Erste Schritte: Business Hub

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

https://businesshelp.avast.com/

Inhalt

Einführung in den Business Hub

Mit dem Business Hub können Sie mehrere Standorte oder Kunden von einer einzigen Konsole aus verwalten. Diese Cloud-basierte Plattform trägt dazu bei, den mit der Wartung, Konfiguration und Optimierung der Endgerätesicherheit verbundenen Arbeitsaufwand zu reduzieren. Der Hub ist ideal für:

- mittelgroße bis große Unternehmen mit mehreren Niederlassungen oder Standorten
- IT-Dienstleister, die mehrere Kunden betreuen
- Bestehende Benutzer der Avast Business Cloud Console, die die Funktion zum Wechseln zwischen Konten nutzen. Weitere Informationen hierzu finden Sie unter Verwalten von Unternehmen (auf Englisch).

Dank der nahtlosen Integration des Business Hubs 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 den Business Hub 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 des Hubs

Überprüfen der Systemanforderungen der Console

Business Hub

Browser (aktuelle Versionen werden empfohlen):

- Google Chrome
- Firefox
- Safari
- Microsoft Edge
- Internet Explorer

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 Avast Business Antivirus-Clients und/oder der Hub 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 (nur für On-Premise Console)
- 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

Registrierung

Selbst als Bestandskunde müssen Sie für den Hub ein neues Konto erstellen und dabei eine eindeutige E-Mail-Adresse verwenden.

Bestehende Partner:

1. Gehen Sie zum Avast Partner-Portal
2. Gehen Sie zum Abschnitt „Avast Business Management Console“, und klicken Sie auf **Register** (Registrieren).
3. Befolgen Sie die Anleitungen zum Erstellen eines Hubs.

Bestands- oder Neukunden:

1. Gehen Sie zu https://new-business.avast.com/
2. Klicken Sie auf **Konto erstellen**.
3. Geben Sie die E-Mail-Adresse des Administrators und das gewünschte Passwort ein.
4. Geben Sie Details zum Unternehmen ein. Wählen Sie „Kleines oder mittleres Unternehmen", „Großes Unternehmen", „Managed Service Provider (MSP)" oder „Anbieter von Sicherheitslösungen (Reseller/VAR/Händler)" aus.
   - **Wenn Sie „MSP" oder „Anbieter von Sicherheitslösungen" auswählen und ein registrierter Avast-Partner sind, werden Sie gebeten, das Partner-Portal zu verwenden.**
5. Wählen Sie **Konsole für mehrere Unternehmen** aus. Klicken Sie dann auf **Fertig stellen und Konsole erstellen**.

Konfiguration der Console

1. Klicken Sie im links angezeigten Dropdown-Menü auf **Standort erstellen** oder **+ Standort**.
   - **Der normale Hub ermöglicht es Benutzern, Standorte zu erstellen. Wenn sich aber ein Partner über das Partner-Portal für den Hub registriert, wird in seiner Console anstelle von „Standorte" die Option „Kunden" angezeigt. Diese beiden Begriffe werden in der Dokumentation mehr oder weniger synonym verwendet.**
2. Machen Sie unter *Standortname* und *Region* entsprechende Angaben.
3. Geben Sie an, ob Sie am Standort einen Testzeitraum für Avast Business Antivirus und Patch Management starten möchten.
4. Klicken Sie auf **Standort erstellen**.

Der Dashboard auf der obersten Ebene wird mit den erstellten Standorten gefüllt.

Benutzer

Sie können einen globalen Administrator (mit Zugriff auf alle Kunden) oder einen Standortbenutzer (mit Zugriff auf einzelne Standorte) hinzufügen.

1. Klicken Sie auf die Registerkarte *Benutzer*.
2. Klicken Sie oben rechts auf **+ Benutzer**.
3. Geben Sie die E-Mail-Adresse des Benutzers ein.

4. Wählen Sie entweder **Globaler Administrator** oder **Standortbenutzer**.
    - **Standortbenutzern können unterschiedliche Zugriffsstufen für die verschiedenen Standorte zugewiesen werden. Über die Funktion zum Wechseln zwischen Konten in der Console können sie auf mehrere Standorte zugreifen.**

Wenn Sie mehrere Standorte haben, können Sie über das links angezeigte Dropdown-Menü zwischen diesen Standorten wechseln.

Aktivieren von Lizenzen im Hub

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. Achten Sie darauf, dass im links angezeigten Dropdown-Menü kein Standort ausgewählt ist. Klicken Sie auf **Dashboard**.
2. Klicken Sie unterhalb des Standorts, den Sie aktivieren möchten, auf **Abonnement aktivieren**.
3. Klicken Sie auf **Aktivierungscode eingeben**.
4. Geben Sie den Aktivierungscode ein und bestätigen Sie, dass er korrekt ist.

Zuweisen von Lizenzen zu Geräten

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

Derzeit gibt es noch keine Geräte-Seite speziell für Partner, die eine Übersicht über alle Kunden oder Standorte bietet. Sie können aber im Dropdown-Menü einen Kunden bzw. Standort auswählen und die zugehörigen Geräte anzeigen. Folgendes wird angezeigt: Gerätenamen, Status und Warnmeldungen, Betriebssystem, zugewiesene Gruppe, zugewiesene Richtlinie, Antivirus-Version, Patch Management-Abonnement, Premium Remote Control-Abonnement sowie der Zeitpunkt der letzten Verbindung des Geräts mit der Cloud Console.

Sie können das einem Gerät zugewiesene Abonnement ändern, z. B. wenn Sie Arbeitsplätze für eine andere Antivirus-Version oder ein Abonnement für Patch Management kaufen.

1. Wählen Sie im Hub im links angezeigten Navigationsbereich den Standort aus, den Sie verwalten möchten.

2. Klicken Sie auf die Registerkarte *Geräte*.
3. Führen Sie eine der folgenden Optionen aus:
    - Aktivieren Sie die Kontrollkästchen neben mehreren Geräten, und klicken Sie oben rechts auf **Mehr**.
    - Klicken Sie auf die drei Punkte in der Geräteliste.
4. Wählen Sie **Ändern** ▸ **Dienstabonnement ändern**.
5. Wählen Sie über die Dropdown-Menüs die Abonnements aus, die Sie für Antivirus und Patch Management verwenden möchten.
6. Klicken Sie auf **Übernehmen**.

Bei diesem Verfahren ist ein Neustart der betroffenen Geräte erforderlich.

Hinzufügen von Geräten über die Installationsdatei oder einen teilbaren Link

Sie können einem Standort direkt vom Dashboard aus Geräte hinzufügen, ohne den Standort selbst aufzurufen. Beim Erstellen von Installationsprogrammen werden die zuvor ausgewählten Einstellungen beibehalten, damit Sie sie nicht erneut auswählen müssen.

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 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.**
3. Wählen Sie die Abonnements für Avast Business Antivirus und Patch Management aus und geben Sie an, ob Remote Control aktiviert werden soll.
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.
6. Achten Sie darauf, dass Sie in der Richtlinie, die Sie auf das Gerät anwenden, gegebenenfalls den richtigen Proxy-Server definiert haben.
7. Klicken Sie auf **Installationsprogramm 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.

Installieren auf dem lokalen Client

Sobald Ihnen eine Installationsdatei oder ein Download-Link vom Business Hub 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.

Globale Richtlinien

Seit 16.12.2020 können Kunden, die den Beta Hub benutzen, Richtlinien erstellen und über ihr gesamtes Netzwerk sowie für bestimmte Standorte oder Kunden verwalten.

Hauptvorteile

- Konfigurieren von Richtlinien auf einer einzigen Seite
- Anwenden von Richtlinien auf alle Geräte, unabhängig vom Betriebssystem
- Erstellen und Verwalten von Ausnahmen an einem Ort
- Erstellen standort- oder kundenspezifischer Ausnahmen beim Öffnen einer globalen Richtlinie auf der Registerkarte „Richtlinien" des Standorts
- Nutzen vordefinierter Einstellungen für Workstations und Server

Begleiterscheinungen

- Bestehende Richtlinien werden wie folgt geändert, um diese Neuerung zu ermöglichen:
- Richtlinien mit Einstellungen für mehrere Betriebssysteme werden in mehrere Betriebssystem-spezifische Richtlinien aufgeteilt
    - **Beispiel: Falls Sie eine Richtlinie mit unterschiedlichen Einstellungen für Windows Workstations, Windows Server und MacOS X haben, sehen Sie künftig drei verschiedene Richtlinien. Am Ende dieser Richtlinien wird jeweils zu Ihrer Information das jeweilige Betriebssystem aufgeführt.**
- Richtliniennamen bleiben gleich.
- Allen Geräten werden automatisch Richtlinien zugewiesen, die auf ihrem Betriebssystem basieren.
    - **Beispiel: Windows Workstations, für die eine Richtlinie verwendet wurde, die Einstellungen für Workstations, Server und MacOS X umfasste, werden der Richtlinie für Workstations zugewiesen.**

Erstellen einer neuen globalen Richtlinie

1. Öffnen Sie den Hub.

2. Klicken Sie auf die Registerkarte **Richtlinien**.
3. Klicken Sie auf **+ Richtlinie**.
4. Geben Sie einen Namen für die Richtlinie ein.
5. Nach Wunsch können Sie auch eine Beschreibung für die Richtlinie eingeben.
6. Entscheiden Sie, ob die neue Richtlinie anhand einer vordefinierten Avast-Richtlinie oder anhand einer bestehenden Richtlinie erstellt werden soll. Wählen Sie im Dropdown-Menü die gewünschte Richtlinie aus.
7. Klicken Sie auf **Erstellen**.

Konfigurieren der Richtlinie

Nachdem Sie eine Richtlinie erstellt haben, können Sie die Einstellungen bearbeiten. Klicken Sie dazu in der Tabelle auf den Namen der Richtlinie. Ein Bereich mit fünf Registerkarten und ein paar Schaltflächen wird oben geöffnet. Mit diesen Schaltflächen können Sie die ursprünglichen Einstellungen der Richtlinie wiederherstellen oder die Richtlinie duplizieren. Wenn Sie Ihre Richtlinie löschen möchten, klicken Sie auf die **drei Punkte** und wählen **Richtlinie löschen**.

Übersicht

Diese Registerkarte enthält ein paar Details zur Richtlinie. Sie können die Beschreibung bearbeiten, indem Sie auf das Stiftsymbol klicken. Ferner können Sie sehen, wann die Richtlinie erstellt und zuletzt aktualisiert wurde.

Allgemeine Einstellungen

Allgemeine Einstellungen: Mit den Schaltern können Sie Passwortschutz, Stiller Modus, Bewertungsdienste, Debug-Protokollierung, Avast Symbol in der Taskleiste und Scans von externen Laufwerken aktivieren oder deaktivieren. Ferner können Sie angeben, welche Version von Avast Business Antivirus die zugewiesenen Geräte verwenden sollen. Dazu geben Sie unter „Versionswechsel" entweder eine Versionsnummer, „neueste Version" oder „stabile Version" ein.

Updates: Wählen Sie für Virendefinitionen und Programme entweder automatische oder manuelle Updates. Weitere Informationen hierzu finden Sie unter Konfigurieren von Updates für Virendefinitionen und Antivirus (auf Englisch). Falls nötig, können Sie Proxy-Einstellungen konfigurieren, die bei Updates verwendet werden. Weitere Informationen hierzu finden Sie unter Konfigurieren von Proxy-Einstellungen für Geräte (auf Englisch).

Fehlerbehandlung: Mit den Schaltern können Sie Anti-Rootkit-Überwachung, Avast Selbstschutz-Modul, beschränkten Programm-Zugriff für Gastkonten und Hardware-unterstützte Virtualisierung aktivieren oder deaktivieren. Sie können auch die Details für Ihre E-Mail-Ports eingeben.

Neustartoptionen: Geben Sie an, wann Endgeräte neu gestartet werden sollen. Neustarts können entweder nur wenn für den Antivirus- oder Patch Management-Dienst erforderlich, automatisch, bei Abmelden des Benutzers oder gar nicht erfolgen. Weitere Informationen zu diesen Optionen finden Sie unter Konfigurieren von Neustarts und Cache-Löschung (auf Englisch).

Diensteinstellungen

Antivirus

Allgemeine Einstellungen: Aktivieren oder deaktivieren Sie „CyberCapture" und „Gehärteter Modus".

Virenscans: Legen Sie die Häufigkeit und den Zeitplan für schnelle Überprüfungen und vollständige System-Virenscans fest. Weitere Informationen finden Sie unterScan-Tasks für Geräte (auf Englisch).

Antivirenschutz: Aktivieren, deaktivieren und konfigurieren Sie Einstellungen für die wichtigsten Schutzkomponenten.

Datenschutz: Aktivieren, deaktivieren und konfigurieren Sie Einstellungen für diese Komponentenkategorie.

Identitätsschutz: Aktivieren, deaktivieren und konfigurieren Sie Einstellungen für diese Komponentenkategorie.

Weitere Informationen zu diesen Komponenten finden Sie unter Übersicht über die Komponenten. Sie können auf die Einstellungen für konfigurierbare Komponenten zugreifen, indem Sie auf den Dropdown-Pfeil neben ihrem Namen klicken.

Patch Management

Patch-Scans und -Bereitstellungen: Legen Sie die Häufigkeit von Scans für fehlende Patches fest. Geben Sie an, ob fehlende Patches sofort, nach einem bestimmten Zeitplan oder manuell bereitgestellt werden sollen.

Andere Einstellungen: Geben Sie an, ob die lokalen Patch-Dateien auf dem Endgerät gelöscht werden sollen.

Weitere Informationen zu den Einstellungen für Patch Management finden Sie unter Patch Management.

Firewall

Firewall-Einstellungen ▸ Netzwerke: Wählen Sie die Firewall-Profile für nicht definierte Netzwerkverbindungen aus, und definieren Sie Netzwerke.

Firewall-Regeln: Legen Sie die verschiedenen Systemregeln, Anwendungsregeln sowie Erweiterte Paketregeln fest.

Weitere Informationen finden Sie in den Artikeln im Bereich *Firewall* von Konfigurieren von Einstellungen und Richtlinien (auf Englisch).

Ausnahmen

Antivirus-Ausnahmen: Geben Sie Ausnahmenpfade an, die entweder von „Allen Scans und Schutzmodulen" oder bestimmten Schutzmodulen ausgeschlossen werden sollen. Weitere Informationen finden Sie unter Konfigurieren von Standardausnahmen für Antivirus (auf Englisch) und Konfigurieren von Komponenten-spezifischer Ausnahmen (auf Englisch).

Patch Management: Geben Sie Ausnahmen für ausgewählte Patch-Anbieter und Schweregrade an. Weitere Informationen finden Sie unter Patch-Ausnahmen (auf Englisch).

Erstellen standortspezifischer Ausnahmen

1. Wählen Sie im Dropdown-Menü oben links den Standort aus.
2. Klicken Sie auf die Registerkarte **Richtlinien**.
3. Wählen Sie den Namen der globalen Richtlinie in der Liste aus.
    - **Achten Sie darauf, dass der Standort auf die globale Richtlinie zugreifen kann, indem Sie sie zuweisen (siehe unten).**
4. Gehen Sie zu **Ausnahmen ▸ Antivirus-Ausnahmen**.
5. Geben Sie die standortspezifischen Ausnahmen auf der gewünschten Registerkarte ein.
6. Klicken Sie auf **Sichern**.

Zuweisungen

Klicken Sie auf **+ Standorten zuweisen**, um es bestimmten Standorten zu ermöglichen, die globale Richtlinie zu verwenden. Sie können Standorte auch aus der Zuweisungsliste entfernen, indem Sie die Kontrollkästchen verwenden und auf **Richtlinienzuweisung aufheben** klicken.

Nachdem Sie Änderungen an der Richtlinie vorgenommen haben, klicken Sie unten rechts im Bereich (Drawer) auf „Speichern".