Antivirus

Benutzerhandbuch

Version R9

Deutsch

März 19, 2015

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

Überblick über Antivirus

Antivirus (KAV) bietet unter Verwendung von Kaspersky Antivirus Endpunktsicherheit für verwaltete Rechner. **Antivirus** schützt Ihren Computer vor bekannten und neuen Bedrohungen. Die verschiedenen Bedrohungstypen werden von separaten Anwendungskomponenten verarbeitet, von denen jede über ein Konfigurationsprofil aktiviert bzw. deaktiviert werden kann. Mithilfe von Konfigurationsprofilen können Sie schnell unterschiedliche **Antivirus**-Lösungstypen gleichzeitig auf viele Rechner anwenden. **Antivirus** kann unabhängig von **Endpoint Security** und **AntiMalware** installiert werden.

Antivirus enthält die folgenden Schutztools:

- Speicherresidente Schutzkomponenten für:
  - Server und Workstations mit jeweils eigenen Lizenzen
  - Dateien und persönliche Daten
  - System
  - Netzwerk
- Geplante, wiederholte Virenscans einzelner Dateien, Ordner, Laufwerke, Bereiche oder des gesamten Computers
- Updates der **Antivirus**-Clients und deren Komponenten sowie der beim Scannen nach bösartigen Programmen eingesetzten **Antivirus**-Definitionsdatenbanken
- Status-Dashboard für alle von **Antivirus** verwalteten Rechner
- Eine Erkennungsseite für alle Virenbedrohungen, die nicht automatisch von **Antivirus** beseitigt werden können
- Über Modul verwaltete Meldungen.
- Überprüfung durch das Windows-Sicherheitscenter
- 'Upgrade verfügbar'-Option, mit der Sie veraltete **Antivirus**-Clients identifizieren und aktualisieren können.
- Über die Richtlinien-Verwaltung können Zuweisungen von **Antivirus**-Profilen verwaltet werden.
- Spezielle Agent-Verfahren werden zusammen mit **Antivirus** bereitgestellt, mit deren Hilfe Sie das **Antivirus**-Installationspaket im Voraus auf Endpunkten bereitstellen und so die während der Installation erforderliche Bandbreite reduzieren können. Lesen Sie dazu den **Knowledge Base-Artikel** *(https://helpdesk.kaseya.com/entries/34261116)*.
- **Anpassung der Benutzeroberfläche des Antivirus-Clients auf dem Endpunkt** *(https://helpdesk.kaseya.com/entries/32410117)*

> **Hinweis:** **Antivirus** 6.5 unterstützt für Workstation- und Server-Endpunkte sowohl Kaspersky Version 10 als auch die Legacy-Version 6. Für die Verwaltung jedes Rechnertyps werden spezielle Profile bereitgestellt. *Endpunkte mit Kaspersky Version 2010 werden von* **Antivirus** *6.5 nicht unterstützt.* **Antivirus** 6.5 installiert bzw. aktualisiert Endpunkte nur auf Kaspersky Version 10. *Version 10 wird dringend empfohlen.* Sie können über die Schaltfläche 'Installieren > **Client-Version aktualisieren**' in der Systemsteuerung einen Endpunkt mit Kaspersky Version 6 auf Version 10 aktualisieren.

LAN-Cache

Der LAN-Cache ermöglicht, dass mehrere Rechner dieselben Dateien von einem lokalen LAN-Rechner abrufen, anstatt diese wiederholt vom Kaseya Server herunterladen zu müssen. Dadurch werden Engpässe bei der Netzwerkbandbreite vermieden. Dateien, die für **Antivirus**-Endpunkte heruntergeladen werden – Installationspakete, Aktualisierungen und Virendefinitionen –, verwenden den LAN-Cache automatisch, sofern dieser bereits für diese Endpunkte konfiguriert ist. Zusätzliche Konfiguration in **Antivirus** ist nicht erforderlich. Nähere

Informationen finden Sie unter 'Agent > **LAN-Cache** *(http://help.kaseya.com/webhelp/DE/VSA/9000000/index.asp#9328.htm)*'.

Hinweis: Siehe **Antivirus-Systemanforderungen** *(siehe 3)*.

Funktionen	Beschreibung
Rechner *(siehe 3)*	Installiert bzw. deinstalliert Antivirus-Software auf ausgewählten Rechnern und bietet eine detaillierte Ansicht des Antivirus-Status ausgewählter Rechnern.
Dashboards *(siehe 13)*	Bietet eine Dashboard-Ansicht des Status aller Rechner, auf denen Antivirus installiert ist.
Erkennungen *(siehe 14)*	Zeigt Virenbedrohungen an, gegen die Sie Maßnahmen ergreifen können.
Profile *(siehe 15)*	Verwaltet Antivirus-Profile, die Rechner-IDs zugewiesen sind.
Meldungen *(siehe 26)*	Verwaltet Antivirus-Modulmeldungen.

Antivirus-Modulanforderungen

Kaseya Server

- Das Antivirus R9-Modul setzt VSA R9 voraus.

Agent-Anforderungen

- KAV R9 setzt die Agent-Version R9.0.0 oder höher voraus.

Anforderungen für verwaltete Workstations

- 1 GHz CPU oder schneller
- 1 GB verfügbarer RAM
- 1 GB freier Speicherplatz auf der Festplatte
- Microsoft Windows XP SP3, Vista, 7, 8, 8.1 werden unterstützt.
- Microsoft Windows Installer 3.0
- Unter **Kaspersky Anti-Virus für Windows Workstation Version 10.x** *(http://support.kaspersky.com/kes10wks#requirements)* finden Sie eine vollständige Liste der Systemanforderungen für Workstations.

Anforderungen für verwaltete Server

- Server 2003, 2003 R2, SBS 2003 R2, 2008 SP1, SBS 2008 SP1, 2008 R2 SP1, SBS 2011, 2012, 2012 R2 werden unterstützt.
- Nur das Betriebssystem von SBS 2011 wird unterstützt. Die von SBS 2011 gehosteten Exchange E-Mail-Server sind davon ausgeschlossen.
- Unter **Kaspersky Anti-Virus für Windows Server Version 10.x** *(http://support.kaspersky.com/kes10fs#requirements)* finden Sie eine vollständige Liste der Systemanforderungen für Server, *einschließlich des für die einzelnen Betriebssysteme erforderlichen Service Packs*.

Hinweis: Siehe allgemeine **Systemanforderungen** *(http://help.kaseya.com/WebHelp/EN/VSA/9000000/reqs/index.asp#home.htm).*

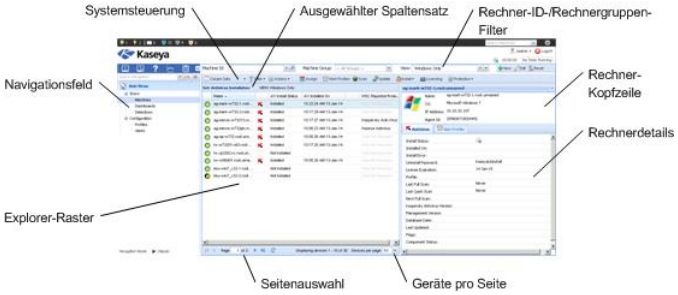
Rechner

Antivirus > Anzeigen > Rechner

Über die Seite **Rechner** können Sie die **Antivirus**-Software auf ausgewählten Rechnern installieren bzw. deinstallieren. Dieselbe Seite bietet darüber hinaus eine detaillierte Ansicht des **Antivirus**-Status aller ausgewählten Rechner.

Seitenlayout

Das Layout der Seite **Rechner** *(siehe 3)* setzt sich aus den folgenden Designelementen zusammen:



- **Navigationsfeld** – Ermöglicht die Navigation zu verschiedenen Seiten des **Antivirus**-Moduls.
- **Explorer-Fenster** – Eine Liste mit allen im VSA verwalteten Rechnern.
  - **Seitenbrowser** – Ermöglicht den Wechsel zwischen Seiten, falls mehr als eine Seite mit Rechnern vorhanden ist.
  - **Zeilen pro Seite** – Legt die Anzahl der Rechner fest, die pro Seite angezeigt werden sollen: 10, 30 oder 100.
- **Rechner-ID-/Gruppen-ID-Filter** – Filtert die Liste der im **Explorer-Fenster** aufgeführten Rechner-IDs.
- **Systemsteuerung** – Führt Aufgaben entweder für das gesamte **Explorer-Fenster** oder für einen einzelnen ausgewählten Rechner aus.
- **Detailfeld** – Dieses Feld zeigt die Eigenschaften und den Status eines einzelnen Rechners an.
  - **Kopfleiste** – Identifiziert den im **Explorer-Fenster** ausgewählten Rechner.
  - **Antivirus** – Zeigt eine Übersicht über den **Antivirus**-Status eines Rechners an.
  - **Meldungsprofile** – Führt die einem Rechner zugewiesenen Meldungsprofile auf.

Explorer-Fenster

Das **Explorer-Fenster** der Seite **Rechner** *(siehe 3)* führt alle Rechner auf, auf denen gegenwärtig **Antivirus** installiert ist *und* die vom **Rechner-ID-/Gruppen-ID-Filter** *(http://help.kaseya.com/webhelp/DE/VSA/9000000/index.asp#209.htm)* erfasst werden.

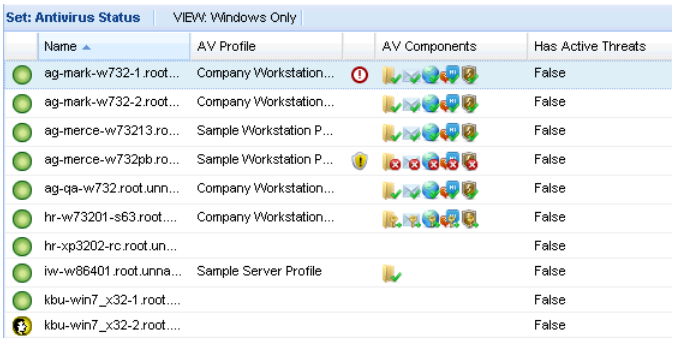
> **Hinweis:** Die einzige Ausnahme liegt bei Auswahl der `Antivirus- Installation` vor. In diesem Fall werden alle Rechner aufgeführt, die vom Rechner-ID-/Gruppen-ID-Filter erfasst werden.

- Die angezeigten *Spaltensätze* hängen von der unter **Spaltensatz** in der **Systemsteuerung** *(siehe 6)* getroffenen Auswahl ab. Der gegenwärtig gewählte Spaltensatz wird in der Leiste direkt über dem **Explorer-Fenster** angezeigt.

  > **Hinweis:** Unter **Antivirus-Spalten** *(siehe 9)* finden Sie eine Beschreibung aller Spalten, die in *allen* Spaltensätzen des **Explorer-Fensters** angezeigt werden können.

- 'Seite vor' zeigt mehrere Seiten mit Rechner an.

- 'Rechner pro Seite' legt die Anzahl der pro Seite angezeigten Zeilen fest.



Spaltensymbole

	Definitionen sind veraltet.
	Neustart erforderlich.
	Vollständiger Scan wird ausgeführt.
	Lizenz ist abgelaufen.
	Endpunkt-Konfiguration stimmt nicht mit dem Profil überein.
	Zuweisung steht an.
	Aktivierung steht an.
	Deaktivierung steht an.
	Scan steht an.
	Deinstallation steht an.
	Bestätigung steht an.
	Installation steht an.
	Update steht an.
	Installation ist fehlgeschlagen.
	Installation war erfolgreich.
	Endpoint Security ist auf diesem Rechner installiert.

Konventionen der Komponentensymbole

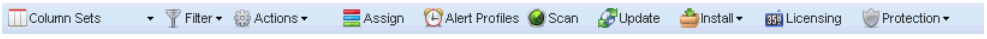
Befindet sich der Mauszeiger über einem Komponentensymbol, wird ein Quickinfo mit der Beschreibung des Status dieser Komponente eingeblendet. Im Allgemeinen werden bei den Komponentensymbolen die folgenden Konventionen verwendet:

Status	Typ des angezeigten Symbols	Beispiel: Dateischutzsymbole
Deaktiviert	graues X-Zeichen	

Versagen	gelbes Ausrufezeichen	
Läuft/Aktiviert	grünes Häkchen	
Startet	ein Schlüssel mit einem grünen Pfeil	
Gestoppt	rotes X-Zeichen	
Wird gestoppt	ein Schlüssel mit rotem Minuszeichen	

Systemsteuerung

Die **Systemsteuerung** oben auf der Seite **Rechner** *(siehe 3)* führt Aufgaben entweder für das gesamte **Explorer-Fenster** *(siehe 4)* oder für einen einzelnen ausgewählten Rechner aus.



Spaltensätze

Über diese Schaltfläche können Sie einen der verschiedenen vordefinierten Spaltensätze auswählen.

- **Spalten anpassen** – Passt den angezeigten Spaltensatz an. Diese Funktion kann auf *alle* Spaltensätze angewendet werden.

  Hinweis: Unter **Antivirus-Spalten** *(siehe 9)* finden Sie eine Beschreibung aller Spalten, die in *allen* Spaltensätzen des **Explorer-Fensters** angezeigt werden können.

- **Antivirus-Installation** – Zeigt die **Antivirus**-Installationsspalten *aller Agent-Rechner* im **Explorer-Fenster** an.
- **Antivirus-Status** – Zeigt die Statusspalten aller Agent-Rechner im **Explorer-Fenster** an, *auf denen ein* **Antivirus**-*Client installiert ist*.

Filter

Filtert die Liste der angezeigten Zeilen anhand der installierten Software, des empfohlenen Upgrades, eines erforderlichen Neustarts, veralteter Definitionen, mangelnder Übereinstimmung von Rechnern mit ihrem Profil, der neuesten installierten Version oder nicht unterstützter Clients.

Hinweis: Der Filter `Antivirus-Upgrade empfohlen` hilft bei der Identifikation der Rechner, die für ein Upgrade auf die neueste Version in Frage kommt. Installieren Sie das Upgrade einfach über die vorhandene **Antivirus**-Installation.

Aktionen

- **Anstehende Aktion abbrechen** – Bricht anstehende Aktionen auf ausgewählten Rechnern ab.
- **Neu starten** – Startet ausgewählte Rechner neu.

Zuweisen

Weist ausgewählten Rechnern ein **Antivirus**-Konfigurationsprofil zu. Workstations und Server können gleichzeitig ausgewählt und zugewiesen werden. Sie brauchen Ihre Auswahl nicht auf entweder Workstations oder Server beschränken. Workstations wird das ausgewählte Workstation-Profil zugewiesen. Servern wird das ausgewählte Serverprofil zugewiesen. Weitere Informationen finden Sie unter **Profile** *(siehe 15)*.

Meldungsprofile

Weist ausgewählten Rechnern ein Meldungsprofil zu bzw. entfernt dieses. Die Registerkarte **Meldungsprofile** im **Detailfeld** *(siehe 11)* zeigt alle einem Rechner zugewiesenen Profile an.

Scannen

Legt auf ausgewählten Rechnern den Zeitpunkt eines **Antivirus**-Scans fest.

- **Startdatum** – Das Startdatum des Scans.
- **Zeit** – Die Startzeit des Scans.
- **Verteilungsfenster** – Plant mehrfache Scans gleichmäßig über einen Zeitraum verteilt neu (nicht später als die angegebene Anzahl von Perioden), um den Datenverkehr und die Serverlast zu verteilen.

Bei **Antivirus** sind zwei Scan-Typen möglich:

- **Vollständiger Scan** – Ein gründlicher Scan des gesamten Systems. Die folgenden Objekte werden standardmäßig gescannt: Systemspeicher, beim Start geladene Programme, System-Backup, E-Mail-Datenbanken, Festplatten, Wechseldatenträger und Netzwerklaufwerke.
- **Schnell-/Kritischer Scan** – Virenscan der Startobjekte des Betriebssystems. Ab **Antivirus** Version 10.x wurde der Schnellscan in kritischer Scan umbenannt.

Aktualisieren

Legt auf ausgewählten Rechnern den Zeitpunkt einer Aktualisierung mit den neuesten **Antivirus**-Definitionen fest.

- **Startdatum** – Das Startdatum der Aktualisierung.
- **Zeit** – Die Startzeit der Aktualisierung.
- **Verteilungsfenster** – Plant mehrfache Scans Aktualisierungen über einen Zeitraum verteilt neu (nicht später als die angegebene Anzahl von Perioden), um den Datenverkehr und die Serverlast zu verteilen.

Installieren

- **Antivirus installieren oder aktualisieren** – Installiert bzw. aktualisiert den **Antivirus**-Client auf ausgewählten Rechnern.

> **Warnung:** Kaseya unterstützt die Installation von Agents im `%windir%` (normalerweise `c:\windows`)-Verzeichnis nicht.

  - **Profilauswahl** – Es können mehrere Workstations und Server gleichzeitig ausgewählt und installiert werden. Workstations wird das ausgewählte Workstation-Profil zugewiesen. Servern wird das ausgewählte Serverprofil zugewiesen. Nur Workstation- und Serverprofile der Version 10.x können ausgewählt werden.
  - **Neustart zulassen** – Ist diese Option markiert, wird bei Bedarf ein Neustart durchgeführt. Nur bei Workstations ist nach einer Installation ein Neustart erforderlich.
  - **Erweiterte Optionen** – Klicken Sie darauf, um die folgenden Optionen anzuzeigen.
    - ✓ **Start-Datum/Zeit** – Das Startdatum und die Startzeit der Installation.
    - ✓ **Verteilungsfenster** – Plant mehrfache Installationen gleichmäßig über einen Zeitraum verteilt neu (nicht später als die angegebene Anzahl von Perioden), um den Datenverkehr und die Serverlast zu verteilen.
    - ✓ **Vor Installation auffordern** – Ist diese Option markiert, wird die Installation nur fortgesetzt, wenn der Benutzer angemeldet ist und der Fortsetzung zustimmt.
    - ✓ **Überspringen, wenn offline** – Ist diese Option markiert und der Rechner zum Zeitpunkt der geplanten Installation offline, wird die Installation übersprungen. Wird das Kontrollkästchen nicht markiert, erfolgt die Installation, sobald der Computer wieder online ist.

- ✓ **Passwort** – Hier können Sie ein Passwort für diesen Rechner eingeben. Passwörter verhindern eine unbefugte Deinstallation oder Neukonfiguration. Wenn Sie das Kontrollkästchen nicht markieren, wird das Standardpasswort verwendet. Das Passwort wird im **Detailfeld** *(siehe 11)* angezeigt. Es muss aus alphanumerischen Zeichen bestehen. Sonderzeichen werden nicht unterstützt.

  Warnung: Das Passwort kann nur während der anfänglichen Installation eingerichtet werden. Um ein vorhandenes Passwort zu ändern, müssen Sie den Endpunkt deinstallieren.

- ✓ **Installation blockierende Probleme** – Führt Probleme auf, die eine erfolgreiche Installation auf ausgewählten Rechnern blockieren können.

Hinweis: Spezielle Agent-Verfahren werden zusammen mit **Antivirus** bereitgestellt, mit deren Hilfe Sie das **Antivirus**-Installationspaket im Voraus auf Endpunkten bereitstellen und so die für die Installation erforderlicher Bandbreite reduzieren können. Lesen Sie dazu den **Knowledge Base-Artikel** *(https://helpdesk.kaseya.com/entries/34261116)*.

- **Antivirus deinstallieren** – Deinstalliert den **Antivirus**-Client von ausgewählten Rechnern.
  - **Startdatum** – Das Startdatum der Deinstallation
  - **Zeit** – Die Startzeit der Deinstallation
  - **Verteilungsfenster** – Plant mehrfache Deinstallationen gleichmäßig über einen Zeitraum verteilt neu (nicht später als die angegebene Anzahl von Perioden), um den Datenverkehr und die Serverlast zu verteilen.
- **Antivirus-Installation reparieren** – Installiert fehlende Dateien auf einem zuvor installierten **Antivirus**-Client neu, um die Installation zu reparieren. Bei der früheren Installation des **Antivirus**-Clients muss derselbe VSA verwendet worden sein.
  - **Startdatum** – Das Startdatum der Reparatur
  - **Zeit** – Die Startzeit der Reparatur
  - **Verteilungsfenster** – Plant mehrfache Reparaturen gleichmäßig über einen Zeitraum verteilt neu (nicht später als die angegebene Anzahl von Perioden), um den Datenverkehr und die Serverlast zu verteilen.
- **Kaseya Antivirus verbinden** – Stellt erneut eine Verbindung zu einem zuvor von **Antivirus** verwalteten Rechner her, auf dem der Kaseya Agent jedoch zwischenzeitlich entfernt und wieder neu installiert wurde. Dies gilt auch für die Herstellung einer neuen Verbindung zu Rechnern, die von einem anderen VSA verwaltet wurden.
  - **Startdatum** – Das Startdatum der Verbindungsherstellung
  - **Zeit** – Die Startzeit der Verbindungsherstellung
  - **Verteilungsfenster** – Plant mehrfache Verbindungsherstellungen gleichmäßig über einen Zeitraum verteilt neu (nicht später als die angegebene Anzahl von Perioden), um den Datenverkehr und die Serverlast zu verteilen.
  - **Profilauswahl** – Wählt die anzuwendenden Workstations- und Serverprofile aus.

Lizenzierung

- **Lizenzanzahl** – Führt die Anzahl der **Antivirus**-Lizenzen für Server und Workstations auf. Lizenzen für Server und Workstations werden separat erworben und verwaltet. **Antivirus**-Lizenzzahlen werden ebenfalls auf der Seite 'Administration > Verwalten > **Lizenzmanager** *(http://help.kaseya.com/webhelp/DE/VSA/9000000/index.asp#2924.htm)*' angezeigt.
  - Gesamt gekauft aktuell
  - Voll verfügbar (erworbene Lizenzen nicht zugewiesen, angewendet, partiell oder abgelaufen)
  - Zugewiesen (für Installation geplant, doch die Installation ist noch nicht abgeschlossen)

- Angewendet (aktive Lizenz auf einem Rechner angewendet)
- Teilweise verfügbar (zuvor einem Rechner zugewiesen, doch vor Ablauf an den Pool zurückgegeben)
- Teilweise zugewiesen (teilweise verfügbar und für Installation geplant, doch die Installation ist noch nicht abgeschlossen)
- Insgesamt (erworbene Lizenzen, abzüglich der abgelaufenen)
- Abgelaufene Lizenzen
- Lizenzen, die in den nächsten 30 Tagen ablaufen
- Lizenzen, die in den nächsten 60 Tagen ablaufen
- Lizenzen, die in den nächsten 90 Tagen ablaufen

Schutz

- **Status abrufen** – Gibt den aktivierten/deaktivierten Status von **Antivirus**-Komponenten eines Rechners zurück und korrigiert gegebenenfalls die Anzeige des entsprechenden Statussymbols im **Explorer-Fenster**. Gibt ebenfalls Versionsinformationen der Installation und Datenbanksignatur zurück.
- **Antivirus vorübergehend aktivieren** – Aktiviert vorübergehend den **Antivirus**-Schutz auf ausgewählten Rechnern.
- **Antivirus vorübergehend deaktivieren** – Deaktiviert vorübergehend den **Antivirus**-Schutz auf ausgewählten Rechnern. Bei einigen Softwareinstallationen muss die **Antivirus**-Software vorübergehend deaktiviert werden, damit die Installation abgeschlossen werden kann.

Antivirus-Spalten

Spaltensätze legen fest, welche Spalten im **Explorer-Fenster** *(siehe 4)* angezeigt werden. Sie können *alle* Spaltensätze bearbeiten, die in der Dropdown-Liste **Spaltensatz** der **Systemsteuerung** *(siehe 6)* aufgeführt werden.

1. Wählen Sie dazu einen Spaltensatz aus der Dropdown-Liste **Spaltensatz** aus.
2. Wählen Sie die Option **Spalten anpassen** aus derselben Dropdown-Liste aus, um das Fenster **Spaltensatz bearbeiten** anzuzeigen.

   Die der rechten Liste zugewiesenen Spalten werden nach Speichern der am Spaltensatz vorgenommenen Änderungen angezeigt.

Die folgenden Spalten können in *allen* Spaltensätzen des **Explorer-Fensters** *(siehe 4)* für die Anpassung ausgewählt werden. Wählen Sie in der **Systemsteuerung** *(siehe 6)* die Option **Spaltensatz**, um einen Spaltensatz anzupassen.

Antivirus

- **AV-Ablaufdatum** – Das Datum, an dem der **Antivirus**-Schutz abläuft.
- **AV-Installationsstatus** – `Nicht installiert`, `Skript geplant`,`Installiert`
- **Symbol der Installationsphase** – Hat das Symbol ein Häkchen, ist **Antivirus** auf dem Rechner installiert.

Erkennungen

- **Gelöscht** – Anzahl der Erkennungen, die automatisch gelöscht wurden.
- **Erkannt** – Anzahl der Erkennungen
- **Desinfiziert** – Anzahl der Erkennungen, die automatisch desinfiziert wurden.
- **Aktive Bedrohungen** – Zeigt die erkannten Bedrohungen an, die nicht automatisch desinfiziert oder gelöscht werden konnten und die die Aufmerksamkeit des Benutzers erfordern.
- **Infiziert** – Anzahl der infizierten Erkennungen

- **Andere** – Anzahl von Erkennungen, die unter keine der anderen Kategorien fallen. Dies geschieht, wenn Kaspersky eine neue Erkennungskategorie eingeführt hat, die **Antivirus** noch nicht erkennt.
- **Verdächtig** – Die Anzahl der verdächtigen Erkennungen, die nicht desinfiziert oder gelöscht wurden und die sich ein Benutzer näher ansehen sollte.

Endpunktschutz

- **Agent-GUID-Zeichenfolge** – Die eindeutige GUID des Kaseya-Agents als Zeichenfolge.
- **ID** – Die eindeutige GUID des Kaseya-Agents im numerischen Format.
- **Letzter Neustart** – Datum und Uhrzeit des letzten Neustarts des Rechners
- **Login-Name** – Der gegenwärtig angemeldete Benutzer
- **Name** – Die Rechner-ID.Gruppen-ID.Organisations-ID des Rechners
- **Online-Status** – Diese Symbole geben den Agent-Anmeldestatus jedes verwalteten Rechners an. Wenn sich der Mauszeiger über einem Anmeldesymbol befindet, wird das Agent QuickView-Fenster 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.
- **Betriebssystem** – Das Betriebssystem des Rechners
- **Zeitzonen-Verschiebung** – Zeigt die Anzahl der Minuten an. Siehe 'System > Benutzereinstellungen > **Voreinstellungen** *(http://help.kaseya.com/webhelp/DE/VSA/9000000/index.asp#503.htm)*'.

Scannen

- **Nächster vollständiger AV-Scan** – Datum und Uhrzeit des nächsten vollständigen **Antivirus**-Scans
- **Letzter vollständiger AV-Scan** – Datum und Uhrzeit des letzten vollständigen **Antivirus**-Scans. Ein vollständiger **Antivirus**-Scan führt einen gründlichen Scan des gesamten Systems durch. Dies umfasst Folgendes: Systemspeicher, beim Start geladene Programme, System-Backup, E-Mail-Datenbanken, Festplatten, Wechseldatenträger und Netzwerklaufwerke.
- **Letzter AV-Schnellscan** – Datum und Uhrzeit des letzten **Antivirus**-Schnellscans von Startobjekten des Betriebssystems. Ab **Antivirus** Version 10.x wurde der Schnellscan in kritischer Scan umbenannt.
- **AV-Scanstatus** – Der Status des Scans

Sicherheit

- **AV installiert am** – Das Datum, an dem **Antivirus** installiert wurde.
- **AV-Profil** – Das diesem Rechner zugewiesene **Antivirus**-Profil

Status

- **AV-Komponenten** – Identifiziert den Status der auf diesem Rechner installierten **Antivirus**-Komponenten.
- **Letzte AV-Statusaktualisierung** – Datum und Uhrzeit der letzten **Antivirus**-Aktualisierung
- **AV-Markierungen** – Folgende Markierungen sind möglich: `Definitions out of date`
- **Ausstehende Aktionen** – Installation, Zuweisung, Aktualisierung und Scan
- **Neustart erforderlich** – Falls `Ja`, ist ein Neustart erforderlich.

Upgrade verfügbar

- **Verfügbare AV-Client-Version** – Die Kaspersky-Versionsnummer des für diesen Rechner verfügbaren **Antivirus**-Client-Upgrades

Version

- **AV-Client-Version** – Die Kaspersky-Versionsnummer des auf diesem Rechner installierten **Antivirus**-Clients
- **AV-Datenbank-Datum** – Datum und Uhrzeit der gegenwärtig von diesem Rechner verwendeten **Antivirus**-Definitionsdatenbank
- **AV-Service-Version** – Die Version des **Antivirus**-Clients
- **Agent-Version** – Die Version des Kaseya-Agents
- **Aktualisierung** – Der Status der Aktualisierung

Windows-Sicherheitscenter

- **Aktiv** – Ist diese Option markiert, wird das Virenschutzprogramm verwendet.
- **Hersteller** – Der Hersteller des Virenschutzprogramms.
- **Auf aktuellem Stand** – Ist diese Option markiert, ist das Virenschutzprogramm auf dem neuesten Stand.
- **Version** – Die Version des Virenschutzprogramms
- **Vom WSC gemeldeter Produktname** – Der Name des beim *Windows Sicherheitscenter* registrierten Virenschutzprogramms. **Antivirus** registriert sich nicht beim *Windows Sicherheitscenter*.

> **Hinweis:** Ab Windows 7 wird das *Windows Sicherheitscenter* als *Wartungscenter* bezeichnet.

Detailfeld

Kopfzeile

- **Name** – Die Rechner-ID.Gruppen-ID.Organisations-ID des Rechners
- **BS** – Das Betriebssystem des Rechners
- **IP-Adresse** – Die dem Rechner zugewiesene IP-Adresse
- **Agent-ID** – Die GUID des Agents auf dem verwalteten Rechner

Registerkarte 'Status'

- **Installationsstatus** – Ist diese Option markiert, ist **Antivirus** Security installiert.
- **Installiert am** – Das Datum, an dem **Antivirus** installiert wurde.
- **Installationsfehler** – Tritt bei der Installation ein Fehler auf, wird der Link `Protokoll anzeigen` angezeigt, über den Sie das Kaspersky-Installationsprotokoll aufrufen können.
- **Passwort für die Deinstallation** – Das Passwort, das für die Neukonfiguration oder Deinstallation des **Antivirus**-Clients erforderlich ist.
- **Ablaufdatum der Lizenz** – Das Datum, an dem der **Antivirus**-Schutz abläuft.
- **Profil** – Das diesem Rechner zugewiesene **Antivirus**-Konfigurationsprofil.
- **Letzter vollständiger Scan** – Datum und Uhrzeit des letzten gründlichen Scans des gesamten Systems. Dies umfasst Folgendes: Systemspeicher, beim Start geladene Programme, System-Backup, E-Mail-Datenbanken, Festplatten, Wechseldatenträger und Netzwerklaufwerke.
- **Letzter Schnellscan** – Datum und Uhrzeit des letzten kritischen Scans von Startobjekten des Betriebssystems. Ab **Antivirus** Version 10.x wurde der Schnellscan in kritischer Scan umbenannt.
- **Nächster vollständiger Scan** – Datum und Uhrzeit eines geplanten **Antivirus**-Scans

- **Kaspersky Antivirus-Version** – Die Kaspersky-Versionsnummer des auf diesem Rechner installierten **Antivirus**-Clients
- **Managementversion** – Die Versionsnummer des auf dem verwalteten Rechner installierten **Antivirus**-Pakets
- **Datenbank-Datum** – Datum und Uhrzeit der gegenwärtig von diesem Rechner verwendeten **Antivirus**-Definitionsdatenbank
- **Zuletzt aktualisiert** – Datum und Uhrzeit der letzten Aktualisierung des **Antivirus**-Clients
- **Markierungen** – Folgende Markierungen sind möglich: `Virus definitions out of date`, `Configuration is out of compliance with the profile`.

  Hinweis: Selbst wenn ein Rechner wieder alle Richtlinien erfüllt, wird die Markierung 'Erfüllt Richtlinien nicht mehr' weiterhin angezeigt. Weisen Sie dem Rechner das Profil erneut zu, um diese Markierung zu entfernen.

- **Komponentenstatus** – Identifiziert den Status der auf diesem Rechner installierten **Antivirus**-Komponenten. Der Komponentenschutz wird auf der Registerkarte 'Profile > **Schutz** *(siehe 17)*' konfiguriert.

  – **Datei-Antivirus aktivieren** – Ist diese Option markiert, werden alle Dateien gescannt, die geöffnet, gespeichert oder ausgeführt werden. *Gilt für Workstations und Server.*

  – **Mail-Antivirus aktivieren** – Ist diese Option markiert, werden ein- und ausgehende Nachrichten auf gefährliche Objekte hin untersucht. Dieses Modul wird mit dem Hochfahren des Betriebssystems gestartet. Es residiert im Arbeitsspeicher des Computers und scannt alle über die Protokolle POP3, SMTP, IMAP, MAPI und NNTP eingehenden E-Mails. *Gilt nur für Workstations.*

  – **Web-Antivirus aktivieren** – Diese Komponente gewährleistet die Sicherheit bei der Internet-Nutzung. Sie schützt Ihren Computer vor Daten, die über das HTTP-Protokoll an Ihren Computer übertragen werden, und verhindert, dass gefährliche Skripte auf dem Computer ausgeführt werden. *Gilt nur für Workstations.*

  – **IM-Antivirus aktivieren** – Diese Komponente gewährleistet den sicheren Betrieb von Instant-Messenger-Clients. Sie schützt die Informationen, die über IM-Protokolle an Ihren Computer übertragen werden. Zu den von dieser Komponente geschützten IM-Anwendungen gehören ICQ, MSN, AIM, Yahoo! Messenger, Jabber, Google Talk, Mail.Ru Agent und IRC. *Gilt nur für Workstations.*

  - **Proaktiven Antivirus aktivieren** – Ist diese Option markiert, wird eine neue Bedrohung auf dem Computer anhand der von einem Programm ausgeführten Aktionssequenz erkannt. Sollte die Analyse der Aktivitätssequenz einer Anwendung etwas Verdächtiges feststellen, blockiert **Antivirus** die Aktivität dieser Anwendung. *Gilt nur für Workstations.*

  – **Anti-Spam aktivieren** – Ist diese Option markiert, wird diese Komponente mit dem auf Ihrem Computer installierten Mail-Client integriert. Sie untersucht alle eingehenden E-Mails auf Spam. Alle Spam enthaltenden E-Mails werden mit einer besonderen Kopfzeile gekennzeichnet. Diese Komponente analysiert ebenfalls den Text der E-Mails, um Phishing-Versuche zu erkennen. *Gilt nur für Workstations.*

  – **Anti-Spy aktivieren** – Ist diese Option markiert, werden die Versuche von Dialern, eine Verbindung mit kostenpflichtigen Nummern herzustellen, abgefangen und blockiert. *Gilt nur für Workstations.*

  – **Zugriffskontrolle aktivieren** – Ist diese Option markiert, wird die automatische Ausführung von Anwendungen auf an den Computer angeschlossenen Wechseldatenträgern und Geräten verhindert. Dies schließt ebenfalls die Ausführung von `autorun.inf`-Dateien ein. *Gilt nur für Workstations.*

Registerkarte 'Meldungsprofile'

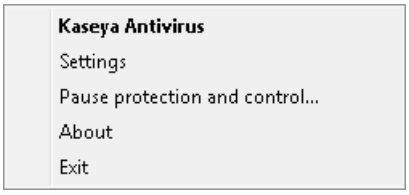
Zeigt die Liste mit den dem ausgewählten Rechner zugewiesenen **Meldungsprofilen** *(siehe 26)* an.

Hinweis: Die Registerkarte 'Meldungen > <Profil> > **Endpunkte** *(siehe 28)*' führt alle Rechner auf, die ein ausgewähltes Meldungsprofil verwenden.

Antivirus-Agent-Menü

Nachdem der **Antivirus**-Agent auf einem Rechner installiert wurde, wird er durch das Symbol im Infobereich der Taskleiste des Rechners angezeigt. Über dieses Symbol können Sie auf die Benutzeroberfläche des **Antivirus**-Agents zugreifen.

Durch das Klicken mit der rechten Maustaste auf das Agent-Symbol rufen Sie das Optionsmenü auf.



- **Kaseya Antivirus** – Zeigt die Benutzeroberfläche des **Antivirus**-Agents an.
- **Einstellungen** – Legt die allgemeinen **Antivirus**-Schutzeinstellungen fest.
- **Schutz anhalten...** – Unterbricht den Schutz des Rechners für eine angegebene Zeitspanne.
- **Über** – Zeigt das Fenster mit Informationen über den **Antivirus**-Agent an.
- **Beenden** - Beendet den **Antivirus**-Agent-Dienst auf dem verwalteten Rechner. Der Rechner wird nicht länger von **Antivirus** geschützt..

Hinweis: ***Anpassung der Benutzeroberfläche des Antivirus-Clients auf dem Endpunkt*** *(https://helpdesk.kaseya.com/entries/32410117)*

Dashboards

Antivirus > Anzeigen > Dashboards

Die Seite **Dashboards** bietet eine Dashboard-Ansicht des Status von Rechnern, auf denen **Antivirus** installiert ist. Die angezeigten Dashboard-Statistiken sind abhängig vom **Rechner-ID-/Gruppen-ID-Filter** *(http://help.kaseya.com/webhelp/DE/VSA/9000000/index.asp#209.htm)* und den Rechnergruppen, zu deren Anzeige über 'System > **Scopes** *(http://help.kaseya.com/webhelp/DE/VSA/9000000/index.asp#4578.htm)*' der Benutzer berechtigt ist.

Aktionen

- **Aktionen**
  - **Neu** – Erstellt ein neues Dashboard.
  - **Speichern** – Speichert die am gegenwärtig angezeigten Dashboard vorgenommenen Änderungen.
  - **Speichern unter** – Speichert das gegenwärtig angezeigte Dashboard unter einem neuen Namen.
  - **Löschen** – Löscht das gegenwärtig angezeigte Dashboard.
- **Dashboard auswählen** – Wählt ein Dashboard für die Anzeige aus.
- **Teile hinzufügen** – Fügt dem gegenwärtig angezeigten Dashboard Teile hinzu. Die verfügbaren Teile finden Sie in der Liste unten.

- **In neuem Fenster öffnen** – Zeigt das ausgewählte Dashboard auf einer neuen Registerkarte oder in einem neuen Fenster an.

Teile des Antivirus-Dashboards

- **Automatische Verlängerung der Antivirus-Lizenz** – Ein Balkendiagramm mit der Anzahl der Rechner, für die die Option **Automatisch verlängern** aktiviert ist und deren Lizenz in 30, 60, 90 oder 91+ Tagen abläuft.
- **Antivirus-Lizenzablauf** – Ein Balkendiagramm mit der Anzahl der Rechner, deren Lizenz bereits abgelaufen ist oder deren Lizenzen in 30, 60, 90 oder 91+ Tagen ablaufen.
- **Antivirus-Rechner, die Aufmerksamkeit benötigen** – Ein Balkendiagramm mit der Anzahl der von **Antivirus** verwalteten Rechner, die Aufmerksamkeit benötigen. Die Rechner sind in die folgenden Kategorien unterteilt: `AV nicht installiert`, `Bestehende Bedrohungen`, `Veraltet`, `Neustart erforderlich`, `Komponenten`.
- **Anzahl der Antivirus-Rechner mit Erkennungen** – Ein Balkendiagramm mit der Anzahl der Erkennungen.
- **Antivirus-Schutzstatus** – Ein Kreisdiagramm, das die Prozentwerte von Rechnern mit **Antivirus**-Schutz in die folgenden Kategorien unterteilt anzeigt: `Nicht installiert`, `Veraltet`, `Nicht aktiviert`, `Auf aktuellem Stand`.
- **Wichtigste Bedrohungen – Antivirus** – Eine Liste der Rechner mit den meisten von Antivirus erkannten Bedrohungen. Nach Klicken auf eine der über Hyperlink verknüpften Rechner-IDs werden die Bedrohungen des dazugehörigen Rechners auf der Seite **Erkennungen** *(siehe 14)* angezeigt.
- **Ungefilterte Antivirus-Lizenzübersicht** – Ein Diagramm mit der Anzahl der Rechner, die `verfügbar`, `abgelaufen` `in Verwendung`, `teilweise verfügbar/verwendet` sind bzw. bei denen die `Installation geplant` ist.

Erkennungen

Antivirus > Anzeigen > Erkennungen

Die Seite **Erkennungen** zeigt die Bedrohungen durch Viren an, die nicht automatisch von **Antivirus** beseitigt werden können. Mit den Informationen auf dieser Seite können Sie Bedrohungen näher untersuchen und manuell entfernen. Die Liste der angezeigten Rechner hängt vom **Rechner-ID-/Gruppen-ID-Filter** *(http://help.kaseya.com/webhelp/DE/VSA/9000000/index.asp#209.htm)* und den Rechnergruppen ab, zu deren Ansicht unter 'System > **Umfang** *(http://help.kaseya.com/webhelp/DE/VSA/9000000/index.asp#4578.htm)*' der Benutzer berechtigt ist.

Aktionen

- **Details** – Klicken Sie hierauf, um auf der Securelist-Website von Kaspersky mehr zu einer ausgewählten Bedrohung zu erfahren.
- **Ausschluss hinzufügen** – Fügt ausgewählte Zeilen der **Ausschlussliste** *(siehe 24)* hinzu.
- **Löschen** – Sendet eine Anforderung an den Endpunkt, die unter Quarantäne stehende Datei zu löschen.
- **Wiederherstellen** – Sendet eine Anforderung an den Endpunkt, die Quarantäne der Datei zu beenden. Die Datei gilt nicht länger als Bedrohung.
- **Ausblenden** – Die ausgewählte Bedrohung wird nicht mehr auf der Liste angezeigt. Durch Ausblenden wird die Bedrohung nicht gelöscht.
- **Filter** – Filtert die Liste anhand einer der folgenden Kriterien:
  - **Aktive Bedrohungen** – Zeigt die von **Antivirus** erkannten Bedrohungen an, die noch nicht desinfiziert worden sind.
  - **Dateien unter Quarantäne** – Zeigt die unter Quarantäne gestellten Dateien an.

- **Gelöschte Dateien** – Zeigt eine Liste der gelöschten Dateien an.
- **Bedrohungen der letzten <N Perioden>** – Filtert die Liste anhand eines oder mehrerer vordefinierter Zeiträume.
- **Filter löschen** – Zeigt den Listeninhalt ungefiltert an.

Tabellenspalten

- **Rechnername** – Die Rechner-ID
- **Name** – Der Name der Bedrohung
- **Pfad** – Der Speicherort der Bedrohung auf dem verwalteten Rechner
- **Zeit** – Datum und Uhrzeit der Erkennung der Bedrohung
- **Status** – Der Status der Bedrohung. Unter anderem sind folgende Statusmeldungen möglich:
  - `Infiziert` – Auf der Datei wurde ein Virus gefunden.
  - `Verdächtig` – Datei ist verdächtig. Dies bedeutet normalerweise, dass Malware gefunden wurde, es sich dabei jedoch nicht um einen bestätigten bekannten Virus handelt.
  - `Desinfiziert` – Kaspersky hat den Virus aus der Datei entfernt.
  - `Gelöscht` – Datei wurde – entweder automatisch oder vom Benutzer über den Quarantänebereich – gelöscht.
  - `In Quarantäne` – Unter Quarantäne gestellte Dateien. Der Benutzer kann nicht direkt auf diese Dateien zugreifen, kann sie jedoch wiederherstellen oder löschen. Für die Wiederherstellung einer unter Quarantäne gestellten Datei benötigen Sie das für den betroffenen Rechner unter 'Rechner > **Detailfeld** *(siehe 11)*' angezeigte Passwort.
  - `Erkannt` – Kaspersky hat eine Bedrohung erkannt, aber keine Maßnahmen ergriffen. D. h. die Datei wurde weder unter Quarantäne gestellt noch gelöscht, kann aber eine möglicherweise aktive Bedrohung enthalten. Der Benutzer muss die Bedrohung manuell mit den unter **Erkennungen verwalten** verfügbaren Optionen handhaben.
  - `Nicht gefunden` – Die Datei ist nicht mehr vorhanden. Möglicherweise wurde sie nach der Erkennung von einem anderen Programm als Kaspersky gelöscht. Dies kann vorkommen, wenn eine temporäre Datei wie beispielsweise ein Cookie oder eine Temp-Datei gefunden wird, die bereits durch das Löschen des Browser-Caches gelöscht wurde.
  - `Unbekannt` – Die Datei wird von Kasperskys Virendefinitionen nicht erkannt. Wenn Sie möchten, dass die Datei näher auf mögliche Gefahren hin untersucht wird, erstellen Sie ein Kaseya **Support-Ticket** *(https://helpdesk.kaseya.com/home)*.
  - `Vom Benutzer gehandhabt` – Der Benutzer hat die Datei manuell gehandhabt. In diesem Fall wurde der Benutzer in einem eingeblendeten Dialog zur Entscheidung aufgefordert, diese Bedrohung entweder zu löschen, unter Quarantäne zu stellen oder zu ignorieren.
- **Typ** – Der Typ der Bedrohung
- **Profilname** – Der Name des Profils, das zum Zeitpunkt der Bedrohungserkennung aktiv war.

Profile

Antivirus > Konfiguration > Profile

Auf der Seite **Profile** werden **Antivirus**-Profile verwaltet. Jedes Profil stellt einen unterschiedlichen Satz an aktivierten bzw. deaktivierten **Antivirus**-Optionen dar. Änderungen an einem Profil wirken sich auf alle Rechner-IDs aus, denen dieses Profil zugewiesen wurde. Ein Profil wird einer Rechner-ID über 'Antivirus > **Rechner** *(siehe 3)* > **Zuweisen**' zugewiesen. Normalerweise benötigen verschiedene Typen von Rechnern oder Netzwerken unterschiedliche Profile. Profile sind nur sichtbar, wenn das Profil von Ihnen erstellt wurde oder einem Rechner innerhalb des von Ihnen verwendeten Scopes zugewiesen ist.

Profiltypen – Server und Workstations

Antivirus-Lizenzen werden separat für Workstations und Server erworben und verwaltet. Workstations und Servern werden verschiedene Profiltypen zugewiesen. Ein Serverprofil kann nur Servern zugewiesen werden. Ein Workstation-Profil kann nur Workstations zugewiesen werden. Es werden Ihnen für jeden Profiltyp Musterprofile bereitgestellt. Workstations und Server können gleichzeitig ausgewählt und zugewiesen werden.

Aktionen

- **Neu** – Erstellt ein neues Konfigurationsprofil. Jeder Profiltyp installiert einen anderen Client-Typ auf dem Endpunkt. Folgende Profiltypen sind verfügbar:
  - `Kaspersky Workstation 10 Profile`
  - `Kaspersky Workstation 6 Profile`
  - `Kaspersky Server 10 Profile`
  - `Kaspersky Server 6 Profile`

  Hinweis: **Antivirus** 6.5 unterstützt für Workstation- und Server-Endpunkte sowohl Kaspersky Version 10 als auch die Legacy-Version 6. Für die Verwaltung jedes Rechnertyps werden spezielle Profile bereitgestellt. *Endpunkte mit Kaspersky Version 2010 werden von* **Antivirus** *6.5 nicht unterstützt.* **Antivirus** 6.5 installiert bzw. aktualisiert Endpunkte nur auf Kaspersky Version 10. *Version 10 wird dringend empfohlen.* Sie können über die Schaltfläche 'Installieren > **Client-Version aktualisieren**' in der Systemsteuerung einen Endpunkt mit Kaspersky Version 6 auf Version 10 aktualisieren.
- **Öffnen** – Öffnet ein vorhandenes Profil für die Bearbeitung. Sie können auf ein Profil auch doppelklicken, um es zu öffnen.
- **Löschen** – Löscht ein vorhandenes Profil.
- **Speichern** – Speichert die am gegenwärtig ausgewählten Profil vorgenommenen Änderungen.
- **Kopieren** – Speichert ein ausgewähltes Profil unter einem neuen Namen. Serverprofile können nur in ein neues Serverprofil kopiert werden. Workstation-Profile können nur in ein neues Workstation-Profil kopiert werden.
  - **Profil Kaspersky 2010** – Kopiert ein ausgewähltes Profil in ein Kaspersky Version 10-Profil.
- **Filter**
  - `Show Kaspersky Workstation Profiles Only`
  - `Show Kaspersky Server Profiles Only`
  - `Show Kaspersky 10.0.0.0 Profiles Only`
  - `Show Kaspersky 6.0.4.1424 Profiles Only`
- **Filter entfernen** – Entfernt den Filter.

Hinzufügen/Bearbeiten von Profilen

Klicken Sie auf **Neu** und dann auf *Profiltyp*, um das Fenster **Neues Profil** anzuzeigen. Klicken Sie alternativ auf ein vorhandenes Profil und dann auf **Öffnen**, um das Fenster **Profil bearbeiten** anzuzeigen.

- **Registerkarte 'Übersicht'** *(siehe 17)*
- **Registerkarte 'Schutz'** *(siehe 17)*
- **Registerkarte 'Schnellscan'** *(siehe 21)*
- **Registerkarte 'Vollständiger Scan'** *(siehe 22)*
- **Registerkarte 'Update-Optionen'** *(siehe 24)*
- **Registerkarte 'Ausschlüsse'** *(siehe 24)*
- **Registerkarte 'Endpunkte'** *(siehe 26)*

Tabellenspalten

- **Name** – Der Name des Profils
- **Profiltyp** – `Kaspersky Dateiserver` oder `Kaspersky Workstation`
- **Auf Rechner angewendet** – Anzahl der Rechner, die dieses Profil verwenden.
- **Erstellt von** – VSA-Benutzer, der dieses Profil erstellt hat.
- **Version**
  - `6.0.4.1424` oder `6.0.4.1611` – Version 6, Server oder Workstation
  - `10.x.x.x` – Kaspersky Endpoint Security for Business, Version 10

Registerkarte 'Übersicht'

Antivirus > Konfiguration > Profile > Übersicht

Hinweis: Die von der jeweiligen Profilversion nicht unterstützten Optionen sind deaktiviert (grau unterlegt).

- **Name** – Der Name des Profils
- **Beschreibung** – Eine Beschreibung des Profils
- **Profiltyp** – **Antivirus**-Dateiserver oder -Workstation
- **Profilversion**
  - `6.0.4.1424` oder `6.0.4.1611` – Version 6, Server oder Workstation
  - `10.x.x.x` – Kaspersky Endpoint Security for Business, Version 10

Registerkarte 'Schutz'

Antivirus > Konfiguration > Profile > Schutz

Hinweis: Die von der jeweiligen Profilversion nicht unterstützten Optionen sind deaktiviert (grau unterlegt).

Optionen

- **Schutz aktivieren** – Ist diese Option markiert, werden alle für dieses Profil ausgewählten Schutzkomponenten aktiviert.
- **Antivirus beim Starten des Rechners starten** – Ist diese Option markiert, werden alle für dieses Profil ausgewählten Schutzkomponenten mit dem Hochfahren des Rechners aktiviert.
- **Selbstschutz aktivieren** – Verhindert unbefugte Zugriffe auf **Antivirus**-Dateien sowie Schutz vor Auto-Clickern.

Interaktiver Schutz

- **Aktion automatisch auswählen** – Ist diese Option markiert, werden die von Kaspersky Lab empfohlenen Aktionen automatisch ausgeführt. Sobald das Programm eine Bedrohung erkennt, versucht es, das Objekt zu desinfizieren. Sollte die Desinfektion fehlschlagen, versucht Kaspersky, die Datei zu löschen. Verdächtige Objekte werden ohne Bearbeitung übersprungen. Meldungen werden eingeblendet, um den Benutzer über neue Ereignisse zu informieren. Wird das Kontrollkästchen nicht aktiviert, verwendet das Programm die folgenden benutzerdefinierten Schutzeinstellungen.
  - **Verdächtige Objekte nicht löschen** – Ist diese Option markiert, werden Aktionen automatisch angewendet, aber verdächtige Objekte werden nicht gelöscht.

- **"Protected by Kaspersky Lab" auf dem Microsoft Windows-Anmeldebildschirm anzeigen** – Ist diese Option markiert, wird diese Ergänzung angezeigt.
- **Symbol in der Taskleiste anzeigen** – Ist diese Option markiert, wird das Symbol des **Antivirus**-Clients im Infobereich der Taskleiste des Benutzercomputers angezeigt. Durch Klicken mit der linken oder rechten Maustaste auf dieses Symbol kann der Benutzer das **Antivirus-Agent-Menü** *(siehe 13)* aufrufen.
- **Im Startmenü anzeigen** – Ist diese Option markiert, wird der **Antivirus**-Client als Programm im Startmenü des Benutzers angezeigt.
- **In der Liste 'Programme hinzufügen/entfernen' (unter 'Programme und Funktionen') anzeigen** – Ist diese Option markiert, wird der **Antivirus**-Client als Programm in der Liste 'Programme hinzufügen/entfernen' des Benutzers angezeigt. Der Benutzer kann den **Antivirus**-Client deinstallieren.

Hinweis: Für jede der unten aufgeführten Komponenten werden auf der Seite **Rechner** im Feld **Komponentenstatus** des **Detailfeldes** *(siehe 11)* entsprechende Symbole angezeigt.

Datei Antivirus

Gilt für Workstations und Server.

- **Datei-Antivirus aktivieren** – Ist diese Option markiert, werden alle Dateien gescannt, die geöffnet, gespeichert oder ausgeführt werden.
- **Nur neue und geänderte Dateien scannen** – Ist diese Option markiert, werden nur neue und seit dem letzten Scan geänderte Dateien gescannt.
- **Netzlaufwerke schützen** – Ist diese Option markiert, werden zugeordnete Netzwerklaufwerke ebenfalls gescannt.
- **Wechseldatenträger schützen** – Ist diese Option markiert, werden Wechseldatenträger ebenfalls gescannt.
- **Archive scannen** – Ist diese Option markiert, werden archivierte Dateien gescannt.
- **Installationspakete scannen** – Ist diese Option markiert, werden Installationspakete gescannt.
- **Eingebettete OLE-Objekte scannen** – Ist diese Option markiert, werden eingebettete OLE-Objekte gescannt.
- **Heuristische Analyse** – Ist diese Option markiert, wird das Verhalten von Objekten mithilfe heuristischer Analysen als bösartig oder verdächtig identifiziert, selbst wenn diese Objekte in der Signaturdatenbank noch nicht als bekannte Bedrohung identifiziert werden. Auf diese Weise können neue Bedrohungen erkannt werden, noch bevor sie von Virenanalytikern erforscht worden sind.
- **Tiefe** – Die bei der heuristischen Analyse zu verwendende Tiefe: `oberflächlich`, `mittel`, `tief`.
- **Zusammengesetzte Dateien im Hintergrund entpacken** – Ist diese Option markiert, werden zusammengesetzte Dateien, deren Größe den unter **Minimale Dateigröße (MB)** angegebenen Wert überschreitet, im Hintergrund entpackt und gescannt, während der Benutzer bereits mit der zusammengesetzten Datei arbeiten kann. Die durch das Scannen großer zusammengesetzter Dateien verursachte Verzögerung entfällt. Zu zusammengesetzten Dateien gehören Archive, Installationsdateien und eingebettete OLE-Objekte.
- **Minimale Dateigröße (MB)** – Gibt die minimale Größe zusammengesetzter Dateien für das Scannen im Hintergrund an.
- **Große zusammengesetzte Dateien nicht entpacken** – Ist diese Option markiert, werden Dateien, deren Größe den unter **Maximale Dateigröße (MB)** angegebenen Wert überschreiten, nicht gescannt. Unabhängig von dieser Einstellung werden Dateien, die aus einem Archiv entpackt werden, immer gescannt.
- **Maximale Dateigröße (MB)** – Gibt die maximale Größe zusammengesetzter Dateien an. Dateien, die diesen Wert überschreiten, werden nicht gescannt.

- **iSwift-Technologie** – Ist diese Option markiert, werden Scans mithilfe der iSwift-Technologie beschleunigt. Bei erneutem Scan werden bereits zuvor gescannte *NTFS-Objekte* ignoriert, wenn sich weder Objekt, Scaneinstellungen noch Antivirendatenbank geändert haben.
- **iChecker-Technologie** – Ist diese Option markiert, werden Scans mithilfe der iChecker-Technologie beschleunigt. Bei erneutem Scan werden bereits zuvor gescannte *Objekte* ignoriert, wenn sich weder Datei, Scaneinstellungen noch Definitionsdatenbank geändert haben.

Mail-Antivirus

Gilt nur für Workstations.

- **Mail-Antivirus aktivieren** – Ist diese Option markiert, werden ein- und ausgehende Nachrichten auf gefährliche Objekte hin untersucht. Dieses Modul wird mit dem Hochfahren des Betriebssystems gestartet. Es residiert im Arbeitsspeicher des Computers und scannt alle über die Protokolle POP3, SMTP, IMAP, MAPI und NNTP eingehenden E-Mails.
- **Nur eingehende E-Mail-Nachrichten überprüfen** – Ist diese Option markiert, werden nur eingehende E-Mail-Nachrichten gescannt. Wird das Kontrollkästchen nicht markiert, werden sowohl ein- als auch ausgehende E-Mail-Nachrichten gescannt.
- **Datenverkehr für POP3/SMTP/NNTP/IMAP** – Ist diese Option markiert, wird der E-Mail-Datenverkehr über POP3/SMTP/NNTP/IMAP gescannt.
- **Datenverkehr für ICQ/MSN** – Ist diese Option markiert, wird der IM-Datenverkehr über ICQ und MSN gescannt.
- **Zusätzlich: Plug-in für Microsoft Office Outlook** – Ist diese Option markiert, wird ein Plug-in für den Outlook-E-Mail-Client installiert, der die Konfiguration von Mail-Anti-Virus-Optionen über die Outlook-Registerkarte '**Extras > Optionen > Mail-Anti-Virus**' ermöglicht.
- **Zusätzlich: Plug-in für The Bat!** – Ist diese Option markiert, wird ein Plug-in für den E-Mail-Client The Bat! installiert, der die Konfiguration von Mail-Anti-Virus-Optionen über '**Eigenschaften > Einstellungen > Virenschutz**' in The Bat! ermöglicht.
- **Links mit Datenbank für schädliche Webadressen untersuchen** – Ist diese Option markiert, wird überprüft, ob sich in E-Mails eingebettete Links in der Datenbank schädlicher Webadressen befinden.
- **Links mit Datenbank für Phishing-Webadressen untersuchen** – Ist diese Option markiert, wird überprüft, ob sich in E-Mails eingebettete Links in der Datenbank mit Phishing-Webadressen befinden.
- **Heuristische Analyse** – Ist diese Option markiert, wird das Verhalten von Objekten mithilfe heuristischer Analysen als bösartig oder verdächtig identifiziert, selbst wenn diese Objekte in der Signaturdatenbank noch nicht als bekannte Bedrohung identifiziert werden. Auf diese Weise können neue Bedrohungen erkannt werden, noch bevor sie von Virenanalytikern erforscht worden sind.
- **Tiefe** – Die bei der heuristischen Analyse zu verwendende Tiefe: `oberflächlich`, `mittel`, `tief`.

Web-Antivirus

Gilt nur für Workstations.

- **Web-Antivirus aktivieren** – Dieses Modul gewährleistet die Sicherheit bei der Internet-Nutzung. Sie schützt Ihren Computer vor Daten, die über das HTTP-Protokoll an Ihren Computer übertragen werden, und verhindert, dass gefährliche Skripte auf dem Computer ausgeführt werden.
- **Links mit Datenbank für schädliche Webadressen untersuchen** – Ist diese Option markiert, wird überprüft, ob sich in E-Mails eingebettete Links in der Datenbank schädlicher Webadressen befinden.
- **Links mit Datenbank für Phishing-Webadressen untersuchen** – Ist diese Option markiert, wird überprüft, ob sich in E-Mails eingebettete Links in der Datenbank mit Phishing-Webadressen befinden.
- **Zwischenspeicherzeit für Fragmente begrenzen** – Ist diese Option markiert, wird die Zeit begrenzt, die für das Scannen einzelner Fragmente eines Objekts beim Herunterladen verwendet wird. Wird bei einem Fragment das Zeitlimit überschritten, wird das Fragment ungescannt heruntergeladen. Wird dieses Kontrollkästchen nicht aktiviert, wird das Scannen von Fragmenten niemals

übersprungen. In beiden Fällen wird das gesamte Objekt gescannt, nachdem es vollständig heruntergeladen worden ist. Diese Option ist hilfreich, wenn die Zwischenspeicherung von Fragmenten die Browser-Geschwindigkeit verlangsamt und bei HTTP-Verbindungen zu Zeitüberschreitungen führt.

- **Zwischenspeicherzeit in Sekunden** – Gibt die zeitliche Begrenzung für die Zwischenspeicherung von Fragmenten an.
- **Heuristische Analyse** – Ist diese Option markiert, wird das Verhalten von Objekten mithilfe heuristischer Analysen als bösartig oder verdächtig identifiziert, selbst wenn diese Objekte in der Signaturdatenbank noch nicht als bekannte Bedrohung identifiziert werden. Auf diese Weise können neue Bedrohungen erkannt werden, noch bevor sie von Virenanalytikern erforscht worden sind.
- **Tiefe** – Die bei der heuristischen Analyse zu verwendende Tiefe: `oberflächlich`, `mittel`, `tief`.

IM-Antivirus

Gilt nur für Workstations.

- **IM-Antivirus aktivieren** – Diese Komponente gewährleistet den sicheren Betrieb von Instant-Messenger-Clients. Sie schützt die Informationen, die über IM-Protokolle an Ihren Computer übertragen werden. Zu den von dieser Komponente geschützten IM-Anwendungen gehören ICQ, MSN, AIM, Yahoo! Messenger, Jabber, Google Talk, Mail.Ru Agent und IRC.

Proaktiver Antivirus

Gilt nur für Workstations.

- **Proaktiven Antivirus aktivieren** – Ist diese Option markiert, wird eine neue Bedrohung auf dem Computer anhand der von einem Programm ausgeführten Aktionssequenz erkannt. Sollte die Analyse der Aktivitätssequenz einer Anwendung etwas Verdächtiges feststellen, blockiert **Antivirus** die Aktivität dieser Anwendung.
- **Anwendungsaktivitätsmonitor aktivieren** – Ist diese Option aktiviert, werden Anwendungsaktivitäten auf einem Computer auf verdächtige Ereignisse hin überwacht.
- **Registry-Schutz aktivieren** – Ist diese Option aktiviert, wird die Registry vor verdächtigen Änderungen an kritischen Anwendungen geschützt.

Zugriffskontrolle

Gilt nur für Workstations.

- **Zugriffskontrolle aktivieren** – Ist diese Option markiert, wird Autorun-Zugriff verhindert.
- **Autorun für alle Geräte deaktivieren** – Ist diese Option markiert, wird die automatische Ausführung von Anwendungen und Geräten auf an den Computer angeschlossenen Wechseldatenträgern verhindert.
- **Verarbeitung von autorun.inf deaktivieren** – Ist diese Option markiert, wird die automatische Ausführung von `autorun.inf` -Dateien verhindert.

Anti-Spy

Gilt nur für Workstations.

- **Anti-Spy aktivieren** – Ist diese Option markiert, werden die Versuche von Dialern, eine Verbindung mit kostenpflichtigen Nummern herzustellen, abgefangen und blockiert.
- **Anti-Banner aktivieren** – Ist diese Option markiert, wird Werbung auf besonderen Bannern im Internet oder Werbung, die in die Benutzeroberfläche gewisser auf dem Computer installierter Programme integriert ist, blockiert.
- **Anti-Dialer aktivieren** – Ist diese Option markiert, weist eine eingeblendete Meldung den Benutzer darauf hin, dass vom Computer des Benutzers aus versucht wird, eine verdeckte Verbindung zu einer Telefonnummer herzustellen. Der Benutzer erhält dann die Möglichkeit, diese Verbindung zu blockieren oder zuzulassen.

Anti-Spam

Gilt nur für Workstations.

- **Anti-Spam aktivieren** – Ist diese Option markiert, wird diese Komponente mit dem auf Ihrem Computer installierten Mail-Client integriert. Sie untersucht alle eingehenden E-Mails auf Spam. Alle Spam enthaltenden E-Mails werden mit einer besonderen Kopfzeile gekennzeichnet. Diese Komponente analysiert ebenfalls den Text der E-Mails, um Phishing-Versuche zu erkennen.
- **Datenverkehr für POP3/SMTP/NNTP/IMAP** – Ist diese Option markiert, wird der E-Mail-Datenverkehr über POP3/SMTP/NNTP/IMAP gescannt.
- **Zusätzlich: Plug-in für Microsoft Office Outlook** – Ist diese Option markiert, wird ein Plug-in für den Outlook-E-Mail-Client installiert, der die Konfiguration von Anti-Spam-Optionen über die Outlook-Registerkarte '**Extras > Optionen > Anti-Spam**' ermöglicht.
- **Zusätzlich: Plug-in für Microsoft Outlook Express** – Ist diese Option markiert, wird ein Plug-in für den Outlook Express-E-Mail-Client installiert, der die Konfiguration von Anti-Spam-Optionen ermöglicht. Wenn Sie auf die Schaltfläche **Einstellungen** neben den Schaltflächen **Spam** und **Nicht Spam** in der Taskleiste von Outlook Express klicken, wird ein besonderes Fenster geöffnet.
- **Zusätzlich: Plug-in für The Bat!** – Ist diese Option markiert, wird ein Plug-in für den E-Mail-Client The Bat! installiert, der die Konfiguration von Anti-Spam-Optionen über '**Eigenschaften > Einstellungen > Spamschutz**' in The Bat! ermöglicht.
- **Bei Empfang von E-Mail über POP3 Mail-Dispatcher öffnen** – Ist diese Option markiert, kann der Benutzer eine Vorschau der auf einem POP3-Server gespeicherten E-Mails in einem **Dispatcher**-Fenster anzeigen, bevor die E-Mails auf den lokalen Computer heruntergeladen werden. Dies reduziert das Risiko, dass Spam oder Viren mit der E-Mail heruntergeladen werden.
- **Ausgehende E-Mail** – Ist diese Option markiert, werden die Empfängeradressen der ersten 50 ausgehenden E-Mails, die der Benutzer nach Aktivierung dieser Option sendet, auf seine Weißliste gesetzt. Die Weißliste besteht aus vertrauenswürdigen E-Mail-Adressen und Ausdrücken, die eine E-Mail als nützlich klassifizieren.
- **Keine Nachrichten von Microsoft Exchange Server überprüfen** – Ist diese Option markiert, werden E-Mails, die intern über den eigenen Microsoft Exchange Server des Benutzers gesendet werden, nicht überprüft.
- **Links mit Datenbank für schädliche Webadressen untersuchen** – Ist diese Option markiert, wird überprüft, ob sich in E-Mails eingebettete Links in der Datenbank schädlicher Webadressen befinden.
- **Links mit Datenbank für Phishing-Webadressen untersuchen** – Ist diese Option markiert, wird überprüft, ob sich in E-Mails eingebettete Links in der Datenbank mit Phishing-Webadressen befinden.

Netzwerkoptionen

- **Folgende Ports von Kaspersky überwachen lassen (kommagetrennt)** – Enthält eine Liste der Netzwerkports, die von den Komponenten Mail-Antivirus, Web-Antivirus und IM-Antivirus überwacht werden.

Registerkarte 'Schnellscan/Kritischer Scan'

Antivirus > Konfiguration > Profile > Schnellscan bzw. Kritischer Scan

Hinweis: Die von der jeweiligen Profilversion nicht unterstützten Optionen sind deaktiviert (grau unterlegt).

Hinweis: Ab **Antivirus** Version 10.x wurde der Schnellscan in kritischer Scan umbenannt.

Ein **Antivirus**-**Schnell- bzw. kritischer Scan** scannt die Startobjekte des Betriebssystems.

- **Sicherheitsstufe** – Drei Sicherheitsstufen stehen zur Wahl:

- **Hoch** – Wählen Sie diese Stufe aus, wenn Sie davon ausgehen, dass für einen Computer ein hohes Infektionsrisiko besteht.
- **Empfohlen** – Diese Stufe bietet ein optimales Gleichgewicht zwischen Effizienz und Sicherheit und ist für die meisten Fälle geeignet.
- **Niedrig** – Wenn der Rechner in einer geschützten Umgebung betrieben wird, ist eine niedrige Sicherheitsstufe unter Umständen ausreichend. Eine niedrige Sicherheitsstufe kann auch dann eingestellt werden, wenn der Rechner mit ressourcenintensiven Anwendungen arbeitet.

- **Planen**
  - **Manuell** – Scans von Rechnern, die dieses Profil verwenden, werden ausschließlich manuell ausgeführt.
  - **Nach Plan/Scan-Ausführungszeit/Ausführen alle** – Scans von Rechnern, die dieses Profil verwenden, werden entsprechend der angegebenen Anzahl von Zeiträumen festgelegt. Die Zeit ist Agent-basiert.
  - **Übersprungene Aufgaben ausführen** – Wird nur angezeigt, wenn die Ausführung täglich, wöchentlich oder monatlich wiederholt werden soll. Wird dieses Kontrollkästchen markiert und der Rechner ist zum geplanten Zeitpunkt offline, wird diese Aufgabe ausgeführt, sobald der Rechner wieder online ist. Wird dieses Kontrollkästchen nicht markiert und der Rechner ist offline, wird diese Aufgabe übersprungen und erst zum nächsten geplanten Zeitpunkt ausgeführt.
  - **Geplante Scans pausieren, wenn Bildschirmschoner nicht aktiv oder Computer nicht gesperrt ist** – Ist diese Option markiert, wird der Scanvorgang unterbrochen, wenn der Computer in Gebrauch ist.
  - **Handlungsaufforderung nach Abschluss des Scans** – Ist diese Option markiert und eine Bedrohung wird während des Scans erkannt, wird der Benutzer am *Ende* des Scans gefragt, ob die unter Quarantäne gestellten Dateien desinfiziert werden sollen. Sollte die Desinfektion fehlschlagen, wird er gefragt, ob die unter Quarantäne gestellten Dateien gelöscht werden sollen.
  - **Handlungsaufforderung während des Scans** – Ist diese Option markiert und eine Bedrohung wird während des Scans erkannt, wird der Benutzer *während* des Scans gefragt, ob eine unter Quarantäne gestellte Datei desinfiziert bzw. bei einem Fehlschlagen der Desinfektion gelöscht werden soll.
  - **Keine Handlungsaufforderung** – Der Benutzer wird zu keiner Handlung aufgefordert, wenn eine Bedrohung erkannt wird.
    - ✓ **Desinfizieren** – Ist diese Option markiert, wird versucht, eine unter Quarantäne gestellte Datei zu desinfizieren.
    - ✓ **Löschen, falls Desinfektion erfolglos** – Lässt sich eine unter Quarantäne gestellte Datei nicht desinfizieren, wird sie gelöscht.
  - **Ressourcen anderen Anwendungen überlassen** – Ist diese Option markiert, werden Scanaufgaben unterbrochen, wenn das Dateisystem durch andere Anwendungen stärker belastet wird.

Registerkarte 'Vollständiger Scan'

Antivirus > Konfiguration > Profile > Vollständiger Scan

Hinweis: Die von der jeweiligen Profilversion nicht unterstützten Optionen sind deaktiviert (grau unterlegt).

Ein **vollständiger Scan** führt einen gründlichen **Antivirus**-Scan des gesamten Systems durch. Die folgenden Objekte werden standardmäßig gescannt: Systemspeicher, beim Start geladene

Programme, System-Backup, E-Mail-Datenbanken, Festplatten, Wechseldatenträger und Netzwerklaufwerke.

- **Sicherheitsstufe** – Drei Sicherheitsstufen stehen zur Wahl:
  - **Hoch** – Wählen Sie diese Stufe aus, wenn Sie davon ausgehen, dass für einen Computer ein hohes Infektionsrisiko besteht.
  - **Empfohlen** – Diese Stufe bietet ein optimales Gleichgewicht zwischen Effizienz und Sicherheit und ist für die meisten Fälle geeignet.
  - **Niedrig** – Wenn der Rechner in einer geschützten Umgebung betrieben wird, ist eine niedrige Sicherheitsstufe unter Umständen ausreichend. Eine niedrige Sicherheitsstufe kann auch dann eingestellt werden, wenn der Rechner mit ressourcenintensiven Anwendungen arbeitet.
- **Planen**
  - **Manuell** – Scans von Rechnern, die dieses Profil verwenden, werden ausschließlich manuell ausgeführt.
  - **Nach Plan/Scan-Ausführungszeit** – Scans von Rechnern, die dieses Profil verwenden, werden entsprechend der angegebenen Anzahl von Zeiträumen festgelegt. Die Zeit ist Agent-basiert.
  - **Übersprungene Aufgaben ausführen** – Wird nur angezeigt, wenn die Ausführung täglich, wöchentlich oder monatlich wiederholt werden soll. Wird dieses Kontrollkästchen markiert und der Rechner ist zum geplanten Zeitpunkt offline, wird diese Aufgabe ausgeführt, sobald der Rechner wieder online ist. Wird dieses Kontrollkästchen nicht markiert und der Rechner ist offline, wird diese Aufgabe übersprungen und erst zum nächsten geplanten Zeitpunkt ausgeführt.
  - **Geplante Scans pausieren, wenn Bildschirmschoner nicht aktiv oder Computer nicht gesperrt ist** – Ist diese Option markiert, wird der Scanvorgang unterbrochen, wenn der Computer in Gebrauch ist.
  - **Handlungsaufforderung nach Abschluss des Scans** – Ist diese Option markiert und eine Bedrohung wird während des Scans erkannt, wird der Benutzer am *Ende* des Scans gefragt, ob die unter Quarantäne gestellten Dateien desinfiziert werden sollen. Sollte die Desinfektion fehlschlagen, wird er gefragt, ob die unter Quarantäne gestellten Dateien gelöscht werden sollen.
  - **Handlungsaufforderung während des Scans** – Ist diese Option markiert und eine Bedrohung wird während des Scans erkannt, wird der Benutzer *während* des Scans gefragt, ob eine unter Quarantäne gestellte Datei desinfiziert bzw. bei einem Fehlschlagen der Desinfektion gelöscht werden soll.
  - **Keine Handlungsaufforderung** – Der Benutzer wird zu keiner Handlung aufgefordert, wenn eine Bedrohung erkannt wird.
    - ✓ **Desinfizieren** – Ist diese Option markiert, wird versucht, eine unter Quarantäne gestellte Datei zu desinfizieren.
    - ✓ **Löschen, falls Desinfektion erfolglos** – Lässt sich eine unter Quarantäne gestellte Datei nicht desinfizieren, wird sie gelöscht.
  - **Ressourcen anderen Anwendungen überlassen** – Ist diese Option markiert, werden Scanaufgaben unterbrochen, wenn das Dateisystem durch andere Anwendungen stärker belastet wird.

Registerkarte 'Update-Optionen'

Antivirus > Konfiguration > Profile > Update-Optionen

Hinweis: Die von der jeweiligen Profilversion nicht unterstützten Optionen sind deaktiviert (grau unterlegt).

Auf der Registerkarte **Update-Optionen** können Sie den Download von **Antivirus**-Updates auf Client-Rechner planen.

Planen

- **Automatisch** – Sucht in den angegebenen Zeitabständen nach Aktualisierungen. Wird eine neue Aktualisierung gefunden, wird sie auf von **Antivirus** verwaltete Rechner mit diesem Profil heruntergeladen und installiert.
- **Manuell** – Aktualisierungen von Rechnern, die dieses Profil verwenden, werden ausschließlich manuell über die Systemsteuerung auf der Seite **Rechner** *(siehe 3)* ausgeführt.
- **Nach Plan/Update-Startzeit/Ausführen alle** – Aktualisierungen des **Antivirus**-Clients und der dazugehörigen Definitionsdatenbank auf allen von **Antivirus** verwalteten Rechnern, die dieses Profil verwenden, werden entsprechend der angegebenen Anzahl von Zeiträumen festgelegt. Die Zeit ist Agent-basiert.
- **Übersprungene Aufgaben ausführen** – Wird nur angezeigt, wenn die Ausführung täglich, wöchentlich oder monatlich wiederholt werden soll. Wird dieses Kontrollkästchen markiert und der Rechner ist zum geplanten Zeitpunkt offline, wird diese Aufgabe ausgeführt, sobald der Rechner wieder online ist. Wird dieses Kontrollkästchen nicht markiert und der Rechner ist offline, wird diese Aufgabe übersprungen und erst zum nächsten geplanten Zeitpunkt ausgeführt.

Proxy-Einstellungen

Geben Sie einen Proxy-Server an, wenn dieser für das Herunterladen der **Antivirus**-Updates vom Internet auf die Client-Rechner erforderlich ist.

- **Benutzerdefinierte Proxy-Servereinstellungen verwenden** – Ist diese Option markiert, geben Sie den für das Herunterladen von Updates verwendeten Proxy-Server manuell ein. Ist dieses Kontrollkästchen nicht markiert, werden die Proxy-Einstellungen automatisch festgestellt.
  - **Adresse** – Geben Sie einen gültigen Proxy-Servernamen oder eine gültige IP-Adresse ein.
  - **Port** – Geben Sie eine Portnummer ein.
- **Authentifizierungsdaten festlegen** – Ist diese Option markiert, ist eine Proxy-Authentifizierung erforderlich.
  - **Benutzername** – Wenn die Option **Authentifizierungsdaten festlegen** markiert ist, geben Sie einen gültigen Benutzernamen ein.
  - **Verschlüsseltes Passwort** – Wenn die Option **Authentifizierungsdaten festlegen** markiert ist, geben Sie ein gültiges Passwort ein.
- **Proxyserver für lokale Adressen umgehen** – Ist diese Option markiert, verwenden lokale IP-Adressen den Proxy-Server nicht.

Registerkarte 'Ausschlüsse'

Antivirus > Konfiguration > Profile > Ausschlüsse

Hinweis: Die von der jeweiligen Profilversion nicht unterstützten Optionen sind deaktiviert (grau unterlegt).

Auf der Registerkarte **Ausschlüsse** für **Antivirus**-Profile können Sie Objekte von der Überwachung

durch **Antivirus** ausschließen.

Ausschluss-Regeln

- **Ausschluss hinzufügen** – Fügt bis zu 256 Datei- bzw. Verzeichnispfadmasken hinzu, die vom Scannen und Schutz ausgeschlossen werden.
- **Löschen** – Löscht eine ausgewählte Ausschluss-Regel.

Folgende Ausschlüsse werden unterstützt:

- Masken ohne Dateipfade
  - `*test*` – Alle Dateien mit `test` im Namen, z. B. `12astestsdsd.sds`
  - `*test.*` – alle Dateien, deren Name in `test` endet: `346dfghtest.gdh`
  - `test.*` – alle Dateien mit dem Namen `test` und einer beliebigen Dateierweiterung
- Masken mit absoluten Dateipfaden
  - `C:\dir\*.*` oder `C:\dir\*` oder `c:\dir\` – alle Dateien im Order `C:\dir`
  - `C:\dir\*.exe` – alle Dateien mit der Erweiterung `exe` im Ordner `C:\dir`
  - `C:\dir\*.ex?` – alle Dateien mit der Erweiterung `ex?` im Ordner `C:\dir`, wobei `?` ein beliebiges einzelnes Zeichen darstellt
  - `C:\dir\test` – nur die Datei `C:\dir\test`
- Dateipfadmasken
  - `dir\*.*` oder `dir\*` – alle Dateien in allen `dir` -Ordnern
  - `dir\test` – alle Dateien namens 'test' in `dir\`-Ordnern
  - `dir\*.exe` – Alle Dateien mit der Erweiterung `exe` in allen `dir`-Ordnern
  - `dir\*.ex?` – Alle Dateien mit der Erweiterung `ex?` in allen `dir`-Ordnern, wobei `?` ein beliebiges einzelnes Zeichen darstellt

Vertrauenswürdige Anwendungen

Vertrauenswürdige Anwendungen werden nicht auf verdächtige Aktivitäten, Datei- und Netzwerkaktivitäten und Versuche, auf die System-Registry zuzugreifen, überwacht.

- **Vertrauenswürdige Anwendung hinzufügen** – Geben Sie den vollständigen Pfad und Dateinamen einer ausführbaren Datei ein.
- **Löschen** – Löscht eine anhand ihres Pfads und Namens ausgewählte Datei.

Geben Sie den Speicherort der Anwendungen in der Standardschreibweise für Umgebungsvariablen an. Beispiele:

- `%SystemRoot%\system32\svchost.exe`
- `%ProgramFiles%\Messenger\msmsgs.exe`
- `%ProgramFiles%\MSN Messenger\MsnMsgr.Exe`

Vertrauenswürdige URLs

Vertrauenswürdige URLs werden von **Web-Antivirus** *(siehe 17)* nicht auf Viren überprüft.

- **Vertrauenswürdige URL hinzufügen** – Geben Sie eine URL ein.
- **Löschen** – Löscht eine ausgewählte URL.

Formatierungsrichtlinien:

- Geben Sie am Anfang aller Adressen `http://` oder `https://` ein.
- * – Repräsentiert eine beliebige Zeichenkombination. Beispiel: `http://www.kaseya.com/*`
- ? – Repräsentiert ein einzelnes beliebiges Zeichen. Beispiel: `http://Patch_123?.com`
- Ist ein * oder ? Bestandteil einer URL, müssen Sie dieses Zeichen mit einem vorangestellten umgekehrten Schrägstrich auskommentieren, wenn Sie diese URL der Liste mit vertrauenswürdigen URLs hinzufügen. Beispiel: `http://www.kaseya.com/test\?`

Registerkarte 'Endpunkte'

Antivirus > Konfiguration > Profile > Endpunkte

Die Registerkarte **Endpunkte** führt alle Rechner auf, die ein ausgewähltes **Antivirus**-Profil verwenden.

Meldungen

Antivirus > Konfiguration > Meldungen

Auf der Seite **Meldungen** werden **Antivirus**-Meldungsprofile verwaltet. Jedes Meldungsprofil definiert einen unterschiedlichen Satz an Meldungsbedingungen und der in Reaktion auf eine Meldung durchzuführenden Aktionen. Demselben Endpunkt können mehrere Meldungsprofile zugewiesen werden. Änderungen an einem Meldungsprofil wirken sich auf alle Rechner-IDs aus, denen dieses Meldungsprofil zugewiesen wurde. Ein Meldungsprofil wird einer Rechner-ID über 'Antivirus > **Rechner** *(siehe 13)* > **Meldungsprofile**' zugewiesen. Verschiedene Typen von Rechnern benötigen möglicherweise unterschiedliche Meldungsprofile. Meldungsprofile sind für alle VSA-Benutzer sichtbar.

Hinweis: Meldungsprofile, die entweder in **Antivirus** oder **AntiMalware** erstellt wurden, sind in beiden Produkten sichtbar und bearbeitbar. Wird einem Rechner ein Meldungsprofil unter Verwendung von entweder **Antivirus** oder **AntiMalware** zugewiesen, wird dieses Profil beiden Produkten auf diesem Rechner zugewiesen.

Von Antivirus-Meldungen erstellte Alarme prüfen

- Monitor > **Alarm-Übersicht** *(http://help.kaseya.com/webhelp/DE/VSA/9000000/index.asp#1959.htm)*
- Monitor > Dashboard-Liste > beliebiges **Alarm-Übersichtsfenster** *(http://help.kaseya.com/webhelp/DE/VSA/9000000/index.asp#4112.htm)* in einem Dashlet
- Agent > Agent-Protokolle > **Agent-Protokoll** *(http://help.kaseya.com/webhelp/DE/VSA/9000000/index.asp#354.htm)*
- Agent > Agent-Protokolle > **Monitor-Aktionsprotokoll** *(http://help.kaseya.com/webhelp/DE/VSA/9000000/index.asp#354.htm)* – Zeigt die Aktionen, die in Reaktion auf eine Meldung durchgeführt wurden. Dabei spielt es keine Rolle, ob ein Alarm dafür erstellt wurde oder nicht.
- **Live Connect** *(http://help.kaseya.com/webhelp/DE/VSA/9000000/index.asp#4796.htm)* > Agent-Daten > Agent-Protokolle > Alarmprotokoll
- Info Center > Berichte > Alte Berichte > Protokolle > Alarmprotokoll

Aktionen

- **Neu** – Erstellt ein neues Meldungsprofil.
- **Öffnen** – Öffnet ein vorhandenes Meldungsprofil für die Bearbeitung. Sie können auf ein Meldungsprofil auch doppelklicken, um es zu öffnen.
- **Löschen** – Löscht ein vorhandenes Meldungsprofil.
- **Speichern** – Speichert die am gegenwärtig ausgewählten Meldungsprofil vorgenommenen Änderungen.
- **Kopieren** – Speichert ein ausgewähltes Meldungsprofil unter einem neuen Namen.
- **Meldungskonfiguration** – Konfiguriert das Format für die verschiedenen Benachrichtigungstypen der Meldungen.

Hinzufügen/Bearbeiten von Profilen

Klicken Sie auf **Neu**, um das Fenster **Neues Meldungsprofil** anzuzeigen, oder klicken Sie auf ein

vorhandenes Profil und dann auf **Öffnen**, um das Fenster **Meldungsprofil bearbeiten** anzuzeigen.

- Registerkarte 'Übersicht'
- Registerkarte 'Meldungstypen'
- Registerkarte 'Aktionen'
- **Registerkarte 'Endpunkte'** *(siehe 28)*

Tabellenspalten

- **Name** – Der Name des Meldungsprofils
- **Beschreibung** – Eine Beschreibung des Meldungsprofils

Registerkarte 'Übersicht'

Antivirus > Konfiguration > Meldungen > Übersicht

- **Name** – Der Name des Meldungsprofils
- **Beschreibung** – Eine Beschreibung des Meldungsprofils

Registerkarte 'Meldungstypen'

Antivirus > Konfiguration > Meldungen > Meldungstypen

Ausgewählte Meldungen und Konfigurationsdaten

- **Schutz von Benutzer entfernt** – Ein verwaltetes Sicherheitsprodukt wurde vom Endpunkt deinstalliert.
- **Schutz deaktiviert (gesamte Engine)** – Der Schutz eines verwalteten Sicherheitsprodukts wurde deaktiviert.
- **Definition nicht aktualisiert in X Tagen / Anzahl von Tagen** – Die Definitionen eines verwalteten Sicherheitsprodukts wurden für eine angegebene Anzahl von Tagen nicht aktualisiert.
- **Definitionsaktualisierung wurde nicht abgeschlossen** – Die Aktualisierung der Definitionen eines verwalteten Sicherheitsprodukts wurde nicht abgeschlossen.
- **Aktive Bedrohung erkannt** – Eine aktive Bedrohung wurde erkannt. Eine aktive Bedrohung ist eine Erkennung, die weder behoben noch gelöscht wurde. Der Benutzer muss manuell auf der Seite **Erkennungen** *(siehe 14)* eingreifen.
- **Bedrohung erkannt und behoben** – Eine Bedrohung wurde erkannt und behoben. Kein Benutzereingriff erforderlich.
- **Scan wurde nicht abgeschlossen** – Ein Scan wurde nicht abgeschlossen.
- **Neustart erforderlich** – Es ist ein Neustart erforderlich.
- **Lizenz läuft ab in X Tagen / Anzahl von Tagen** – Die Lizenz läuft in einer angegebenen Anzahl von Tagen ab.
- **Lizenz abgelaufen und nicht verlängert** – Die Lizenz eines verwalteten Sicherheitsprodukts ist abgelaufen und wurde nicht verlängert.
- **Profil nicht konform** – Ein Endpunkt entspricht nicht seinem Profil.
- **Profilzuweisung fehlgeschlagen** – Die Zuweisung eines Profils an einen Rechner ist fehlgeschlagen.
- **Client-Installation fehlgeschlagen** – Die Installation eines verwalteten Sicherheitsprodukts ist fehlgeschlagen.
- **Client-Reparatur fehlgeschlagen** – Die Reparatur eines verwalteten Sicherheitsprodukts ist fehlgeschlagen.

- **Client-Installation fehlgeschlagen** – Die Installation eine verwalteten Sicherheitsprodukts ist fehlgeschlagen.

Registerkarte 'Aktionen'

Antivirus > Konfiguration > Meldungen > Aktionen

Die Registerkarte **Aktionen** eines Meldungsprofils legt fest, welche Aktionen ein Endpunkt mit diesem Meldungsprofil in Reaktion auf die verschiedenen **Meldungstypen** *(siehe 27)* ausführen soll.

- **Alarm erstellen** – Wenn diese Option aktiviert ist und ein Meldungstyp auftritt, wird ein Alarm erstellt.
- **Ticket erstellen** – Ist diese Option aktiviert und es tritt eine Meldungsbedingung auf, wird ein Ticket erstellt.
- **E-Mail-Empfänger (kommagetrennt)** – Wenn diese Option aktiviert ist und eine Meldungsbedingung auftritt, wird eine E-Mail an die angegebenen E-Mail-Adressen gesendet.
- **Skript ausführen** – Wenn diese Option aktiviert ist und eine Meldungsbedingung auftritt, wird ein Agent-Verfahren ausgeführt.
  - **Skriptname** – Wählt den Namen des Agent-Verfahrens aus.
- **Nachricht an Info Center senden** – Wenn diese Option aktiviert ist und eine Meldungsbedingung auftritt, wird eine E-Mail an die angegebenen E-Mail-Adressen gesendet.
  - **Zu benachrichtigende Benutzer auswählen** – Wählen Sie aus, welche Benutzer über die Info Center > **Inbox** *(http://help.kaseya.com/webhelp/DE/VSA/9000000/index.asp#9460.htm)* über **Antivirus**-Meldungen informiert werden sollen.
- **Nachricht an Benachrichtigungsleiste senden** – Wenn diese Option aktiviert ist und eine Meldungsbedingung auftritt, wird eine E-Mail an die angegebenen E-Mail-Adressen gesendet.
  - **Zu benachrichtigende Benutzer auswählen** – Wählen Sie aus, welche Benutzer über die **Benachrichtigungsleiste** *(http://help.kaseya.com/webhelp/DE/VSA/9000000/index.asp#10634.htm)* über **Antivirus**-Meldungen informiert werden sollen.

Registerkarte 'Endpunkte'

Endpoint Protection > Konfiguration > Meldungen > Endpunkte

Die Registerkarte **Endpunkte** führt alle Rechner auf, die das ausgewählte Meldungsprofil verwenden.

Hinweis: Die Registerkarte 'Meldungsprofile (Rechner > Details > **Meldungsprofile**) enthält eine Liste mit den einem ausgewählten Rechner zugewiesenen Meldungsprofilen.

Inhaltsverzeichnis