
Bitdefender ENTERPRISE
SMALL OFFICE SECURITY
Schnellstart-Anleitung ››

Small Office Security
Schnellstart-Anleitung

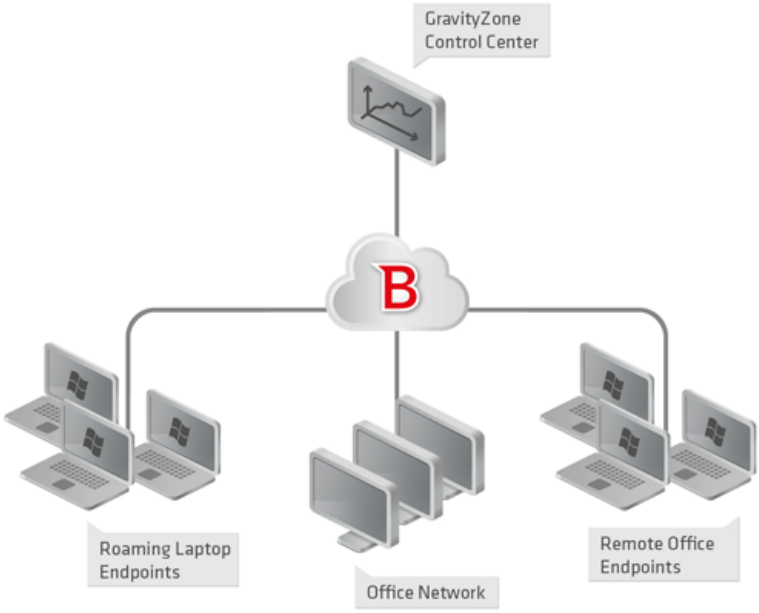
Veröffentlicht 2014.02.28


Bitdefender

Inhaltsverzeichnis

1. Über Small Office Security

Small Office Security ist ein Cloud-basierter Dienst zum Schutz vor Malware, der von Bitdefender für Computer mit Microsoft-Windows- und Macintosh-Betriebssystemen entwickelt wurde. Der Dienst nutzt ein zentrales Software-as-a-Service-Model mit verschiedenen Bereitstellungsoptionen, die sich besonders für Unternehmenskunden eignen. Gleichzeitig kommen bewährte Malware-Schutz-Technologien zum Einsatz, die von Bitdefender für den Privatanwendermarkt entwickelt wurden.



Small Office Security-Architektur

Die Sicherheitsdienste werden in der öffentlichen Cloud von Bitdefender gehostet. Abonnenten erhalten Zugriff auf eine Web-basierte Verwaltungsoberfläche, die sogenannte **Control Center**. Über diese Oberfläche können Administratoren per Fernzugriff den Malware-Schutz auf allen Windows- und Macintosh-Computern installieren und verwalten. Dazu gehören: Server und Arbeitsplatzrechner im internen Netzwerk, Laptop-Endpunkte im Roaming oder Endpunkte in Zweigniederlassungen.

Eine lokale Anwendung mit dem Namen **Endpoint Security** wird auf jedem geschützten Rechner installiert. Lokale Anwender haben nur begrenzten Einblick in die

Sicherheitseinstellungen und können sie selbst nicht verändern. Die Einstellungen werden vom Administrator zentral über die Control Center verwaltet; Scans, Updates und Konfigurationsänderungen werden in der Regel im Hintergrund durchgeführt.

2. Erste Schritte

Security for Endpoints kann mit der Control Center konfiguriert und verwaltet werden. Dabei handelt es sich um eine von Bitdefender gehostete, webbasierte Oberfläche.

Nach Ihrer Anmeldung für die Testversion oder dem Erwerb des Dienstes erhalten Sie eine E-Mail vom Bitdefender-Registrierungsservice. Die E-Mail enthält Ihre Anmeldeinformationen.

2.1. Verbinden mit dem Control Center

Der Zugriff auf die Control Center erfolgt über Benutzerkonten. Sie erhalten Ihre Anmeldeinformationen per E-Mail, sobald Ihr Konto angelegt wurde.

Vorbereitende Maßnahmen:

- Internet Explorer 9+, Mozilla Firefox 14+, Google Chrome 15+, Safari 5+
- Empfohlene Bildschirmauflösung: 1024x768 oder höher.

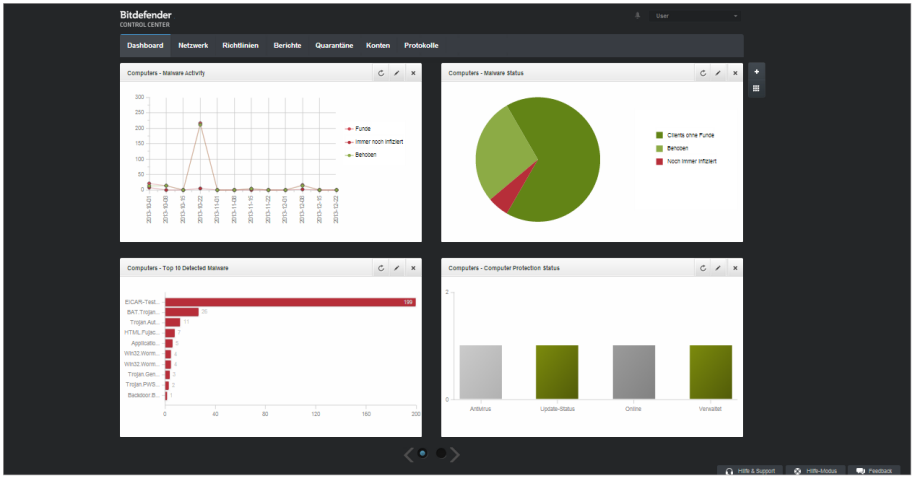
So stellen Sie eine Verbindung zum Control Center her:

1. Öffnen Sie Ihren Internet-Browser.
2. Rufen Sie die folgende Seite auf: https://gravityzone.bitdefender.com
3. Geben Sie die E-Mail-Adresse und das Passwort für Ihr Konto ein.
4. Klicken Sie auf **Anmelden**.

Beachten Sie
Sollten Sie Ihr Passwort vergessen haben, verwenden Sie den Link für die Passwortwiederherstellung, um ein neues Passwort anzufordern. Sie müssen die E-Mail-Adresse Ihres Kontos angeben.

2.2. Control Center auf einen Blick

Control Center ist so aufgebaut, dass Sie schnellen Zugriff auf alle Funktionen erhalten. Verwenden Sie die Menüleiste im oberen Bereich, um durch die Konsole zu navigieren. Welche Funktionen zur Verfügung stehen, hängt davon ab, welcher Benutzertyp auf die Konsole zugreift.



Das Dashboard

2.2.1. Übersicht über die Control Center

Benutzer mit der Unternehmensadministrator-Rolle haben volle Konfigurationsrechte für das Control Center und die Netzwerk Sicherheitsseinstellungen. Benutzer mit der Administrator-Rolle haben Zugriff auf Netzwerksicherheitsfunktion wie die Benutzerverwaltung.

Je nach ihrer Rolle können Small Office Security-Administratoren auf folgende Bereiche aus der Menüleiste zugreifen:

Dashboard
Übersichtliche Diagramme anzeigen, die wichtige Sicherheitsinformationen über Ihr Netzwerk enthalten.

Netzwerk
Schutz installieren, Richtlinien zur Verwaltung von Sicherheitseinstellungen anwenden, Aufgaben aus der Ferne ausführen und Schnellberichte erstellen.

Richtlinien
Sicherheitsrichtlinien erstellen und verwalten.

Berichte
Sicherheitsberichte über verwaltete Clients erhalten.

Quarantäne
Dateien in Quarantäne per Fernzugriff verwalten.

Konten
Zugriff zum Control Center anderer Mitarbeiter der Unternehmens verwalten.

Beachten Sie
Dieses Menü steht nur Benutzern zur Verfügung, die das Recht haben, Benutzer zu verwalten.

Protokolle
Das Benutzeraktivitätsprotokoll einsehen.

Außerdem erhalten Sie oben rechts in der Konsole über das Symbol  **Benachrichtigungen** schnellen Zugriff auf die Seite **Benachrichtigungen**.

Wenn Sie den Mauszeiger über den Benutzernamen in der rechten oberen Ecke der Konsole bewegen, erhalten Sie die folgenden Optionen:

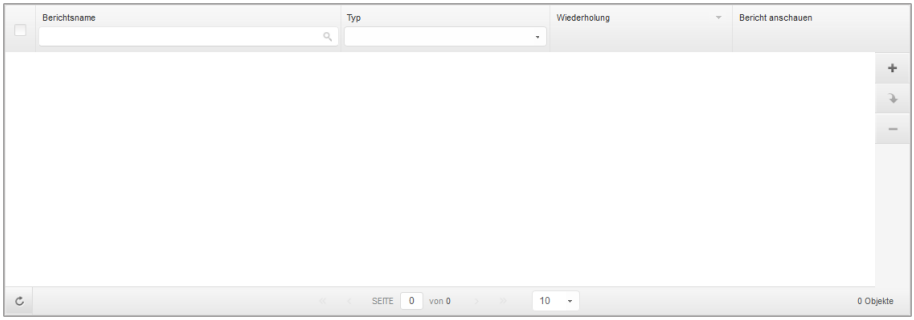
- **Mein Konto**. Klicken Sie auf diese Option, um Ihre Benutzerkontoinformationen und -einstellungen zu bearbeiten.
- **Mein Unternehmen**. Klicken Sie auf diese Option, um Ihre Unternehmenskontoinformationen und -einstellungen zu verwalten.
- **Zugangsdaten-Manager**. Klicken Sie auf diese Option, um die für Ferninstallationsaufgaben nötigen Authentifizierungsdaten hinzuzufügen und zu verwalten.
- **Abmelden**. Klicken Sie auf diese Option, um sich bei Ihrem Konto abzumelden.

In der rechten unteren Ecke der Konsole stehen die folgenden Links zur Verfügung:

- **Hilfe und Support**. Klicken Sie auf diese Schaltfläche, um Hilfe- und Support-Informationen zu erhalten.
- **Hilfe-Modus**. Klicken Sie auf diese Schaltfläche, um die Hilfefunktion zu aktivieren, mit der vergrößerbare Tooltipps für Control Center-Objekte angezeigt werden. Dadurch erhalten Sie nützliche Informationen zu den Funktionen des Control Center.
- **Feedback**. Klicken Sie auf diese Schaltfläche, um ein Formular anzuzeigen, in dem Sie uns Rückmeldung zu Ihren Erfahrungen mit Small Office Security zusenden können.

2.2.2. Tabellendaten

Tabellen kommen in der Konsole häufig zum Einsatz, um die Daten in einem übersichtlichen Format zu organisieren.



The Reports page - Reports Table

Durch Tabellenseiten blättern

Tabellen mit mehr als 10 Einträgen haben mehr als eine Seite. Standardmäßig werden nur 10 Einträge pro Seite angezeigt.Verwenden Sie die Navigationsschaltflächen am unteren Rand der Tabelle, um zwischen den Seiten zu wechseln.Sie können die Anzahl der Einträge, die pro Seite angezeigt werden, ändern, indem Sie eine andere Option aus dem Menü neben den Navigationsschaltflächen wählen.

Nach bestimmten Einträgen suchen

Über die Suchfelder unter den Spaltenüberschriften können Sie leicht bestimmte Einträge finden.

Geben Sie den Suchbegriff in das entsprechende Feld ein.Passende Suchtreffer werden bereits während der Eingabe in der Tabelle angezeigt.Um den Inhalt der Tabelle wieder herzustellen, löschen Sie einfach die Suchfelder.

Daten sortieren

Sie können die Daten in der Tabelle nach dem Inhalt einer bestimmten Spalte sortieren, indem Sie auf die entsprechende Spaltenüberschrift klicken.Mit einem erneuten Klick auf die Spaltenüberschrift kehren Sie die Sortierreihenfolge um.

Tabellendaten aktualisieren

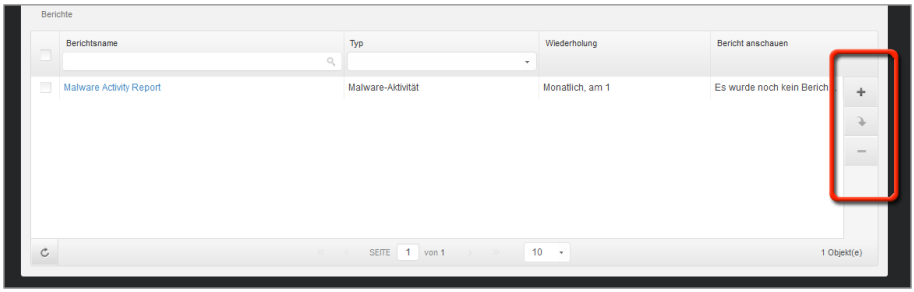
Um sicherzustellen, dass die aktuellsten Informationen angezeigt werden, klicken Sie im unteren linken Bereich der Tabelle auf **Aktualisieren**.

2.2.3. Symbolleisten

Im Control Center können Sie über Symbolleisten bestimmte Operationen ausführen, die zu dem Bereich gehören, indem Sie sich gerade befinden.Jede Symbolleiste besteht aus

mehreren Symbolen, die meistens auf der rechten Seite der Tabelle angezeigt werden.Über die Symbolleiste im Bereich **Berichte** können Sie zum Beispiel die folgenden Aktionen ausführen:

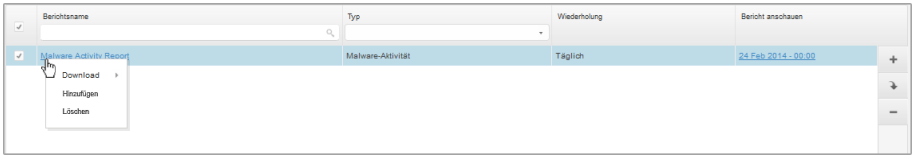
- Neuen Bericht erstellen.
- Geplant erstellte Berichte herunterladen.
- Einen geplanten Bericht löschen.



Die Berichtsübersicht - Symbolleisten

2.2.4. Kontextmenü

Die Symbolleistenbefehle stehen auch über das Kontextmenü zur Verfügung. Klicken Sie mit der rechten Maustaste auf den Bereich des Control Centers, den Sie gerade benutzen, und wählen Sie den gewünschten Befehl aus der Liste.

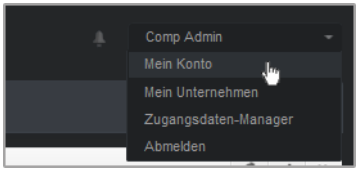


Die Berichtsübersicht - Kontextmenü

2.3. Verwalten Ihres Kontos

So überprüfen oder ändern Sie Ihre Kontodetails und -Einstellungen:

1. Bewegen Sie den Mauszeiger auf Ihren Benutzernamen in der rechten oberen Ecke der Konsole, und wählen Sie **Mein Konto**.



Das Benutzerkontomenü

2. Korrigieren oder aktualisieren Sie Ihre Kontoinformationen unter **Kontodetails**.
   - **Vollständiger Name.** Geben Sie Ihren vollen Namen ein.
   - **E-Mail.** Dies ist Ihre E-Mail-Adresse für die Anmeldung und den Kontakt.An diese Adresse werden Berichte und wichtige Sicherheitsbenachrichtigungen geschickt.Es werden automatisch E-Mail-Benachrichtigungen versandt, sobald wichtige Risikobedingungen im Netzwerk erkannt werden.
   - **Passwort.** Über den Link **Passwort ändern** können Sie Ihr Anmeldepasswort ändern.
3. Konfigurieren Sie die Kontoeinstellungen unter **Einstellungen** nach Ihren Wünschen.
   - **Zeitzone.** Wählen Sie im Menü die Zeitzone für das Konto. Die Konsole zeigt die aktuelle Zeit entsprechend der ausgewählten Zeitzone.
   - **Sprache.**Wählen Sie im Menü die Anzeigesprache für die Konsole aus.
   - **Zeitüberschreitung der Sitzung.** Legen Sie den Inaktivitätszeitraum fest, nach dem Ihre Sitzung abläuft.
4. Klicken Sie auf **Speichern**, um die Änderungen zu speichern.

Beachten Sie
Sie können Ihr eigenes Konto nicht löschen.

2.4. Ändere Login Passwort

Nachdem Ihr Konto angelegt wurde, erhalten Sie eine E-Mail mit den Anmeldedaten.

- Ändern Sie das Standardpasswort nach dem ersten Aufrufen von Control Center.
- Ändern Sie Ihr Kennwort regelmäßig.

Um das Anmeldepasswort zu ändern:

1. Bewegen Sie den Mauszeiger auf Ihren Benutzernamen in der rechten oberen Ecke der Konsole, und wählen Sie **Mein Konto**.
2. Klicken Sie unter **Kontodetails** auf **Passwort ändern**.
3. Geben Sie Ihr aktuelles Passwort und das neue Passwort in die entsprechenden Felder ein.
4. Klicken Sie auf **Speichern**, um die Änderungen zu speichern.

3. Lizenzmanagement

Die Sicherheitsdienste in Small Office Security erfordern einen gültigen Lizenzschlüssel.

Sie können Small Office Security 30 Tage lang kostenlos testen. Während der Testphase stehen alle Funktionen uneingeschränkt zur Verfügung. Sie können den Dienst auf beliebig vielen Computern nutzen. Falls Sie den Dienst weiterhin nutzen möchten, müssen Sie vor Ablauf der Testphase ein kostenpflichtiges Abonnement auswählen und abschließen.

Die Anmeldung für den Dienst kann auf zwei Arten erfolgen:

- Anmeldung über einen Bitdefender-Wiederverkäufer.Unsere Wiederverkäufer stellen Ihnen alle benötigten Informationen zur Verfügung und unterstützen Sie bei der Auswahl eines Abonnements, das Ihren Zwecken gerecht wird.Einige Wiederverkäufer bieten Mehrwertdienstleistungen, so zum Beispiel Premium-Support, andere wiederum umfassende Managed Services.

  So finden Sie einen Bitdefender-Wiederverkäufer in Ihrem Land:

  1. Gehen Sie zu http://www.bitdefender.de/partners.
  2. Öffnen Sie den **Partnerfinder**.
  3. Die Kontaktinformationen der Bitdefender-Partner sollten automatisch angezeigt werden. Sollte dies nicht der Fall sein, so wählen Sie Ihr Land aus, um die Informationen anzuzeigen.
  4. Falls Sie in Ihrem Land keinen Bitdefender-Händler finden, können Sie uns gerne unter vertrieb@bitdefender.de kontaktieren.Bitte schreiben Sie uns Ihre E-Mail in Englisch, damit wir Ihnen umgehend helfen können.
- Anmeldung über die Bitdefender-Website.

Ihr Abonnement wird von Bitdefender oder dem Bitdefender-Partner verwaltet, über den Sie den Dienst erworben haben. Manche Bitdefender-Partner sind Sicherheitsdienstleister. Abhängig von Ihrer Abonnementvereinbarung wird der tägliche Betrieb von Small Office Security entweder intern von Ihrem Unternehmen oder extern durch den Sicherheitsdienstleister übernommen.

3.1. Aktivieren einer Lizenz

Beim ersten Abschluss eines kostenpflichtigen Abonnements erhalten Sie einen Lizenzschlüssel. Durch das Aktivieren dieses Lizenzschlüssels aktivieren Sie auch Ihr Small Office Security-Abonnement.

Warnung

Die Aktivierung einer Lizenz überträgt deren Umfang NICHT auf die aktuelle Lizenz. Die alte Lizenz wird vielmehr durch die neue überschrieben. Wenn Sie zum Beispiel eine Lizenz für 10 Endpunkte über einer bestehenden Lizenz für 100 Endpunkte aktivieren, erhalten Sie KEIN Lizenzvolumen von 110 Endpunkten. Im Gegenteil, die Anzahl der lizenzierten Endpunkte sinkt von 100 auf 10.

Der Lizenzschlüssel wird Ihnen nach Erwerb per E-Mail zugesendet. Abhängig von Ihrer Dienstleistungsvereinbarung wird Ihr Dienstleister unter Umständen den freigegebenen Lizenzschlüssel für Sie aktivieren. Alternativ können Sie Ihre Lizenz auch manuell aktivieren. Gehen Sie dazu folgendermaßen vor:

1. Melden Sie sich über Ihr Kundenkonto an der Control Center an.
2. Bewegen Sie den Mauszeiger auf Ihr Benutzerkonto in der rechten oberen Ecke der Konsole, und wählen Sie **Mein Unternehmen**.
3. Details zu Ihrer aktuellen Lizenz finden Sie im Bereich **Lizenz**.
4. Geben Sie im Feld **Lizenz** Ihren Lizenzschlüssel ein.
5. Klicken Sie auf die **Überprüfen**-Schaltfläche und warten Sie, bis die Control Center die Informationen über den eingegebenen Lizenzschlüssel abgerufen hat.
6. Klicken Sie auf **Speichern**.

3.2. Aktuelle Lizenzinformationen anzeigen

Um Ihren Abonnementstatus zu überprüfen:

1. Melden Sie mit Ihrer E-Mail-Adresse und dem per E-Mail zugesandten Passwort an der Control Center an.
2. Bewegen Sie den Mauszeiger auf Ihr Benutzerkonto in der rechten oberen Ecke der Konsole, und wählen Sie **Mein Unternehmen**.
3. Details zu Ihrer aktuellen Lizenz finden Sie im Bereich **Lizenz**. Alternativ können Sie auch auf die **Überprüfen**-Schaltfläche klicken und warten, bis die Control Center die aktuellen Informationen zum vorliegenden Lizenzschlüssel abgerufen hat.
4. Geben Sie im Feld **Lizenz** Ihren Lizenzschlüssel ein.
5. Klicken Sie auf die **Überprüfen**-Schaltfläche und warten Sie, bis die Control Center die Informationen über den eingegebenen Lizenzschlüssel abgerufen hat.
6. Klicken Sie auf **Speichern**.

4. Installation und Einrichtung

Die Installation und Einrichtung gestalten sich relativ einfach.Im Folgenden die wichtigsten Schritte:

1. Schritt 1 - Vorbereiten der Installation
2. Schritt 2 - Installieren des Dienstes auf den Computern
3. Schritt 3 - Aufteilen von Computern in Gruppen (optional)
4. Schritt 4 - Anlegen und Konfigurieren einer Sicherheitsrichtlinie

Für die ersten beiden Schritte benötigen Sie die Computer-Anmeldedaten. Die folgenden zwei Schritte werden über die Control Center durchgeführt.

4.1. Vor der Installation

Bevor Sie mit der Installation beginnen, sollten Sie die folgenden Hinweise beachten, um einen reibungslosen Ablauf zu garantieren:

1. Stellen Sie sicher, dass die Computer die Mindestsystemanforderungen erfüllen.Bei manchen Computern kann es notwendig werden, das neueste Service Pack für das Betriebssystem zu installieren oder Speicherplatz zu schaffen.Legen Sie eine Liste mit den Computern an, die die notwendigen Anforderungen nicht erfüllen, damit Sie diese von der Verwaltung ausschließen können.
2. Entfernen Sie alle bereits installierten Anti-Malware-, Internet-Sicherheits- und Firewall-Lösungen von Ihren Computern (eine Deaktivierung ist nicht ausreichend).Wenn Endpoint Security gleichzeitig mit anderen Sicherheitslösungen auf einem Computer betrieben wird, kann dies die jeweilige Funktion stören und massive Probleme auf dem System verursachen.

   Viele der Sicherheitsprogramme, mit denen Endpoint Security nicht kompatibel ist, werden bei der Installation automatisch erkannt und entfernt.Weitere Informationen und eine Übersicht über die Sicherheitslösungen, die erkannt werden, erhalten Sie in diesem Artikel in der Wissensdatenbank.

   Wichtig
   Um die Windows-Sicherheitsfunktionen (Windows Defender, Windows Firewall) müssen Sie sich nicht kümmern. Diese werden vor Beginn der Installation automatisch deaktiviert.

3. Für die Installation benötigen Sie Administratorrechte und Zugriff auf das Internet. Sorgen Sie dafür, dass Sie alle nötigen Zugangsdaten für alle Computer zur Hand haben.
4. Computer müssen eine funktionierende Verbindung zur Control Center haben.

4.2. Installieren des Dienstes auf den Computern

Security for Endpoints wurde für Arbeitsplatzrechner, Laptops und Server mit Microsoft® Windows als Betriebssystem entwickelt.Um Computer mit Security for Endpoints zu schützen, müssen Sie Endpoint Security (die Client-Software) auf jedem Computer installieren. Endpoint Security verwaltet den Schutz auf dem lokalen Computer. Zudem kommuniziert er mit dem Control Center, um Befehle des Administrators entgegenzunehmen und die Ergebnisse seiner Aktionen zu übermitteln.

Sie können Endpoint Security mit einer der folgenden Rollen (verfügbar über den Installationsassistenten) installieren:

1. **Endpunkt**, wenn der entsprechende Computer ein regulärer Endpunkt im Netzwerk ist.
2. **Endpoint Security Relay**, wenn der entsprechende Computer von anderen Endpunkten im Netzwerk verwendet wird, um mit der Control Center zu kommunizieren. Die Endpoint Security Relay-Rolle installiert Endpoint Security zusammen mit einem Update-Server, über den alle anderen Clients im Netzwerk aktualisiert werden können. Endpunkte im gleichen Netzwerk können über Richtlinien so konfiguriert werden, dass sie mit der Control Center über einen oder mehrere Computer mit der Endpoint Security Relay-Rolle kommunizieren. Ist ein Endpoint Security Relay nicht verfügbar, wird so der nächst verfügbare berücksichtigt, um die Kommunikation des Computers mit der Control Center sicherzustellen.

Warnung

- Der erste Computer, auf dem Sie den Schutz installieren, muss die Endpoint Security Relay-Rolle haben, sonst können Sie Endpoint Security nicht auf anderen Computern im Netzwerk bereitstellen.
- Der Computer mit der Endpoint Security Relay-Rolle muss eingeschaltet und online sein, damit die Clients mit der Control Center kommunizieren können.

Es gibt zwei Installationsmethoden:

- **Lokale Installation**. Laden Sie die Installationspakete von der Control Center auf die einzelnen Computer herunter und führen Sie die Endpoint Security-Installation lokal durch. Eine weitere Option ist es, das Paket herunterzuladen und auf einer Netzwerkfreigabe zu speichern. Schicken Sie den Benutzern im Unternehmen danach E-Mail-Einladungen mit einem Link zu dem Paket und bitten Sie sie, es herunterzuladen und den Schutz auf ihren Computern zu installieren. Die lokale Installation wird durch einen Assistenten unterstützt.
- **Remote-Installation**. Nachdem Sie den ersten Client mit der Endpoint Security Relay-Rolle lokal installiert haben, kann es einige Minuten dauern, bis die anderen Netzwerk-Computer in der Control Center angezeigt werden. Der Security for Endpoints-Schutz kann dann über die Konsole per Fernzugriff auf den anderen Computern

im Netzwerk installiert werden. Die Remote-Installation erfolgt im Hintergrund, ohne dass der Benutzer dies bemerkt.

Endpoint Security verfügt über eine stark eingeschränkte Benutzeroberfläche. Über sie können Anwender den Sicherheitsstatus einsehen und grundlegende Sicherheitsaufgaben (Updates und Scans) ausführen, haben jedoch keinen Zugriff auf die Einstellungen.

Die Anzeigesprache der Benutzeroberfläche auf geschützten Computern wird bei der Installation standardmäßig entsprechend der für Ihr Konto eingestellten Sprache festgelegt.Um die Benutzeroberfläche auf bestimmten Computern mit einer anderen Sprache einzurichten, können Sie ein Installationspaket erstellen und die bevorzugte Sprache in den Konfigurationsoptionen für dieses Paket festlegen. Weitere Informationen zur Erstellung von Installationspaketen finden Sie unter „Endpoint Security Installationspakete erstellen“ (S. 13).

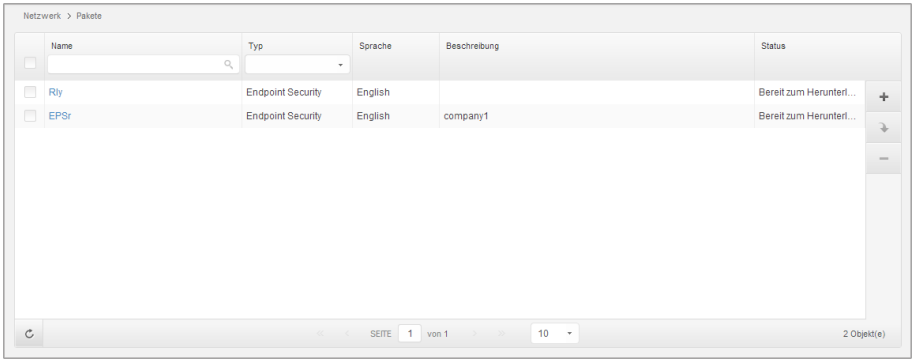
4.2.1. Lokale Installation

Die lokale Installation erfordert den Download des Installationspakets von der Control Center und dessen Ausführung auf jedem Zielcomputer. Sie können verschiedene Installationspakete in Übereinstimmung mit den Anforderungen der verschiedenen Computer erstellen (so zum Beispiel der Installationspfad oder die Sprache der Benutzeroberfläche).

Endpoint Security Installationspakete erstellen

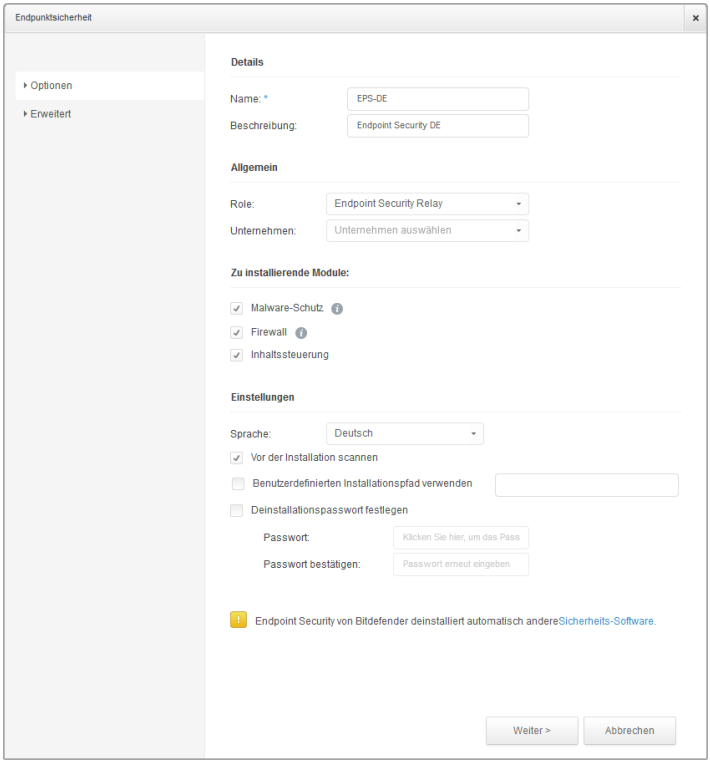
So erstellen Sie ein Installationspaket für Endpoint Security:

1. Stellen Sie eine Verbindung zur Control Center her und melden Sie sich mit Ihrem Benutzerkonto an.
2. Gehen Sie zur Seite **Netzwerk > Pakete**.



Die Paketübersicht

3. Klicken Sie auf die Schaltfläche + **Hinzufügen** auf der rechten Seite der Tabelle. Ein Konfigurationsfenster wird sich öffnen.



Erstellen von Endpoint Security-Paketen - Optionen

4. Geben Sie einen aussagekräftigen Namen und eine Beschreibung für das zu erstellende Installationspaket ein.
5. Wählen Sie die Rolle des gewünschten Computers:
   - **Endpunkt**. Wählen Sie diese Option aus, um das Paket für einen regulären Endpunkt zu erstellen.
   - **Endpoint Security Relay**. Wählen Sie diese Option aus, um das Paket für einen Endpunkt mit der Endpoint Security Relay-Rolle zu erstellen. Endpoint Security Relay ist eine spezielle Rolle, die zusammen mit dem Endpoint Security einen Update-Server auf der Zielmaschine installiert, über den alle anderen Clients im Netzwerk aktualisiert werden können. Dadurch sinkt die benötigte Bandbreite zwischen den Clients und der Control Center.

6. Wählen Sie das Unternehmen aus, in dem das Installationspaket zum Einsatz kommt.
7. Wählen Sie die Schutzmodule aus, die Sie installieren möchten.
8. Wählen Sie aus dem Feld **Sprache** die gewünschte Sprache für die Client-Oberfläche.
9. Wählen Sie **Vor der Installation scannen**, wenn Sie sichergehen möchten, dass die Computer sauber sind, bevor Sie Endpoint Security auf ihnen installieren. Ein Cloud-Schnell-Scan wird auf den entsprechenden Computern ausgeführt, bevor die Installation gestartet wird.
10. Endpoint Security wird im Standardinstallationsordner auf den ausgewählten Computern installiert.Wählen Sie **Benutzerdefinierten Installationspfad verwenden**, wenn Sie Endpoint Security in einem anderen Ordner installieren möchten.Geben Sie in diesem Fall den gewünschten Pfad in das entsprechende Feld ein.Verwenden Sie dabei Windows-Konventionen (zum Beispiel `D:\Ordner`).Wenn der angegebene Ordner nicht existiert, wird er während der Installation erstellt.
11. Bei Bedarf können Sie ein Passwort einrichten, um zu verhindern, dass Benutzer Ihren Schutz entfernen.Wählen Sie **Deinstallationspasswort festlegen** und geben Sie das gewünschte Passwort in die entsprechenden Felder ein.
12. Klicken Sie auf **Weiter**.
13. Wählen Sie je nach der Rolle des Installationspakets (Endpunkt oder Endpoint Security Relay), mit welcher Entität sich die Zielcomputer in regelmäßigen Abständen verbinden, um den Client zu aktualisieren:
    - **Bitdefender Cloud**, wenn Sie die Clients direkt aus dem Internet aktualisieren wollen.
    - **Endpoint Security Relay**, wenn Sie die Clients über die in Ihrem Netzwerk installierten Endpoint Security Relay-Endpunkte aktualisieren möchten. In diesem Fall werden alle in Ihrem Netzwerk gefundenen Endpunkte mit der Endpoint Security Relay-Rolle in der unten angezeigten Tabelle aufgelistet. Wählen Sie den Endpoint Security Relay, den Sie für Client-Updates benutzen möchten.
14. Klicken Sie auf **Speichern**.

Das neue Installationspaket erscheint in der Liste der Pakete für das Zielunternehmen.

Herunterladen und Installieren von Endpoint Security

1. Verwenden Sie Ihr Konto auf dem Computer, auf dem Sie den Schutz installieren wollen, um https://gravityzone.bitdefender.com/ aufzurufen.
2. Gehen Sie zur Seite **Netzwerk > Pakete**.
3. Wählen Sie das entsprechende Unternehmen aus der Liste unter der Spaltenüberschrift **Unternehmen**. Es werden nur die für das ausgewählte Unternehmen verfügbaren Pakete angezeigt.
4. Wählen Sie das Endpoint Security-Installationspaket aus, das Sie herunterladen möchten.

5. Klicken Sie auf die Schaltfläche **Herunterladen** auf der rechten Seite der Tabelle und wählen Sie den Installer-Typ aus, den Sie verwenden möchten. Es gibt zwei Arten von Installationsdateien:
   - **Downloader**. Der Downloader lädt zunächst das vollständige Installationspaket von den Bitdefender-Cloud-Servern herunter und beginnt dann mit der Installation. Der Installer ist ein kleines Programm und kann sowohl auf 32-Bit- als auch auf 64-Bit-Systemen ausgeführt werden (und vereinfacht so die Verteilung). Er erfordert jedoch eine aktive Internet-Verbindung.
   - **Installationspaket**. Das vollständige Installationspaket wird verwendet, um den Schutz auf Computern mit einer langsamen bzw. keiner Internet-Verbindung zu installieren. Laden Sie diese Datei auf einen mit dem Internet verbundenen Computer herunter und nutzen Sie externe Speichermedien oder eine Netzwerkfreigabe für die Verteilung auf andere Computer. Bitte beachten Sie, dass für Windows zwei Versionen zur Verfügung stehen: eine für 32-Bit-Systeme und eine weitere für 64-Bit-Systeme. Stellen Sie sicher, dass Sie die zum jeweiligen Computer passende Version wählen.
6. Speichern Sie die Datei auf dem Computer.
7. Führen Sie das Installationspaket aus.

Beachten Sie
Damit die Installation ordnungsgemäß funktioniert, muss das Installationspaket mit Administratorrechten oder unter einem Administratorkonto ausgeführt werden.

8. Folgen Sie den Instruktionen auf dem Bildschirm.

Einige Minuten nachdem Endpoint Security installiert wurde, taucht der Computer als verwaltet im Control Center auf (**Netzwerk**-Seite).

4.2.2. Remote-Installation

Nachdem Sie den ersten Client mit der Endpoint Security Relay-Rolle lokal installiert haben, kann es einige Minuten dauern, bis die anderen Netzwerk-Computer in der Control Center angezeigt werden. Von hier an können Sie Endpoint Security per Fernzugriff auf Computern unter Ihrer Verwaltung mithilfe der Installationsaufgaben in der Control Center installieren.

Um die Bereitstellung zu vereinfachen, verfügt Security for Endpoints über einen automatischen Mechanismus zur Netzwerkerkennung, mit dem Computer im gleichen Netzwerk gefunden werden können. Gefundene Computer werden als **Nicht verwaltete Computer** in der **Netzwerk**übersicht angezeigt.

Damit Sie die Netzwerkerkennung und Ferninstallation durchführen können, muss Endpoint Security bereits auf mindestens einem Computer im Netzwerk installiert sein. Dieser Computer wird dann eingesetzt, um das Netzwerk zu scannen und Endpoint Security auf den noch nicht geschützten Computern zu installieren. Es kann einige Minuten dauern, bis die anderen Netzwerk-Computer in der Control Center angezeigt werden.

Anforderungen für die Ferninstallation

Um die Netzwerkerkennung zu funktionieren, müssen eine Reihe von Systemanforderungen erfüllt werden. Für weitere Informationen lesen Sie bitte „Wie die Netzwerkerkennung funktioniert“ (S. 31).

Damit die Ferninstallation funktioniert, müssen die folgenden Punkte gegeben sein:

- Auf jedem Zielcomputer muss die Administrator-Netzwerkfreigabe admin$ aktiviert sein. Konfigurieren Sie jeden Zielarbeitsplatzrechner für die erweiterte Freigabe von Dateien.
- Schalten Sie vorübergehend die Benutzerkontensteuerung auf allen Computern mit Windows-Betriebsystemen, die diese Sicherheitsfunktion beinhalten (Windows Vista, Windows 7, Windows Server 2008 etc.) aus. Wenn die Computer Teil einer Domain sind, können Sie die Benutzerkontensteuerung aus der Ferne über eine Gruppenrichtlinie ausschalten.
- Deaktivieren oder schließen Sie etwaige Firewalls auf den Computern. Wenn die Computer Teil einer Domain sind, können Sie die Windows-Firewall aus der Ferne über eine Gruppenrichtlinie ausschalten.

Durchführen von Endpoint Security-Ferninstallationsaufgaben

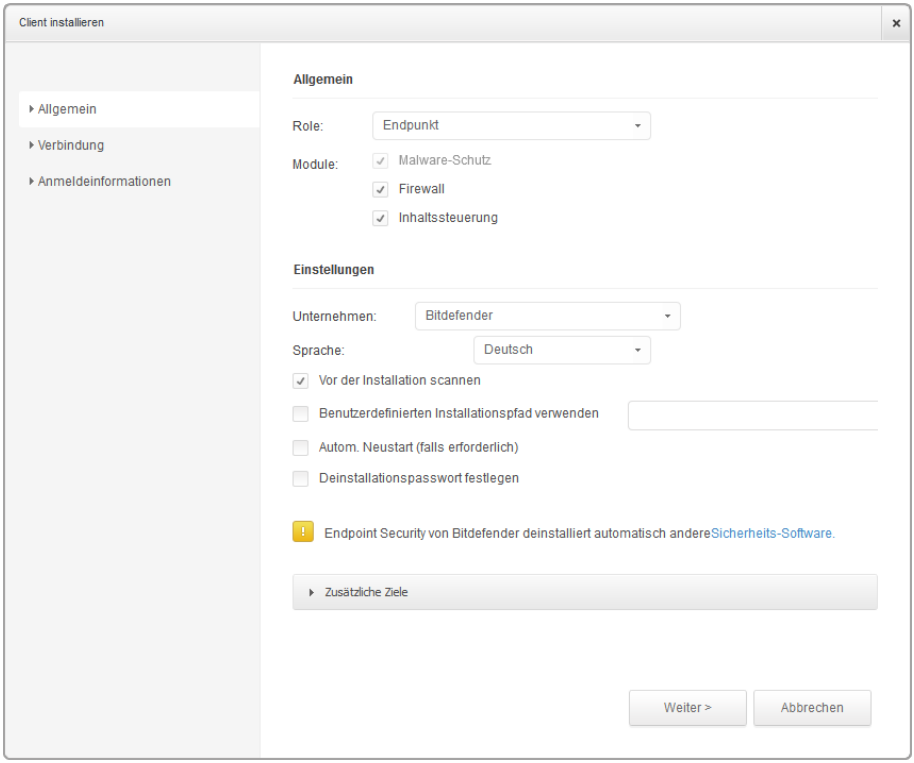
So führen Sie eine Ferninstallationsaufgabe aus:

1. Stellen Sie eine Verbindung zur Control Center her und melden Sie sich an.
2. Gehen Sie zur Seite **Netzwerk**.
3. Wählen Sie die gewünschte Netzwerkgruppe aus dem linken Fenster aus.Die Entitäten der ausgewählten Gruppe werden in der Tabelle im rechten Fenster angezeigt.

   Beachten Sie
   Sie können optional auch Filter anwenden, um ausschließlich die nicht verwalteten Computer anzuzeigen. Klicken Sie auf die **Filter**-Schaltfläche und wählen Sie die folgenden Optionen: **Nicht verwaltet** aus der Kategorie **Sicherheit** und **Alle Objekte rekursiv** aus der Kategorie **Tiefe**.

4. Wählen Sie die Entitäten (Computer oder Gruppen von Computern) aus, auf denen Sie den Schutz installieren möchten.
5. Klicken Sie auf die Schaltfläche **Aufgaben** auf der rechten Seite der Tabelle, und wählen Sie **Client installieren**.Der Assistent **Client installieren** wird angezeigt.



Installieren von Endpoint Security über das Aufgabenmenü

6. Konfigurieren Sie die Installationsoptionen:
   - Wählen Sie die Rolle, die der Client haben soll:
     - **Endpunkt**. Wählen Sie diese Option aus, wenn Sie den Client auf einem regulären Endpunkt installieren möchten.
     - **Endpoint Security Relay**. Wählen Sie diese Option aus, um den Client mit Endpoint Security Relay-Rolle auf dem Ziel-Computer zu installieren. Endpoint Security Relay ist eine spezielle Rolle, die zusammen mit dem Endpoint Security einen Update-Server auf der Zielmaschine installiert, über den alle anderen Clients im Netzwerk aktualisiert werden können. Dadurch sinkt die benötigte Bandbreite zwischen den Clients und der Control Center.
   - Wählen Sie die Schutzmodule aus, die Sie installieren möchten. Bitte beachten Sie, dass für Server-Betriebssysteme nur der Malware-Schutz verfügbar ist.
   - Wählen Sie aus dem Feld **Sprache** die gewünschte Sprache für die Client-Oberfläche.

- Wählen Sie **Vor der Installation scannen**, wenn Sie sichergehen möchten, dass die Computer sauber sind, bevor Sie Endpoint Security auf ihnen installieren.Ein Cloud-Schnell-Scan wird auf den entsprechenden Computern ausgeführt, bevor die Installation gestartet wird.
- Endpoint Security wird im Standardinstallationsordner auf den ausgewählten Computern installiert.Wählen Sie **Benutzerdefinierten Installationspfad verwenden**, wenn Sie Endpoint Security in einem anderen Ordner installieren möchten.Geben Sie in diesem Fall den gewünschten Pfad in das entsprechende Feld ein.Verwenden Sie dabei Windows-Konventionen (zum Beispiel `D:\Ordner`).Wenn der angegebene Ordner nicht existiert, wird er während der Installation erstellt.
- Während der automatischen Installation wird der Computer nach Malware durchsucht. In einigen Fällen kann es notwendig sein, einen Neustart durchzuführen, um die Entfernung der Malware abzuschließen.

  Wählen Sie **Automatischer Neustart (falls nötig)**, um sicherzustellen, dass gefundene Malware vor der Installation vollständig entfernt wurde. Sonst könnte die Installation fehlschlagen.
- Bei Bedarf können Sie ein Passwort einrichten, um zu verhindern, dass Benutzer Ihren Schutz entfernen.Wählen Sie **Deinstallationspasswort festlegen** und geben Sie das gewünschte Passwort in die entsprechenden Felder ein.
- Klicken Sie auf **Weiter**.
- Wählen Sie je nach der Client-Rolle (Endpunkt oder Endpoint Security Relay), über welche Entität die Clients kommunizieren sollen:
  - **Bitdefender Cloud**, wenn Sie die Clients direkt aus dem Internet aktualisieren wollen.
  - **Endpoint Security Relay**, wenn Sie die Clients über die in Ihrem Netzwerk installierten Endpoint Security Relay-Endpunkte aktualisieren möchten. In diesem Fall werden alle in Ihrem Netzwerk gefundenen Endpunkte mit der Endpoint Security Relay-Rolle in der unten angezeigten Tabelle aufgelistet. Wählen Sie den Endpoint Security Relay, den Sie für Client-Updates benutzen möchten.

7. Klicken Sie auf **Weiter**.
8. Geben Sie im Bereich **Zugangsdaten-Manager** die Administratorzugangsdaten an, die für die Fernauthentifizierung auf den ausgewählten Endpunkte benötigt wird.

   Sie können die erforderlichen Zugangsdaten hinzufügen, indem Sie den Benutzer und das Passwort der Zielbetriebssysteme eingeben.

   Beachten Sie

   Wenn Sie noch keine Zugangsdaten ausgewählt haben, wird eine Warnmeldung angezeigt.Dieser Schritt ist für die Ferninstallation von Endpoint Security auf Computern unumgänglich.

So fügen Sie erforderlichen OS-Zugangsdaten hinzu:

a. Geben Sie in den entsprechenden Feldern den Namen und das Passwort eines Administratorkontos für jedes der Betriebssysteme ein.Sie können jedem Konto eine Beschreibung hinzufügen, um es später leichter identifizieren zu können.Wenn Computer in einer Domäne sind, reicht es aus, die Anmeldeinformationen des Domänenadministrators einzugeben.Verwenden Sie Windows-Konventionen, wenn Sie den Namen eines Domänenbenutzerkontos eingeben (z.B. `domain\user` oder `user@domain.com`).

Beachten Sie

Die angegebenen Zugangsdaten werden automatisch im Zugangsdaten-Manager gespeichert, sodass Sie sie beim nächsten Mal nicht mehr eingeben müssen.

b. Klicken Sie auf den Button **Hinzufügen**.Das Konto wird zu der Liste der Zugangsdaten hinzugefügt.

c. Markieren Sie das Kästchen für das Konto, das Sie verwenden möchten.

9. Klicken Sie auf **Speichern**.Eine Bestätigungsmeldung wird angezeigt.

Auf der Seite **Netzwerk > Aufgaben** können Sie Aufgaben anzeigen und verwalten.

4.3. Aufteilen von Computern (optional)

Unternehmensnetzwerke werden im linken Fenster der **Netzwerk**übersicht angezeigt. Es gibt eine Standardstammgruppe für jedes Ihrer Unternehmen. Alle dazugehörigen geschützten oder gefundenen Computer werden automatisch in diese Gruppe aufgenommen.

Wenn Sie eine größere Anzahl Computer verwalten (zehn und mehr), empfiehlt es sich, diese in Gruppen aufzuteilen. Durch die Aufteilung der Computer in Gruppen können Sie diese effizienter verwalten. Ein großer Vorteil ist, dass Sie Gruppenrichtlinien verwenden können, um verschiedene Sicherheitsanforderungen zu erfüllen.

Sie können die Computer ordnen, indem Sie unter der standardmäßigen Unternehmensgruppe weitere Gruppen anlegen und die Computer in die entsprechenden Gruppen verschieben.

Bevor Sie Gruppen erstellen, sollten Sie sich überlegen, warum Sie diese Gruppen brauchen und sie dann nach einem bestimmten System erstellen. Sie können Computer zum Beispiel anhand von einem oder einer Kombination der folgenden Kriterien in Gruppen einteilen:

- Organisationsstruktur (Vertrieb, Marketing, Qualitätssicherung, Unternehmensführung usw.).
- Sicherheitsanforderungen (Desktop-Rechner, Laptops, Server usw.).
- Standort (Hauptsitz, Niederlassungen, mobile Angestellte, Heimarbeitsplätze usw.).

Beachten Sie

- Eine angelegte Gruppe kann sowohl Computer als auch andere Gruppen enthalten.
- Wenn Sie im linken Fenster eine Gruppe auswählen, können Sie alle enthaltenen Computer einsehen - ausgenommen der, die in Untergruppen eingeordnet wurden. Wenn Sie alle Computer in einer Gruppe und in ihren Untergruppen anzeigen möchten, klicken Sie auf das Filtermenü oberhalb der Tabelle, und wählen Sie dann **Typ > Computer** sowie **Tiefe > Alle Objekte rekursiv**.

Um das Netzwerk eines Kunden in Gruppen aufzuteilen:

1. Gehen Sie zur Seite **Netzwerk**.
2. Wählen Sie im Fenster links unter **Unternehmen** das Kundenunternehmen aus, das Sie verwalten möchten.

   ### Beachten Sie
   Wählen Sie für Partnerunternehmen unter Ihrem Konto, die die Berechtigung zur Netzwerkverwaltung haben, die **Netzwerke**gruppe aus.

3. Klicken Sie auf die Schaltfläche + **Gruppe hinzufügen** im oberen Bereich des linken Fensters.
4. Geben Sie einen aussagekräftigen Namen für die Gruppe ein, und klicken Sie auf **OK** Die neue Gruppe wird unter dem entsprechenden Unternehmen angezeigt.
5. Wiederholen Sie die vorausgegangenen Schritte, um weitere Gruppen anzulegen.
6. Verschieben Sie Computer von der Stammgruppe in die passende Gruppe:
   a. Markieren Sie die Kästchen für die Computer, die Sie verschieben möchten.
   b. Verschieben Sie Ihre Auswahl per Drag und Drop in die gewünschte Gruppe im Bereich links.

4.4. Anlegen und Zuweisen einer Sicherheitsrichtlinie

Nach der Installation kann der Security for Endpoints-Schutz über die Control Center mit Hilfe von Sicherheitsrichtlinien konfiguriert und verwaltet werden. Eine Richtlinie legt die Sicherheitseinstellungen fest, die auf die Ziel-Computer angewendet werden sollen.

Direkt nach der Installation wird den Computern die Standardrichtlinie zugewiesen, die mit den empfohlenen Schutzeinstellungen vorkonfiguriert ist. Öffnen Sie die **Richtlinien**übersicht und klicken Sie auf den Namen der Standardrichtlinie, um die Standardschutzeinstellungen anzuzeigen. Sie können die Sicherheitseinstellungen nach Belieben ändern und/oder zusätzliche Sicherheitsfunktionen konfigurieren, indem Sie benutzerdefinierte Richtlinien erstellen und zuweisen.

Beachten Sie

Die Standardrichtlinie können sie weder ändern noch löschen. Sie können Sie nur als Vorlage zur Erstellung neuer Richtlinien verwenden.

Sie können je nach Sicherheitsanforderungen beliebig viele Richtlinien erstellen. Sie können zum Beispiel unterschiedliche Richtlinien für Arbeitsplatzrechner, Laptops und Server konfigurieren. Sie können aber auch unterschiedliche Richtlinien für die einzelnen Kundennetzwerke erstellen.

Was Sie über Richtlinien wissen sollten:

- Richtlinien werden in der **Richtlinien**übersicht erstellt und in der **Netzwerk**übersicht den Endpunkten zugewiesen.
- Endpunkte können jeweils nur eine aktive Richtlinie haben.
- Richtlinien werden sofort, nachdem sie angelegt oder verändert wurden, per Push an die Ziel-Computer übertragen. Die Einstellungen sollten in weniger als einer Minute auf den Endpunkten übernommen werden (vorausgesetzt, dass sie online sind). Wenn ein Computer offline ist, werden die Einstellungen übernommen, sobald er wieder online ist.
- Die Richtlinie bezieht sich nur auf die installierten Schutzmodule. Bitte beachten Sie, dass für Server-Betriebssysteme nur der Malware-Schutz verfügbar ist.
- Sie können Richtlinien, die von anderen Benutzern erstellt wurden, nicht bearbeiten (es sei denn, der Ersteller der entsprechenden Richtlinie lässt dies in den Richtlinieneinstellungen zu), Sie können sie jedoch außer Kraft setzen, indem Sie den Zielobjekten eine andere Richtlinie zuweisen.
- Die Computer unter einem Unternehmenskonto können mithilfe von Richtlinien sowohl von dem Unternehmensadministrator als auch von dem Partner verwaltet werden, der das Konto angelegt hat. Richtlinien, die über das Partnerkonto erstellt wurden, können nicht über das Unternehmenskonto verwaltet werden.

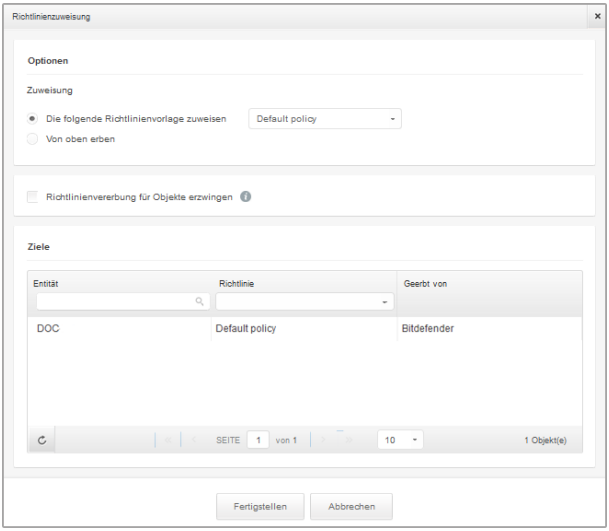
Um eine neue Richtlinie anzulegen:

1. Gehen Sie zur **Richtlinien**-Seite.
2. Klicken Sie auf die Schaltfläche **+ Hinzufügen** auf der rechten Seite der Tabelle. Hierüber können Sie ausgehend von der Standardrichtlinienvorlage eine neue Richtlinie erstellen.
3. Geben Sie einen eindeutigen Namen für die Richtlinie ein. Wenn Sie einen Namen festlegen, berücksichtigen Sie den Zweck und das Ziel der Richtlinie.
4. Konfigurieren Sie dann die Richtlinieneinstellungen. In den meisten Fällen empfiehlt sich die Nutzung der Standardsicherheitseinstellungen.
5. Klicken Sie auf **Speichern**. Die neue Richtlinie wird in der Tabelle **Richtlinien** angezeigt.

Nachdem Sie alle nötigen Richtlinien erstellt haben, können Sie anfangen, sie Netzwerkobjekten zuzuweisen.

So weisen Sie eine Richtlinie zu:

1. Gehen Sie zur Seite **Netzwerk**.
2. Wählen Sie die Netzwerkentitäten (Endpunkte oder Gruppen) aus, denen Sie die Richtlinie zuweisen wollen. Sie können ein oder mehrere Objekte auswählen, diese müssen jedoch von der selben Ebene sein.
3. Klicken Sie auf die Schaltfläche **Richtlinie zuweisen** auf der rechten Seite der Tabelle. Das Fenster **Richtlinienzuweisung** wird angezeigt:



Einstellungen für die Richtlinienzuweisung

Beachten Sie

Die Schaltfläche **Richtlinie** ist ausgegraut, wenn Sie ein nicht verwaltetes Netzwerkobjekt direkt ausgewählt haben (das gilt nicht für Gruppen).

4. Konfigurieren Sie die Einstellungen für die Richtlinienzuweisung für die ausgewählten Objekte:
   - Die aktuellen Richtlinienzuweisungen für die ausgewählten Objekte können Sie in der Tabelle im Bereich **Ziele** einsehen.
   - **Die folgende Richtlinienvorlage zuweisen**. Wählen Sie diese Option aus, um den Zielobjekten eine Richtlinie aus dem rechts angezeigten Menü zuzuweisen. In diesem Menü finden Sie nur die Richtlinien, die über Ihr Benutzerkonto angelegt wurden.
   - **Von oben erben**. Wählen Sie die Option **Von oben erben** aus, um den ausgewählten Netzwerkobjekten die Richtlinie der übergeordneten Gruppe zuzuweisen.

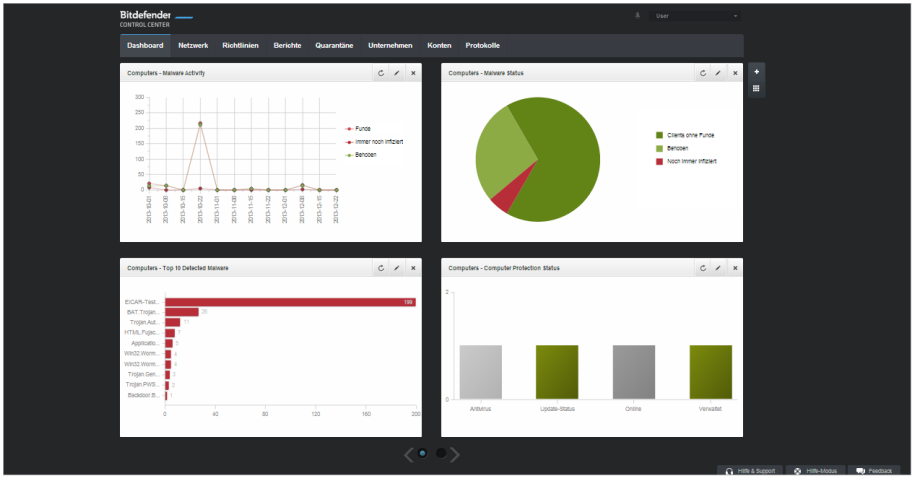
- **Richtlinienvererbung für Objekte erzwingen**. Standardmäßig erbt jedes Netzwerkobjekt die Richtlinie der übergeordneten Gruppe. Von Änderungen der Gruppenrichtlinie sind auch alle untergeordneten Objekte dieser Gruppe davon betroffen. Dies gilt jedoch nicht für Gruppenmitglieder, denen ausdrücklich eine andere Richtlinie zugewiesen wurde.

  Wählen Sie die Option **Richtlinienvererbung für Objekte erzwingen** aus, um die ausgewählte Richtlinie auf eine Gruppe anzuwenden, und dabei auch alle untergeordneten Gruppenobjekte zu berücksichtigen, denen eine abweichende Richtlinie zugewiesen wurde. In diesem Fall zeigt die Tabelle darunter alle untergeordneten Objekte der ausgewählten Gruppe an, die die Gruppenrichtlinie nicht erben.

5. Klicken Sie auf **Fertigstellen**, um die Änderungen zu speichern und zu übernehmen.

5. Überwachen des Sicherheitsstatus

Das Control Center-Dashboard ist das wichtigste Überwachungsinstrument in Security for Endpoints. Dabei handelt es sich um eine individuell anpassbare Anzeige, die Ihnen einen schnellen Überblick über die Sicherheitslage in Ihrem Netzwerk verschafft.



Das Dashboard

Rufen Sie die **Dashboard**-Seite regelmäßig auf, um Echtzeitinformationen über den Sicherheitsstatus des Netzwerks zu erhalten.

In den Dashboard-Portlets werden verschiedenste Sicherheitsinformationen in übersichtlichen Diagrammen angezeigt. Sie bieten einen schnellen Überblick über Bereiche, die Ihre Aufmerksamkeit erfordern.

Mit den folgenden Punkten zur Verwaltung Ihres Dashboards sollten Sie vertraut sein:

- Die Control Center verfügt über verschiedene vordefinierte Dashboard-Portlets. Sie können weitere Portlets über die **Portlet hinzufügen**-Schaltfläche auf der rechten Seite des Dashboards hinzufügen.
- Jedes Dashboard-Portlet enthält im Hintergrund einen detaillierten Bericht, der mit einem einfachen Klick auf das Diagramm abgerufen werden kann.
- Die von den Portlets angezeigten Informationen beziehen sich ausschließlich auf die Netzwerkobjekte, die zu Ihrem Benutzerkonto gehören. Sie können die im Portlet

angezeigten Informationen (Typ, Berichtsintervall, Ziele) individuell anpassen, indem Sie auf das **Portlet bearbeiten**-Symbol in der jeweiligen Titelleiste klicken.

So können Sie die Portlets zum Beispiel so konfigurieren, dass Sie Informationen zu einem bestimmten Unternehmen in Ihrem Netzwerk anzeigen.

- Sie können ein Portlet ganz einfach entfernen, indem Sie in seiner Titelleiste auf das Symbol **Entfernen** klicken. Wenn Sie ein Portlet einmal entfernt haben, können Sie es nicht wiederherstellen. Sie können aber ein neues Portlet mit genau denselben Einstellungen erstellen.
- Klicken Sie auf die einzelnen Einträge in der Diagrammlegende, um die entsprechende Variable, falls verfügbar, auf dem Graphen anzuzeigen bzw. auszublenden.
- Sie können Dashboard-Portlets gemäß Ihrer Anforderungen neu anordnen, indem Sie auf die **Portlets neu anordnen**-Schaltfläche auf der rechten Seite des Dashboards klicken. Danach können Sie die Portlets auf die gewünschte Position ziehen.
- Die Portlets werden in Vierergruppen angezeigt. Verwenden Sie den Schieberegler unten auf der Seite, um zwischen den Portlet-Gruppen umzuschalten.

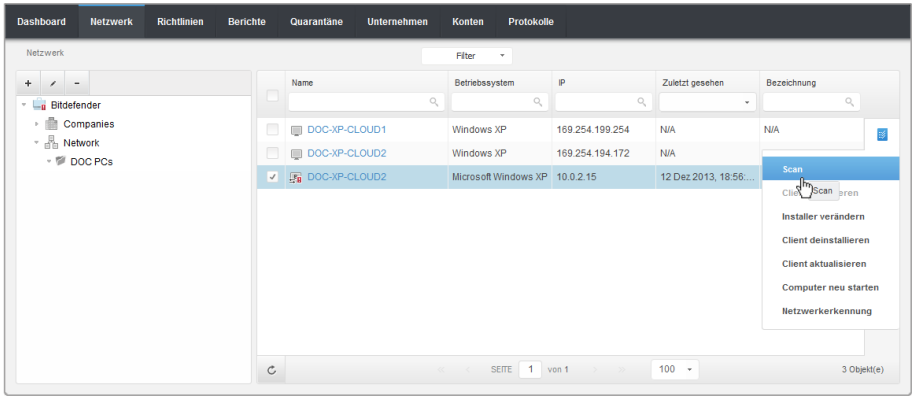
6. Scannen von verwalteten Computern

Es gibt drei Möglichkeiten, Computer zu scannen, die durch Endpoint Security geschützt sind:

- Der am Computer angemeldete Benutzer kann einen Scan über die Endpoint Security-Benutzeroberfläche starten.
- Sie können mithilfe der Richtlinie Scan-Aufgaben einplanen.
- Führen Sie eine Sofort-Scan-Aufgabe über die Konsole aus.

Um eine Scan-Aufgabe per Fernzugriff auf einem oder mehreren Computern auszuführen:

1. Gehen Sie zur Seite **Netzwerk**.
2. Wählen Sie die gewünschte Netzwerkgruppe aus dem linken Fenster aus. Alle Computer der ausgewählten Gruppe werden in der Tabelle im rechten Fenster angezeigt.
3. Wählen Sie die Entitäten aus, die Sie scannen möchten. Sie können einzelne verwaltete Computer oder auch eine ganze Gruppe auswählen.
4. Klicken Sie auf die Schaltfläche **Aufgabe** auf der rechten Seite der Tabelle, und wählen Sie **Scan**. Ein Konfigurationsfenster wird sich öffnen.



Computer-Scan-Aufgabe

5. Wählen Sie im Reiter **Allgemein** den Scan-Typ im Menü **Typ** aus.
   - Der **Quick Scan** sucht nach aktiver Malware im System, ohne dabei entsprechende Aktionen auszuführen. Wenn während eines Quick Scan Malware gefunden wird, müssen Sie eine Vollständiger-Scan-Aufgabe ausführen, um die gefundene Malware zu entfernen

- Der **Vollständige Scan** durchsucht den gesamten Computer nach allen Typen von Malware, die ein Sicherheitsrisiko darstellen, so z. B. Viren, Spyware, Adware, Rootkits usw.
- **Benutzerdefinierter Scan** Hierbei können Sie die Bereiche, die gescannt werden sollen, selbst auswählen und die Scan-Optionen festlegen.

6. Klicken Sie auf **Speichern**, um die Scan-Aufgabe zu erstellen.Eine Bestätigungsmeldung wird angezeigt.

Beachten Sie
Die Scan-Aufgabe startet sofort nach Erstellung auf Computern, die online sind. Wenn ein Computer offline ist, wird dieser gescannt, sobald er wieder online ist.

7. Auf der Seite **Netzwerk > Aufgaben** können Sie Aufgaben anzeigen und verwalten.

7. Hilfe erhalten

Für weitere Informationen oder Hilfe direkt von Bitdefender:

- Klicken Sie in der unteren rechten Bildschirmecke der Control Center auf **Hilfe und Support**.
- Besuchen Sie unser Online-Support-Center.

Um ein Support Ticket zu eröffnen, bitte füllen Sie dieses Web Formular aus.

A. Anforderungen

A.1. Anforderungen für Security for Endpoints

A.1.1. Unterstützte Betriebssysteme

Security for Endpoints bietet derzeit Sicherheit für die folgenden Betriebssysteme:

Betriebssysteme Arbeitsplatzrechner:

- Windows 8.1
- Windows 8
- Windows 7
- Windows Vista mit Service Pack 1
- Windows XP mit Service Pack 3
- Mac OS X Lion (10.7.x)
- Mac OS X Mountain Lion (10.8.x)
- Mac OS X Mavericks (10.9.x)

Tablets und eingebettete Betriebssysteme*:

- Windows Embedded Standard 7
- Windows Embedded Compact 7
- Windows Embedded POSReady 7
- Windows Embedded Enterprise 7
- Windows Embedded POSReady 2009
- Windows Embedded Standard 2009
- Windows XP Embedded mit Service Pack 2
- Windows XP Tablet PC Edition

*Bestimmte Betriebssystemmodule müssen für die Funktionalität von Security for Endpoints installiert werden.

Betriebssysteme Server:

- Windows Server 2012 R2
- Windows Server 2012
- Windows Small Business Server (SBS) 2011
- Windows Small Business Server (SBS) 2008
- Windows Server 2008 R2
- Windows Server 2008
- Windows Small Business Server (SBS) 2003
- Windows Server 2003 R2
- Windows Server 2003 SP1

- Windows Home Server

A.1.2. Hardware-Anforderungen

- Mit Intel® Pentium kompatibler Prozessor:

  Betriebssysteme Arbeitsplatzrechner
  - 1 GHz oder schneller bei Microsoft Windows XP SP3, Windows XP SP2 64 Bit und Windows 7 Enterprise (32 und 64 Bit)
  - 2 GHz oder schneller bei Microsoft Windows Vista SP1 oder neuer (32 und 64 Bit), Microsoft Windows 7 (32 und 64 Bit), Microsoft Windows 7 SP1 (32 und 64 Bit), Windows 8
  - 800 MHZ oder schneller bei Microsoft Windows Embedded Standard 7 SP1, Microsoft Windows POSReady 7, Microsoft Windows POSReady 2009, Microsoft Windows Embedded Standard 2009, Microsoft Windows XP Embedded mit Service Pack 2, Microsoft Windows XP Tablet PC Edition

  Betriebssysteme Server
  - Minimum: 2,4 GHz Single-Core-CPU
  - Empfohlen: 1,86 GHz oder schnellere Intel Xeon Multi-Core-CPU
- **Freier RAM**:
  - Für Windows: Mindestens 512 MB, 1 GB empfohlen
  - Für Mac: Mindestens 1 GB
- **Speicherplatz (Festplatte)**:
  - 1.5 GB freier Speicherplatz

Beachten Sie
Für Entitäten mit Endpoint Security Relay-Rolle werden mindestens 6 GB freier Festplattenspeicher benötigt, da dort alle Updates und Installationspakete gespeichert sind.

A.1.3. Unterstützte Web-Browser

Security for Endpoints funktioniert mit folgenden Browsern:

- Internet Explorer 8+
- Mozilla Firefox 8+
- Google Chrome 15+
- Safari 4+

A.2. Wie die Netzwerkerkennung funktioniert

Security for Endpoints verfügt über einen automatischen Netzwerkerkennungsmechanismus zur Erkennung von Arbeitsgruppen-Computern.

Security for Endpoints nutzt den **Microsoft-Computersuchdienst** für die Netzwerkerkennung. Der Computersuchdienst ist eine Netzwerktechnologie, die auf Windows-basierten Computern zum Einsatz kommt, um immer aktuelle Listen von Domänen, Arbeitsgruppen und den Computern darin zu verwalten und diese Listen bei Bedarf an Client-Computer weiterzugeben. Computer, die über den Computersuchdienst im Netzwerk erkannt wurden, können durch Eingabe des **Net View**-Befehls im Eingabeaufforderungsfenster angezeigt werden.

Der Net-View-Befehl

Damit die Netzwerkerkennung funktioniert, müssen Sie Endpoint Security bereits auf mindestens einem Computer im Netzwerk installiert haben. Von diesem Computer aus wird das Netzwerk gescannt.

Wichtig

Control Center bezieht keine Netzwerkinformationen über Active Directory oder über die Netzwerkübersichtsfunktion in Windows Vista und höher.Die Netzwerkübersicht nutzt eine andere Technologie zur Netzwerkerkennung: das Link-Layer-Topology-Discovery-Protokoll (LLTD).

Control Center übernimmt keine aktive Rolle bei der Ausführung des Computersuchdienstes. Endpoint Security fragt beim Computersuchdienst lediglich die Liste der aktuell im Netzwerk sichtbaren Arbeitsstationen und Server ab (die Suchliste) und leitet diese dann an die Control Center weiter.Die Control Center verarbeitet die Suchliste und fügt neu erkannte Computer zur der Liste der **nicht verwalteten Computer** hinzu.Bereits erkannte Computer werden nach einer Netzwerkerkennungsabfrage nicht gelöscht, daher müssen Computer, die sich nicht mehr länger im Netzwerk befinden, manuell ausgeschlossen und gelöscht werden.

Die erste Abfrage nach der Suchliste wird vom ersten im Netzwerk installierten Endpoint Security durchgeführt.

- Falls Endpoint Security auf einem Arbeitsgruppen-Computer installiert wurde, werden in der Control Center nur die Computer dieser Arbeitsgruppe angezeigt.
- Falls Endpoint Security auf einem Domänen-Computer installiert wurde, werden in der Control Center nur die Computer dieser Domäne angezeigt.Computer aus anderen Domänen können erkannt werden, wenn eine Vertrauensstellung mit der Domäne besteht, in der Endpoint Security installiert ist.

Nachfolgende Netzwerkerkennungsabfragen werden danach stündlich wiederholt. Bei jeder neuen Abfrage teilt die Control Center die verwalteten Computer in Sichtbarkeitsbereiche auf und bestimmt in jedem Bereich einen Endpoint Security zur Durchführung der Aufgabe.Ein Sichtbarkeitsbereich ist eine Gruppe von Computern, die sich gegenseitig erkennen. Normalerweise wird ein Sichtbarkeitsbereich anhand einer Arbeitsgruppe oder Domäne definiert, im Einzelfall hängt dies jedoch von der Netzwerktopologie und Konfiguration ab. Unter Umständen besteht ein Sichtbarkeitsbereich auch aus mehreren Domänen oder Arbeitsgruppen.

Falls ein ausgewählter Endpoint Security die Abfrage nicht durchführt, wartet die Control Center auf die nächste geplante Abfrage, ohne einen anderen Endpoint Security für einen weiteren Versuch auszuwählen.

Um das gesamte Netzwerk sichtbar zu machen, muss Endpoint Security auf mindestens einem Computer in jeder Arbeitsgruppe oder Domäne in Ihrem Netzwerk installiert sein. Im Idealfall sollte Endpoint Security auf mindestens einem Computer in jedem Subnetzwerk installiert sein.

A.2.1. Weitere Informationen zum Microsoft-Computersuchdienst

Der Computersuchdienst auf einen Blick:

- Funktioniert unabhängig von Active Directory.
- Läuft ausschließlich über IPv4-Netzwerken und funktioniert unabhängig innerhalb der Grenzen einer LAN-Gruppe (Arbeitsgruppe oder Domäne).Eine Suchliste wird für jede LAN-Gruppe erstellt und verwaltet.
- Nutzt für die Kommunikation zwischen den Knoten üblicherweise verbindungslose Server-Übertragungen.
- Nutzt NetBIOS über TCP/IP (NetBT).
- Benötigt NetBIOS-Namensauflösung. Es wird empfohlen im Netzwerk eine Windows-Internet-Name-Service-Infrastruktur (WINS) zu unterhalten.
- Ist standardmäßig nicht in Windows Server 2008 und 2008 R2 aktiviert.

Weitere Informationen zum Computersuchdienst finden Sie in der Computer Browser Service Technical Reference im Microsoft Technet.

A.2.2. Anforderungen für Netzwerkerkennung

Um alle Computer (Server und Arbeitsplatzrechner) erfolgreich zu erkennen, die über das Control Center verwaltet werden sollen, ist Folgendes erforderlich:

- Die Computer müssen in einer Arbeitsgruppe oder Domäne zusammengefasst und über ein lokales IPv4-Netzwerk verbunden sein.Der Computersuchdienst funktioniert nicht über IPv6-Netzwerke.
- In jeder LAN-Gruppe (Arbeitsgruppe oder Domäne) müssen mehrere Computer den Computersuchdienst ausführen. Auch die primären Domänencontroller müssen den Dienst ausführen.
- NetBIOS über TCP/IP (NetBT) muss auf den Computern aktiviert sein.Die lokale Firewall muss NetBT-Verkehr zulassen.
- Die Freigabe von Dateien muss auf den Computern aktiviert sein.Die lokale Firewall muss die Freigabe von Dateien zulassen.
- Eine Windows-Internet-Name-Service-Infrastruktur (WINS) muss eingerichtet und funktionsfähig sein.
- Für Windows Vista und höher muss die Netzwerkerkennung aktiviert werden (**Systemsteuerung > Netzwerk- und Freigabecenter > Erweiterte Freigabeeinstellungen ändern**).

  Um diese Funktion aktivieren zu können, müssen zunächst die folgenden Dienste gestartet werden:
  - DNS-Client
  - Funktionssuche-Ressourcenveröffentlichung
  - SSDP-Suche
  - UPnP-Gerätehost
- In Umgebungen mit mehreren Domänen empfiehlt es sich, Vertrauensstellungen zwischen den Domänen einzurichten, damit die Computer auch auf Suchlisten aus anderen Domänen zugreifen können.

Computer, über die Endpoint Security den Computersuchdienst abfragt, müssen in der Lage sein, NetBIOS-Namen aufzulösen.

Beachten Sie

Der Mechanismus zur Netzwerkerkennung funktioniert auf allen unterstützten Betriebssystemen, einschließlich der Windows-Embedded-Versionen, vorausgesetzt, dass alle Anforderungen erfüllt werden.