DriveLock Defender Integration

Dokumentation 2021.2

DriveLock SE 2021

Inhaltsverzeichnis

1 Integration von Microsoft Defender in DriveLock

DriveLock bietet die Möglichkeit, Microsoft Defender über die DriveLock Management Konsole (DMC) mit Richtlinien zu konfigurieren und den aktuellen Status der DriveLock Agenten im DriveLock Operations Center (DOC) zu überwachen.

In der DMC können alle vorhandenen Einstellungen der Microsoft Defender Antivirus Gruppenrichtlinien (GPO) konfiguriert werden.

Ausgewählte Einstellungen werden direkt in der Taskpad-Ansicht angeboten und können so schnell konfiguriert werden:

- Scan-Einstellungen bei Dateizugriffen und Art der Reaktion bei gefundener Schadsoftware
- Ausnahmeregelungen für Dateiüberprüfungen oder Prozesse
- Regelmäßige Scan-Überprüfungen mit Datum und Uhrzeit, Häufigkeit und Art der Reaktion
- Art und Inhalt der Benachrichtigungen des Endbenutzers

Des Weiteren können Einstellungen für den Defender-Scan von externen Laufwerken vorgenommen werden:

- Einsatz des Virenscanners beim Verbinden von externen Laufwerken und ggf. automatische Sperre des Zugriffs bei festgestellter Schadsoftware

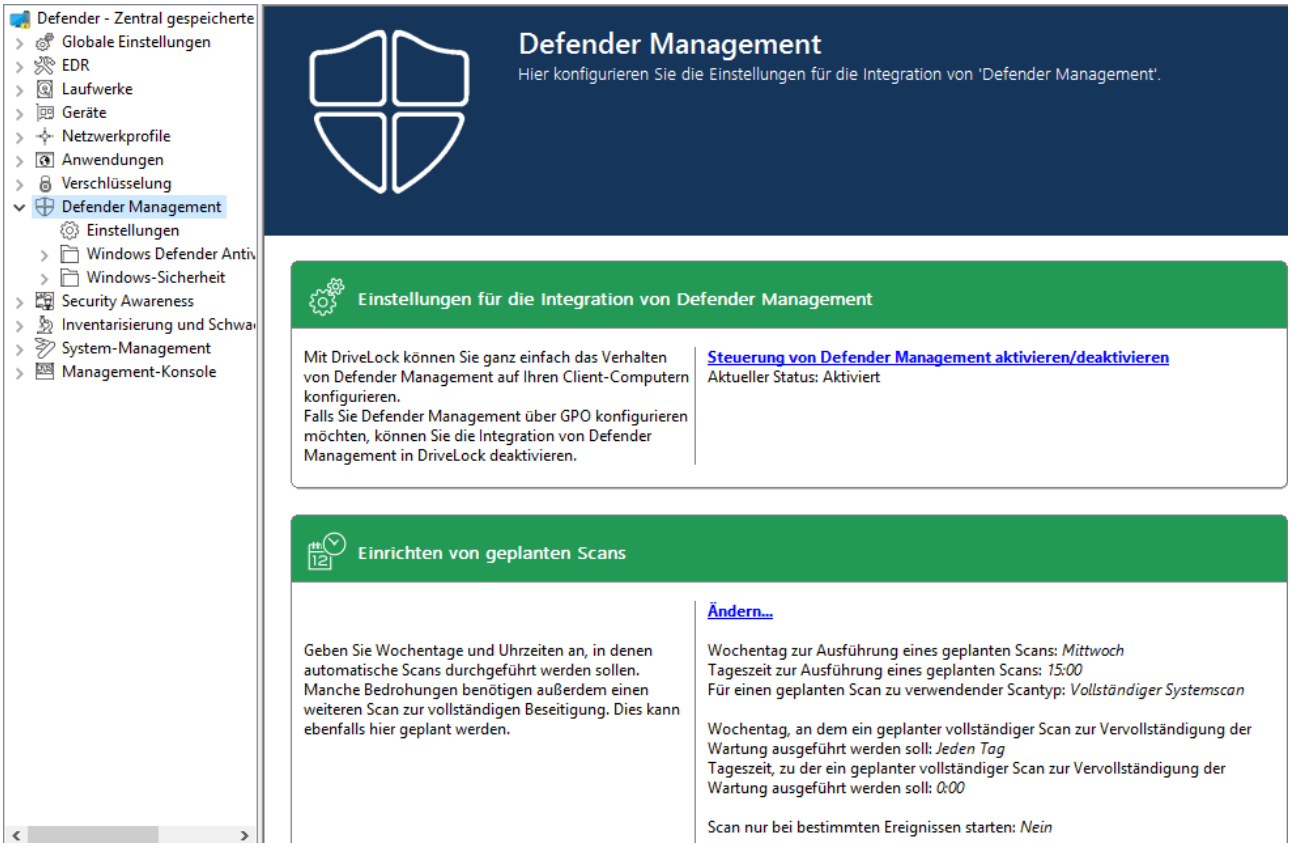
Im DriveLock Operations Center (DOC) können Sie sich Statusberichte über aktuelle Bedrohungen und den Zustand der DriveLock Agenten anzeigen lassen. Gefundene Bedrohungen lassen sich dort exakt analysieren und bei Bedarf können Benachrichtigungen bei Falschmeldungen oder irrelevanten Meldungen unterdrückt werden.

> Achtung: Für das Microsoft Defender Management ist eine Lizenz erforderlich.

2 Konfiguration

2.1 Übersicht in der DriveLock Management Konsole

Sobald die Lizenzierung durchgeführt wurde, enthält die Richtlinie den neuen Knoten **Defender Management**. Hier kann die Konfiguration vorgenommen werden. In dieser Übersicht nehmen Sie zunächst die Aktivierung (oder ggf. spätere Deaktivierung) vor und integrieren somit die Steuerung der Microsoft-Defender-Funktionalitäten in DriveLock.

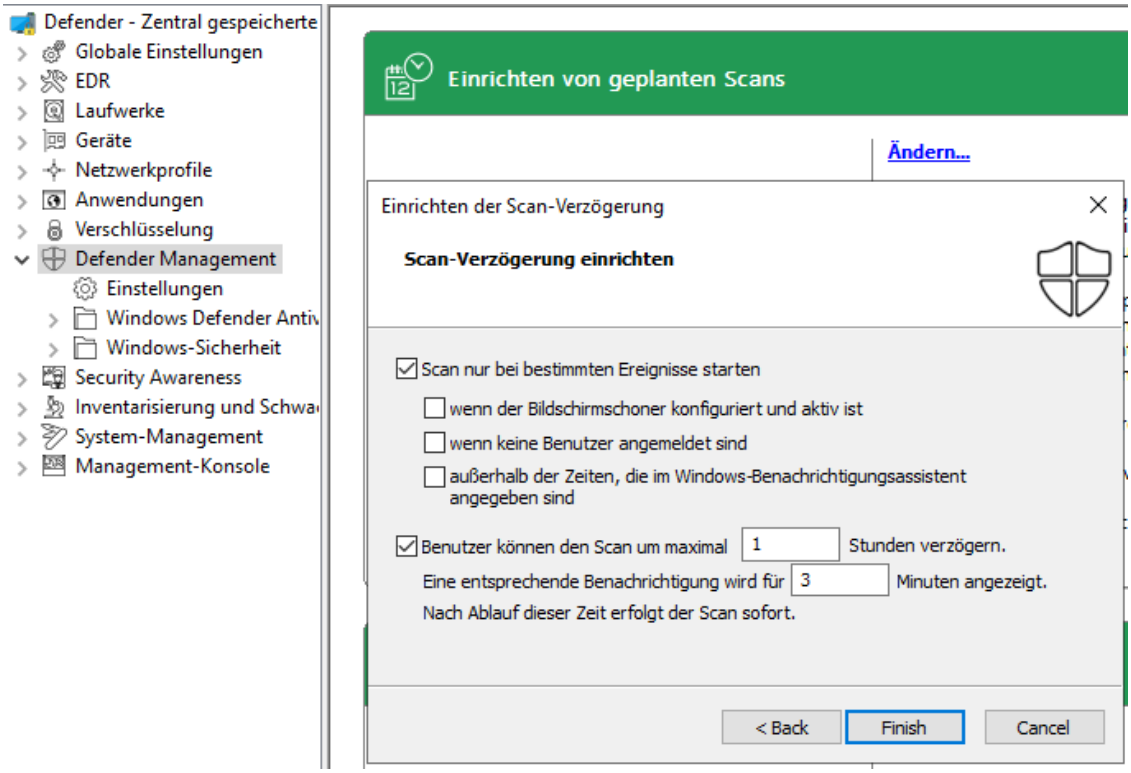


Sollte sich eine andere Ansicht in Ihrer Richtlinie öffnen, liegt das an der Einstellung **Show basic configuration**. Um die vereinfachten Einstellungsmöglichkeiten sehen zu können, muss diese Einstellung auf der höchsten Ebene der Richtlinie aktiviert sein, siehe Abbildung:

2.2 Vereinfachte Konfiguration in der Taskpad-Ansicht

Neben der Aktivierung der Steuerung für Microsoft Defender, lassen sich in der Taskpad-Ansicht des Knotens **Microsoft Defender** weitere grundlegende Einstellungen konfigurieren.

1. **Einrichten von geplanten Scans**:
   Hier können Sie folgendes konfigurieren:
   - Zeit und Typ des Scans: Wird die Zeit für den geplanten Scan an dieser Stelle festgelegt, verwendet DriveLock einen eigenen Scheduler, um den Scan zu der definierten Uhrzeit zu starten. Dabei werden die Microsoft Defender-eigenen Einstellungen wie **Zufälliges Festlegen von Zeiten für geplante Aufgaben** oder **Starten des geplanten Scans ausschließlich zu dem Zeitpunkt, zu dem der Computer eingeschaltet ist, aber nicht verwendet wird** nicht berücksichtigt.
   - Zeit zur Vervollständigung der Wartung: Diese Angabe ist nötig, weil manche Bedrohungen erst nach einem weiteren vollständigen Scan vom Microsoft Defender beseitigt werden können.
   - Scan-Verzögerung und Scan-Ereignisse: Bei der Einrichtung von geplanten Scans können Sie angeben, dass Scans nur unter bestimmten Bedingungen starten und Benutzer Scans aufschieben dürfen.



> Hinweis: Wenn Sie den Microsoft Defender-eigenen Scheduler verwenden möchten, nehmen Sie bitte die entsprechenden Einstellungen im Unterknoten **Windows Defender Antivirus**, Einstellung **Scan** vor.

2. **Scanoptionen**:
   Konfigurieren Sie hier die Antivirus-Scanoptionen.
3. **Ausschlüsse**:
   Konfigurieren Sie hier die Ausschlüsse, um bestimmte Dateien von Microsoft Defender-Antivirus-Scans auszuschließen. Weitere Informationen finden Sie bei Microsoft.
4. **Automatische Wartungsaktion**:
   Konfigurieren Sie hier die automatische Wartungsaktion für die einzelnen Bedrohungswarnungsebenen.
   Die Klassifizierung der einzelnen Bedrohungen nach der Bedrohungswarnungsebene (niedrig, mittel, hoch, schwerwiegend) ist in den Defender-Signaturdefinitionen hinterlegt. Man kann sich diese Information z.B. über Powershell mit dem Befehl Get-MpThreatCatalog anzeigen lassen. Die SeverityID entspricht der Bedrohungswarnungsebene:
   1 = Niedrig (Low)
   2 = Mittel (Medium)
   4 = Hoch (High)
   5 = Schwerwiegend (Severe)
5. **Verringerung der Angriffsfläche**:
   Legen Sie hier Regeln zur Verringerung der Angriffsfläche (Attack Surface Reduction - ASR) an.

2.3 Einstellungen

2.3.1 Allgemeine Einstellungen

Folgende allgemeine Einstellungen lassen sich für die Integration von Microsoft Defender in DriveLock konfigurieren:

- Steuerung von Microsoft Defender aktivieren/deaktivieren
- Bestehende Microsoft Defender-Konfiguration löschen
- Erweiterte Konfigurationsmöglichkeiten anzeigen

2.3.1.1 Steuerung von Microsoft Defender aktivieren/deaktivieren

Um die Steuerung des Microsoft Defenders auf DriveLock Agenten zu ermöglichen, muss in der Richtlinie die Einstellung **Steuerung von Microsoft Defender**

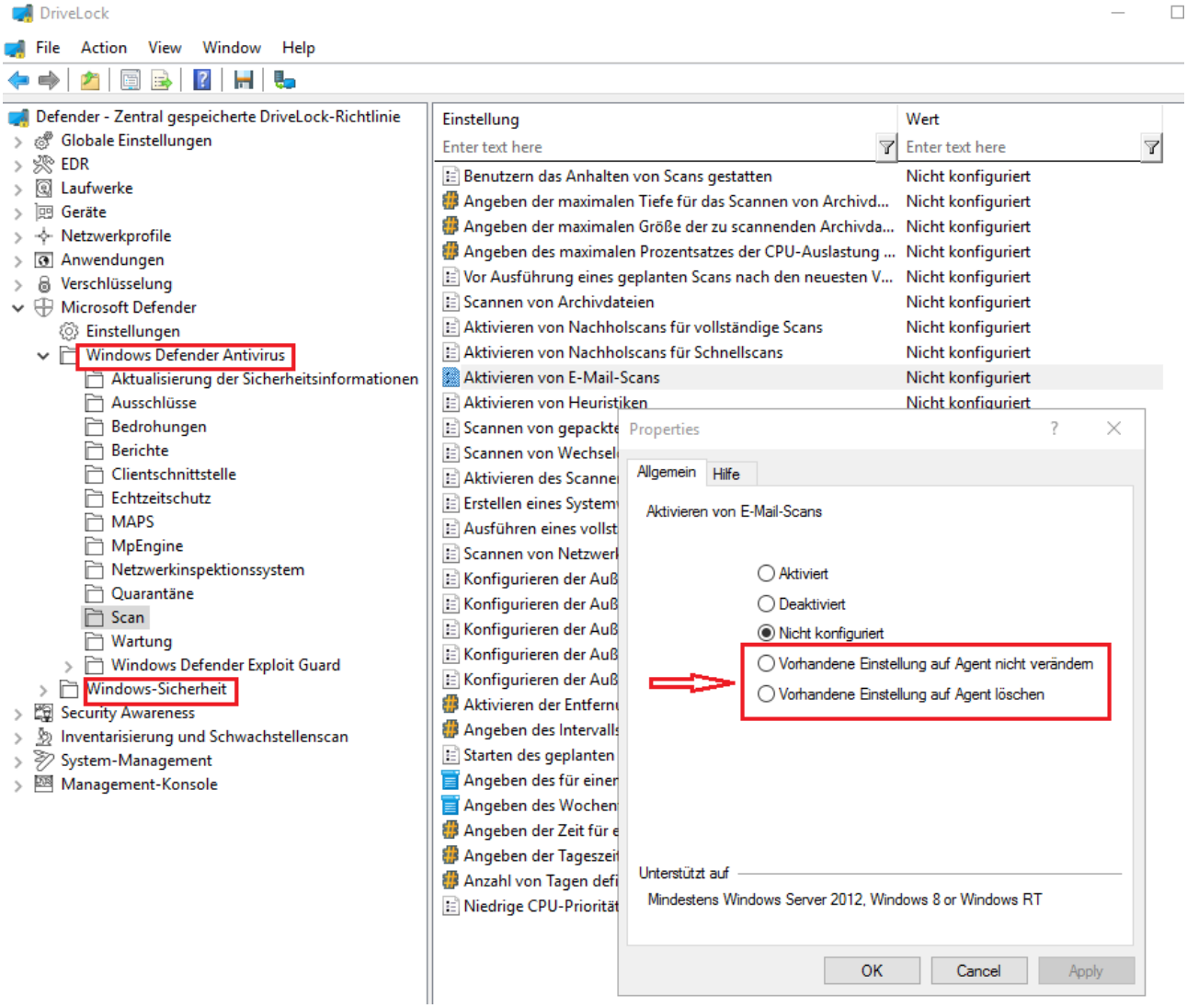
aktivieren/deaktivieren aktiviert sein. Dies ist standardmäßig der Fall.

> Hinweis: Diese Einstellung betrifft lediglich die Steuerung durch DriveLock und nicht die eigentliche Funktionalität von Microsoft Defender.

2.3.1.2 Erweiterte Konfigurationsmöglichkeiten anzeigen

Wenn Sie die Einstellung **Erweiterte Konfigurationsmöglichkeiten anzeigen** aktivieren, werden Ihnen zwei zusätzliche Konfigurationsmöglichkeiten in den Einstellungsdialogen der Knoten **Windows Defender Antivirus und Windows-Sicherheit** eingeblendet, die ansonsten nicht angezeigt werden.

Im Beispiel sehen Sie den Dialog für die Scan-Einstellungen für E-Mails:



Die Konfigurationsmöglichkeiten haben folgenden Effekt:

- **Vorhandene Einstellung auf Agent nicht verändern**:
  Wenn die Einstellung bereits auf dem Agenten gesetzt ist, wird DriveLock diese nicht verändern.

  > Hinweis: Im Unterschied zu **Not configured** verändert DriveLock eine solche Einstellung nicht, unabhängig davon, ob sie in einer anderen zugewiesenen DriveLock Richtlinie gesetzt ist oder nicht. Das trifft auf Richtlinien zu, die in der Reihenfolge der Zuweisungen **vor** dieser Richtlinie kommen.

  Anwendungsbeispiel:
  Auf allen DriveLock Agenten sollen bestimmte Defender-Einstellungen gesetzt werden. Sie erstellen eine DriveLock-Richtlinie mit den entsprechenden Einstellungen und weisen diese Ihren Agenten zu. Nun soll eine Abteilung einige dieser Einstellungen selbst konfigurieren können (z.B. per Gruppenrichtlinie, manuell oder mit einem anderen externen Tool). Um nicht die komplette Richtlinie kopieren zu müssen und nur diese wenigen Einstellungen zu verändern, können Sie eine neue Richtlinie erstellen und in dieser Richtlinie die betroffenen Einstellungen auf **Vorhandene Einstellung auf Agent nicht verändern** setzen. Diese neue Richtlinie weisen Sie den Agenten zu, und zwar so, dass sie in der die Reihenfolge nach der bestehenden Defender Richtlinie kommt.

- **Vorhandene Einstellung auf Agent löschen**:
  Wenn eine Defender Einstellung aus dem Knoten **Windows Defender Antivirus** auf diesen Wert gesetzt wird, wird diese Defender Einstellung auf dem DriveLock Agenten gelöscht. Der Defender wird somit seine Standardeinstellung verwenden.
  Diese Option ist vergleichbar mit der Einstellung Bestehende Microsoft Defender-Konfiguration löschen, mit dem Unterschied, dass sie für eine einzelne Einstellung verwendet wird, während **Bestehende Microsoft Defender-Konfiguration löschen** alle Einstellungen löscht.

2.3.1.3 Bestehende Microsoft Defender-Konfiguration löschen

Mit der Einstellung **Bestehende Microsoft Defender-Konfiguration löschen** legen Sie fest, ob DriveLock existierende Defender-Einstellungen auf dem Agenten beibehalten oder vor dem Anwenden der Richtlinie löschen soll.

Standardmäßig behält DriveLock Agent die bestehende Defender-Konfiguration bei und setzt nur diejenigen Einstellungen, die in der DriveLock Richtlinie enthalten sind.

2.3.2 Einstellungen für Defender-Scans mit dem DriveLock Scheduler

Folgende Einstellungen betreffen die Ausführung der geplanten Scans mithilfe des DriveLock Schedulers:

- Geplanter Scantag
- Geplante Scanzeit
- Scan nur bei bestimmten Ereignissen starten
- Benutzern ermöglichen, den Beginn des Scans zu verzögern
- Maximale Anzahl von Stunden, um die der Start des Scans verzögert werden kann
- Anzahl der Minuten, nach denen die Benachrichtigung automatisch geschlossen wird

2.3.2.1 Geplanter Scantag

Legen Sie hier einen Tag fest, an dem gescannt werden soll.

Diese Einstellung ermöglicht es Ihnen, einen bereits festgelegte Wochentag für den Defender-Scan zu ändern oder ggf. auch zu löschen, in dem Sie die Einstellung auf **Nicht konfiguriert** setzen.

2.3.2.2 Geplante Scanzeit

Legen Sie hier eine Zeit fest, zu der gescannt werden soll.

Diese Einstellung ermöglicht es Ihnen, eine bereits festgelegte Zeit für den Defender-Scan zu ändern oder ggf. auch zu löschen, in dem Sie die Einstellung auf **Nicht konfiguriert** setzen.

2.3.2.3 Scan nur bei bestimmten Ereignissen starten

Mit dieser Einstellung können Sie festlegen, dass der Defender-Scan nur bei bestimmten Ereignissen gestartet werden darf. Benutzer werden dadurch nicht bei ihrer Arbeit beeinträchtigt.

> Hinweis: Beachten Sie, dass der Bildschirmschoner für die entsprechende Option aktiviert sein muss. Solange der Bildschirmschoner ausgeschaltet ist, wird diese Option ignoriert.

Im Windows-Benachrichtigungsassistenten kann eine granulare Einstellung von Zeiten für Benachrichtigungen angegeben werden, die DriveLock abfragt. Mit dieser Option wird der

Scan nur außerhalb dieser konfigurierten Zeiten durchgeführt (bzw. Benachrichtigungen nur dann angezeigt).

2.3.2.4 Benutzern ermöglichen, den Beginn des Scans zu verzögern

Um die Auslastung der CPU auf den jeweiligen Client-Computern möglichst gering zu halten, können Sie hier festlegen, dass die Benutzer einen Defender-Scan aufschieben dürfen. Dazu wählen Sie die Option **Aktiviert**.

Sie können sowohl die Dauer der Verzögerung als auch die Anzeige einer entsprechenden Benachrichtigung beim Benutzer konfigurieren.

2.3.2.5 Maximale Anzahl von Stunden, um die der Start des Scans verzögert werden kann

In manchen Fällen ist es für Benutzer wichtig, den Start eines Defender-Scans hinauszuschieben, beispielsweise um ungestört weiterarbeiten zu können oder automatisierte Arbeiten durchzuführen. Aus diesem Grund kann eine Verzögerung von bis zu 16 Stunden konfiguriert werden.

Geben Sie in dem Dialog einen entsprechenden Wert ein.

Sobald die Verzögerung verstrichen ist, wird der Benachrichtigungsdialog beim Benutzer beendet und der Scan anschließend direkt gestartet.

2.3.2.6 Anzahl der Minuten, nach denen die Benachrichtigung automatisch geschlossen wird

Mit dieser Einstellung konfigurieren Sie, wie lange der Benachrichtigungsdialog beim Benutzer offen bleibt.

Sobald der Benachrichtigungsdialog automatisch geschlossen wird, ohne dass der Benutzer eine Verzögerung eingegeben hat, wird der Scan gestartet. Dabei gilt immer die kürzere konfigurierte Zeit (Verzögerungs- bzw. Anzeigezeit).

2.4 Windows Defender Antivirus und Windows-Sicherheit

Die Unterknoten **Windows Defender Antivirus** und **Windows-Sicherheit** enthalten alle Einstellungen für den Microsoft Defender, die mit der Gruppenrichtlinie Stand Juni 2019 verteilt werden können.

Der DriveLock Agent speichert die Einstellungen aus der DriveLock Richtlinie an der gleichen Stelle in der Registry ab, an der auch Gruppenrichtlinieneinstellungen gespeichert werden. Die Defender-Einstellungen sind dann zu finden unter:

- `HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows Defender` bzw.
- `HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows Defender Security Center`

Wenn die Einstellung Bestehende Microsoft Defender-Konfiguration löschen deaktiviert ist, ist es möglich, zusätzlich zu der DriveLock Richtlinie einen Teil der Einstellungen über die Gruppenrichtlinie oder mit einem anderen externen Tool zu verteilen.

2.5 Externe Laufwerke

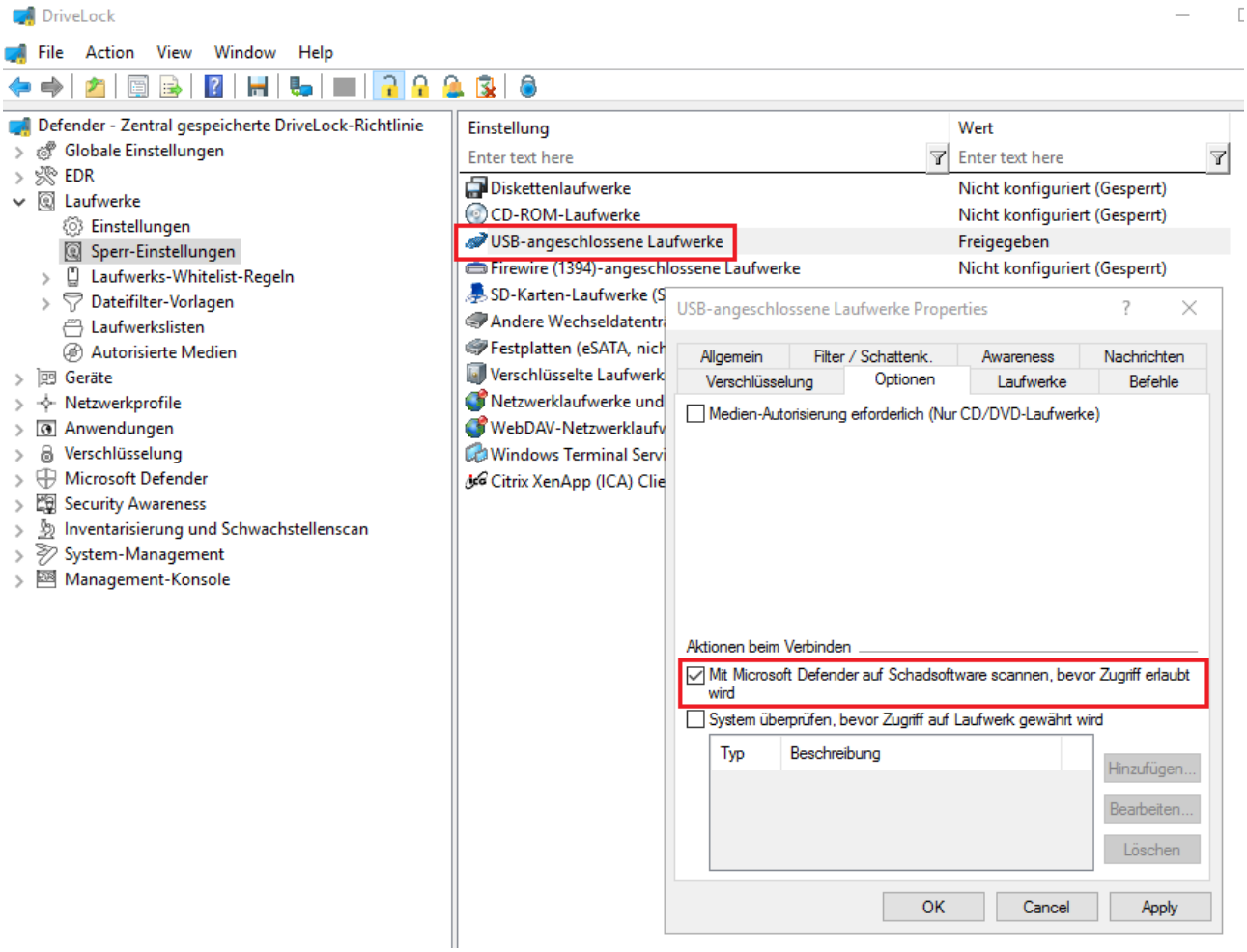
2.5.1 Externe Laufwerke scannen

Sie können ein externes Laufwerk in Richtlinien so konfigurieren, dass automatisch ein Virenscan gestartet wird, sobald es an den Computer angeschlossen wird. Anwender können dann erst auf das Laufwerk zugreifen, wenn der Scan abgeschlossen ist und keine Schadsoftware gefunden wurde.

2.5.2 Konfiguration über Sperr-Einstellungen

Gehen Sie folgendermaßen vor:

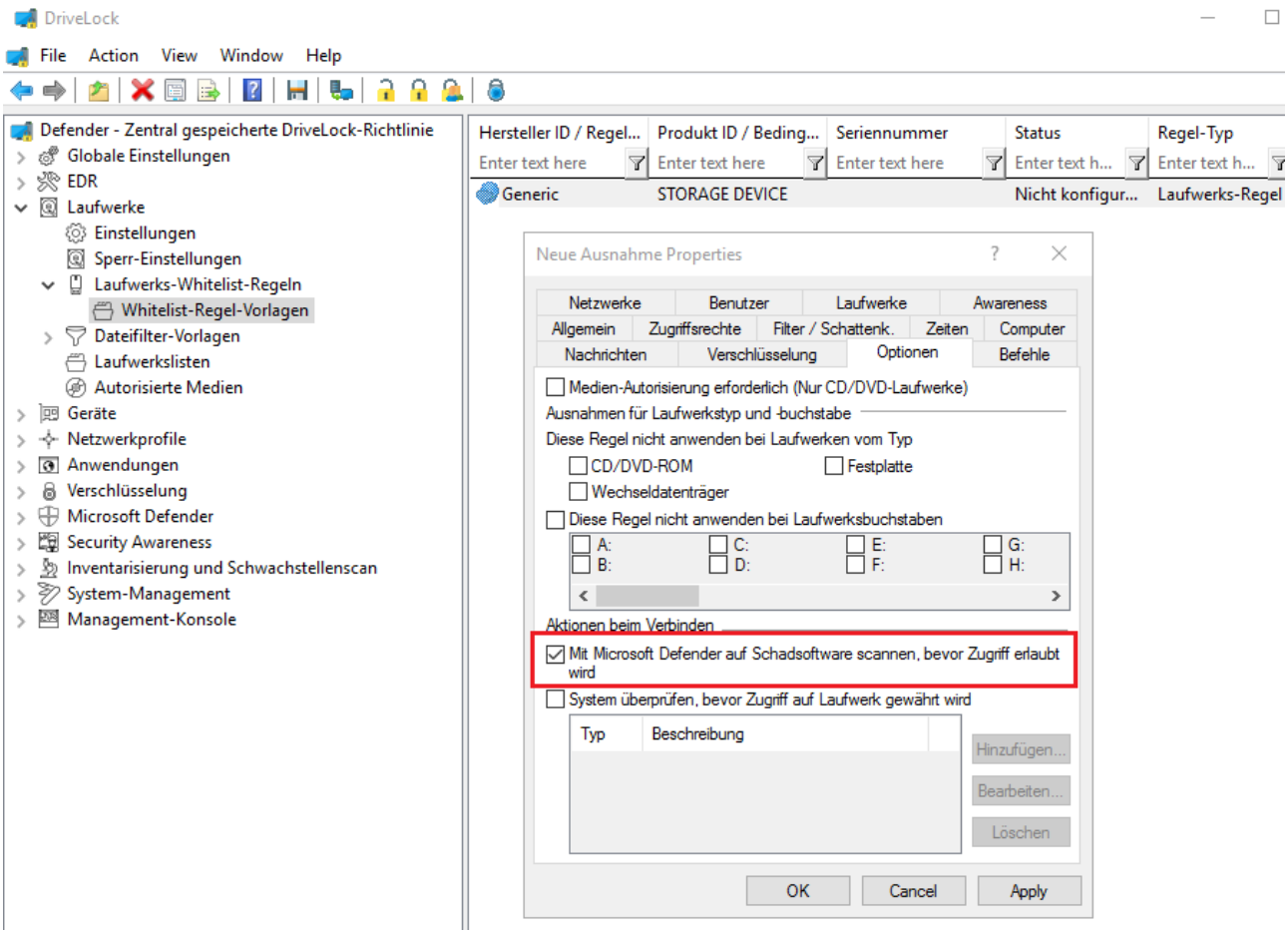
1. Öffnen Sie in der Richtlinie im Knoten **Laufwerke** den Unterknoten **Sperr-Einstellungen** und wählen Sie darin das entsprechende Laufwerk zum Bearbeiten aus.
2. Wechseln Sie im Dialog auf den Reiter **Optionen**.
3. Setzen Sie ein Häkchen bei der Option **Mit Microsoft Defender auf Schadsoftware scannen, bevor Zugriff erlaubt wird**.



2.5.3 Konfiguration über Laufwerks-Whitelist-Regeln

Gehen Sie folgendermaßen vor:

1. Öffnen Sie in der Richtlinie im Knoten **Laufwerke** den Unterknoten **Laufwerks-Whitelist-Regeln**. Legen Sie eine neue Whitelist-Regel an oder öffnen Sie eine bestehende zum Bearbeiten aus.
2. Wechseln Sie im Dialog auf den Reiter **Optionen**.
3. Setzen Sie ein Häkchen bei der Option **Mit Microsoft Defender auf Schadsoftware scannen, bevor Zugriff erlaubt wird**.



Hinweis: Wenn es sich um ein verschlüsseltes Laufwerk handelt, startet DriveLock den Scan, sobald das Laufwerk verbunden und entschlüsselt ist.

Auf dem DriveLock Agenten wird eine Nachricht im Taskleistensymbol angezeigt.

Wenn Microsoft Defender eine Bedrohung auf dem Laufwerk findet, macht sich das durch längere Scan-Laufzeit bemerkbar. Microsoft Defender versucht dann die Bedrohungen zu

beseitigen. Wenn das nicht gelingt, muss das Laufwerk getrennt und neu verbunden werden, damit Microsoft Defender das Entfernen der Bedrohung abschließen kann.

Der Benutzer bekommt eine Nachricht angezeigt, ob das Entfernen erfolgreich war und das Laufwerk damit zugreifbar ist.

Hinweis: Kann Microsoft Defender die Bedrohung nicht beseitigen, bleibt noch die Möglichkeit über eine temporäre Freigabe auf das Laufwerk zuzugreifen.

3 Agenten-Fernkontrolle

3.1 Eigenschaften des DriveLock Agenten

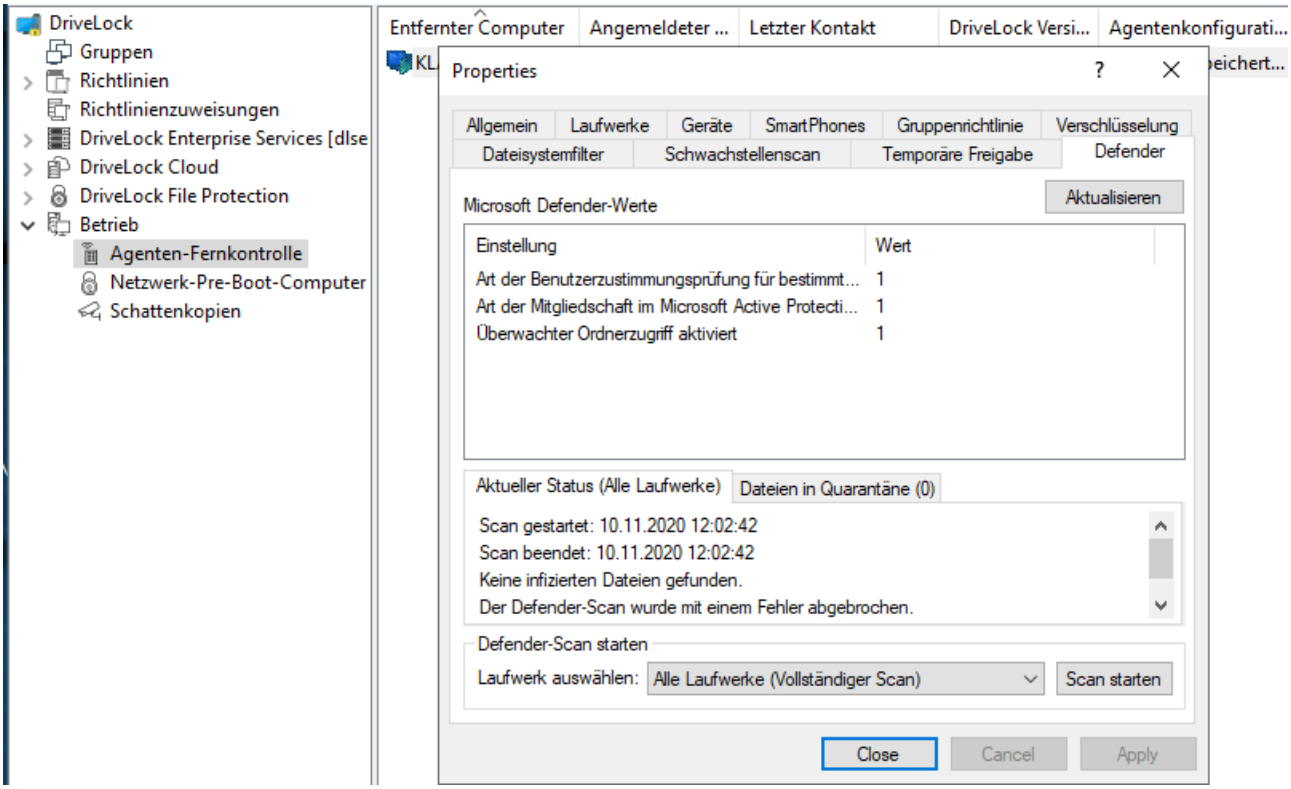
Verbinden Sie sich über die **Agenten-Fernkontrolle** mit einem DriveLock Agenten und öffnen Sie dessen Eigenschaftendialog durch Doppelklick.

Auf dem Reiter **Defender** finden Sie aktuelle Informationen zum Defender-Status auf dem jeweiligen DriveLock Agenten.

> Hinweis: Allgemeine Informationen zur Agenten-Fernkontrolle finden Sie im Administrationshandbuch unter DriveLock Online Help.

3.1.1 Optionen im Defender-Dialog

Auf diesem Reiter sehen Sie wann der letzte Scan auf dem Agenten durchgelaufen ist, ob dabei Fehler aufgetreten sind und ob z.B. der Antivirus-Schutz aktiviert ist oder welche Version die Signatur hat.



Folgende Optionen sind im Dialog möglich:

- Klicken Sie auf **Aktualisieren**, um die Werte neu zu laden.
- Klicken Sie auf **Scan starten**, um sofort einen Defender-Scan zu starten. Wenn Sie dann auf **Aktualisieren** klicken, erscheint der aktuelle Status auf dem gleichnamigen

Reiter.

- Der Reiter **Aktueller Status** gibt einen Überblick über den Verlauf und das Resultat des zuletzt durchgeführten Scans.
- Auf dem Reiter **Dateien in Quarantäne** werden sämtliche Dateien in Quarantäne angezeigt (nicht nur die des letzten Scans).

3.2 Deaktivierung im Agenten-Freigabeassistenten

DriveLock Defender Management lässt sich im Freigabeassistenten für einzelne Agenten temporär deaktivieren. Dies ist sinnvoll, wenn Sie Defender-Einstellungen manuell ändern wollen, um beispielsweise das Verhalten eines Agenten zu analysieren, bestimmte Software zu installieren oder Viren manuell zu entfernen.

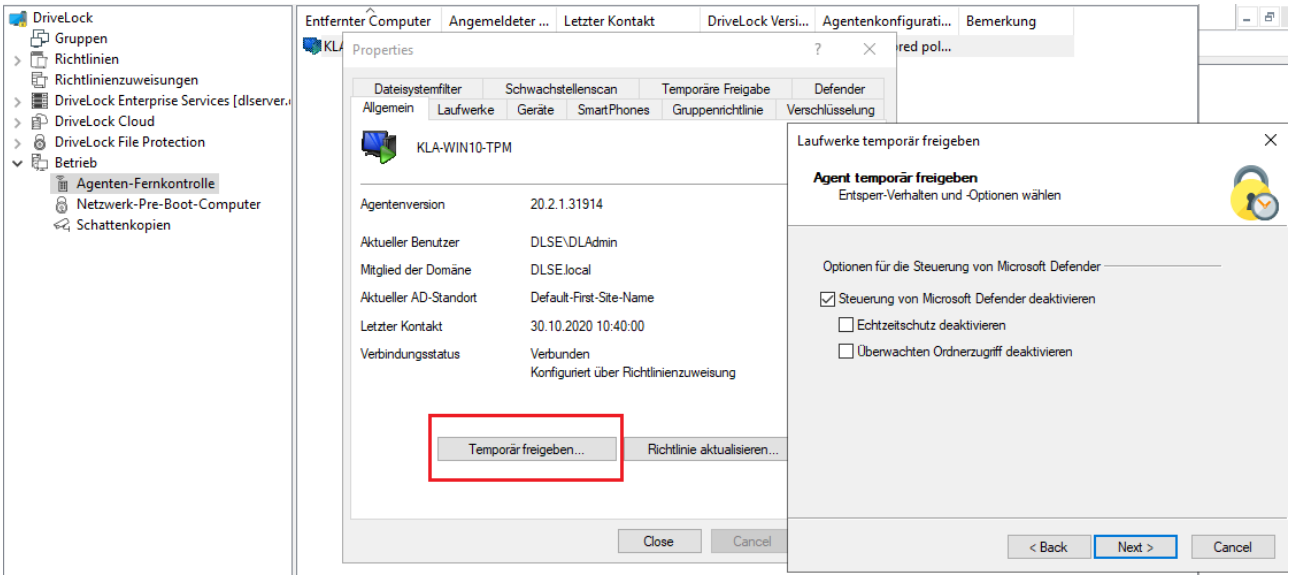
Hinweis: Allgemeine Informationen zur temporären Freigabe von Agenten finden Sie im Administrationshandbuch unter DriveLock Online Help.

3.2.1 Steuerung von Microsoft Defender deaktivieren

Gehen Sie folgendermaßen vor:

1. Wählen Sie den DriveLock Agenten aus, auf dem Sie die Defender Steuerung deaktivieren wollen.
2. Öffnen Sie den Freigabeassistenten über die Schaltfläche **Temporär freigeben**.
3. Klicken Sie **Weiter** bis Sie zu den Defender Optionen gelangen.
4. Deaktivieren Sie die Steuerung für Microsoft Defender wie unten abgebildet. Sie können dabei auch gezielt den Echtzeitschutz oder den überwachten Ordnerschutz deaktivieren.
5. Geben Sie auf der letzten Dialogseite an, wie lange die Freigabe dauern soll und klicken Sie dann **Fertigstellen**.

Hinweis: Sobald die temporäre Freigabe beendet ist, wendet DriveLock wieder die auf den Agenten zugewiesene Richtlinie an. Je nach Konfiguration kann dies jedoch bedeuten, dass manuelle Änderungen rückgängig gemacht werden.



3.2.2 Deaktivierung auf dem DriveLock Agenten

Wenn Sie in Ihrer Richtlinie die Agenten-Benutzeroberfläche entsprechend konfiguriert haben, so dass der Benutzer die temporäre SB-Freigabe verwenden darf, kann auch hier die Steuerung von Microsoft Defender temporär deaktiviert werden.

Hinweis: Weitere Informationen zur Konfiguration der Agenten-Benutzeroberfläche bzw. der SB-Freigabe finden Sie ebenfalls im Administrationshandbuch.

4 Ereignisse

4.1 Statusbericht und Ereignisse

Der DriveLock Agent sendet regelmäßig den aktuellen Defender Status an den DriveLock Enterprise Service (DES). Der Status umfasst Informationen wie Versionsnummern der Definitionen, letzte Scanzeiten und gefundene Bedrohungen.

Der Status wird nach dem Start des Dienstes und danach alle 24 Stunden gesendet. Zusätzlich passiert das auch nach Konfigurationsänderungen, nach dem Aktualisieren des Microsoft Defenders und beim Auftreten der Bedrohungen.

> Hinweis: Der Status wird immer gesendet, unabhängig davon, ob die Option **Steuerung von Microsoft Defender aktivieren/deaktivieren** gesetzt ist oder nicht.

4.2 Microsoft Defender-Ereignisse

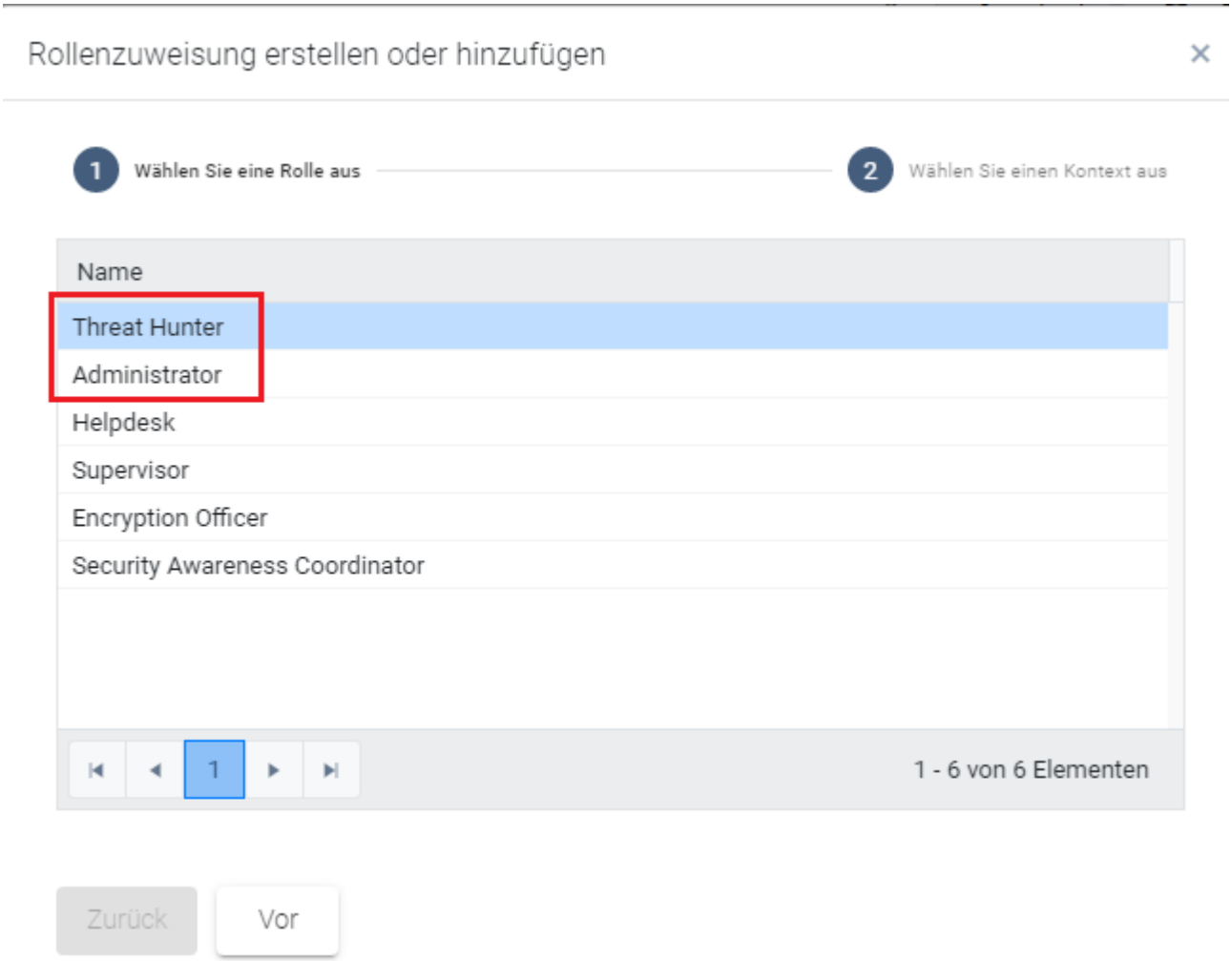
Der DriveLock Enterprise Service (DES) generiert spezielle Ereignisse für Defender. Ob diese Ereignisse an den DES gesendet und im DriveLock Operations Center (DOC) angezeigt werden, legen Sie in der Richtlinie im Knoten **EDR**, Unterknoten **Ereignisse** und dann **Microsoft Defender** in der Spalte **DriveLock Enterprise Service** fest.

Eine vollständige Liste aller DriveLock Ereignisse können Sie in der entsprechenden Dokumentation auf DriveLock OnlineHelp einsehen.

5 Microsoft Defender Management im DOC

Im DriveLock Operations Center (DOC) wird der Status des Microsoft Defender auf den Agenten in der **Microsoft Defender**-Ansicht angezeigt. Weitere Informationen zum DOC finden Sie in der **DriveLock Control Center** Dokumentation auf DriveLock OnlineHelp.

Um die Microsoft Defender-Ansicht sehen zu können, benötigen Sie die Administrator- oder Threat Hunter-Rolle (s. Abbildung).



Das DOC Dashboard zeigt den Microsoft Defender-Status mit verschiedenen Widgets ebenfalls an. Falls das Microsoft Defender-Dashboard nicht automatisch angezeigt wird, können Sie es über die entsprechende Vorlage hinzufügen.

5.1 Dashboard

Erläuterung der Widgets auf dem Standard Microsoft Defender-Dashboard:

- **Schutz-Status** zeigt den aktuellen Status der Computer
  - Offene Bedrohungen
    Anzahl der Computer, die offene Bedrohungen aufweisen, die nicht vom Microsoft Defender entfernt werden konnten
  - Signaturen oder Status nicht aktuell
    Anzahl der Computer, die keine offenen Bedrohungen haben, deren Microsoft Defender Signatur-Definitionen aktualisiert wurden und deren letzte Statusmeldung nicht länger als 1 Woche zurückliegt
  - Geschützt
    Anzahl der Computer, deren Microsoft Defender Signatur-Definitionen älter als 1 Woche sind oder deren letzte Statusmeldung länger als 1 Woche zurückliegt
  - Inaktiv
    Anzahl der Computer, auf denen Microsoft Defender Service nicht läuft
- **Service-Übersicht** zeigt die Anzahl der Computer an, auf denen der Windows Defender Antimalware Service bzw. Windows Defender Antivirus Network Inspection Service laufen.
- **Feature-Übersicht**
  Zeigt die Anzahl der Computer an, auf denen die einzelnen Microsoft Defender-Features aktiviert sind.
- **Bedrohungen nach Schweregrad**
  Zeigt alle aufgetretenen Bedrohungen an und gruppiert sie nach Schweregrad. Es wird nicht unterschieden, ob die Bedrohung bereits behoben oder noch offen ist.
- **Bedrohungen nach Kategorie**
  Zeigt alle aufgetretenen Bedrohungen an und gruppiert sie nach Kategorie. Es wird nicht unterschieden, ob die Bedrohung bereits behoben oder noch offen ist.
- **Microsoft Defender-Status** gibt einen Überblick über den Status von Microsoft Defender auf den Computern:
  - Nicht gesetzt: Der Status wurde bisher nicht gemeldet
  - Aktiv
  - Teilweise aktiv: Eine oder mehrere Microsoft Defender-Komponenten werden

nicht ausgeführt, z.B. Echtzeitschutz

- Inaktiv: Der Microsoft Defender Service läuft nicht

- **Verlauf nach Anzahl**
  Zeigt den Verlauf der betroffenen Computer nach Anzahl an
- **Verlauf der Bedrohungen nach Schweregrad**
  Zeigt den Verlauf der Bedrohungen nach Schweregrad an
- **Verlauf der Bedrohungen nach Kategorie**
  Zeigt den Verlauf der Bedrohungen nach Kategorie an

5.2 Ansicht

Als vorkonfigurierte Ansicht wird standardmäßig **Offene Bedrohungen** aus der Liste **Computer** geöffnet.

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

1. **Computer**
   Im Bereich Computer werden entsprechend der gewählten Ansicht die jeweiligen betroffenen Computer angezeigt.
   Beispielsweise zeigt die vorkonfigurierte Ansicht **Aktivierbare Features** die Anzahl der Computer an, auf denen Microsoft Defender Features vorhanden, aber nicht aktiv sind. Aktivierbare Features sind der Zugriffsschutz, Echtzeitschutz, Verhaltensschutz und Manipulationsschutz. Dabei wird berücksichtigt, ob das entsprechende Feature überhaupt vorhanden ist. Z.B. ist der Manipulationsschutz erst ab Windows 10 1903 vorhanden.

   Durch Klick auf  können Sie sich die Detailansicht für jeden Computer einblenden lassen, die sich aus verschiedenen Blöcken zusammensetzt:
   - **Computer-Gesamtstatus** gibt einen Überblick über den Status des Microsoft Defender, wie z.B. Versionsnummern, vorhandene Features und Services und das letzte Aktualisierungsdatum. In dieser Ansicht sind diejenigen Zeilen rot unterlegt, die auf ein Problem hindeuten.

- **Offene/ Behobene/ Unterdrückte Bedrohungen**
  Je nach Status der vorhandenen Bedrohungen werden sie unter offenen, behobenen oder unterdrückten Bedrohungen angezeigt. Bei den offenen Bedrohungen haben Sie die Möglichkeit, diese für den für den gewählten oder für alle Computer zu unterdrücken.
  Der Link **Enzyklopädie öffnen** führt Sie zu einer Informations-Seite von Microsoft, auf der Sie weitergehende Informationen zu der Bedrohung bekommen.
  Der Link **Details zur Bedrohung anzeigen** öffnet die Detailansicht zu dieser Bedrohung auf dem Computer, in der Sie sehen können welche Dateien betroffen sind oder wann die Bedrohung gefunden wurde.

- **Eigenschaften**
  Die Eigenschaften beinhalten allgemeine Betriebssystem-Informationen und den detaillierten Status des Microsoft Defenders, so wie er z.B. über das Powershell-Befehl Get-MpComputerStatus auf einem Computer ausgegeben wird.
  Die Zeile Letzte Aktualisierung zeigt an, wann der DES zum letzten Mal einen Status vom Agenten bekommen hat.

2. **Erkannte Bedrohungen**
   Hier können Sie auswählen, nach welcher Gruppierung die erkannten Bedrohungen angezeigt werden (nach Kategorie oder nach Schweregrad) oder ob alle unterdrückten Bedrohungen als vorkonfigurierte Ansicht angezeigt werden.

3. **Details zu erkannten Bedrohungen**
   Jede Bedrohung kann mehrfach auf dem gleichen Computer auftreten, z.B. in verschiedenen Verzeichnissen, auf verschiedenen USB Sticks oder mehrfach hintereinander. Die in der Liste angezeigten Elemente entsprechen dem Auftreten einer Bedrohung auf einem Computer. Es ist also möglich, dass mehrere Zeilen den gleichen Computer mit gleicher Bedrohung enthalten.
   In der Detailansicht werden betroffene Dateien und die Eigenschaften der Bedrohung angezeigt. In den Eigenschaften sieht man u.a. den Status der Bedrohung und wann die letzte Defender Aktion stattgefunden hat.

6 Fehlerbehebung

Bei aktiviertem Tracing werden folgende Protokolldateien auf dem Agenten erstellt:

- DlSvcDefender.log
- DES.log

Es ist möglich, den letzten Status, den der Agent an den DES geschickt hat, sich zusätzlich in eine Datei speichern zu lassen. Dafür muss Tracing aktiviert sein und folgender Registryschlüssel auf dem Agenten gesetzt werden:

- Registryschlüssel: `HKLM\Software\CenterTools\TraceLog`
- DWORD-Wert: DlSvcDefender_LogStatus
- Im Trace-Verzeichnis wird dann die Datei **DefenderStatus.json** abgespeichert.

Copyright