Erste Schritte: Avast Business On-Premise Console

Weitere hilfreiche Informationen und Anleitungen zur Fehlerbehebung finden Sie in unserer Online-Dokumentation:

https://businesshelp.avast.com/

Inhalt

Einführung in die Avast Business On-Premise Console

Mit der Avast Business On-Premise Console ist es leichter denn je, jedem PC, Mac und Server wichtige Schutzmaßnahmen hinzuzufügen. Dank flexibler Verwaltung gestaltet sich der Schutz von Unternehmen überaus einfach. Die On-Premise Console bietet Folgendes:

- Vollständige Kontrolle über das Verhalten von Antivirus auf Endgeräten
- Zentrale Verwaltung mehrerer Geräte vor Ort
- Komplette Übersicht über den aktuellen Zustand der gesamten Umgebung mit sofortigen Warnmeldungen
- Automatische und nahtlose Updates

Dank der nahtlosen Integration der Avast Business On-Premise Console mit Avast Business Antivirus können Sie:

- Virtualisierung zum Schutz vertraulicher Daten einsetzen
- Mehrere Plattformen schützen – PCs, Macs und Server
- Automatisch oder manuell auf die neueste Version aktualisieren
- Zusätzlichen Firewall-Schutz für Remote-Endgeräte einrichten
- Umfassenden Serverschutz bereitstellen
- E-Mail-Client absichern

Wenn Sie Avast Business Antivirus über die Avast Business On-Premise Console auf Geräten installieren, können Sie Avast Business Antivirus auf diesen Geräten per Fernzugriff steuern. Sie können die Einstellungen für jedes Gerät einzeln ändern und anwenden, ohne die einzelnen Geräte vor Ort aufzusuchen oder aus dem Außeneinsatz zurückzurufen.

Einrichten der On-Premise Console

Überprüfen der Systemanforderungen der Console

Avast Business On-Premise Console

Windows:

- 7 SP1 oder höher, 8.x, 10
- Server 2008 R2 SP1, 2012 und 2012 R2, 2016, 2019 beliebige Edition
- Small Business Server 2008, 2011 (nur 64-Bit)
- Exchange Server 2003 x86 (bis zu 18.8), 2007, 2010, 2013, 2016, 2019 (nur 64-Bit)
- SharePoint Server 2003, 2007, 2010, 2012, 2016, 2019 (nur 64-Bit)

Mac oder Linux (Docker):

- Beliebiges MacOS, das Docker ausführen kann, vorzugsweise MacOS 10.10 oder neuer
- Beliebiges Linux-Betriebssystem, das Docker ausführen kann, vorzugsweise CentOS 7
- Docker Engine 1.10.0 oder höher
- Docker Compose 1.6.0 oder höher

Avast Business Antivirus-Endgeräte

Windows:

- 7 SP1 oder höher, 8.x außer RT und Starter Edition, 10 außer Mobile und IoT Core Edition
- Server 2008 R2, 2012 R2, 2016, 2019, beliebige Edition mit aktuellem Service Pack außer Server Core
- Microsoft Exchange Server 2010 SP2, 2013, 2016, 2019
- Microsoft SharePoint Services 3.0 und SharePoint Server 2010 und höher

Mac:

- MacOS 10.10 (Yosemite) oder höher mit mindestens 500 MB freiem Festplattenspeicher

Linux:

- CentOS ab Version 7
- Debian ab Version 8
- Red Hat Enterprise Linux 7.4
- Ab Ubuntu LTS 16.04

Überprüfen der Firewall-Anforderungen der Console

Sie müssen bestimmten Ports und URL-Adressen gestatten, Ihre Firewall oder Ihren Proxy-Server zu passieren, damit die Gesamtfunktionalität gewährleistet ist und Clients und/oder Management Consoles authentifiziert/aktualisiert werden können.

Ports

TCP und UDP:

- 53 – Secure DNS-Dienste (nur bei Verwendung der Real Site-Komponente)
- 80 – Überprüfung von Sicherheitsrisiken und Aktualisierung von Funktionen
- 443 – Aushandlung von FFL Verschlüsselungsschlüssel
- 8080, 8090 – Kommunikation zwischen Konsole und Clients im lokalen Netzwerk
- 4158 – Spiegelung, für lokale Updates im lokalen Netzwerk
- 7074 – Remote-Bereitstellung im lokalen Netzwerk

URLs

- *.avast.com
- *.avcdn.net
- *.mailshell.net (nur bei Verwendung von Anti-Spam)

Einrichten der Console

1. Gehen Sie zu https://www.avast.com/installation-files
2. Klicken Sie auf der Registerkarte „Business" auf eine der folgenden Download-Optionen:

- Installationsprogramm der Console für Windows (empfohlen für Microsoft Windows Server-Betriebssysteme)
- Image der Console für Docker (empfohlen für alle anderen Serverbetriebssysteme wie MacOS X oder Linux)

Befolgen Sie bei der Installation der On-Premise Console die Anweisungen für Ihr Betriebssystem unter:

- **Windows:** Management der On-Premise Console (auf Englisch)
- **MacOS X:** Management der On-Premise Console in MacOS X (auf Englisch)
- **Linux:** Management der On-Premise Console in Linux (auf Englisch)

Aktivieren von Lizenzen in der On-Premise Console

Zusammen mit Ihrer Kaufbestätigung erhalten Sie einen Aktivierungscode. Er enthält Informationen zu der von Ihnen erworbenen Edition. Ihr Code ist die zur Aktivierung der Software verwendete Lizenz.

1. Wenn Sie die Console zum ersten Mal ausführen, werden Sie zur Eingabe Ihres Lizenzcodes aufgefordert.
2. Geben Sie den Lizenzcode ein.
3. Klicken Sie auf **Lizenzcode aktivieren**.

Aktivieren zusätzlicher Lizenzen

1. Gehen Sie zur Seite *Abonnements*.
2. Führen Sie eine der folgenden Optionen aus:
   - Wenn Sie einen Lizenzcode haben, klicken Sie auf **Aktivierungscode abrufen?**. Geben Sie den Code ein, und klicken Sie auf **Aktivieren**.
   - Klicken Sie neben dem Abonnement, das Sie erwerben möchten, auf **Kaufen**. Schließen Sie dann die Transaktion ab.

Zuweisen von Lizenzen zu Geräten

Sie können diese Aktion erst ausführen, nachdem Sie Ihrem Netzwerk ein Gerät hinzugefügt haben.

Bei diesem Verfahren ist ein Neustart des Geräts erforderlich.

1. Führen Sie auf der Seite *Geräte* eine der folgenden Aktionen aus:
    - Wenn Sie alle einer Gruppe angehörenden Geräte miteinbeziehen möchten, klicken Sie neben dem Namen der Gruppe auf die Schaltfläche **Mehr**. Klicken Sie dann auf **Gruppe bearbeiten**.
    - Wenn Sie mehrere Geräte miteinbeziehen möchten, wählen Sie die Kontrollkästchen der jeweiligen Geräte aus. Klicken Sie dann auf **Aktionen ▸ Abonnement ändern**.
    - Geht es um ein einzelnes Gerät, klicken Sie neben dem Gerät auf die Schaltfläche **Mehr** und dann auf **Abonnement ändern**.
2. Wählen Sie in den Dropdown-Menüs die gewünschte Lizenz aus.
3. Klicken Sie für die Lizenz, zu der Sie wechseln möchten, auf **Übernehmen**. Wenn Sie das Abonnement für eine ganze Gerätegruppe ändern, klicken Sie auf **Gruppe speichern**.

Hinzufügen von Geräten über die Installationsdatei oder einen teilbaren Link

Über Console

Herunterladen des Installationsprogramms

1. Wählen Sie den benötigten Typ des Installationsprogramms aus:
   - Windows .exe (für Arbeitsstationen und Server)
   - Windows .msi (für Bereitstellung mit GPO)
   - MacOS X .dmg
2. Wählen Sie die Abonnementprodukte aus.
3. Klicken Sie auf **Erweiterte Einstellungen**, um die folgenden Optionen anzuzeigen.
4. Wählen Sie die Gruppe und Richtlinie für das Gerät.
   - **Nach Wunsch können Sie die Aktivierung Ihrer Geräte und die Auswahl der zu verwendenden Abonnements nach der Installation durchführen. Aktivieren Sie dazu das Kästchen neben der entsprechenden Option.**
5. Geben Sie an, ob Sie Antivirus-Produkte anderer Hersteller automatisch entfernen möchten.
   - **Die Option zum Entfernen von Antivirus-Produkten anderer Hersteller ist standardmäßig aktiviert. Es wird empfohlen, diese Option aktiviert zu lassen, wenn Sie den Antivirus-Dienst installieren.**
6. Wählen Sie die Größe der Installationsdatei (Standard oder Vollständig).
   - **Bei Auswahl von „Standard" werden die anderen Dienste nach der Installation des Antivirus-Agenten heruntergeladen. Diese Option wird nicht empfohlen, wenn Sie Antivirus auf mehreren Geräten gleichzeitig installieren. Der Grund ist, dass von jedem einzelnen Gerät eine Verbindung mit den Avast-Servern hergestellt wird, um die anderen Dienste herunterzuladen.**

7. Achten Sie darauf, dass Sie in der Richtlinie, die Sie auf das Gerät anwenden, gegebenenfalls den richtigen Proxy-Server definiert haben.
8. Klicken Sie auf **Jetzt herunterladen**. Legen Sie den Speicherort für das Installationspaket fest, z. B. ein Speicherstick oder Netzwerk.

Sie können auch von dieser Seite einen Download-Link senden. Klicken Sie dazu unter der Schaltfläche *Jetzt herunterladen* auf **Download-Link teilen**. Dann können Sie die private Download-URL kopieren und an alle gewünschten Empfänger senden.

Senden eines Download-Links per E-Mail

Zunächst müssen Sie Ihren SMTP-Server definieren, damit Sie Download-Links von der On-Premise Console senden können.

1. Geben Sie im Feld *Senden an* die E-Mail-Adressen der Zielbenutzer ein. Trennen Sie die einzelnen Einträge jeweils durch ein Komma voneinander.
2. Ändern Sie nach Wunsch die *Betreffzeile* der zu sendenden E-Mail.
3. Wenn Sie den Text der E-Mail-Nachricht selbst schreiben möchten, aktivieren Sie *Fügen Sie eine benutzerdefinierte Meldung hinzu* . Geben Sie den Text im hierfür vorgesehenen Feld ein.
4. Wählen Sie die Abonnementprodukte aus.
5. Klicken Sie auf **Erweiterte Einstellungen**, um die folgenden Optionen anzuzeigen.
6. Wählen Sie die Gruppe und Richtlinie für das Gerät.
    - **Nach Wunsch können Sie die Aktivierung Ihrer Geräte und die Auswahl der zu verwendenden Abonnements nach der Installation durchführen. Aktivieren Sie dazu das Kästchen neben der entsprechenden Option.**
7. Geben Sie an, ob Sie Antivirus-Produkte anderer Hersteller automatisch entfernen möchten.
    - **Die Option zum Entfernen von Antivirus-Produkten anderer Hersteller ist standardmäßig aktiviert. Es wird empfohlen, diese Option aktiviert zu lassen, wenn Sie den Antivirus-Dienst installieren.**
8. Wählen Sie die Größe der Installationsdatei (Standard oder Vollständig).

- **Bei Auswahl von „Standard" werden die anderen Dienste nach der Installation des Antivirus-Agenten heruntergeladen. Diese Option wird nicht empfohlen, wenn Sie Antivirus auf mehreren Geräten gleichzeitig installieren. Der Grund ist, dass von jedem einzelnen Gerät eine Verbindung mit den Avast-Servern hergestellt wird, um die anderen Dienste herunterzuladen.**

9. Achten Sie darauf, dass Sie in der Einstellungsvorlage, die Sie auf das Gerät anwenden, gegebenenfalls den richtigen Proxy-Server definiert haben.
10. Klicken Sie auf **Senden**.

Installieren auf dem lokalen Client

Sobald Ihnen eine Installationsdatei oder ein Download-Link von der Avast Business Management Console vorliegt, müssen Sie Avast Business Antivirus auf den Endgeräten installieren.

1. Kopieren Sie die Installationsdatei an einen Speicherort, auf die das Endgerät Zugriff hat.
2. Doppelklicken Sie auf die Installationsdatei, um sie auszuführen.
3. Wenn die Frage angezeigt wird, ob die Anwendung auf Ihrem Gerät Änderungen vornehmen darf, klicken Sie auf **Ja**.
4. Warten Sie, bis Avast Business Antivirus auf dem Gerät installiert wurde.
5. Starten Sie das Gerät neu, wenn Sie hierzu aufgefordert werden.
6. Das Gerät müsste nun in der Console angezeigt werden.

Hinzufügen von Geräten über Remote-Bereitstellung

Anforderungen für die Remote-Bereitstellung

- Administrator-Anmeldedaten für den Computer oder die Windows-Domäne. Wenn Sie Domänen-Anmeldedaten verwenden, müssen Sie auch den Namen der Domäne angeben: (z. B. IHRE_DOMÄNE\Benutzername).
- Netzwerkinformationen zu den Geräten, auf denen die Bereitstellung erfolgt. Sie benötigen diese Informationen, um die Geräte in Ihrem Netzwerk zu finden.
- Vorbereitung des Computers für die Client-Installation. Deinstallieren Sie Antivirus-Software anderer Hersteller, wenn Sie Avast Business Antivirus installieren.

Konfigurieren Sie auf jedem Gerät Folgendes:

Windows Vista/7/8.x/10

WMI-Datenverkehr aktivieren

- Führen Sie den NETSH-Befehl aus: netsh advfirewall firewall set rule group="windows management instrumentation (wmi)" new enable=yes

Administrative Freigabe aktivieren

- Öffnen Sie „Regedit".
- Navigieren Sie zu: HKLM\Software\Microsoft\Windows\CurrentVersion\Policies\System
- Erstellen Sie einen neuen DWORD-Wert „LocalAccountTokenFilterPolicy" mit dem Wert „1".

Drucker- und Dateifreigabe aktivieren

- Wählen Sie „Systemsteuerung" ▸ „Netzwerk und Internet" ▸ „Netzwerk- und Freigabecenter".
- Klicken Sie auf „Erweiterte Freigabeeinstellungen ändern", und aktivieren Sie „Datei- und Druckerfreigabe".

Firewall

1. Öffnen Sie die Firewall-Einstellungen.
2. Gehen Sie zu „Einstellungen" ▸ „Profile" ▸ „Direkt mit dem Internet verbunden" ▸ „Anwendungen" ▸ „Generic Host Process" - und „Generic Host Process 2".
3. Zulassen:
    - DCOM-Serverdaten
    - Microsoft DCOM-Server
    - DCOM-Clientdaten (sollten standardmäßig zugelassen sein)
    - Microsoft DCOM-Client (sollte standardmäßig zugelassen sein)

DCOM aktivieren

1. Führen Sie „dcomcnfg" aus.
2. Gehen Sie zu „Komponentendienste" ▸ „Computer".
3. Klicken Sie mit der rechten Maustaste auf „Arbeitsplatz ▸ Eigenschaften".

4. Klicken Sie auf die Registerkarte „Standardeigenschaften".
5. Markieren Sie das Kontrollkästchen *DCOM (Distributed COM) auf diesem Computer aktivieren*.

RPC aktivieren

1. Führen Sie „services.msc" aus.
2. Gehen Sie zur Option „Remoteprozeduraufruf (RPC)" und aktivieren Sie sie.

Details zur Remote-Bereitstellung

Die Option für die Remote-Bereitstellung ist nur dann verfügbar, wenn dem Netzwerk mindestens ein Gerät mit einer anderen Installationsmethode hinzugefügt wurde. Ferner müssen Sie einen Master-Agenten festlegen. Idealerweise sollten Sie das erste Gerät, das Sie dem Netzwerk hinzufügen, als Master-Agenten benutzen. Nachstehend finden Sie eine Zusammenfassung des Prozesses für die Remote-Bereitstellung:

Geräteerkennung

Beim Geräteerkennungsprozess wird das Adressauflösungsprotokoll (ARP) verwendet, um Pings an alle IP-Adressen im Subnetz zu senden und deren MAC-Adresse abzurufen. Dieser Prozess kann bis zu 15 Minuten dauern und je nach Netzwerk auch länger dauern.

Wenn eine Rückmeldung von einer MAC-Adresse empfangen wird, wird eine umgekehrte DNS-Suche ausgeführt, um den Hostnamen für die IP-Adresse abzurufen. Wenn der Hostname erhalten wird, wird ein Gerätedatensatz erzeugt und in einer Liste gespeichert, die an den Webdienst übertragen wird, sobald die Erkennung abgeschlossen ist.

Nach der ersten Authentifizierung führt der Prozess regelmäßig eine Suche nach Hostgeräten durch und vergleicht diese mit den bereits gespeicherten Geräten. Von nun an fügt der Prozess nur neue Geräte hinzu; es werden keine Geräte gelöscht.

Authentifizierung

Bei der Remote-Bereitstellung wird eine Liste mit Administrator-Anmeldedaten – z. B. IHRE DOMÄNE\Benutzername und Kennwort – an den Prozess zur Remote-Bereitstellung übermittelt, bis die entsprechenden Anmeldedaten gefunden werden und der Zugriff auf den Zielcomputer freigegeben wird. Wenn die Anmeldedaten nicht erkannt werden, wird der Prozess beendet und eine Fehlermeldung ausgegeben.

Der Client wartet, bis Änderungen an den Geräte-/Login-Tabellen vorgenommen wurden und überprüft, ob – basierend auf der MAC-Adresse des Hostcomputers – etwas für die Bereitstellung gekennzeichnet wird.

Anforderungen

Für die automatische Remote-Bereitstellung von Antivirus auf mehreren Geräten benötigen Sie Folgendes:

- Cloud Console oder On-Premise Console 6.0 oder höher
- Antivirus 18.6 oder höher
- Mindestens ein installiertes und aktiviertes Gerät
- Einen funktionstüchtigen Master-Agenten
- Aktivierte Datei- und Druckerfreigabe für Microsoft-Netzwerke
- Microsoft Windows-Betriebssystem mit Active Directory-Unterstützung
- Gültige Anmeldedaten für Active Directory mit Administratorrechten
- Alle notwendigen Ports offen (7074)

Remote-Bereitstellung von Installationsprogrammen

Netzwerk-Scan

1. Klicken Sie auf **Bereitstellungsprozess starten**.
    - Falls kein Master-Agent verfügbar ist, klicken Sie auf **Neuen Master-Agenten hinzufügen**. Befolgen Sie dann den Prozess zur Einrichtung eines Master-Agenten.
    - Falls ein oder mehrere Master-Agenten verfügbar sind, wählen Sie den gewünschten aus.
2. Geben Sie im Abschnitt „Anmeldedaten für Active Directory" Folgendes ein:
    - Domäne
    - Benutzername
    - Kennwort
3. Klicken Sie auf **Ihr Netzwerk scannen** und warten Sie, bis die Geräteerkennung abgeschlossen ist.

Netzwerkbereitstellung

1. Gehen Sie im Abschnitt *Active Directory-Gruppen* zu einem Ordner, der ungeschützte Geräte enthält. Wählen Sie die Kontrollkästchen neben den Geräten aus, an die die Bereitstellung erfolgen soll.
2. Klicken Sie auf **Einstellungen des Installationsprogramms definieren**.
3. Wählen Sie im Abschnitt *Lizenz auswählen* eines der verfügbaren Antivirus-Abonnements aus.
4. Führen Sie im Abschnitt *In der Avast Business-Konsole für eine Gruppe bereitstellen* beliebige der folgenden Aktionen aus:
    - Wählen Sie eine Gruppe aus.
    - Wählen Sie **Active Directory-Gruppenstruktur in die ausgewählte Gruppe kopieren** aus, um die bestehende Gruppenstruktur von Active Directory zu verwenden.
    - Wählen Sie eine Richtlinie aus.
5. Geben Sie an, ob Sie andere in Antivirus-Programme anderer Hersteller automatisch entfernen möchten.
6. Klicken Sie auf **Bereitstellung der Geräte starten**.
    - **Warten Sie, bis Antivirus auf den Geräten bereitgestellt wurde. In der Zwischenzeit können Sie zu anderen Seiten gehen. Über die Taste „Remote-Bereitstellung" im Navigationsmenü können Sie zur Remote-Bereitstellung zurückkehren und den Status anzeigen.**
7. Klicken Sie auf **Remote-Bereitstellung beenden**.

Richtlinienkonfiguration und Komponenten

Bei der Verwaltung Ihrer Geräte stützen Sie sich primär auf Richtlinien. Dabei handelt es sich um Gruppen von Sicherheitsregeln, mit denen die Funktionsweise von Avast Business Antivirus auf den Endgeräten festgelegt wird. Alle Änderungen an einer Richtlinie werden auf alle Geräte und Gruppen angewendet, die ihr zugewiesen sind.

Die Avast Business Management Consoles enthalten eine Standardvorlage, in der die vorgeschlagene Konfiguration bereits eingerichtet wurde. Sie können diese Vorlage anwenden, die Standardvorlage duplizieren und das Duplikat an Ihre Anforderungen anpassen oder aber eine völlig neue Vorlage erstellen. Die Standardvorlage kann erst gelöscht werden, nachdem eine andere Richtlinie erstellt wurde.

Antivirus-Komponenten nach Produktlizenz

Komponente	Avast Business Antivirus	Avast Business Antivirus Pro	Avast Business Antivirus Pro Plus
Dateisystem-Schutz	X	X	X
Web-Schutz	X	X	X
E-Mail-Schutz	X	X	X
Verhaltensschutz	X	X	X
WLAN-Inspektor	X	X	X
Real Site	X	X	X
Firewall	X	X	X
Sandbox	X	X	X
Anti-Spam	X	X	X
Exchange		X	X
Sharepoint		X	X
SecureLine VPN			X
Daten-Schredder		X	X
Browser Cleanup			X
Rettungsmedium	X	X	X

Aktivieren und Deaktivieren von Komponenten

Fast alle der in Avast Business Antivirus verfügbaren Schutzmodule und Tools können in der Richtlinie aktiviert oder deaktiviert werden. Dies ist insbesondere nützlich, wenn

Sie lediglich ein paar der Komponenten auf einem Server installieren oder die Anzahl der Tools möglichst gering halten möchten. Einige Tools können aber nur vollständig installiert oder deinstalliert werden, darunter Sandbox und Rettungsmedium.

1. Wählen Sie in der Richtlinie, die Sie gerade konfigurieren, die Registerkarte *Aktiver Schutz* aus.
2. Wählen Sie die Registerkarte für das relevante Betriebssystem aus (Windows Workstation, Windows Server oder MacOS X).
3. Führen Sie neben den zu ändernden Komponenten einen der folgenden Schritte aus:
    - Ziehen Sie den Schieberegler in die Position **Ein**, um die Komponente zu aktivieren.
    - Ziehen Sie den Schieberegler in die Position **Aus**, um die Komponente zu deaktivieren.

Installieren und Deinstallieren von Komponenten

Die meisten Funktionen von „Aktiver Schutz" werden mit Avast Business Antivirus installiert. Diese Komponenten können aber nach Bedarf über die Richtlinie deinstalliert und erneut installiert werden. MacOS X-Schutzkomponenten können nicht installiert oder deinstalliert werden. Es ist aber möglich, sie auszuschalten.

1. Wählen Sie in der Richtlinie, die Sie gerade konfigurieren, die Registerkarte *Aktiver Schutz* aus.
2. Wählen Sie die Registerkarte für das relevante Betriebssystem aus (Windows Workstation, Windows Server oder MacOS X).
3. Führen Sie neben den zu ändernden Komponenten einen der folgenden Schritte aus:
    - Wenn die Komponente noch nicht installiert ist, klicken Sie auf **Diese Komponente installieren**. Klicken Sie dann auf **OK. Komponente installieren**.
    - Wenn die Komponente bereits installiert ist, klicken Sie neben der Komponente auf die Schaltfläche **Mehr** und dann auf **Diese Komponente deinstallieren**. Klicken Sie dann auf **OK. Komponente deinstallieren**.

Weitere Einzelheiten zum Konfigurieren der in den Richtlinien der Avast Business Management Consoles verfügbaren Komponenten finden Sie unter

Konfigurieren von Einstellungen und Richtlinien in den Avast Business Management Consoles (nur auf Englisch).

Konfigurieren von Ausnahmen

Platzhalter

Viele der Schutzmodule und andere Komponenten von Avast Business Antivirus sowie Antivirus selbst ermöglichen es Ihnen, Ausnahmen zu konfigurieren oder bestimmte Pfade zu blockieren. Platzhalter sind hilfreich, wenn Sie den genauen Dateipfad oder Dateinamen von Dateien, die Sie ein- oder ausschließen möchten, nicht kennen oder wenn Sie mehrere Dateien in einem Pfad angeben möchten. Die Verwendung von Platzhaltern ist nicht in allen Dateipfaden möglich.

Zeichen	Bedeutung
?	Ersetzt einen einzelnen Buchstaben **Zum Beispiel:** `ab?.html` entspricht den Dateien `abc.html`, `abd.html`, `abe.html` etc. Es entspricht **nicht** der Datei`abc.htm`.
*	Ersetzt null oder mehr Zeichen **Zum Beispiel:** `*mtl` entspricht den Dateien `abc.html` und `d.html`. `*txt` entspricht den Dateien `abc.txt`, `x.txt` und `xyztxt`.

Ausnahmen

Auf der Registerkarte *Ausnahmen* oder *Antivirus-Einstellungen* Ihrer Richtlinien können Sie Ausnahmen konfigurieren, die über alle Schutzmodule und Komponenten von Avast Business Antivirus verteilt werden.

Alle Änderungen an Ausnahmen in Richtlinien werden innerhalb von 5 bis 10 Minuten über Ihr Netzwerk verteilt. Console-Richtlinien setzen lokale Einstellungen außer Kraft.

1. Gehen Sie zur Registerkarte *Antivirus-Einstellungen* für das gewünschte Betriebssystem.
2. Führen Sie im Abschnitt *Ausnahmen* eine der folgenden Aktionen aus:
   - Klicken Sie auf **Dateipfade**. Geben Sie den auszuschließenden Dateipfad ein, und klicken Sie dann auf **Hinzufügen**.

- Klicken Sie auf **URL-Adressen**. Geben Sie die auszuschließende URL ein, und klicken Sie dann auf **Hinzufügen**.

3. Klicken Sie zum Abschluss auf **Änderungen übernehmen**.

Wenn Sie die gleiche Richtlinie für mehrere Betriebssystemtypen verwenden, achten Sie darauf, die Ausnahmen diesem Abschnitt auf der Registerkarte „Windows Workstation" und/oder „Windows Server" hinzuzufügen.

Konfigurieren automatischer Updates

Sie können Ihre Geräte so einrichten, dass das Programm Avast Business Antivirus sowie die Virendefinitionen automatisch aktualisiert werden.

Konfigurieren von Updates

Avast Business On-Premise Console

1. Klicken Sie auf die Richtlinie, die Sie ändern möchten.
2. Wählen Sie das Betriebssystem aus, für das Sie automatische Updates einrichten möchten.
3. Klicken Sie auf die Registerkarte *Allgemeine Einstellungen*.
4. Wählen Sie im Abschnitt **Zeitpunkt für Update** jeweils eine der folgenden Update-Optionen für *Updates der Virusdefinitionen* und *Programm-Updates* aus:
   - Automatisch, wenn ein neues Update verfügbar ist (Empfohlen)
   - Manuell
5. Klicken Sie auf **Änderungen übernehmen**.

Updates werden entweder direkt über Avast-Server oder über konfigurierte Master-Agenten/Lokale Update-Server im Netzwerk gesendet. Wenn Sie manuelle Updates ausgewählt haben, müssen Sie Updates manuell über die Seite *Geräte* vornehmen, damit auf allen Geräten im Netzwerk stets die aktuellen Schutzmodule verfügbar sind.

Erstellen und Konfigurieren von Scans

Welche Datei- und Programmtypen von Avast Business Antivirus gescannt werden, können Sie bei der Einrichtung des Scan-Tasks festlegen. Voraussetzung ist, dass Sie einen erweiterten Scantyp gewählt haben (Benutzerdefinierter Scan, Startzeit-Prüfung).

Die wesentlichen Details für die Scanziele werden daher nicht in Richtlinien konfiguriert, abgesehen von Ausnahmen.

Arten von Scans

- **Schnelle Überprüfung**: dient zum Scannen nach gängigen Bedrohungen
- **Vollständiger Systemscan**: dient zur ausführlichen Überprüfung jeder Datei auf einem Gerät
- **Benutzerdefinierter Scan**: ermöglicht es Ihnen, Dateitypen, Wirkungsgrad, Leistung und Aktionen zu wählen und anzugeben, ob komprimierte Dateien in den Scan miteinbezogen werden sollen
- **Startzeit-Prüfung (nur MS Windows)**: dient zur Überprüfung beim Starten des Geräts

Erstellen eines Scans

1. Klicken Sie auf **Gerät scannen**.
2. Wählen Sie einen Typ aus:
    - **Schnelle Überprüfung**: dient zum Scannen nach gängigen Bedrohungen
    - **Vollständiger Systemscan**: dient zur ausführlichen Überprüfung jeder Datei auf einem Gerät
    - **Wechseldatenträger-Überprüfung**: dient zur Überprüfung der mit dem Gerät verbundenen USBs und tragbaren Medien
    - **Benutzerdefinierter Scan**: ermöglicht es Ihnen, Dateitypen, Wirkungsgrad, Leistung und Aktionen zu wählen und anzugeben, ob komprimierte Dateien in den Scan miteinbezogen werden sollen
    - **Startzeit-Prüfung (nur MS Windows)**: dient zur Überprüfung beim Starten des Geräts

    o **Falls Sie sich für „Benutzerdefinierter Scan" oder „Startzeit-Prüfung", wählen Sie zusätzliche Konfigurationsoptionen für den Scan aus.**
3. Wenn der Task wiederholt ausgeführt werden soll, wählen Sie *Scan planen*. Geben Sie die Häufigkeit an (einmalig, täglich, wöchentlich oder monatlich), und legen Sie Anfangsdatum und Uhrzeit fest.
4. Geben Sie für den Scan einen benutzerdefinierten Namen ein.
5. Klicken Sie auf **Prüfung starten**.

Alle Bedrohungen, die bei diese, Scan erkannt werden, werden in der Regel an den Virus-Container des Geräts gesendet. Sie können sie in „Gerätedetails" anzeigen und verwalten.

Scan-Konfiguration

Konfigurieren von Startzeit-Prüfungen

Startzeit-Prüfungen sind nur für Microsoft Windows-Geräte verfügbar. Ihr Gerät wird zu Beginn des Start- oder „Boot"-Vorgangs geprüft.

Zu scannende Windows-Speicherorte: Sie können im Dropdown-Menü voreingestellte Speicherorte auswählen, die dann der Liste hinzugefügt werden. Nach Wunsch können Sie auch den Pfad zu einem bestimmten Speicherort eingeben, in den Scan miteinbezogen werden soll. Alle Speicherorte, die nicht miteinbezogen werden sollen, können durch einen Klick auf die Löschen-Taste aus der Liste entfernt werden.

Gerät jetzt neu starten: Hierdurch starten Sie das Gerät sofort neu, um eine Startzeit-Prüfung durchzuführen. Wenn Sie diese Option nicht aktivieren, wird die Startzeit-Prüfung beim nächsten Neustart des Geräts ausgeführt.

Benutzer vor dem Neustart mit einer Meldung benachrichtigen: Geben Sie eine Nachricht ein, mit der der Endbenutzer auf den in Kürze anstehenden Geräteneustart aufmerksam gemacht wird.

Legen Sie fest, wann die oben angeführte Meldung angezeigt wird: Geben Sie den Zeitpunkt der Meldungsanzeige an, d. h. 1 Minute, 10 Minuten, 30 Minuten oder 1 Stunde vor dem Neustart.

Heuristik: Die Heuristik-Funktion ermöglicht es Antivirus, unbekannte Malware durch Analysieren des Programmcodes auf Befehle, die möglicherweise böswillige Absichten signalisieren, zu erkennen. Die Standardeinstellung ist „Normal". Je höher der Wirkungsgrad, desto wahrscheinlicher ist es, dass Malware von Antivirus erkannt wird. Aber auch die Anzahl der False-Positives nimmt gegebenenfalls zu, d. h. mehr Dateien werden fälschlicherweise als Malware identifiziert.

Potentiell unerwünschte Programme und verdächtige Dateien: Geben Sie an, ob nach PUPs (Potenziell unerwünschten Programmen) gescannt werden soll.

Archivdateien entpacken: Geben Sie an, ob Archivdateien beim Scan entpackt werden sollen. Der Vorgang ist dann langsamer, aber gründlicher.

Wenn keine Bedrohung gefunden wird: Geben Sie an, welche Aktion von Avast ausgeführt werden soll, wenn eine Bedrohung erkannt wird. Zur Auswahl stehen

„Automatisch bereinigen"; „In den Container verschieben, „Reparieren", „Löschen" oder „Keine Aktion".

Scan auf der Arbeitsstation abbrechen: Geben Sie an, ob der Scan auf der Arbeitsstation während der Ausführung abgebrochen werden kann.

Konfigurieren benutzerdefinierter Scans

Benutzerdefinierte Scans bieten die größtmögliche Kontrolle darüber, welche Arten von Dateien, Ordnern, Programmen und Prozessen in die Avast Business Antivirus-Scans miteinbezogen werden.

Konfigurieren von Speicherorten

Sie können im Dropdown-Menü voreingestellte Speicherorte auswählen, die dann der Liste hinzugefügt werden. Nach Wunsch können Sie auch den Pfad zu einem bestimmten Speicherort eingeben, in den Scan miteinbezogen werden soll. Alle Speicherorte, die nicht miteinbezogen werden sollen, können durch einen Klick auf die Löschen-Taste aus der Liste entfernt werden.

Registerkarte „Dateitypen"

Sie können entscheiden, ob Sie alle Dateien scannen möchten (oder nur die für Bedrohungen besonders anfälligen Bereiche). Außerdem können Sie den Scan so konfigurieren, dass Dateitypen an ihrem Inhalt erkannt werden (hierzu muss die gesamte Datei gescannt werden) oder an ihrer Namenserweiterung (hierbei werden nur die Dateien mit den Erweiterungen gescannt, die Sie in das bei der Auswahl der Option angezeigte Textfeld eingeben). Ferner können Sie entscheiden, ob Packer-Dateien (.zip etc.) extrahiert und gescannt werden sollen.

Registerkarte „Wirkungsgrad"

Wirkungsgrad: Die Heuristik-Funktion ermöglicht es Antivirus, unbekannte Malware durch Analysieren des Programmcodes auf Befehle, die möglicherweise böswillige Absichten signalisieren, zu erkennen. Die Standardeinstellung ist „Normal". Je höher der Wirkungsgrad, desto wahrscheinlicher ist es, dass Malware von Antivirus erkannt wird. Aber auch die Anzahl der False-Positives nimmt gegebenenfalls zu, d. h. mehr Dateien werden fälschlicherweise als Malware identifiziert. Durch Code-Emulation werden mutmaßliche Malware-Dateien entpackt und in einer emulierten Umgebung getestet, in

der sie keinen Schaden an Geräten anrichten können. *Code-Emulation verwenden* ist standardmäßig aktiviert.

Wirkungsgrad: Sie können entscheiden, Dateien vollständig zu testen. Hierdurch ist der Scan zwar langsamer, aber auch gründlicher.

Potentiell unerwünschte Programme und verdächtige Dateien: Geben Sie an, ob nach PUPs (Potenziell unerwünschten Programmen) gescannt werden soll.

Links: Geben Sie an, ob Links in Dateien beim Scan verfolgt werden sollen. Hierdurch ist der Scan zwar langsamer, aber auch gründlicher.

Registerkarte „Leistung"

Priorität: Geben Sie die Priorität des Scans auf den Endgeräten an. Eine höhere Priorität führt zu einer schnelleren Überprüfung, aber es werden dabei auch mehr Ressourcen verbraucht.

Persistenter Cache: Geben Sie an, ob der Scanvorgang mithilfe des persistenten Caches beschleunigt werden soll und/oder ob Daten über gescannte Dateien im persistenten Cache gespeichert werden sollen, wodurch der Scanvorgang verlangsamt wird.

Dateizugriff: Geben Sie an, ob der Scan-Vorgang durch Auslesen der Dateien in der Reihenfolge, in der sie auf dem Laufwerk gespeichert sind, beschleunigt werden soll. Dies ist nur auf NFTS-Volumen wirkungsvoll.

Registerkarte „Aktionen"

Eine Aktion anwenden: Geben Sie an, ob Aktionen während des Scans automatisch ausgeführt werden sollen, wenn ein Virus, ein potenziell unerwünschtes Programm (PUP) oder eine verdächtige Datei gefunden wurde. Zur Auswahl stehen „Automatisch bereinigen", „In den Container verschieben, „Reparieren", „Löschen" und „Keine Aktion".

Wenn die Hauptaktionen von Avast aus irgendeinem Grund nicht ausgeführt werden kann, wird von Avast versucht, die unter *Folgende Aktion durchführen, wenn die oben ausgewählte Aktion fehlschlägt* angegebene Aktion auszuführen.

Optionen: Geben Sie an, ob die ausgewählte Aktion beim Neustart ausgeführt werden soll.

Verarbeitung von infizierten Archiven: Geben Sie an, ob nur die komprimierte Datei aus dem Archiv gelöscht werden soll (und im Fehlerfall nichts) oder ob die komprimierte Datei aus dem Archiv gelöscht werden soll (und im Fehlerfall das ganze Archiv) oder ob das ganze Archiv entfernt werden soll.

Konfigurieren benutzerdefinierter Scans

Benutzerdefinierte Scans bieten die größtmögliche Kontrolle darüber, welche Arten von Dateien, Ordnern, Programmen und Prozessen in die Avast Business Antivirus-Scans miteinbezogen werden. Sie können für innerhalb des gleichen Scan-Tasks unterschiedliche Scan-Optionen für Windows Workstations, Windows Server und MacOS X Geräte auswählen.

Konfigurieren von Speicherorten

Sie können im Dropdown-Menü voreingestellte Speicherorte auswählen, die dann der Liste hinzugefügt werden. Nach Wunsch können Sie auch den Pfad zu einem bestimmten Speicherort eingeben, in den Scan miteinbezogen werden soll. Alle Speicherorte, die nicht miteinbezogen werden sollen, können durch einen Klick auf die Löschen-Taste aus der Liste entfernt werden.

Registerkarte „Dateitypen"

Sie können entscheiden, ob Sie alle Dateien scannen möchten (oder nur die für Bedrohungen besonders anfälligen Bereiche). Außerdem können Sie den Scan so konfigurieren, dass Dateitypen an ihrem Inhalt erkannt werden (hierzu muss die gesamte Datei gescannt werden) oder an ihrer Namenserweiterung (hierbei werden nur die Dateien mit den Erweiterungen gescannt, die Sie in das bei der Auswahl der Option angezeigte Textfeld eingeben).

Registerkarte „Wirkungsgrad"

Wirkungsgrad: Die Heuristik-Funktion ermöglicht es Antivirus, unbekannte Malware durch Analysieren des Programmcodes auf Befehle, die möglicherweise böswillige Absichten signalisieren, zu erkennen. Die Standardeinstellung ist „Normal". Je höher der Wirkungsgrad, desto wahrscheinlicher ist es, dass Malware von Antivirus erkannt wird. Aber auch die Anzahl der False-Positives nimmt gegebenenfalls zu, d. h. mehr Dateien werden fälschlicherweise als Malware identifiziert. Durch Code-Emulation werden mutmaßliche Malware-Dateien entpackt und in einer emulierten Umgebung getestet, in

der sie keinen Schaden an Geräten anrichten können. *Code-Emulation verwenden* ist standardmäßig aktiviert.

Wirkungsgrad: Sie können entscheiden, Dateien vollständig zu testen. Hierdurch ist der Scan zwar langsamer, aber auch gründlicher.

Potentiell unerwünschte Programme und verdächtige Dateien: Geben Sie an, ob nach PUPs (Potenziell unerwünschten Programmen) gescannt werden soll.

Links: Geben Sie an, ob Links in Dateien beim Scan verfolgt werden sollen. Hierdurch ist der Scan zwar langsamer, aber auch gründlicher.

Registerkarte „Leistung"

Priorität: Geben Sie die Priorität des Scans auf den Endgeräten an. Eine höhere Priorität führt zu einer schnelleren Überprüfung, aber es werden dabei auch mehr Ressourcen verbraucht.

Persistenter Cache: Geben Sie an, ob der Scanvorgang mithilfe des persistenten Caches beschleunigt werden soll und/oder ob Daten über gescannte Dateien im persistenten Cache gespeichert werden sollen, wodurch der Scanvorgang verlangsamt wird.

Dateizugriff: Geben Sie an, ob der Scan-Vorgang durch Auslesen der Dateien in der Reihenfolge, in der sie auf dem Laufwerk gespeichert sind, beschleunigt werden soll. Dies ist nur auf NFTS-Volumen wirkungsvoll.

Registerkarte „Aktionen"

Eine Aktion anwenden: Geben Sie an, ob Aktionen während des Scans automatisch ausgeführt werden sollen, wenn ein Virus, ein potenziell unerwünschtes Programm (PUP) oder eine verdächtige Datei gefunden wurde. Zur Auswahl stehen „Automatisch bereinigen", „In den Container verschieben, „Reparieren", „Löschen" und „Keine Aktion".

Wenn die Hauptaktionen von Avast aus irgendeinem Grund nicht ausgeführt werden kann, wird von Avast versucht, die unter *Folgende Aktion durchführen, wenn die oben ausgewählte Aktion fehlschlägt* angegebene Aktion auszuführen.

Optionen: Geben Sie an, ob die ausgewählte Aktion beim Neustart ausgeführt werden soll.

Verarbeitung von infizierten Archiven: Geben Sie an, ob nur die komprimierte Datei aus dem Archiv gelöscht werden soll (und im Fehlerfall nichts) oder ob die komprimierte Datei aus dem Archiv gelöscht werden soll (und im Fehlerfall das ganze Archiv) oder ob das ganze Archiv entfernt werden soll.

Registerkarte „Archive (Packer)"

Geben Sie an, ob alle Archivdateien für den Scan extrahiert werden sollen.

In den Avast Business Management Consoles sind viele weitere Funktionen und Optionen verfügbar. Weitere Informationen finden Sie in unserer Knowledge Base unter https://businesshelp.avast.com/.