

DriveLock Vulnerability Scanner

Dokumentation 2021.2

DriveLock SE 2021



Inhaltsverzeichnis

1 DRIVELOCK SCHWACHSTELLENSCAN	3
1.1 Voraussetzungen	3
1.2 Konfiguration in der DriveLock Management Konsole	3
1.2.1 Schwachstellenkataloge	3
1.2.1.1 Aktualisieren der Schwachstellenkataloge	4
1.2.2 Schwachstellenscan einrichten	4
1.3 Aktionen auf dem DriveLock Agenten	5
1.3.1 Schwachstellenscan auf dem DriveLock Agenten	5
1.3.1.1 Schwachstellenscan über die Agenten-Fernkontrolle starten	6
1.3.1.2 Schwachstellenscan über die Kommandozeile starten	7
1.4 DriveLock Operations Center (DOC)	7
1.4.1 Schwachstellenscan im DOC	7
1.4.1.1 Ansicht	7
2 INVENTARISIERUNG	9
2.1 Hardware- und Softwareinventarisierung	9
2.2 Client Compliance	10
2.2.1 Client-Compliance-Einstellungen	10
COPYRIGHT	12

1 DriveLock Schwachstellenscan

Mit dem DriveLock Schwachstellenscan können Sie auf einem Computersystem automatisiert und regelmäßig nach bisher bekannten Windows- und Drittanbieter-Schwachstellen scannen.

Dabei greift DriveLock auf eine mehrmals täglich aktualisierte Datenbank zurück. Die gefundenen Ergebnisse werden dann im [DriveLock Operations Center \(DOC\)](#) in einer eigenen Ansicht und mit Bewertung des Risikos und der Auswirkungen angezeigt, einschließlich fehlender Patches, veralteter Softwareprogramme oder Bibliotheken mit bekannten Schwachstellen.

1.1 Voraussetzungen

Lizenzierungsoptionen:

- Vulnerability Scanner Basic: Scannen nach Betriebssystem-Schwachstellen (OS Vulnerabilities)
- Vulnerability Scanner Extended: Scannen nach Betriebssystem-Schwachstellen sowie Schwachstellen von Drittanbietern (Third Party Vulnerabilities)

Systemvoraussetzungen:

- DriveLock: ab Version 2020.1 HF1
- Agenten-Betriebssysteme: Windows 8.1, Windows 10; Server 2012R2, 2016, 2019

1.2 Konfiguration in der DriveLock Management Konsole

1.2.1 Schwachstellenkataloge


Der Schwachstellenscan basiert auf Katalogen, die aus der Cloud erst auf den zentralen DriveLock Enterprise Service (DES) geladen und dann auf die DriveLock Agenten verteilt werden.

Es gibt getrennte Kataloge für Betriebssystem- und Drittanbieter-Schwachstellen.

Um die Kataloge zu laden, greift der DES

- auf einen Webservice unter <https://service.drivelock.cloud> und
- eine Konfiguration unter <https://download.drivelock.com/vulnerability-definitions/catalogs.json> zurück.

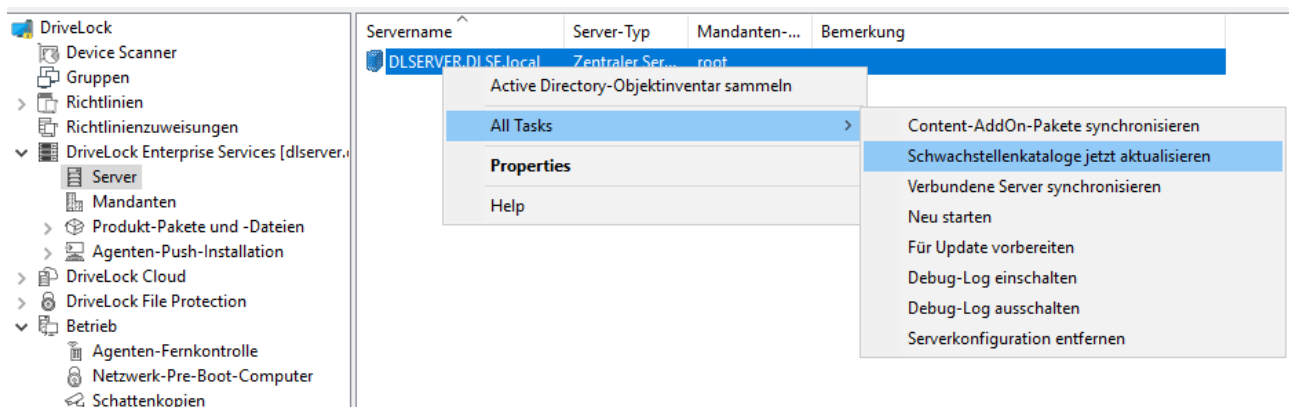
Beim ersten Einrichten kann es etwas dauern, bis der Katalog komplett auf den DES geladen ist. Spätere Aktualisierungen übertragen nur noch die Änderungen und sind somit erheblich schneller.

 Hinweis: Starten Sie den DES nach Eintragen der Lizenz entweder neu oder [aktualisieren](#) Sie in der Management Konsole die Kataloge.

1.2.1.1 Aktualisieren der Schwachstellenkataloge

Gehen Sie folgendermaßen vor:

Klicken Sie im Kontextmenü des jeweiligen DES auf **Alle Aufgaben (All Tasks)** und dann auf **Schwachstellenkataloge jetzt aktualisieren** (s. Abbildung).

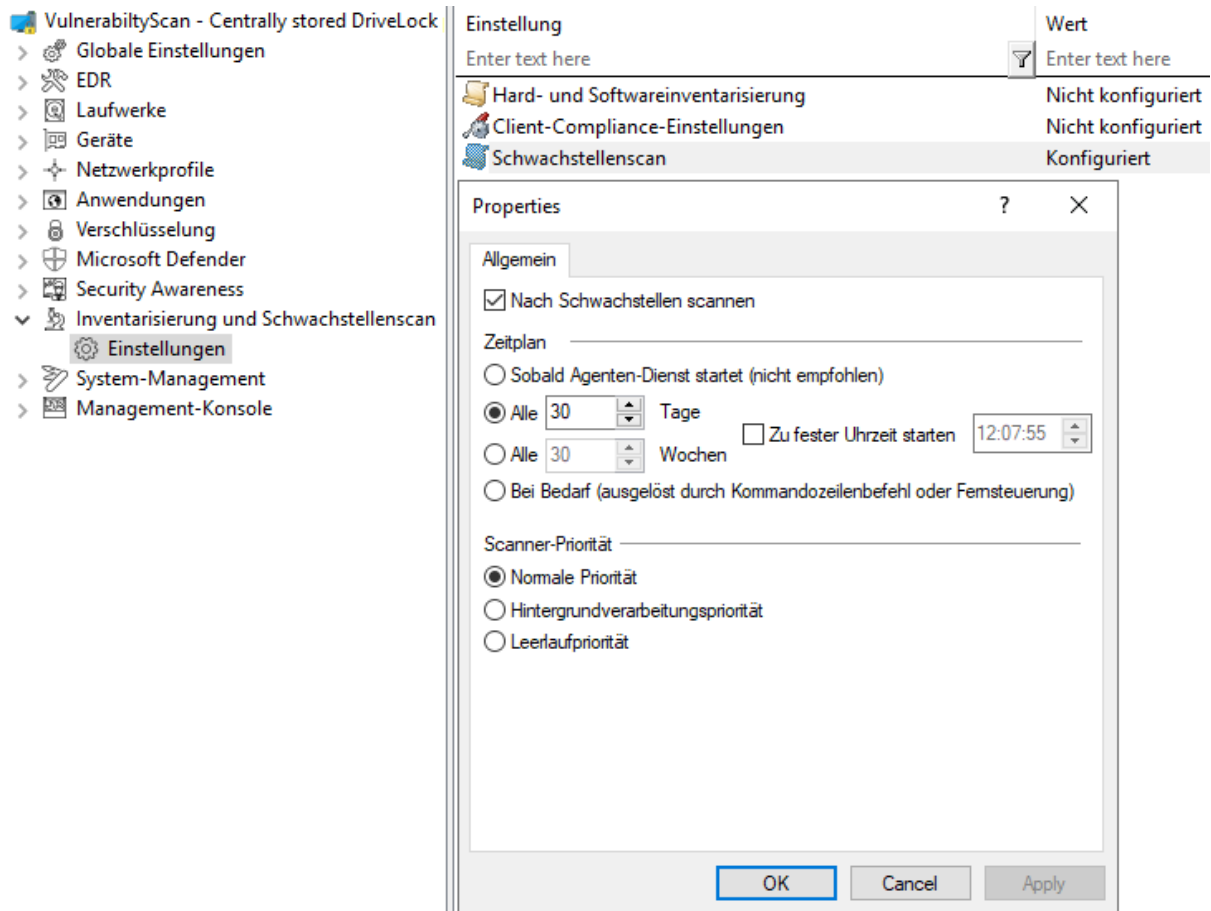


1.2.2 Schwachstellenscan einrichten

Da das Scannen nach Schwachstellen standardmäßig abgeschaltet ist, muss es zunächst in der Richtlinie, in der Sie Vulnerability Scanner lizenziert haben, aktiviert und konfiguriert werden.

Gehen Sie folgendermaßen vor:

1. Öffnen Sie im Knoten **Inventarisierung und Schwachstellenscan** den Unterknoten **Einstellungen**.
2. Öffnen Sie die Einstellung **Schwachstellenscan**.



3. Setzen Sie ein Häkchen bei **Nach Schwachstellen scannen**.
4. Wenn Sie die Option **Bei Bedarf (...)** auswählen, muss der Schwachstellenscan über die [Agenten-Fernkontrolle](#) oder alternativ über die [Kommandozeile des Agenten](#) gestartet werden.
5. Über die Optionen zur **Scanner-Priorität** können Sie die Prozesspriorität des Scanners auf dem Agenten festlegen. Falls der CPU-Verbrauch reduziert werden soll und eine längere Laufzeit akzeptabel ist, kann hier **Hintergrundverarbeitungspriorität** oder sogar **Leerlaufpriorität** gewählt werden.

1.3 Aktionen auf dem DriveLock Agenten

1.3.1 Schwachstellenscan auf dem DriveLock Agenten

Auf dem DriveLock Agenten werden die Schwachstellenkataloge vom DriveLock Enterprise Service (DES) heruntergeladen und regelmäßig aktualisiert.

Die Kataloge liegen auf dem Agenten unter:

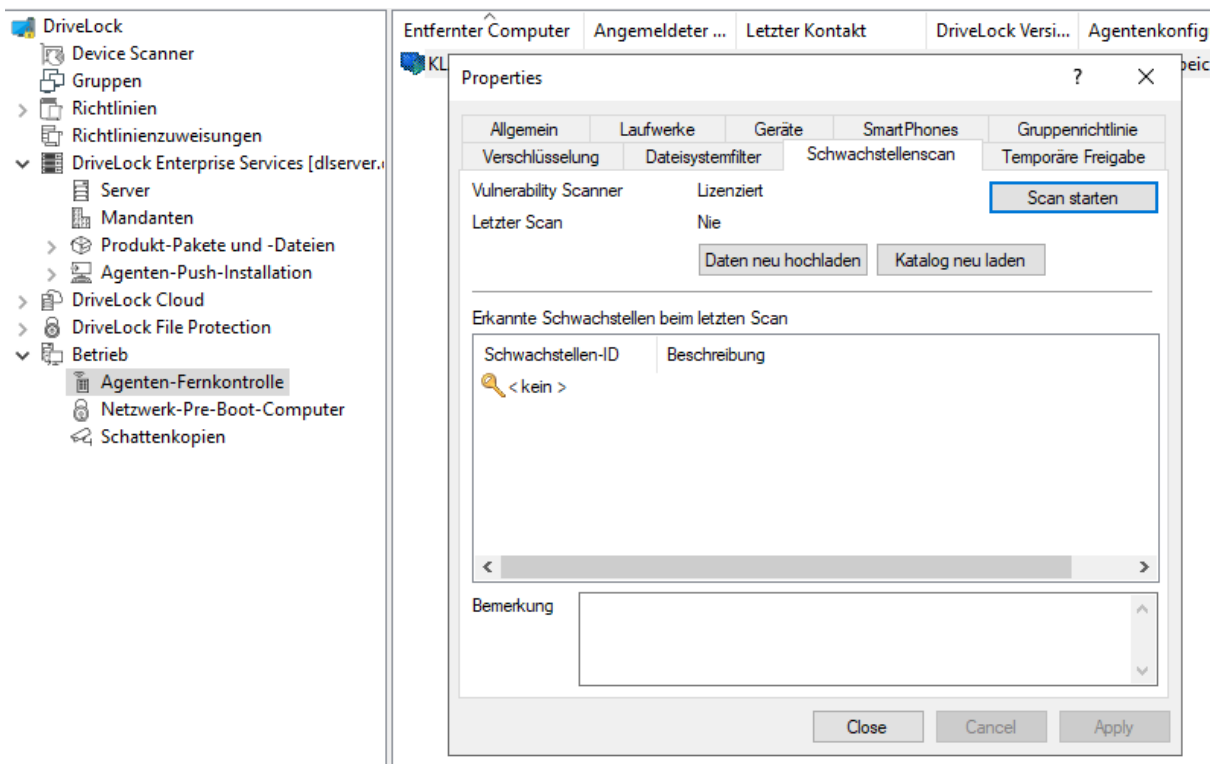
- C:\ProgramData\CenterTools DriveLock\VulScan\3P und
- C:\ProgramData\CenterTools DriveLock\VulScan\OS.

Der eigentliche Schwachstellenscan wird von **DLVulScan.exe** ausgeführt. An der Übertragung der Kataloge auf den Agenten ist auch die **DLOvalHelper.exe** beteiligt. Beide befinden sich im DriveLock-Verzeichnis auf dem Agenten.

1.3.1.1 Schwachstellenscan über die Agenten-Fernkontrolle starten

Gehen Sie folgendermaßen vor:

1. Verbinden Sie sich über die **Agenten-Fernkontrolle** mit dem jeweiligen Agenten. Weitere Informationen zum Thema Agenten-Fernkontrolle finden Sie im Administrationshandbuch unter [DriveLock Online Help](#).
2. Klicken Sie die Schaltfläche **Scan starten**.



3. Klicken Sie die Schaltfläche **Daten neu hochladen**, um sich die Scanergebnisse neu hochladen zu lassen.
4. Oder klicken Sie **Katalog neu laden**, damit der Scankatalog neu geladen wird.

 Hinweis: Diese beiden Optionen dienen vornehmlich der Fehlerbehebung.

5. Sofern beim letzten Scan Schwachstellen erkannt wurde, werden Ihnen diese mit ID und Beschreibung im Dialog angezeigt.

1.3.1.2 Schwachstellenscan über die Kommandozeile starten

Auf dem Agenten können per Kommandozeile Aktionen ausgelöst werden.

Weitere Informationen zum Thema **Agentenstatus über die Kommandozeile abfragen** finden Sie im Administrationshandbuch unter [DriveLock Online Help](#).

Aktionen per Kommandozeile auslösen:

```
drivelock -vulscan: Scannen nach Schwachstellen starten
```

```
drivelock -vsupload: Ergebnisse neu hochladen
```

```
drivelock -vsresetcatalog: Kataloge neu laden
```

Die Optionen sind auch per "drivelock /?" dokumentiert:

```
connected during boot as allowed devices
-resetdeviceusagepolicy ... Reset usage policy shown list for devi
Vulnerability scan:
-vulscan ... execute vulnerablity scan
-vsupload ... re-upload last vulnerablity scan result
-vsresetcatalog ... reload vulnerability catalog
```

1.4 DriveLock Operations Center (DOC)

1.4.1 Schwachstellenscan im DOC

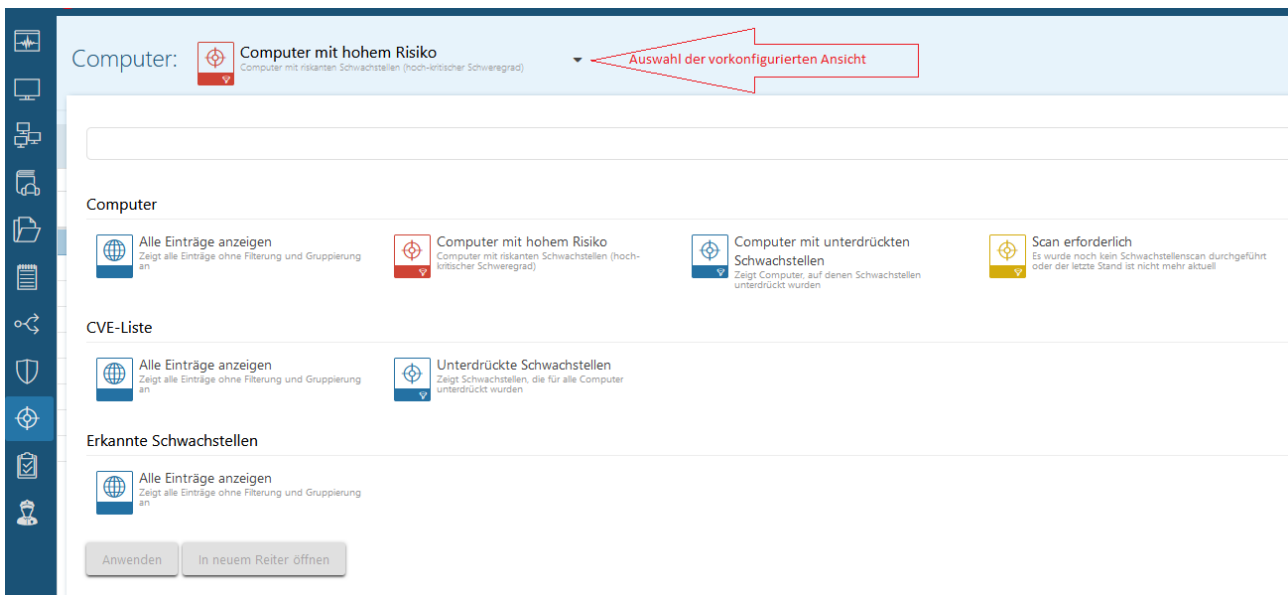
Im DriveLock Operations Center (DOC) wird der Status des Schwachstellenscans auf den Agenten in der **Schwachstellenscan**-Ansicht angezeigt.

Um die Kritikalität einer Schwachstelle anzugeben, wird als Bewertungssystem das Common Vulnerability Scoring System verwendet. Dabei gibt der Base Score die Kritikalität einer Schwachstelle an. Dieser liegt in einem Bereich von S1 (unkritisch) bis S10 (höchste Kritikalität).

Allgemeine Informationen zum DOC finden Sie in der **DriveLock Control Center** Dokumentation auf [DriveLock OnlineHelp](#).

1.4.1.1 Ansicht

Als vorkonfigurierte Ansicht ist standardmäßig **Computer mit hohem Risiko** eingestellt. Das umfasst alle Computer, die offene Schwachstellen mit einen Base Score $\geq S7$ haben.



Durch Klick auf den Pfeil nach unten können Sie weitere vorkonfigurierte Ansichten aus drei verschiedenen Listen auswählen:

1. **Computer** (Computerübersicht)
 - Zeigt die offenen oder unterdrückten Schwachstellen für einen Computer an
 - Erlaubt das Unterdrücken der Schwachstelle für einen oder alle Computer
2. **CVE-Liste** (Common Vulnerabilities and Exposures (CVE®))
 - Zeigt an, welche CVEs existieren
 - > Erlaubt das Unterdrücken für alle Computer
 - Zeigt in der Detailansicht eines CVE die gefährdeten Computer an
 - > Erlaubt die Navigation zu den gefährdeten Computern (öffnet die Liste Erkannte Schwachstellen)
3. **Erkannte Schwachstellen** (Schwachstellenübersicht)
 - Zeigt für einen Computer, wann eine bestimmte Schwachstelle erkannt wurde
 - Erlaubt das Unterdrücken für einen oder alle Computer

2 Inventarisierung

Der DriveLock Agent ist in der Lage, in regelmäßigen bzw. zu bestimmten Zeitpunkten Informationen zur aktuellen Hard- oder Software seines Computers zu ermitteln und an den DriveLock Enterprise Service zu übertragen. Damit erhalten Sie z.B. schnell einen Überblick, welche Programme oder Software-Patches auf Ihren Computern installiert sind, da sich die gesammelten Daten zentral über das DriveLock Control Center analysieren lassen.

2.1 Hardware- und Softwareinventarisierung

Die Einstellungen für diese Funktionalität legen fest, wann der DriveLock Agent welche Informationen sammelt, oder ob diese Funktion deaktiviert bleibt.

Gehen Sie folgendermaßen vor:

1. Öffnen Sie im Knoten **Inventarisierung und Schwachstellenscan** den Unterknoten **Einstellungen** und klicken Sie dann auf **Hard- und Softwareinventarisierung**.

The screenshot shows the DriveLock Control Center interface. On the left, a tree view shows the navigation path: **VulnerabilityScan - Centrally stored DriveLock** > **Einstellungen**. The main window displays a table of settings:

Einstellung	Wert
Enter text here	Enter text here
Hard- und Softwareinventarisierung	Nicht konfiguriert
Client-Compliance-Einstellungen	Nicht konfiguriert
Schwachstellenscan	Konfiguriert

Below the table, the 'Properties' dialog box for 'Hard- und Softwareinventarisierung' is open, showing the 'Allgemein' tab. The following options are checked:

- Inventarisierungsdaten sammeln
- Gerätedaten sammeln
- Laufwerksdaten sammeln
- Daten zu installierter Software sammeln
- Patch- und Hotfixinformationen sammeln

The 'Zeitplan' (Schedule) section shows:

- Sobald Agenten-Dienst startet (nicht empfohlen)
- Alle 30 Tage Zu fester Uhrzeit starten 13:19:04
- Alle 30 Wochen
- Bei Bedarf (ausgelöst durch Kommandozeilenbefehl oder Fernsteuerung)

Buttons: OK, Cancel, Apply

2. Damit der Agent Informationen über den Computer sammelt, aktivieren Sie **Inventarisierungsdaten sammeln**.

3. Legen Sie nun mit Hilfe der jeweiligen Auswahlpunkte fest, welche Daten der Agent ermitteln und an den DriveLock Enterprise Service übermitteln soll.
4. Anschließend legen Sie noch den Zeitpunkt fest, an dem der Agent mit der Informationsbeschaffung beginnt und die Daten an den DriveLock Enterprise Service gesendet werden.



Hinweis: Bitte beachten Sie, dass der Agent für das Ermitteln der Daten etwas Zeit benötigt und das System geringfügig mehr als im normalen Betrieb belastet wird. Aus diesem Grund beginnt der Scan nach dem Start des Agenten auch einige Minuten verzögert (sofern Sie diese Option gewählt haben).

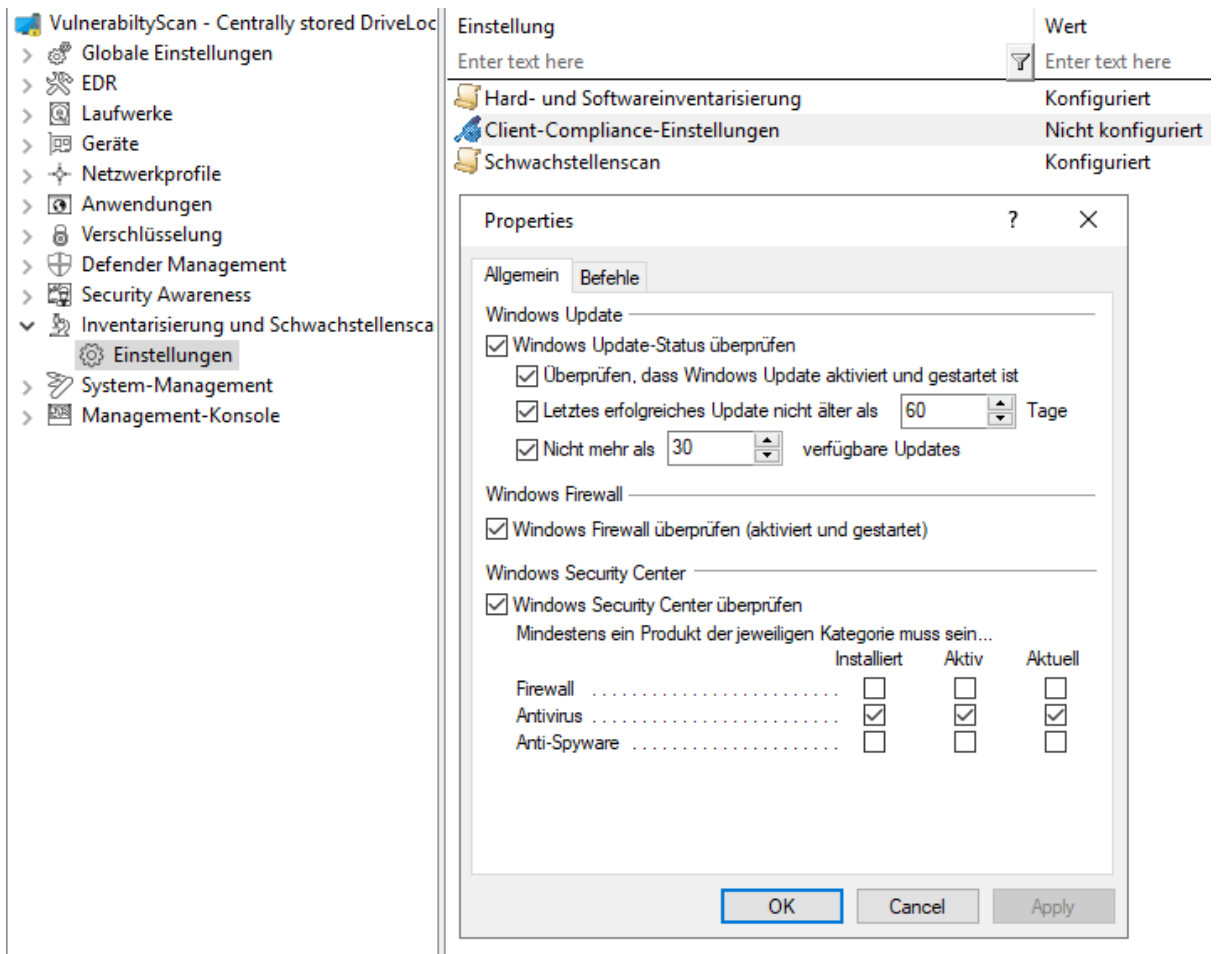
2.2 Client Compliance

Mit dieser Option können Sie einstellen, welche Parameter auf dem PC für den Client Compliance Status überprüft werden sollen.

2.2.1 Client-Compliance-Einstellungen

Gehen Sie folgendermaßen vor:

1. Öffnen Sie im Knoten **Inventarisierung und Schwachstellenscan** den Unterknoten **Einstellungen** und klicken Sie dann auf **Client-Compliance-Einstellungen**.



2. Setzen Sie die gewünschten Einstellungen.

3. Auf dem Reiter **Befehle** können Sie beliebige ausführbare Programme oder Skripte konfigurieren.

Nehmen Sie diese vorher im Richtliniendateispeicher auf und wählen sie von dort aus. Die Programme oder Skripte werden vom DriveLock Agenten auf den Clients aufgerufen und müssen als Rückgabewert 1 für compliant und 0 für nicht compliant liefern.

Im DriveLock Control Center (DCC / Helpdesk) wird der Compliance Status der Agenten detailliert angezeigt.

Copyright

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.

© 2021 DriveLock SE. Alle Rechte vorbehalten.