Kaseya 2

Endpoint Security

Benutzerhandbuch

Versión 7.0

Deutsch

September 15, 2014

Agreement

The purchase and use of all Software and Services is subject to the Agreement as defined in Kaseya's "Click-Accept" EULATOS as updated from time to time by Kaseya at http://www.kaseya.com/legal.aspx. If Customer does not agree with the Agreement, please do not install, use or purchase any Software and Services from Kaseya as continued use of the Software or Services indicates Customer's acceptance of the Agreement."

Inhalt

Willkommen **1**
Sicherheit – Übersicht **1**
Endpoint Security-Modulanforderungen **4**
Dashboard **4**
Sicherheitsstatus **5**
    Resident Shield durch Agent-Verfahren aktivieren/deaktivieren **8**
Manuelle Aktualisierung **9**
Scan planen **11**
Bedrohungen anzeigen **12**
Protokolle anzeigen **14**
Erweitern/Zurück **15**
Benachrichtigen **16**
Installation: Sicherheit **17**
    Installation oder Aktualisierung eines Endpunktes **21**
    Installationsoptionen **22**
Profil definieren **23**
Profil zuweisen **31**
Protokolleinstellungen: Sicherheit **32**
Exchange-Status **33**
Alarm-Sets definieren **34**
Alarm-Sets anwenden **35**
Sicherheitsberichte **37**
    Executive Summary – Endpunktsicherheit **37**
    Sicherheit – Konfiguration **38**
    Sicherheit – Aktuelle Bedrohungen **38**
    Sicherheit – Historische Bedrohungen **39**
    Sicherheit – KES-Protokoll **39**
Inhaltsverzeichnis **41**

Willkommen

Endpoint Security-Online-Benutzerhilfe

Bitte beachten Sie die folgenden Punkte beim Navigieren in der Online-Hilfe:

- Stellen Sie sicher, dass in Internet Explorer die Einstellungen für Cookies akzeptieren und JavaScript aktiviert sind.
- Klicken Sie auf  , um kontextspezifische Hilfe für die gegenwärtig ausgewählte Funktion anzuzeigen.

Dokumentation

Sie können eine PDF-Version der folgenden Dokumente herunterladen. Zum Anzeigen der PDF-Dateien muss Acrobat Reader auf Ihrem System installiert sein.

Endpoint Security Benutzerhandbuch *(http://help.kaseya.com/webhelp/DE/KES/7000000/DE_kesguide70.pdf#zoom=70&navpanes=0)*	Weist denselben Inhalt auf wie die Online-Hilfe für Endpoint Security.
Versionsanmerkungen *(http://help.kaseya.com/webhelp/DE/RN/7000000/index.asp#KESReleaseNotes.htm)*	Überblick über die Versionsänderungen in Endpoint Security

Siehe **Online-Hilfen und Benutzerhandbücher für andere Produkte** *(http://help.kaseya.com/WebHelp/DE/doc/7000000/index.asp#home.htm)*.

Diese 7.0Version der Online-Hilfe für Endpoint Security wurde am 9/15/2014 generiert.

Sicherheit – Übersicht

Endpoint Security (KES) bietet unter Verwendung der voll integrierten Anti-Malware-Technologie von AVG Technologies Sicherheitsschutz für verwaltete Rechner. Der Begriff **Malware** umfasst Viren, Spyware, Adware und andere Arten unerwünschter Programme. **Endpoint Security** desinfiziert oder entfernt infizierte Dateien und andere Bedrohungen wie Trojaner, Würmer und Spyware automatisch. **Endpoint Security** überwacht ununterbrochen den Sicherheitsstatus aller Windows-Server, -Workstations und -Notebooks, auf denen der Sicherheitsschutz installiert ist. Alarme können durch Ereignisse bezüglich des Sicherheitsschutzes ausgelöst werden und können das Senden von E-Mail-Benachrichtigungen, Ausführen von Verfahren und Erstellen von Job-Tickets einschließen.

Zentral verwaltete Sicherheitsprofile werden definiert und über die VSA-Konsolenoberfläche auf den verwalteten Rechnern bereitgestellt. Die an einem Sicherheitsprofil vorgenommenen Änderungen werden automatisch auf alle Rechner mit diesem Profil angewendet. **Endpoint Security** wird mit einem vordefinierten Standard-Sicherheitsprofil geliefert. Darüber hinaus können Sie Ihre eigenen Sicherheitsprofile erstellen.

Alle Sicherheitsschutz-Ereignisse werden im System gespeichert und stehen für eine ausführende Zusammenfassung und detaillierte Managementberichte zur Verfügung. Nach der Bereitstellung werden Aktualisierungen automatisch auf geplanter Basis und ohne Benutzereingriff verarbeitet.

Antivirenschutz

Basierend auf dem Sicherheitsprofil entfernt **Endpoint Security** infizierte Dateien oder blockiert den Zugriff darauf:

- **Scannt die Systemregistrierung** auf verdächtige Einträge, temporäre Internetdateien, Verfolgungs-Cookies und sonstige Arten unerwünschter Objekte.
- **Ermittelt Computerviren** unter Verwendung der folgenden Methoden:
  - **Scannen** – Führt Scanvorgänge sowohl beim Zugriff als auch nach Bedarf aus.
  - **Heuristische Analyse** – Emuliert dynamisch die Anweisungen eines gescannten Objekts in einer virtuellen Computing-Umgebung.
  - **Generische Ermittlung** – Ermittelt Anweisungsmerkmale eines Virus oder einer Virusgruppe.
  - **Ermittlung bekannter Viren** – Sucht nach Zeichenfolgenmerkmalen eines Virus.
- **E-Mail-Scans** – Überprüft ein- und ausgehende E-Mail-Nachrichten mithilfe von Plugins für die gängigsten E-Mail-Programme. Dateien mit Viren werden sofort nach ihrer Erkennung desinfiziert oder unter Quarantäne gestellt. Manche E-Mail-Clients unterstützen Nachrichten mit Text, der bestätigt, dass gesendete und empfangene E-Mail auf Viren gescannt wurde. Darüber hinaus kann der Anhangsfilter durch Definieren unerwünschter oder verdächtiger Dateien eingestellt werden, um die Arbeit mit E-Mail noch weiter abzusichern.
- **Speicherresidenter Schutz** – Scannt Dateien, während sie kopiert, geöffnet oder gespeichert werden. Wenn ein Virus entdeckt wird, wird der Dateizugriff angehalten und dem Virus nicht gestattet, sich zu aktivieren. Der speicherresidente Schutz wird während des Systemstarts in den Speicher des Computers geladen und bietet wichtigen Schutz für die Systembereiche des Computers.
- **Scans nach Bedarf** – Scans können nach Bedarf oder zeitplanmäßig und periodisch ausgeführt werden, wann immer es in den Arbeitsablauf passt.
- **Scans von MS Exchange-Servern** – Scannt ein- und ausgehende E-Mail-Nachrichten und Posteingangsordner auf Bedrohungen durch Viren/Spyware/Malware und löscht diese sofort, bevor E-Mail-Empfänger des MS Exchange-Servers infiziert werden.
- **Scans von Websites und Downloads** – Scannt Websites und Website-Links. Auf Ihren Computer heruntergeladene Dateien werden ebenfalls gescannt. Bietet eine Sicherheitsbewertung für Links, die von gängigen Suchengines ausgegeben werden.
- **ID-Schutz** – Verwendet "Verhaltensanalyse", um verdächtige Aktivitäten auf einem Rechner zu ermitteln, und verhindert so den gezielten Diebstahl von Passwörtern, Bankkontodetails, Kreditkartennummern und sonstigen digitalen Wertsachen.

Anti-Spyware

Spyware ist Software, die ohne Wissen oder Erlaubnis des Benutzers Informationen von einem Computer abruft. Manche Spyware-Anwendungen können heimlich installiert werden und enthalten häufig Werbung, Fenster-Popups oder sonstige Arten unangenehmer Software. Gegenwärtig stellen Websites mit potenziell schädlichem Inhalt die häufigste Infektionsquelle dar. Zu anderen Ansteckungsherden gehören E-Mail-Nachrichten oder die Übertragung durch Würmer oder Viren. Der wichtigste Schutz gegen Spyware besteht in einem **speicherresidenten Schutzschild** wie beispielsweise der technologisch ausgereiften **Endpoint Security**-Spyware-Komponente. Ein speicherresidenter Schutzschild scannt Anwendungen im Hintergrund, während sie ausgeführt werden. Der Anti-Spyware-Schutz von **Endpoint Security** erkennt Spyware, Adware, DLL-Trojaner, Keylogger, in Datenströmen und Archiven verborgene Malware, Spyware-Einträge in der Windows-Registrierung und andere Arten unerwünschter Objekte.

> **Hinweis:** Siehe Endpoint Security-Systemanforderungen.

Endpoint Security-Lizenzierung

Jede MSE-KES-Arbeitsplatzlizenz gestattet dem Kunden die Installation und zeitlich unbefristete Nutzung eines MSE-KES-Agents. Außerdem erhält er Aktualisierungen als Abonnement mit einer Laufzeit von jeweils 365 aufeinander folgenden Tagen. Das Aktualisierungsabonnement läuft unabhängig für jeden Arbeitsplatz und beginnt am Datum der Installation des MSE-KES-Agents auf dem jeweiligen Rechner. Dieser Arbeitsplatz erhält die während der Abonnementslaufzeit veröffentlichten KES-Aktualisierungen. Alle während der Abonnementslaufzeit veröffentlichten

Aktualisierungen werden ebenfalls zeitlich unbefristet lizenziert. Wenn das Abonnement abläuft bzw. nicht erneuert wird, erlischt der Anspruch auf neue KES-Aktualisierungen.

Bei Ausgabe einer neuen Arbeitsplatzlizenz an einen Rechner mit einer vorhandenen Subskriptionsperiode werden die Perioden zusammengelegt und weitere 365 Tage zu der verbleibenden Subskriptionsperiode auf dem Arbeitsplatz hinzugefügt. Beim Übertragen einer solchen zusammengelegten Periode auf einen neuen Rechner werden alle restlichen Tage für beide vorherigen Arbeitsplätze übertragen.

Für jeden geschützten Rechner und/oder Exchange-Posteingang muss die entsprechende KES-Arbeitsplatzlizenz erworben werden. Der Kunde darf MSE-KES nur auf einem Rechner bereitstellen, der über eine gültige VSA-Lizenz verfügt. MSE-KES-Lizenzen können über die Webbenutzeroberfläche von Kaseya zentral verwaltet werden. Die Lizenzierung wird durchgesetzt, und für jedes benutzte Postfach ist eine Lizenz erforderlich.

Hinweis: KES-Lizenzen werden Gruppen-IDs über 'System > **Lizenzmanager** *(http://help.kaseya.com/webhelp/DE/VSA/7000000/index.asp#2924.htm)*' zugeordnet.

Funktionen	Beschreibung
Dashboard *(siehe 4)*	Zeigt eine Dashboard-Ansicht des Status aller Rechner, auf denen Endpoint Security installiert ist.
Sicherheitsstatus *(siehe 11)*	Zeigt den aktuellen Sicherheitsstatus von Rechner-IDs an.
Manuelle Aktualisierung *(siehe 9)*	Plant Aktualisierungen der neuesten Version der Definitionsdateien für den Sicherheitsschutz.
Scan planen *(siehe 11)*	Plant Sicherheitsschutz-Scans von Rechner-IDs.
Bedrohungen anzeigen *(siehe 12)*	Listet Dateien auf, die wegen einer verdächtigten oder bestätigten Bedrohung in Quarantäne gestellt wurden.
Protokolle anzeigen *(siehe 14)*	Zeigt das Ereignisprotokoll des Sicherheitsschutzes von Rechner-IDs an.
Erweitern/Zurück *(siehe 15)*	Verlängert die Anzahl der jährlichen Lizenzen für ausgewählte Rechner-IDs oder gibt diese zurück.
Benachrichtigen *(siehe 16)*	Ermöglicht die automatische Benachrichtigung über den Ablauf von Endpoint Security-Lizenzen.
Installation *(siehe 17)*	Installiert oder entfernt den Sicherheitsschutz für Rechner-IDs.
Profil definieren *(siehe 23)*	Verwaltet Sicherheitsprofile. Jedes Sicherheitsprofil stellt einen unterschiedlichen Satz an aktivierten oder deaktivierten Sicherheitsoptionen dar.
Profil zuweisen *(siehe 31)*	Weist Rechner-IDs Sicherheitsprofile zu.
Protokolleinstellungen *(siehe 32)*	Gibt an, für wie viele Tage die Protokolldaten des Sicherheitsschutzes aufbewahrt werden sollen.
Exchange-Status *(siehe 33)*	Zeigt den Status des E-Mail-Schutzes auf MS Exchange-Servern an, auf denen Endpoint Security installiert ist.
Alarm-Sets definieren *(siehe 34)*	Auf der Seite 'Alarmsätze anwenden' können Sie Sätze von Meldungsbedingungen definieren, bei deren Eintreten Meldungen ausgesendet werden.
Alarm-Sets anwenden *(siehe 35)*	Erstellt Alarme als Reaktion auf Sicherheitsschutz-Ereignisse.

Endpoint Security-Modulanforderungen

Kaseya Server

- Das Endpoint Security 7.0-Modul setzt VSA 7.0 voraus.
- Zugriff auf `http://download.avg.com`

Anforderungen für verwaltete Rechner

- 256 MB RAM
- 60 MB freier Plattenspeicherplatz
- Microsoft Windows Server 2003, 2003 R2, 2008, 2008 R2, 2012, 2012 R2
- Microsoft Windows XP, Vista, 7, 8, 8.1

Hinweis: Siehe allgemeine **Systemanforderungen** *(http://help.kaseya.com/webhelp/DE/VSA/7000000/reqs/index.asp#home.htm).*

Dashboard

Sicherheit > Dashboard

- Ähnliche Informationen werden über 'Info Center > Berichterstellung > Berichte > Sicherheit' bereitgestellt.

Die Seite **Dashboard** bietet eine Dashboard-Ansicht des Status von Rechnern, auf denen **Endpoint Security** installiert ist.

- **Antivirus-Statistik**
- **Lizenzstatus**
- **Lizenzanzahl**
- **Am meisten bedrohte Rechner**
- **Höchste Bedrohungen erkannt**

Hinweis: Die Liste der angezeigten Rechner-IDs ist abhängig vom Rechner-ID-/Gruppen-ID-Filter und den Rechnergruppen, zu deren Anzeige der Benutzer über System > Benutzersicherheit > Scopes autorisiert ist.

Antivirus-Statistik

Der Abschnitt **Endpunkt-Sicherheitsstatistik** bietet verschiedene Statistiken zum Sicherheitsstatus von Endpunkten und zum Status der Sicherheitsdefinitionen.

- <N> Endpunkte müssen neu gestartet werden
- <N> Signaturversionen älter als '<Version>'
- <N> Endpunkte mit älteren **Endpoint Security**-Versionen
- <N> Endpunkte, die in dieser Woche nicht gescannt wurden
- <N> Endpunkte mit aktueller Scan-Ausführung
- <N> Endpunkte mit deaktiviertem Resident Shield

Klicken Sie auf eine dieser mit Hyperlinks versehenen Statistiken, um ein Dialogfeld mit Registerkarten einzublenden, das jedes zu dieser Statistik gehörende Mitglied zeigt.

Lizenzstatus

Ein Kreisdiagramm zeigt den Prozentsatz der Rechner an, deren Lizenzen abgelaufen sind oder in 30, 60, 90 oder 91+ Tagen ablaufen werden. Klicken Sie auf ein Segment oder eine Bezeichnung des Kreisdiagramms, um eine Liste der einzelnen Rechner anzuzeigen, die zu diesem Segment gehören.

Lizenzanzahl

Zeigt die Lizenzanzahl wie folgt an:

- Erworbene Lizenzen
- Voll verfügbare Lizenzen (erworbene Lizenzen, die weder zugewiesen noch installiert noch abgelaufen sind)
- Zugewiesene Lizenzen (Installation geplant, doch die Installation ist noch nicht abgeschlossen)
- Angewendete Lizenzen (auf einem Rechner angewendete aktive Lizenz)
- Teilweise verfügbare Lizenzen (zuvor einem Rechner zugewiesen, doch vor Ablauf an den Pool zurückgegeben)
- Teilweise zugewiesene Lizenzen (teilweise verfügbar und Installation geplant, doch die Installation ist noch nicht abgeschlossen)
- Gesamtzahl der Lizenzen (erworbene Lizenzen abzüglich der abgelaufenen)
- Abgelaufene Lizenzen

Am meisten bedrohte Rechner

Listet die Rechner mit der höchsten Anzahl von aktuellen Bedrohungen auf. Die Anzahl der unter Quarantäne gestellten Bedrohungen wird ebenfalls aufgeführt. Klicken Sie auf den Hyperlink einer Rechner-ID, um deren Bedrohungen auf der Seite **Bedrohungen anzeigen** *(siehe 12)* anzuzeigen.

Höchste Bedrohungen erkannt

Ein Kreisdiagramm zeigt an, welche Bedrohungen auf dem höchsten Prozentsatz von Rechnern gefunden wurden. Klicken Sie auf ein Segment oder eine Bezeichnung des Kreisdiagramms, um auf der Seite **Bedrohungen anzeigen** eine Liste der einzelnen Rechner anzuzeigen, die zu diesem Segment gehören.

Sicherheitsstatus

Sicherheit > Sicherheitsstatus

- Ähnliche Informationen werden über 'Info Center > Berichterstellung > Berichte > Sicherheit *(siehe 38)*' bereitgestellt.

Auf der Seite **Sicherheitsstatus** wird der aktuelle Sicherheitsstatus der einzelnen Rechner-IDs angezeigt, die über eine **Endpoint Security**-Lizenz verfügen. Die Liste der angezeigten Rechner-IDs ist abhängig vom Rechner-ID-/Gruppen-ID-Filter und den Rechnergruppen, zu deren Anzeige der Benutzer über System > Benutzersicherheit > Scopes autorisiert ist. Damit Rechner-IDs auf dieser Seite angezeigt werden, muss die **Endpoint Security**-Client-Software über die Seite 'Sicherheit > **Installation** *(siehe 17)*' auf dem verwalteten Rechner installiert worden sein.

Indikatoren umfassen den Resident Shield-Schutz, E-Mail-Schutz, die Anzahl der erkannten unbeseitigten Bedrohungen, die Anzahl der unter Quarantäne gestellten Bedrohungen und die Version des auf den einzelnen Rechner-IDs installierten Sicherheitsschutzes.

Aktionen

- **Resident Shield aktivieren** – Klicken Sie, um den speicherresidenten Anti-Malware-Schutz auf ausgewählten Rechner-IDs zu aktivieren.
- **Resident Shield deaktivieren** – Klicken Sie, um den speicherresidenten Anti-Malware-Schutz auf ausgewählten Rechner-IDs zu deaktivieren.

> **Hinweis:** In manchen Fällen muss der Sicherheitsschutz deaktiviert werden, um Software auf einem verwalteten Rechner zu installieren oder zu konfigurieren.

> Hinweis: Sie können alternativ den **Resident Shield mit einem Agent-Verfahren aktivieren/deaktivieren** *(siehe 8)*.

- **E-Mail-Schutz aktivieren** – Klicken Sie, um den E-Mail-Schutz auf ausgewählten Rechner-IDs zu aktivieren.
- **E-Mail-Schutz deaktivieren** – Klicken Sie, um den E-Mail-Schutz auf ausgewählten Rechner-IDs zu deaktivieren.
- **Tresor leeren** – Klicken Sie, um alle in Quarantäne gestellten Malware-IDs aus dem Virustresor zu löschen.
- **Jetzt neu starten** – Startet ausgewählte Rechner-IDs neu. Manche Sicherheitsaktualisierungen erfordern einen Neustart, um installiert zu werden. Bei einem anstehenden Neustart wird ein Neustart-Symbol neben der vor der Aktualisierung liegenden Versionsnummer angezeigt. Der Rechner ist weiterhin geschützt.

Kopfzeileninformationen

- **Aktuell verfügbare Signatur-Version** – Die neueste verfügbare Version des Sicherheitsschutzes. Über 'Sicherheit > **Manuelle Aktualisierungen** *(siehe 35)*' können Sie eine oder mehrere Rechner-IDs mit der **aktuell verfügbaren Version** aktualisieren.
- **Aktuelle Version des Installationsprogramms** – Die Versionsnummer des AVG-Installationsprogramms, das bei neuen Installationen verwendet werden sollte.

Tabellenspalten

- **Check-in-Symbole** – Diese Symbole geben den Agent-Anmeldestatus jedes verwalteten Rechners an. Wenn Sie den Cursor über ein Anmeldesymbol bewegen, wird das Agent-Schnellansichtsfenster angezeigt.
  - Online, aber in Wartestellung bis zum Abschluss des ersten Audits
  - Agent online
  - Agent online und Benutzer gegenwärtig angemeldet.
  - Agent online und Benutzer gegenwärtig angemeldet, doch Benutzer seit mehr als 10 Minuten nicht aktiv
  - Agent ist gegenwärtig offline
  - Agent hat nie eingecheckt.
  - Agent ist online, aber die Fernsteuerung wurde deaktiviert.
  - Agent wurde ausgesetzt.
- **(Kontrollkästchen 'Alle auswählen')** – Klicken Sie auf dieses Kontrollkästchen, um alle Zeilen im Seitenbereich auszuwählen. Falls das Kontrollkästchen aktiviert ist, klicken Sie auf dieses Kontrollkästchen, um die Auswahl aller Zeilen im Seitenbereich aufzuheben.
- **Rechner.Gruppen-ID** – Ein eindeutiger Rechner-ID/Gruppen-ID-/Organisations-ID-Name für einen Rechner im VSA.
- **Profilname** – Das der Rechner-ID zugewiesene Sicherheitsprofil
- **Status** – Der aktuelle Status des Sicherheitsschutzes einer Rechner-ID wird durch den Satz der in der Spalte **Status** angezeigten Statussymbole angegeben. Dies sind die möglichen Statussymbole:


Resident Shield Ein


Resident Shield Aus


Resident Shield teilweise


Resident Shield-Aktivierung/-Deaktivierung anstehend


E-Mail-Scanner Ein


E-Mail-Scanner Aus


E-Mail-Scanner teilweise


E-Mail-Scanner-Aktivierung/-Deaktivierung anstehend


Link-Scanner Ein


Link-Scanner Aus


Link-Scanner teilweise


Link-Scanner-Aktivierung/-Deaktivierung anstehend


Web-Shield Ein


Web-Shield Aus


Web-Shield teilweise


Web-Shield-Aktivierung/-Deaktivierung anstehend

- **Bedrohungen** – Die Anzahl der nicht beseitigten Bedrohungen auf der Rechner-ID. Dies sind aktuelle Bedrohungen, die die Aufmerksamkeit des Benutzers erfordern. Sie können auf den Hyperlink der Nummer in einer Zeile klicken, um diese Bedrohungen auf der Registerkarte **Aktuelle Bedrohungen** der Seite **Bedrohungen anzeigen** *(siehe 12)* anzuzeigen.
- **Virenquarantäne** – Die Anzahl der auf der Rechner-ID unter Quarantäne gestellten Bedrohungen. Sie stellen keine Gefahr dar und werden, falls die jeweiligen Profileinstellungen darauf zutreffen, automatisch gelöscht. Sie können auf die mit einem Hyperlink verknüpfte Nummer in einer Zeile klicken, um diese Bedrohungen auf der Registerkarte **Virenquarantäne** der Seite **Bedrohungen anzeigen** *(siehe 12)* anzuzeigen.
- **Version** – Die Version des Sicherheitsschutzes, der gegenwärtig auf dieser Rechner-ID verwendet wird. Zum Beispiel: `8.5.322 270.12.6/2084`
  - `8.5.322` – Die Version des installierten AVG-Programms
  - `270.12.6/2084` – Die komplette *Virendatenbankversion*. Dabei ist `270.12.6` die Versionsnummer der *Definition* und `2084` die Versionsnummer der *Signatur*. Dies wird in rotem Text angezeigt, wenn die *Signatur*version älter als die letzten 5 verfügbaren *Signatur*versionen oder die *Definitions*version älter als die letzten 2 verfügbaren *Definitions*versionen und der Agent aktiv ist.

Hinweis: Falls die Version einer Rechner-ID veraltet ist, können Sie sie manuell über 'Sicherheit > **Manuelle Aktualisierung** *(siehe 9)*' aktualisieren.

Hinweis: Die Installation einiger Sicherheitsaktualisierungen erfordert einen Neustart. Bei einem anstehenden Neustart wird ein Neustart-Symbol neben der vor der Aktualisierung liegenden Versionsnummer angezeigt. Der Rechner ist weiterhin geschützt.

Resident Shield durch Agent-Verfahren aktivieren/deaktivieren

Sie können den **Resident Shield** in einem Agent-Verfahren mit **executeShellCommand()** aktivieren/deaktivieren. Führen Sie im **Arbeitsverzeichnis** *(http://help.kaseya.com/webhelp/DE/VSA/7000000/index.asp#368.htm)* des Agents Folgendes aus:

```
C:\kworking\kes>KasAVCmd -setFileMonitorEnable 0   ;disables Resident Shield
C:\kworking\kes>KasAVCmd -setFileMonitorEnable 1   ;enables Resident Shield
```

```
Script Name: KES_Enable Resident Shield
Script Description: Enables Resident Shield temporarily (until next scan or
reboot...unless it is enabled by default and is being re-enabled after being
temporarily disabled)
IF True
THEN
   Get Variable
     Parameter 1 : 10
     Parameter 2 :
     Parameter 3 : agenttemp
         OS Type : 0
   Execute File
     Parameter 1 : #agenttemp#\kes\KasAVCmd.exe
     Parameter 2 : -setFileMonitorEnable 1
     Parameter 3 : 3
         OS Type : 0
ELSE
```

```
Script Name: KES_Disable Resident Shield
Script Description: Disables Resident Shield temporarily (until next scan or
reboot)
IF True
THEN
   Get Variable
     Parameter 1 : 10
     Parameter 2 :
     Parameter 3 : agenttemp
         OS Type : 0
   Execute File
     Parameter 1 : #agenttemp#\kes\KasAVCmd.exe
     Parameter 2 : -setFileMonitorEnable 0
     Parameter 3 : 3
         OS Type : 0
ELSE
```

Manuelle Aktualisierung

Sicherheit > Manuelle Aktualisierung

Auf der Seite **Manuelle Aktualisierungen** können Sie festlegen, wie Rechner-IDs mit **Endpoint Security**-Lizenz auf die neueste verfügbare Version des Sicherheitsschutzes aktualisiert werden. *Aktualisierungen sind standardmäßig für eine automatische Ausführung geplant.* Sie können die automatische Aktualisierung nach Rechner deaktivieren und erneut aktivieren. Normalerweise wird diese Funktion nur zur Überprüfung des Aktualisierungsstatus von Agents oder gegebenenfalls zum Erzwingen einer sofortigen Aktualisierungsüberprüfung verwendet.

Die Liste der auswählbaren Rechner-IDs basiert auf dem Rechner-ID-/Gruppen-ID-Filter und dem verwendeten Scope. Damit Rechner-IDs auf dieser Seite angezeigt werden, muss die **Endpoint Security**-Client-Software über die Seite 'Sicherheit > **Installation** *(siehe 17)*' auf dem verwalteten Rechner installiert worden sein.

Aktionen

- **Aktualisieren** – Klicken Sie, um unter Verwendung der vorher ausgewählten Aktualisierungsoptionen die Aktualisierung einer Virusdefinition auf ausgewählten Rechner-IDs zu planen.
- **Update abbrechen** – Klicken Sie, um eine geplante Aktualisierung abzubrechen.
- **Automatische Aktualisierungen aktivieren** – Aktiviert die Aktualisierung von Virusdefinitionen.
- **Automatische Aktualisierungen deaktivieren** – Deaktiviert die Aktualisierung von Virusdefinitionen. Dies verhindert, dass Aktualisierungen von Virusdefinitionen das Netzwerk während der Hauptarbeitsstunden verlangsamen. In einer zukünftigen Version werden Sie in der Lage sein, den Zeitpunkt der Aktualisierung von Virusdefinitionen zu planen. Wenn automatische Aktualisierungen deaktiviert sind, wird ein rotes Kreuzsymbol in der Spalte **Geplante Zeit** angezeigt, selbst wenn eine manuelle Aktualisierung geplant ist.

Kopfzeileninformationen

- **Aktuell verfügbare Version** – Die neueste verfügbare Version des Sicherheitsschutzes. Markieren Sie die Versionsspalte auf dieser Seite, um zu festzustellen, auf welchen Rechner-IDs die neueste verfügbare Version des Sicherheitsschutzes oder die aktuellste **Endpoint Security**-Client-Software installiert werden muss.

- **Aktuelle KES-Client-Version** – Dies ist die neueste verfügbare KES-Client-Software.

Planeinstellungen

- **Sofort** – Markieren Sie diese Option, um diese Aufgabe sofort auszuführen.
- **Datum/Zeit** – Geben Sie Jahr, Monat, Tag, Stunde und Minute ein, um die Ausführung dieser Aufgabe zeitlich festzulegen.
- **Staffeln um** – Sie können die Last auf das Netzwerk verteilen, indem Sie diese Aufgabe staffeln. Wenn Sie diesen Parameter auf 5 Minuten einstellen, wird die Aufgabe auf jeder Rechner-ID um 5 Minuten versetzt. Beispiel: Rechner 1 läuft um 10:00, Rechner 2 läuft um 10:05, Rechner 3 läuft um 10:10.
- **Überspringen, wenn Rechner offline ist** – Falls ein Häkchen ✓ angezeigt wird und der Rechner offline ist, wird diese Aufgabe übersprungen und zur nächsten geplanten Uhrzeit ausgeführt. Wenn kein Häkchen angezeigt wird, wird diese Aufgabe ausgeführt, sobald der Rechner nach der ursprünglich geplanten Zeit wieder verbunden ist.
- **Aktualisierung über KServer (Dateiquelle ignorieren)** – Ist diese Option aktiviert, werden die Aktualisierungen vom Kaseya Server heruntergeladen. Ist diese Option nicht aktiviert, werden die Aktualisierungen mithilfe der unter 'Patch-Management > **Dateiquelle** *(http://help.kaseya.com/webhelp/DE/VSA/7000000/index.asp#366.htm)*' angegebenen Methode heruntergeladen.

Tabellenspalten

- **Check-in-Status** – Diese Symbole geben den Agent-Anmeldestatus jedes verwalteten Rechners an. Wenn Sie den Cursor über ein Anmeldesymbol bewegen, wird das Agent-Schnellansichtsfenster angezeigt.
  - Online, aber in Wartestellung bis zum Abschluss des ersten Audits
  - Agent online
  - Agent online und Benutzer gegenwärtig angemeldet.
  - Agent online und Benutzer gegenwärtig angemeldet, doch Benutzer seit mehr als 10 Minuten nicht aktiv
  - Agent ist gegenwärtig offline
  - Agent hat nie eingecheckt.
  - Agent ist online, aber die Fernsteuerung wurde deaktiviert.
  - Agent wurde ausgesetzt.
- **(Kontrollkästchen 'Alle auswählen')** – Klicken Sie auf dieses Kontrollkästchen, um alle Zeilen im Seitenbereich auszuwählen. Falls das Kontrollkästchen aktiviert ist, klicken Sie auf dieses Kontrollkästchen, um die Auswahl aller Zeilen im Seitenbereich aufzuheben.
- **Rechner.Gruppen-ID** – Ein eindeutiger Rechner-ID/Gruppen-ID-/Organisations-ID-Name für einen Rechner im VSA.
- **Quelle** – Wenn unter 'Patch-Management > Dateiquelle' eine Dateiquelle definiert ist, werden die Aktualisierungen von diesem Speicherort heruntergeladen. Ansonsten werden sie aus dem Internet geladen. Wenn die Option **Aus dem Internet herunterladen, wenn der Rechner keine Verbindung zum Dateiserver herstellen kann** unter 'Patch-Management > Dateiquelle' ausgewählt wurde:
  - Falls während der Installation eines **Endpoint Security** v2.x-Endpunktes die Dateiquelle ausgefallen ist oder die Anmeldedaten ungültig sind, wird das Installationsprogramm vom Kaseya Server heruntergeladen. Das Installationsprogramm schließt dann die Endpunktinstallation ab.
  - Falls während einer manuellen **Endpoint Security** v2.x-Aktualisierung die Dateiquelle ausgefallen ist oder die Anmeldedaten ungültig sind, wird das Update aus dem Internet heruntergeladen.

  In den beiden oben genannten Fällen weist die Seite **Protokolle anzeigen** *(siehe 14)* in einer Fehlermeldung darauf hin, warum das Herunterladen von der Dateiquelle fehlgeschlagen ist und dass nun das Herunterladen aus dem Internet versucht wird.

- **Letztes Update** – Dieser Zeitstempel zeigt, wann die Rechner-ID zuletzt aktualisiert wurde. Wenn sich dieses Datum ändert, steht ein neues Update zur Verfügung.
- **Version** – Die Version des Sicherheitsschutzes, der gegenwärtig auf dieser Rechner-ID verwendet wird. Zum Beispiel: `8.5.322 270.12.6/2084`
  - `8.5.322` – Die Version des installierten AVG-Programms
  - `270.12.6/2084` – Die komplette *Virendatenbankversion*. Dabei ist `270.12.6` die Versionsnummer der *Definition* und `2084` die Versionsnummer der *Signatur*. Dies wird in rotem Text angezeigt, wenn die *Signatur*version älter als die letzten 5 verfügbaren *Signatur*versionen oder die *Definitions*version älter als die letzten 2 verfügbaren *Definitions*versionen und der Agent aktiv ist.
  - `[KES 2.1.0.87]` – Dies ist die Version der **Endpoint Security**-Client-Software.
- **Geplante Zeit** – Zeitstempel der nächsten geplanten manuellen oder automatischen Aktualisierung, sofern eine solche festgelegt wurde. Bei einem ausgewählten Rechner gilt Folgendes:
  - Wenn für einen ausgewählten Rechner *automatische Aktualisierungen aktiviert sind* und KES eine AVG-Aktualisierung ermittelt, wird ein Zeitstempel angezeigt. Bei einer geplanten Aktualisierung mehrerer Rechner unterscheiden sich die Zeitstempel, da automatische Aktualisierungen einen versetzten Zeitplan verwenden.
  - Falls *automatische Aktualisierungen aktiviert sind*, aber keine AVG-Aktualisierung ermittelt wird, ist die Tabellenzelle leer, es sei denn, es ist auch eine manuelle Aktualisierung geplant.
  - Wenn *automatische Aktualisierungen deaktiviert sind*, wird ein rotes Kreuzsymbol angezeigt, selbst wenn eine manuelle Aktualisierung geplant ist.
  - Wenn eine *manuelle Aktualisierung geplant ist*, wird ein Zeitstempel angezeigt.

Scan planen

Sicherheit > Scan planen

Auf der Seite **Scan planen** werden Sicherheitsschutz-Scans ausgewählter Rechner-IDs mit **Endpoint Security**-Lizenz geplant. Die Liste der auswählbaren Rechner-IDs basiert auf dem Rechner-ID-/Gruppen-ID-Filter und dem verwendeten Scope. Damit Rechner-IDs auf dieser Seite angezeigt werden, muss die **Endpoint Security**-Client-Software über die Seite 'Sicherheit > **Installation** *(siehe 17)*' auf dem verwalteten Rechner installiert worden sein.

Aktionen

- **Scan** – Klicken Sie, um unter Verwendung der vorher ausgewählten Scanoptionen einen Scan der ausgewählten Rechner-IDs zu planen.
- **Abbrechen** – Klicken Sie, um einen geplanten Scan zu löschen.

Planeinstellungen

- **Sofort** – Markieren Sie diese Option, um diese Aufgabe sofort auszuführen.
- **Datum/Zeit** – Geben Sie Jahr, Monat, Tag, Stunde und Minute ein, um die Ausführung dieser Aufgabe zeitlich festzulegen.
- **Staffeln um** – Sie können die Last auf das Netzwerk verteilen, indem Sie diese Aufgabe staffeln. Wenn Sie diesen Parameter auf 5 Minuten einstellen, wird die Aufgabe auf jeder Rechner-ID um 5 Minuten versetzt. Beispiel: Rechner 1 läuft um 10:00, Rechner 2 läuft um 10:05, Rechner 3 läuft um 10:10.
- **Überspringen, wenn Rechner offline ist** – Falls ein Häkchen angezeigt wird und der Rechner offline ist, wird diese Aufgabe übersprungen und zur nächsten geplanten Uhrzeit ausgeführt.

Wenn kein Häkchen angezeigt wird, wird diese Aufgabe ausgeführt, sobald der Rechner nach der ursprünglich geplanten Zeit wieder verbunden ist.

- **Alle N Perioden** – Aktivieren Sie dieses Kontrollkästchen, um diese Aufgabe zu einer wiederholten Aufgabe zu machen. Geben Sie die Anzahl der Perioden ein, die gewartet werden soll, bevor die Aufgabe erneut ausgeführt wird.

Tabellenspalten

- **Check-in-Status** – Diese Symbole geben den Agent-Anmeldestatus jedes verwalteten Rechners an. Wenn Sie den Cursor über ein Anmeldesymbol bewegen, wird das Agent-Schnellansichtsfenster angezeigt.
  - Online, aber in Wartestellung bis zum Abschluss des ersten Audits
  - Agent online
  - Agent online und Benutzer gegenwärtig angemeldet.
  - Agent online und Benutzer gegenwärtig angemeldet, doch Benutzer seit mehr als 10 Minuten nicht aktiv
  - Agent ist gegenwärtig offline
  - Agent hat nie eingecheckt.
  - Agent ist online, aber die Fernsteuerung wurde deaktiviert.
  - Agent wurde ausgesetzt.
- **(Kontrollkästchen 'Alle auswählen')** – Klicken Sie auf dieses Kontrollkästchen, um alle Zeilen im Seitenbereich auszuwählen. Falls das Kontrollkästchen aktiviert ist, klicken Sie auf dieses Kontrollkästchen, um die Auswahl aller Zeilen im Seitenbereich aufzuheben.
- **Rechner.Gruppen-ID** – Ein eindeutiger Rechner-ID/Gruppen-ID-/Organisations-ID-Name für einen Rechner im VSA.
- **Letzter Scan** – Dieser Zeitstempel zeigt, wann der letzte Scan ausgeführt wurde. Wenn sich dieses Datum ändert, können neue Scandaten angezeigt werden.
- **Nächster Scan/Plan** – Dieser Zeitstempel zeigt, wann der nächste Scan geplant ist. Datum-/Zeitstempel für überfällige Vorgänge werden als roter Text mit gelber Hervorhebung angezeigt. Ein grünes ✓ Häkchen weist auf einen wiederholten Scan hin.

Bedrohungen anzeigen

Sicherheit > Bedrohungen anzeigen

- Ähnliche Informationen werden über 'Info Center > Berichterstellung > Berichte > Sicherheit *(siehe 38)*' bereitgestellt.

Auf der Seite **Bedrohungen anzeigen** werden Bedrohungen angezeigt, zu denen Sie handeln können. Bedrohungen sind je nach ihrem Status auf zwei verschiedenen Registerkarten gruppiert:

- **Aktuelle Bedrohungen** – Listet entdeckte Bedrohungen auf Rechnern auf, die nicht automatisch behoben werden konnten. Jede nicht behobene Bedrohung verbleibt unverändert auf dem Rechner und erfordert eine Benutzeraktion. Durch das Löschen einer Bedrohung auf der Registerkarte **Aktuelle Bedrohungen** wird die Datei sofort gelöscht, ohne in den **Virustresor** verschoben zu werden.

  Hinweis: Beim Scannen eines Rechners werden alle aktuellen Bedrohungen darauf desinfiziert und als beseitigt markiert. Sollte eine Bedrohung bestehen bleiben, wird sie erneut entdeckt und wieder in die Liste der aktuellen Bedrohungen aufgenommen.

- **Virenquarantäne** – Bedrohungen werden durch einen Scan oder vom Resident Shield entdeckt. Bei der Desinfektion der Bedrohung wird die Originaldatei durch eine bereinigte Kopie ersetzt. Die ursprüngliche, nicht desinfizierte Datei wird in eine verborgene Partition auf der Festplatte des

Computers verschoben, die als **Virenquarantäne** bezeichnet wird. Die **Virenquarantäne** dient also als eine Art Papierkorb für Bedrohungen: Sie haben die Möglichkeit, einzelne Dateien aus der Quarantäne zu nehmen, bevor Sie die restlichen Dateien permanent von Rechnern löschen.

Bereinigung

Die Bereinigung umfasst die folgenden Schritte:

1. Es wird ein Versuch unternommen, die Datei zu desinfizieren.
2. Falls dies fehlschlägt, wird versucht, die Datei in die **Virenquarantäne** zu verschieben.
3. Sollte dies fehlschlagen, wird versucht, die Datei zu löschen.
4. Wenn dies nicht erfolgreich ist, verbleibt die Datei unverändert auf dem Rechner und wird auf der Registerkarte **Aktuelle Bedrohungen** der Seite **Bedrohungen anzeigen** angezeigt.

MS Exchange-Server-Bedrohungen

Jegliche Malware, die vom E-Mail-Schutz des MS Exchange-Servers ermittelt wird, wird sofort vom MS Exchange-Server gelöscht und *nur* auf der Registerkarte **Virustresor** angezeigt.

Registerkarte 'Aktuelle Bedrohungen'

Aktionen

- **Beheben** – Versucht, eine Datei zu bereinigen, ohne sie zu löschen. Behobene Bedrohungen werden von der Registerkarte **Aktuelle Bedrohungen** entfernt und auf der Registerkarte **Virustresor** angezeigt.
- **Löschen** – Versucht, eine Datei zu löschen. Gelöschte Bedrohungen werden sofort vom Computer gelöscht.

  Hinweis: Falls sowohl die Desinfektion als auch der Löschvorgang fehlschlagen, kann dies bedeuten, dass die Datei geöffnet ist. Beenden Sie alle Prozesse, die die Datei offen halten, und versuchen Sie erneut, die Datei zu löschen.

- **Aus dieser Liste entfernen** – Entfernt die Bedrohung von der Seite **Bedrohungen anzeigen**, ohne dass eine weitere Aktion ausgeführt wird.
- **Anstehenden Vorgang abbrechen** – Alle anderen Aktionen werden abgebrochen, falls sie noch nicht abgeschlossen wurden.
- **Zu PUP-Ausschlussliste hinzufügen** – Eine Bedrohung wird auf der Seite **Bedrohungen anzeigen** durch ein `(P)` neben dem Namen als potenziell unerwünschtes Programm (PUP) gekennzeichnet. PUP-Bedrohungen können zu der Ausnahmenliste für das Profil des Rechners hinzugefügt werden, auf dem sie gefunden wurden. "Ausnahme" bedeutet, dass die Datei nicht mehr als potenzielle Bedrohung auf *allen* Rechnern gescannt wird, die diesem Profil zugewiesen wurden. Führen Sie diese Aktion nur aus, wenn Sie wissen, dass die Datei sicher verwendet werden kann. Die gesamte PUP-Ausschlussliste wird über die Registerkarte '**Profil definieren** *(siehe 23)* > PUP-Ausschlüsse' verwaltet.

  Hinweis: Andere Bedrohungen als PUP-Bedrohungen können der PUP-Ausschlussliste nicht hinzugefügt werden.

Registerkarte 'Virenquarantäne'

Aktionen

- **Wiederherstellen** – Stellt die Originaldatei wieder her, die als Bedrohung erkannt wurde. Führen Sie diese Aktion nur aus, wenn Sie wissen, dass die Datei sicher verwendet werden kann.
- **Löschen** – Löscht die als Bedrohung erkannte Originaldatei aus dem **Virustresor**.

> **Hinweis:** Eine aus der **Virenquarantäne** gelöschte Datei kann nicht wiederhergestellt werden.

- **Aus dieser Liste entfernen** – Entfernt die Bedrohung von der Seite **Bedrohungen anzeigen**, ohne dass eine weitere Aktion ausgeführt wird.
- **Anstehenden Vorgang abbrechen** – Alle anderen Aktionen werden abgebrochen, falls sie noch nicht abgeschlossen wurden.
- **Zu PUP-Ausschlussliste hinzufügen** – Eine Bedrohung wird auf der Seite **Bedrohungen anzeigen** durch ein `(P)` neben dem Namen als potenziell unerwünschtes Programm (PUP) gekennzeichnet. PUP-Bedrohungen können zu der Ausnahmenliste für das Profil des Rechners hinzugefügt werden, auf dem sie gefunden wurden. "Ausnahme" bedeutet, dass die Datei nicht mehr als potenzielle Bedrohung auf *allen* Rechnern gescannt wird, die diesem Profil zugewiesen wurden. Führen Sie diese Aktion nur aus, wenn Sie wissen, dass die Datei sicher verwendet werden kann. Die gesamte PUP-Ausschlussliste wird über die Registerkarte '**Profil definieren** *(siehe 23)* > PUP-Ausschlüsse' verwaltet.

> **Hinweis:** Andere Bedrohungen als PUP-Bedrohungen können der PUP-Ausschlussliste nicht hinzugefügt werden.

Filter anwenden/Filter zurücksetzen

Klicken Sie auf **Filter anwenden**, um die Zeilen zu filtern, die durch den in die Felder **Rechner.Gruppe**, **Bedrohungspfad** oder **Bedrohungsname** eingegebenen Text angezeigt werden. **Zeit**filterung und **Aktions**sortierung werden sofort ausgeführt. Klicken Sie auf **Filter zurücksetzen**, um alle Datenzeilen anzuzeigen.

Filterspalten

Filtern Sie die Anzeige von Bedrohungen mithilfe von Textfeldern, einem Datumsbereich und/oder Dropdown-Listen. Schließend Sie ein Sternchen (*) in den eingegebenen Text ein, um Übereinstimmungen mit mehreren Datensätzen zu finden.

- **Rechner.Gruppe** – Filtern Sie nach der Rechner-ID.Gruppen-ID der verwalteten Rechner, die Bedrohungen melden.
- **Bedrohungspfad** – Filtern Sie nach dem Pfadnamen des Dateispeicherorts auf verwalteten Rechnern mit gemeldeten Bedrohungen.
- **Zeit** – Filtern Sie nach einem Bereich von Datums- und Zeitangaben, in dem die Bedrohungen *zuletzt* ermittelt wurden. Die **Zeit**filterung wird sofort ausgeführt.
- **Bedrohungsname** – Filtern Sie nach dem Namen der Bedrohung, so wie er in den zum Ermitteln einer Bedrohung verwendeten Anti-Malware-Definitionen festgelegt wurde.
- **Aktion** – Filtern Sie nach anstehenden oder abgeschlossenen Aktionen, die bezüglich der Datensätze in `Bedrohungen anzeigen` unternommen wurden. Wählen Sie `Alle AUS` oder `Alle EIN`, um Aktionen zu aktivieren/deaktivieren. Die Aktionssortierung wird sofort ausgeführt.

Protokolle anzeigen

Sicherheit > Protokolle anzeigen

- Ähnliche Informationen werden über 'Info Center > Berichterstellung > Berichte > Sicherheit *(siehe 38)*' bereitgestellt.

Auf der Seite **Protokolle anzeigen** wird das Ereignisprotokoll zum Sicherheitsschutz der einzelnen Rechner-IDs mit einer **Endpoint Security**-Lizenz angezeigt. Die Liste der angezeigten Rechner-IDs ist abhängig vom Rechner-ID-/Gruppen-ID-Filter und den Rechnergruppen, zu deren Anzeige der Benutzer über System > Benutzersicherheit > Scopes autorisiert ist. Damit Rechner-IDs auf dieser Seite angezeigt werden, muss die **Endpoint Security**-Client-Software über die Seite 'Sicherheit > **Installation** *(siehe 17)*' auf dem verwalteten Rechner installiert worden sein.

Klicken Sie auf eine Rechner-ID.Gruppen-ID, um ein Ereignisprotokoll anzuzeigen. Für jedes Ereignis werden die **Zeit**, ein **Ereigniscode** und in den meisten Fällen eine **Meldung** mit weiteren Informationen angezeigt. Ereigniscodes zum Sicherheitsschutz beschreiben einen von drei Typen von Protokolleinträgen:

- Fehler
- Ereignisse
- Befehle

Filter anwenden/Filter zurücksetzen

Klicken Sie auf **Filter anwenden**, um die Zeilen nach dem in den**Zeit**-Feldern bzw. dem in das Feld **Meldung** eingegebenen Datumsbereich zu filtern. Klicken Sie auf **Filter zurücksetzen**, um alle Datenzeilen anzuzeigen.

Filterspalten

Filtern Sie die Anzeige von Bedrohungen mithilfe von Textfeldern, einem Datumsbereich und/oder Dropdown-Listen. Schließend Sie ein Sternchen (*) in den eingegebenen Text ein, um Übereinstimmungen mit mehreren Datensätzen zu finden. Seitenzeilen können sortiert werden, indem Sie auf die Links der Spaltenüberschriften klicken.

- **Zeit, Min, Max** – Filtern Sie nach einem Datums- bzw. Zeitbereich.
- **Code** – Filtern Sie nach der Kategorie des gemeldeten Protokollereignisses. Wählen Sie `Alle AUS` oder `Alle EIN`, um Aktionen zu aktivieren/deaktivieren.
- **Meldung** – Filtern Sie nach dem Meldungstext.

Erweitern/Zurück

Sicherheit > Verlängern/Zurückgeben

Auf der Seite **Verlängern/Zurückgeben** wird die Jahreslizenz für ausgewählte Rechner-IDs verlängert oder zurückgegeben. Eine Jahreslizenz kann von einer Rechner-ID zurückgegeben und auf eine andere Rechner-ID angewendet werden. Jeder Rechner-ID können mehrere Jahre an Sicherheitsschutz zugewiesen werden. **Endpoint Security**-Lizenzen werden Gruppen-IDs über 'System > **Lizenzmanager** *(http://help.kaseya.com/webhelp/DE/VSA/7000000/index.asp#2924.htm)*' zugeordnet.

Hinweis: Siehe **Endpoint Security-Lizenzierung** im Thema **Sicherheit - Übersicht** *(siehe 1)*.

Die Liste der auswählbaren Rechner-IDs basiert auf dem Rechner-ID-/Gruppen-ID-Filter und dem verwendeten Scope. Damit Rechner-IDs auf dieser Seite angezeigt werden, muss die **Endpoint Security**-Client-Software über die Seite 'Sicherheit > **Installation** *(siehe 17)*' auf dem verwalteten Rechner installiert worden sein.

Aktionen

- **Verlängern** – Verlängert die Jahreslizenzen ausgewählter Rechner-IDs.
- **Zurückgeben** – Gibt die Jahreslizenzen ausgewählter Rechner-IDs zurück.
- **Automatische Verlängerung** – Aktiviert die automatische Zuweisung einer neuen Lizenz an dem Tag, an dem die alte Lizenz ausgewählter Rechner-IDs abläuft. Über die **automatische Verlängerung** werden nur Volllizenzen zugewiesen. Wenn keine zusätzlichen Lizenzen vorhanden sind, schlägt die Zuweisung fehl und der Sicherheitsschutz für den Endpunkt läuft ab. Dies ist standardmäßig aktiviert.
- **Automatische Verlängerung aufheben** – Deaktiviert die automatische Verlängerung für ausgewählte Rechner-IDs.
- **Lizenzanzahl** – Blendet ein Fenster mit den folgenden Lizenzinformationen ein:

- Erworbene Lizenzen
- Voll verfügbare Lizenzen (erworbene Lizenzen, die weder zugewiesen noch installiert noch abgelaufen sind)
- Zugewiesene Lizenzen (Installation geplant, doch die Installation ist noch nicht abgeschlossen)
- Angewendete Lizenzen (auf einem Rechner angewendete aktive Lizenz)
- Teilweise verfügbare Lizenzen (zuvor einem Rechner zugewiesen, doch vor Ablauf an den Pool zurückgegeben)
- Teilweise zugewiesene Lizenzen (teilweise verfügbar und Installation geplant, doch die Installation ist noch nicht abgeschlossen)
- Gesamtzahl der Lizenzen (erworbene Lizenzen abzüglich der abgelaufenen)
- Abgelaufene Lizenzen

- **Nur Lizenzen anzeigen, die innerhalb von 30 Tagen ablaufen** – Im Seitenbereich werden nur die Lizenzen angezeigt, die innerhalb von 30 Tagen ablaufen.

Tabellenspalten

- **(Check-in-Status)** – Diese Symbole geben den Agent-Anmeldestatus jedes verwalteten Rechners an. Wenn Sie den Cursor über ein Anmeldesymbol bewegen, wird das Agent-Schnellansichtsfenster angezeigt.
  - Online, aber in Wartestellung bis zum Abschluss des ersten Audits
  - Agent online
  - Agent online und Benutzer gegenwärtig angemeldet.
  - Agent online und Benutzer gegenwärtig angemeldet, doch Benutzer seit mehr als 10 Minuten nicht aktiv
  - Agent ist gegenwärtig offline
  - Agent hat nie eingecheckt.
  - Agent ist online, aber die Fernsteuerung wurde deaktiviert.
  - Agent wurde ausgesetzt.
- **(Kontrollkästchen 'Alle auswählen')** – Klicken Sie auf dieses Kontrollkästchen, um alle Zeilen im Seitenbereich auszuwählen. Falls das Kontrollkästchen aktiviert ist, klicken Sie auf dieses Kontrollkästchen, um die Auswahl aller Zeilen im Seitenbereich aufzuheben.
- **Rechner.Gruppen-ID** – Ein eindeutiger Rechner-ID/Gruppen-ID-/Organisations-ID-Name für einen Rechner im VSA.
- **Zurückgebbar** – Die Anzahl der Jahreslizenzen, die von einer Rechner-ID zurückgegeben werden kann. Eine Rechner-ID mit nur einer einzigen Jahreslizenz kann keine zusätzlichen Jahreslizenzen zurückgeben.
- **Läuft ab am** – Das Datum, an dem der Sicherheitsschutz einer Rechner-ID abläuft. Dies hängt von der Anzahl der Jahreslizenzen der Rechner-ID an.
- **Automatische Verlängerung** – Ist diese Option markiert, wird die automatische Verlängerung für diese Rechner-ID aktiviert.
- **Höchstzahl erreicht** – Wenn die Höchstzahl der einer Gruppen-ID verfügbaren Jahreslizenzen verwendet wird, wird für jede lizenzierte Rechner-ID in dieser Gruppen-ID ein `Ja` in der Spalte **Höchstzahl erreicht** angezeigt. Dies weist den Benutzer darauf hin, dass eventuell weitere Jahreslizenzen für diese Gruppen-ID benötigt werden. **Endpoint Security**-Lizenzen werden Gruppen-IDs über 'System > **-Lizenzmanager** *(http://help.kaseya.com/webhelp/DE/VSA/7000000/index.asp#2924.htm)*' zugewiesen.

Benachrichtigen

Sicherheit > Benachrichtigen

Die Seite **Benachrichtigen** bietet die Möglichkeit, Kunden, VSA-Benutzern und Rechnerbenutzern eine angegebene Anzahl von Tagen vor Ablauf der **Endpoint Security**-Lizenzen eine Benachrichtigung zu senden. **Endpoint Security**-Lizenzen werden Gruppen-IDs über 'System > **Lizenzmanager** *(http://help.kaseya.com/webhelp/DE/VSA/7000000/index.asp#2924.htm)*' zugeordnet.

> **Hinweis:** Siehe **Endpoint Security-Lizenzierung** im Thema **Sicherheit - Übersicht** *(siehe 1)*.

Die Liste der auswählbaren Rechner-IDs basiert auf dem Rechner-ID-/Gruppen-ID-Filter und dem verwendeten Scope. Damit Rechner-IDs auf dieser Seite angezeigt werden, muss die **Endpoint Security**-Client-Software über die Seite 'Sicherheit > **Installation** *(siehe 17)*' auf dem verwalteten Rechner installiert worden sein.

Aktionen

- **Benachrichtigung senden, wenn Lizenz abläuft in N Tagen** – Geben Sie ein, wie viele Tage vor Ablauf einer **Endpoint Security**-Lizenz Kunden und Benutzer darüber benachrichtigt werden sollen.
- **E-Mail-Empfänger (mehrere Adressen durch Kommas trennen)** – Geben Sie die E-Mail-Adressen ein, an die die Benachrichtigungen gesendet werden sollen. Mehrfache E-Mail-Adressen müssen durch Kommata getrennt werden.
- **Anwenden** – Klicken Sie darauf, um Parameter auf die ausgewählten Rechner-IDs anzuwenden. Prüfen Sie in der Liste der Rechner-IDs, ob die Parameter korrekt angewendet wurden.
- **Löschen** – Klicken Sie darauf, um alle Parametereinstellungen auf ausgewählten Rechner-IDs zu löschen.

Tabellenspalten

- **(Check-in-Status)** – Diese Symbole geben den Agent-Anmeldestatus jedes verwalteten Rechners an. Wenn Sie den Cursor über ein Anmeldesymbol bewegen, wird das Agent-Schnellansichtsfenster angezeigt.
  - Online, aber in Wartestellung bis zum Abschluss des ersten Audits
  - Agent online
  - Agent online und Benutzer gegenwärtig angemeldet.
  - Agent online und Benutzer gegenwärtig angemeldet, doch Benutzer seit mehr als 10 Minuten nicht aktiv
  - Agent ist gegenwärtig offline
  - Agent hat nie eingecheckt.
  - Agent ist online, aber die Fernsteuerung wurde deaktiviert.
  - Agent wurde ausgesetzt.
- **Alle auswählen/Auswahl aufheben** – Klicken Sie auf den Link **Alle auswählen**, um alle Zeilen auf der Seite zu markieren. Klicken Sie auf dem Link **Alle abwählen**, um die Markierung aller Zeilen auf der Seite rückgängig zu machen.
- **Rechner.Gruppen-ID** – Ein eindeutiger Rechner-ID/Gruppen-ID-/Organisations-ID-Name für einen Rechner im VSA.
- **Tage** – Zeigt an, wie viele Tage vor dem Datum des Lizenzablaufs die Benachrichtigung gesendet wird.
- **E-Mail-Adressliste** – Listet die E-Mail-Adressen auf, an die die Benachrichtigungen gesendet werden.
- **Benachrichtigen** – Ist diese Option markiert, werden E-Mail-Empfänger im Voraus gewarnt, dass die Sicherheitslizenz dieser Rechner-ID in Kürze abläuft. Falls dies nicht aktiviert ist, wird keine Benachrichtigung gesendet.

Installation: Sicherheit

Sicherheit > Installation

Auf der Seite **Installation** wird der Sicherheitsschutz für ausgewählte Rechner-IDs installiert bzw. deinstalliert.

- Die Liste der angezeigten Rechner-IDs ist abhängig vom Rechner-ID-/Gruppen-ID-Filter und den Rechnergruppen, zu deren Anzeige der Benutzer über System > Benutzersicherheit > Scopes autorisiert ist.
- Vor der Installation bzw. einer Aktualisierung von Endpunkt-Clients muss die Benutzerzugriffssteuerung (UAC) deaktiviert werden.
- Nach Installation von **Endpoint Security** 2.3 auf dem VSA werden die Endpunkt-Installer von AVG heruntergeladen.
  - Neue **Endpoint Security** 2.3-Endpunkt-Installer basieren auf AVG 2012 SP1, aber **Endpoint Security** unterstützt weiterhin vorhandene AVG 9-Endpunkte.
  - Endpunkt-Installer basieren jeweils auf dem Workstation-, Server- und CPS-Typ: 32 Bit oder 64 Bit. Bei der Installation auf einem Endpunkt wird der jeweils passende Installer ausgewählt.
  - Der Endpunkt-Installer für Server enthält Exchange-Installationskomponenten.
  - Die Download-Zeit der Endpunkt-Installer von AVG kann – basierend auf einem etwa 500 MB großem Paket – unterschiedlich sein.
  - Unter Umständen muss VSA neu gestartet werden.
- AVG 2012 registriert sich nicht selbsttätig im Windows-Sicherheitscenter.
- **Endpoint Security**-Lizenzen werden Gruppen-IDs über 'System > **Lizenzmanager** *(http://help.kaseya.com/webhelp/DE/VSA/7000000/index.asp#2924.htm)*' zugeordnet.

Neustarten des Endpunkts während der Installation und Aktualisierung

Nach der Installation von AVG 2012 wird der Computer möglicherweise neu gestartet. Bei einem Update auf AVG 2012 wird der Endpunkt zuerst nach der Deinstallation der früheren **Endpoint Security**-Client-Software und anschließend nach der Installation von AVG 2012 erneut neu gestartet.

Hinweis: AVG 2012 sollte außerhalb der Arbeitszeit installiert und aktualisiert werden, um den Benutzer nicht zu stören. Es besteht die Möglichkeit, den Endbenutzer vor Ausführung der Installation oder Aktualisierung um seine Einwilligung zu bitten.

AVG 8 nicht unterstützt

Warnung: AVG 8-Endpunkte werden von Endpoint Security 2.3 nicht unterstützt. Es wird Benutzern strengstens empfohlen, entweder Endpunkte vor einem Update auf KES 2.3 auf AVG 9 zu aktualisieren oder AVG 8-Versionen komplett von diesen Endpunkten zu deinstallieren und anschließend nach der Installation von KES 2.3 AVG 2012 darauf zu installieren.

Richtlinien für Installationsoptionen

Die Installation der folgenden Optionen auf *Servern* ist nicht empfohlen:

- E-Mail-Scanner

Die Installation der folgenden Optionen auf *Servern, auf denen Exchange installiert ist,* ist nicht empfohlen:

- Web Shield
- Link Scanner
- Identity Protection

Bei sowohl *Servern* als auch *Workstations* wird AVG Firewall nicht auf AVG 2012-Endpunkten, aber weiterhin auf AVG 9-Endpunkten unterstützt.

Aktionen

Auf dieser Seite können Sie Folgendes ausführen:

- **Installieren** – Installieren Sie **Endpoint Security** auf ausgewählten Rechner-IDs. Siehe **Installation oder Aktualisierung eines Endpunktes** *(siehe 21)*.

  > **Warnung:** Deinstallieren Sie jegliche Antiviren-/Spyware-/Malware-Software auf dem verwalteten Rechner, bevor Sie die **Endpoint Security**-Client-Software installieren.

- **Upgrade** – Aktualisiert AVG 9-Endpunkt-Clients auf AVG 2012. In der Spalte **Installationsstatus** werden Endpunkte identifiziert, die aktualisiert werden können. Siehe **Installation oder Aktualisierung eines Endpunktes** *(siehe 21)*.
- **Client verbinden** – Installiert *nur den Endpoint Security-Client-Dienst* auf dem Endpunkt. Dies ermöglicht Ihnen Folgendes:
  - Zu überprüfen, ob auf dem Endpunkt eine unterstützte AVG-Engine vorhanden ist.
  - Nur den **Endpoint Security**-Client-Dienst ohne Auswirkungen auf die AVG-Komponente zu aktualisieren oder neu zu installieren. Dies ist möglicherweise erforderlich, wenn der **Endpoint Security**-Client-Dienst veraltet oder beschädigt ist.
- **Entfernen** – Deinstalliert **Endpoint Security** von ausgewählten Rechner-IDs.
- **Anstehenden Vorgang abbrechen** – Die drei ersten Aktionen können abgebrochen werden, solange sie noch nicht abgeschlossen worden sind.
- **Benutzeraufforderungen bearbeiten** – Bearbeiten Sie die Warnungsaufforderung, die den Benutzern angezeigt wird. Außerdem können Sie festlegen, für wie viele Minuten der Benutzer die Installation aufschieben darf.
- **Installationsoptionen** – Hier können Sie die **Installationsoptionen** *(siehe 22)* für Installationen oder Aktualisierungen auf *Modulebene* oder als Standardeinstellungen auswählen.
- **Neu starten** – Startet den ausgewählten Computer neu. AVG gibt regelmäßig neue Updates heraus, die einen Neustart erfordern. In diesem Fall wird in der Spalte **Version** `Neustart erforderlich` angezeigt.
- **Lizenzanzahl** – Blendet ein Fenster mit den folgenden Lizenzinformationen ein:
  - Erworbene Lizenzen
  - Voll verfügbare Lizenzen (erworbene Lizenzen, die weder zugewiesen noch installiert noch abgelaufen sind)
  - Zugewiesene Lizenzen (Installation geplant, doch die Installation ist noch nicht abgeschlossen)
  - Angewendete Lizenzen (auf einem Rechner angewendete aktive Lizenz)
  - Teilweise verfügbare Lizenzen (zuvor einem Rechner zugewiesen, doch vor Ablauf an den Pool zurückgegeben)
  - Teilweise zugewiesene Lizenzen (teilweise verfügbar und Installation geplant, doch die Installation ist noch nicht abgeschlossen)
  - Gesamtzahl der Lizenzen (erworbene Lizenzen abzüglich der abgelaufenen)
  - Abgelaufene Lizenzen

Tabellenspalten

- **(Check-in-Status)** – Diese Symbole geben den Agent-Anmeldestatus jedes verwalteten Rechners an. Wenn Sie den Cursor über ein Anmeldesymbol bewegen, wird das Agent-Schnellansichtsfenster angezeigt.
  - Online, aber in Wartestellung bis zum Abschluss des ersten Audits
  - Agent online

- Agent online und Benutzer gegenwärtig angemeldet.
- Agent online und Benutzer gegenwärtig angemeldet, doch Benutzer seit mehr als 10 Minuten nicht aktiv
- Agent ist gegenwärtig offline
- Agent hat nie eingecheckt.
- Agent ist online, aber die Fernsteuerung wurde deaktiviert.
- Agent wurde ausgesetzt.

- **(Kontrollkästchen 'Alle auswählen')** – Klicken Sie auf dieses Kontrollkästchen, um alle Zeilen im Seitenbereich auszuwählen. Falls das Kontrollkästchen aktiviert ist, klicken Sie auf dieses Kontrollkästchen, um die Auswahl aller Zeilen im Seitenbereich aufzuheben.
- **Rechner.Gruppen-ID** – Ein eindeutiger Rechner-ID/Gruppen-ID-/Organisations-ID-Name für einen Rechner im VSA.
- **Installationsstatus** – Folgende Meldungen können angezeigt werden:
  - (leer) – **Endpoint Security**-Client-Software ist auf der Rechner-ID *nicht* installiert. Es gibt keine Voraussetzungen, die eine Installation des Clients auf diesem Rechner verhindern.
  - `Application Conflict` <Produktname> – Auf diesem Rechner ist bereits ein Virenschutzprogramm installiert, das mit der Installation von **Endpoint Security** in Konflikt steht.
  - `Agent-Aktualisierung erforderlich` – Die Version der Agent-Software ist älter als 4.7.1. Auf der Seite 'Agent > **Agent aktualisieren** *(http://help.kaseya.com/webhelp/DE/VSA/7000000/index.asp#549.htm)*' können Sie diesen Agent aktualisieren.
  - `Installation anstehend` <Datum/Zeit> – Die Installation ist für einen bestimmten Zeitpunkt geplant. Datum-/Zeitstempel für überfällige Vorgänge werden als roter Text mit gelber Hervorhebung angezeigt.
  - `Warten auf Dienst` – Der vom Agent für die Kommunikation mit der AVG-Engine verwendete Dienst hat die Installation begonnen. Diese Meldung wird so lange anzeigt, bis die Installation abgeschlossen ist.
  - – Die Installation ist abgeschlossen. Durch Klicken auf dieses Symbol können Sie die auf eine Rechner-ID angewendeten Installationsoptionen anzeigen.
  - `FEHLGESCHLAGEN um <Zeit/Datum und Fehlermeldung>` – Zeigt gegebenenfalls Details zu Installationsfehlern an, die von der AVG-Client-Software gemeldet werden.
  - `AVG von Benutzer entfernt` – Der Rechnerbenutzer hat den AVG-Client manuell deinstalliert.
- **Installationsquelle** – Wenn eine Dateiquelle unter 'Patch-Management > **Dateiquelle** *(http://help.kaseya.com/webhelp/DE/VSA/7000000/index.asp#366.htm)*' definiert ist, werden die Installationspakete von diesem Speicherort heruntergeladen. Ansonsten werden sie aus dem Internet geladen. Wenn die Option **Aus dem Internet herunterladen, wenn der Rechner keine Verbindung zum Dateiserver herstellen kann** unter 'Patch-Management > Dateiquelle' ausgewählt wurde:
  - Falls während der Installation eines **Endpoint Security** v2.x-Endpunktes die Dateiquelle ausgefallen ist oder die Anmeldedaten ungültig sind, wird das Installationsprogramm vom Kaseya Server heruntergeladen. Das Installationsprogramm schließt dann die Endpunktinstallation ab.
  - Falls während einer manuellen **Endpoint Security** v2.x-Aktualisierung die Dateiquelle ausgefallen ist oder die Anmeldedaten ungültig sind, wird das Update aus dem Internet heruntergeladen.

  In den beiden oben genannten Fällen weist die Seite **Protokolle anzeigen** *(siehe 14)* in einer Fehlermeldung darauf hin, warum das Herunterladen von der Dateiquelle fehlgeschlagen ist und dass nun das Herunterladen aus dem Internet versucht wird.
- **Installiert am** – Dies gibt das Datum an, an dem die **Endpoint Security**-Client-Software auf der Rechner-ID installiert wurde.

- **Version** – Die Version des Sicherheitsschutzes, der gegenwärtig auf dieser Rechner-ID verwendet wird. Zum Beispiel: `8.5.322 270.12.6/2084`
  - `8.5.322` – Die Version des installierten AVG-Programms
  - `270.12.6/2084` – Die komplette *Virendatenbankversion*. Dabei ist `270.12.6` die Versionsnummer der *Definition* und `2084` die Versionsnummer der *Signatur*. Dies wird in rotem Text angezeigt, wenn die *Signatur*version älter als die letzten 5 verfügbaren *Signatur*versionen oder die *Definitions*version älter als die letzten 2 verfügbaren *Definitions*versionen und der Agent aktiv ist.
  - `[KES 2.1.0.87]` – Dies ist die Version der **Endpoint Security**-Client-Software.

Installation oder Aktualisierung eines Endpunktes

Sicherheit > Installation > Installieren oder Aktualisieren

Nach dem Klicken auf die Schaltfläche **Installation** oder **Upgrade** können Sie die folgenden Optionen festlegen. Die Standardeinstellungen konfigurieren Sie über die Schaltfläche **Installationsoptionen** *(siehe 22)*. Nach der Installation des **Endpoint Security**-Clients auf einer Rechner-ID können Sie die auf diese Rechner-ID angewendeten Installationsoptionen anzeigen, indem Sie auf das grüne Häkchen in der Spalte **Installationsstatus** klicken.

Profilauswahl

- **Profil auswählen** – Wählen Sie das Profil aus, das während der Installation angewendet werden soll.

Installer-Optionen

- **Installation/Aktualisierung über KServer (Dateiquelle ignorieren)** – Ist diese Option aktiviert, werden die Installationspakete vom Kaseya Server heruntergeladen. Wenn diese Option nicht aktiviert ist, werden die Installationspakete mithilfe der unter 'Patch-Management > **Dateiquelle** *(http://help.kaseya.com/webhelp/DE/VSA/7000000/index.asp#366.htm)*' angegebenen Methode heruntergeladen.
- **Benutzer vor Installation auffordern/Installation ohne Warnung des Benutzers erzwingen** – Die Installation erfordert den Neustart des verwalteten Rechners. Bei Auswahl von **Benutzer vor Installation auffordern** erhält der Benutzer die Möglichkeit, die Installation für eine angegebene Anzahl von Minuten hinauszuschieben. Andernfalls wird die Software mit **Installation ohne Warnung des Benutzers erzwingen** zu dem geplanten Zeitpunkt installiert, ohne dass der Benutzer hierauf hingewiesen wird.

> **Hinweis:** Klicken Sie auf **Benutzeraufforderungen bearbeiten**, um die Anzahl der Minuten anzugeben, um die der Benutzer die Installation hinauszögern kann.

Planen

- **Sofort** – Aktivieren Sie das Kontrollkästchen **Sofort**, um unmittelbar nach dem Klicken auf **Installieren** mit dem Installationsvorgang zu beginnen.
- **Datum/Zeit** – Geben Sie Jahr, Monat, Tag, Stunde und Minute ein, um die Ausführung dieser Aufgabe zeitlich festzulegen.
- **Staffeln um** – Sie können die Last auf das Netzwerk verteilen, indem Sie diese Aufgabe staffeln. Wenn Sie diesen Parameter auf 5 Minuten einstellen, wird die Aufgabe auf jeder Rechner-ID um 5 Minuten versetzt. Beispiel: Rechner 1 läuft um 10:00, Rechner 2 läuft um 10:05, Rechner 3 läuft um 10:10.

- **Überspringen, wenn Rechner offline ist** – Aktivieren Sie diese Option, um die Aufgabe nur zur geplanten Zeit auszuführen. Falls der Rechner offline ist, wird dies übergangen und zur nächsten geplanten Uhrzeit ausgeführt. Deaktivieren Sie diese Einstellung, um diese Aufgabe auszuführen, sobald der Rechner nach der geplanten Zeit eine Verbindung herstellt.

Komponenten

Workstation-Komponenten

- **Link Scanner** – Blockiert gefährliche Websites und prüft Links, die von den gängigsten Suchengines ausgegeben werden. Der Link-Scanner wird nicht auf Browsern installiert, die unter dem Windows Server-Betriebssystem ausgeführt werden.
  - **Aktive sichere Suche** – Scannt einen auf einer Webseite angezeigten Link, bevor Sie darauf klicken.
  - **Such-Shield** – Identifiziert die Sicherheitsbewertung für einen Such-Link in Google-, Yahoo- und MSN-Suchlisten.
- **Web-Shield** – Scannt heruntergeladene Dateien und über Instant-Messaging ausgetauschte Dateien.
- **E-Mail-Scanner** – Wenn dies aktiviert ist, ermittelt die Installation den standardmäßigen E-Mail-Client auf einem Rechner und installiert automatisch das entsprechende E-Mail-Scan-Plugin.
- **ID-Schutz** – Wenn dies aktiviert ist, wird die AVG-Option zum Identitätsschutz aktiviert. Der ID-Schutz verwendet "Verhaltensanalyse", um verdächtige Aktivitäten auf einem Rechner zu ermitteln, und verhindert so den gezielten Diebstahl von Passwörtern, Bankkontodetails, Kreditkartennummern und sonstigen digitalen Wertsachen.
- **Firewall (nicht von Kaseya verwaltet)** – Wenn dies aktiviert ist, wird die AVG-Firewall-Option aktiviert. Sie blockiert den unbefugten Zugriff, gestattet jedoch autorisierte Kommunikationen. *Die von dieser Option erforderten Weiß- und Schwarzlisten können nicht vom* **Endpoint Security***-Client verwaltet werden.*

Serverkomponenten

- **Sharepoint Server-Add-in** – Ist diese Option markiert, wird der **Endpoint Security**-Schutz für Sharepoint Server-Dokumente installiert.
- **Exchange Server-Add-in** – Ist diese Option markiert, wird der **Endpoint Security**-Schutz auf MS Exchange-Servern installiert. Diese Einstellung wird ignoriert, wenn der **Endpoint Security**-Client auf einem Rechner ohne MS Exchange-Server installiert wird.

Installation läuft

Lizenzierungsausnahmen werden im Meldungsbereich des Dialogfeldes angegeben.

Installationsoptionen

Sicherheit > Installation > Installationsoptionen

Gewisse **Installationsoptionen** dienen als Standardeinstellungen, die bei der **Installation oder Aktualisierung eines Endpunktes** *(siehe 21)* aufgehoben werden können.

Andere **Installationsoptionen** dienen als Einstellungen auf *Modulebene*, die normalerweise auf alle Installationen angewendet werden. Einstellungen auf Modulebene können für eine bestimmte Installation oder Aktualisierung nicht aufgehoben werden, sondern gelten für alle später von Ihnen durchgeführten Installationen.

Installationsoptionen

- **Benutzername** – *Modulebene* – Ist diese Option markiert, geben Sie einen mit dieser Installation von **Endpoint Security** verknüpften Namen ein.
- **Firmenname** – *Modulebene* – Ist diese Option markiert, geben Sie einen mit dieser Installation von **Endpoint Security** verknüpften Firmennamen ein.
- **Zielverzeichnis** – *Modulebene* – Ist diese Option markiert, geben Sie ein Zielverzeichnis ein. Wenn dies nicht aktiviert ist, wird das standardmäßige Installationsverzeichnis verwendet.
- **Profil auswählen** – Wählen Sie das Profil aus, das während der Installation angewendet werden soll.
- **Alle laufenden Anwendungen beenden, die die Installation verhindern** – *Modulebene* – Ist diese Option markiert, werden alle Anwendungen beendet, die eine erfolgreiche Installation verhindern könnten.
- **Windows Defender deaktivieren** – *Modulebene* – Die Ausführung von Windows Defender resultiert in einer bedeutenden Beeinträchtigung der **Endpoint Security**-Leistung und sollte mithilfe dieser Option standardmäßig deaktiviert werden.
- **Verzeichnisscans durch Endbenutzer aktivieren** – *Modulebene* – Es wird eine Rechtsklickoption zum Windows Explorer hinzugefügt, über die der Benutzer eine einzelne Datei oder ein Verzeichnis sofort scannen kann.

Optionen zu Agent-Verfahren

- **Vor der Installation auszuführendes Agent-Verfahren** – *Modulebene* – Wählen Sie ein Agent-Verfahren aus.
- **Nach der Installation auszuführendes Agent-Verfahren** – *Modulebene* – Wählen Sie ein Agent-Verfahren aus.

Komponenten

Workstation-Komponenten

- **Link Scanner** – Blockiert gefährliche Websites und prüft Links, die von den gängigsten Suchengines ausgegeben werden. Der Link-Scanner wird nicht auf Browsern installiert, die unter dem Windows Server-Betriebssystem ausgeführt werden.
  - **Aktive sichere Suche** – Scannt einen auf einer Webseite angezeigten Link, bevor Sie darauf klicken.
  - **Such-Shield** – Identifiziert die Sicherheitsbewertung für einen Such-Link in Google-, Yahoo- und MSN-Suchlisten.
- **Web-Shield** – Scannt heruntergeladene Dateien und über Instant-Messaging ausgetauschte Dateien.
- **E-Mail-Scanner** – Wenn dies aktiviert ist, ermittelt die Installation den standardmäßigen E-Mail-Client auf einem Rechner und installiert automatisch das entsprechende E-Mail-Scan-Plugin.
- **ID-Schutz** – Wenn dies aktiviert ist, wird die AVG-Option zum Identitätsschutz aktiviert. Der ID-Schutz verwendet "Verhaltensanalyse", um verdächtige Aktivitäten auf einem Rechner zu ermitteln, und verhindert so den gezielten Diebstahl von Passwörtern, Bankkontodetails, Kreditkartennummern und sonstigen digitalen Wertsachen.

Serverkomponenten

- **Sharepoint Server-Add-in** – Ist diese Option markiert, wird der **Endpoint Security**-Schutz für Sharepoint Server-Dokumente installiert.
- **Exchange Server-Add-in** – Ist diese Option markiert, wird der **Endpoint Security**-Schutz auf MS Exchange-Servern installiert. Diese Einstellung wird ignoriert, wenn der **Endpoint Security**-Client auf einem Rechner ohne MS Exchange-Server installiert wird.

Profil definieren

Sicherheit > Profil definieren

Auf der Seite **Profil definieren** werden Sicherheitsprofile verwaltet. Jedes Sicherheitsprofil stellt einen unterschiedlichen Satz an aktivierten oder deaktivierten Sicherheitsoptionen dar. Änderungen an einem Sicherheitsprofil wirken sich auf alle Rechner-IDs aus, denen dieses Sicherheitsprofil zugewiesen wurde. Ein Sicherheitsprofil wird einer Rechner-ID über 'Sicherheit > **Profil zuweisen** *(siehe 31)*' zugewiesen. Normalerweise benötigen verschiedene Typen von Rechnern oder Netzwerken unterschiedliche Sicherheitsprofile. Es wird Ihnen ein Musterprofil bereitgestellt. Dieses Musterprofil kann zwar nicht geändert werden, aber Sie können es unter einem neuen Namen speichern und dann Änderungen an der Kopie vornehmen. Endpunkte mit AVG 9 und AVG 2012 können mit demselben Profil verwaltet werden.

Auf dieser Seite können Sie die folgenden Aktionen ausführen:

- **Speichern** – Speichert die Änderungen an einem Sicherheitsprofil.
- **Speichern unter** – Erstellt ein neues Sicherheitsprofil, indem es unter einem anderen Namen gespeichert wird.
- **Löschen** – Löscht ein vorhandenes Sicherheitsprofil.
- **Gemeinsam nutzen** – Gibt ein privates Sicherheitsprofil frei. Andere Benutzer können keine privaten Sicherheitsprofile sehen. Durch die Freigabe eines privaten Sicherheitsprofils wird es zu einem öffentlichen Sicherheitsprofil. Freigaberechte werden *nach Objekt* zugewiesen. Es gibt drei Kontrollkästchenoptionen für die Freigabe. Die ersten beiden Kontrollkästchen *schließen einander aus* und bestimmen, welche Freigaberechte zugewiesen werden. Wird keins der beiden ersten Kontrollkästchen aktiviert, kann das Freigabeobjekt nur von den Benutzern gesehen werden, denen Freigabezugriff gewährt wurde. Das Objekt kann weder verwendet noch bearbeitet werden. Die Listenfelder **Freigegeben** und **Nicht freigegeben** und das dritte Kontrollkästchen bestimmen, wer das Objekt *sehen* kann.
  - **Anderen Administratoren gestatten zu ändern** – Wenn dies aktiviert ist, umfassen die Freigaberechte für das Objekt die Fähigkeit, es zu verwenden, seine Details anzuzeigen und es zu bearbeiten.
  - **Andere Administratoren dürfen verwenden, dürfen nicht anzeigen oder bearbeiten** – Wenn dies aktiviert ist, lassen die Freigaberechte für das Objekt nur dessen Verwendung zu.
  - **Als öffentlich festlegen (wird von allen Administratoren gesehen)** – Wenn dies aktiviert ist, wird sichergestellt, dass *alle* aktuellen und zukünftigen VSA-Benutzer das Objekt *sehen* können. Wenn es nicht aktiviert wird, können nur ausgewählte Benutzerrollen und Benutzer das Freigabeobjekt sehen. Wenn in diesem Fall später neue Benutzer oder Benutzerrollen hinzugefügt werden, müssen Sie zu diesem Dialogfeld zurückkehren und einstellen, dass sie das bestimmte Objekt sehen können.
- **Eigentumsrecht übernehmen** – Übernehmen Sie das **Eigentumsrecht** *(http://help.kaseya.com/webhelp/DE/VSA/7000000/index.asp#5537.htm)* zu jedem öffentlichen Sicherheitsprofil.

So definieren oder pflegen Sie ein Sicherheitsprofil:

1. Wählen Sie ein Sicherheitsprofil aus der Dropdown-Liste **Profil auswählen**.
2. Stellen Sie Optionen auf den Registerkarten für das Sicherheitsprofil ein:
   - **Allgemein**
   - **Resident Shield**
   - **E-Mail-Scanner**
   - **Vollständiger Scan**
   - **Exchange**
   - **Verzeichnisse ausschließen**

- **PUPs ausschließen**
- **Aktualisierungen**

3. Klicken Sie auf die Schaltfläche **Speichern** oder **Speichern unter**, um das Sicherheitsprofil zu speichern.

Allgemein

Kennwort für das AVG Desktop-GUI

- **AVG Desktop-GUI mit Kennwort schützen** – Geben Sie ein Kennwort ein, um den Benutzer zu zwingen, vor dem Ausblenden des AVG-Desktops, AVG-Taskleistensymbols und der AVG-Verknüpfungen im Startmenü ein Kennwort einzugeben. Wird diese Option nicht aktiviert, wird die Eingabe eines Kennwortes nicht erwartet.

Virenquarantäne

- **Größenbegrenzung der Virenquarantäne** – Ist diese Option markiert, wird die Größe des Quarantänebereichs den folgenden Optionen entsprechend beschränkt:
  - **Maximale Größe der Virenquarantäne: <N> % der lokalen Festplatte** – Geben Sie den maximalen Prozentsatz an Speicherplatz für unter Quarantäne gestellte Bedrohungen ein.
  - **Mindestspeicherplatz, der auf der lokalen Festplatte verbleiben muss** – Geben Sie die Mindestmenge von Megabyte für das Speichern der in Quarantäne gestellten Bedrohungen ein.
- **Automatische Dateilöschung** – Wenn dies aktiviert ist, werden Dateien den folgenden Optionen entsprechend automatisch gelöscht:
  - **Dateien löschen, die älter sind als <N> Tage** – Geben Sie an, wie viele Tage unter Quarantäne gestellte Bedrohungen gespeichert werden, bevor sie automatisch gelöscht werden.
  - **Max. Anzahl der zu speichernden Dateien** – Geben Sie die maximale Anzahl der in Quarantäne gestellten Dateien ein, die gespeichert werden sollen.

Benachrichtigungen in der Taskleiste

- **Systemablage-Benachrichtigungen anzeigen** – Wenn dies markiert ist, können die folgenden Systemablage-Benachrichtigungen optional aktiviert werden. Alle Benachrichtigungen werden neben der Systemablage auf dem verwalteten Rechner angezeigt.
- **Benachrichtigungen zu Aktualisierungen im Infobereich anzeigen** – Ist diese Option markiert, wird der Benutzer durch eine Benachrichtigung auf eine Aktualisierung der **Endpoint Security**-Software hingewiesen.
- **Systemablage-Benachrichtigungen zu Scans anzeigen** – Wenn dies aktiviert ist, wird der Benutzer über eine Benachrichtigung auf den Scan des Rechners hingewiesen.
- **Ablagebenachrichtigungen zu Resident Shield anzeigen (automatischer Vorgang)** – Wenn dies aktiviert ist, wird der Benutzer über eine Benachrichtigung darauf hingewiesen, dass der Resident Shield gegen eine Bedrohung vorgegangen ist.
- **Benachrichtigungen über Änderungen des Komponentenzustands anzeigen** – Ist diese Option markiert, wird der Benutzer durch eine Benachrichtigung darauf hingewiesen, dass sich der Zustand einer **Endpoint Security**-Komponente geändert hat.
- **E-Mail-Scanner-Benachrichtigungen anzeigen** – Wenn dies aktiviert ist, wird der Benutzer über eine Benachrichtigung darauf hingewiesen, dass der E-Mail-Scan gegen eine E-Mail-Bedrohung vorgegangen ist.

Symbolmenü des Agent

- **Option zum Aktivieren/Deaktivieren des Resident Shield im Symbolmenü des Agents anzeigen** – Wenn dies aktiviert ist, geschieht Folgendes:

- Im Agent-Menü des verwalteten Rechners werden Optionen für **Sicherheit aktivieren** und **Scan abbrechen** angezeigt.
- Der Benutzer kann im Agent-Menü auf die Option **Sicherheit aktivieren** klicken, um den Sicherheitsschutz ein- oder auszuschalten.
- Der Benutzer kann im Agent-Menü auf die Option **Scan abbrechen** klicken, um einen Sicherheitsschutz-Scan abzubrechen, der gerade ausgeführt wird.

> **Hinweis:** Über 'Sicherheit > **Sicherheitsstatus** *(siehe 5)*' kann der Benutzer den Sicherheitsschutz auch remote aktivieren bzw. deaktivieren.

Resident Shield

Der Resident Shield ist eine speicherresidente Funktion.

- **Resident Shield aktivieren** – Wenn dies aktiviert ist, werden die folgenden Dateitypen beim Kopieren, Öffnen oder Speichern gescannt. Wenn dies nicht aktiviert ist, werden keine anderen **Resident Shield**-Options ausgewertet.

> **Hinweis:** Sie können alternativ den **Resident Shield mit einem Agent-Verfahren aktivieren/deaktivieren** *(siehe 8)*.

Dateitypen

- **Alle Dateien überprüfen**– Wenn dies aktiviert ist, werden sämtliche Dateien auf dem verwalteten Rechner gescannt.
- **Infizierbare Dateien und ausgewählte Dokumenttypen überprüfen** – Wenn dies aktiviert ist, geben Sie über die folgenden Optionen die ein- oder auszuschließenden *zusätzlichen* Dateierweiterungen von Programmen und Dokumenten an:
  - **Dateien mit den folgenden Erweiterungen von der Überprüfung ausschließen** – Geben Sie die Dateierweiterung von Programmen und Dokumenten an, die aus dem Scan ausgeschlossen werden sollen. Ausgeschlossene Erweiterungen haben Vorrang vor eingeschlossenen Erweiterungen. Trennen Sie jede Erweiterung durch ein Semikolon (;).
  - **Dateien mit den folgenden Erweiterungen immer überprüfen** – Geben Sie die Dateierweiterung von Programmen und Dokumenten an, die in den Scan eingeschlossen werden sollen. Trennen Sie jede Erweiterung durch ein Semikolon (;). Resident Shield scannt die folgenden Dateierweiterungen, ohne dass Sie sie angeben müssen: 386; ASP; BAT; BIN; BMP; BOO; CHM; CLA; CLASS; CMD; CNM; COM; CPL; DEV; DLL; DO*; DRV; EML; EXE; GIF; HLP; HT*; INI; JPEG*; JPG; JS*; LNK; MD*; MSG; NWS; OCX; OV*; PCX; PGM; PHP*; PIF; PL*; PNG; POT; PP*; SCR; SHS; SMM; SYS; TIF; VBE; VBS; VBX; VXD; WMF; XL*; XML; ZL*.
  - **Dateien ohne Erweiterung überprüfen** – Wenn dies aktiviert ist, schließt der Scan Dateien ohne Erweiterung ein.

Weitere Optionen

- **Auf Verfolgungs-Cookies überprüfen** – Wenn dies aktiviert ist, schließt der Scan Verfolgungs-Cookies aus Internet-Browsern ein. Gefundene Verfolgungs-Cookies werden sofort gelöscht und nicht in den Virustresor verschoben.
- **Potenziell ungewollte Programme und Spyware-Bedrohungen überprüfen** – Wenn dies aktiviert ist, ermittelt der Scan ausführbare Anwendungen oder DLL-Bibliotheken, die potenziell unerwünschte Programme sein könnten. Manche Programme, besonders die kostenlosen, enthalten Adware und werden von **Endpoint Security** möglicherweise als **potenziell unerwünschtes Programm** erkannt und gemeldet.
- **Dateien beim Schließen überprüfen** – Wenn dies aktiviert ist, werden Dateien beim Schließen gescannt.

- **Bootsektor von Wechselmedien überprüfen** – Wenn dies aktiviert ist, schließt der Scan den Bootsektor von Wechselmedien ein.
- **Heuristik verwenden** – Wenn dies aktiviert ist, schließt der Scan eine heuristische Analyse ein. Eine heuristische Analyse führt eine dynamische Emulation der Anweisungen eines gescannten Objekts in einer virtuellen Computing-Umgebung aus.

E-Mail-Scanner

- **E-Mail-Scanner aktivieren** – Wenn dies aktiviert ist, werden ein- und ausgehende E-Mail-Nachrichten und -Anhänge auf Viren gescannt. Wenn dies nicht aktiviert ist, werden keine anderen Optionen des **E-Mail-Schutzes** ausgewertet.

> **Hinweis:** Der **E-Mail-Scanner** ist für *Server* nicht empfohlen. Siehe Registerkarte **Exchange** unten.

E-Mail-Scan

- **Eingehende E-Mail-Nachrichten überprüfen** – Wenn dies aktiviert ist, werden eingehende E-Mail-Nachrichten gescannt.

> **Zertifizierung:** Manche E-Mail-Clients unterstützen das Anhängen von Text an E-Mail-Nachrichten, der bestätigt, dass die Nachricht auf Viren gescannt wurde.

  - **E-Mail-Nachrichten nicht zertifizieren** – Wenn dies aktiviert ist, werden eingehende E-Mail-Nachrichten nicht zertifiziert.
  - **Alle E-Mail-Nachrichten zertifizieren** – Wenn dies aktiviert ist, werden sämtliche eingehenden E-Mail-Nachrichten zertifiziert.
  - **Nur E-Mail-Nachrichten mit Anhängen zertifizieren** – Wenn dies aktiviert ist, werden nur eingehende E-Mail-Nachrichten mit Anhängen zertifiziert.
  - **Zertifizierung eingehender E-Mail-Nachrichten** – Zertifizierungstext wird an eingehende E-Mail-Nachrichten angehängt.
- **Ausgehende E-Mail-Nachrichten überprüfen** – Wenn dies aktiviert ist, werden ausgehende E-Mail-Nachrichten gescannt.
  - **E-Mail-Nachrichten nicht zertifizieren** – Wenn dies aktiviert ist, werden ausgehende E-Mail-Nachrichten nicht zertifiziert.
  - **Alle E-Mail-Nachrichten zertifizieren** – Wenn dies aktiviert ist, werden sämtliche ausgehenden E-Mail-Nachrichten zertifiziert.
  - **Nur E-Mail-Nachrichten mit Anhängen zertifizieren** – Wenn dies aktiviert ist, werden nur ausgehende E-Mail-Nachrichten mit Anhängen zertifiziert.
  - **Zertifizierung ausgehender E-Mail-Nachrichten** – Zertifizierungstext wird an ausgehende E-Mail-Nachrichten angehängt.
- **Betreff von als Virus markierten Nachrichten ändern** – Fügt Präfixtext zum Betreff einer Nachricht hinzu, die einen Virus enthält.

Scaneigenschaften

- **Heuristik verwenden** – Gilt für eine E-Mail-Nachricht. Wenn dies aktiviert ist, schließt der Scan eine heuristische Analyse ein. Eine heuristische Analyse führt eine dynamische Emulation der Anweisungen eines gescannten Objekts in einer virtuellen Computing-Umgebung aus.
- **Potenziell ungewollte Programme und Spyware-Bedrohungen überprüfen** – Wenn dies aktiviert ist, schließt der E-Mail-Scan eine Überprüfung auf Spyware, Adware und potenziell unerwünschte Programme ein.
- **In Archiven überprüfen** (RAR, RAR 3.0, ZIP, ARJ, CAB) – Wenn dies aktiviert ist, werden E-Mail-Archive gescannt.

Berichterstattung zu E-Mail-Anhängen (als Bedrohung)

- **Passwortgeschützte Archive melden** – Wenn dies aktiviert ist, werden passwortgeschützte Archivanhänge (zip, rar usw.) in E-Mail-Nachrichten als Bedrohungen gemeldet.
- **Passwortgeschützte Dokumente melden** – Wenn dies aktiviert ist, werden passwortgeschützte Dokumente in E-Mail-Nachrichten als Bedrohungen gemeldet.
- **Dateien mit Makro melden** – Wenn dies aktiviert ist, werden an E-Mail-Nachrichten angehängte Dateien mit Makros als Bedrohungen gemeldet.
- **Verborgene Erweiterungen melden** – Wenn dies aktiviert ist, werden Dateien mit einer verborgenen Erweiterung gemeldet. Manche Viren verstecken sich, indem sie ihre Dateierweiterung verdoppeln. Der `VBS/Iloveyou`-Virus beispielsweise hängt E-Mails eine Datei namens `ILOVEYOU.TXT.VBS` an. Der Windows-Standardeinstellung entsprechend werden bekannte Erweiterungen ausgeblendet. Deshalb sieht die Datei wie `ILOVEYOU.TXT` aus. Wenn Sie sie öffnen, öffnen Sie keine `.TXT`-Textdatei, sondern führen stattdessen eine `.VBS`-Prozedurdatei aus.
- **Gemeldete Anhänge in den Virustresor verschieben (nur eingehende E-Mail-Nachrichten)** – Wenn dies aktiviert ist, werden gemeldete E-Mail-Anhänge in den Virustresor verschoben. Sie werden auf der Registerkarte **Virustresor** der Seite **Bedrohungen anzeigen** *(siehe 5)* anstatt auf der Registerkarte **Aktuelle Bedrohungen** angezeigt.

Vollständiger Scan

Scaneinstellungen

- **Potenziell ungewollte Programme und Spyware-Bedrohungen überprüfen** – Wenn dies aktiviert ist, ermittelt der Scan ausführbare Anwendungen oder DLL-Bibliotheken, die potenziell unerwünschte Programme sein könnten. Manche Programme, besonders die kostenlosen, enthalten Adware und werden von **Endpoint Security** möglicherweise als **potenziell unerwünschtes Programm** erkannt und gemeldet.
- **Auf Verfolgungs-Cookies überprüfen** – Wenn dies aktiviert ist, schließt der Scan Verfolgungs-Cookies aus Internet-Browsern ein. Gefundene Verfolgungs-Cookies werden sofort gelöscht und nicht in den Virustresor verschoben.
- **In Archiven überprüfen** – Wenn dies aktiviert ist, schließt der Scan Archivdateien, z. B. ZIP- und RAR-Dateien, ein.
- **Heuristik verwenden** – Wenn dies aktiviert ist, schließt der Scan eine heuristische Analyse ein. Eine heuristische Analyse führt eine dynamische Emulation der Anweisungen eines gescannten Objekts in einer virtuellen Computing-Umgebung aus.
- **Systemumgebung überprüfen** – Wenn dies aktiviert ist, werden die Systembereiche gescannt, bevor der volle Scan beginnt.
- **Nur infizierbare Dateien überprüfen** – Wenn dies aktiviert ist, wird der Inhalt von "infizierbaren" Dateien ungeachtet ihrer Dateierweiterung gescannt. Beispielsweise könnte eine EXE-Datei zwar umbenannt werden, aber sie könnte dennoch infiziert sein. Die folgenden Dateitypen werden als "infizierbare" Dateien betrachtet:
  - **EXE-Typ** – COM; DRV; EXE; OV?; PGM; SYS; BIN; CMD; DEV; 386; SMM; VXD; DLL; OCX; BOO; SCR; ESL; CLA; CLASS; BAT; VBS; VBE; WSH; HTA; HTM; HTML; ?HTML; CHM; INI; HTT; INF; JS; JSE; HLP; SHS; PRC; PDB; PIF; PHP; ZL?; ASP; LNK; EML; NWS; CPL; WMF
  - **DOC-Typ** – DO?; XL?; VBX; RTF; PP?; POT; MDA; MDB; XML; DOC?; DOT?; XLS?; XLT?; XLAM; PPT?; POT?; PPS?; SLD?; PPAM; THMX

Leistung

- **Systempriorität für Scan auswählen** – Definiert, wie schnell der Scan ausgeführt wird und wie viele Systemressourcen er verbraucht. Sie können die Scanausführung auf so schnell wie möglich einstellen, wodurch ein Computer deutlich verlangsamt wird. Oder Sie können den Scan so

einstellen, dass er möglichst wenige Systemressourcen verbraucht, wodurch jedoch die Laufzeit des Scans verlängert wird.

Exchange

- **AVG für Exchange-Server aktivieren** – Aktivieren oder deaktivieren Sie das Scannen von E-Mail-Nachrichten für ausgewählte MS Exchange-Server.

> **Hinweis:** Erstellen Sie, wenn Sie den E-Mail-Schutz auf einem oder mehreren der MS Exchange-Server installieren, ein eindeutiges Profil für MS Exchange-Server und wenden dieses nur auf diese MS Exchange-Server an. Die Einstellungen auf der Registerkarte '**Profil definieren** > Exchange' sollten nur für MS Exchange-Server aktiviert und auf diese angewendet werden.

E-Mail-Zertifizierung:

- **Aktivieren** – Ist diese Option markiert, wird gescannten E-Mails auf MS Exchange-Servern eine Zertifizierungsanmerkung hinzugefügt. Passen Sie die Zertifizierungsanmerkung im Textfeld an.

Leistung

- **Scans im Hintergrund ausführen** – Aktivieren oder deaktivieren Sie das Scannen im Hintergrund. Das Scannen im Hintergrund ist eine der Funktionen der VSAPI 2.0/2.5-Anwendungsoberfläche. Sie bietet ein Thread-Scannen der Exchange Messaging-Datenbanken. Wenn in den Posteingangsordnern der Benutzer ein noch nicht gescanntes Objekt gefunden wird, wird es an AVG für einen Scan von Exchange 2000/2003-Servern übermittelt. Das Scannen und Suchen nach nicht untersuchten Objekten wird parallel ausgeführt. Für jede Datenbank wird ein spezifischer Thread niedriger Priorität verwendet. Dies garantiert, dass andere Aufgaben, z. B. das Speichern von E-Mail-Nachrichten in der Microsoft Exchange-Datenbank, immer vorrangig ausgeführt werden.
- **Proaktiv überprüfen** – Aktivieren oder deaktivieren Sie das proaktive VSAPI 2.0/2.5-Scannen. Das proaktive Scannen umfasst eine dynamische Prioritätsverwaltung von Objekten in der Scan-Warteschlange. Objekte mit einer niedrigeren Priorität werden erst gescannt, nachdem alle Objekte mit einer höheren Priorität gescannt wurden. Die Priorität eines Objekts wird erhöht, wenn ein Client versucht, es zu verwenden. Der Objektvorrang ändert sich also dynamisch entsprechend der Benutzeraktivität.
- **RTF-Dateien überprüfen** – Geben Sie an, ob RTF-Dateien gescannt werden oder nicht.
- **Threads überprüfen** – Der Scanprozess verläuft standardmäßig nach Thread, um die Gesamtleistung des Scans um einen gewissen Grad an Parallelität zu erhöhen. Die Standardanzahl der Threads wird als 2 x die 'Anzahl_der_Prozessoren' + 1 berechnet.
- **Scan-Zeitlimit** – Das maximale, fortlaufende Intervall in Sekunden, während dessen ein Thread auf eine gescannte Nachricht zugreift.

Verzeichnisse ausschließen

Verzeichnisse ausschließen

> **Warnung:** Schließen Sie Verzeichnisse nur dann aus, wenn Sie wissen, dass ihr Inhalt frei von Bedrohungen ist.

- **Neuen Datensatz hinzufügen** – Fügt die aus einem Scan ausgeschlossenen Verzeichnisse hinzu. Manche Verzeichnisse können zwar frei von Bedrohungen sein, enthalten aber Dateien, die irrtümlicherweise als Malware interpretiert wurden.
  - **Dateiname** – Geben Sie den Namen der Datei ein.

Resident Shield-Dateien ausschließen

Resident Shield-Dateien ausschließen (nur bei AVG 2012 Resident Shield verfügbar, bei AVG 9 ignoriert)

> **Warnung:** Schließen Sie Dateien nur dann aus, wenn Sie wissen, dass ihr Inhalt frei von Bedrohungen ist.

Verwenden Sie diese Registerkarte, um angegebene Dateien *manuell* auszuschließen. Diese Ausschlussliste ist nur beim aktiven Scan von Resident Shield aktiv.

- **Neuen Datensatz hinzufügen** – Fügt PUP-Dateien hinzu, die aus einem Scan ausgeschlossenen werden sollen. Manche Dateien können zwar frei von Bedrohungen sein, aber irrtümlicherweise als potenziell unerwünschte Programme (PUPs) interpretiert worden sein.
  - **Dateiname** – Geben Sie den Namen der Datei ein.

PUPs ausschließen

Potenziell ungewollte Programme ausschließen

> **Warnung:** Schließen Sie Dateien nur dann aus, wenn Sie wissen, dass ihr Inhalt frei von Bedrohungen ist.

Verwenden Sie diese Registerkarte, um potenziell unerwünschte Programme (PUPs) *manuell* auszuschließen. Andere Bedrohungen als PUP-Bedrohungen können der PUP-Ausschlussliste nicht hinzugefügt werden. Auf der Seite 'Bedrohungen anzeigen' können PUPs schneller identifiziert und ausgeschlossen werden.

- **Neuen Datensatz hinzufügen** – Fügt PUP-Dateien hinzu, die aus einem Scan ausgeschlossenen werden sollen. Manche Dateien können zwar frei von Bedrohungen sein, aber irrtümlicherweise als potenziell unerwünschte Programme (PUPs) interpretiert worden sein.
  - **Dateiname** – Geben Sie den Namen der Datei ein.
  - **Prüfsumme** – Geben Sie den Prüfsummenwert der Datei ein. Um den Prüfsummenwert zu ermitteln, öffnen Sie die **AVG-Benutzeroberfläche** auf dem Rechner, der die Datei enthält. Wählen Sie **Extras > Erweiterte Einstellungen** aus. Wählen Sie das Eigenschaftenblatt **PUP-Ausnahmen** aus. Klicken Sie auf die Schaltfläche **Ausnahme hinzufügen**. Wählen Sie die Datei aus, indem Sie durch das lokale Verzeichnis des Rechners blättern. Der entsprechende Prüfsummenwert wird angezeigt. Kopieren Sie den Prüfsummenwert aus der **AVG-Benutzeroberfläche** und fügen Sie ihn in das Dialogfeld **Neuen Datensatz hinzufügen** auf der Registerkarte **PUPs ausschließen** unter 'Sicherheit > **Profil definieren** ein.
  - **Dateigröße** – Geben Sie die Dateigröße in Byte ein. Um die Dateigröße zu ermitteln, klicken Sie mit der rechten Maustaste in Windows Explorer und markieren den Wert **Größe** in Byte.

Aktualisierungen

Konfigurieren Sie auf dieser Registerkarte, wie AVG-Aktualisierungen heruntergeladen werden.

Proxy-Einstellungen

Aktiviert/deaktiviert die Verwendung eines Proxy-Servers, um AVG-Aktualisierungen herunterzuladen.

- **Proxy nicht verwenden** – Deaktiviert die Proxy-Einstellungen.
- **Proxy verwenden** – Aktiviert die Proxy-Einstellungen.
- **Verbindung über Proxy versuchen und bei Fehlschlagen direkt verbinden** – Aktiviert die Proxy-Einstellungen. Beim Fehlschlagen der Proxy-Verbindung wird eine direkte Verbindung hergestellt.

Die Einstellungen **Manuell** und **Automatisch** gelten nur, wenn oben eine Proxy-Option ausgewählt wurde.

- **Manuell** – Stellt die Proxy-Einstellungen manuell ein.
  - **Server** – Geben Sie einen gültigen Proxy-Servernamen oder eine gültige IP-Adresse ein.

- **Port** – Geben Sie eine Portnummer ein.
- **PROXY-Authentifizierung verwenden** – Wenn dies aktiviert ist, ist Proxy-Authentifizierung erforderlich.
  - ✓ **Benutzername** – Wenn **PROXY-Authentifizierung** aktiviert ist, geben Sie einen gültigen Benutzernamen ein.
  - ✓ **Passwort** – Wenn **PROXY-Authentifizierung** aktiviert ist, geben Sie ein gültiges Passwort ein.

- **Auto** – Stellt die Proxy-Einstellungen automatisch ein.
  - **Von Browser** – Wählen Sie einen Standardbrowser aus der Dropdown-Liste aus, um Proxy-Einstellungen festzulegen.
  - **Von Skript** – Geben Sie den vollständigen Pfad eines Skripts ein, das die Adresse des Proxy-Servers angibt.
  - **Autom. ermitteln** – Versucht, die Einstellungen direkt vom Proxy-Server abzurufen.

URL aktualisieren

AVG stellt eine Standard-URL zum Herunterladen von Aktualisierungen bereit. Wenn Sie es vorziehen, können Sie die Aktualisierungen auch von einer benutzerdefinierten URL herunterladen.

- **Benutzerdefinierte Aktualisierungs-URL verwenden** – Wählen Sie diese Option aus, um Aktualisierungen von einer benutzerdefinierten URL herunterzuladen.
  - **Name** – Geben Sie den Namen der benutzerdefinierten Aktualisierungs-URL ein.
  - **URL** – Geben Sie die URL ein.

Profil zuweisen

Sicherheit > Profil zuweisen

Auf der Seite **Profil zuweisen** werden Rechner-IDs mit **Endpoint Security**-Lizenzen Sicherheitsprofile zugewiesen. Sicherheitsprofile werden über 'Sicherheit > **Profil definieren** *(siehe 23)*' definiert.

Die Liste der auswählbaren Rechner-IDs basiert auf dem Rechner-ID-/Gruppen-ID-Filter und dem verwendeten Scope. Damit Rechner-IDs auf dieser Seite angezeigt werden, muss die **Endpoint Security**-Client-Software über die Seite 'Sicherheit > **Installation** *(siehe 17)*' auf dem verwalteten Rechner installiert worden sein.

Aktionen

- **Konfiguration anwenden** – Klicken Sie auf **Konfiguration anwenden**, um das in der Dropdown-Liste **Profil auswählen** angezeigte Sicherheitsprofil auf ausgewählte Rechner-IDs anzuwenden.
- **Profil auswählen** – Wählen Sie ein Sicherheitsprofil aus, das auf ausgewählte Rechner-IDs angewendet werden soll.
- **Nur Rechner mit dem ausgewählten Profil anzeigen** – Ist diese Option markiert, wird der Seitenbereich nach dem ausgewählten Sicherheitsprofil gefiltert.

Tabellenspalten

- **Check-in-Status** – Diese Symbole geben den Agent-Anmeldestatus jedes verwalteten Rechners an. Wenn Sie den Cursor über ein Anmeldesymbol bewegen, wird das Agent-Schnellansichtsfenster angezeigt.
  - Online, aber in Wartestellung bis zum Abschluss des ersten Audits
  - Agent online
  - Agent online und Benutzer gegenwärtig angemeldet.
  - Agent online und Benutzer gegenwärtig angemeldet, doch Benutzer seit mehr als 10 Minuten nicht aktiv

 Agent ist gegenwärtig offline
 Agent hat nie eingecheckt.
 Agent ist online, aber die Fernsteuerung wurde deaktiviert.
 Agent wurde ausgesetzt.

- **(Kontrollkästchen 'Alle auswählen')** – Klicken Sie auf dieses Kontrollkästchen, um alle Zeilen im Seitenbereich auszuwählen. Falls das Kontrollkästchen aktiviert ist, klicken Sie auf dieses Kontrollkästchen, um die Auswahl aller Zeilen im Seitenbereich aufzuheben.
- **Rechner.Gruppen-ID** – Ein eindeutiger Rechner-ID/Gruppen-ID-/Organisations-ID-Name für einen Rechner im VSA.
- **Profilname** – Zeigt das einer Rechner-ID zugewiesene Sicherheitsprofil an. Falls ein Problem vorliegt, wird der Status der Rechner-ID angezeigt.

Protokolleinstellungen: Sicherheit

Sicherheit > Protokolleinstellungen

Auf der Seite **Protokolleinstellungen** wird angegeben, wie viele Tage die Protokolldaten des Sicherheitsschutzes für Rechner-IDs mit **Endpoint Security**-Lizenzen aufbewahrt werden. Bei gewissen Rechnern, beispielsweise Webservern, ist es eventuell gerechtfertigt, die Historie von Virusangriffen länger zu speichern als bei anderen Rechnertypen.

Die Liste der auswählbaren Rechner-IDs basiert auf dem Rechner-ID-/Gruppen-ID-Filter und dem verwendeten Scope. Damit Rechner-IDs auf dieser Seite angezeigt werden, muss die **Endpoint Security**-Client-Software über die Seite 'Sicherheit > **Installation** *(siehe 17)*' auf dem verwalteten Rechner installiert worden sein.

Aktionen

- **Konfiguration anwenden** – Klicken Sie auf **Konfiguration anwenden**, um die im Feld **<N> Tage für die Aufbewahrung von Protokolleinträgen** festgelegte Anzahl von Tagen auf ausgewählte Rechner-IDs anzuwenden.
- **<N> Tage für die Aufbewahrung von Protokolleinträgen** – Geben Sie an, wie viele Tage die Protokolldaten des Sicherheitsschutzes aufbewahrt werden sollen.

Tabellenspalten

- **Check-in-Status** – Diese Symbole geben den Agent-Anmeldestatus jedes verwalteten Rechners an. Wenn Sie den Cursor über ein Anmeldesymbol bewegen, wird das Agent-Schnellansichtsfenster angezeigt.
   Online, aber in Wartestellung bis zum Abschluss des ersten Audits
   Agent online
   Agent online und Benutzer gegenwärtig angemeldet.
   Agent online und Benutzer gegenwärtig angemeldet, doch Benutzer seit mehr als 10 Minuten nicht aktiv
   Agent ist gegenwärtig offline
   Agent hat nie eingecheckt.
   Agent ist online, aber die Fernsteuerung wurde deaktiviert.
   Agent wurde ausgesetzt.
- **(Kontrollkästchen 'Alle auswählen')** – Klicken Sie auf dieses Kontrollkästchen, um alle Zeilen im Seitenbereich auszuwählen. Falls das Kontrollkästchen aktiviert ist, klicken Sie auf dieses Kontrollkästchen, um die Auswahl aller Zeilen im Seitenbereich aufzuheben.
- **Rechner.Gruppen-ID** – Ein eindeutiger Rechner-ID/Gruppen-ID-/Organisations-ID-Name für einen Rechner im VSA.

- **Speichertage vor Ablauf** – Zeigt an, wie viele Tage die Protokolldaten des Sicherheitsschutzes für eine Rechner-ID aufbewahrt werden.

Exchange-Status

Sicherheit > Exchange-Status

Auf der Seite **Exchange-Status** wird der Status des E-Mail-Schutzes auf MS Exchange-Servern angezeigt, auf denen **Endpoint Security** installiert ist. Wenn während der Installation von **Endpoint Security** auf einem Rechner MS Exchange festgestellt wird, wird das Plugin für den MS Exchange-E-Mail-Schutz automatisch installiert. Server mit Exchange können auf der Seite **Profil definieren** *(siehe 23)* von der Nutzung des Exchange Mailbox-Schutzes ausgeschlossen werden.

Hinweis: Jegliche Malware, die vom E-Mail-Schutz des MS Exchange-Servers erkannt wird, wird sofort vom MS Exchange-Server gelöscht und *nur* auf der Registerkarte **Virenquarantäne** der Seite **Bedrohungen anzeigen** *(siehe 12)* angezeigt.

Die Liste der auswählbaren Rechner-IDs basiert auf dem Rechner-ID-/Gruppen-ID-Filter und dem verwendeten Scope. Darüber hinaus muss der MS Exchange-Server auf der Rechner-ID installiert sein.

Geschützte Posteingänge/Posteingangslizenzen

Zeigt die Anzahl der geschützten Exchange-Server-Posteingänge sowie die Anzahl der verwendeten und verfügbaren Posteingangslizenzen an. Die Lizenzierung wird durchgesetzt, und für jedes benutzte Postfach ist eine Lizenz erforderlich.

Hinweis: Siehe **Endpoint Security-Lizenzierung** im Thema **Sicherheit – Übersicht** *(siehe 1)*.

Aktionen

- **Entfernen** – Deinstalliert die Exchange-Installation.
- **Anstehende Aktion abbrechen** – Bricht die Deinstallation des Exchange-Schutzes ab.

Tabellenspalten

- **Check-in-Status** – Diese Symbole geben den Agent-Anmeldestatus jedes verwalteten Rechners an. Wenn Sie den Cursor über ein Anmeldesymbol bewegen, wird das Agent-Schnellansichtsfenster angezeigt.
  - Online, aber in Wartestellung bis zum Abschluss des ersten Audits
  - Agent online
  - Agent online und Benutzer gegenwärtig angemeldet.
  - Agent online und Benutzer gegenwärtig angemeldet, doch Benutzer seit mehr als 10 Minuten nicht aktiv
  - Agent ist gegenwärtig offline
  - Agent hat nie eingecheckt.
  - Agent ist online, aber die Fernsteuerung wurde deaktiviert.
  - Agent wurde ausgesetzt.
- **(Kontrollkästchen 'Alle auswählen')** – Klicken Sie auf dieses Kontrollkästchen, um alle Zeilen im Seitenbereich auszuwählen. Falls das Kontrollkästchen aktiviert ist, klicken Sie auf dieses Kontrollkästchen, um die Auswahl aller Zeilen im Seitenbereich aufzuheben.
- **Rechner.Gruppen-ID** – Ein eindeutiger Rechner-ID/Gruppen-ID-/Organisations-ID-Name für einen Rechner im VSA.
- **Installationsstatus** – Ist diese Option markiert, wird die **Endpoint Security**-Client-Software auf der Rechner-ID installiert. Falls die Version der Agent-Software älter als 4.7.1 ist, wird die Meldung

`Aktualisierung des Agents erforderlich` angezeigt. Wenn diese Option nicht aktiviert ist, wird die **Endpoint Security**-Client-Software *nicht* auf der Rechner-ID installiert.

- **Installationsquelle** – Wenn eine Dateiquelle unter 'Patch-Management > **Dateiquelle** *(http://help.kaseya.com/webhelp/DE/VSA/7000000/index.asp#366.htm)*' definiert ist, werden die Installationspakete von diesem Speicherort heruntergeladen. Ansonsten werden sie aus dem Internet geladen. Wenn die Option **Aus dem Internet herunterladen, wenn der Rechner keine Verbindung zum Dateiserver herstellen kann** unter 'Patch-Management > Dateiquelle' ausgewählt wurde:
  - Falls während der Installation eines **Endpoint Security** v2.x-Endpunktes die Dateiquelle ausgefallen ist oder die Anmeldedaten ungültig sind, wird das Installationsprogramm vom Kaseya Server heruntergeladen. Das Installationsprogramm schließt dann die Endpunktinstallation ab.
  - Falls während einer manuellen **Endpoint Security** v2.x-Aktualisierung die Dateiquelle ausgefallen ist oder die Anmeldedaten ungültig sind, wird das Update aus dem Internet heruntergeladen.

  In den beiden oben genannten Fällen weist die Seite **Protokolle anzeigen** *(siehe 14)* in einer Fehlermeldung darauf hin, warum das Herunterladen von der Dateiquelle fehlgeschlagen ist und dass nun das Herunterladen aus dem Internet versucht wird.
- **Postfächer** – Dies ist die Anzahl der E-Mail-Konten auf dem MS Exchange-Server.
- **Installiert am** – Dies ist das Datum, an dem der E-Mail-Schutz des MS Exchange-Servers auf der Rechner-ID installiert wurde.

Alarm-Sets definieren

Sicherheit > Alarmsätze definieren

Auf der Seite **Alarmsätze definieren** werden Sätze von Alarmbedingungen definiert, die über die Seite **Alarmsätze anwenden** *(siehe 35)* eingestellte Alarme auslösen.

Aktionen

- **Speichern** – Speichern Sie den Alarmsatz.
- **Speichern unter** – Speichern Sie einen Alarmsatz unter einem neuen Namen.
- **Löschen** – Löschen Sie einen Alarmsatz.
- **Gemeinsam nutzen** – Wird angezeigt, wenn Sie Eigentümer eines ausgewählten Alarmsatzes sind. Nutzen Sie diesen Alarmsatz gemeinsam mit Benutzern und Benutzerrollen oder machen Sie ihn für alle Benutzer öffentlich. Freigaberechte werden *nach Objekt* zugewiesen. Es gibt drei Kontrollkästchenoptionen für die Freigabe. Die ersten beiden Kontrollkästchen *schließen einander aus* und bestimmen, welche Freigaberechte zugewiesen werden. Wird keins der beiden ersten Kontrollkästchen aktiviert, kann das Freigabeobjekt nur von den Benutzern gesehen werden, denen Freigabezugriff gewährt wurde. Das Objekt kann weder verwendet noch bearbeitet werden. Die Listenfelder **Freigegeben** und **Nicht freigegeben** und das dritte Kontrollkästchen bestimmen, wer das Objekt *sehen* kann.
  - **Anderen Administratoren gestatten zu ändern** – Wenn dies aktiviert ist, umfassen die Freigaberechte für das Objekt die Fähigkeit, es zu verwenden, seine Details anzuzeigen und es zu bearbeiten.
  - **Andere Administratoren dürfen verwenden, dürfen nicht anzeigen oder bearbeiten** – Wenn dies aktiviert ist, lassen die Freigaberechte für das Objekt nur dessen Verwendung zu.
  - **Als öffentlich festlegen (wird von allen Administratoren gesehen)** – Wenn dies aktiviert ist, wird sichergestellt, dass *alle* aktuellen und zukünftigen VSA-Benutzer das Objekt *sehen* können. Wenn es nicht aktiviert wird, können nur ausgewählte Benutzerrollen und Benutzer das Freigabeobjekt sehen. Wenn in diesem Fall später neue Benutzer oder Benutzerrollen hinzugefügt werden, müssen Sie zu diesem Dialogfeld zurückkehren und einstellen, dass sie das bestimmte Objekt sehen können.

- **Eigentumsrecht übernehmen** – Wird angezeigt, wenn Sie nicht der *Eigentümer* eines ausgewählten öffentlichen Alarmsatzes sind. Klicken Sie, um das **Eigentumsrecht** *(http://help.kaseya.com/webhelp/DE/VSA/7000000/index.asp#5537.htm)* zu übernehmen und Änderungen am Alarmsatz vorzunehmen.

So erstellen Sie einen neuen Alarmsatz:

1. Wählen Sie `<Keine gespeicherten Alarmsätze>` aus der Dropdown-Liste **Profil auswählen** aus. Sie können aber auch einen vorhandenen Alarmsatz auswählen und auf **Speichern unter** klicken.
2. Aktivieren Sie eins oder mehrere Kontrollkästchen für Meldungsbedingungen.
3. Geben Sie unter **Zusätzliche Alarme ignorieren für <N> <Perioden>** an, wie viele Minuten derselbe Satz an Meldungsbedingungen ignoriert werden soll. Stellen Sie dies auf 0 ein, um bei jedem Auftreten einer Meldungsbedingung einen Alarm auszulösen.
4. Klicken Sie auf **Speichern**, um den Alarmsatz zu speichern.

So löschen Sie einen Alarmsatz:

1. Wählen Sie einen Alarmsatz aus der Dropdown-Liste **Profil auswählen**.
2. Klicken Sie auf **Löschen**, um den Alarmsatz zu löschen.

Zusätzliche Alarme ignorieren für >N< >Perioden>

Geben Sie die Anzahl von Perioden an, für die derselbe Alarmtyp nach dem Auslösen des ersten Alarms ignoriert werden soll.

Alarmbedingungen

Markieren Sie beliebige der folgenden Alarmbedingungstypen, um sie in einen **Endpoint Security**-Alarmsatz einzuschließen.

- **Bedrohung ermittelt, jedoch nicht behoben** – Zur Registerkarte **Aktuelle Bedrohungen** der Seite **Bedrohungen anzeigen** *(siehe 12)* wurde eine Bedrohung hinzugefügt, die nicht automatisch behoben werden konnte.
- **Schutz deaktiviert** – Der Sicherheitsschutz wurde deaktiviert.
- **Definition aktualisiert** – Der Sicherheitsschutz wurde auf die neueste **Endpoint Security**-Version aktualisiert.
- **Geplanter Scan abgeschlossen** – Ein Sicherheitsschutz-Scan wurde abgeschlossen.
- **Neustart erforderlich** – Es ist ein Neustart erforderlich.
- **Schutz aktiviert** – Der Sicherheitsschutz wurde aktiviert.
- **Dienstfehler** – Der **Endpoint Security**-Dienst wurde gestoppt.
- **Definition nicht aktualisiert für <N> Tage** – Der Sicherheitsschutz wurde seit der angegebenen Anzahl von Tagen nicht aktualisiert.
- **Geplanter Scan wurde nicht abgeschlossen** – Ein geplanter Sicherheitsschutz-Scan wurde nicht abgeschlossen.
- **AVG von Benutzer entfernt** – Ein Rechnerbenutzer hat den AVG-Client auf dem verwalteten Rechner deinstalliert.

Alarm-Sets anwenden

Sicherheit >Alarmsätze anwenden

Auf der Seite **Alarmsätze anwenden** werden Meldungen als Reaktion auf Meldungsbedingungen des Sicherheitsschutzes erstellt, die über **Alarmsätze definieren** *(siehe 34)* definiert wurden. Die Alarmsätze werden auf ausgewählte Rechner-IDs mit **Endpoint Security**-Lizenzen angewendet.

Die Liste der auswählbaren Rechner-IDs basiert auf dem Rechner-ID-/Gruppen-ID-Filter und dem

verwendeten Scope. Damit Rechner-IDs auf dieser Seite angezeigt werden, muss die **Endpoint Security**-Client-Software über die Seite 'Sicherheit > **Installation** *(siehe 17)*' auf dem verwalteten Rechner installiert worden sein.

Auf dieser Seite können Sie vier Aktionen ausführen:

- **Anwenden** – Wenden Sie einen ausgewählten Alarmsatz auf ausgewählte Rechner-IDs an.
- **Entfernen** – Entfernen Sie einen ausgewählten Alarmsatz von ausgewählten Rechner-IDs.
- **Alle entfernen** – Entfernen Sie alle Alarmsätze, die ausgewählten Rechner-IDs zugewiesen wurden.

So erstellen Sie eine Meldung:

1. Aktivieren Sie beliebige dieser Kontrollkästchen, um bei Auftreten einer Meldungsbedingung die entsprechenden Aktionen auszuführen:
   - **A**larm erstellen
   - **T**icket erstellen
   - **S**kript ausführen
   - **E**-Mail-Empfänger
2. Legen Sie weitere E-Mail-Parameter fest.
3. Wählen Sie einen Alarmsatz aus.
4. Markieren Sie die Rechner-IDs, auf die der Alarmsatz angewendet werden soll.
5. Klicken Sie auf **Anwenden**, um den Alarmsatz auf ausgewählte Rechner-IDs anzuwenden.

So brechen Sie eine Meldung ab:

1. Markieren Sie Rechner-ID-Kontrollkästchen.
2. Klicken Sie auf **Entfernen**, um den zugewiesenen Alarmsatz von ausgewählten Rechner-IDs zu entfernen.

Optionen

- **Alarm erstellen** – Ist diese Option aktiviert und es tritt eine Meldungsbedingung ein, wird ein Alarm erstellt. Alarme werden unter 'Kontrolle > Dashboard-Liste', 'Kontrolle > Alarmübersicht' und 'Info Center > Berichterstellung > Berichte > Protokolle > Alarmprotokoll' angezeigt.
- **Ticket erstellen** – Ist diese Option aktiviert und es tritt eine Meldungsbedingung auf, wird ein Ticket erstellt.
- **Skript nach Meldung ausführen** – Wenn dies aktiviert ist und eine Meldungsbedingung auftritt, wird ein Agent-Verfahren ausgeführt. Sie müssen auf den Link **Agent-Verfahren auswählen** klicken, um ein auszuführendes Agent-Verfahren zu wählen. Sie können das Agent-Verfahren optional anweisen, in einem angegebenen Bereich von Rechner-IDs zu laufen, indem Sie auf den Link **diese Rechner-ID** klicken. Diese angegebenen Rechner-IDs müssen nicht der Rechner-ID aus der Meldungsbedingung entsprechen.
- **E-Mail-Empfänger** – Ist diese Option aktiviert und es tritt eine Meldungsbedingung ein, werden E-Mails an die angegebenen E-Mail-Adressen gesendet. E-Mails werden vom VSA direkt an die in der Meldung angegebene E-Mail-Adresse gesendet. Den **Absender** können Sie über 'System > Ausgehende E-Mail' festlegen.
- **Alarmsatz auswählen** – Wählen Sie einen Alarmsatz aus, der auf ausgewählte Rechner-IDs angewendet werden soll.

Tabellenspalten

- **(Check-in-Status)** – Diese Symbole geben den Agent-Anmeldestatus jedes verwalteten Rechners an. Wenn Sie den Cursor über ein Anmeldesymbol bewegen, wird das Agent-Schnellansichtsfenster angezeigt.
  - Online, aber in Wartestellung bis zum Abschluss des ersten Audits
  - Agent online

 Agent online und Benutzer gegenwärtig angemeldet.

 Agent online und Benutzer gegenwärtig angemeldet, doch Benutzer seit mehr als 10 Minuten nicht aktiv

 Agent ist gegenwärtig offline

 Agent hat nie eingecheckt.

 Agent ist online, aber die Fernsteuerung wurde deaktiviert.

 Agent wurde ausgesetzt.

- **(Kontrollkästchen 'Alle auswählen')** – Klicken Sie auf dieses Kontrollkästchen, um alle Zeilen im Seitenbereich auszuwählen. Falls das Kontrollkästchen aktiviert ist, klicken Sie auf dieses Kontrollkästchen, um die Auswahl aller Zeilen im Seitenbereich aufzuheben.
- **Rechner.Gruppen-ID** – Ein eindeutiger Rechner-ID/Gruppen-ID-/Organisations-ID-Name für einen Rechner im VSA.
- **Alarmsatz** – Listet die Alarmsätze auf, die den einzelnen Rechner-IDs zugewiesen wurden.
- **ATSE** – Der ATSE-Antwortcode, der Rechner-IDs oder SNMP-Geräten zugewiesen wird:
  - A = **A**larm erstellen
  - T = **T**icket erstellen
  - S = Agent-Verfahren ausführen
  - E = **E**-Mail-Empfänger
- **E-Mail-Adresse** – Eine kommagetrennte Liste von E-Mail-Adressen, an die Benachrichtigungen gesendet werden.

Sicherheitsberichte

Die folgenden Datensätze stehen bei der Erstellung von benutzerdefinierten **Endpoint Security**-Berichtsdefinitionen und Berichtsvorlagen zu Verfügung. Sie finden sie unter 'Info Center > Konfiguration und Design > **Berichtsteile**.

- KES-Alarmsatz
- Zuweisung des KES-Alarmsatzes
- KES-Ereignisprotokoll
- KES Exchange-Status
- KES-Rechnerstatus
- KES-Bedrohungen
- KES-Bedrohungsstatistiken

Darüber hinaus sind die folgenden Berichtsdefinition im nicht anpassbaren Format verfügbar.

In diesem Abschnitt

Executive Summary – Endpunktsicherheit 37
Sicherheit – Konfiguration 38
Sicherheit – Aktuelle Bedrohungen 38
Sicherheit – Historische Bedrohungen 39
Sicherheit – KES-Protokoll 39

Executive Summary – Endpunktsicherheit

Executive Summary

Der Bericht unter 'Info Center > Berichterstellung > Berichte > Executive Summary' enthält

einen Abschnitt namens **Endpunktsicherheit der letzten N Tage**. Er umfasst die folgenden Statistiken.

- Gesamtzahl der ermittelten Bedrohungen
- Aktuelle aktive Bedrohungen
- Aktuelle Bedrohungen im Tresor
- Aufgelöste Bedrohungen
- Abgeschlossene Scans
- Durchgeführte Aktualisierungen
- Rechner, auf denen KES installiert ist

Der Abschnitt **Netzwerk-Leistungsauswertung** der **ausführenden Zusammenfassung** enthält die Kategorie **Endpunktbewertung**. Nicht behandelte Bedrohungen sind Bedrohungen, die auf der Registerkarte **Aktuelle Bedrohungen** der Seite 'Sicherheit > **Bedrohungen anzeigen** *(siehe 12)*' aufgeführt werden. Nicht behandelte Bedrohungen stellen potenzielle Systemprobleme dar. Die Anzahl der nicht behandelten Bedrohungen, die von jedem Rechner über den vorgegebenen Zeitraum generiert wurden, werden folgendermaßen bewertet:

0 nicht behandelte Bedrohungen	100%
1 bis 4 nicht behandelte Bedrohungen	75%
5 bis 10 nicht behandelte Bedrohungen	50%
mehr als 10 nicht behandelte Bedrohungen	25%

Sie können einstellen, wie sich jede Kategorie auf die ganze **Netzwerk-Leistungsbewertung** auswirkt, indem Sie den **Stellenwert** jeder Kategorie justieren. Die Stellenwerte reichen von 0 bis 100. Stellen Sie den Stellenwert auf Null ein, um diese Kategorie zu deaktivieren.

Sicherheit – Konfiguration

Info Center > Reporting > Berichte > Sicherheit > Konfiguration

- Wird nur angezeigt, wenn das Sicherheits-Zusatzmodul installiert ist.
- Ähnliche Informationen werden über Sicherheit > Sicherheitsstatus *(siehe 5)*, Protokolle anzeigen *(siehe 14)* und Bedrohungen anzeigen *(siehe 12)* bereitgestellt.

Mit der Berichtsdefinition **Sicherheit – Konfiguration** werden Berichte für die folgenden Arten von Sicherheitsdaten generiert, die vom VSA gepflegt werden.

- Installationszeit
- Installer
- Version
- Ablaufdatum der Lizenz
- Zugewiesenes Profil
- Profildetails
- Alarmeinstellungen

Sicherheit – Aktuelle Bedrohungen

Info Center > Reporting > Berichte > Sicherheit > Aktuelle Bedrohungen

- Wird nur angezeigt, wenn das Sicherheits-Zusatzmodul installiert ist.
- Ähnliche Informationen werden über Sicherheit > Sicherheitsstatus *(siehe 5)*, Protokolle anzeigen *(siehe 14)* und Bedrohungen anzeigen *(siehe 12)* bereitgestellt.

Mit der Berichtsdefinition **Sicherheit – Aktuelle Bedrohungen** werden Berichte für die folgenden Arten von Sicherheitsdaten generiert, die vom VSA gepflegt werden.

- Übersicht
- Übersicht über Bedrohungskategorie
- Aktuelle Bedrohungen

Zeitauswahl

- **Zeitbereichstyp auswählen** – Filtert Daten nach einem bestimmten Typ von Datumsbereich.
- **Anzahl der Tage** – Diese Option ist nur anwendbar, wenn `Letzte N Tage` als Zeitbereichstyp ausgewählt ist.
- **Benutzerdefinierte(s) Startdatum/-zeit** – Diese Option ist nur anwendbar, wenn `Festgelegter Bereich` als Zeitbereichstyp ausgewählt ist.
- **Benutzerdefinierte(s) Enddatum/-zeit** – Diese Option ist nur anwendbar, wenn `Festgelegter Bereich` als Zeitbereichstyp ausgewählt ist.

Sicherheit – Historische Bedrohungen

Info Center > Reporting > Berichte > Sicherheit > Historische Bedrohungen

- Wird nur angezeigt, wenn das Sicherheits-Zusatzmodul installiert ist.
- Ähnliche Informationen werden über Sicherheit > Sicherheitsstatus *(siehe 5)*, Protokolle anzeigen *(siehe 14)* und Bedrohungen anzeigen *(siehe 12)* bereitgestellt.

Mit der Berichtsdefinition **Sicherheit – Historische Bedrohungen** werden Berichte für die folgenden Arten von Sicherheitsdaten generiert, die vom VSA gepflegt werden.

- Übersicht
- Übersicht über Bedrohungskategorie
- Aktuelle Bedrohungen

Zeitauswahl

- **Zeitbereichstyp auswählen** – Filtert Daten nach einem bestimmten Typ von Datumsbereich.
- **Anzahl der Tage** – Diese Option ist nur anwendbar, wenn `Letzte N Tage` als Zeitbereichstyp ausgewählt ist.
- **Benutzerdefinierte(s) Startdatum/-zeit** – Diese Option ist nur anwendbar, wenn `Festgelegter Bereich` als Zeitbereichstyp ausgewählt ist.
- **Benutzerdefinierte(s) Enddatum/-zeit** – Diese Option ist nur anwendbar, wenn `Festgelegter Bereich` als Zeitbereichstyp ausgewählt ist.

Sicherheit – KES-Protokoll

Info Center > Reporting > Berichte > Sicherheit > KES-Protokoll

- Wird nur angezeigt, wenn das Sicherheits-Zusatzmodul installiert ist.
- Unter Agent > Agent-Protokolle werden Protokolleinträge nach Protokolltyp und Rechner-ID angezeigt.

Mit der Berichtsdefinition KES-Protokoll wird ein Bericht der Endpoint Security-Protokolleinträge nach Rechner-ID generiert.

Konfigurieren Sie Ihre Berichtsoption unter Verwendung der folgenden Parameter:

- **Anzahl der Tage, die das Protokoll durchsucht werden soll*** – Anzahl der Tage rückwirkend vom aktuellen Datum/Uhrzeit, die in den Bericht eingeschlossen werden sollen
- **Einträge anzeigen, die folgender Beschreibung entsprechen (* als Stellvertreterzeichen verwenden)** – Geben Sie eine Zeichenfolge ein, um Einträge nach ihrer Beschreibung zu filtern. Schließend Sie ein Sternchen (*) in den eingegebenen Text ein, um Übereinstimmungen mit mehreren Datensätzen zu finden.

- **Rechner ohne Daten ignorieren** – Aktivieren Sie diese Option, wenn nur Rechner-IDs mit Daten angezeigt werden sollen, die den anderen Filterparametern entsprechen.

Inhaltsverzeichnis

A

Alarm-Sets anwenden • 35
Alarm-Sets definieren • 34

B

Bedrohungen anzeigen • 12
Benachrichtigen • 16

D

Dashboard • 4

E

Endpoint Security-Modulanforderungen • 4
Erweitern/Zurück • 15
Exchange-Status • 33
Executive Summary – Endpunktsicherheit • 37

I

Installation
    Sicherheit • 17
Installation oder Aktualisierung eines Endpunktes • 21
Installationsoptionen • 22

M

Manuelle Aktualisierung • 9

P

Profil definieren • 23
Profil zuweisen • 31
Protokolle anzeigen • 14
Protokolleinstellungen
    Sicherheit • 32

R

Resident Shield durch Agent-Verfahren
  aktivieren/deaktivieren • 8

S

Scan planen • 11
Sicherheit – Aktuelle Bedrohungen • 38
Sicherheit – Historische Bedrohungen • 39
Sicherheit – KES-Protokoll • 39
Sicherheit – Konfiguration • 38
Sicherheit – Übersicht • 1
Sicherheitsberichte • 37
Sicherheitsstatus • 5

W

Willkommen • 1