spalten und Zeilen.

### Spalten und Zeilen festlegen

Ziehen Sie ein oder mehrere Felder aus der Felddauswahl auf die X-Achse, Y-Achse oder zurück in die Felddauswahl. Eine Besonderheit stellt das Feld *Zeit* dar, welches selbst automatisch in unterschiedliche Zeitabschnitte unterteilt ist, die sich aber nicht getrennt voneinander als einzelne Felder verwenden lassen.

### Spalten und Zeilen gruppieren

Mehrere Felder in der X-Achse oder Y-Achse werden automatisch gruppiert. Ziehen Sie die Felder an eine andere Position, um die Gruppierung anzupassen. Klicken sie auf (v) oder (>) links vom Feldnamen, um Gruppen ein- oder auszublenden. Klicken Sie z.B. im Feld **Monat** auf dieses Symbol, werden die Daten nach Monaten zusammengefasst und die Untergruppen *Woche*, *Tag* und *Stunde* ausgeblendet.

### Sortieren und Filtern

Klicken Sie auf den Pfeil rechts vom Feldnamen, um die Sortierung umzukehren. Wenn Sie die Maus über einen Feldnamen bewegen, zeigt ein kleines Filtersymbol an, wenn Sie hier nach Werten filtern können. Klicken Sie auf das Filtersymbol und selektieren Sie die gewünschten Werte.

### Grafische Darstellung

Markieren Sie mit der Maus Zeilen, Spalten oder Summenfelder, um schnell nach Werten zu filtern. Die grafische Darstellung passt sich automatisch entsprechend an.

Diese Markierung wird nicht abgespeichert. Wenn Sie einen Statistik Reports wiederverwenden oder automatisiert versenden möchten, nutzen Sie Filter um den Wertebereich einzuschränken.

Wählen Sie im Menüband einen passenden Diagrammtyp aus. Insbesondere bei Tortendiagrammen müssen die Werte in Zeilen angeordnet sein. Mit **Tauschen** im Menüband können Sie Zeilen und Spalten vertauschen, um so zum gewünschten Ergebnis zu kommen.

# Teil V

## Ereignisreporte

## 5 Ereignisreporte

Das DriveLock Control Center stellt eine umfassende Berichtsumgebung zur Verfügung. Sie erlaubt es Administratoren, Aktivitäten und Trends zu verfolgen. Diese können ausgedruckt oder per E-Mail versendet werden, um die Details dieser Aktivitäten zu dokumentieren. Ereignisreporte sind Berichte, welche in tabellarischer Form bestimmte, ausgesuchte Ereignisse darstellen können. Sie beantworten grundsätzlich Fragestellungen, wie zum Beispiel:

- Welche Daten haben auf Wechseldatenträgern das Unternehmen verlassen?
- Welche Benutzer haben die Verwendungsrichtlinien wann akzeptiert bzw. abgelehnt?
- Welche USB-Sticks wurden wann wo gesperrt?

Wie Sie Ereignisreporte an ihre Bedürfnisse anpassen, speichern, freigeben, ausdrucken, exportieren, und automatisiert bereitstellen, ist in Kapitel [Arbeitsbereich](#) beschrieben.



# Teil VI

## Forensische Analysen



## 6 Forensische Analysen

Forensische Analysen sind ein mächtiges Werkzeug, um bei Sicherheitsvorfällen schnell die Ursache, den Urheber oder die Quelle zu ermitteln. Basis der Analyse sind die selben, vom DriveLock Agenten übermittelten Ereignisdaten, die auch in den Ereignisreporten tabellarisch dargestellt werden. Bei der forensischen Analyse geht man in diesen Daten, ausgehend von einem bekannten Vorfall, von Ereignis zu Ereignis, bis man dem Ursprung auf die Spur gekommen ist.

Zum Beispiel wollen Sie herausfinden, von welchem Benutzer ein gefundener USB-Stick angesteckt wurde und dann weiter untersuchen, an welchen anderen Computern dieser USB-Stick verwendet wurde und welche Dateien kopiert wurden. Oder Sie wollen herausfinden ob eine bestimmte Datei auf ein externes Laufwerk kopiert wurde, und von wem und wann.

Wie auch die Ereignisreporte können Sie forensische Analysen an ihre Bedürfnisse anpassen, ausdrucken und exportieren (siehe Kapitel [Arbeitsbereich](#)). Zusätzlich haben Sie Zugriff auf verschiedene Tools, die es Ihnen erlauben, Daten dynamisch zu filtern. Mit dem sog. Drill down können Sie weitere zusätzliche Informationen von bestimmten Ereignissen gewinnen.

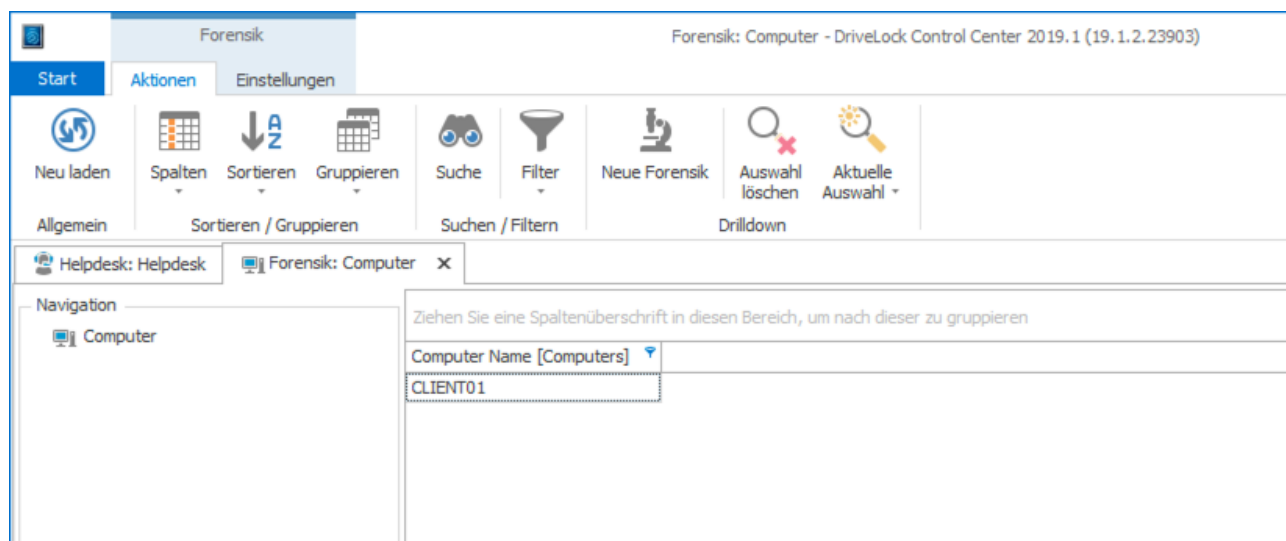
Im Gegensatz zu Ereignisreporten können forensische Analysen nicht gespeichert, veröffentlicht und automatisiert versendet werden, da zu einem späteren Zeitpunkt nicht die gleichen Ergebnisse geliefert werden können.

### 6.1 Forensische Analysen durchführen

#### Beispiel für eine einfache forensische Analyse

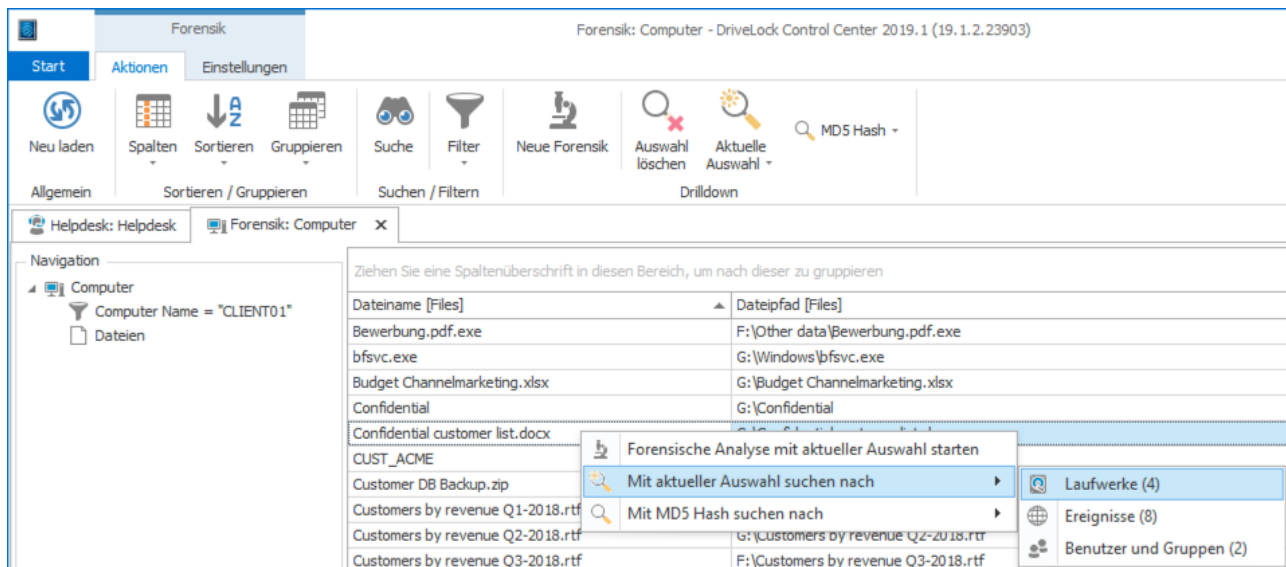
Sie haben den Verdacht, dass an Computer `Client01` sensible Informationen über USB-Sticks abgeflossen sind.

Direkt in der Forensik-Ansicht klicken Sie mit der rechten Maustaste in die Zeile mit dem Computer und wählen dann **Forensische Analyse mit der aktuellen Auswahl starten**. Im DCC Arbeitsbereich öffnet sich eine neue forensische Analyse.

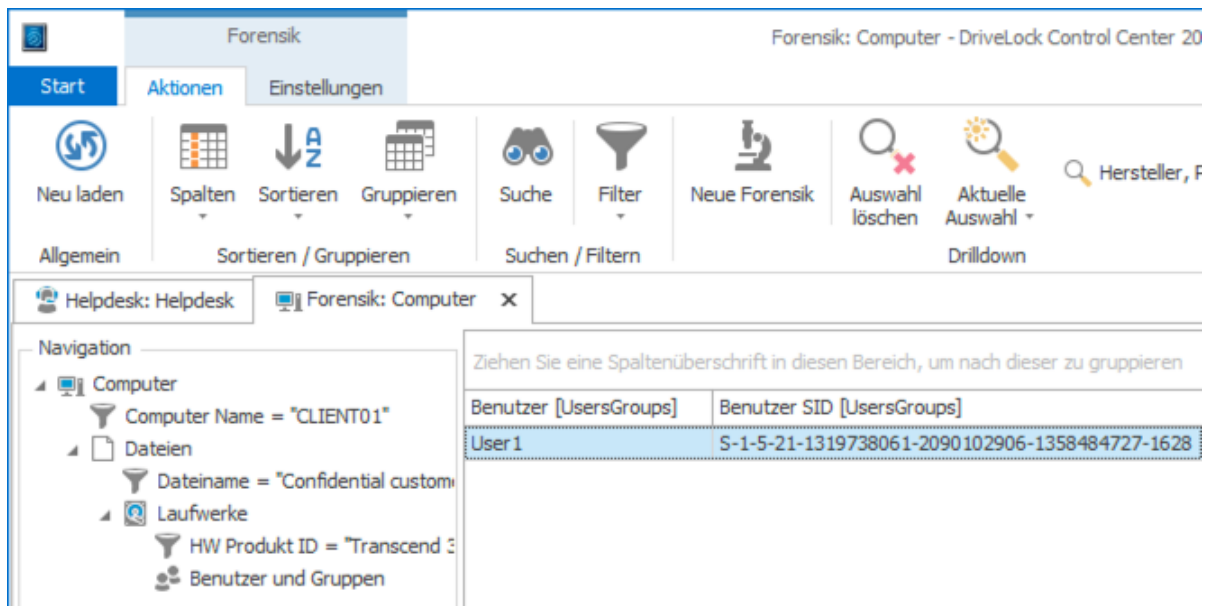


Als nächstes rechtsklicken Sie im Ergebnis auf `Client01` und wählen **Mit aktueller Ansicht suchen nach / Dateien**. Als Ergebnis sehen Sie alle Dateien, die von diesem Computer auf Wechseldatenträger geschrieben wurden.

Wiederholen Sie die Vorgehensweise für die entsprechende Datei – im Beispiel `Confidential customer list.docx`. Klicken Sie wieder rechts und wählen Sie dann **Mit aktueller Ansicht suchen nach / Laufwerke**. Sie sehen nun, dass die Datei auf ein externes Laufwerk kopiert wurde.



Weiter mit einem Rechtsklick auf die Datei - **Mit aktueller Ansicht suchen nach / Benutzer und Gruppen** erkennen Sie, dass `User1` die entsprechende Datei kopiert hat und können entsprechende Maßnahmen ergreifen.



### Forensische Analysen starten

Wie im Beispiel direkt aus dem Helpdesk können Sie forensische Analysen auch direkt aus einem Ereignisreport anstoßen.

Im Funktionsbereich **Forensik** selbst finden Sie eine Vielzahl von vorinstallierten forensischen Analysen und zwei spezielle Aktionen.

### Nach verbundenen Laufwerken filtern

Sie finden einen USB-Stick, z.B. in einem Meetingraum oder auf dem Parkplatz. Stecken Sie den USB-Stick an ihrem Administrationsrechner an und klicken auf **Nach verbundenen Laufwerken filtern**. Nun können Sie eine Analyse starten und untersuchen, ob dieser Stick an Computern in ihrem Unternehmen von welchen Anwendern benutzt wurde.

### Nach ausgewählter Datei filtern

Starten Sie eine Analyse, öffnen die Datei und suchen mit Rechtsklick - **Mit MD5 Hash suchen nach / Ereignisse** nach allen Ereignissen die genau zu dieser Datei protokolliert wurden.

Wenn anonyme Ereignisreporte eingeschaltet sind, lässt sich ein direkter Bezug zwischen Ereignissen und einer bestimmten Person nicht herstellen (siehe [Anonyme Daten](#)).



# Teil VII

## Inventar

## 7 Inventar

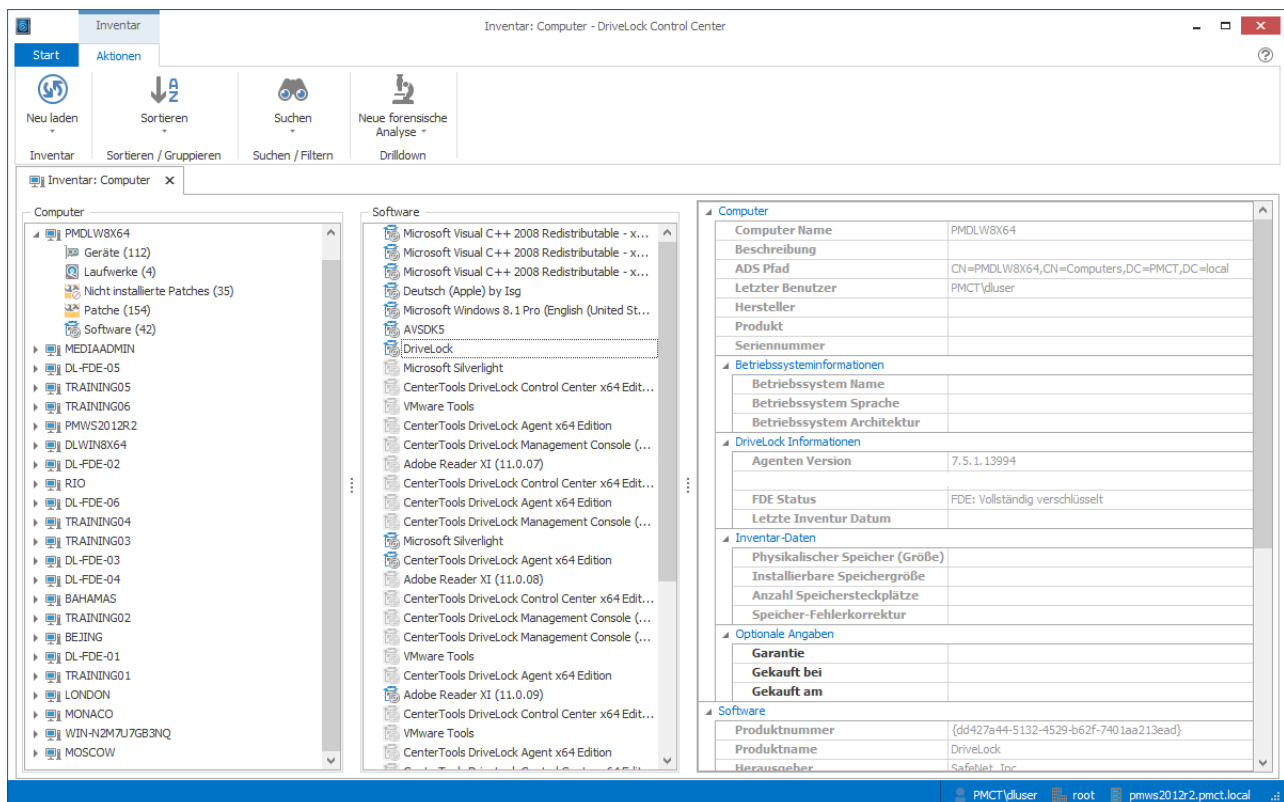
Durch die integrierte Inventarisierung kann neben der Hardware auch der komplette Bestand an Software inventarisiert und geprüft werden. So ist es möglich, die tatsächliche Zahl von benötigten Software-Lizenzen zu erheben und ggf. die Lizenzzahlungen zu korrigieren. Neben diesem nicht unerheblichen finanziellen Einsparungsaspekt für das Unternehmen, erhöht das auch die Sicherheit, sich rechtlich nicht mehr in Grauzonen zu bewegen und belegbare Zahlen über die benützte Software zu haben.

Diese Funktion steht in allen Produkten, die die Applikationskontrolle beinhalten, zur Verfügung.

Damit der DriveLock-Agent die entsprechenden Inhalte für das Inventar sammelt, muss dies in der DriveLock Richtlinie aktiviert werden. Weitere Informationen hierzu finden Sie im DriveLock Administrationshandbuch im Kapitel Hard- und Softwareinventarisierung.

### 7.1 Inventar anzeigen

Öffnen Sie den Funktionsbereich Inventar. Im Arbeitsbereich werden alle verfügbaren Entitäten angezeigt mit denen Sie eine Analyse starten können. Klicken Sie z.B. auf **Computer**, doppelklicken Sie einen angezeigten Eintrag (hier: *PMDLW8X64*) und wählen Sie **Software** als untergeordnete Entität aus.



Die Inventar-Ansicht ist in drei Bereiche unterteilt:

- **Links:** Ausgangs-Entität, die Sie beim Aufruf des Inventars gewählt haben (hier: Computer)
- **Mitte:** Untergeordnete Entität, in dem die in der linken Seite ausgewählten Entitäten angezeigt werden (hier: Software)  
Aktuell vorhandene Einträge erkennt man am kontrastreichen Icon.

- *Rechts*: Detail-Bereich, der zusätzliche Informationen zu den ausgewählten Elementen enthält.

## 7.2 Garantie- und Wartungslaufzeit eingeben

Zu den beiden Entitäten *Computer* und *Software* können Sie zusätzliche Informationen eingeben.

- Computer: Garantie, Gekauft bei, Gekauft am
- Software: Lizenzschlüssel, Lizenzanzahl, Ablaufdatum

Wenn Sie in den Feldern Garantie und Ablaufdatum ein Datum eintragen, kann DriveLock Sie automatisch per Email benachrichtigen, bevor dieses Datum erreicht wird. Aktivieren Sie die E-Mail-Benachrichtigung auf der DCC Startseite unter **Einstellungen / Inventarbenachrichtigung einstellen...**

Damit Benachrichtigungen verschickt werden können, muss am DriveLock Enterprise Service ein SMTP-Server eingestellt werden. Weitere Informationen hierzu finden Sie im DriveLock Administrationshandbuch.

# Teil VIII

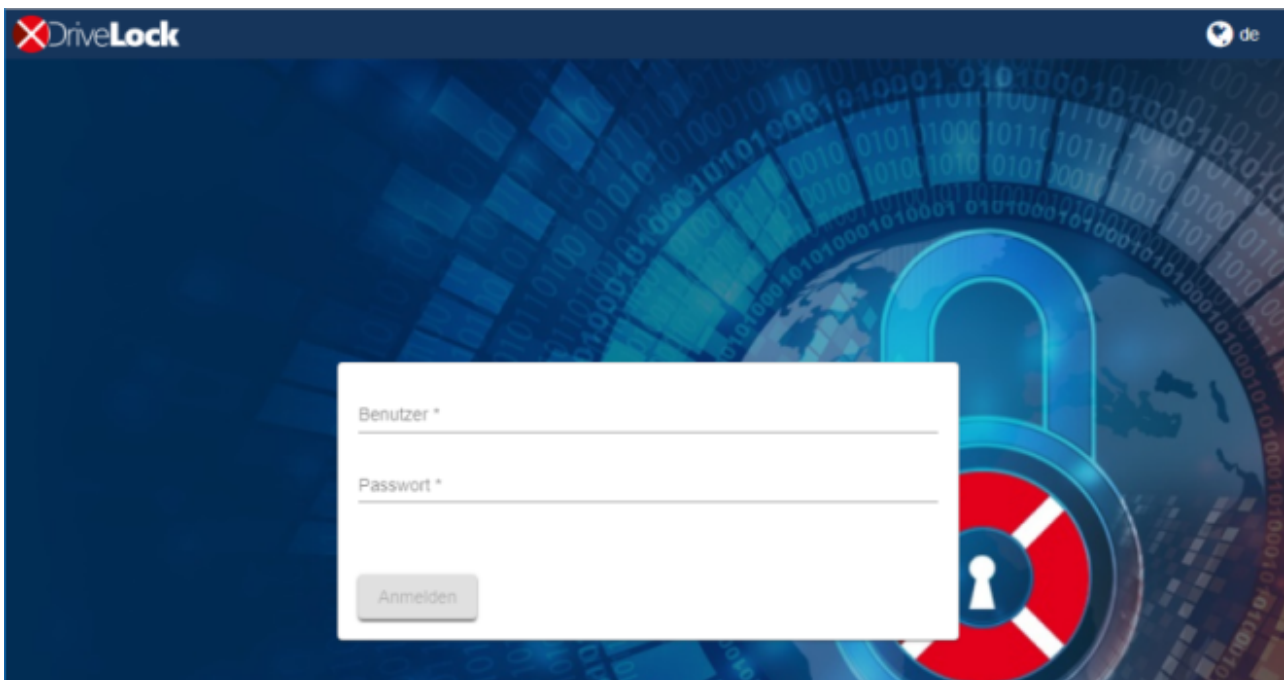
## DOC öffnen

## 8 DOC öffnen

Informationen zum **DriveLock Operations Center (DOC)** finden Sie in der entsprechenden Dokumentation auf [DriveLock Online Help](#)

### 8.1 Anmeldung am DOC

Klicken Sie im DCC Menü auf **DOC öffnen**, um zu folgender Anmeldemaske zu gelangen:



Beachten Sie bitte folgendes:

- Es können sich nur AD-Benutzer anmelden.
- Da SSL-Zertifikate verwendet werden, kann es unter Umständen zu Warnungen kommen. Lesen Sie den entsprechenden Hinweis.
- Sie können bereits an dieser Stelle die Sprache ein- bzw. umstellen.
- Jeder DriveLock Benutzer, der volle Helpdesk-Berechtigungen hat, kann sich mit seinem jeweiligen Kennwort anmelden.
- Der erste gültige angemeldete Benutzer wird Administrator im DOC, alle folgenden werden Benutzer. Der Administrator kann einen Benutzer aber später auch zum Administrator hochstufen.

#### 8.1.1 Hinweise zur Verwendung von Zertifikaten

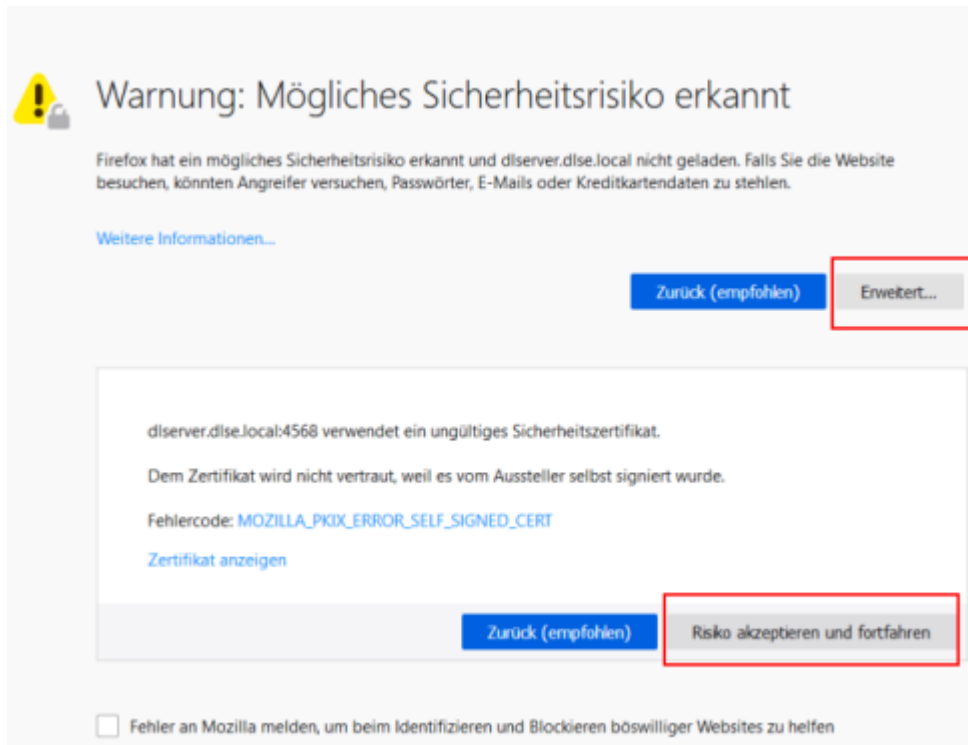
DriveLock verwendet für die Kommunikation mit dem DriveLock Operations Center (DOC) SSL-Zertifikate. Sie können diese bereits bei der Installation des DriveLock Enterprise Service (DES) angeben oder alternativ ein selbstsigniertes Zertifikat erstellen. Mehr Informationen zum Thema Zertifikate finden Sie im Installations- und Administrationshandbuch auf [Drivelock Online Help](#).

Wir empfehlen, sich ein Zertifikat für den DES von einer anerkannten Zertifizierungsstelle (CA) erstellen lassen!

Falls Sie ein selbstsigniertes Zertifikat verwenden, erscheinen beim Öffnen des DOC je nach Browser unterschiedliche Warnungen, weil das Zertifikat aus Sicht des Browsers nicht vertrauenswürdig ist.

In den Beispielen unten lautet der Name des DES **dlserver.dlse.local**.

**Wenn Sie Mozilla Firefox verwenden, gilt folgendes:**

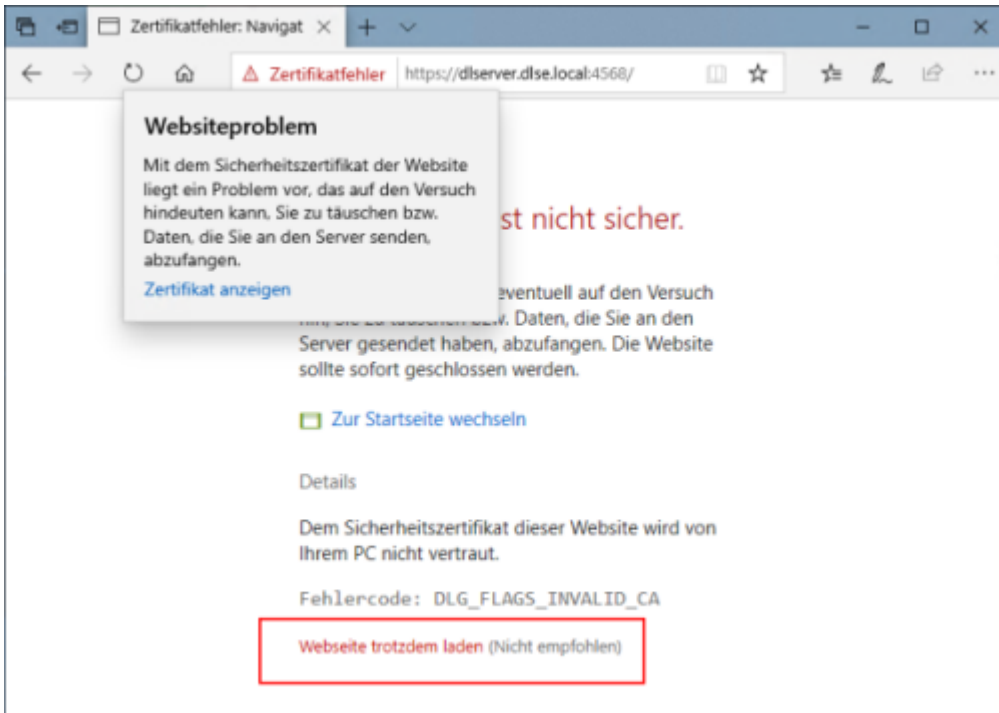


Klicken Sie auf **Risiko akzeptieren und fortfahren**, um das Zertifikat zu akzeptieren. Sie müssen sich weder die Zertifikatsdetails anzeigen lassen, noch das Zertifikat importieren. Firefox fügt nur eine Sicherheitsausnahme für diese Webseite hinzu. Weitere Schritte sind nicht notwendig.

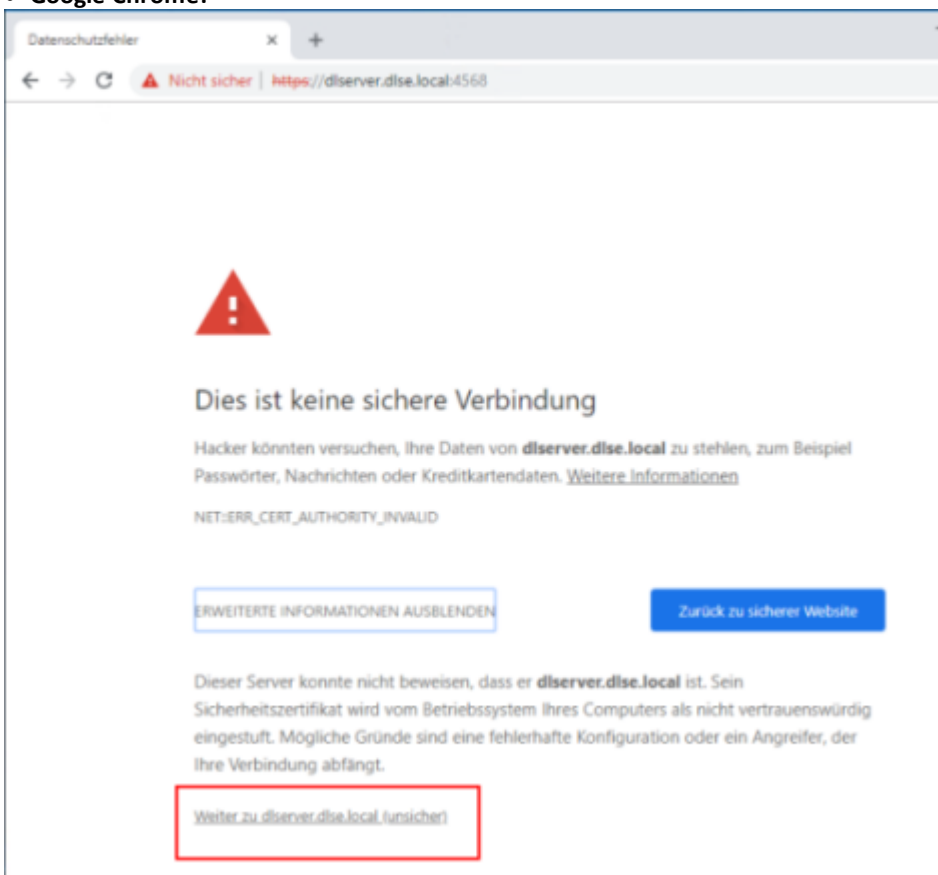
**Für Google Chrome und Microsoft Edge gilt folgendes:**

Bei beiden Browsern sollten Sie das Zertifikat in den Zertifikatsspeicher eintragen, damit Sie nicht bei jedem Start des DOC eine Warnung erhalten.

- **Microsoft Edge:**



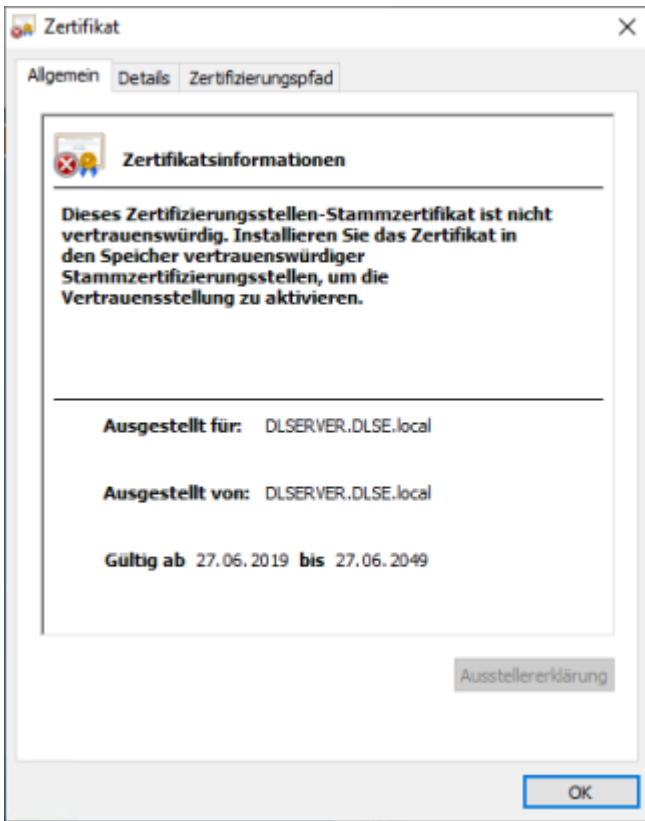
• Google Chrome:



**Vorgehensweise:**

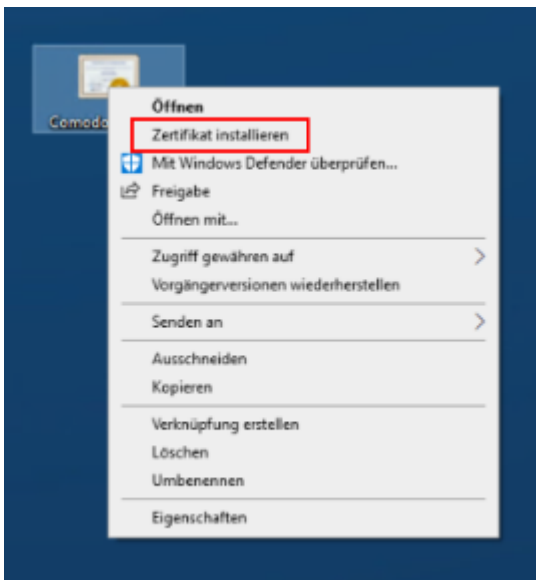
1. Akzeptieren Sie bei beiden Browsern die Warnung und öffnen Sie das Zertifikat.

2. Sie können sich die Details des Zertifikats ansehen und das Zertifikat mithilfe des **Zertifikatimport-Assistenten** in den lokalen Zertifikatsspeicher importieren.



3. Speichern Sie das Zertifikat in einem Verzeichnis Ihrer Wahl.

4. Öffnen Sie das Kontextmenü des Zertifikats und klicken Sie auf **Zertifikat installieren**.

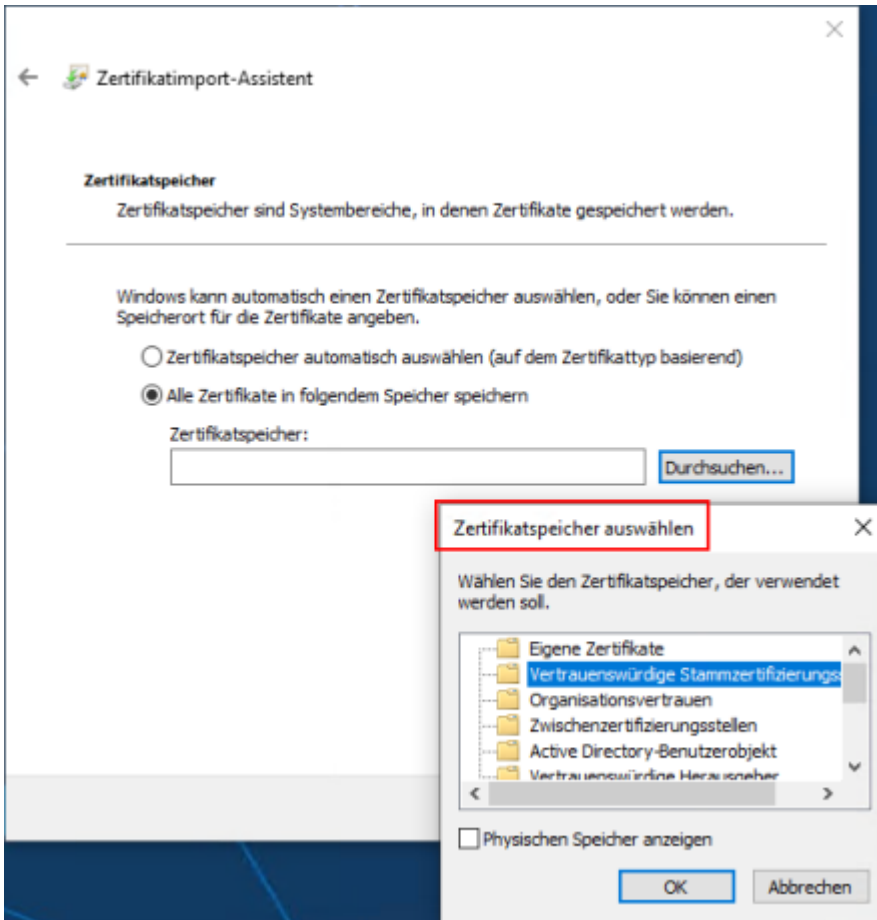


5. Der **Zertifikatimport-Assistent** öffnet sich. Lassen Sie auf der ersten Seite die Voreinstellung X.509.

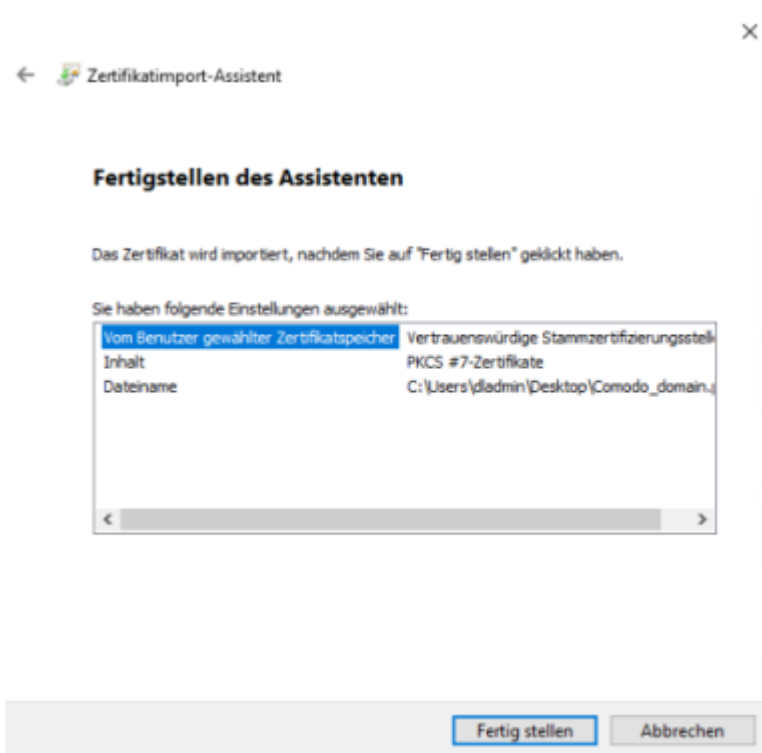
6. Wählen Sie auf der nächsten Seite die Option **Lokaler Computer** aus.

7. Auf der dritten Seite wählen Sie als **Zertifikatsspeicher** die Option **Vertrauenswürdige Stammzertifizierungsstelle**:



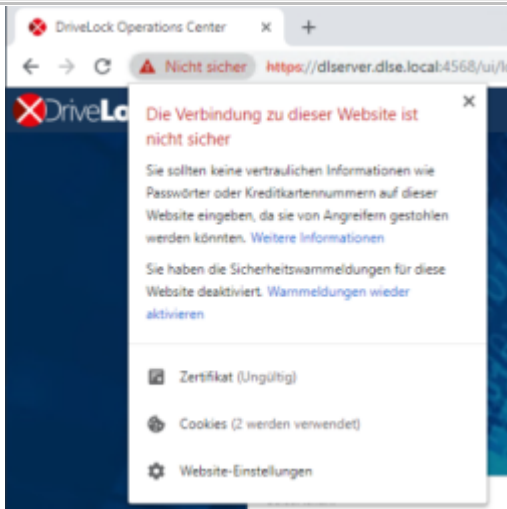


8. Klicken Sie **Fertigstellen** im nächsten Dialog.



9. Das Zertifikat ist nun eingetragen und beim nächsten Öffnen der DOC gelangen Sie ohne Fehlermeldung direkt zur DOC Anmeldemaske.

Beachten Sie allerdings, dass auch dann das Zertifikat vom Browser als nicht sicher angesehen wird und weiterhin folgende Warnung erscheint (im Beispiel unten Google Chrome):



## 8.2 Überblick über das DOC

Sobald Sie sich angemeldet haben, öffnet sich als erstes das DOC Standard-Dashboard.

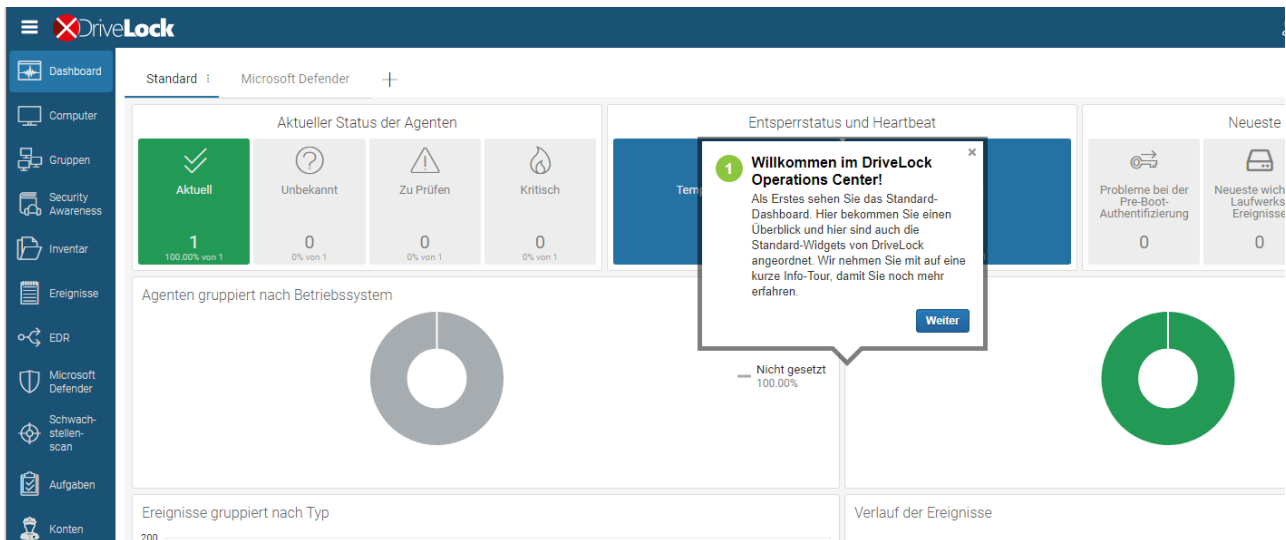
### 8.2.1 DOC Dashboard

Das Standard-Dashboard bietet Ihnen eine generelle Übersicht über die DriveLock Agenten-Computer in Ihrem Netzwerk. Neue Dashboards lassen sich jederzeit durch Klicken auf das + Symbol hinzufügen.

Folgen Sie hier als erstes der DOC-Tour, in der Sie einen Überblick über die Arbeit mit dem Dashboard bekommen.

Um sich die Inhalte der vorhandenen DOC-Touren erneut anzusehen, gehen Sie folgendermaßen vor:

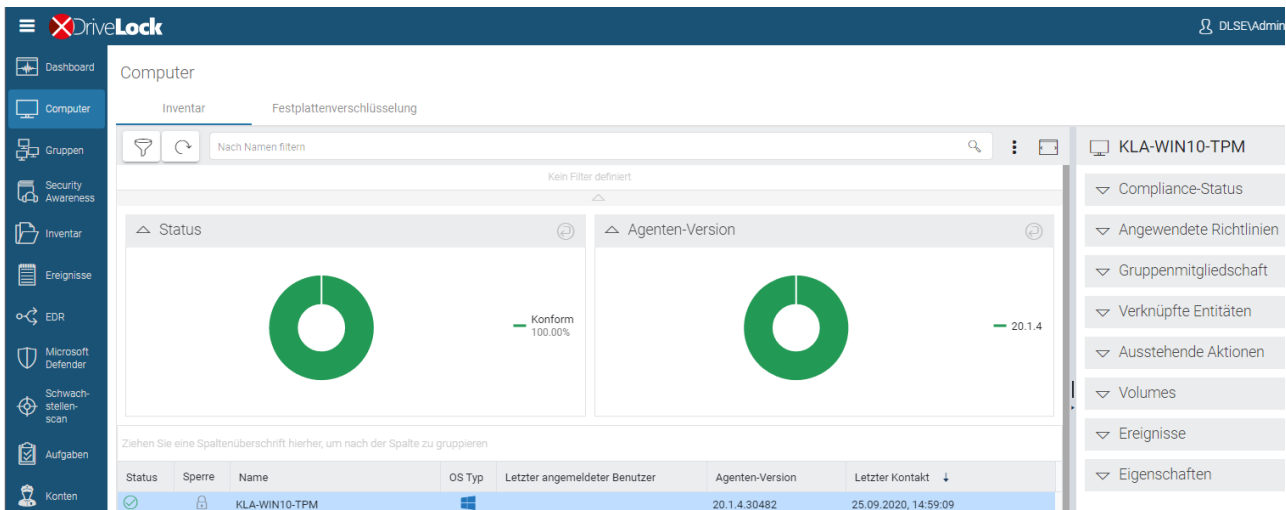
1. Öffnen Sie **Kontodaten bearbeiten** unter **Mein Konto**.
2. Klicken Sie **DOC-Tour neu starten**.
3. Beim Öffnen des entsprechenden Dashboards fängt die entsprechende Tour wieder von vorne an.
4. So können Sie die verschiedenen Touren beliebig oft neu starten.



- Jeder Benutzer kann sich sein eigenes Dashboard anlegen und sich die Widgets passend arrangieren.
- Es können beliebig viele Dashboards angelegt und angepasst werden.
- Für Application Control, Microsoft Defender, BitLocker Management, Security Awareness, Festplattenverschlüsselung oder Schwachstellen-scan (sofern lizenziert) gibt es vordefinierte Dashboards.
- Widgets werden einfach angeklickt, um zur entsprechenden Ansicht zu gelangen.

## 8.2.2 Computer

Die Computer-Ansicht bietet eine Übersicht aller Agenten-Computer. So sehen Sie beispielsweise, welche Agenten-Version auf dem jeweiligen Computer installiert ist oder wann der Computer zuletzt mit dem DES Kontakt hatte.

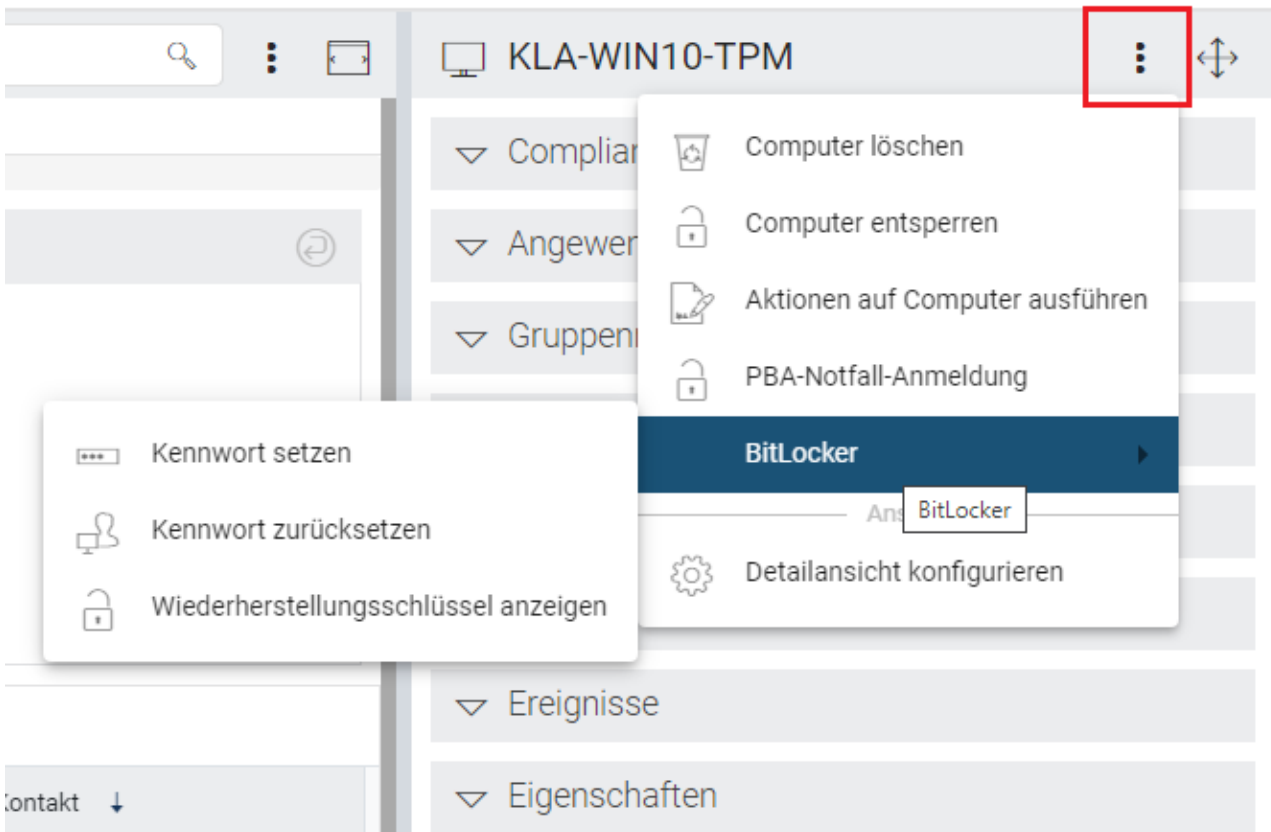


**Auch hier lässt sich die Anzeige individualisieren:**

- Nach **Spalten sortieren**: ein Klick auf den Spaltenkopf sortiert aufsteigend, ein zweiter absteigend und der letzte entfernt die Sortierung.

- **Neue Spalten** hinzufügen: Fügen Sie aus einer Auswahl von verschiedenen Spalten diejenigen hinzu, die für Sie besonders wichtig sind. Wenn Sie beispielsweise mit DriveLock BitLocker Management arbeiten, können Sie sich den Verschlüsselungsstatus der Agenten anzeigen lassen und entsprechend die Verschlüsselung steuern.
- **Filter setzen**: Filtern Sie nach Eigenschaften des Objekts. Sie können dabei Bedingungen mit und/oder verknüpfen und beliebig schachteln.
- Die Anzeige lässt sich in eine Excel-Tabelle zur weiteren Verwendung **exportieren**.
- **Benutzerdefinierte Widgets** lassen sich hier auch erstellen und auf jedem Ihrer Dashboards ablegen.

#### Bearbeitung der einzelnen Computer:

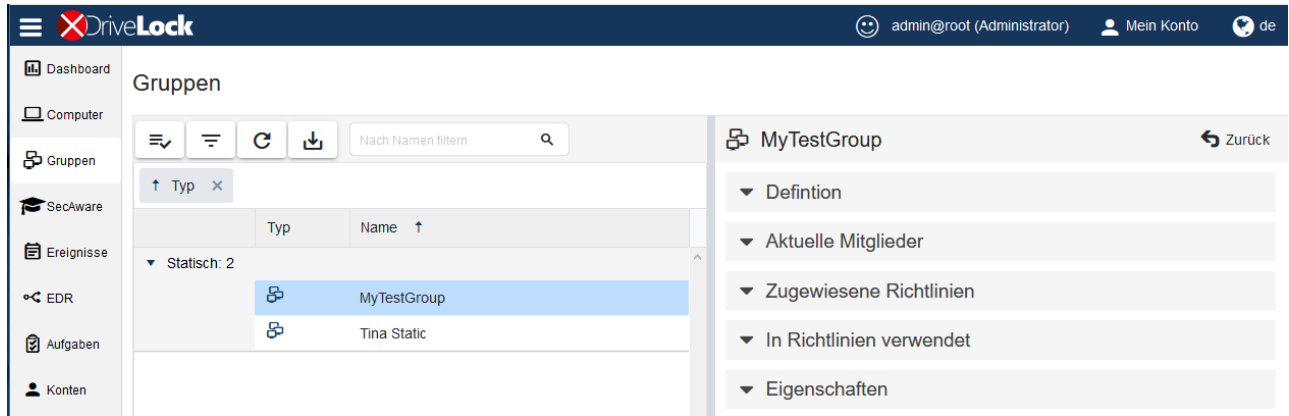


- **Computer löschen**: Wenn Sie einen Computer löschen wollen, müssen Sie bedenken, dass dieser endgültig gelöscht wird.
- **Computer entsperren**: Um diese Aktion durchzuführen, benötigen Sie das Kennwort, das in der entsprechenden Richtlinie angegeben ist.
- **Aktionen auf Computer ausführen**: Hier lassen sich einzelne Aktionen auswählen, die dann unter **Ausstehende Aktionen** in der Computer-Ansicht angezeigt werden.
- **PBA-Notfall-Anmeldung**: Verwenden Sie diesen Befehl, um die PBA-Notfall-Anmeldedaten auszulesen und einem Benutzer beim Anmelden zu helfen.
- Im Bereich BitLocker können Sie für den gewählten Computer ein neues BitLocker-**Kennwort setzen** oder eines zurücksetzen, sowie einen BitLocker-Wiederherstellungsschlüssel anfordern.

In der BitLocker-Dokumentation unter [DriveLock Online Help](#) finden Sie weitere Informationen zum Thema DriveLock BitLocker Management / Pre-Boot-Authentifizierung.

### 8.2.3 Gruppen

Die Gruppen-Ansicht gibt Ihnen einen Überblick über die Gruppenzugehörigkeit Ihrer DriveLock Agenten. Weitere Information zu DriveLock-Gruppen erhalten Sie im Administrationshandbuch auf [DriveLock OnlineHelp](#).



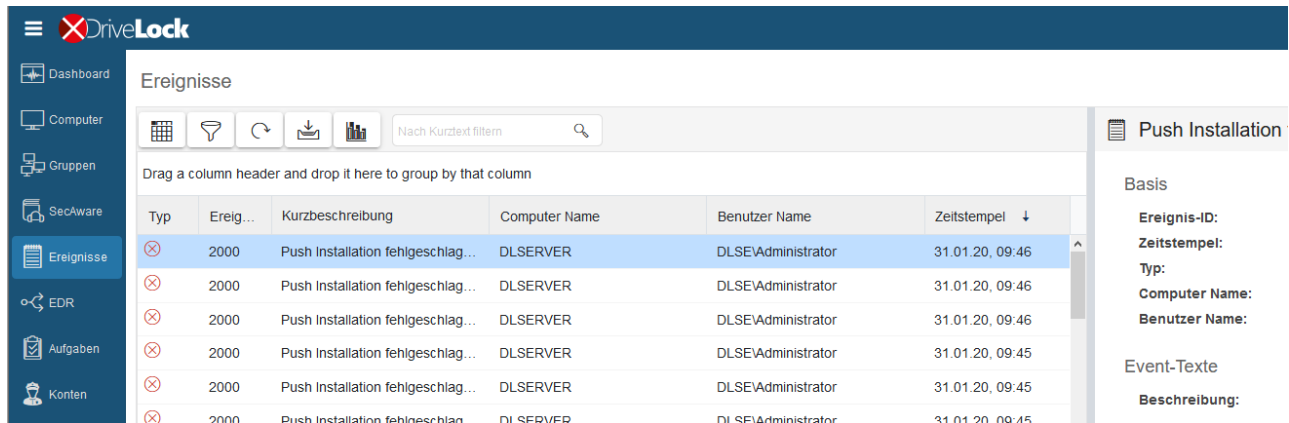
### 8.2.4 SecAware

Zur SecAware-Ansicht und dem Security-Awareness-Dashboard finden Sie weiterführende Informationen in der Security-Awareness-Dokumentation auf [DriveLock OnlineHelp](#).

### 8.2.5 Ereignisse

Wie im Ereignisreport des DCC sind hier die Ereignisse auf den jeweiligen Agenten-Computern nach Typ (Warnung, Fehler, Information), Ereignis-ID, Beschreibung und weiteren Kriterien aufgelistet.

Sie haben auch hier die Möglichkeit, diese Ansicht zu individualisieren, indem Sie Spalten sortieren und hinzufügen, Filter setzen usw.



### 8.2.6 EDR

Die Ansicht EDR (Event Detection & Response) bietet eine optimierte Darstellung der einzelnen Ereignisse verbunden mit verschiedenen Konfigurationsmöglichkeiten. Mit den EDR-Funktionalitäten lassen sich beispielsweise Regeln erstellen, mit denen die Reaktion auf das Eintreten eines Ereignisses definiert wird. Mithilfe von konfigurierbaren Responses (z.B. Reaktion durch Ausführung eines Skripts) kann so auf Alerts (Sicherheitswarnungen) schnell reagiert werden.

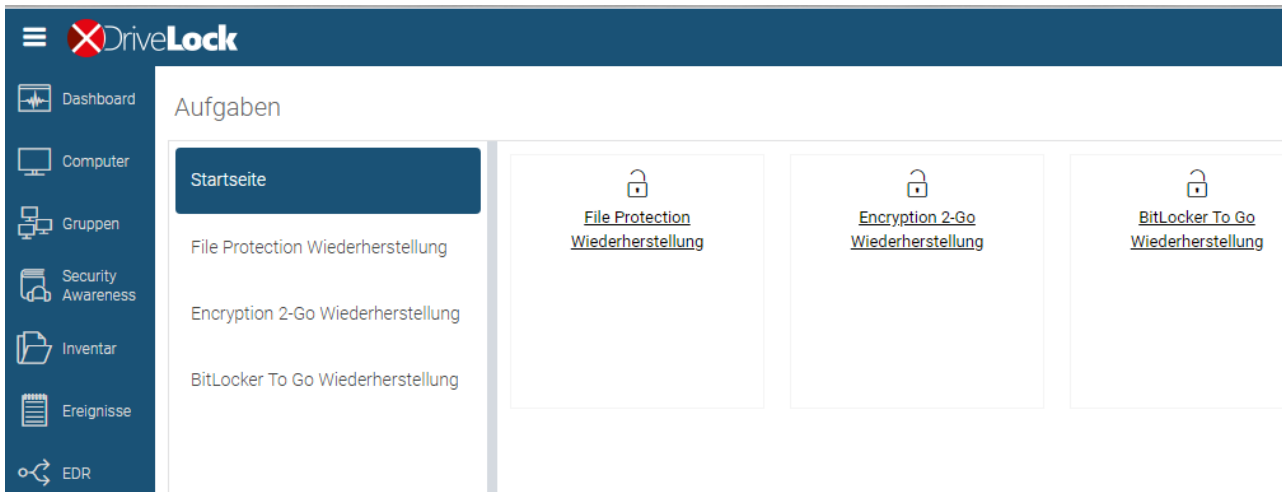
Das DOC zeigt Alerts nach Schweregrad und Kategorie an und gibt einen Überblick über die betroffenen Computer und Benutzer.

## 8.2.7 Microsoft Defender

Zur Microsoft Defender-Ansicht finden Sie weiterführende Informationen in der Defender Integration-Dokumentation auf [DriveLock OnlineHelp](#).

## 8.2.8 Aufgaben

In der Aufgaben-Ansicht gibt es drei Bereiche.



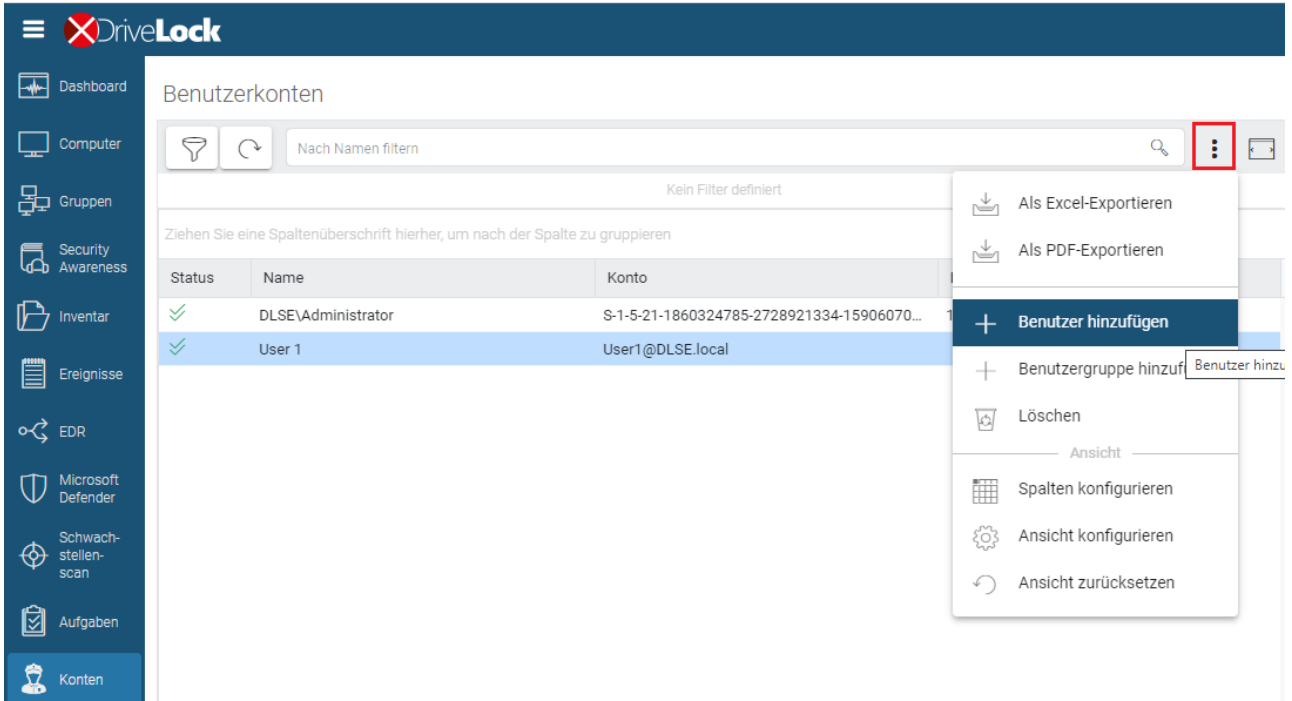
Weiterführende Informationen zu den jeweiligen Themen finden Sie in den entsprechenden Kapiteln des DriveLock Administrationshandbuchs auf [DriveLock Online Help](#).

- File Protection Wiederherstellung
- Encryption 2-Go Wiederherstellung
- BitLocker To Go Wiederherstellung: Weitere Informationen zu diesem Bereich erhalten Sie in der BitLocker Management Dokumentation ebenfalls auf [DriveLock Online Help](#).

## 8.2.9 Konten

In der Konten-Ansicht sehen Sie eine Auflistung aller Benutzerkonten des DriveLock Operation Centers mit Namen, Status und letzter Anmeldung. Wie in den anderen Ansichten auch, können Sie hier Spalten sortieren, neue Spalten hinzufügen, Filter setzen und die Ansicht in Excel exportieren.

**Wenn Sie die Rolle des Administrators haben, können Sie in dieser Ansicht neue Benutzerkonten hinzufügen, löschen oder die Rolle eines Benutzers ändern.**



Benutzerkonten

Nach Namen filtern


Kein Filter definiert

Ziehen Sie eine Spaltenüberschrift hierher, um nach der Spalte zu gruppieren

Status	Name	Konto
✓	DLSE\Administrator	S-1-5-21-1860324785-2728921334-15906070...
✓	User 1	User1@DLSE.local

- Als Excel-Exportieren
- Als PDF-Exportieren
- + Benutzer hinzufügen**
- + Benutzergruppe hinzufügen
- Löschen
- Ansicht
- Spalten konfigurieren
- Ansicht konfigurieren
- Ansicht zurücksetzen

### So fügen Sie einen neuen Benutzer hinzu:

1. Klicken Sie auf das Symbol  und wählen dann den Menübefehl **Benutzer hinzufügen**.
2. Geben Sie den Namen des neuen Benutzers an und lassen Sie die Option **Rollenzuweisung für neuen AD-Benutzer anlegen** ausgewählt.



Active Directory-Benutzer hinzufügen

Active Directory-Benutzer suchen. Verwenden Sie die Schreibweise domäne\benutzer um eine Domäne anzugeben.

User2@DLSE.local

Rollenzuweisung für neuen AD-Benutzer anlegen

Ausgewählten Benutzer hinzufügen

3. Wählen Sie im nächsten Schritt die Rollen für den Benutzer aus.

Rollenzuweisung erstellen oder hinzufügen ✕

---

**1** Wählen Sie eine Rolle aus
**2** Wählen Sie einen Kontext aus

Name
Threat Hunter
Administrator
Helpdesk
Supervisor
Encryption Officer
Security Awareness Coordinator

⏪ ⏩ 1 ⏪ ⏩

1 - 6 von 6 Elementen

4. Speichern Sie den neuen Benutzer.

**So bearbeiten Sie die Benutzerrolle:**

1. Klicken Sie auf **Rollenzuweisung erstellen oder hinzufügen**:

Ziehen Sie eine Spaltenüberschrift hierher, um nach der Spalte zu gruppieren

Status	Name	Konto	Letzte Anmeldung ↓
✔	DLSE\Administrator	S-1-5-21-1860324785-2728921334-15906070...	15.09.2020, 11:34:37
✔	User 2	User2@DLSE.local	
✔	User 1	User1@DLSE.local	

Info

Benutzer: User 2

Letzte Anmeldung:

Rollenzuweisungen

Rollenzuweisung erstellen oder hinzufügen

2. Wählen Sie die gewünschte Benutzerrolle aus.

**Hinweis zum Löschen: Sie können niemals Ihr eigenes Benutzerkonto löschen!**





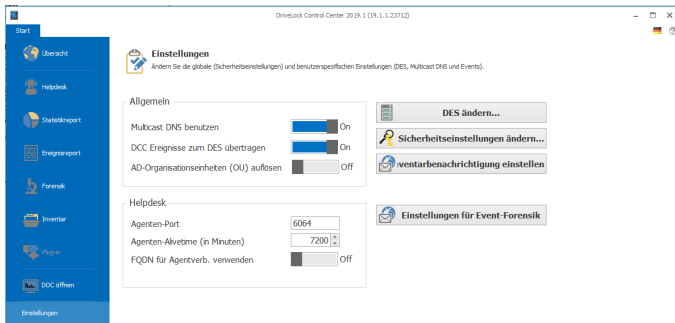
# Teil IX

## Einstellungen



## 9 Einstellungen

Hier ändern Sie die globalen Sicherheitseinstellungen und benutzerspezifischen Einstellungen des DriveLock Control Centers.



### Mandant

Die Auswahl wird nur angeboten, wenn in ihrer Umgebung zusätzliche Mandanten (z.B. unterschiedliche Zweigstellen oder verschiedene Kunden (Security as a Service)) angelegt sind und der angemeldete Benutzer Berechtigungen für mehrere Mandanten hat. Die Auswahl eines anderen Mandanten wirkt sich auf alle im DCC angezeigten Daten aus. Eine mandanten-übergreifende Anzeige ist aus Datenschutzgründen nicht möglich.

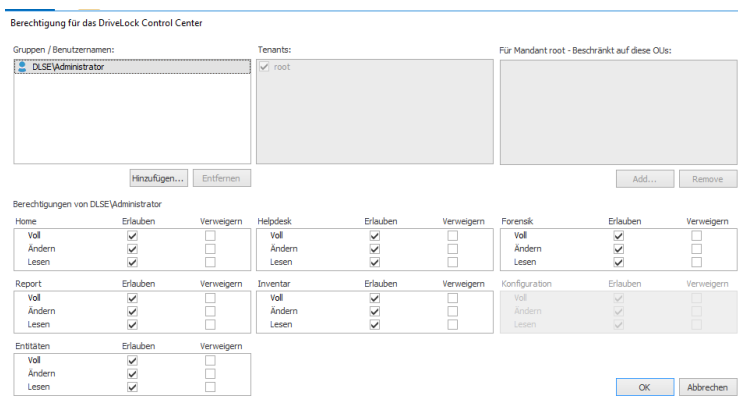
### Serververbindung

Beim ersten Start des DriveLock Control Centers werden sie nach dem Namen und Port des *DriveLock Enterprise Servers (DES)* gefragt. Um sich mit einem anderen DES zu verbinden, klicken Sie **DES ändern...** und geben Namen und Port ein. Der Standard-Port für die Verbindung lautet 6067.

### Berechtigungen

Für die Funktionsbereiche im DCC können Sie getrennt Berechtigungen vergeben. So können Sie sicherstellen, dass z.B. ein Helpdesk-Mitarbeiter nur Zugriff auf die Helpdesk-Aufgaben hat und keine Reports oder forensischen Analysen öffnen darf.

Öffnen Sie **Sicherheitseinstellungen ändern...**



Klicken Sie auf **Hinzufügen** oder **Entfernen**, um die Benutzer und Gruppen zu ändern, die Berechtigungen haben sollen und **Erlauben** oder **Verweigern** Sie die Nutzung der Funktionsbereiche.

- **Voll:** Kann die Funktion sehen und verwenden, Änderungen vornehmen und Berechtigungen darauf ändern
- **Ändern:** Kann die Funktion sehen und verwenden und Änderungen (z.B. bei Reports) vornehmen
- **Lesen:** Kann den Bereich sehen und verwenden, aber keine Änderungen vornehmen

Wenn Ihre DriveLock Datenbank mehrere Mandanten enthält (z.B. unterschiedliche Zweigstellen oder verschiedene Kunden (Security as a Service), können Sie zusätzlich die Berechtigungen für den Zugriff auf die Daten dieser Mandanten festlegen.

#### Multicast DNS benutzen

Wenn Multicast DNS (auch DNS-SD) eingeschaltet ist, kann das DCC automatisch alle verfügbaren DriveLock Enterprise Server als Auswahl im Verbindungsdiallog anbieten. In den Helpdesk Ansichten zeigt es auch Computer mit DriveLock Agenten an, die dem verbundenen DES nicht bekannt sind. Wenn man das nicht möchte, z.B. in Umgebungen für Test- und Trainingszwecke mit mehr als einem DES im selben Netz, schaltet man Multicast DNS ab.

#### DCC Ereignisse zum DES übertragen

In der Voreinstellung werden DCC Ereignisse zum DriveLock Enterprise Server übertragen und können in den Ereignisreporten (z.B. Administrationsereignisse) ausgewertet werden. Nutzer mit vollen Rechten für den Bereich Konfiguration können diese Einstellung ändern.

#### Agenten-Port

Hier stellen Sie den Port ein, den Sie in der Richtlinie (*Globale Einstellungen / Einstellungen / Agentenfernkontroll-Einstellungen*), für die Agentenfernkontrolle konfiguriert haben. Voreinstellung ist HTTP **6064**. Wenn sie am Agenten verschlüsselte Kommunikation verwenden/erzwingen, können/müssen Sie hier entsprechend HTTPS **6065** eingeben.

#### Agenten-Alivetime

Nach der hier eingestellten Zeit nimmt das DCC an, dass ein Agent nicht online ist und zeigt im Helpdesk als Status *Nicht erreichbar*.

#### Inventarbenachrichtigung einstellen

Um die Inventarbenachrichtigung zu konfigurieren, öffnen Sie diesen Dialog, wählen die gewünschten Optionen und fügen Empfänger hinzu (siehe auch [Garantie- und Wartungslaufzeit eingeben](#)).

#### Einstellen der Sprache

Als Anzeigesprache wird die in Windows eingestellte Sprache übernommen, sofern verfügbar, ansonsten Englisch. Derzeit stehen die Sprachen Deutsch und Englisch zur Verfügung.

## DriveLock Control Center Benutzerhandbuch

Die in diesen Unterlagen enthaltenen Angaben und Daten, einschließlich URLs und anderen Verweisen auf Internetwebsites, können ohne vorherige Ankündigung geändert werden. Die in den Beispielen verwendeten Firmen, Organisationen, Produkte, Personen und Ereignisse sind frei erfunden. Jede Ähnlichkeit mit bestehenden Firmen, Organisationen, Produkten, Personen oder Ereignissen ist rein zufällig. Die Verantwortung für die Beachtung aller geltenden Urheberrechte liegt allein beim Benutzer. Unabhängig von der Anwendbarkeit der entsprechenden Urheberrechtsgesetze darf ohne ausdrückliche schriftliche Erlaubnis der DriveLock SE kein Teil dieser Unterlagen für irgendwelche Zwecke vervielfältigt oder übertragen werden, unabhängig davon, auf welche Art und Weise oder mit welchen Mitteln, elektronisch oder mechanisch, dies geschieht. Es ist möglich, dass DriveLock SE Rechte an Patenten bzw. angemeldeten Patenten, an Marken, Urheberrechten oder sonstigem geistigen Eigentum besitzt, die sich auf den fachlichen Inhalt dieses Dokuments beziehen. Das Bereitstellen dieses Dokuments gibt Ihnen jedoch keinen Anspruch auf diese Patente, Marken, Urheberrechte oder auf sonstiges geistiges Eigentum, es sei denn, dies wird ausdrücklich in den schriftlichen Lizenzverträgen von DriveLock SE eingeräumt. Weitere in diesem Dokument aufgeführte tatsächliche Produkt- und Firmennamen können geschützte Marken ihrer jeweiligen Inhaber sein.

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

DriveLock and others are either registered trademarks or trademarks of DriveLock SE or its subsidiaries in the United States and/or other countries.

The names of actual companies and products mentioned herein may be the trademarks of their respective owners.