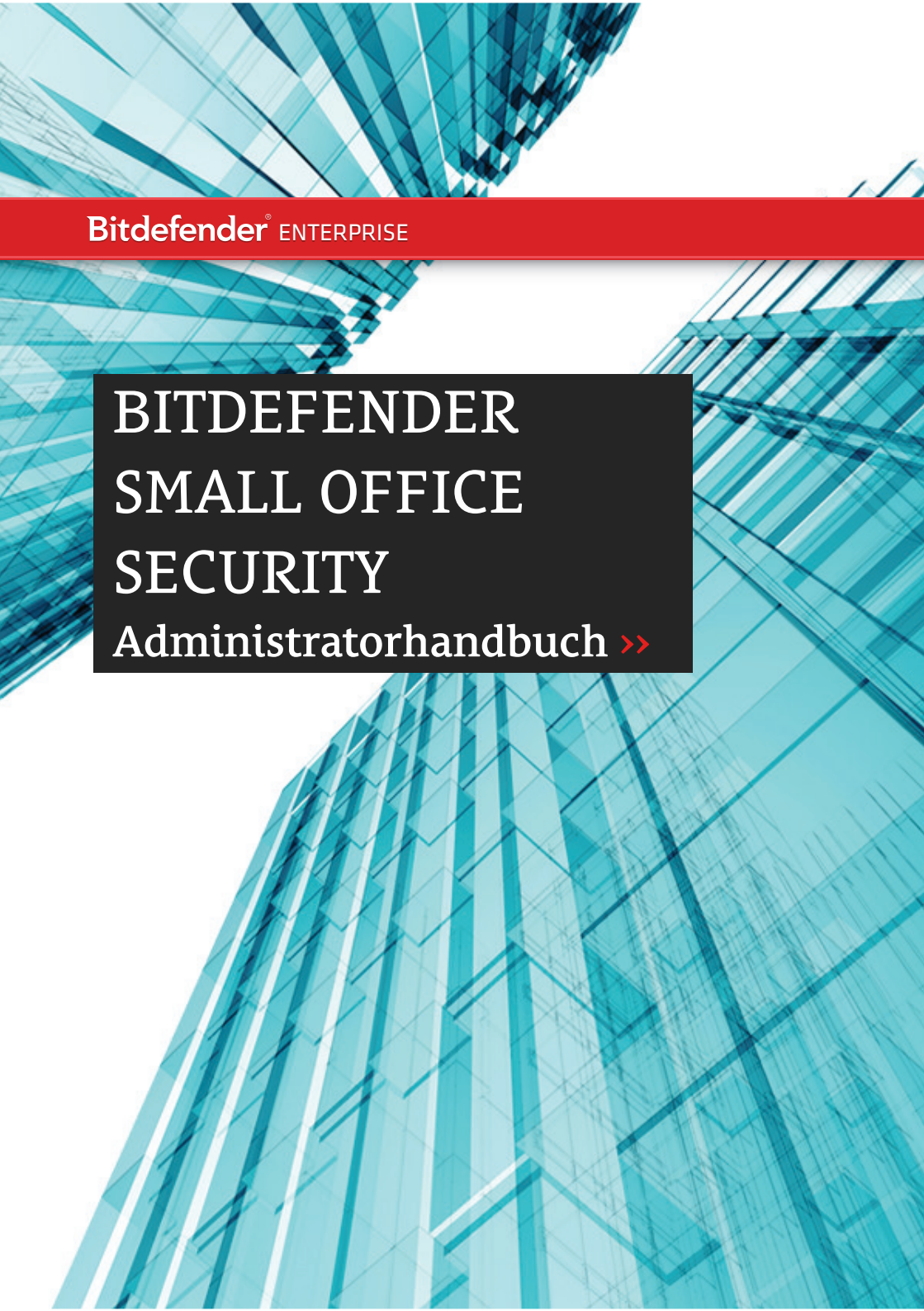

Bitdefender ENTERPRISE
BITDEFENDER
SMALL OFFICE
SECURITY
Administratorhandbuch ››

Bitdefender Small Office Security
Administratorhandbuch

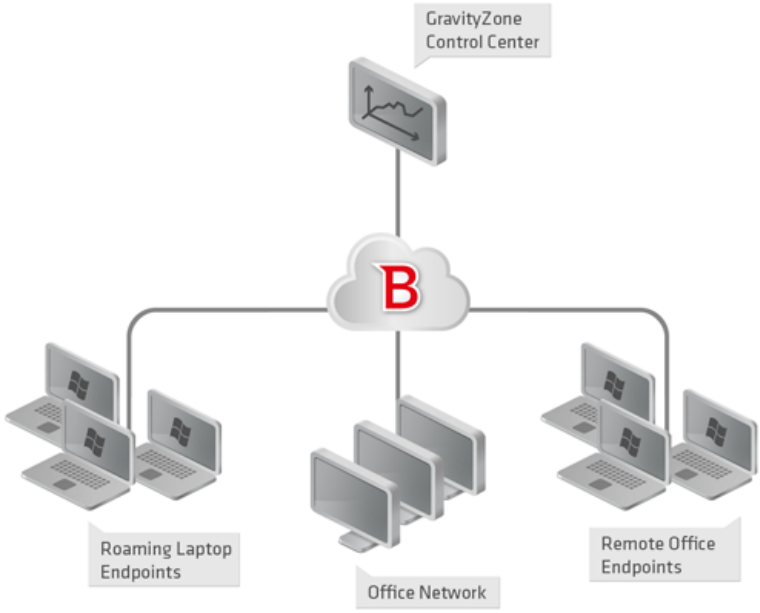
Veröffentlicht 2014.02.28


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

Die Small Office Security-Funktionen können über eine zentrale Verwaltungsplattform namens Control Center konfiguriert und verwaltet werden. Control Center hat eine Web-basierte Oberfläche, auf die Sie mit einem Benutzernamen und einem Passwort zugreifen können.

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.

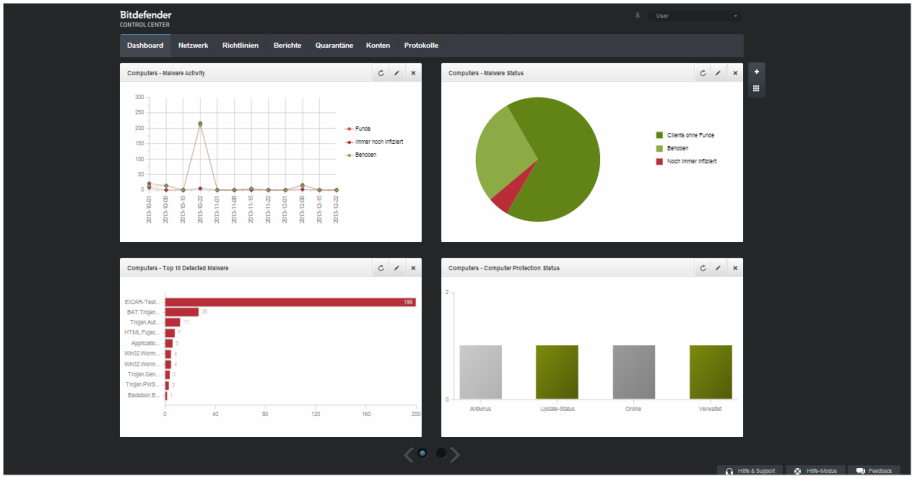
So stellen Sie eine Verbindung zum Control Center her:

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:

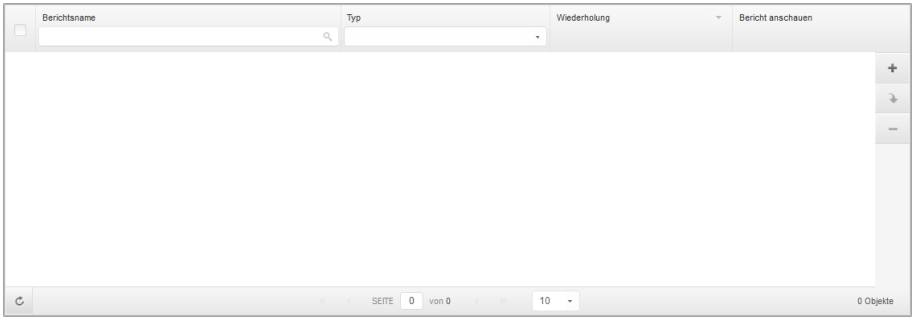
- **Mein Konto**. Klicken Sie auf diese Option, um Ihre Benutzerkontoinformationen und -einstellungen zu bearbeiten.
- **Mein Unternehmen**. Klicken Sie auf diese Option, um Ihre Unternehmenskontoinformationen und -einstellungen zu verwalten.
- **Zugangsdaten-Manager**. Klicken Sie auf diese Option, 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.



Die Berichtsübersicht - Berichtstabelle

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

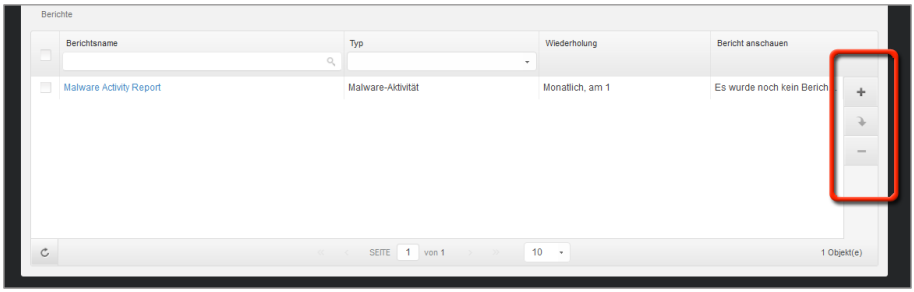
Um sicherzustellen, dass die aktuellsten Informationen angezeigt werden, klicken Sie im unteren linken Bereich der Tabelle auf **Aktualisieren**.

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:

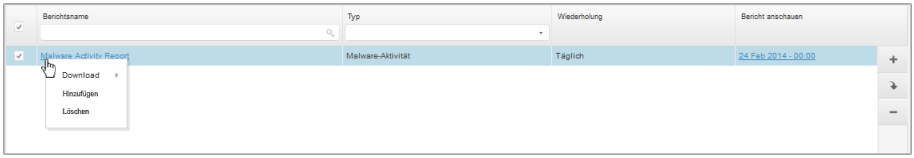
- Neuen Bericht erstellen.
- Geplant erstellte Berichte herunterladen.
- Einen geplanten Bericht löschen.



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.

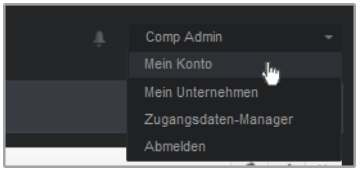


Die Berichtsübersicht - Kontextmenü

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:

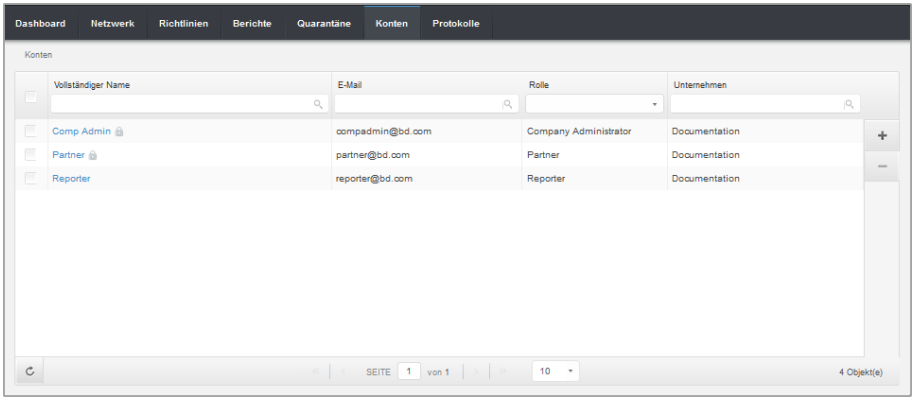
1. Melden Sie mit Ihrer E-Mail-Adresse und dem per E-Mail zugesandten Passwort an der Control Center an.
2. Bewegen Sie den Mauszeiger auf Ihr Benutzerkonto in der rechten oberen Ecke der Konsole, und wählen Sie **Mein Unternehmen**.
3. Details zu Ihrer aktuellen Lizenz finden Sie im Bereich **Lizenz**. 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. Benutzerkonten verwalten

Der Security for Endpoints-Dienst kann über die Control Center mit dem Konto eingerichtet und verwaltet werden, das Ihnen nach der Anmeldung für den Dienst zugewiesen wurde.

Mit den folgenden Punkten zu den Small Office Security-Benutzerkonten sollten Sie vertraut sein:

- Sie können interne Benutzerkonten anlegen, um anderen Mitarbeitern im Unternehmen Zugriff auf die Control Center zu ermöglichen. Sie können Benutzerkonten verschiedene Rollen mit unterschiedlichen Zugriffsrechten zuweisen.
- Für jedes Benutzerkonto können Sie den Zugriff auf Small Office Security-Funktionen oder bestimmte Teile des Netzwerks, zu dem es gehört, festlegen.
- Alle Konten mit der Berechtigung **Benutzer verwalten** können andere Konten erstellen, bearbeiten und löschen.
- Sie können ausschließlich Konten verwalten, die die gleichen oder weniger Rechte wie Ihr eigenes Konto haben.
- Auf der Seite **Konten** können Sie Benutzerkonten erstellen und verwalten.



Die Kontenübersicht

Bestehende Konten werden in der Tabelle angezeigt. Sie können das Folgende für jedes Benutzerkonto einsehen:

– Der Benutzername des Kontos (wird zur Anmeldung an der Control Center verwendet).

- E-Mail-Adresse des Kontos (wird als Kontaktadresse verwendet). An diese Adresse werden Berichte und wichtige Sicherheitsbenachrichtigungen geschickt. Es werden automatisch E-Mail-Benachrichtigungen versandt, sobald wichtige Risikobedingungen im Netzwerk erkannt werden.
- Benutzerrolle (Partner / Unternehmensadministrator / Administrator / Berichterstatter / benutzerdefiniert)

4.1. Benutzerrollen

Eine Benutzerrolle umfasst eine bestimmte Kombination aus Benutzerrechten. Wenn Sie ein Benutzerkonto anlegen, können Sie eine der vordefinierten Rollen wählen oder eine benutzerdefinierte Rolle erstellen, indem Sie nur die gewünschten Benutzerrechte auswählen.

Beachten Sie
Sie können anderen Benutzerkonten nur die Rechte zuweisen, über die Sie selbst verfügen.

Die folgenden Benutzerrollen sind verfügbar:

1. **Unternehmensadministrator** - Geeignet für Manager von Kundenunternehmen, die eine Small Office Security-Lizenz von einem Partner erworben haben. Ein Unternehmensadministrator verwaltet die Lizenz, das Unternehmensprofil und die gesamte Small Office Security-Installation. Er erhält somit umfassende Kontrolle über alle Sicherheitseinstellungen (es sei denn, dies wurde im Rahmen eines Dienstleisterszenarios von dem übergeordneten Partnerkonto außer Kraft gesetzt). Unternehmensadministratoren können ihre Aufgaben mit untergeordneten Administrator- und Berichterstatterkonten teilen oder diese an sie delegieren.
2. **Administrator** - Für ein Unternehmen können mehrere Benutzerkonten mit der Administrator-Rolle angelegt werden. Diese verfügen über Administratorrechte für alle Security for Endpoints-Installationen im Unternehmen bzw. für eine festgelegte Gruppe von Computern, einschließlich der Benutzerverwaltung. Administratoren sind zuständig für die aktive Verwaltung der Sicherheitseinstellungen im Netzwerk.
3. **Berichterstatter** - Berichterstatterkonten sind interne Konten, die ausschließlich über Lesezugriff verfügen. Über sie erhält man nur Zugriff auf Berichte und Protokolle. Diese Benutzerkonten können Mitarbeitern bereitgestellt werden, die Überwachungsaufgaben wahrnehmen oder über die Sicherheitslage auf dem Laufenden gehalten werden müssen.
4. **Benutzerdefiniert** - Vordefinierte Benutzerrollen beinhalten eine bestimmte Kombination aus Berechtigungen. Sollte eine vordefinierte Benutzerrolle Ihren Anforderungen nicht entsprechen, können Sie ein benutzerdefiniertes Konto mit genau den Rechten anlegen, die Sie benötigen.

Die nachfolgende Tabelle gibt einen Überblick über die Zusammenhänge zwischen den verschiedenen Rollen und ihren Berechtigungen. Detaillierte Informationen finden Sie unter „Benutzerrechte“ (S. 13).

Rolle des Kontos	Zugelassene untergeordnete Konten	Benutzerrechte
Unternehmensadministrator	Unternehmensadministratoren, Administratoren, Berichterstatter	Unternehmen verwalten Benutzer verwalten Netzwerke verwalten Berichte verwalten
Administrator	Administratoren, Berichterstatter	Benutzer verwalten Netzwerke verwalten Berichte verwalten
Berichterstatter	-	Berichte verwalten

4.2. Benutzerrechte

Sie können den Small Office Security-Benutzerkonten die folgenden Benutzerrechte zuweisen:

- **Benutzer verwalten**. Benutzerkonten erstellen, bearbeiten oder löschen.
- **Unternehmen verwalten**. Benutzer können ihren eigenen Small Office Security-Lizenzschlüssel verwalten und die Einstellungen für ihr Unternehmensprofil bearbeiten. Dieses Recht haben nur Unternehmensadministratoren.
- **Netzwerke verwalten**. Gewährt Administrationsrechte über die Netzwerksicherheitseinstellungen (Netzwerkinventar, Richtlinien, Aufgaben, Installationspakete, Quarantäne). Dieses Recht haben nur Administratoren.
- **Berichte verwalten**. Berichte anlegen, bearbeiten, löschen und das Dashboard verwalten.

4.3. Benutzerkonten erstellen

Bevor Sie ein Benutzerkonto anlegen, sollten Sie sicherstellen, dass Sie die benötigte E-Mail-Adresse zur Hand haben. Diese Adresse wird zwingend für das Anlegen des Small Office Security-Benutzerkontos benötigt. Den Benutzern werden ihre Small Office Security-Zugangsdaten an die angegebene E-Mail-Adresse gesendet. Benutzer werden die E-Mail-Adresse auch für die Small Office Security-Anmeldung verwenden.

Um ein Benutzerkonto anzulegen:

1. Rufen Sie die Seite **Konten** auf.

2. Klicken Sie auf die Schaltfläche + **Hinzufügen** auf der rechten Seite der Tabelle. Ein Konfigurationsfenster wird geöffnet.
3. Geben Sie im Bereich **Details** die Benutzerkontoinformationen ein.
   - **E-Mail**. Geben Sie die E-Mail-Adresse des Benutzers ein. Die Anmeldeinformationen werden an diese E-Mail-Adresse versandt, sobald das Konto angelegt wurde.

     Beachten Sie
     Die E-Mail-Adresse darf nur einmal vergeben werden. Sie können keine weiteren Benutzerkonten mit der gleichen E-Mail-Adresse anlegen.

   - **Vollständiger Name**. Geben Sie den vollständigen Namen des Kontoinhabers ein.
4. Konfigurieren Sie im Bereich **Einstellungen und Rechte** die folgenden Einstellungen:
   - **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.
   - **Rolle**. Wählen Sie die Rolle des Benutzers aus. Weitere Details zu Benutzerrollen finden Sie unter „Benutzerrollen“ (S. 12).
   - **Rechte**. Jede vordefinierte Benutzerrolle verfügt über einen bestimmten Satz von Rechten. Sie können dabei aber genau die Rechte auswählen, die Sie benötigen. Die Benutzerrolle wechselt dann zu **Benutzerdefiniert**. Weitere Informationen zu den Benutzerrechten finden Sie unter „Benutzerrechte“ (S. 13).
   - **Ziele wählen**. Scrollen Sie im Konfigurationsbereich nach unten, um den Ziele-Bereich anzuzeigen. Wählen Sie die Netzwerkgruppen aus, auf die der Benutzer Zugriff haben wird. Sie können den Benutzerzugriff auf bestimmte Netzwerkbereiche beschränken.
5. Klicken Sie auf **Speichern**, um den Benutzer hinzuzufügen. Das neue Konto erscheint in der Liste der Benutzerkonten.

Beachten Sie
Das Passwort für jedes Benutzerkonto wird automatisch nach Anlegen des Kontos vergeben und gemeinsam mit den anderen Kontodaten an die E-Mail-Adresse des Benutzers gesendet.
Sie können das Passwort nach Anlegen des Kontos ändern. Klicken Sie in der **Konten**-Übersicht auf den Kontonamen, um das Passwort zu bearbeiten. Benutzer werden per E-Mail umgehend über die Änderung des Passworts informiert.
Benutzer können ihr Anmeldepasswort über die Control Center ändern, indem Sie die Seite **Mein Konto** aufrufen.

4.4. Konten bearbeiten

Bearbeiten Sie Konten, um die Kontoinformationen auf dem neuesten Stand zu halten oder die Kontoeinstellungen anzupassen.

Um ein Benutzerkonto zu bearbeiten:

1. Melden Sie sich an der Control Center an.
2. Rufen Sie die Seite **Konten** auf.
3. Klicken Sie auf den Benutzernamen.
4. Ändern Sie die Kontoinformationen und -einstellungen nach Bedarf.
5. Klicken Sie auf **Speichern**, um die Änderungen zu speichern.

Beachten Sie
Alle Konten mit der Berechtigung **Benutzer verwalten** können andere Konten erstellen, bearbeiten und löschen. Sie können ausschließlich Konten verwalten, die die gleichen oder weniger Rechte wie Ihr eigenes Konto haben.

4.5. Benutzerkonten löschen

Löschen Sie Konten, wenn diese nicht mehr benötigt werden.So zum Beispiel wenn ein Kontoinhaber das Unternehmen verlassen hat.

Um ein Konto zu löschen:

1. Melden Sie sich an der Control Center an.
2. Rufen Sie die Seite **Konten** auf.
3. Wählen Sie das Konto aus der Liste aus.
4. Klicken Sie auf die Schaltfläche **– Löschen** auf der rechten Seite der Tabelle.

4.6. Anmeldepasswörter zurücksetzen

Kontoinhaber, die ihr Passwort vergessen haben, können es über den Link für die Passwortwiederherstellung auf der Anmeldeseite zurücksetzen.Sie können ein vergessenes Anmeldepasswort auch zurücksetzen, indem Sie das entsprechende Konto über die Konsole bearbeiten.

Um das Anmeldepasswort für einen Benutzer zurückzusetzen:

1. Melden Sie sich an der Control Center an.
2. Rufen Sie die Seite **Konten** auf.
3. Klicken Sie auf den Benutzernamen.
4. Geben Sie in die entsprechenden Felder ein neues Passwort ein (unter **Details**).
5. Klicken Sie auf **Speichern**, um die Änderungen zu speichern.Der Kontoeigentümer erhält dann eine E-Mail mit dem neuen Passwort.

5. Security for Endpoints installieren

Security for Endpoints wurde für Arbeitsplatzrechner, Laptops und Server mit Microsoft® Windows als Betriebssystem entwickelt. Um Ihre physischen 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.

Sie können Endpoint Security auf Computern installieren indem Sie Installationspakete lokal ausführen oder über Control Center Installationsaufgaben aus der Ferne ausführen.

Es ist wichtig, dass Sie die Anleitung sorgfältig lesen und befolgen, um die Installation richtig vorzubereiten.

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. 20).

5.1. Systemanforderungen

5.1.1. 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

5.1.2. 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.

5.1.3. Unterstützte Web-Browser

Security for Endpoints funktioniert mit folgenden Browsern:

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

5.2. 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.

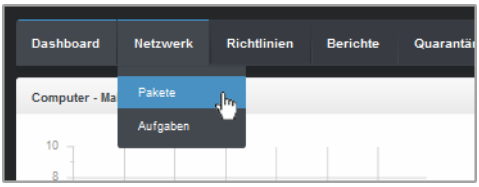
   Wichtig
   Um die Windows-Sicherheitsfunktionen (Windows Defender, Windows Firewall) müssen Sie sich nicht kümmern. Diese werden vor Beginn der Installation automatisch deaktiviert.

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.

5.3. Lokale Installation

Eine Möglichkeit, Endpoint Security auf einem Computer zu installieren ist es, ein Installationspaket lokal auf einem Computer auszuführen.

Auf der Seite **Netzwerk > Pakete** können Sie auf Ihre Bedürfnisse zugeschnittene Installationspakete erstellen und verwalten.



Das Netzwerk- und Pakete-Menü

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.

Nach seiner Installation wird der Computer mit der Endpoint Security Relay-Rolle verwendet, um andere Computer über den Netzwerkerkennungsmechanismus im gleichen Netzwerk zu erkennen. Weitere Informationen zur Netzwerkerkennung finden Sie unter „Wie die Netzwerkerkennung funktioniert“ (S. 27).

Für die lokale Installation von Endpoint Security auf einem Computer gehen Sie folgendermaßen vor:

1. Sie können ein Installationspaket erstellen, das Ihren Anforderungen entspricht.

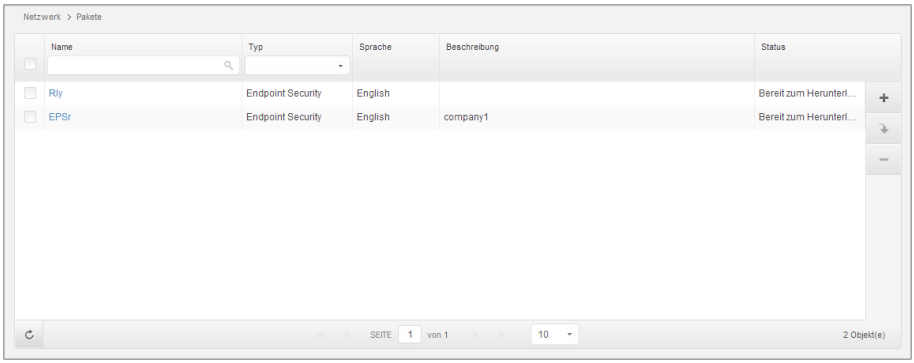
   Beachten Sie
   Dieser Schritt muss nicht durchgeführt werden, falls unter Ihrem Benutzerkonto bereits ein Installationspaket für das Netzwerk erstellt worden ist.

2. Jetzt müssen Sie das Installationspaket herunterladen.
3. Im nächsten Schritt Führen Sie das Installationspaket aus.

5.3.1. Endpoint Security Installationspakete erstellen

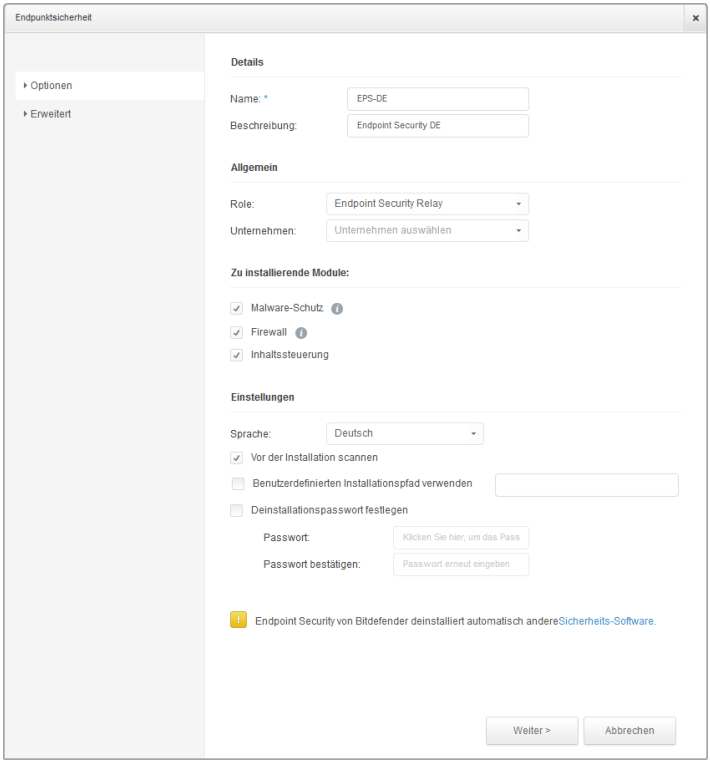
So erstellen Sie ein Installationspaket für Endpoint Security:

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.

5.3.2. Installationspakete herunterladen

So laden Sie Installationspakete für Endpoint Security herunter:

1. Melden Sie sich über den Computer, auf dem Sie den Schutz installieren möchten, an der Control Center an.
2. Gehen Sie zur Seite **Netzwerk > Pakete**.
3. Wählen Sie das Endpoint Security-Installationspaket aus, das Sie herunterladen möchten.
4. 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.

Beachten Sie
Verfügbare Installationspaket-Versionen:

– **Windows OS:** 32-Bit- und 64-Bit-Systeme

– **Mac OS X:** nur 64-Bit-Systeme

Stellen Sie sicher, dass Sie die zum jeweiligen Computer passende Version wählen.

5. Speichern Sie die Datei auf dem Computer.

5.3.3. Installationspakete ausführen

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

1. Stellen Sie eine Verbindung zur Control Center her und melden Sie sich an.
2. Speichern oder kopieren Sie die Installationsdatei auf dem Zielcomputer oder auf einer Netzwerkfreigabe, auf die von dem Computer aus zugegriffen werden kann.
3. Führen Sie das Installationspaket aus.
4. 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).

5.4. 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.

Security for Endpoints verfügt über einen automatischen Netzwerkerkennungsmechanismus, mit dem andere Computer im gleichen Netzwerk gefunden werden können. Gefundene Computer werden als **Nicht verwaltete Computer** in der **Netzwerk**übersicht angezeigt.

Weitere Informationen zur Netzwerkerkennung finden Sie unter „Wie die Netzwerkerkennung funktioniert“ (S. 27).

5.4.1. Anforderungen für die Endpoint Security-Ferninstallation

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.

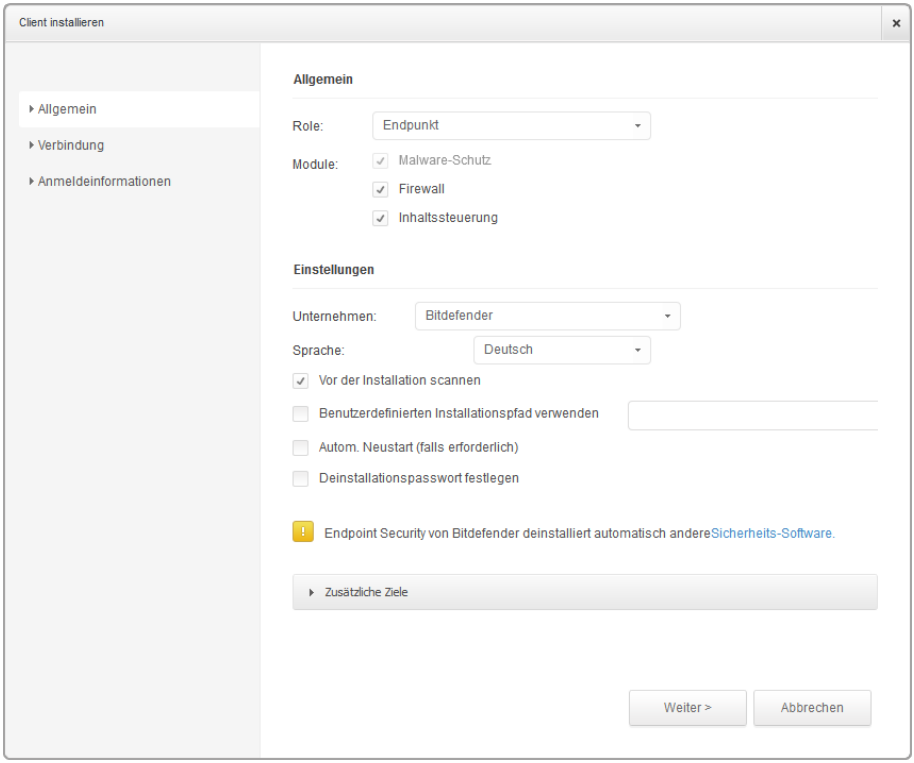
5.4.2. Durchführen von Endpoint Security-Ferninstallationsaufgaben

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.

5.5. 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.

5.5.1. 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.

5.5.2. 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.

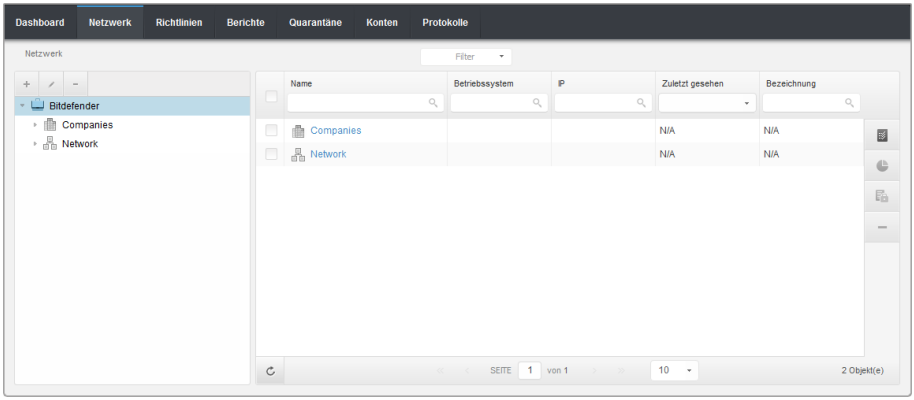
Computer, über die Endpoint Security den Computersuchdienst abfragt, müssen in der Lage sein, NetBIOS-Namen aufzulösen.

Beachten Sie

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

6. Computer verwalten

In der **Netzwerk**übersicht finden sich viele Funktionen zum Durchsuchen und Verwalten der verfügbaren Computer. Die **Netzwerk**ansicht besteht aus einer Oberfläche mit zwei Fenstern, in denen der Status aller Netzwerkobjekte in Echtzeit angezeigt wird.



Die Netzwerk-Übersicht

1. Im linken Fenster wird die verfügbare Netzwerkbaumstruktur angezeigt.

   Beachten Sie
   Sie können nur diejenigen Gruppen verwalten, für die Sie Administratorrechte haben.

2. Im rechten Fenster wird der Inhalt der Gruppe, die Sie im Netzwerkbaum ausgewählt haben, angezeigt.Dieses Fenster besteht aus einem Raster, in dem in jeder Zeile ein Netzwerkobjekt steht und in jeder Spalte bestimmte Informationen zu diesen Objekten.

   In diesem Fenster können Sie Folgendes tun:

   - Detaillierte Informationen zu jedem Netzwerkobjekt in Ihrem Konto einsehen.Der Status jedes Objekts wird durch das Symbol neben seinem Namen angezeigt.Klicken Sie auf den Namen des Objekts, um ein Fenster mit weiteren Informationen anzuzeigen.
   - Über die Symbolleiste auf der rechten Seite der Tabelle können Sie bestimmte Operationen für jedes Netzwerkobjekt ausführen (z. B. Aufgaben ausführen, Berichte erstellen Richtlinien zuweisen und löschen).
   - Tabellendaten aktualisieren.

Im Bereich **Netzwerk** können Sie auch die Installationspakete sowie die Liste der Aufgaben für jeden Netzwerkobjekttyp verwalten.

Um die Computer anzuzeigen, die zu Ihrem Konto gehören, öffnen Sie die **Netzwerk**übersicht und wählen Sie die gewünschte Netzwerkgruppe links auf der Seite aus.

Im linken Fenster sehen Sie das verfügbare Computernetzwerk und im rechten Fenster Details zu jedem Computer.

Im Bereich **Netzwerk** stehen Ihnen folgende Verwaltungsoptionen für Computer zur Verfügung:

- Überprüfen Sie den Status des Computers.
- Computer in Gruppen organisieren.
- Computer-Details anzeigen.
- Computer sortieren, filtern und suchen.
- Aufgaben auf Computern ausführen.
- Schnellberichte erstellen.
- Regeln zuweisen.
- Computer aus dem Netzwerkinventar löschen.

6.1. Überprüfen Sie den Status des Computers

Jeder Computer wird in der Netzwerkübersicht seinem Status entsprechend durch ein Symbol dargestellt. In der folgenden Tabelle finden Sie die verschiedenen Computer-Status und die dazugehörigen Symbole:

Symbol	Status
	Computer, verwaltet, keine Probleme, online
	Computer, verwaltet, mit Sicherheitsproblemen, online
	Computer, verwaltet, keine Probleme, offline
	Computer, verwaltet, mit Sicherheitsproblemen, offline
	Nicht verwaltet
	Gelöscht

Detaillierte Informationen finden Sie unter:

- „Verwaltete, nicht verwaltete und gelöschte Computer“ (S. 33)
- „Computer - online und offline“ (S. 33)
- „Computer mit Sicherheitsproblemen“ (S. 34)

6.1.1. Verwaltete, nicht verwaltete und gelöschte Computer

Computer können verschiedene Verwaltungsstatus haben:

- **Verwaltet** - Computer, auf denen Endpoint Security installiert ist.
- **Nicht verwaltet** - gefundene Computer, auf denen Endpoint Security noch nicht installiert wurde.
- **Gelöscht** - Computer, die Sie aus der Control Center gelöscht haben.Weitere Informationen finden Sie unter „Computer aus dem Netzwerkinventar löschen“ (S. 57).

6.1.2. Computer - online und offline

Der Verbindungsstatus betrifft nur verwaltete Computer.Verwaltete Computer können verschiedene Verbindungsstatus haben:

- **Online**.Ein blaues Symbol zeigt an, dass der Computer online ist.
- **Offline**.Ein graues Symbol zeigt an, dass der Computer offline ist.

Ein Computer ist offline, wenn Endpoint Security für länger als 5 Minuten inaktiv ist.Mögliche Gründe, warum Computer als offline angezeigt werden:

- Der Computer ist ausgeschaltet, im Ruhezustand oder im Energiesparmodus.

  Beachten Sie
  Computer werden normalerweise auch dann als online angezeigt, wenn sie gesperrt sind oder der Benutzer sich abgemeldet hat.

- Endpoint Security hat keine Verbindung zur Bitdefender Control Center oder zum zugewiesenen Endpoint Security Relay:
  - Die Verbindung des Computers zum Netzwerk könnte unterbrochen worden sein.
  - Eine Netzwerk-Firewall oder ein Router können die Kommunikation zwischen Endpoint Security und der Bitdefender Control Center oder dem zugewiesenen Endpoint Security Relay blockieren.
- Endpoint Security wurde manuell deinstalliert, während der Computer nicht mit der Bitdefender Control Center oder dem zugewiesenen Endpoint Security Relay verbunden war. Normalerweise wird die Control Center über die manuelle Deinstallation von Endpoint Security benachrichtigt und der Computer wird als nicht verwaltet gekennzeichnet.
- Endpoint Security funktioniert unter Umständen nicht richtig.

So finden Sie heraus, wie lange Computer inaktiv waren:

1. Zeigen Sie nur die verwalteten Computer an.Klicken Sie auf das **Filtermenü** über der Tabelle und wählen Sie **Verwaltet (Endpunkte)** und **Verwaltet (Endpoint Security Relay)** in der Kategorie **Sicherheit** und klicken Sie anschließend auf **Speichern**.

2. Klicken Sie auf die Spaltenüberschrift **Zuletzt gesehen**, um die Computer nach dem Zeitraum ihrer Inaktivität zu sortieren.

Sie können kürzere Inaktivitätszeiträume (Minuten, Stunden) ignorieren, da diese vermutlich auf ein temporäres Problem zurückzuführen sind.Der Computer ist zum Beispiel gerade ausgeschaltet.

Längere Inaktivitätszeiträume (Tage, Wochen) deuten in der Regel auf ein Problem mit dem Computer hin.

6.1.3. Computer mit Sicherheitsproblemen

Der Sicherheitsstatus betrifft nur verwaltete Computer.Computer mit Sicherheitsproblemen lassen sich durch das Warnsymbol im Statussymbol erkennen:

- Computer verwaltet, mit Problemen, online.
- Computer verwaltet, mit Problemen, offline.

Ein Computer hat dann Sicherheitsprobleme, wenn mindestens einer der folgenden Punkte zutrifft:

- Malware-Schutz ist deaktiviert.
- Die Lizenz für Endpoint Security ist abgelaufen.
- Endpoint Security ist veraltet.
- Malware wurde gefunden.

Wenn Ihnen ein Computer mit Sicherheitsproblemen auffällt, klicken Sie auf seinen Namen, um die Seite **Computer-Details** anzuzeigen.Sicherheitsprobleme erkennen Sie an diesem Symbol.Weitere Details erfahren Sie, wenn Sie den Mauszeiger über das Symbol bewegen.Eventuell muss dem Problem auf lokaler Ebene weiter nachgegangen werden.

6.2. Computer in Gruppen organisieren

Sie können Computergruppen im linken Fenster der **Netzwerk**übersicht in den **Netzwerk**gruppen verwalten.

Ein großer Vorteil ist, dass Sie Gruppenrichtlinien verwenden können, um verschiedene Sicherheitsanforderungen zu erfüllen.

Unter der **Netzwerk**gruppe, die zu Ihrem Unternehmen gehört, können Sie Computer-Gruppen innerhalb einer benutzerdefinierten Baumstruktur erstellen, löschen, umbenennen und verschieben.

Wichtig
Bitte beachten Sie Folgendes:

- Eine Gruppe kann sowohl Computer als auch andere Gruppen enthalten.

- Wenn Sie im linken Bereich eine Gruppe auswählen, können Sie alle enthaltenen Computer einsehen - ausgenommen der, die in die jeweiligen Untergruppen eingeordnet wurden.Wenn Sie alle Computer der Gruppe und ihrer Untergruppen anzeigen möchten, klicken Sie auf das **Filter**menü über der Tabelle, und wählen Sie **Alle Objekte rekursiv** im Bereich **Tiefe**.

Gruppen erstellen

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, Software-Entwicklung, Unternehmensführung usw.).
- Sicherheitsanforderungen (Desktop-Rechner, Laptops, Server usw.).
- Standort (Hauptsitz, Niederlassungen, mobile Angestellte, Heimarbeitsplätze usw.).

Um Ihr Netzwerk in Gruppen aufzuteilen:

1. Wählen Sie im linken Fenster die **Netzwerk** Gruppe aus.
2. Klicken Sie auf die Schaltfläche + **Gruppe hinzufügen** im oberen Bereich des linken Fensters.
3. Geben Sie einen aussagekräftigen Namen für die Gruppe ein, und klicken Sie auf **OK**

Gruppen umbenennen

So benennen Sie eine Gruppe um:

1. Wählen Sie im linken Fenster die Gruppe aus.
2. Klicken Sie auf die Schaltfläche ✎ **Gruppe bearbeiten** im oberen Bereich des linken Fensters.
3. Geben Sie den neuen Namen in das entsprechende Feld ein.
4. Klicken Sie zur Bestätigung auf **OK**.

Gruppen und Computer verschieben

In der **Netzwerk**gruppenhierarchie können Sie Gruppen und Benutzer beliebig verschieben. Um eine Gruppe oder einen Benutzer zu verschieben, verschieben Sie sie/ihn einfach per Drag und Drop von der derzeitigen Position zur neuen.

Beachten Sie

Die Entität, die verschoben wird, erbt die Richtlinieneinstellungen der neuen übergeordneten Gruppe, sofern ihr keine abweichende Richtlinie zugewiesen wurde.Weitere Informationen über Richtlinienvererbung finden Sie unter „Netzwerkobjekten Richtlinien zuweisen“ (S. 70).

Gruppen löschen

Eine Gruppe kann nicht gelöscht werden, wenn Sie mindestens einen Computer enthält.Verschieben Sie alle Computer aus der zu löschenden Gruppe in eine andere Gruppe.Wenn die Gruppe Untergruppen enthält, können Sie anstelle von einzelnen Computern auch alle Untergruppen verschieben.

Um eine Gruppe zu löschen:

1. Wählen Sie die leere Gruppe im rechten Fenster der Seite **Netzwerk** aus.
2. Klicken Sie auf die Schaltfläche – **Gruppe entfernen** im oberen Bereich des linken Fensters.Sie werden aufgefordert, Ihre Aktion zu bestätigen. Klicken Sie dazu auf **Ja**.

6.3. Anzeigen von Computer-Details

Auf der Seite **Netzwerk** finden Sie detaillierte Informationen zu jedem Computer, darunter Betriebssystem, IP-Adresse, Zeit und Datum, an dem der Computer zuletzt gesehen wurde usw.

So erhalten Sie weitere Details zu einem Computer:

1. Gehen Sie zur Seite **Netzwerk**.
2. Wählen Sie die gewünschte Netzwerkgruppe aus dem linken Fenster aus.

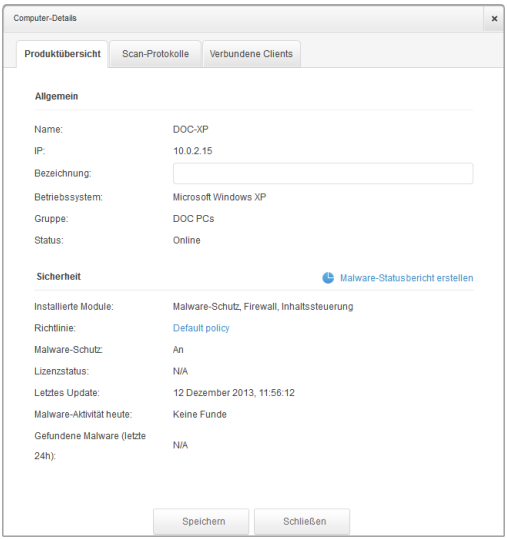
   Alle Computer der ausgewählten Gruppe werden in der Tabelle im rechten Fenster angezeigt.
3. Der Status eines Computers ist durch ein Symbol klar gekennzeichnet. Detaillierte Informationen finden Sie unter „Überprüfen Sie den Status des Computers“ (S. 32).
4. Die einzelnen Spalten enthalten verschiedene Informationen zu jedem Computer:
   - **Name**: der Name des Computers.
   - **Betriebssystem**: auf dem Computer installiertes Betriebssystem.
   - **IP**: IP-Adresse des Computers.
   - **Zuletzt gesehen**: Datum und Zeitpunkt, zu denen der Computer zuletzt online gesehen wurde.

Beachten Sie

Sie sollten regelmäßig das Feld **Zuletzt gesehen** überprüfen, da lange Zeiträume der Inaktivität bedeuten können, dass Kommunikationsprobleme vorliegen oder der Computer vom Netzwerk getrennt wurde.

- **Bezeichnung**: die Bezeichnung, die dem Computer im Fenster **Computer-Details** gegeben wurde.

5. Klicken Sie auf den Namen des verwalteten Computers, der Sie interessiert.Das Fenster **Computer-Details** wird angezeigt:



Computer-Details

- Im Reiter **Übersicht** finden Sie die folgenden Informationen:
  - Allgemeine Informationen zum Computer wie Name, IP-Adresse, Betriebssystem, übergeordnete Gruppe und aktueller Status. Sie können dem Computer auch eine Bezeichnung zuweisen. So können Sie Computer nach ihrer Bezeichnung suchen und filtern, indem Sie die Suchfeldspalte Bezeichnung in der Tabelle rechts auf der Seite **Netzwerk** verwenden.
  - Sicherheitsdetails zu dem auf dem ausgewählten Computer installierten Endpoint Security, so zum Beispiel installierte Module, zugewiesene Richtlinie, Malware-Schutz-Status, Lizenzstatus, letztes Update und in den letzten 24 Stunden gefundene Malware. Sie können sich auch einen schnellen Überblick über die Menge gefundener Malware für den Computer an diesem Tag verschaffen.

– Klicken Sie auf **Malware-Statusbericht erstellen**, um auf die Malware-Berichtoptionen für den ausgewählten Computer zuzugreifen.

Weitere Informationen finden Sie unter „Berichte erstellen“ (S. 122)

Beachten Sie

Jede Eigenschaft, die Sicherheitsprobleme bringt, ist mit dem Symbol markiert.Weitere Details erfahren Sie, wenn Sie den Mauszeiger über das Symbol bewegen.Eventuell muss dem Problem auf lokaler Ebene weiter nachgegangen werden.

- Klicken Sie auf den Reiter **Scan-Protokolle**, um detaillierte Informationen zu allen auf dem Computer ausgeführten Scan-Aufgaben einzusehen. Klicken Sie auf den gewünschten Scan-Bericht, um ihn in einer neuen Seite im Browser zu öffnen.

  Über die Navigation am unteren Rand der Tabelle können Sie zwischen den Seiten wechseln. Wenn Sie sehr viele Einträge haben, können Sie die Filteroptionen über der Tabelle nutzen.

  Klicken Sie auf die Schaltfläche **Neu laden** in der linken unteren Ecke der Tabelle, um die Liste der Scan-Protokolle neu zu laden.

6.4. Sortieren, Filtern und Suchen von Computern

Abhängig von der Anzahl der Computer kann sich die Computer-Tabelle über mehrere Seiten erstrecken (standardmäßig werden nur 10 Einträge pro Seite angezeigt).Verwenden Sie die Navigationsschaltflächen am unteren Rand der Tabelle, um zwischen den Seiten zu wechseln.Um die Anzahl der Einträge zu ändern, die pro Seite angezeigt werden, wählen Sie die entsprechende Option aus dem Menü neben den Navigationsschaltflächen aus.

Sollten zu viele Einträge angezeigt werden, können Sie die Suchfelder unterhalb der Spaltenüberschriften oder das **Filter** Menü über der Tabelle verwenden, um die angezeigten Daten zu filtern.So können Sie zum Beispiel nach einem bestimmten Computer suchen oder nur verwaltete Computer anzeigen.

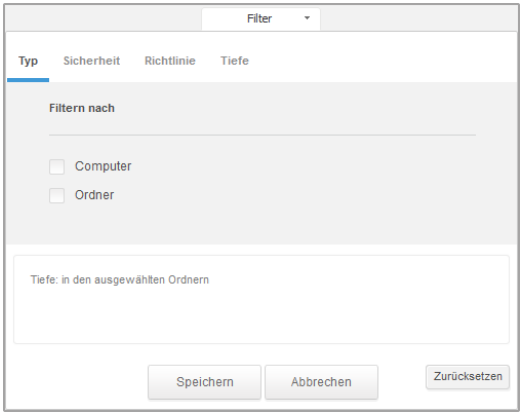
6.4.1. Computer sortieren

Sie können die Daten in der Tabelle nach dem Inhalt einer bestimmten Spalte sortieren, indem Sie auf die entsprechende Spaltenüberschrift klicken.Wenn Sie zum Beispiel möchten, dass die Computer nach ihrem Namen geordnet werden, klicken Sie auf die Überschrift **Name**.Wenn Sie erneut auf den Titel klicken, werden die Computer in umgekehrter Reihenfolge angezeigt.

Computer sortieren

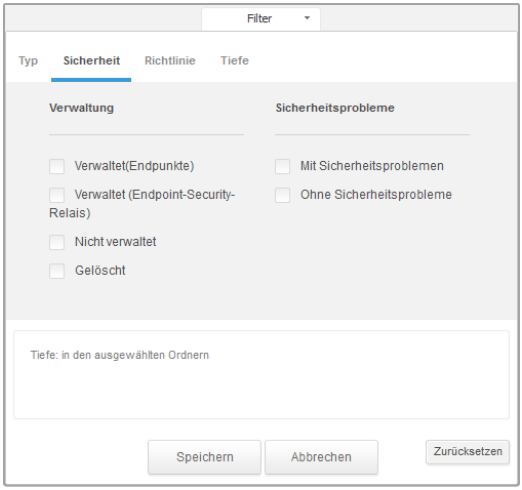
6.4.2. Computer filtern

1. Wählen Sie die gewünschte Gruppe im linken Fenster.
2. Klicken Sie auf das **Filter**-Menü oberhalb der Tabelle.
3. Wählen Sie die Filterkriterien wie folgt aus:
   - **Typ**.Wählen Sie die Art der Entitäten aus, die angezeigt werden sollen (Computer, Ordner oder beides).



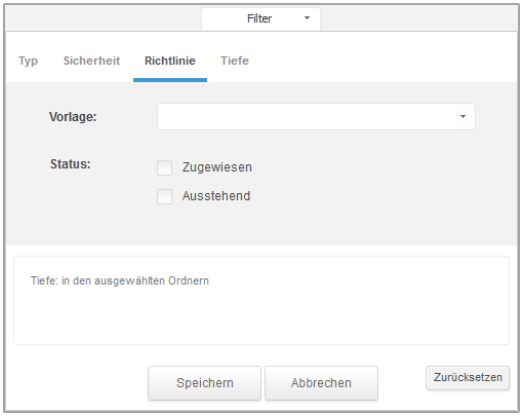
Computer - nach Art filtern

   - **Sicherheit**.Zeigen Sie Computer nach Verwaltungs- und Sicherheitsstatus an.



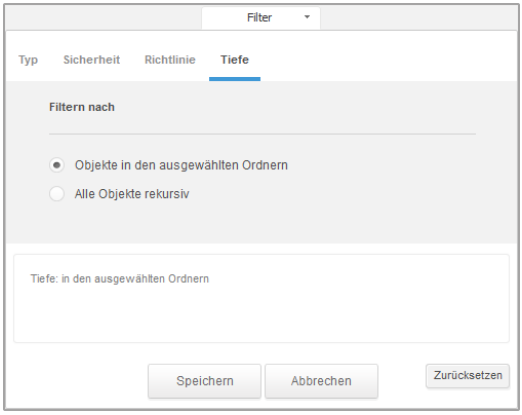
Computer - nach Sicherheit filtern

- **Richtlinie**.Wählen Sie die Richtlinienvorlage, nach der Sie die Computer filtern möchten, sowie den Richtlinienzuweisungsstatus (zugewiesen oder ausstehend).



Computer - nach Richtlinie filtern

- **Tiefe**.Bei der Verwaltung eines Computernetzwerks mit Baumstruktur werden Computer, die sich in Untergruppen befinden, bei Auswahl der Stammgruppe nicht angezeigt.Wählen Sie **Alle Objekte rekursiv**, um alle Computer der aktuellen Gruppe und ihrer Untergruppen anzuzeigen.



Computer - nach Tiefe filtern

Beachten Sie
Die ausgewählten Filterkriterien werden im unteren Teil des **Filter**-Fensters angezeigt. Klicken Sie auf **Zurücksetzen**, um alle Filter zu löschen.

4. Klicken Sie auf **Speichern**, um die Computer nach den gewählten Kriterien zu filtern. Der Filter bleibt aktiv in der **Netzwerk**-Übersicht, bis Sie sich abmelden oder den Filter löschen.

6.4.3. Nach Computern suchen

1. Wählen Sie die gewünschte Gruppe im linken Fenster.
2. Geben Sie den Suchbegriff in das entsprechende Feld unter der Spaltenüberschrift (Name, Betriebssystem oder IP) vom rechten Fenster rein. Geben Sie zum Beispiel die IP-Adresse des Computers, den Sie suchen, in das Feld **IP** ein. Nur der passende Computer wird in der Tabelle angezeigt.

   Leeren Sie das Suchfeld, um die vollständige Liste der Computer anzuzeigen.

Nach Computern suchen

6.5. Aufgaben auf Computern ausführen

Über die Seite **Netzwerk** können Sie per Fernzugriff eine Reihe administrativer Aufgaben auf Computern ausführen.

Sie haben die folgenden Möglichkeiten:

- „Scan“ (S. 42)
- „Client installieren“ (S. 49)
- „Installer verändern“ (S. 52)
- „Client Deinstallieren“ (S. 53)
- „Client aktualisieren“ (S. 54)
- „Computer neu starten“ (S. 54)
- „Netzwerkerkennung“ (S. 55)

Sie können Aufgaben individuell für einzelne Computer oder für Gruppen von Computern erstellen.Sie können zum Beispiel per Ferninstallation Endpoint Security auf einer Gruppe von nicht verwalteten Computern installieren.Später können Sie eine Scan-Aufgabe für einen bestimmten Computer aus dieser Gruppe erstellen.

Auf jedem Computer können Sie nur kompatible Aufgaben ausführen.Wenn Sie zum Beispiel einen nicht verwalteten Computer auswählen, können Sie nur die Aufgabe **Client installieren** wählen. Alle anderen Aufgaben sind nicht verfügbar.

Bei einer Gruppe wird die ausgewählte Aufgabe nur für kompatible Computer erstellt.Wenn kein Computer der Gruppe mit der ausgewählten Aufgabe kompatibel ist, werden Sie benachrichtigt, dass die Aufgabe nicht erstellt werden konnte.

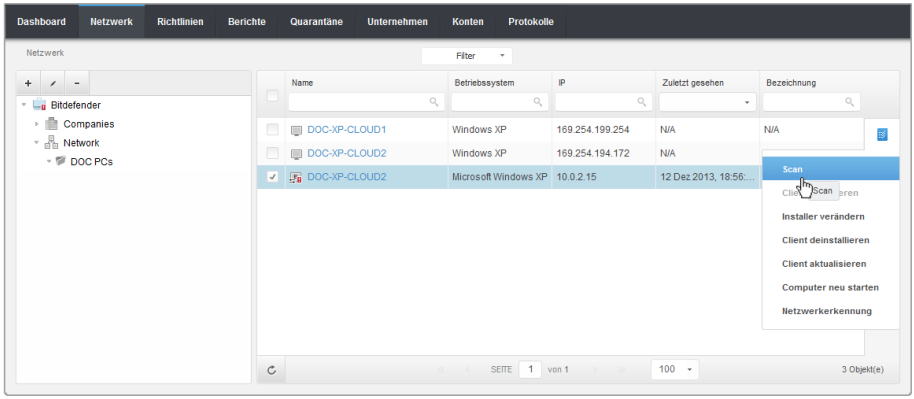
Sofort nach der Erstellung startet die Aufgabe auf Computern, die online sind.Wenn ein Computer offline ist, wird die Aufgabe ausgeführt, sobald er wieder online ist.

Auf der Seite **Netzwerk > Aufgaben** können Sie die Aufgabe anzeigen und verwalten. Weitere Informationen finden Sie unter Viewing and Managing Tasks.

6.5.1. Scan

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

1. Gehen Sie zur Seite **Netzwerk**.
2. Wählen Sie die gewünschte Gruppe aus dem linken Fenster.Alle Computer der ausgewählten Gruppe werden in der Tabelle im rechten Fenster angezeigt.
3. Markieren Sie die Kästchen für die Computer, die Sie scannen möchten.
4. Klicken Sie auf die Schaltfläche **Aufgabe** auf der rechten Seite der Tabelle, und wählen Sie **Scan**.

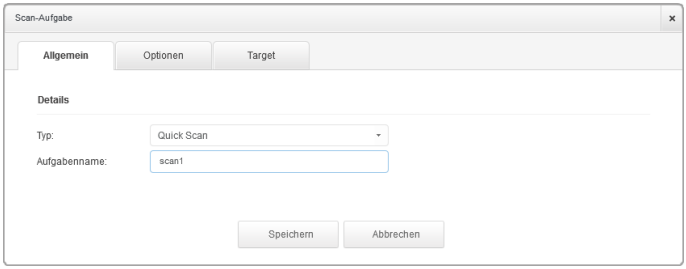


Computer-Scan-Aufgabe

Ein Konfigurationsfenster wird sich öffnen.

5. Konfigurieren Sie die Scan-Optionen:

   - Im Reiter **Allgemein** können Sie den Scan-Typ auswählen und der Scan-Aufgabe einen Namen geben.Der Name dient nur dazu, dass Sie den Scan auf der Seite **Aufgaben** leicht wiederfinden.



Computer-Scan-Aufgabe - Konfigurieren der allgemeinen Einstellungen

Wählen Sie den gewünschten Typ aus dem Menü **Typ**:

– **Quick Scan** setzt auf In-the-Cloud-Scans, um auf Ihrem System laufende Malware aufzuspüren.Die Ausführung eines Quick Scans dauert im Normalfall weniger als eine Minute und beansprucht nur einen Bruchteil der Systemressourcen, die ein normaler Virenscan in Anspruch nehmen würde.

Beachten Sie

Quick Scan findet bestehende Malware, ohne aber irgeneine Aktion 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.So definieren Sie einen benutzerdefinierten Scan:

  • Gehen Sie zum Reiter **Optionen**, um die Scan-Optionen festzulegen.Klicken Sie auf die Sicherheitsstufe, die Ihren Ansprüchen entspricht (aggressiv, normal oder tolerant).Orientieren Sie sich bei Ihrer Auswahl an den Beschreibungen auf der rechten Seite der Skala.

    Je nach ausgewähltem Profil werden die Scan-Optionen im Bereich **Einstellungen** automatisch konfiguriert.Bei Bedarf können Sie diese aber auch im Detail konfigurieren.Markieren Sie dazu das Kästchen **Benutzerdefiniert** und gehen Sie dann zum Bereich **Einstellungen**.

Computer-Scan-Aufgabe

Die folgenden Optionen sind verfügbar:

– **Dateitypen.** Verwenden Sie diese Optionen, um festzulegen, welche Dateien gescannt werden sollen.Sie können Endpoint Security so einrichten, dass Scans durchgeführt werden für alle Dateien (unabhängig von der Dateiendung), nur für Anwendungsdateien oder nur für bestimmte Dateiendungen, die Sie für gefährlich erachten.Das Scannen aller Dateien bietet den besten Schutz, während das Scannen nur von Anwendungen verwendet wird, um einen schnelleren Scan durchzuführen.

Beachten Sie

Anwendungsdateien sind weitaus anfälliger für Malware-Angriffe als andere Dateitypen.Weitere Informationen finden Sie unter „Liste der Anwendungsdateitypen“ (S. 145).

Wenn Sie nur bestimmte Dateiendungen scannen lassen möchten, wählen Sie **Benutzerdefinierte Endungen** aus dem Menü, und geben Sie dann die Endungen in das Eingabefeld ein. Klicken Sie nach jeder Eingabe auf `Speichern`.

Optionen für die Computer-Scan-Aufgabe - Hinzufügen von benutzerdefinierten Endungen

– **Archive.** Archive mit infizierten Dateien sind keine unmittelbare Bedrohung für die Systemsicherheit.Die Malware kann das System nur beeinflussen, wenn die infizierten Datei aus einem Archiv extrahiert und ohne aktivierten Echtzeitschutz ausgeführt wird.Wir empfehlen jedoch, diese Option zu nutzen, um jegliche potentiellen Bedrohungen aufzuspüren und zu entfernen, auch wenn es sich nicht um unmittelbare Bedrohungen handelt.

Beachten Sie

Das Scannen archivierter Dateien erhöht die Gesamt-Scandauer und erfordert mehr Systemressourcen.

- **Inhalt von Archiven scannen.** Wählen Sie diese Option, wenn Sie archivierte Dateien nach Malware durchsuchen möchten.Sollten Sie sich zur Verwendung dieser Option entscheiden, können Sie die folgenden Optimierungsoptionen konfigurieren:
  - **Archivgröße begrenzen auf (MB).** Sie können Sie die maximale Größe der Archive angeben, die gescannt werden sollen.Markieren Sie das entsprechende Kästchen und geben Sie die maximale Archivgröße in MB ein.
  - **Maximale Archivtiefe (Ebenen).** Markieren Sie das entsprechende Kästchen und wählen Sie die maximale Archivtiefe aus dem Menü.Für optimale Leistung wählen Sie den niedrigsten Wert, für maximalen Schutz wählen Sie den höchsten Wert.

- **E-Mail-Archive scannen.** Wählen Sie diese Option, wenn Sie möchten, dass E-Mail-Dateien und E-Mail-Datenbanken (Dateiformate wie EML, MSG, PST, DBX, MBX, TBB usw.) gescannt werden.

Beachten Sie
Das Scannen von E-Mail-Archiven kann viele Ressourcen beansprucht und die Systemleistung beeinträchtigen.

– **Verschiedenes.** Markieren Sie die entsprechenden Kästchen, um die gewünschten Scan-Optionen zu aktivieren.

- **Boot-Sektoren scannen.** Prüft die Bootsektoren des Systems.Dieser Sektor der Festplatte beinhaltet den notwendigen Computercode um den Boot-Prozess zu starten.Wenn ein Virus den Boot-Sektor infiziert, könnte das Laufwerk unzugänglich werden und es könnte Ihnen nicht mehr möglich sein, Ihr System zu starten und auf Ihre Daten zuzugreifen.
- **Registry scannen.** Wählen Sie diese Option, um die Registry-Schlüssel zu scannen.Die Windows-Registry ist eine Datenbank, in der Konfigurationseinstellungen und Optionen für die Windows-Betriebssystemkomponenten sowie für die installierten Anwendungen gespeichert sind.
- **Nach Rootkits suchen.** Wählen Sie diese Option, um nach Rootkits und Objekten zu suchen, die mit dieser Art von Software versteckt werden.
- **Nach Keyloggern suchen.** Wählen Sie diese Option, wenn nach Keylogger-Software gesucht werden soll.
- **Speicher scannen.** Wählen Sie diese Option, um Programme zu scannen, die im Speicher des Systems laufen.
- **Cookies scannen.** Wählen Sie diese Option, um die Cookies zu scannen, die von Ihrem Browser auf dem Computer gespeichert werden.
- **Nur neue und geänderte Dateien.** Indem nur neue und geänderte Dateien gescannt werden, können Sie die allgemeine Systemreaktionsfähigkeit mit minimalen Sicherheitsabstrichen erheblich verbessern.
- **Aufgabe mit niedriger Priorität ausführen.** Verringert die Priorität des Scan-Vorgangs. Dadurch können andere Programme schneller laufen, der Scan dauert aber länger.
- **Computer nach Abschluss der Aufgabe herunterfahren.** Diese Option kann nützlich sein, wenn Sie Scans außerhalb der Arbeitszeiten durchführen.

– **Aktionen.** Abhängig vom gefundenen Dateityp werden folgende Aktionen automatisch ausgeführt:

  • **Wenn eine infizierte Datei gefunden wird.** Als infiziert eingestufte Dateien stimmen mit einer Malware-Signatur der Bitdefender Malware-Signaturen-Datenbank überein.Endpoint Security kann normalerweise den Malware-Code aus einer infizierten Datei entfernen und die ursprüngliche Datei rekonstruieren. Diesen Vorgang bezeichnet man als Desinfektion.

    Wenn eine infizierte Datei gefunden wird, versucht Endpoint Security automatisch, diese zu desinfizieren.Falls die Desinfizierung fehlschlägt, wird die Datei in die Quarantäne verschoben, um dort die Infizierung einzudämmen.

    Wichtig
    Bestimmte Malware-Typen können nicht desinfiziert werden, da die komplette Datei betroffen ist. In diesen Fällen wird die infizierte Datei von der Festplatte gelöscht.

  • **Wenn eine verdächtige Datei gefunden wird.** Dateien werden von der heuristischen Analyse als verdächtig klassifiziert.Da es sich bei B-HAVE um eine heuristische Analysetechnologie handelt, kann Endpoint Security nicht sicher sein, ob die Datei tatsächlich mit Malware infiziert ist.Verdächtige Dateien können nicht desinfiziert werden, da hierfür keine Desinfektionsroutine verfügbar ist.

    Scan-Aufgaben sind standardmäßig so konfiguriert, dass verdächtigte Dateien ignoriert werden.Es könnte ratsam sein, die Standardaktion zu ändern, damit verdächtige Dateien in Quarantäne verschoben werden.Dateien in Quarantäne werden zu Analysezwecken in regelmäßigen Abständen an die Bitdefender-Labs geschickt.Sollten das Vorhandensein von Malware bestätigt werden, wird eine Signatur veröffentlicht, um das Entfernen der Malware zu ermöglichen.

  • **Wenn ein Rootkit gefunden wurde.** Rootkits sind spezielle Software-Wekzeuge, die verwendet werden, um Dateien vor dem Betriebssystem zu verbergen.Obwohl sie nicht zwangsläufig als schädlich anzusehen sind, werden Rootkits häufig genutzt, um Malware zu verbergen oder Eindringlinge im System zu tarnen.

    Erkannte Rootkits und versteckte Dateien werden standardmäßig ignoriert.

  Sie können die standardmäßigen Aktionen verändern, dies wird aber nicht empfohlen.Sie können eine zweite Aktion auswählen, für den Fall, dass die Erste fehlschlägt und außerdem verschiedene Aktionen für jede

Kategorie.Wählen Sie aus den entsprechenden Menus die erste und zweite Aktion, die für jeden entdeckten Dateityp vorgenommen werden soll.Folgende Aktionen stehen zur Verfügung:

Desinfizieren
Den Malware-Kode aus den entdeckten infizierten Dateien entfernen.Es wird empfohlen, dass dies immer die erste Aktion bleibt, die für infizierte Dateien durchgeführt wird.

In Quarant. versch.
Verschieben Sie infizierte Dateien von ihrem Speicherort in den Quarantäne-Ordner.Dateien in der Quarantäne können nicht ausgeführt oder geöffnet werden; aus diesem Grund besteht kein Infektionsrisiko.Sie können die Dateien in Quarantäne über die Quarantäne-Seite in der Konsole verwalten.

Löschen
Infizierte Dateien ohne vorherige Benachrichtigung von der Festplatte löschen.Es wird empfohlen, die Anwendung dieser Aktion zu vermeiden.

Ignorieren
Für gefundene Dateien wird keine Aktion durchgeführt. Diese Dateien werden nur in das Scan-Protokoll aufgenommen.

- Gehen Sie zum Reiter **Ziel**, um die Speicherorte hinzuzufügen, die auf den Ziel-Computern gescannt werden sollen.

  Im Bereich **Scan-Ziel** können Sie eine neue Datei oder einen neuen Ordner hinzufügen, die/der gescannt werden soll:

  a. Wählen Sie einen vorgegebenen Speicherort aus dem Klappmenü, oder geben Sie **Bestimmte Pfade** ein, die sie scann lassen möchten.

  b. Geben Sie den Pfad des zu scannenden Objekts im Bearbeitungsfeld ein.

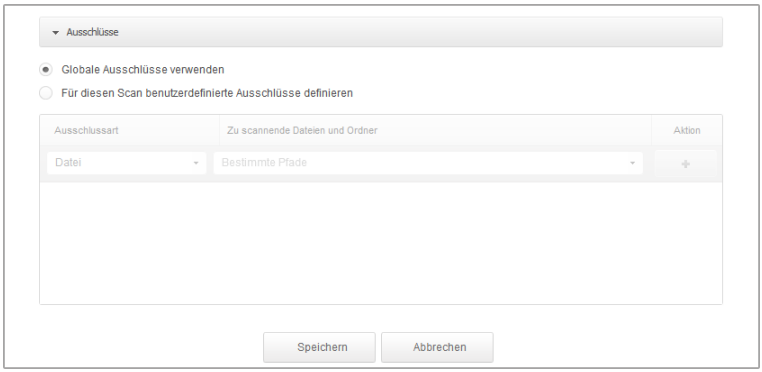
  – Wenn Sie einen vorgegebenen Pfad ausgewählt haben, vervollständigen Sie den Pfad nach Bedarf.Um zum Beispiel den gesamten Ordner `Programme` zu scannen, müssen Sie lediglich den entsprechenden vorgegebenen Pfad aus dem Klappmenü auswählen.Um einen bestimmten Order im Ordner `Programme` zu scannen, müssen Sie den Pfad vervollständigen indem Sie einen Backslash (\) und den Namen des Ordners hinzufügen.

  – Wenn Sie **Bestimmte Pfade** ausgewählt haben, geben Sie den vollständigen Pfad des Objektes ein, das gescannt werden soll.Es empfiehlt sich, (nach Möglichkeit) Systemvariablen zu verwenden, um sicherzustellen, dass der Pfad auf allen Computern gültig ist. Weitere Informationen zu den Systemvariablen finden Sie unter„Systemvariablen verwenden“ (S. 145)

c. Klicken Sie auf den entsprechenden + **Hinzufügen**-Link.

Um einen bestehenden Pfad zu bearbeiten, klicken Sie ihn an.Um einen Server aus der Liste zu entfernen, bewegen Sie den Mauszeiger darüber, und klicken Sie auf die entsprechende − **Löschen**-Schaltfläche.

Klicken Sie auf die Bereiche **Ausschlüsse**, wenn Sie bestimmte Ziele vom Scan ausschließen möchten.



Computer-Scan-Aufgabe - Definieren von Ausschlüssen

Sie können entweder die globalen Ausschlüsse für einen bestimmten Scan verwenden oder konkrete Ausschlüsse für jeden Scan selbst festlegen.Weitere Informationen finden Sie unter „Ausschlüsse“ (S. 93).

6. Klicken Sie auf **Speichern**, um die Scan-Aufgabe zu erstellen.Eine Bestätigungsmeldung wird angezeigt.
7. Auf der Seite **Netzwerk > Aufgaben** können Sie die Aufgabe anzeigen und verwalten. Weitere Informationen finden Sie unter Viewing and Managing Tasks.

6.5.2. Client installieren

Um Ihre Computer mit Security for Endpoints zu schützen, müssen Sie Endpoint Security auf jedem Computer installieren.

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.

Nachdem Sie einen Endpoint Security-Client mit der Endpoint Security Relay-Rolle in einem Netzwerk installiert haben, wird er alle nicht geschützten Computer in diesem Netzwerk automatisch erkennen.

Security for Endpoints kann dann auf diesen Computern per Fernzugriff vom Control Center aus installiert werden.

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

Warnung

Vor der Installation sollten Sie bereits installierte Malware-Schutz- und Firewall-Software deinstallieren.Wenn Security for Endpoints über bestehende Sicherheits-Software installiert wird, kann dies die jeweilige Funktion stören und massive Probleme auf dem System verursachen.Windows Defender und die Windows-Firewall werden beim Start der Installation automatisch deaktiviert.

So installieren Sie Security for Endpoints per Fernzugriff auf einem oder mehreren Computern:

1. Gehen Sie zur Seite **Netzwerk**.
2. 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**.

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

6. Klicken Sie auf **Weiter**.
7. 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.

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

Auf der Seite **Netzwerk > Aufgaben** können Sie die Aufgabe anzeigen und verwalten. Weitere Informationen finden Sie unter Viewing and Managing Tasks.

6.5.3. Installer verändern

So ändern Sie die Schutzmodule, die auf einem oder mehreren Computern installiert sind:

1. Gehen Sie zur Seite **Netzwerk**.
2. Wählen Sie die gewünschte Gruppe aus dem linken Fenster.Alle Computer der ausgewählten Gruppe werden in der Tabelle im rechten Fenster angezeigt.
3. Markieren Sie die Kästchen für die verwalteten Computer, auf denen Sie die installierten Sicherheitsmodule ändern möchten.
4. Klicken Sie auf die Schaltfläche **Aufgabe** auf der rechten Seite der Tabelle, und wählen Sie **Installer verändern**.
5. Wellen Sie im Bereich **Module** nur diejenigen Sicherheitsmodule, die Sie installieren möchten:

Malware-Schutz
Das Modul für den Malware-Schutz schützt Sie vor allen Arten von Bedrohungen durch Malware (Viren, Trojaner, Spyware, Rootkits, Adware usw.).

Firewall
Die Firewall schützt Ihren Computer vor nicht autorisierten Zugriffsversuchen bei eingehendem und ausgehendem Datentransfer.

Inhaltssteuerung
Mit dem Modul Inhaltssteuerung können Sie den Benutzerzugriff auf das Internet und auf Anwendungen steuern.Bitte beachten Sie, dass die Einstellungen für die Inhaltssteuerung auf alle Benutzer angewendet werden, die sich an den Ziel-Computern anmelden.

Beachten Sie
Bitte beachten Sie, dass für Server-Betriebssysteme nur der Malware-Schutz verfügbar ist.

6. Markieren Sie die Option **Wenn nötig, neu starten**, um den Computer automatisch neu starten zu lassen, um die Installation fertigzustellen.
7. Klicken Sie auf **Speichern**. Eine Bestätigungsmeldung wird angezeigt.

   Auf der Seite **Netzwerk > Aufgaben** können Sie die Aufgabe anzeigen und verwalten. Weitere Informationen finden Sie unter Viewing and Managing Tasks.

6.5.4. Client Deinstallieren

Um den Security for Endpoints-Schutz per Fernzugriff auf einem oder mehreren erkannten Computern zu deinstallieren:

1. Gehen Sie zur Seite **Netzwerk**.
2. Wählen Sie die gewünschte Gruppe aus dem linken Fenster.Alle Computer der ausgewählten Gruppe werden in der Tabelle im rechten Fenster angezeigt.
3. Markieren Sie die Kästchen für die Computer, von denen Sie Security for Endpoints deinstallieren möchten.
4. Klicken Sie auf die Schaltfläche **Aufgabe** auf der rechten Seite der Tabelle, und wählen Sie **Client deinstallieren**.
5. Ein Konfigurationsfenster wird angezeigt, in dem Sie sich für den Verbleib Quarantäne-Objekte auf der Client-Maschine entscheiden können.
6. Klicken Sie auf **Speichern**, um die Aufgabe zu erstellen. Eine Bestätigungsmeldung wird angezeigt.

   Auf der Seite **Netzwerk > Aufgaben** können Sie die Aufgabe anzeigen und verwalten. Weitere Informationen finden Sie unter Viewing and Managing Tasks.

Beachten Sie
Wenn Sie den Schutz erneut installieren möchten, müssen Sie den Computer zuerst neu starten.

6.5.5. Client aktualisieren

Überprüfen Sie den Status verwalteter Computer in regelmäßigen Abständen.Wenn Ihnen ein Computer mit Sicherheitsproblemen auffällt, klicken Sie auf seinen Namen, um die Seite **Computer-Details** anzuzeigen.Weitere Informationen finden Sie unter „Computer mit Sicherheitsproblemen“ (S. 34).

Ein veralteter Client stellt ein Sicherheitsproblem dar.In diesem Fall sollten Sie ein Client-Update auf dem entsprechenden Computer durchführen.Diese Aufgabe kann lokal vom Computer aus oder per Fernzugriff von der Control Center aus durchgeführt werden.

So können Sie den Client auf verwalteten Computern per Fernzugriff aktualisieren:

1. Gehen Sie zur Seite **Netzwerk**.
2. Wählen Sie die gewünschte Gruppe aus dem linken Fenster.Alle Computer der ausgewählten Gruppe werden in der Tabelle im rechten Fenster angezeigt.
3. Markieren Sie die Kästchen der Computer ,auf denen Sie ein Client-Update durchführen möchten.
4. Klicken Sie auf die Schaltfläche **Aufgabe** auf der rechten Seite der Tabelle, und wählen Sie **Client aktualisieren**.
5. Sie werden aufgefordert, Ihre Aktion zu bestätigen. Klicken Sie dazu auf **Ja**. Eine Bestätigungsmeldung wird angezeigt.

   Auf der Seite **Netzwerk > Aufgaben** können Sie die Aufgabe anzeigen und verwalten. Weitere Informationen finden Sie unter Viewing and Managing Tasks.

6.5.6. Computer neu starten

Sie können verwaltete Computer aus der Ferne neu starten, wenn Sie möchten.

Beachten Sie
Bevor Sie einzelne Computer neu starten, sollten Sie einen Blick auf die Seite **Netzwerk > Aufgaben** werfen.Zuvor erstellte Aufgaben könnten zurzeit noch auf den ausgewählten Computern laufen.

1. Gehen Sie zur Seite **Netzwerk**.
2. Wählen Sie die gewünschte Gruppe aus dem linken Fenster.Alle Computer der ausgewählten Gruppe werden in der Tabelle im rechten Fenster angezeigt.
3. Markieren Sie die Kästchen für die Computer, die Sie neu starten möchten.

4. Klicken Sie auf die Schaltfläche **Aufgabe** auf der rechten Seite der Tabelle, und wählen Sie **Computer neu starten**.
5. Wählen Sie den Zeitpunkt des Neustarts:
   - Wählen Sie **Jetzt neu starten**, um die Computer sofort neu zu starten.
   - Wählen Sie **Neustadt am**, und nutzen Sie die Eingabefelder weiter unten, um den Neustart für einen beliebigen Zeitraum zu planen.
6. Klicken Sie auf **Speichern**. Eine Bestätigungsmeldung wird angezeigt.

   Auf der Seite **Netzwerk > Aufgaben** können Sie die Aufgabe anzeigen und verwalten. Weitere Informationen finden Sie unter Viewing and Managing Tasks.

6.5.7. Netzwerkerkennung

Der Endpoint Security mit der Endpoint Security Relay-Rolle führt stündlich eine automatische Netzwerkerkennung durch. Sie können über die Control Center ausgehend von jeder beliebigen von Endpoint Security geschützten Maschine auch jederzeit eine Netzwerkerkennungsaufgabe manuell durchführen.

So führen Sie eine Netzwerkerkennungsaufgabe in Ihrem Netzwerk durch:

1. Gehen Sie zur Seite **Netzwerk**.
2. Wählen Sie die gewünschte Computergruppe aus dem linken Fenster.Alle Computer der ausgewählten Gruppe werden in der Tabelle im rechten Fenster angezeigt.
3. Markieren Sie die Kästchen für die Computer, mit denen Sie eine Netzwerkerkennung durchführen möchten.
4. Klicken Sie auf die Schaltfläche **Aufgabe** auf der rechten Seite der Tabelle, und wählen Sie **Netzwerkerkennung**.
5. Eine Bestätigungsmeldung wird angezeigt. Klicken Sie auf **Ja**.

   Auf der Seite **Netzwerk > Aufgaben** können Sie die Aufgabe anzeigen und verwalten. Weitere Informationen finden Sie unter Viewing and Managing Tasks.

6.6. Schnellberichte erstellen

Auf der Seite **Netzwerk** können Sie Sofortberichte auf verwalteten Computern erstellen:

1. Gehen Sie zur Seite **Netzwerk**.
2. Wählen Sie die gewünschte Gruppe aus dem linken Fenster. Alle Computer der ausgewählten Gruppe werden in der Tabelle im rechten Fenster angezeigt.

   Optional können Sie den Inhalt der ausgewählten Gruppe nur nach verwalteten Computern filtern.
3. Markieren Sie die Kästchen für die Computer, die Sie in den Bericht aufnehmen möchten.

4. Klicken Sie auf die Schaltfläche **Bericht** auf der rechten Seite der Tabelle, und wählen Sie den Berichtstyp aus dem Menü. Aktivitätsberichte enthalten ausschließlich Daten aus der letzten Woche. Weitere Informationen finden Sie unter „Verfügbare Berichtstypen“ (S. 119).
5. Konfigurieren Sie die Berichtsoptionen.Weitere Informationen finden Sie unter „Berichte erstellen“ (S. 122)
6. Klicken Sie auf **Generieren**.Der Bericht wird sofort angezeigt.Es dauert unterschiedlich lange, bis Berichte erstellt sind, je nach Anzahl der gewählten Computer.

6.7. Richtlinien zuweisen

Die Sicherheitseinstellungen auf den Computern werden über Richtlinien verwaltet.

Im Bereich **Netzwerk** können Sie Richtlinien für jeden Computer bzw. Gruppe von Computern anzeigen, ändern und zuweisen.

Beachten Sie

Sie können die Sicherheitseinstellungen für verwaltete Computer oder für Gruppen anzeigen oder ändern.Um diese Arbeit zu erleichtern, können Sie die Tabelle nach verwalteten Computern filtern.

So zeigen Sie an, welche Richtlinie einem bestimmten Computer zugewiesen wurde:

1. Gehen Sie zur Seite **Netzwerk**.
2. Wählen Sie die gewünschte Gruppe aus dem linken Fenster.Alle Computer der ausgewählten Gruppe werden in der Tabelle im rechten Fenster angezeigt.
3. Klicken Sie auf den Namen des verwalteten Computers, der Sie interessiert.Ein Fenster mit Details wird angezeigt.
4. Klicken Sie im Bereich **Sicherheit** auf den Namen der aktuellen Richtlinie, um ihre Einstellungen anzuzeigen.
5. Sie können die Sicherheitseinstellungen nach Bedarf ändern, sofern der Richtlinienersteller Änderungen an dieser Richtlinie durch andere Benutzer erlaubt hat. Bitte beachten Sie, dass Ihre Änderungen sich auch auf alle anderen Computer auswirken, denen diese Richtlinie zugewiesen wurde.

   Weitere Informationen über das Ändern von Computer-Richtlinien finden Sie unter „Richtlinien für Computer“ (S. 72).

So weisen Sie einem Computer oder einer Gruppe eine Richtlinie zu:

1. Gehen Sie zur Seite **Netzwerk**.
2. Wählen Sie die gewünschte Gruppe aus dem linken Fenster.Alle Computer der ausgewählten Gruppe werden in der Tabelle im rechten Fenster angezeigt.

3. Markieren Sie das Kästchen des gewünschten Computers bzw. der gewünschten Gruppe.Sie können auch mehrere Objekte auswählen, diese müssen dann jedoch Objekte desselben Typs und von derselben Ebene sein.
4. Klicken Sie auf die Schaltfläche **Richtlinie** auf der rechten Seite der Tabelle.
5. Nehmen Sie im Fenster **Richtlinienzuweisung** die nötigen Einstellungen vor.Weitere Informationen finden Sie unter „Netzwerkobjekten Richtlinien zuweisen“ (S. 70).

6.8. Computer aus dem Netzwerkinventar löschen

Wenn Sie einige der gefundenen Computer nicht verwalten möchten, können Sie sie aus dem Netzwerkinventar ausschließen. Außerdem können Sie ausgeschlossene Computer dauerhaft aus dem Netzwerkinventar löschen.

6.8.1. Ausschließen von Computern aus dem Netzwerkinventar

So schließen Sie Computer aus dem Netzwerkinventar aus:

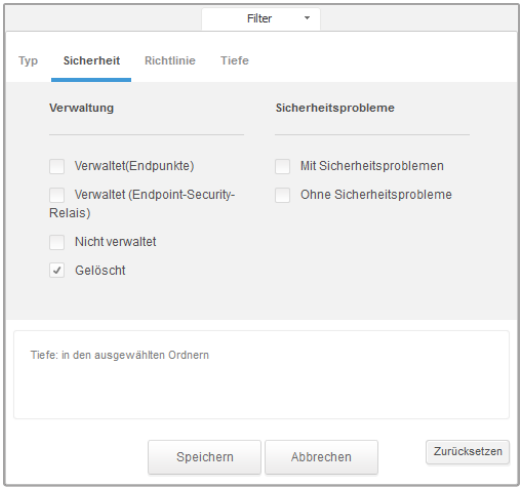
1. Gehen Sie zur Seite **Netzwerk**.
2. Wählen Sie die gewünschte Gruppe aus dem linken Fenster.Alle Computer der ausgewählten Gruppe werden in der Tabelle im rechten Fenster angezeigt.
3. Markieren Sie das Kästchen des Computers, den Sie ausschließen möchten.
4. Klicken Sie auf die Schaltfläche **Löschen** auf der rechten Seite der Tabelle.Sie werden aufgefordert, Ihre Aktion zu bestätigen. Klicken Sie dazu auf **Ja**.

   Beachten Sie

   Wenn Sie einen verwalteten Computer löschen, wird Endpoint Security automatisch von ihm deinstalliert.

   Nachdem Sie einen Computer gelöscht haben, wird er nicht mehr in der Tabelle angezeigt.Gelöschte Computer existieren weiterhin in der Small Office Security-Datenbank, aber sie sind nicht mehr sichtbar.

   Zu einem späteren Zeitpunkt möchten Sie die gelöschten Computer eventuell wieder verwalten.In diesem Fall müssen Sie die gelöschten Computer anzeigen und auf denen, die Sie verwalten möchten, Endpoint Security installieren.Um gelöschte Computer anzuzeigen, klicken Sie auf das **Filter**-Menü über der Tabelle, öffnen Sie den Reiter **Sicherheit**, wählen Sie die Option **Gelöscht** und klicken Sie danach auf **Speichern**.



Computer - nach gelöschten Endpunkten filtern

Beachten Sie
Wenn Sie den Schutz auf einem ausgeschlossenen Computer wieder installieren, wird dieser als verwaltet erkannt und in der Tabelle wiederhergestellt.

6.8.2. Computer dauerhaft löschen

So löschen Sie Computer dauerhaft aus dem Netzwerkinventar:

1. Gehen Sie zur Seite **Netzwerk**.
2. Wählen Sie die gewünschte Gruppe aus dem linken Fenster.Alle Computer der ausgewählten Gruppe werden in der Tabelle im rechten Fenster angezeigt.
3. Filtern Sie die Tabelle nach Computern, die **Gelöscht** sind.
4. Markieren Sie die Kästchen der Computer, die Sie löschen möchten.
5. Klicken Sie auf die Schaltfläche **– Löschen** auf der rechten Seite der Tabelle.Sie werden aufgefordert, Ihre Aktion zu bestätigen. Klicken Sie dazu auf **Ja**.

   Die entsprechenden Computer werden dauerhaft aus der Small Office Security-Datenbank gelöscht.

Warnung
Einen dauerhaft gelöschten Computer können Sie in der Small Office Security-Datenbank nicht wiederherstellen.

6.9. Installationspakete

Die Schutzkomponenten von Small Office Security können auf den Zielobjekten im Netzwerk installiert werden, indem sie entweder über die Control Center bereitgestellt werden oder indem das notwendige Installationspaket heruntergeladen und manuell auf dem gewünschten Netzwerkobjekt ausgeführt wird.

Sie können die Installationspakete auf der Seite **Netzwerk > Pakete** verwalten.

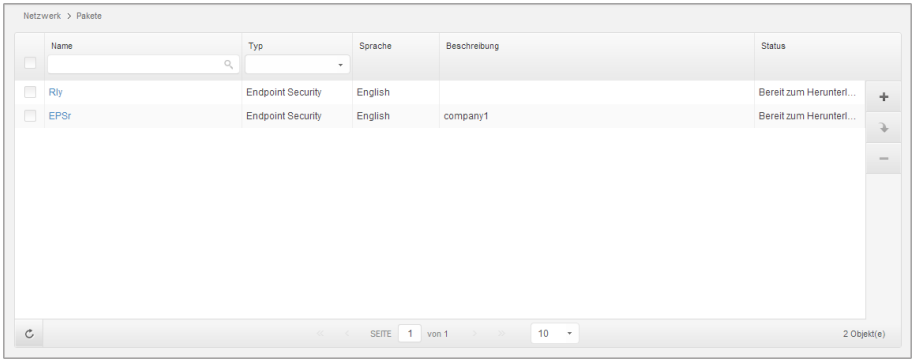
6.9.1. Installationspakete erstellen

Eventuell müssen Sie einige Dinge in den Installationspaketen anpassen.

Endpoint Security Installationspakete erstellen

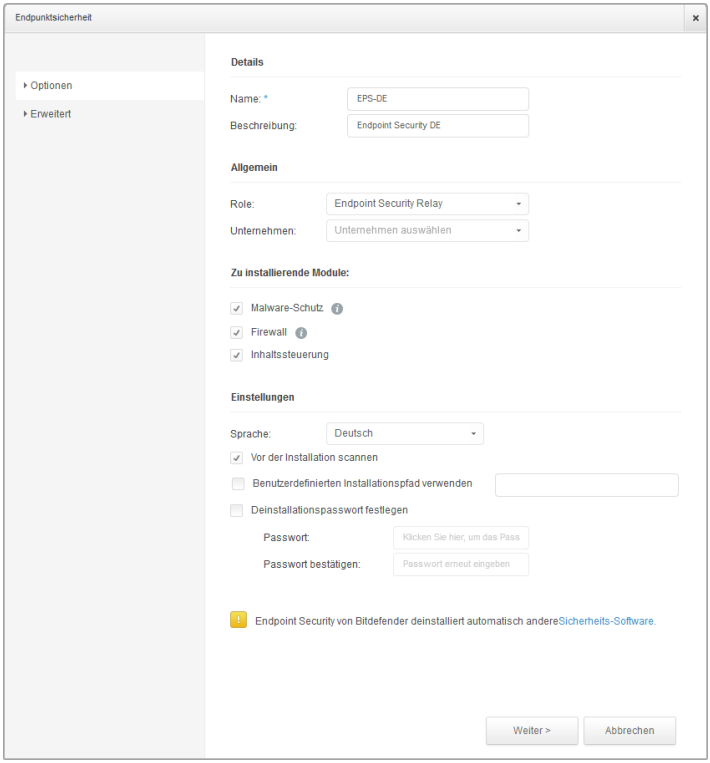
So erstellen Sie ein Installationspaket für Endpoint Security:

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.

6.9.2. Installationspakete herunterladen

So laden Sie Installationspakete für Endpoint Security herunter:

1. Melden Sie sich über den Computer, auf dem Sie den Schutz installieren möchten, an der Control Center an.
2. Gehen Sie zur Seite **Netzwerk > Pakete**.
3. Wählen Sie das Endpoint Security-Installationspaket aus, das Sie herunterladen möchten.
4. 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.

Beachten Sie
Verfügbare Installationspaket-Versionen:

– **Windows OS:** 32-Bit- und 64-Bit-Systeme

– **Mac OS X:** nur 64-Bit-Systeme

Stellen Sie sicher, dass Sie die zum jeweiligen Computer passende Version wählen.

5. Speichern Sie die Datei auf dem Computer.

6.10. Aufgaben anzeigen und verwalten

Auf der Seite **Netzwerk > Aufgaben** können Sie alle Aufgaben, die Sie erstellt haben, einsehen und verwalten.

Sobald Sie eine Aufgabe für Netzwerkobjekte erstellt haben, wird sie in der Aufgabentabelle aufgeführt.

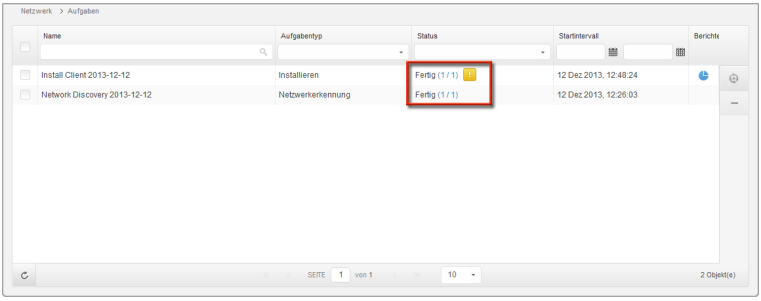
Auf der Seite **Netzwerk > Aufgaben** haben Sie folgende Möglichkeiten:

- Aufgabenstatus überprüfen
- Aufgabenberichte anzeigen
- Aufgaben erneut ausführen
- Aufgaben löschen

6.10.1. Aufgabenstatus überprüfen

Wenn Sie eine Aufgabe für Netzwerkobjekte erstellen, werden Sie den Fortschritt der Aufgabe überprüfen wollen und benachrichtigt werden, wenn Fehler auftreten.

Auf der Seite **Netzwerk > Aufgaben** informiert Sie die Spalte **Status** der einzelnen Aufgaben über den jeweiligen Status.Sie können den Status der Hauptaufgabe überprüfen und detaillierte Informationen über jede Teilaufgabe abrufen.



Die Aufgabenübersicht

- **Status der Hauptaufgabe überprüfen**.

  Die Hauptaufgabe ist die Aktion, die auf die Netzwerkobjekte angewendet wird (wie zum Beispiel Installation des Clients oder Scan). Sie enthält bestimmte Teilaufgaben, eine für jedes Netzwerkobjekt.So enthält eine Installationshauptaufgabe für acht Computer zum Beispiel acht Teilaufgaben.Die Zahlen in Klammern geben an, wie viele Teilaufgaben schon abgeschlossen wurden.So bedeutet (2/8) zum Beispiel, dass zwei von acht Teilaufgaben abgeschlossen sind.

  Die Hauptaufgabe kann einen der folgenden Status haben:
  - **Ausstehend**, wenn bisher keine der Teilaufgaben gestartet wurde.
  - **Wird ausgeführt** - wenn alle Teilaufgaben laufen.Die Hauptaufgabe bleibt in diesem Status, bis die letzte Teilaufgabe abgeschlossen ist.
  - **Fertig**, wenn alle Teilaufgaben (erfolgreich oder erfolglos) beendet wurden.Bei erfolglosen Teilaufgaben wird ein Warnsymbol angezeigt.

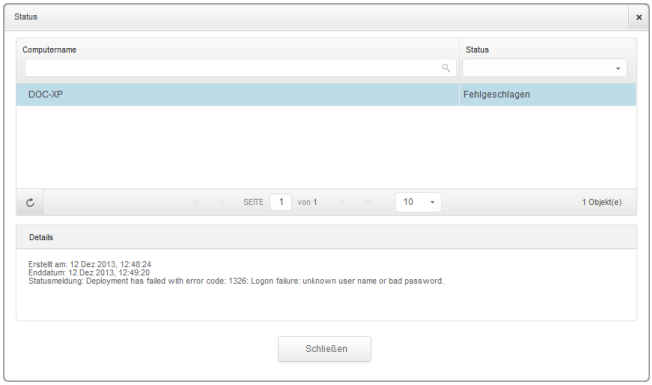
- **Status der Teilaufgaben überprüfen**.

  Gehen Sie zur Aufgabe, die Sie interessiert, und klicken Sie auf den Link in der Spalte **Status**, um das Fenster **Status** zu öffnen.Dort werden die Netzwerkobjekte, auf die die Hauptaufgabe sich bezieht, sowie der Status jeder Teilaufgabe angezeigt.Die Teilaufgaben können folgende Status haben:

  - **Wird ausgeführt** - wenn die Teilaufgabe noch läuft.
  - **Fertig** - wenn die Teilaufgabe erfolgreich abgeschlossen wurde.
  - **Ausstehend** - wenn die Teilaufgabe noch nicht gestartet wurde.Das kann in den folgenden Situationen passieren:
    - Die Teilaufgabe wartet in einer Warteschlange.
    - Es gibt Verbindungsprobleme zwischen der Control Center und dem Zielobjekt im Netzwerk.

– **Fehlgeschlagen** - wenn die Teilaufgabe nicht gestartet werden konnte oder wegen eines Fehlers wie ungültigen Zugangsdaten oder zu geringem Speicher angehalten wurde.

Sie können Details zu einzelnen Teilaufgaben anzeigen, indem Sie sie auswählen und im Bereich **Details** unten in der Tabelle nachsehen.



Aufgabenstatusdetails

Dort finden Sie die folgenden Informationen:

– Datum und Uhrzeit des Aufgabenstarts.

– Datum und Uhrzeit des Aufgabenendes.

– Beschreibung aufgetretener Fehler.

6.10.2. Aufgabenberichte anzeigen

Auf der Seite **Netzwerk > Aufgaben** können Sie Schnellberichte zu Scan-Aufgaben lesen.

1. Gehen Sie zur Seite **Netzwerk > Aufgaben**.
2. Markieren Sie das Kästchen der Scan-Aufgabe, die Sie interessiert.
3. Klicken Sie auf die entsprechende Schaltfläche in der Spalte **Berichte**.Warten Sie, bis der Bericht angezeigt wird.Weitere Informationen finden Sie unter „Berichte verwenden“ (S. 119).

6.10.3. Erneutes Ausführen von Aufgaben

Die Client-Installation, Deinstallation oder Update-Aufgaben können aus verschiedenen Gründen fehlschlagen. Sie müssen solche fehlgeschlagenen Aufgaben nicht neu anlegen, sondern können sie wir folgt erneut ausführen:

1. Gehen Sie zur Seite **Netzwerk > Aufgaben**.
2. Markieren Sie die Kästchen für die fehlgeschlagenen Aufgaben.
3. Klicken Sie auf die Schaltfläche **Erneut ausführen** auf der rechten Seite der Tabelle. Die ausgewählten Aufgaben werden neu gestartet und der Aufgabenstatus wechselt auf **Neuer Versuch**.

Beachten Sie
Bei Aufgaben mit mehreren Teilaufgaben ist die Option **Erneut ausführen** nur dann verfügbar, wenn alle Teilaufgaben abgeschlossen wurden. Es werden nur die fehlgeschlagenen Teilaufgaben erneut ausgeführt.

6.10.4. Aufgaben löschen

Wir empfehlen, nicht mehr benötigte Aufgaben zu löschen, um zu verhindern, dass die Aufgabenliste unübersichtlich wird.

1. Gehen Sie zur Seite **Netzwerk > Aufgaben**.
2. Markieren Sie das Kästchen der Aufgabe, die Sie löschen möchten.
3. Klicken Sie auf die Schaltfläche **Löschen** auf der rechten Seite der Tabelle.Sie werden aufgefordert, Ihre Aktion zu bestätigen. Klicken Sie dazu auf **Ja**.

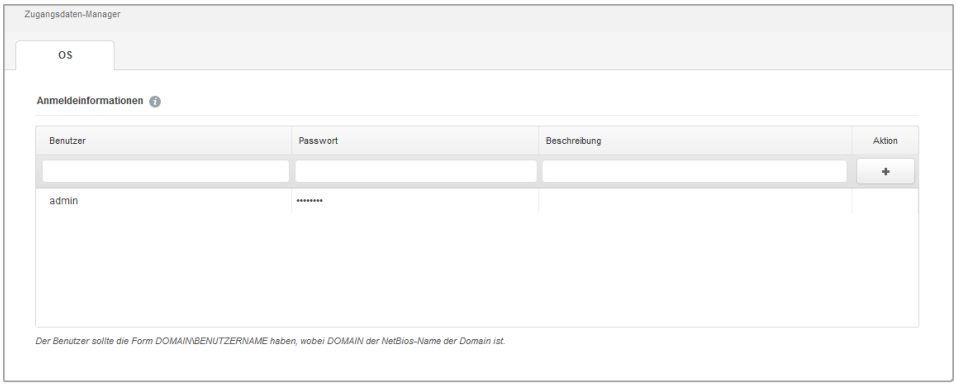
Warnung
Wenn Sie eine ausstehende Aufgabe löschen, wird die Aufgabe auch abgebrochen. Wenn eine laufende Aufgabe gelöscht wird, werden etwaige ausstehende Teilaufgaben abgebrochen. In diesem Fall können abgeschlossene Teilaufgaben nicht rückgängig gemacht werden.

6.11. Zugangsdaten-Manager

Der Zugangsdaten-Manager unterstützt Sie bei der Verwaltung der Zugangsdaten, die Sie für die Fernauthentifizierung an den verschiedenen Betriebssystemen in Ihrem Netzwerk benötigen.

Um den Zugangsdaten-Manager zu öffnen, bewegen Sie den Mauszeiger auf Ihren Benutzernamen in der rechten oberen Ecke der Seite, und wählen Sie **Zugangsdaten-Manager**.

6.11.1. Hinzufügen von Zugangsdaten zum Zugangsdaten-Manager



Zugangsdaten-Manager

1. Geben Sie im entsprechenden Feld den Benutzernamen und das Passwort eines Administratorkontos 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`).
2. Klicken Sie auf den Button **Hinzufügen**.Die neuen Zugangsdaten werden der Tabelle hinzugefügt.

Beachten Sie
Wenn Sie die Authentifizierungsdaten noch nicht angegeben haben, müssen Sie diese bei Ausführung von Installationsaufgaben eingeben. Die angegebenen Zugangsdaten werden automatisch im Zugangsdaten-Manager gespeichert, sodass Sie sie beim nächsten Mal nicht mehr eingeben müssen.

6.11.2. Zugangsdaten aus dem Zugangsdaten-Manager löschen

So löschen Sie obsolete Zugangsdaten aus dem Zugangsdaten-Manager:

1. Bewegen Sie den Mauszeiger zur Tabellenzeile mit den Zugangsdaten, die Sie löschen möchten.
2. Klicken Sie auf die Schaltfläche **Löschen** auf der rechten Seite der entsprechenden Tabellenzeile.Das ausgewählte Konto wird gelöscht.

7. Sicherheitsrichtlinien

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

Direkt nach der Installation wird den Netzwerkinventarobjekten die Standardrichtlinie zugewiesen, die mit den empfohlenen Schutzeinstellungen vorkonfiguriert ist.Die Standardrichtlinie können sie weder ändern noch löschen.Sie können Sie nur als Vorlage zur Erstellung neuer Richtlinien verwenden.

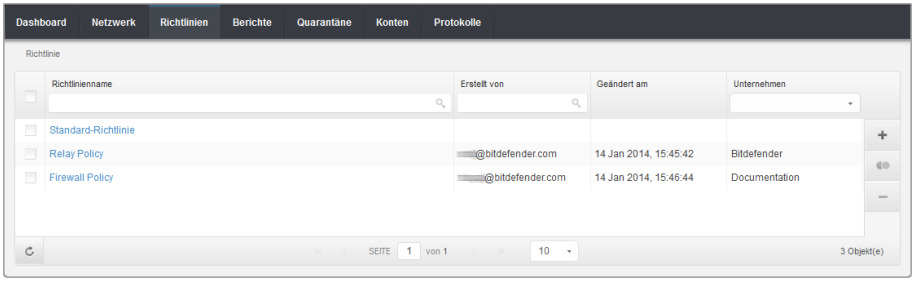
Sie können je nach Sicherheitsanforderungen beliebig viele Richtlinien erstellen.

Was Sie über Richtlinien wissen sollten:

- Richtlinien werden in der **Richtlinien**übersicht erstellt und in der **Netzwerk**übersicht den Netzwerkobjekten zugewiesen.
- Netzwerkobjekte können jeweils nur eine aktive Richtlinie haben.
- Richtlinien werden sofort, nachdem sie angelegt oder verändert wurden, per Push an die Netzwerkobjekte übertragen. Die Einstellungen sollten in weniger als einer Minute auf den Netzwerkobjekten übernommen werden (vorausgesetzt, dass sie online sind). Wenn ein Netzwerkobjekt offline ist, werden die Einstellungen übernommen, sobald es 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.

7.1. Policies verwalten

Auf der **Richtlinien**-Seite können Sie die Richtlinien einsehen und verwalten.



Die Richtlinienübersicht

Bestehende Richtlinien werden in der Tabelle angezeigt. Sie können das Folgende für jede Richtlinie einsehen:

- Richtlinienname.
- Benutzer, der die Richtlinie angelegt hat.
- Datum und Zeitpunkt, zu dem die Richtlinie zuletzt verändert wurde.

Sie können die bestehenden Richtlinien sortieren und über auswählbare Kriterien nach bestimmen Richtlinien suchen.

7.1.1. Richtlinien erstellen

Richtlinien können auf zwei Arten erstellt werden: eine neue hinzufügen oder eine bestehende kopieren (klonen).

Um eine neue Richtlinie anzulegen:

1. Gehen Sie zur **Richtlinien**-Seite.
2. Wählen Sie die Art der Richtlinienerstellung:
   - **Neue Richtlinie hinzufügen**.
     - Klicken Sie auf die Schaltfläche **Hinzufügen** auf der rechten Seite der Tabelle.Hierüber können Sie ausgehend von der Standardrichtlinienvorlage eine neue Richtlinie erstellen.
   - **Bestehende Richtlinie klonen**.
     a. Markieren Sie das Kästchen der Richtlinie, die Sie klonen möchten.
     b. Klicken Sie auf die Schaltfläche **Klonen** auf der rechten Seite der Tabelle.

3. Konfigurieren Sie die Richtlinieneinstellungen. Detaillierte Informationen finden Sie unter „Richtlinien für Computer“ (S. 72).
4. Klicken Sie auf **Speichern**, um eine Richtlinie zu erstellen und zur Liste der Richtlinien zurückzukehren.

7.1.2. Richtlinieneinstellungen ändern

Richtlinieneinstellungen können zunächst beim Erstellen der Richtlinie festgelegt werden.Sie können diese später aber auch jederzeit wieder ändern.

Beachten Sie
Standardmäßig kann nur der Benutzer die Richtlinie ändern, der sie erstellt hat. Um das zu ändern, muss der Ersteller der Richtlinie auf der Seite **Details** der Richtlinie die Option **Anderen Benutzern erlauben, diese Richtlinie zu ändern** markieren.

So ändern Sie die Einstellungen einer bestehenden Richtlinie:

1. Gehen Sie zur **Richtlinien**-Seite.
2. Finden Sie die Richtlinie in der Liste, und klicken Sie auf ihren Namen, um sie zu bearbeiten.
3. Konfigurieren Sie die Richtlinieneinstellungen nach Ihren Wünschen. Detaillierte Informationen finden Sie unter „Richtlinien für Computer“ (S. 72).
4. Klicken Sie auf **Speichern**.

   Richtlinien werden sofort nach einer Änderung der Richtlinienzuweisung oder der Richtlinieneinstellungen per Push an die entsprechenden Netzwerkobjekte übertragen.Die Einstellungen sollten in weniger als einer Minute auf den Netzwerkobjekten übernommen werden (vorausgesetzt, dass sie online sind).Wenn ein Netzwerkobjekt offline ist, werden die Einstellungen übernommen, sobald es wieder online ist.

7.1.3. Richtlinien umbenennen

Achten Sie bei Richtlinien auf einen eindeutigen Namen, damit Sie oder andere Administratoren diese schnell identifizieren können.

Um eine Richtlinie umzubenennen:

1. Gehen Sie zur **Richtlinien**-Seite.
2. Klicken Sie auf den Richtliniennamen.Dadurch öffnet sich die Richtlinienseite.
3. Geben Sie einen neuen Namen für die Richtlinie ein.
4. Klicken Sie auf **Speichern**.

Beachten Sie
Jeder Richtlinienname ist einzigartig. Sie müssen für jede Richtlinie einen eigenen Namen eingeben.

7.1.4. Richtlinien löschen

Löschen Sie eine Richtlinie, wenn Sie sie nicht mehr länger benötigt wird.Nach dem Löschen der Richtlinie wird den Netzwerkobjekten, auf die sie zuvor angewendet wurde, die Richtlinie der übergeordneten Gruppe zugewiesen.Sollte keine andere Richtlinie angewendet werden, wird zwangsläufig die Standardrichtlinie übernommen.

Beachten Sie
Standardmäßig kann nur der Benutzer eine Richtlinie löschen, der sie erstellt hat. Um das zu ändern, muss der Ersteller der Richtlinie auf der Seite **Details** der Richtlinie die Option **Anderen Benutzern erlauben, diese Richtlinie zu ändern** markieren.

Um eine Richtlinie zu löschen:

1. Gehen Sie zur **Richtlinien**-Seite.
2. Aktivieren Sie das entsprechende Kästchen.
3. Klicken Sie auf die Schaltfläche **Löschen** auf der rechten Seite der Tabelle.Sie werden aufgefordert, Ihre Aktion zu bestätigen. Klicken Sie dazu auf **Ja**.

7.1.5. Netzwerkobjekten Richtlinien zuweisen

Nachdem Sie die nötigen Richtlinien im Bereich **Richtlinien** eingerichtet haben, können Sie sie im Bereich **Netzwerk** bestimmten Netzwerkobjekten zuweisen.

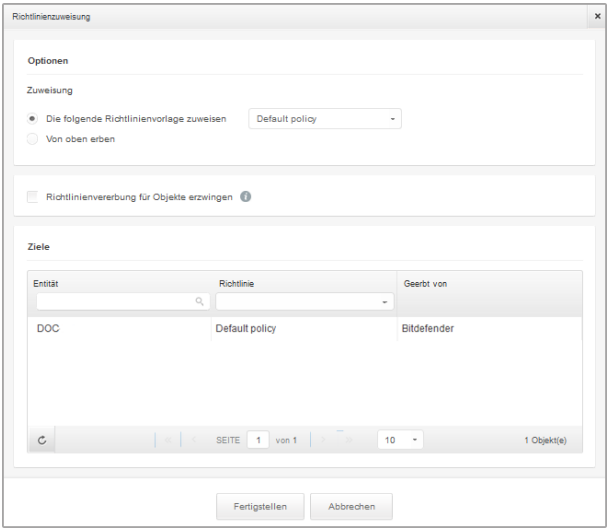
Allen Netzwerkobjekten ist zunächst die Standardrichtlinie zugewiesen.

Beachten Sie
Sie können nur Richtlinien zuweisen, die auch von Ihnen erstellt wurden. Um eine Richtlinie zuzuweisen, die von einem anderen Benutzer erstellt wurde, müssen Sie sie zunächst auf der Seite **Richtlinien** klonen.

So weisen Sie eine Richtlinie zu:

1. Gehen Sie zur Seite **Netzwerk**.
2. Markieren Sie das Kästchen des gewünschten Netzwerkobjekts.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

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.

Richtlinien werden sofort nach einer Änderung der Richtlinienzuweisung oder der Richtlinieneinstellungen per Push an die entsprechenden Netzwerkobjekte übertragen. Die Einstellungen sollten in weniger als einer Minute auf den Netzwerkobjekten übernommen werden (vorausgesetzt, dass sie online sind). Wenn ein Netzwerkobjekt offline ist, werden die Einstellungen übernommen, sobald es wieder online ist.

Um zu überprüfen, ob die Richtlinie erfolgreich zugewiesen wurde, öffnen Sie die **Netzwerk**-Seite und klicken Sie auf den Namen des Objekts, das Sie im Fenster **Details** anzeigen wollen. Im Bereich **Richtlinie** können Sie den Status der aktuellen Richtlinie einsehen. Beim Status "Ausstehend" wurde die Richtlinie bisher noch nicht auf das Zielobjekt angewendet.

7.2. Richtlinien für Computer

Richtlinieneinstellungen können zunächst beim Erstellen der Richtlinie festgelegt werden. Sie können diese später aber auch jederzeit wieder ändern.

So konfigurieren Sie die Einstellungen einer Richtlinie:

1. Gehen Sie zur **Richtlinien**-Seite.
2. Klicken Sie auf den Richtliniennamen. Dadurch öffnet sich die Richtlinieneinstellungsseite
3. Konfigurieren Sie die Richtlinieneinstellungen nach Ihren Wünschen.Es gibt die folgenden Kategorien von Einstellungen:
   - Allgemein
   - Malware-Schutz
   - Firewall
   - Inhaltssteuerung

   Sie können die Einstellungskategorie über das Menü auf der linken Seite auswählen.
4. Klicken Sie auf **Speichern**, um die Änderungen zu speichern und auf die Ziel-Computer anzuwenden.Wenn Sie die Richtlinienseite verlassen möchten, ohne die Änderungen zu speichern, klicken Sie auf **Abbrechen**.

Beachten Sie
Wie Sie Richtlinien verwenden, erfahren Sie unter „Policies verwalten“ (S. 68).

7.2.1. Allgemein

Über die allgemeinen Einstellungen können Sie die Anzeigeoptionen der Benutzeroberfläche, Kommunikationsoptionen, Update-Einstellungen, den Passwortschutz und andere Endpoint Security-Einstellungen verwalten.

Die Einstellungen sind in die folgenden Bereiche eingeteilt:

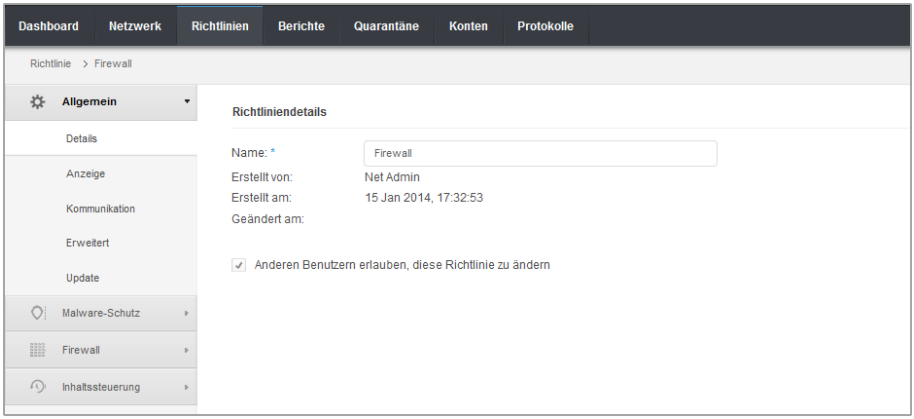
- Details

- Anzeige
- Kommunikation
- Erweitert
- Update

Details

Auf der Seite Details finden Sie allgemeine Informationen zur jeweiligen Richtlinie:

- Richtlinienname
- Benutzer, der die Richtlinie angelegt hat
- Datum und Zeitpunkt, zu dem die Richtlinie erstellt wurde.
- Datum und Zeitpunkt, zu dem die Richtlinie zuletzt verändert wurde



Richtlinien für Computer

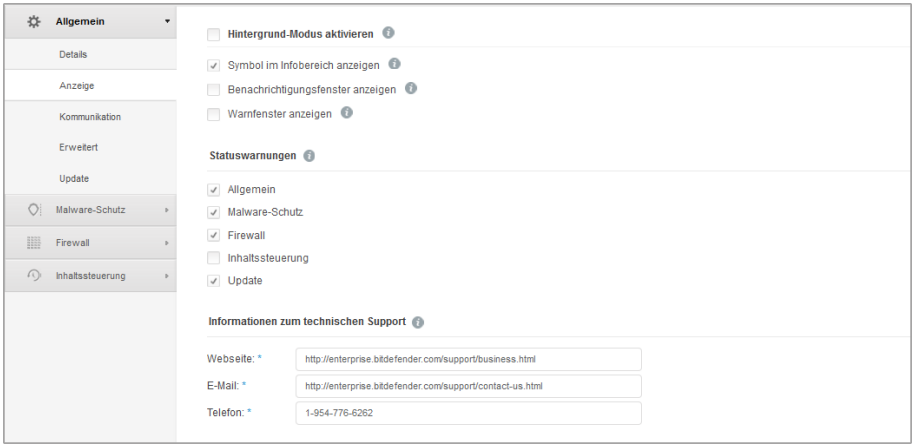
Sie können die Richtlinie umbenennen, indem Sie den neuen Namen in das entsprechende Feld eingeben und auf **Speichern** klicken.Achten Sie bei Richtlinien auf einen eindeutigen Namen, damit Sie oder andere Administratoren diese schnell identifizieren können.

Beachten Sie

Standardmäßig kann nur der Benutzer die Richtlinie ändern, der sie erstellt hat. Um das zu ändern, muss der Ersteller der Richtlinie auf der Seite **Details** der Richtlinie die Option **Anderen Benutzern erlauben, diese Richtlinie zu ändern** markieren.

Anzeige

In diesem Bereich können Sie die Anzeigeoptionen für die Benutzeroberfläche konfigurieren.



Computer-Richtlinien - Anzeigeeinstellungen

- **Hintergrund-Modus aktivieren.** Über das Kästchen können Sie den Hintergrundmodus an- und ausschalten.Der Lautlos-Modus soll Ihnen helfen, Benutzereingriffe in Endpoint Security einfach zu unterbinden.Bei der Aktivierung des Lautlos-Modus werden die folgenden Änderungen an der Richtlinienkonfiguration aktiv:
  - Die Optionen **Symbol im Benachrichtigungsbereich anzeigen**, **Benachrichtigungsfenster anzeigen** und **Warnfenster anzeigen** in diesem Bereich werden deaktiviert.
  - Wenn die Firewall-Sicherheitsstufe auf **Bestehende Regeln und nachfragen** oder **Bestehende Regeln, bekannte Dateien und nachfragen** eingestellt war, wird jetzt auf **Bestehende Regeln, bekannte Dateien und zulassen** eingestellt. Ansonsten wird die Einstellung der Sicherheitsstufe nicht verändert.
- **Symbol im Infobereich anzeigen.** Wählen Sie diese Option, um das Bitdefender-Symbol im Benachrichtigungsbereich (in der Task-Leiste) anzuzeigen.Das Symbol zeigt dem Benutzer den Sicherheitsstatus an, indem es sein Aussehen verändert und ein entsprechendes Benachrichtigungsfenster anzeigt. Außerdem kann der Benutzer mit der rechten Maustaste auf das Symbol klicken, um das Hauptfenster von Endpoint Security oder das **Über**-Fenster zu öffnen. Wenn Sie das **Über**-Fenster öffnen, wird dadurch automatisch ein Bedarf-Update gestartet.
- **Benachrichtigungsfenster anzeigen.** Wählen Sie diese Option, um Benutzer mithilfe von kleinen Benachrichtigungsfenstern über wichtige Sicherheitsereignisse wie den Fund von Malware und die daraufhin ausgeführte Aktion zu informieren. Diese Benachrichtigungsfenster werden automatisch nach ein paar Sekunden ausgeblendet, ohne dass der Benutzer etwas tun muss.

- **Warnfenster anzeigen.** Anders als Benachrichtigungsfenster fordern Warnfenster Benutzer zur Auswahl einer Aktion aus. Wenn Sie Warnfenster nicht anzeigen lassen, führt Endpoint Security automatisch die empfohlene Aktion aus.Warnfenster werden in den folgenden Situationen angezeigt:
  - Wenn die Firewall so konfiguriert ist, dass der Benutzer entscheidet, welche Aktion ausgeführt wird, wenn unbekannte Anwendungen auf Netzwerk oder Internet zugreifen wollen.
  - Wenn Active Virus Control/Angriffserkennungssystem aktiviert wird, wenn eine potenziell schädliche Anwendung gefunden wird.
  - Wenn der Geräte-Scan aktiviert ist und ein externes Speichermedium an den Computer angeschlossen wird.Diese Einstellung kann unter **Malware-Schutz > Bei Bedarf** vorgenommen werden.
- **Statuswarnungen.** Benutzer werden über Ihren Schutzstatus auf zwei Wegen informiert:
  - Der Sicherheitsstatusbereich im Hauptfenster zeigt eine entsprechende Statusnachricht und wechselt seine Farbe je nach gefundenem Problem.
  - Das Bitdefender-Symbol im Benachrichtigungsbereich ändert sein Aussehen, wenn Probleme entdeckt werden.

  Der Schutzstatus wird anhand der ausgewählten Statuswarnungen bestimmt und bezieht sich auf Probleme in der Sicherheitskonfiguration oder andere Sicherheitsrisiken.Wenn zum Beispiel die Option **Status des Malware-Schutzes** ausgewählt ist, wird der Benutzer informiert, sobald Probleme beim Malware-Schutz auftreten(so zum Beispiel ob Zugriff-Scans deaktiviert wurden oder ein System-Scan überfällig ist).

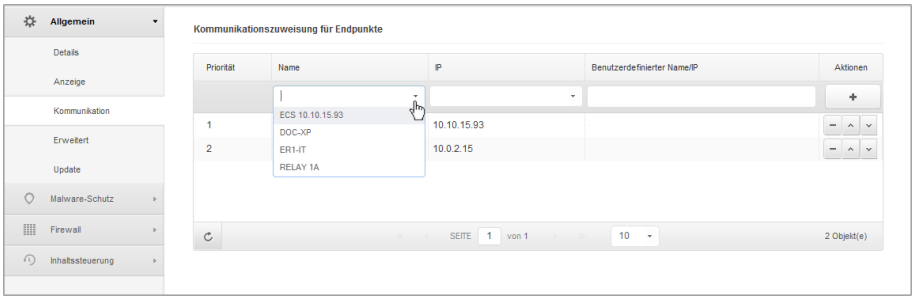
  Wählen Sie die Sicherheitsaspekte aus, die überwacht werden sollen.Wenn Sie nicht möchten, das die Benutzer über bestehende Probleme informiert werden, deaktivieren Sie alle Kästchen.
- **Informationen zum technischen Support.** Durch Ausfüllen der entsprechenden Felder können Sie die in Endpoint Security angezeigten Informationen zum technischen Support und Kontaktdaten selbst anpassen.Benutzer können diese Informationen über das Endpoint Security-Fenster durch einen Klick auf das -Symbol in der rechten unteren Bildschirmecke aufrufen (oder durch einen Rechtsklick auf das Endpoint Security-Symbol in der Task-Leiste und die Auswahl des Menüpunktes **Über**).

Kommunikation

Wenn im Zielnetzwerk mehrere Endpoint Security Relayen verfügbar sind, können Sie den ausgewählten Computern per Richtlinie einen oder mehrere Endpoint Security Relayn zuweisen.

So weisen Sie Ziel-Computern einen Endpoint Security Relay zu:

1. Klicken Sie in der Tabelle **Kommunikationszuweisung für Endpunkte** auf das Feld **Name**. Die Liste der in Ihrem Netzwerk erkannten Endpoint Security Relayen wird angezeigt.
2. Wählen Sie eine Entität.



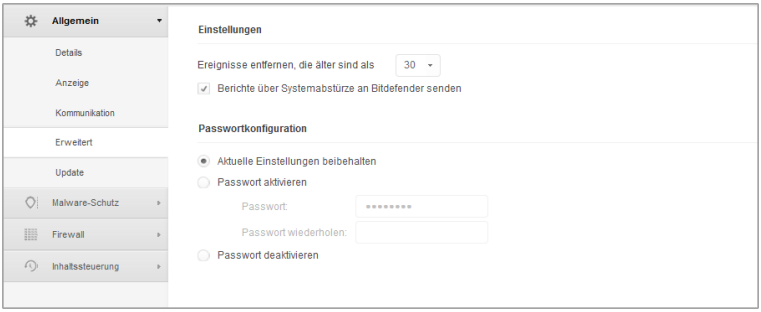
Computer-Richtlinien - Kommunikationseinstellungen

3. Klicken Sie auf die Schaltfläche ⁺ **Hinzufügen** auf der rechten Seite der Tabelle.

   Die Endpoint Security Relay wird der Liste hinzugefügt. Alle Zielcomputer werden über die angegebenen Endpoint Security Relay mit dem Control Center kommunizieren.
4. Wiederholen Sie diese Schritte, wenn Sie mehrere Endpoint Security Relay hinzufügen möchten, falls es mehrere gibt.
5. Sie können die Priorität der Endpoint Security Relay konfigurieren, indem Sie auf die rechts von jeder Entität angezeigten Pfeile klicken. Die Kommunikation mit den Zielcomputern läuft über die Entität, die ganz oben in der Liste steht. Sollte die Kommunikation über diese Entität nicht möglich sein, wird es über die nächste in der Liste versucht.
6. Um eine Entität aus der Liste zu entfernen, klicken Sie auf die entsprechende Schaltfläche ⁻ **Löschen** auf der rechten Seite der Tabelle.

Erweitert

In diesem Bereich können Sie allgemeine Einstellungen und das Deinstallationspasswort festlegen.



Computer-Richtlinien - erweiterte Einstellungen

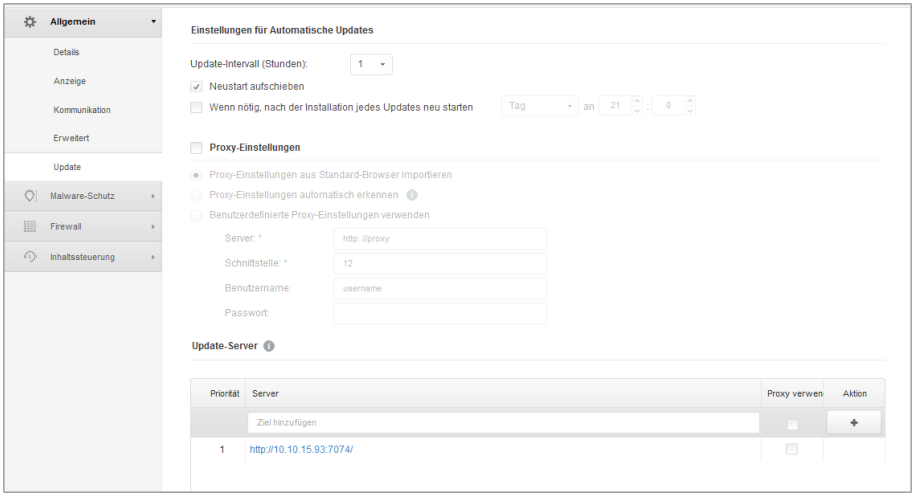
- **Ereignisse entfernen, die älter sind als (Tage).** Endpoint Security führt ein detailliertes Ereignisprotokoll über alle Aktivitäten der Software auf Ihrem Computer (einschließlich der Computer-Aktivitäten, die von der Inhaltssteuerung überwacht werden).Ereignisse werden standardmäßig nach 30 Tagen aus dem Protokoll gelöscht.Um dieses Intervall zu ändern, wählen Sie im Menü eine andere Option aus.
- **Berichte über Systemabstürze an Bitdefender schicken.** Wählen Sie diese Option, damit Berichte zur Analyse an die Bitdefender-Labors geschickt werden, wenn es bei Endpoint Security zu Systemabstürzen kommt.Die Berichte helfen unseren Mitarbeitern dabei, die Ursache des Problems zu finden und ein Wiederauftreten zu verhindern.Es werden keine persönlichen Informationen mitgesendet.
- **Passwortkonfiguration.** Um zu verhindern, dass Benutzer mit Administratorenrechten den Schutz deinstallieren, müssen Sie ein Passwort festlegen.

  Das Deinstallationspasswort kann schon vor der Installation festgelegt werden, indem Sie das Installationspaket individuell anpassen. Falls Sie dies getan haben, wählen Sie **Aktuelle Einstellungen beibehalten**, um das aktuelle Passwort beizubehalten.

  Um das Passwort einzurichten oder das aktuelle Passwort zu ändern, wählen Sie **Passwort aktivieren** und geben Sie das gewünschte Passwort ein.Um den Passwortschutz zu entfernen, wählen Sie **Passwort deaktivieren**.

Update

In diesem Bereich können Sie die Endpoint Security-Update-Einstellungen konfigurieren.Updates sind von großer Wichtigkeit, da nur so den neuesten Bedrohungen begegnet werden kann.



Computer-Richtlinien - Aktualisierungsoptionen

- **Update-Intervall (Stunden).** Endpoint Security wird stündlich automatisch nach Updates suchen und diese herunterladen und installieren (Standardeinstellung).Automatische Updates werden unauffällig im Hintergrund durchgeführt.

  Um das automatische Update-Intervall zu ändern, wählen Sie im Menü eine andere Option aus.Bitte beachten Sie, dass automatische Updates nicht deaktiviert werden können.

- **Neustart aufschieben.** Manche Updates machen einen Neustart des Systems erforderlich, um die Installation abzuschließen.Wenn Sie diese Option auswählen, wird das Programm weiterhin mit den alten Dateien arbeiten, bis der Computer neu gestartet wird, ohne den Nutzer vorher zu informieren.Ansonsten wird eine Benachrichtigung in der Benutzeroberfläche den Benutzer auffordern, das System neu starten, sollte dies wegen eines Updates erforderlich sein.

  Wenn Sie den Zeitpunkt des Neustarts verschieben möchten, können Sie eine passendere Zeit festlegen, zu der die Computer automatisch neu gestartet werden, sollte dies (weiterhin) nötig sein. Dies erweist sich insbesondere bei Servern als sehr nützlich.Klicken Sie auf **Wenn nötig, nach der Installation von Updates neu starten** und legen Sie eine passende Zeit für den Neustart fest (täglich, wöchentlich an einem bestimmten Tag, zu einer bestimmten Uhrzeit).

- **Proxyverwaltung.** Wählen Sie diese Option, wenn die Computer über einen Proxy-Server mit dem Internet (oder dem lokalen Update-Server) verbunden sind.Sie können Proxy-Einstellungen auf drei verschiedene Arten vornehmen:

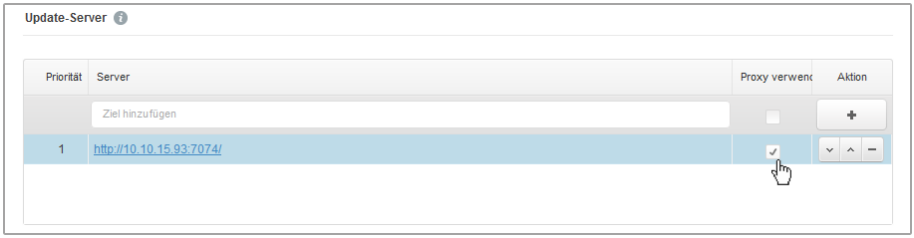
  – **Proxy-Einstellungen aus Standard-Browser importieren.** Endpoint Security kann die Proxy-Einstellungen aus den gängigsten Browsern importieren, einschließlich der neuesten Versionen von Internet Explorer, Mozilla Firefox und Opera.

- **Netzwek-Proxy automatisch erkennen.** Endpoint Security setzt das WPAD-Protokoll (Web-Proxy-Auto-Erkennung) ein, das in Windows enthalten ist, um Proxy-Einstellungen automatisch von einer im Netzwerk veröffentlichten PAC-Datei (Proxy auto configuration) zu beziehen. Wenn keine PAC-Datei verfügbar ist, werden Updates fehlschlagen.
- **Benutzerdefinierte Proxy-Einstellungen verwenden.** Wenn Sie die Proxy-Einstellungen kennen, wählen Sie diese Option und geben Sie sie dann an:
  - **Server** - Geben Sie die IP-Adresse des Proxy-Servers ein.
  - **Port** - Geben Sie den Port ein, über den die Verbindung zum Proxy-Server hergestellt wird.
  - **Name** - Geben Sie einen für den Proxy-Server gültigen Benutzernamen ein.
  - **Passwort** - Geben Sie das Passwort für den zuvor angegebenen Benutzer ein.

Beachten Sie

Wenn Sie die Proxy-Konfigurationsoption ändern, werden dadurch die bestehenden Proxy-Einstellungen in Endpoint Security überschrieben.

Zudem müssen Sie das Kästchen **Proxy benutzen** für die Update-Adresse aktivieren, auf die die Einstellungen angewendet werden sollen (die lokale oder die Internet-Update-Server-Adresse).



Computer-Richtlinien - Update-Adressen

- **Update-Adressen**. Um überhöhten Netzwerkverkehr nach außen zu vermeiden, ist Endpoint Security so konfiguriert, dass Updates vom Small Office Security-Update-Server geladen werden. Sie können auch andere lokale Update-Server-Adressen der Liste hinzufügen und mithilfe der Richtungsschaltflächen ihre Priorität festlegen. Wenn der erste Update-Server in der Liste nicht verfügbar ist, wird der zweite angefragt usw.

  Um die lokale Update-Adresse einzurichten:

  1. Geben Sie die Adresse des lokalen Update-Servers in das Feld **Location hinzufügen** ein.Verwenden Sie dazu eine der folgenden Syntaxoptionen:
     - `update_server_ip:port`
     - `update_server_name:port`

     Der Standard-Port ist 7074.

2. Falls sich Client-Computer über einen Proxy-Server mit dem lokalen Update-Server verbinden, aktivieren Sie **Proxy benutzen**.
3. Klicken Sie auf die Schaltfläche **Hinzufügen** auf der rechten Seite der Tabelle.
4. Nutzen Sie die Aufwärts- / Abwärtspfeile in der Spalte **Aktion**, um die lokale Update-Adresse in der Liste nach ganz oben zu bewegen. Bewegen Sie dazu den Mauszeiger über die entsprechende Zeile; daraufhin werden die Pfeile angezeigt.

Um einen Server aus der Liste zu entfernen, bewegen Sie den Mauszeiger darüber, und klicken Sie auf die entsprechende **Löschen**-Schaltfläche.Es ist zwar möglich, die standardmäßige Update-Adresse zu entfernen, dies wird jedoch nicht empfohlen.

7.2.2. Malware-Schutz

Das Modul für den Malware-Schutz schützt Sie vor allen Arten von Bedrohungen durch Malware (Viren, Trojaner, Spyware, Rootkits, Adware usw.).Der Schutz wird in zwei Kategorien unterteilt:

- Zugriff-Scans: Verhindern, dass neue Malware-Bedrohungen auf das System gelangen.
- Bedarf-Scans: Malware, die sich bereits im System befindet, kann entdeckt und entfernt werden.

Wenn Endpoint Security einen Virus oder andere Malware findet, versucht das Programm automatisch, den Malware-Code aus der infizierten Datei zu entfernen und die Originaldatei wiederherzustellen.Diese Operation bezeichnet man als Desinfektion.Dateien, die nicht desinfiziert werden können, werden in die Quarantäne verschoben, um so die Infizierung einzudämmen.Die in der Quarantäne enthaltenen Dateien können weder ausgeführt noch geöffnet werden.

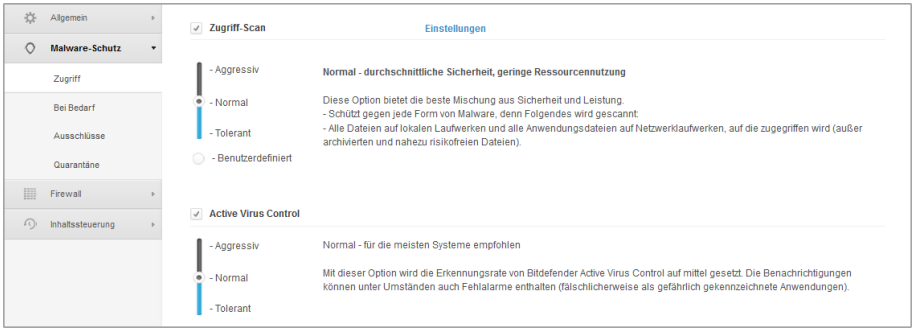
Erfahrene Benutzer können Scan-Ausschlüsse konfigurieren, wenn Sie nicht möchten, dass bestimmte Dateien oder Dateitypen gescannt werden.

Die Einstellungen sind in die folgenden Bereiche eingeteilt:

- Zugriff
- Bedarf-Scan
- Ausschlüsse
- Quarantäne

Zugriff

In diesem Anschnitt können Sie die zwei Komponenten für den Echtzeit-Malware-Schutz konfigurieren:



Computer-Richtlinien - Zugriffeinstellungen

- Zugriff-Scan
- Active Virus Control

Einstellungen für den Zugriff-Scan

Durch Zugriff-Scans wird verhindert, dass neue Malware-Bedrohungen auf das System gelangen - dabei werden Dateien bei jedem Zugriff (Öffnen, Verschieben, Kopieren oder Ausführen), E-Mail-Nachrichten jeweils bei Versand und Empfang und jeglicher Internet-Datenverkehr gescannt.

Um die Zugriffs-Scans zu konfigurieren:

1. Über das Kästchen können Sie Zugriffs-Scans aktivieren oder deaktivieren.Wenn Sie Zugriffs-Scans deaktivieren, werden die Computer anfällig für Malware.
2. Für eine schnelle Konfiguration, klicken Sie auf die Sicherheitsstufe, die Ihren Anforderungen entspricht (aggressiv, normal, tolerant).Orientieren Sie sich bei Ihrer Auswahl an den Beschreibungen auf der rechten Seite der Skala.
3. Erfahrene Benutzer können Details der Scan-Einstellungen konfigurieren, indem sie die Sicherheitsstufe **Benutzerdefiniert** wählen und auf den Link **Einstellungen** klicken. Das Fenster für die **Zugriff-Scan-Einstellungen** wird angezeigt. Hier finden Sie unter den Reitern **Allgemein** und **Erweitert** eine Reihe von Optionen. Im Folgenden werden die Optionen vom ersten bis zum letzten Reiter beschrieben:

   - **Datei-Speicherort**. Verwenden Sie diese Optionen, um festzulegen, welche Dateien gescannt werden sollen. Die Scan-Einstellungen für lokale Dateien (auf dem lokalen Computer gespeichert) und Netzwerkdateien (auf den Netzwerklaufwerken gespeichert) können separat festgelegt werden. Wenn der Malware-Schutz auf allen Computern im Netzwerk installiert ist, ist es möglich, den Scan der Netzwerkdateien zu deaktivieren, um den Netzwerkzugriff zu beschleunigen.

     Sie können Endpoint Security so einrichten, dass Scans durchgeführt werden für alle aufgerufenen Dateien (unabhängig von der Dateiendung), nur für Anwendungsdateien

oder nur für bestimmte Dateiendungen, die Sie für gefährlich erachten. Das Scannen aller Dateien bietet den besten Schutz, während das ausschließliche Scannen der Anwendungen nur für die Verbesserung der Systemleistung verwendet werden kann.

Beachten Sie
Anwendungsdateien sind weitaus anfälliger für Malware-Angriffe als andere Dateitypen. Weitere Informationen finden Sie unter „Liste der Anwendungsdateitypen“ (S. 145).

Wenn Sie nur bestimmte Dateiendungen scannen lassen möchten, wählen Sie **Benutzerdefinierte Endungen** aus dem Menü, und geben Sie dann die Endungen in das Eingabefeld ein. Klicken Sie nach jeder Eingabe auf `Speichern`.

Sie können auch große Dateien vom Scan ausschließen, um die Systemleistung nicht zu stark zu beeinträchtigen. Markieren Sie das Kästchen **Maximale Größe (MB)** geben Sie die Größe an, bis zu der Dateien gescannt werden sollen. Gehen Sie mit dieser Einstellung vorsichtig um, denn Malware kann auch größere Dateien befallen.

- **Archive** Wählen Sie **Inhalt von Archiven scannen**, wenn Sie Zugriff-Scans für archivierte Dateien aktivieren möchten. Das Scannen von Archiven ist ein langsamer und ressourcen-intensiver Vorgang, der aus diesem Grund nicht für den Echtzeitschutz empfohlen wird. Archive mit infizierten Dateien sind keine unmittelbare Bedrohung für die Systemsicherheit. Die Malware kann das System nur beeinträchtigen, wenn die infizierte Datei aus dem Archiv extrahiert und bei deaktivierten Zugriff-Scans ausgeführt wird.

  Sollten Sie sich zur Verwendung dieser Option entscheiden, können Sie die folgenden Optimierungsoptionen konfigurieren:

  – **Maximale Archivgröße (MB).** Sie können Sie die maximale Größe der Archive angeben, die beim Zugriff-Scan durchsucht werden sollen.Markieren Sie das entsprechende Kästchen und geben Sie die maximale Archivgröße in MB ein.

  – **Maximale Archivtiefe (Ebenen).** Markieren Sie das entsprechende Kästchen und wählen Sie die maximale Archivtiefe aus dem Menü.Für optimale Leistung wählen Sie den niedrigsten Wert, für maximalen Schutz wählen Sie den höchsten Wert.

- **Verschiedenes.** Markieren Sie die entsprechenden Kästchen, um die gewünschten Scan-Optionen zu aktivieren.

  – **Boot-Sektoren scannen.** Prüft die Bootsektoren des Systems.Dieser Sektor der Festplatte beinhaltet den notwendigen Computercode um den Boot-Prozess zu starten.Wenn ein Virus den Boot-Sektor infiziert, könnte das Laufwerk unzugänglich werden und es könnte Ihnen nicht mehr möglich sein, Ihr System zu starten und auf Ihre Daten zuzugreifen.

  – **Nur neue oder geänderte Dateien scannen.** Indem nur neue und geänderte Dateien gescannt werden, können Sie die allgemeine Systemreaktionsfähigkeit mit minimalen Sicherheitsabstrichen erheblich verbessern.

- **Nach Keyloggern suchen.** Keylogger zeichnen auf, was Sie auf Ihrer Tastatur tippen, und schicken dann via Internet Berichte an Hacker.Der Hacker kann über diese gestohlenen Daten sensible Informationen erfahren, so wie Kontonummern und Passwörter und kann Sie zu seinem eigenen Profit verwenden.
- **Nach potenziell unerwünschten Anwendungen (PUA) scannen.** Eine potenziell unerwünschte Anwendung (PUA) ist ein Programm, das auf dem PC vermutlich nicht erwünscht ist und häufig in Verbindung mit Freeware installiert wurde. Diese Art von Programmen kann ohne Zustimmung des Benutzers installiert werden (wird auch als Adware bezeichnet) oder wird standardmäßig bei der Express-Installation mitinstalliert (werbeunterstützt). Diese Programme können Pop-up-Werbung anzeigen, unerwünschte Symbolleisten im Standard-Browser installieren oder Hintergrundprozesse ausführen und so den PC verlangsamen.

- **Prüfaktionen.** Abhängig vom gefundenen Dateityp werden folgende Aktionen automatisch ausgeführt:
  - **Standardaktion für infizierte Dateien.** Als infiziert eingestufte Dateien stimmen mit einer Malware-Signatur der Bitdefender Malware-Signaturen-Datenbank überein.Endpoint Security kann normalerweise den Malware-Code aus einer infizierten Datei entfernen und die ursprüngliche Datei rekonstruieren. Diesen Vorgang bezeichnet man als Desinfektion.

    Wenn eine infizierte Datei gefunden wird, versucht Endpoint Security automatisch, diese zu desinfizieren.Falls die Desinfizierung fehlschlägt, wird die Datei in die Quarantäne verschoben, um dort die Infizierung einzudämmen.

    Wichtig
    Bestimmte Malware-Typen können nicht desinfiziert werden, da die komplette Datei betroffen ist. In diesen Fällen wird die infizierte Datei von der Festplatte gelöscht.

  - **Standardaktion für verdächtige Dateien.** Dateien werden von der heuristischen Analyse als verdächtig klassifiziert.Da es sich bei B-HAVE um eine heuristische Analysetechnologie handelt, kann Endpoint Security nicht sicher sein, ob die Datei tatsächlich mit Malware infiziert ist.Verdächtige Dateien können nicht desinfiziert werden, da hierfür keine Desinfektionsroutine verfügbar ist.

    Wenn eine verdächtige Datei gefunden wird, wird den Benutzern der Zugriff auf diese Datei verwehrt, um eine potenzielle Infektion zu verhindern.

  Sie können die standardmäßigen Aktionen verändern, dies wird aber nicht empfohlen.Sie können für jeden Dateityp zwei Aktionen festlegen.Folgende Aktionen stehen zur Verfügung:

  Zugriff verweigern
  Zugriff auf infizierte Dateien verweigern.

Desinfizieren

Den Malware-Kode aus den entdeckten infizierten Dateien entfernen.Es wird empfohlen, dass dies immer die erste Aktion bleibt, die für infizierte Dateien durchgeführt wird.

Löschen

Infizierte Dateien ohne vorherige Benachrichtigung von der Festplatte löschen.Es wird empfohlen, die Anwendung dieser Aktion zu vermeiden.

In Quarant. versch.

Verschieben Sie infizierte Dateien von ihrem Speicherort in den Quarantäne-Ordner.Dateien in der Quarantäne können nicht ausgeführt oder geöffnet werden; aus diesem Grund besteht kein Infektionsrisiko.Sie können die Dateien in Quarantäne über die Quarantäne-Seite in der Konsole verwalten.

Active Virus Control Einstellungen

Active Virus Control von Bitdefender ist eine innovative und vorbeugende Erkennungstechnologie, die hoch entwickelte heuristische Methoden nutzt, um mögliche neue Bedrohungen in Echtzeit zu erkennen.

Die Active Virus Control überwacht kontinuierlich die auf Ihrem Computer laufenden Applikationen auf Malware-ähnliche Aktionen. Jede dieser Aktionen wird eingestuft, für jeden Prozess wird weiterhin eine Allgemeineinstufung erstellt.Wenn diese Gesamteinstufung einen bestimmten Grenzwert überschreitet, wird der entsprechende Prozess als schädlich eingestuft.Active Virus Control wird den erkannten Prozess automatisch blockieren.

Beachten Sie

Weitere Informationen erhalten Sie im Active-Virus-Control-Whitepaper auf unserer Website.

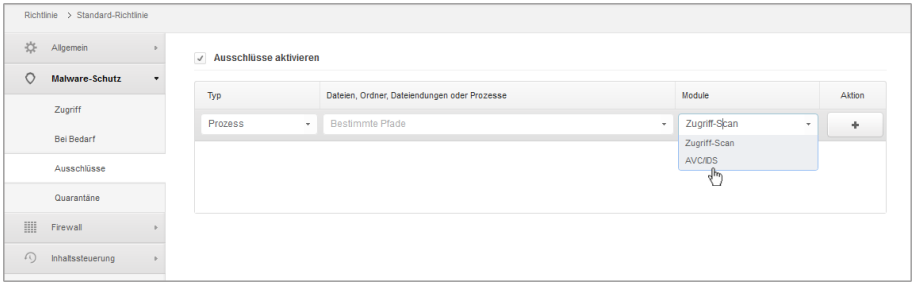
Konfiguration der Active Virus Control:

1. Über das Kästchen können Sie Active Virus Control aktivieren oder deaktivieren.Wenn Sie Active Virus Control deaktivieren, werden die Computer anfällig für unbekannte Malware.
2. Klicken Sie auf die Sicherheitsstufe, die Ihren Ansprüchen entspricht (aggressiv, normal oder tolerant).Orientieren Sie sich bei Ihrer Auswahl an den Beschreibungen auf der rechten Seite der Skala.

Beachten Sie

Je höher Sie die Sicherheitsstufe einstellen, desto weniger Anzeichen verdächtiger Aktivitäten braucht Active Virus Control, um einen Prozess zu melden. Dadurch steigt die Zahl der gemeldeten Anwendungen, aber auch die Wahrscheinlichkeit von Fehlalarmen (ungefährlichen Anwendungen, die dennoch als schädlich eingestuft wurden).

3. Sie sollten Ausschlussregeln für häufig genutzte oder bekannte Anwendungen erstellen, um Fehlalarme zu vermeiden (ungefährliche Anwendungen, die fälschlicherweise erkannt werden).Klicken Sie auf den Reiter Ausschlüsse und konfigurieren Sie die **AVC/IDS-Prozessausschlussregeln** für vertrauenswürdige Anwendungen.



Computer-Richtlinie - AVC/IDS Prozess Ausschluss

Bedarf-Scan

In diesem Bereich können Sie die Scan-Aufgaben zum Malware-Schutz konfigurieren, die dann regelmäßig nach einem von Ihnen festgelegten Zeitplan auf den Ziel-Computern ausgeführt werden.

Computer-Richtlinien - Bedarf-Scan-Aufgaben

Das Scannen wird im Hintergrund durchgeführt.Der Benutzer wird darüber informiert, dass der Scan-Prozess nur über ein Symbol ausgeführt werden kann, das in dem Benachrichtigungsfeld erscheint.

Obwohl nicht zwingend erforderlich, empfiehlt es sich, einen umfassenden System-Scan einzuplanen, der wöchentlich auf allen Computern ausgeführt wird.Regelmäßige Scans der Computer bieten vorbeugende Sicherheit. Nur so können Malware-Bedrohungen erkannt und blockiert werden, die den Echtzeitschutz unter Umständen umgangen haben.

Neben den regelmäßigen Scans können Sie auch eine automatische Erkennung und Prüfung von externen Speichermedien konfigurieren.

Scan-Aufgaben verwalten

Die Scan-Aufgaben-Tabelle informiert Sie über bestehende Scan-Aufgaben und enthält wichtige Informationen zu den einzelnen Aufgaben:

- Name und Art der Aufgabe.
- Zeitplan, anhand dessen die Aufgabe regelmäßig ausgeführt wird (Wiederholung).
- Zeitpunkt, zu dem die Aufgabe das erste Mal ausgeführt wurde.

Es gibt zwei Standard-Aufgaben für den System-Scan, deren Durchführung Sie nach Ihren Anforderungen konfigurieren können:

- **Quick Scan** setzt auf In-the-Cloud-Scans, um auf Ihrem System laufende Malware aufzuspüren.Die Ausführung eines Quick Scans dauert im Normalfall weniger als eine Minute und beansprucht nur einen Bruchteil der Systemressourcen, die ein normaler Virenscan in Anspruch nehmen würde.
- Der **Vollständige Scan** durchsucht den gesamten Computer nach allen Typen von Malware, die ein Sicherheitsrisiko darstellen, so z. B. Viren, Spyware, Adware, Rootkits usw.

Die Scan-Optionen der Standard-Scan-Aufgaben sind vorkonfiguriert und können nicht verändert werden.

Neben den Standard-Scan-Aufgaben (die Sie nicht löschen oder kopieren können) können Sie beliebig viele benutzerdefinierte Scan-Aufgaben erstellen. Bei einem benutzerdefinierten Scan können Sie die Orte, die gescannt werden sollen, selbst auswählen und die Scan-Optionen festlegen.

Um eine neue benutzerdefinierte Scan-Aufgabe zu erstellen und zu konfigurieren, klicken Sie auf die Schaltfläche + **Hinzufügen** auf der rechten Seite der Tabelle.Um die Einstellungen für eine bestehende Scan-Aufgabe zu ändern, klicken Sie auf den Namen der entsprechenden Aufgabe.Bitte rufen Sie das folgende Thema auf, um mehr über die Konfiguration der Aufgabeneinstellungen zu erfahren.

Um eine Aufgabe aus der Liste zu entfernen, klicken Sie auf die Schaltfläche − **Löschen** auf der rechten Seite der Tabelle.

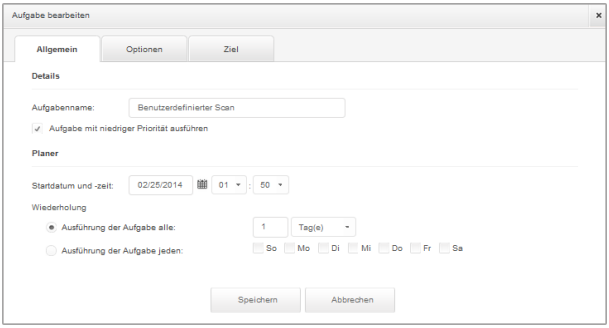
Konfiguration einer Prüfaufgabe

Die Einstellungen für die Scan-Aufgaben sind auf drei Reiter verteilt:

- **Allgemein**: Aufgabenname und Zeitplanung festlegen.
- **Optionen**: Scan-Profil für eine schnelle Konfiguration der Scan-Einstellungen auswählen und Einstellungen für benutzerdefinierte Scans festlegen.

- **Ziel**: Dateien und Ordner auswählen, die gescannt werden sollen.

Im Folgenden werden die Optionen vom ersten bis zum letzten Reiter beschrieben:



Computer-Richtlinien - Konfiguration der allgemeinen Einstellungen für Bedarf-Scan-Aufgaben

- **Details.** Geben Sie der Aufgabe einen eindeutigen Namen, der ihren Inhalt widerspiegelt.Wenn Sie einen Namen festlegen, berücksichtigen Sie das Ziel der Scan-Aufgabe und unter Umständen auch die Scan-Einstellungen.
- **Planer.** Verwenden Sie die Planungsoptionen, um den Scan-Zeitplan zu konfigurieren.Sie können festlegen, dass der Scan alle paar Stunden, Tage oder Wochen durchgeführt wird und Datum und Zeit des ersten Scans bestimmen.

  Bitte beachten Sie, dass die Computer eingeschaltet sein müssen, wenn der Termin fällig ist.Eine zeitgesteuerte Scan-Aufgabe kann nicht ausgeführt werden, wenn der Computer zu diesem Zeitpunkt nicht eingeschaltet ist, sich im Ruhezustand oder Energiesparmodus befindet oder wenn kein Benutzer angemeldet ist.In diesen Fällen wird der Scan bis zum nächsten Mal verschoben.

  ### Beachten Sie
  Der geplante Scan wird zur lokalen Zeit des Zielendpunkts ausgeführt. Wenn der geplante Scan zum Beispiel um 18:00 starten soll und der Endpunkt in einer anderen Zeitzone als das Control Center ist, wird der Scan um 18:00 Uhr (Endpunkt-Zeit) gestartet.

- **Scan-Optionen.** Klicken Sie auf die Sicherheitsstufe, die Ihren Ansprüchen entspricht (aggressiv, normal oder tolerant).Orientieren Sie sich bei Ihrer Auswahl an den Beschreibungen auf der rechten Seite der Skala.

  Je nach ausgewähltem Profil werden die Scan-Optionen im Bereich **Einstellungen** automatisch konfiguriert. Bei Bedarf können Sie diese aber auch im Detail konfigurieren.Markieren Sie dazu das Kästchen **Benutzerdefiniert** und gehen Sie dann zum Bereich **Einstellungen**.

Computer-Scan-Aufgabe

- **Dateitypen.** Verwenden Sie diese Optionen, um festzulegen, welche Dateien gescannt werden sollen.Sie können Endpoint Security so einrichten, dass Scans durchgeführt werden für alle Dateien (unabhängig von der Dateiendung), nur für Anwendungsdateien oder nur für bestimmte Dateiendungen, die Sie für gefährlich erachten.Das Scannen aller Dateien bietet den besten Schutz, während das Scannen nur von Anwendungen verwendet wird, um einen schnelleren Scan durchzuführen.

  Beachten Sie

  Anwendungsdateien sind weitaus anfälliger für Malware-Angriffe als andere Dateitypen.Weitere Informationen finden Sie unter „Liste der Anwendungsdateitypen“ (S. 145).

  Wenn Sie nur bestimmte Dateiendungen scannen lassen möchten, wählen Sie **Benutzerdefinierte Endungen** aus dem Menü, und geben Sie dann die Endungen in das Eingabefeld ein. Klicken Sie nach jeder Eingabe auf `Speichern`.

- **Archive.** Archive mit infizierten Dateien sind keine unmittelbare Bedrohung für die Systemsicherheit.Die Malware kann das System nur beeinflussen, wenn die infizierten Datei aus einem Archiv extrahiert und ohne aktivierten Echtzeitschutz ausgeführt wird.Wir empfehlen jedoch, diese Option zu nutzen, um jegliche potentiellen Bedrohungen aufzuspüren und zu entfernen, auch wenn es sich nicht um unmittelbare Bedrohungen handelt.

  Beachten Sie

  Das Scannen archivierter Dateien erhöht die Gesamt-Scandauer und erfordert mehr Systemressourcen.

  – **Inhalt von Archiven scannen.** Wählen Sie diese Option, wenn Sie archivierte Dateien nach Malware durchsuchen möchten.Sollten Sie sich zur Verwendung dieser Option entscheiden, können Sie die folgenden Optimierungsoptionen konfigurieren:

- **Archivgröße begrenzen auf (MB).** Sie können Sie die maximale Größe der Archive angeben, die gescannt werden sollen.Markieren Sie das entsprechende Kästchen und geben Sie die maximale Archivgröße in MB ein.
- **Maximale Archivtiefe (Ebenen).** Markieren Sie das entsprechende Kästchen und wählen Sie die maximale Archivtiefe aus dem Menü.Für optimale Leistung wählen Sie den niedrigsten Wert, für maximalen Schutz wählen Sie den höchsten Wert.

– **E-Mail-Archive scannen.** Wählen Sie diese Option, wenn Sie möchten, dass E-Mail-Dateien und E-Mail-Datenbanken (Dateiformate wie EML, MSG, PST, DBX, MBX, TBB usw.) gescannt werden.

Beachten Sie
Das Scannen von E-Mail-Archiven kann viele Ressourcen beansprucht und die Systemleistung beeinträchtigen.

- **Verschiedenes.** Markieren Sie die entsprechenden Kästchen, um die gewünschten Scan-Optionen zu aktivieren.
  - **Boot-Sektoren scannen.** Prüft die Bootsektoren des Systems.Dieser Sektor der Festplatte beinhaltet den notwendigen Computercode um den Boot-Prozess zu starten.Wenn ein Virus den Boot-Sektor infiziert, könnte das Laufwerk unzugänglich werden und es könnte Ihnen nicht mehr möglich sein, Ihr System zu starten und auf Ihre Daten zuzugreifen.
  - **Registry scannen.** Wählen Sie diese Option, um die Registry-Schlüssel zu scannen.Die Windows-Registry ist eine Datenbank, in der Konfigurationseinstellungen und Optionen für die Windows-Betriebssystemkomponenten sowie für die installierten Anwendungen gespeichert sind.
  - **Nach Rootkits suchen.** Wählen Sie diese Option, um nach Rootkits und Objekten zu suchen, die mit dieser Art von Software versteckt werden.
  - **Nach Keyloggern suchen.** Wählen Sie diese Option, wenn nach Keylogger-Software gesucht werden soll.
  - **Speicher scannen.** Wählen Sie diese Option, um Programme zu scannen, die im Speicher des Systems laufen.
  - **Cookies scannen.** Wählen Sie diese Option, um die Cookies zu scannen, die von Ihrem Browser auf dem Computer gespeichert werden.
  - **Nur neue und geänderte Dateien.** Indem nur neue und geänderte Dateien gescannt werden, können Sie die allgemeine Systemreaktionsfähigkeit mit minimalen Sicherheitsabstrichen erheblich verbessern.
  - **Nach potenziell unerwünschten Anwendungen (PUA) scannen.** Eine potenziell unerwünschte Anwendung (PUA) ist ein Programm, das auf dem PC vermutlich nicht erwünscht ist und häufig in Verbindung mit Freeware installiert wurde. Diese Art von

Programmen kann ohne Zustimmung des Benutzers installiert werden (wird auch als Adware bezeichnet) oder wird standardmäßig bei der Express-Installation mitinstalliert (werbeunterstützt). Diese Programme können Pop-up-Werbung anzeigen, unerwünschte Symbolleisten im Standard-Browser installieren oder Hintergrundprozesse ausführen und so den PC verlangsamen.

- **Aktionen.** Abhängig vom gefundenen Dateityp werden folgende Aktionen automatisch ausgeführt:
  - **Standardaktion für infizierte Dateien.** Als infiziert eingestufte Dateien stimmen mit einer Malware-Signatur der Bitdefender Malware-Signaturen-Datenbank überein.Endpoint Security kann normalerweise den Malware-Code aus einer infizierten Datei entfernen und die ursprüngliche Datei rekonstruieren. Diesen Vorgang bezeichnet man als Desinfektion.

    Wenn eine infizierte Datei gefunden wird, versucht Endpoint Security automatisch, diese zu desinfizieren.Falls die Desinfizierung fehlschlägt, wird die Datei in die Quarantäne verschoben, um dort die Infizierung einzudämmen.

    Wichtig
    Bestimmte Malware-Typen können nicht desinfiziert werden, da die komplette Datei betroffen ist. In diesen Fällen wird die infizierte Datei von der Festplatte gelöscht.

  - **Standardaktion für verdächtige Dateien.** Dateien werden von der heuristischen Analyse als verdächtig klassifiziert.Da es sich bei B-HAVE um eine heuristische Analysetechnologie handelt, kann Endpoint Security nicht sicher sein, ob die Datei tatsächlich mit Malware infiziert ist.Verdächtige Dateien können nicht desinfiziert werden, da hierfür keine Desinfektionsroutine verfügbar ist.

    Scan-Aufgaben sind standardmäßig so konfiguriert, dass verdächtigte Dateien ignoriert werden.Es könnte ratsam sein, die Standardaktion zu ändern, damit verdächtige Dateien in Quarantäne verschoben werden.Dateien in Quarantäne werden zu Analysezwecken in regelmäßigen Abständen an die Bitdefender-Labs geschickt.Sollten das Vorhandensein von Malware bestätigt werden, wird eine Signatur veröffentlicht, um das Entfernen der Malware zu ermöglichen.

  - **Standardaktion für Rootkits.** Rootkits sind spezielle Software-Wekzeuge, die verwendet werden, um Dateien vor dem Betriebssystem zu verbergen.Obwohl sie nicht zwangsläufig als schädlich anzusehen sind, werden Rootkits häufig genutzt, um Malware zu verbergen oder Eindringlinge im System zu tarnen.

    Erkannte Rootkits und versteckte Dateien werden standardmäßig ignoriert.

  Sie können die standardmäßigen Aktionen verändern, dies wird aber nicht empfohlen.Sie können eine zweite Aktion auswählen, für den Fall, dass die Erste fehlschlägt und außerdem verschiedene Aktionen für jede Kategorie.Wählen Sie aus den entsprechenden Menus die erste und zweite Aktion, die für jeden entdeckten Dateityp vorgenommen werden soll.Folgende Aktionen stehen zur Verfügung:

Keine Aktion ausführen
Für gefundene Dateien wird keine Aktion durchgeführt. Diese Dateien werden nur in das Scan-Protokoll aufgenommen.

Desinfizieren
Den Malware-Kode aus den entdeckten infizierten Dateien entfernen.Es wird empfohlen, dass dies immer die erste Aktion bleibt, die für infizierte Dateien durchgeführt wird.

Löschen
Infizierte Dateien ohne vorherige Benachrichtigung von der Festplatte löschen.Es wird empfohlen, die Anwendung dieser Aktion zu vermeiden.

In Quarant. versch.
Verschieben Sie infizierte Dateien von ihrem Speicherort in den Quarantäne-Ordner.Dateien in der Quarantäne können nicht ausgeführt oder geöffnet werden; aus diesem Grund besteht kein Infektionsrisiko.Sie können die Dateien in Quarantäne über die Quarantäne-Seite in der Konsole verwalten.

- **Scan-Ziel.** Fügen Sie der Liste alle Pfade hinzu, die auf den Ziel-Computern gescannt werden sollen.

  Um eine neue Datei oder einen neuen Ordner zum Scan hinzuzufügen:

  1. Wählen Sie einen vorgegebenen Speicherort aus dem Klappmenü, oder geben Sie **Bestimmte Pfade** ein, die sie scann lassen möchten.
  2. Geben Sie den Pfad des zu scannenden Objekts im Bearbeitungsfeld ein.
     - Wenn Sie einen vorgegebenen Pfad ausgewählt haben, vervollständigen Sie den Pfad nach Bedarf.Um zum Beispiel den gesamten Ordner `Programme` zu scannen, müssen Sie lediglich den entsprechenden vorgegebenen Pfad aus dem Klappmenü auswählen.Um einen bestimmten Order im Ordner `Programme` zu scannen, müssen Sie den Pfad vervollständigen indem Sie einen Backslash (\) und den Namen des Ordners hinzufügen.
     - Wenn Sie **Bestimmte Pfade** ausgewählt haben, geben Sie den vollständigen Pfad des Objektes ein, das gescannt werden soll.Es empfiehlt sich, (nach Möglichkeit) Systemvariablen zu verwenden, um sicherzustellen, dass der Pfad auf allen Computern gültig ist.
  3. Klicken Sie auf den entsprechenden + **Hinzufügen**-Link.

  Um einen bestehenden Pfad zu bearbeiten, klicken Sie ihn an.Um einen Server aus der Liste zu entfernen, bewegen Sie den Mauszeiger darüber, und klicken Sie auf die entsprechende − **Löschen**-Schaltfläche.

- **Ausschlüsse.** Sie können entweder die globalen Ausschlüsse für einen bestimmten Scan verwenden oder konkrete Ausschlüsse für jeden Scan selbst festlegen.Weitere Informationen finden Sie unter „Ausschlüsse“ (S. 93).

Geräte-Scan

Sie können festlegen, dass Endpoint Security externe Speichermedien automatisch erkennt und scannt, sobald diese mit dem Computer verbunden werden.Entdeckte Geräte fallen in eine dieser Kategorien:

- CDs/DVDs
- USB-Speichergeräte, sowie Flashstifte und externe Festplatten
- Zugeordnete Netzlaufwerke
- Geräte mit mehr als einer bestimmten Menge gespeicherter Daten.

Bei den Geräte-Scans werden als infiziert erkannte Dateien automatisch desinfiziert oder, falls eine Desinfektion nicht möglich ist, in die Quarantäne verschoben.Bitte beachten Sie, dass für infizierte Dateien auf CDs/DVDs oder auf zugeordneten Netzlaufwerken mit schreibgeschütztem Zugriff keine Aktionen durchgeführt werden können.

Beachten Sie
Der Benutzer kann während eines Geräte-Scans weiterhin auf alle Daten auf dem Gerät zugreifen.

Wenn Warnfenster unter **Allgemein > Anzeige** aktiviert wurden, wird der Benutzer zunächst gefragt, ob ein erkanntes Gerät gescannt werden soll. Es erfolgt kein automatischer Scan.

Wenn ein Geräte-Scan beginnt:

- Ein Benachrichtigungsfenster informiert den Benutzer über den Geräte-Scan, vorausgesetzt das Benachrichtigungsfenster unter **Allgemein > Anzeige** aktiviert wurden.
- In der Task-Leiste wird ein Scan-Symbol angezeigt .Mit einem Doppelklick auf dieses Symbol kann der Benutzer das Scan-Fenster öffnen und den Scan-Fortschritt anzeigen.

Nach Abschluss des Scans muss der Benutzer eventuell erkannte Bedrohungen überprüfen.

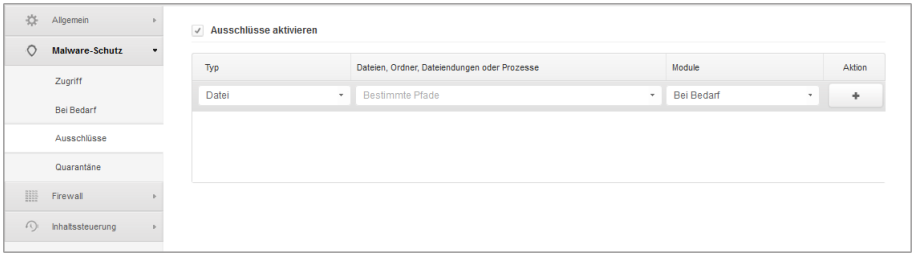
Wählen Sie die **Geräte-Scan**-Option, um die automatische Erkennung und Prüfung von Speichergeräten zu aktivieren. Mit den folgenden Optionen können Sie den Geräte-Scan für jeden Gerätetyp individuell festlegen:

- **CD-/DVD-Datenträger**
- **USB-Speichergeräte**
- **Zugeordnete Netzlaufwerke**
- **Keine Geräte scannen, die mehr Daten gespeichert haben als (MB)**. Mit dieser Option können Sie die Scans von erkannten Geräten automatisch überspringen, wenn die darauf gespeicherten Daten einen festgelegten Umfang überschreiten. Geben Sie das Grössenlimit (in MB) in das entsprechende Feld ein. Null bedeutet, dass kein Grössenlimit angegeben wurde.

Beachten Sie
Diese Option betrifft nur CDs/DVDs und USB Speichergeräte.

Ausschlüsse

In diesem Bereich können Sie die Scan-Ausschlussregeln konfigurieren. Ausschlüsse können auf Zugriff-Scans, Bedarf-Scans oder beide Scan-Arten angewendet werden. Je nach ausgeschlossenem Objekt gibt es vier Ausschlussarten:



Computer-Richtlinien - Malware-Schutz-Ausschlüsse

- **Dateiausschlüsse:** Nur die angegebene Datei wird vom Scan ausgeschlossen.
- **Ordnerausschlüsse:** Alle Dateien in dem angegebenen Ordner und alle Unterordner werden vom Scan ausgeschlossen.
- **Ausschlüsse für Dateiendungen:** Alle Dateien mit der angegebenen Dateiendung werden vom Scan ausgeschlossen.
- **Prozessausschlüsse:** Jedes Objekt, auf das von dem ausgeschlossenen Prozess zugegriffen wird, wird ebenfalls vom Scan ausgeschlossen.Sie können auch für Active Virus Control und das Angriffserkennungssystem (IDS) Prozessausschlüsse festlegen.

Wichtig
Scan-Ausschlüsse sollten unter besonderen Umständen eingesetzt werden oder wenn dies von Microsoft oder Bitdefender empfohlen wird.Eine aktualisierte Liste der von Microsoft empfohlenen Ausschlüsse finden Sie in diesem Artikel.Sollten Sie eine EICAR-Testdatei verwenden, um den Malware-Schutz regelmäßig zu überprüfen, sollten Sie diese von den Zugriff-Scans ausschließen.

Über das Kästchen **Ausschlüsse aktivieren** können Sie Ausschlüsse aktivieren oder deaktivieren.

Um eine Ausschlussregel zu konfigurieren:

1. Wählen Sie die Art des Ausschlusses aus dem Menü.
2. Je nach Ausschlussart geben Sie das auszuschließende Objekt wie folgt an:

- **Ausschlüsse für Dateiendungen.** Geben Sie mindestens eine Dateiendung ein (Mehrfachnenneungen mit Semikolon ";" getrennt), die vom Scan ausgeschlossen werden sollen. Sie können die Endungen dabei mit oder ohne den führenden Punkt eingeben.Geben Sie zum Beispiel die Endung `txt` ein, um Textdateien auszuschließen.

  Beachten Sie
  Bevor Sie Dateiendungen ausschließen, sollten Sie sich eingehend darüber informieren, welche Endungen häufig im Visier von Malware stehen und welche nicht.

- **Datei-, Ordner- und Prozessausschlüsse.** Sie müssen den Pfad des ausgeschlossenen Objekts auf den Ziel-Computern angeben.

  a. Im Menü können Sie entweder einen vorgegebenen Pfad oder die Option **Bestimmte Pfade** auswählen.

  b. Wenn Sie einen vorgegebenen Pfad ausgewählt haben, vervollständigen Sie den Pfad nach Bedarf.Um zum Beispiel den gesamten Ordner `Programme` auszuschließen, müssen Sie lediglich den entsprechenden vorgegebenen Pfad aus dem Menü auswählen.Um einen bestimmten Order im Ordner `Programme` auszuschließen, müssen Sie den Pfad vervollständigen indem Sie einen Backslash (\) und den Namen des Ordners hinzufügen. Bei Prozessausschlüssen müssen Sie auch den Namen der ausführbaren Datei der Anwendung angeben.

  c. Wenn Sie **Bestimmte Pfade** ausgewählt haben, geben Sie den vollständigen Pfad des Objektes ein, das ausgeschlossen werden soll.Es empfiehlt sich, (nach Möglichkeit) Systemvariablen zu verwenden, um sicherzustellen, dass der Pfad auf allen Computern gültig ist.

3. Wählen Sie die Scan-Arten aus, für die die Regel angewendet werden soll.Einige Ausschlüsse sind möglicherweise nur für Zugriff-Scans von Bedeutung, einige wiederum nur für Bedarf-Scans und andere empfehlen sich unter Umständen für beide Arten von Scans.Sie können für die Zugriff-Scans, Active Virus Control und das Angriffserkennungssystem (IDS) Prozessausschlüsse festlegen.

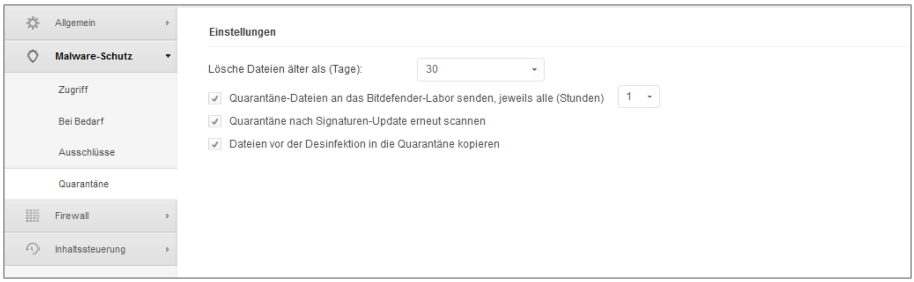
   Beachten Sie
   Bitte beachten Sie, dass Ausschlüsse für Bedarf-Scans bei Kontext-Scans NICHT berücksichtigt werden.Klicken Sie mit der rechten Maustaste auf eine Datei oder einen Ordner und wählen Sie **Mit Endpoint Security von Bitdefender scannen**, um einen Kontext-Scan zu starten.

4. Klicken Sie auf den Button **Hinzufügen**.Die neue Regel wird der Liste hinzugefügt.

Um eine Regel aus der Liste zu löschen, klicken Sie auf den entsprechenden **Löschen**-Link.

Quarantäne

In diesem Bereich können Sie die Quarantäne-Einstellungen konfigurieren.



Computer-Richtlinien - Quarantäne

Sie können Endpoint Security so einstellen, dass er automatisch die folgenden Aktionen ausführt:

- **Delete files older than (days).** Standardmäßig werden Dateien in der Quarantäne, die älter als 30 Tage sind, automatisch gelöscht. Um dieses Intervall zu ändern, wählen Sie im Menü eine andere Option aus.
- **Dateien in der Quarantäne jede Stunde an das Bitdefender-Virenlabor senden.** Lassen Sie diese Option aktiviert, um Dateien in Quarantäne automatisch an die Bitdefender-Labors zu senden. Sie können das Intervall einstellen, in dem in die Quarantäne verschobene Dateien gesendet werden (standardmäßig 1 Stunde). Die Beispieldateien werden dann von den Bitdefender-Malware-Forschern analysiert. Sollten das Vorhandensein von Malware bestätigt werden, wird eine Signatur veröffentlicht, um das Entfernen der Malware zu ermöglichen.

  Die Dateien in Quarantäne werden standardmäßig einmal pro Stunde automatisch an die Bitdefender-Labors geschickt. Um dieses Intervall zu ändern, wählen Sie im Menü eine andere Option aus.
- **Quarantäne nach Signaturen-Update erneut scannen.** Lassen Sie diese Option aktiviert, um Dateien in Quarantäne automatisch nach jedem Update der Malware-Signaturen zu scannen. Gesäuberte Dateien werden automatisch an ihren Ursprungsort zurück gelegt.
- **Dateien vor der Desinfektion in die Quarantäne kopieren.** Aktivieren Sie diese Option, um im Falle von Fehlalarmen Datenverlust zu vermeiden, indem als infiziert erkannte Dateien vor der Desinfektion in die Quarantäne kopiert werden. Später können Sie unbedenkliche Dateien von der Seite **Quarantäne** aus wiederherstellen.

7.2.3. Firewall

Die Firewall schützt Ihren Computer vor nicht autorisierten Zugriffsversuchen bei eingehendem und ausgehendem Datentransfer.

Die Funktionsweise der Firewall basiert auf Netzwerkprofilen. Die Profile wiederum basieren auf Vertrauensstufen, die für jedes Netzwerk definiert werden müssen.

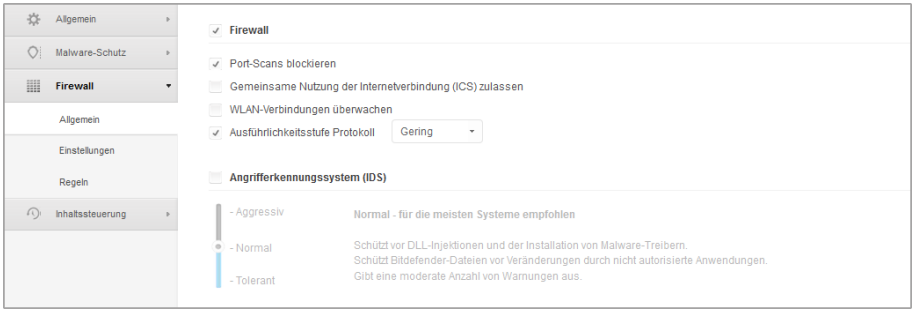
Jedes Mal, wenn eine neue Verbindung hergestellt wird, erkennt die Firewall sie und vergleicht die Adapterinforationen dieser Verbindung mit den Informationen der bestehenden Profile, um dann das passende Profil auf die Verbindung anzuwenden. Nähere Informationen zur Anwendung der Profile finden Sie unter Netzwerkeinstellungen.

Die Einstellungen sind in die folgenden Bereiche eingeteilt:

- Allgemein
- Einstellungen
- Regeln

Allgemein

In diesem Bereich können Sie die Bitdefender-Firewall aktivieren und deaktivieren und die allgemeinen Einstellungen konfigurieren.



Computer-Richtlinien - Allgemeine Firewall-Einstellungen

- **Firewall.** Über das Kästchen können Sie die Firewall aktivieren oder deaktivieren.Wenn Sie den Firewall-Schutz deaktivieren, werden die Computer anfällig für Angriffe über das Netzwerk und das Internet.
- **Port-Scans blockieren.** Portscans werden von Hackern verwendet, um herauszufinden, welche Ports auf einem Computer geöffnet sind.Wenn Sie dann einen unsicheren Port finden, können Sie in den Computer eindringen.
- **Gemeinsame Nutzung der Internetverbindung (ICS) zulassen.** Wählen Sie diese Option, damit die Firewall die gemeinsame Nutzung der Internetverbindung zulässt.

Beachten Sie
Diese Option aktiviert nicht automatisch die gemeinsame Nutzung der Internetverbindung (Internet Connection Sharing) auf dem Computer des Benutzers.

- **WLAN-Verbindungen überwachen.** Endpoint Security kann Benutzer in einem Drahtlosnetzwerk über neu zum Netzwerk hinzugekommene Computer informieren.Wählen Sie diese Option aus, um solche Benachrichtigungen auf dem Bildschirm des Benutzers anzuzeigen.
- **Ausführlichkeitsstufe Protokoll.** Endpoint Security erstellt ein Protokoll der Ereignisse, die im Zusammenhang mit der Nutzung des Firewall-Moduls auftreten (Aktivieren/Deaktivieren der Firewall, Blockieren des Datenverkehrs, Einstellungsänderungen) und die durch Aktivitäten erzeugt wurden, die von diesem Modul erkannt wurden (Port-Scans, regelbasiertes Blockieren von Verbindungsversuchen und Datenverkehr).Wählen Sie unter **Ausführlichkeitsstufe Protokoll** eine Option aus, um festzulegen, wie viele Informationen im Protokoll enthalten sein sollen.
- **Angriffserkennungssystem (IDS).** Das Angriffserkennungssystem (IDS) überwacht das System und sucht nach verdächtigen Aktivitäten (so zum Beispiel unerlaubte Versuche, Bitdefender-Dateien zu verändern, DLLs einzuschleusen, Tastaturanschläge zu protokollieren, etc.).

  Um das Angriffserkennungssystem (IDS) zu konfigurieren:

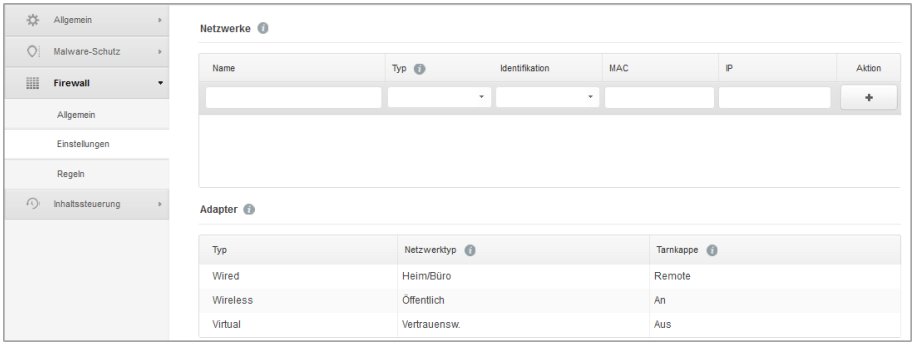
  1. Über das Kästchen können Sie das Angriffserkennungssystem (IDS) aktivieren oder deaktivieren.
  2. Klicken Sie auf die Sicherheitsstufe, die Ihren Ansprüchen entspricht (aggressiv, normal oder tolerant).Orientieren Sie sich bei Ihrer Auswahl an den Beschreibungen auf der rechten Seite der Skala.

  Um zu verhindern, dass eine harmlose Anwendung vom Angrifferkennungssystem erkannt wird, fügen Sie eine **AVC/IDS-Prozessausschlussregel** für diese Anwendung unter **Malware-Schutz > Ausschlüsse** hinzu.

Einstellungen

Je nach Netzwerkart wendet die Firewall automatisch ein Profil an. Sie können die generischen Profile, die angewendet werden sollen, je nach Art des Adapters festlegen und Profile speziell für Unternehmensnetzwerke festlegen.Die Einstellungen sind in den folgenden Tabellen sortiert:

- Netzwerke
- Adapter



Computer-Richtlinien - Firewall-Einstellungen

Netzwerkeinstellungen

Damit die Firewall ordnungsgemäß funktioniert, muss der Administrator die Netzwerke, die verwaltet werden sollen, in der Tabelle **Netzwerke** definieren.Die Felder der Tabelle **Netzwerke** werden folgend beschrieben:

- **Name.** Ein Name, anhand dessen der Administrator das Netzwerk in der Liste identifizieren kann.
- **Typ.** Hier können Sie aus dem Menü die Art des Profils wählen, das dem Netzwerk zugewiesen wird.

  Endpoint Security wendet automatisch eins von vier Firewall-Profilen auf jede erkannte Netzwerkverbindung an, um die grundlegenden Datenverkehrfilteroptionen festzulegen.Es gibt die folgenden Firewall-Profile:

  - **Vertrauenswürdiges** Netzwerk.Deaktiviert die Firewall für den entsprechenden Adapter.
  - **Heim-/Büronetzwerk**.Datenverkehr zwischen Computern im lokalen Netzwerk in beide Richtungen zulassen.
  - **Öffentliches** Netzwerk.Sämtlicher Datenverkehr wird gefiltert.
  - **Nicht vertrauenswürdiges** Netzwerk.Der Netzwerk- und Internet-Datenverkehr über den entsprechenden Adapter wird vollständig blockiert.
- **Identifikation.** Wählen Sie aus dem Menü die Methode, nach der Endpoint Security ein Netzwerk identifiziert. Es gibt drei Methoden zur identifizierung: **DNS**, **Gateway** und **Netzwerk**.
- **MAC.** In diesem Feld können Sie die MAC-Adresse eines bestimmten DNS-Servers angeben.

Beachten Sie
Dieses Feld muss ausgefüllt werden, wenn Sie die Identifizierungsmethode DNS wählen.

- **IP.** In diesem Feld können Sie bestimmte IP-Adressen in einem Netzwerk definieren. Sie können auch ein ganzes Sub-Netzwerk über eine Maske definieren.

Nachdem Sie ein Netzwerk definiert haben, klicken Sie auf die Schaltfläche **Hinzufügen** auf der rechten Seite der Tabelle, um das Netzwerk der Liste hinzuzufügen.

Adaptereinstellungen

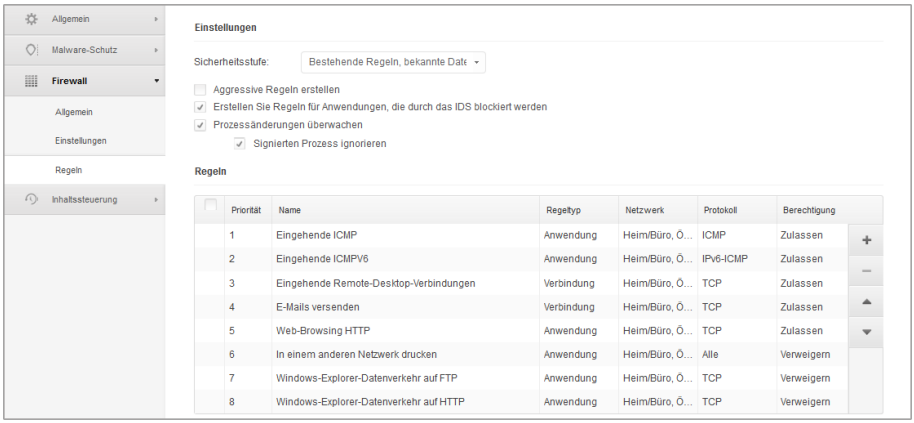
Wenn ein Netzwerk erkannt wird, das nicht in der Tabelle **Netzwerke** definierte ist, erkennt Endpoint Security die Art des Netzwerkadapters und wendet ein passendes Profil auf die Netzwerkverbindung an.Die Felder der Tabelle **Adapter** werden folgend beschrieben:

- **Typ.** Zeigt die Art des Netzwerkadapters an. Endpoint Security kann drei verschiedene vordefinierte Adaptertypen erkennen: **Kabelgebunden**, **Kabellos** und **Virtuell** (Virtuelles Privates Netzwerk).
- **Netzwerktyp.** Beschreibt das Netzwerkprofil, das einem bestimmten Adaptertyp zugewiesen ist. Die Netzwerktyen sind im Abschnitt Netzwerkeinstellungen beschrieben. Wenn Sie auf das Netzwerktypfeld klicken, können Sie die Einstellung ändern. Wenn Sie **Windows entscheiden lassen** wählen, wendet Endpoint Security für jede neue Netzwerkverbindung, die erkannt wird, nachdem die Richtlinie angewendet wurde, ein Firewall-Profil an, das auf der Netzwerkklassifikation in Windows basiert. Die Einstellungen der Tabelle **Adapter** werden dabei ignoriert.

  Wenn die Erkennung auf der Basis des Windows-Netzwerkmanagers fehlschlägt, wird eine einfache Erkennung versucht. Ein generisches Profil wird angewendet, in dem der Netzwerktyp **Öffentlich** zugrundegelegt und die Tarnkappeneinstellung auf **Ein** gestellt wird. Wenn die IP-Adresse der Domain, in der der Computer gefunden wurde, in einem der mit dem Adapter assoziierten Netzwerke liegt, wird die Vertrauensstufe **Heim/Büro** zugrundegelegt und die Tarnkappeneinstellungnstellung auf **Entfernt Ein** gestellt. Wenn der Computer nicht in einer Domain ist, wird diese Bedingung ignoriert.
- **Tarnkappe.** Macht Ihren Computer im Netzwerk oder Internet unsichtbar für schädliche Software und Hacker.Konfigurieren Sie den Tarnkappenmodus nach Bedarf für jeden Adaptertypen, indem Sie eine der folgenden Optionen auswählen:
  - **An.** Der Computer ist sowohl im lokalen Netzwerk als auch im Internet unsichtbar.
  - **Aus.** Jeder Benutzer in lokalen Netzwerk oder dem Internet kann den Computer anpingen oder erkennen.
  - **Remote.** Der Computer kann nicht über das Internet erkannt werden.Jeder Benutzer im lokalen Netzwerk kann den Computer anpingen oder erkennen.

Regeln

In diesem Bereich können Sie den Netzwerkzugriff für Anwendungen und die Firewall-Regeln für den Datenverkehr festlegen.Bitte beachten Sie, dass die verfügbaren Einstellungen nur auf die **Heim/Büro**- oder **Öffentlichen** Firewall-Profile angewendet werden können.



Computer-Richtlinien - Firewall-Regeleinstellungen

Einstellungen

Sie können die folgenden Einstellungen vornehmen:

- **Sicherheitsstufe.** Die ausgewählte Sicherheitsstufe definiert die Firewall-Entscheidungslogik, die verwendet wird, wenn Anwendungen den Zugriff auf Netzwerk- oder Internet-Dienste anfordern.Die folgenden Optionen sind verfügbar:

  Bestehende Regeln, sonst zulassen
  Bestehende Firewall-Regeln anwenden und alle weiteren Verbindungsversuche automatisch zulassen.Für jeden neuen Verbindungsversuch wird eine Regel angelegt und zum Regelsatz hinzugefügt.

  Bestehende Regeln und nachfragen
  Bestehende Firewall-Regeln anwenden und den Benutzer für alle weiteren Verbindungsversuche zur Auswahl einer Aktion auffordern.Ein Warnfenster mit detaillierten Informationen über den unbekannten Verbindungsversuch wird auf dem Bildschirm des Benutzers angezeigt.Für jeden neuen Verbindungsversuch wird eine Regel angelegt und zum Regelsatz hinzugefügt.

  Bestehende Regeln, sonst verweigern
  Bestehende Firewall-Regeln anwenden und alle weiteren Verbindungsversuche automatisch verweigern.Für jeden neuen Verbindungsversuch wird eine Regel angelegt und zum Regelsatz hinzugefügt.

Bestehende Regeln, bekannte Dateien, sonst zulassen
Bestehende Firewall-Regeln anwenden, die Verbindungsversuche von bekannten Anwendungen automatisch zulassen und alle weiteren unbekannten Verbindungsversuche automatisch zulassen.Für jeden neuen Verbindungsversuch wird eine Regel angelegt und zum Regelsatz hinzugefügt.

Bestehende Regeln, bekannte Dateien und nachfragen
Bestehende Firewall-Regeln anwenden, die Verbindungsversuche von bekannten Anwendungen automatisch zulassen und den Benutzer für alle weiteren unbekannten Verbindungsversuche zur Auswahl einer Aktion auffordern.Ein Warnfenster mit detaillierten Informationen über den unbekannten Verbindungsversuch wird auf dem Bildschirm des Benutzers angezeigt.Für jeden neuen Verbindungsversuch wird eine Regel angelegt und zum Regelsatz hinzugefügt.

Bestehende Regeln, bekannte Dateien, sonst verweigern
Bestehende Firewall-Regeln anwenden, die Verbindungsversuche von bekannten Anwendungen automatisch zulassen und alle weiteren unbekannten Verbindungsversuche automatisch verweigern.Für jeden neuen Verbindungsversuch wird eine Regel angelegt und zum Regelsatz hinzugefügt.

Beachten Sie

Bekannte Dateien sind eine Sammlung von sicheren und vertrauenswürdigen Anwendungen, die von Bitdefender zusammengestellt und fortlaufend gepflegt wird.

- **Aggressive Regeln erstellen.** Wenn diese Option aktiviert ist, werden für jeden Prozess, der die Anwendung öffnet, die Zugriff auf das Netzwerk oder das Internet anfordert, von der Firewall Regeln erstellt.
- **Erstellen Sie Regeln für Anwendungen, die durch das IDS blockiert werden.** Wenn diese Option ausgewählt ist, erstellt die Firewall jedes Mal, wenn das Angriffserkennungssystem eine Anwendung blockiert, automatisch eine **Verweigern**-Regel.
- **Prozessänderungen überwachen.** Wählen Sie diese Option, wenn Sie möchten, dass jede Anwendung, die sich mit dem Internet verbinden möchte, darauf überprüft wird, ob sie seit der Festlegung der Regel für ihren Internetzugriff verändert wurde.Falls die Anwendung geändert wurde, wird eine neue Regel in Übereinstimmung mit dem aktuellen Sicherheitsstufe angelegt.

Beachten Sie

Normalerweise werden Anwendungen durch Updates verändert.Es kann aber auch sein, dass eine Anwendung durch Malware verändert wird um den lokalen Computer oder andere Computer in dem Netzwerk zu infizieren.

Signierte Anwendungen sind in normalerweise vertrauenswürdig und haben einen höheren Sicherheitsgrad.Wählen Sie **Signierten Prozess ignorieren**, um veränderten signierten Anwendungen automatisch die Verbindung mit dem Internet zu erlauben.

Regeln

In der Regeltabelle werden die aktuellen Firewall-Regeln mit wichtigen Informationen zu den einzelnen Regel angezeigt:

- Name der Regel oder Anwendung, auf die sie sich bezieht.
- Protokoll, auf das die Regel angewendet werden soll.
- Aktion der Regel (Pakete zulassen oder verweigern).
- Für die Regel verfügbare Aktionen.
- Regelpriorirät.

Beachten Sie

Diese Firewall-Regeln werden ausdrücklich von der Richtlinie umgesetzt.Zusätzliche Regeln werden unter Umständen auf Computern als Folge der Anwendung von Firewall-Einstellungen konfiguriert.

Eine Reihe von Standardregeln für die Firewall helfen Ihnen dabei, häufig genutzte Datenverkehrstypen ohne viel Aufwand zuzulassen oder zu verweigern.Wählen Sie die gewünschte Option aus dem **Berechtigung**-Menü.

Eingehende ICMP / ICMPv6
ICMP- / ICMPv6-Nachrichten zulassen oder verweigern.ICMP-Nachrichten werden häufig von Hackern für Angriffe auf Computer-Netzwerke genutzt.Standardmäßig wird diese Art Datenverkehr nicht zugelassen.

Eingehende Remote-Desktop-Verbindungen
Den Zugriff anderer Computer über Remote-Desktop-Verbindungen zulassen oder verweigern.Standardmäßig wird diese Art Datenverkehr zugelassen.

E-Mails versenden
Versand von E-Mails über SMTP zulassen oder verweigern.Standardmäßig wird diese Art Datenverkehr zugelassen.

Web-Browsing HTTP
HTTP-Browsing zulassen oder verweigern.Standardmäßig wird diese Art Datenverkehr zugelassen.

In einem anderen Netzwerk drucken
Den Zugriff auf Drucker in anderen lokalen Netzwerken erlauben oder verweigern.Standardmäßig wird diese Art Datenverkehr nicht zugelassen.

Windows-Explorer-Datenverkehr auf HTTP / FTP

HTTP- und FTP-Datenverkehr aus Windows Explorer heraus zulassen oder verweigern.Standardmäßig wird diese Art Datenverkehr nicht zugelassen.

Neben den Standardregeln können Sie weitere Firewall-Regeln für andere auf den Computern installierte Anwendungen erstellen.Diese Konfiguration bleibt jedoch Administratoren vorbehalten, die über umfangreiche Netzwerkkenntnisse verfügen.

Um eine neue Regel zu erstellen und zu konfigurieren, klicken Sie auf die Schaltfläche + **Hinzufügen** auf der rechten Seite der Tabelle.Bitte rufen Sie das folgende Thema auf, um weitere Informationen zu erhalten.

Um eine Regel aus der Liste zu entfernen, klicken Sie auf die entsprechende Schaltfläche − **Löschen** auf der rechten Seite der Tabelle.

Beachten Sie
Sie können die Standard-Firewall-Regeln weder löschen noch bearbeiten.

Benutzerdefinierte Regeln konfigurieren

Sie können zwei Arten von Firewall-Regeln konfigurieren:

- **Anwendungsbasierte Regeln.** Diese Regeln gelten für bestimmte Programme auf den Client-Computern.
- **Verbindungbasierte Regeln.** Diese Regeln gelten für alle Anwendungen oder Dienste, die eine bestimmte Verbindung nutzen.

Um eine neue Regel zu erstellen und zu konfigurieren, klicken Sie auf die Schaltfläche + **Hinzufügen** auf der rechten Seite der Tabelle, und wählen Sie den gewünschten Regeltyp aus dem Menü.Um eine bestehende Regel zu bearbeiten, klicken Sie auf den Namen der Regel.

Die folgenden Einstellungen können konfiguriert werden:

- **Name der Regel.** Geben Sie den Namen ein, unter dem die Regel in der Regeltabelle aufgeführt werden soll (so zum Beispiel den Namen der Anwendung, auf die die Regel angewendet wird).
- **Anwendungspfad** (nur für anwendungsbasierte Regeln).Sie müssen den Pfad der ausführbaren Anwendungsdatei auf den Ziel-Computern angeben.
  - Wählen Sie einen vorgegebenen Pfad aus dem Menü und vervollständigen Sie den Pfad nach Bedarf.So müssen Sie für eine Anwendung, die im Ordner `Programme` installiert ist, den Ordner `%Programme%` auswählen und den Pfad vervollständigen, indem Sie einen Backslash (\) und den Namen des Anwendungsordners hinzufügen.
  - Geben Sie den vollständigen Pfad in das Bearbeitungsfeld ein.Es empfiehlt sich, (nach Möglichkeit) Systemvariablen zu verwenden, um sicherzustellen, dass der Pfad auf allen Computern gültig ist.

- **Befehlszeile** (nur für anwendungsbasierte Regeln).Wenn die Regel nur angewendet werden soll, wenn die ausgewählte Anwendung mit einem bestimmten Befehl in der Windows-Befehlszeile geöffnet wird, geben Sie den entsprechenden Befehl in das Bearbeitungsfeld ein. Andernfalls lassen Sie das Feld frei.
- **Anwendungs-MD5** (nur für anwendungsbasierte Regeln).Wenn die Regel die Integrität der Dateidaten der Anwendung anhand des MD5-Hashcodes überprüfen soll, geben Sie ihn in das Bearbeitungsfeld ein. Lassen Sie das Feld ansonsten frei.
- **Lokale Adresse.** Geben Sie die lokale IP-Adresse und den Port an, auf den die Regel angewendet werden soll.Wenn Sie mehr als einen Netzwerkadapter haben, können sie die Markierung im Kästchen **Alle** aufheben und eine bestimmte IP-Adresse eingeben.Um Verbindungen über einen bestimmten Port oder Port-Bereich zu filtern, deaktivieren Sie das Kästchen **Alle** und geben Sie den gewünschten Port oder Port-Bereich in das entsprechende Feld ein.
- **Remote-Adresse.** Geben Sie die Remote-IP-Adresse und den Port an, auf den die Regel angewendet werden soll.Um den ein- und ausgehenden Datenverkehr auf einem bestimmten Computer zu filtern, deaktivieren Sie das Kästchen **Alle** und geben Sie seine IP-Adresse ein.
- **Regel nur für direkt verbundene Computer anwenden.** Sie können den Zugriff anhand der MAC-Adresse filtern.
- **Protokoll.** Wählen Sie das IP-Protokoll, auf das die Regel angewendet werden soll.
  - Wenn Sie möchten, dass die Regel für alle Protokolle angewendet wird, wählen Sie **Alle**.
  - Wenn Sie möchten, dass die Regel für TCP-Protokolle angewendet wird, wählen Sie **TCP**.
  - Wenn Sie möchten, dass die Regel für UDP-Protokolle angewendet wird, wählen Sie **UDP**.
  - Wenn die Regeln für ein bestimmtes Protokoll gelten soll, wählen Sie das gewünschte Protokoll aus dem Menü **Sonstige**.

Beachten Sie

Die Nummern von IP-Protokollen werden von der Internet Assigned Numbers Authority (IANA) zugewiesen.Die komplette Liste zugewiesener Nummern von IP-Protokollen finden Sie unter http://www.iana.org/assignments/protocol-numbers.

- **Richtung.** Wählen Sie die Datenverkehrsrichtung an, auf die die Regel angewendet werden soll.

Richtung	Beschreibung
Ausgehend	Die Regel bezieht sich nur auf den ausgehenden Datenverkehr.

Richtung	Beschreibung
Eingehend	Die Regel bezieht sich nur auf den eingehenden Datenverkehr.
Beides	Die Regel findet in beiden Richtungen Anwendung.

- **IP-Version.** Wählen Sie die IP-Version (IPv4, IPv6 oder andere), auf die die Regel angewendet werden soll.
- **Netzwerk.** Wählen Sie den Netzwerktyp aus, auf den die Regel angewendet werden soll.
- **Berechtigung.** Wählen Sie eine der verfügbaren Erlaubnis-Optionen:

Berechtigung	Beschreibung
Zulassen	Der eingestellten Anwendung wird die Verbindung unter den angegebenen Umständen erlaubt.
Verweigern	Der eingestellten Anwendung wird die Verbindung unter den angegebenen Umständen verweigert.

Klicken Sie auf **Speichern**, um die Regel hinzuzufügen.

Ordnen Sie die Regeln, die Sie erstellt haben, mithilfe der Pfeile auf der rechten Seite der Tabelle nach ihrer Priorität. Je weiter oben eine Regel in der Liste steht, desto höher ist ihre Priorität.

7.2.4. Inhaltssteuerung

Über das Inhaltssteuerungsmodul können Sie die gewünschten Einstellungen für Inhaltsfilter und Identitätsschutz für die Benutzeraktivität (Surfen, E-Mail und Software-Anwendungen) vornehmen. Sie können den Zugriff auf das Internet und bestimmte Anwendungen einschränken und Datenverkehr-Scans, Phishing-Schutz- und Identitätschutzregeln konfigurieren.Bitte beachten Sie, dass die Einstellungen für die Inhaltssteuerung auf alle Benutzer angewendet werden, die sich an den Ziel-Computern anmelden.

Die Einstellungen sind in die folgenden Bereiche eingeteilt:

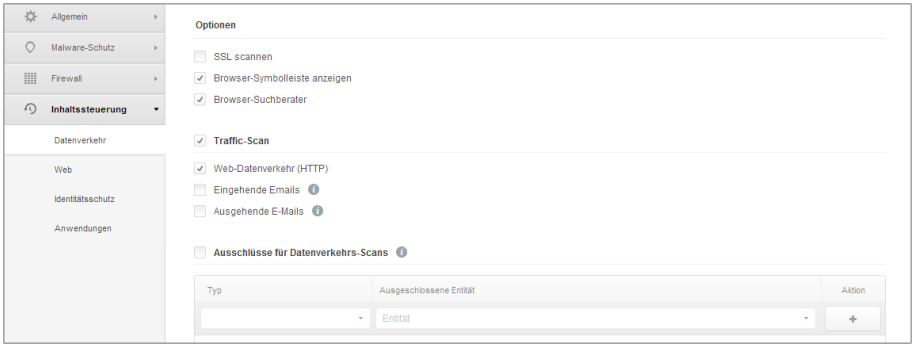
- Datenverkehr
- Web
- Identitätsschutz
- Anwendungen

Datenverkehr

Hier können Sie Einstellungen zur Sicherheit des Datenverkehrs in den folgenden Bereichen vornehmen:

- Optionen

- Traffic-Scan
- Ausschlüsse für Datenverkehrs-Scans



Computer-Richtlinien - Inhaltssteuerung - Datenverkehr

Optionen

- **SSL scannen**. Wählen Sie diese Option, wenn der SSL-Datenverkehr (Secure Sockets Layer) von den Endpoint Security-Schutzmodulen überprüft werden soll.
- **Browser-Symbolleiste anzeigen**. Die Bitdefender-Symbolleiste informiert Benutzer über die Bewertung der Webseiten, die sie aufrufen. Die Bitdefender-Symbolleiste ist anders als andere Browser-Symbolleisten. Sie fügt lediglich einen kleinen Dragger zu Ihrem Browser hinzu, der am oberen Rand jeder Webseite angezeigt wird. Mit einem Klick auf den Dragger öffnen Sie die Symbolleiste.

  Abhängig davon, wie Bitdefender die Webseite einstuft, wird eine der folgenden Bewertungen auf der linken Seite der Symbolleiste eingeblendet:

  – Die Nachricht "Diese Website ist nicht sicher" erscheint auf rotem Hintergrund.

  – Die Nachricht "Vorsicht ist geboten" erscheint auf orangefarbenem Hintergrund.

  – Die Nachricht "Diese Website ist sicher" erscheint auf grünem Hintergrund.
- **Browser-Suchberater.** Der Suchberater bewertet sowohl die Suchergebnisse von Google, Bing und Yahoo! als auch Links auf Facebook und Twitter, indem es ein Symbol vor jedem Ergebnis platziert.Verwendete Symbole und ihre Bedeutung:

  Sie sollten diese Webseite nicht aufrufen.

  Diese Webseite könnte gefährliche Inhalte haben. Seien Sie vorsichtig, wenn Sie sie dennoch aufrufen möchten.

  Diese Seite ist sicher.

Traffic-Scan

Eingehende E-Mails und der Internet-Datenverkehr werden in Echtzeit gescannt, um zu verhindern, dass Malware auf den Computer heruntergeladen wird. Ausgehende E-Mails werden gescannt, um zu verhindern, dass Malware andere Computer infiziert. Das Scannen des Web-Datenverkehrs kann Ihren Webbrowser geringfügig verlangsamen, dadurch können aber über das Internet übertragene Malware, einschließlich Drive-by-Downloads, blockiert werden.

Wenn eine infizierte E-Mail erkannt wird, wird diese automatisch mit einer Standard-E-Mail ersetzt, die den Empfänger über die ursprüngliche infizierte E-Mail informiert. Wenn eine Webseite Malware enthält oder verbreitet, wird diese automatisch blockiert. Anstelle der Webseite wird eine Warnung angezeigt, die den Anwender darüber informiert, das die aufgerufene Seite gefährlich ist.

Sie können zur Steigerung der Systemleistung das Scannen des E-Mail- und Internet-Datenverkehrs deaktivieren, dies wird aber nicht empfohlen. Dabei handelt es sich nicht um eine ernstzunehmende Bedrohung, solange die Zugriff-Scans für lokale Dateien aktiviert bleiben.

Ausschlüsse für Datenverkehrs-Scans

Wenn die Internet-Datenverkehr-Scan-Optionen aktiviert sind, können Sie bestimmte Arten von Datenverkehr vom Scan auf Malware ausschließen.

So definieren Sie einen Datenverkehr-Scan-Ausschluss:

1. Wählen Sie die Art des Ausschlusses aus dem Menü.
2. So definieren Sie je nach Ausschlusstyp die Datenverkehrsentität, die vom Scan ausgeschlossen werden soll:
   - **IP**. Geben Sie die IP-Adresse ein, deren eingehenden und ausgehenden Datenverkehr Sie nicht scannen möchten.
   - **URL**. Schließt die eingegebenen Web-Adressen vom Scan aus. So definieren Sie einen URL-Scan-Ausschluss:
     – Geben Sie eine bestimmte URL ein, z. B. `www.example.com/example.html`
     – Mit Platzhaltern können Sie Web-Adressenmuster definieren:
       - Ein Sternchen (*) ersetzt null oder mehr Zeichen.
       - Ein Fragezeichen (?) ersetzt genau ein Zeichen. Sie können mehrere Fragezeichen benutzen, um eine beliebige Kombination einer bestimmten Anzahl von Zeichen zu ersetzen. So steht ??? z. B. für eine beliebige Folge von genau drei Zeichen.

     In der folgenden Tabelle finden Sie eine Reihe von Beispielsyntaxen für die Angabe von Internet-Adressen.

Syntax	Anwendungsbereich des Ausschlusses
`www.beispiel*`	Jeder Website oder Web-Seite, die mit `www.beispiel` beginnt (unabhängig von der Domänenerweiterung). Der Ausschluss gilt nicht für die Unterdomänen der angegebenen Website, so zum Beispiel `unterdomäne.beispiel.com`.
`*beispiel.com`	Jede Website, die mit `beispiel.com` aufhört, einschließlich aller Seiten und Unterdomänen.
`*Zeichenfolge*`	Jeder Website oder Web-Seite, in deren Adresse die angegebene Zeichenfolge enthalten ist.
`*.com`	Jede Website mit der Domänenerweiterung `.com`, einschließlich aller Seiten und Unterdomänen. Mit dieser Syntax können Sie eine gesamte Top-Level-Domain vom Scan ausschließen.
`www.beispiel?.com`	Jede Internet-Adresse, die mit `www.beispiel?.com` beginnt. Das Fragezeichen kann dabei für jedes beliebige einzelne Zeichen stehen.Beispiele hierfür sind `www.beispiel1.com` oder `www.beispielA.com`.

- **Anwendung**. Schließt den angegebenen Prozess oder die Anwendung vom Scan aus. So definieren Sie einen Anwendungs-Scan-Ausschluss:
  - Geben Sie den vollständigen Anwendungspfad ein. Zum Beispiel `C:\Programme\Internet Explorer\iexplore.exe`
  - Sie können auch Umgebungsvariablen verwenden, um den Anwendungspfad anzugeben. Zum Beispiel: `%programme%\Internet Explorer\iexplore.exe`
  - Oder Sie verwenden Platzhalter, um alle Anwendungen zusammenzufassen, die einem bestimmten Muster folgen. Zum Beispiel:
    - `c*.exe` erfasst alle Anwendungen, die mit "c" beginnen (z. B. chrome.exe).
    - `??????.exe` umfasst alle Anwendungen, deren Name genau sechs Zeichen lang ist (chrome.exe, safari.exe, usw.).
    - `[^c]*.exe` umfasst alle Anwendungen, außer denen, die mit "c" beginnen.
    - `[^ci]*.exe` umfasst alle Anwendungenimmer außer denen, die mit "c" oder "i" beginnen.

3. Klicken Sie auf die Schaltfläche **Hinzufügen** auf der rechten Seite der Tabelle.

Um eine Entität aus der Liste zu löschen, klicken Sie auf die entsprechende **Löschen**-Schaltfläche.

Web

In diesem Bereich können Sie die Surf-Sicherheitseinstellungen konfigurieren.

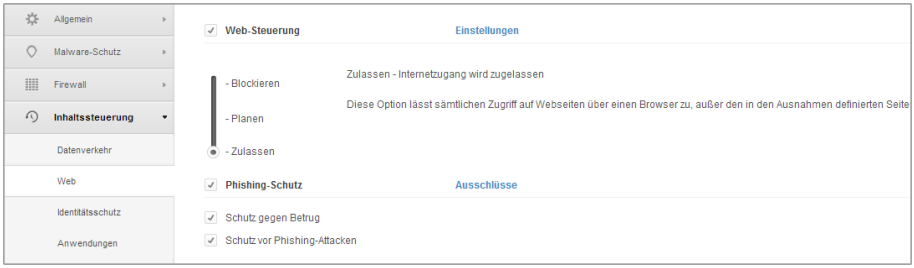
Die Einstellungen sind in die folgenden Bereiche eingeteilt:

- Web-Steuerung
- Phishing-Schutz

Web-Steuerung

Mit der Web-Steuerung können Sie den Internetzugang für Benutzer oder Anwendungen, während bestimmten Zeiträumen blockieren oder zulassen.

Die Webseiten die von der Web-Steuerung blockiert werden, werden nicht im Browser angezeigt. Stattdessen wird eine Standardseite angezeigt, die den Nutzer darüber informiert, dass die angeforderte Webseite von der Web-Steuerung blockiert wurde.



Computer-Richtlinien - Inhaltssteuerung - Internet

Über den Schalter können Sie die **Web-Steuerung** aktivieren oder deaktivieren.

Sie haben drei Konfigurationsoptionen:

- Mit **Zulassen** lassen Sie den Internetzugriff immer zu.
- Mit **Blockieren** lassen Sie den Internetzugriff nie zu.
- Mit **Planen** können Sie einen Zeitplan für den Internetzugriff festlegen.

Wenn Sie den Internetzugriff zulassen oder blockieren, können Sie Ausnahmen zu diesen Einstellungen definieren; für ganze Internetkategorien oder für bestimmte einzelne Internetadressen. Klicken Sie auf **Einstellungen** und konfigurieren Sie den Zeitplan bzw. die Ausnahmen wie folgt:

Planer

So schränken Sie den Internet-Zugang auf bestimmte Tageszeiten während der Woche ein:

1. Wählen Sie im Raster die Zeitintervalle, in denen der Internetzugriff blockiert werden soll.

   Sie können auf individuelle Zellen klicken oder eine Zelle anklicken und mit der Maus einen längeren Zeitraum definieren. Wenn Sie erneut auf die Zelle klicken, kehren Sie die Auswahl um.

Eine neue Auswahl starten Sie, indem Sie, je nach Wunsch, auf **Alle zulassen** oder **Alle blockieren** klicken.

2. Klicken Sie auf **Speichern**.

Beachten Sie

Endpoint Security führt unabhängig davon, ob der Internetzugriff gesperrt ist, stündliche Updates durch.

Kategorien

Internetkategorienfilter filtern den Zugriff auf Websites dynamisch anhand derer Inhalte. Sie können den Internetkategorienfilter verwenden, um Ausnahmen zur gewählten Aktion (Zulassen oder Blockieren) für ganze Kategorien (z. B. Spiele, nicht jugendfreies Material oder Online-Netzwerke) zu definieren.

So konfigurieren Sie die Internetkategorienfilter:

1. Wählen Sie **Internet-Kategorienfilter**.
2. Für eine schnelle Konfiguration können Sie auf eines der vordefinierten Profile (**aggressiv**, **normal**, **tolerant**) klicken. Orientieren Sie sich bei Ihrer Auswahl an den Beschreibungen auf der rechten Seite der Skala. Mit einem Klick auf die Schaltfläche **Kategorien** können Sie die vordefinierten Aktionen für bestehende Internetkategorien anzeigen.
3. Wenn Sie mit den Standardeinstellungen nicht zufrieden sein sollten, können Sie einen benutzerdefinierten Filter anlegen:
   a. Wählen Sie **Benutzerdefiniert**.
   b. Klicken Sie auf die Schaltfläche **Kategorien**, um den entsprechenden Bereich einzublenden.
   c. Suchen Sie die gewünschte Kategorie in der Liste und wählen Sie die gewünschte Aktion aus dem Menü.
4. Sie können auch **Internetkategorien als Ausnahmen für den Internetzugriff behandeln**, wenn Sie die bestehenden Internetzugriffseinstellungen ignorieren und nur der Internetkategorienfilter benutzen möchten.
5. Klicken Sie auf **Speichern**.

Beachten Sie

- Bestimmte Internetadressen, für die Berechtigung **Zulassen** eingestellt ist, werden während der Zeiten, zu denen der Internetzugang durch die Web-Steuerung blockiert ist, berücksichtigt.
- Das **Zulassen** funktioniert nur, wenn der Internetzugang durch die Web-Steuerung blockiert ist. Das **Blockieren** funktioniert nur, wenn der Internetzugang über die Web-Steuerung zugelassen ist.

- Sie können die Kategorieberechtigung für einzelne Internetadressen außer Kraft setzen, indem Sie sie mit der gegenteiligen Berechtigungen im folgenden Bereich hinzufügen: **Web-Steuerung > Einstellungen > Ausschlüsse**. Wenn eine Internetadresse durch die Internet-Kategorienfilter blockiert wird, können Sie für diese Adresse eine Web-Steuerung festlegen und die Berechtigung **Zulassen** erteilen.

Ausschlüsse

Sie können auch Internetregeln erstellen, um bestimmte Internet-Adressen konkret zu blocken oder zuzulassen. Diese Regeln ignorieren die Einstellungen der Web-Steuerung. Wenn also zum Beispiel der Internetzugang durch die Web-Steuerung blockiert ist, können Benutzer trotzdem auf bestimmte Webseiten zugreifen.

So legen Sie eine Internetregel an:

1. Wählen Sie **Ausnahmen verwenden**, um Internet-Ausnahmen zu verwenden.
2. Geben Sie die Adresse, die Sie zulassen oder blockieren möchten in das Feld **Internetadresse** ein.
3. Wählen Sie **Zulassen** oder **Blockieren** aus dem Menü **Berechtigung**.
4. Klicken Sie auf die Schaltfläche + **Hinzufügen** auf der rechten Seite der Tabelle, um die Adresse der Liste der Ausnahmen hinzuzufügen.
5. Klicken Sie auf **Speichern**.

So bearbeiten Sie eine Internet-Regel:

1. Klicken Sie auf die Internet-Adresse, die Sie bearbeiten wollen:
2. Die bestehende URL verändern.
3. Klicken Sie auf **Speichern**.

So entfernen Sie eine Internet-Regel:

1. Bewegen Sie den Mauszeiger über die Internetadresse, die Sie entfernen möchten.
2. Klicken Sie auf die Schaltfläche − **Löschen**.
3. Klicken Sie auf **Speichern**.

Phishing-Schutz

Der Phishing-Schutz blockiert automatisch bekannte Phishing-Seiten, um zu verhindern, dass Benutzer unbeabsichtigt persönliche oder vertrauliche Informationen an Online-Betrüger weitergeben. Anstelle der Phishing-Seite wird eine spezielle Warnseite im Browser eingeblendet, die den Benutzer darüber informiert, dass die angeforderte Webseite gefährlich ist.

Wählen Sie **Phishing-Schutz**, um den Phishing-Schutz zu aktivieren. Sie können den Phishing-Schutz über die folgenden Einstellungen an Ihre Bedürfnisse anpassen:

- **Schutz vor Betrug**. Wählen Sie diese Option, wenn Sie den Schutz auf weitere Betrugsarten neben Phishing ausweiten möchten. So zum Beispiel Webseiten von Scheinfirmen, die zwar nicht direkt private Informationen anfordern, aber versuchen, sich als legitime Unternehmen auszugeben und Geld verdienen, indem Sie Menschen so manipulieren, dass Sie eine Geschäftsbeziehung mit ihnen aufnehmen.
- **Schutz vor Phishing-Attacken**. Lassen Sie diese Option aktiviert, um Benutzer vor Phishing-Versuchen zu schützen.

Wenn eine legitime Webseite fälschlicherweise als Phishing-Seite identifiziert und blockiert wird, können Sie diese zur Whitelist hinzufügen, damit Benutzer darauf zugreifen können. Diese Liste sollte nur Websites enthalten, denen Sie uneingeschränkt vertrauen.

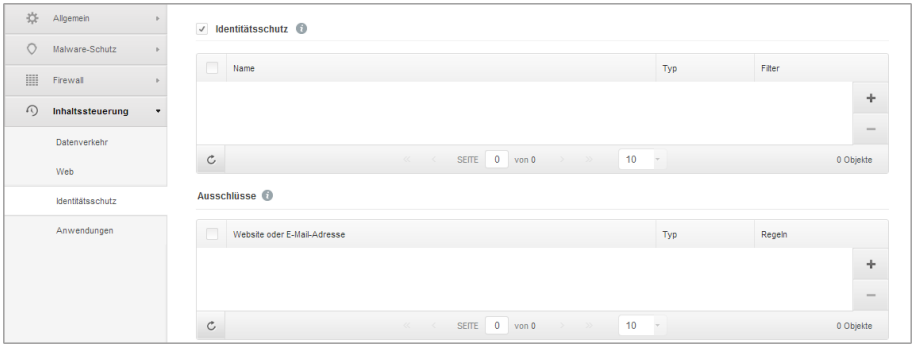
So verwalten Sie Phishing-Schutz-Ausnahmen:

1. Klicken Sie auf **Ausschlüsse**.
2. Geben Sie die Internet-Adresse ein und klicken Sie auf die Schaltfläche + **Hinzufügen**.

   Um eine Ausnahme aus der Liste zu entfernen, bewegen Sie den Mauszeiger darüber, und klicken Sie auf die − **Löschen**-Schaltfläche.
3. Klicken Sie auf **Speichern**.

Identitätsschutz

Mit dem Identitätsschutz kann der Administrator Regeln definieren, die eine unautorisierte Weitergabe von sensiblen Daten verhindern.



Computer-Richtlinien - Inhaltssteuerung - Identitätsschutz

Sie können Regeln erstellen, um personenbezogene oder vertrauliche Daten jeder Art zu schützen, so zum Beispiel:

- Persönliche Kundeninformationen
- Namen und Schlüsseldaten von Entwicklungsprodukten und -technologien

- Kontaktinformationen von Führungskräften im Unternehmen

Geschützte Informationen können Namen, Telefonnummern, Kreditkarten- und Bankdaten, E-Mail-Adressen usw. sein.

Basierend auf den von Ihnen angelegten Identitätsschutzregeln scannt Endpoint Security den ausgehenden Web- und E-Mail-Verkehr nach bestimmten Zeichenfolgen (z.B. Kreditkartennummern). Wird eine Übereinstimmung gefunden, wird die entsprechende Webseite oder E-Mail-Nachricht blockiert, um zu verhindern, dass geschützte Daten versendet werden.Der Benutzer wird per Benachrichtigungsseite im Browser oder E-Mail sofort über die Aktionen des Endpoint Security informiert.

So konfigurieren Sie den Identitätsschutz:

1. Markieren Sie das Kästchen, um den Identitätsschutz einzuschalten.
2. Legen Sie Identitätsschutzregeln für alle sensiblen Daten an, die Sie schützen möchten.Um eine Regel anzulegen:
   a. Klicken Sie auf die Schaltfläche + **Hinzufügen** auf der rechten Seite der Tabelle.Ein Konfigurationsfenster wird geöffnet.
   b. Geben Sie den Namen ein, unter dem die Regel in der Regeltabelle aufgeführt werden soll.Wählen Sie einen eindeutigen Namen, damit Sie oder andere Administrationen die Regel entsprechend zuordnen können.
   c. Geben Sie die Daten ein, die Sie schützen möchten (so zum Beispiel die Telefonnummer einer Führungskraft oder den internen Namen eines neuen Produkts in der Entwicklungsphase).Jede beliebige Kombination von Wörtern, Zahlen oder Zeichenfolgen aus alphanumerischen Zeichen und Sonderzeichen (z.B. @, # oder $) ist möglich.

      Geben Sie mindestens fünf Zeichen ein, um ein versehentliches Blockieren von E-Mail-Nachrichten oder Webseiten zu verhindern.

      Wichtig

      Vorausgesetzt die Daten werden verschlüsselt auf geschützten Computern gespeichert, können aber über Ihr Control Center-Konto angezeigt werden.Für noch bessere Sicherheit sollten Sie die Daten, die Sie schützen möchten, nicht vollständig eingeben.In diesem Fall müssen Sie die Option **Ganze Wörter abgl.** deaktivieren.

   d. Konfigurieren Sie den Datenverkehrs-Scan nach Ihren Anforderungen.
      - **Web-Datenverkehr (HTTP) scannen** - Scannt den HTTP- (Web-) Datenverkehr und blockiert ausgehende Daten, die den Regeln entsprechen.
      - **E-Mail-Verkehr (SMTP) scannen** - Scannt den SMTP- (E-Mail-) Datenverkehr und blockiert alle ausgehenden E-Mail-Nachrichten, die den Regeln entsprechen.

      Sie können wählen, ob die Regeln nur zutreffen, wenn die Daten der Regeln wörtlich übereinstimmen oder ob die komplette Zeichenfolge übereinstimmen muss.

e. Klicken Sie auf **Speichern**.Die neue Regel wird der Liste hinzugefügt.

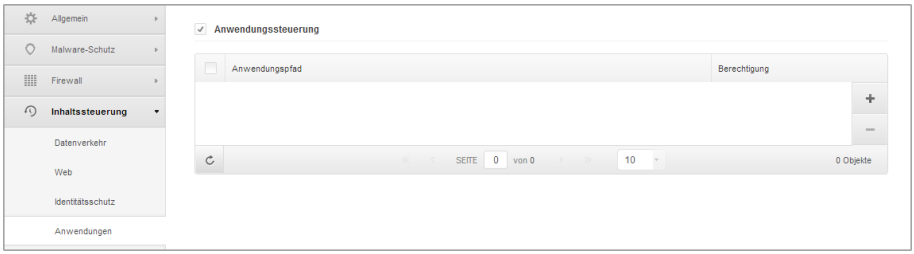
3. Konfigurieren Sie Ausschlüsse für die Identitätsschutzregeln, damit Benutzer weiterhin geschützte Daten an autorisierte Webseiten und Empfänger versenden können.Ausschlüsse können global (auf alle Regeln) oder nur auf bestimmte Regeln angewendet werden.Um einen Ausschluss hinzuzufügen:
   a. Klicken Sie auf die Schaltfläche **Hinzufügen** auf der rechten Seite der Tabelle.Ein Konfigurationsfenster wird geöffnet.
   b. Geben Sie die Web- oder E-Mail-Adresse ein, an die Benutzer geschützte Daten weitergeben dürfen.
   c. Wählen Sie die Art des Ausschlusses (Web- oder E-Mail-Adresse).
   d. Wählen Sie aus der Tabelle **Regeln** die Identitätsschutzregel(n), auf die dieser Ausschluss angewendet werden soll.
   e. Klicken Sie auf **Speichern**. Die neue Ausschlussregel wird der Liste hinzugefügt.

Beachten Sie
Wird eine E-Mail mit blockierten Inhalten an mehrere Empfänger adressiert, wird die Nachricht an die Empfänger verschickt, für die Ausschlüsse definiert wurden.

Um eine Regel oder einen Ausschluss aus der Liste zu entfernen, klicken Sie auf die entsprechende Schaltfläche **Löschen** auf der rechten Seite der Tabelle.

Anwendungen

In diesem Bereich können Sie die Anwendungssteuerung konfigurieren. Mit der Anwendungssteuerung können Sie den Benutzerzugriff auf Anwendungen auf ihren jeweiligen Computern blockieren oder einschränken. Sie können jede beliebige Anwendung sperren – neben Spiel-, Medien- und Chatprogrammen auch andere Arten von Software.



Computer-Richtlinien - Inhaltssteuerung - Anwendungen

Um die Anwendungssteuerung zu konfigurieren:

1. Aktivieren Sie die Anwendungssteuerung.
2. Legen Sie die Anwendungen fest, auf die Sie den Zugriff beschränken möchten. Um den Zugriff auf eine Anwendung einzuschränken:

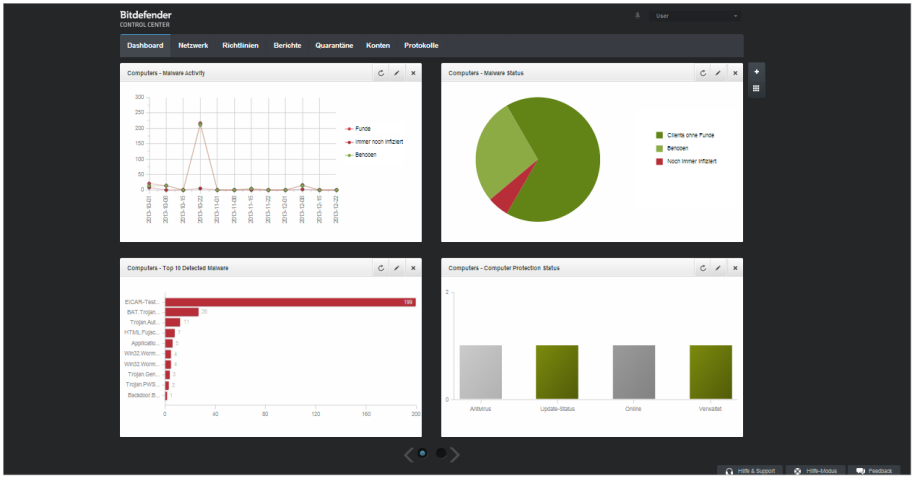
a. Klicken Sie auf die Schaltfläche + **Hinzufügen** auf der rechten Seite der Tabelle. Ein Konfigurationsfenster wird geöffnet.
b. Sie müssen den Pfad der ausführbaren Anwendungsdatei auf den Ziel-Computern angeben. Dafür gibt es zwei Möglichkeiten:
   - Wählen Sie einen vorgegebenen Pfad aus dem Menü und vervollständigen Sie den Pfad im Bearbeitungsfeld nach Bedarf. So müssen Sie für eine Anwendung, die im Ordner `Programme` installiert ist, den Ordner `%Programme` auswählen und den Pfad vervollständigen, indem Sie einen Backslash (\) und den Namen des Anwendungsordners hinzufügen.
   - Geben Sie den vollständigen Pfad in das Bearbeitungsfeld ein. Es empfiehlt sich, (nach Möglichkeit) Systemvariablen zu verwenden, um sicherzustellen, dass der Pfad auf allen Computern gültig ist.
c. **Zugriffsplaner**. Legen Sie den Anwendungszugriff für bestimmte Tageszeiten während der Woche fest:
   - Wählen Sie im Raster die Zeitintervalle, in denen der Zugriff auf die Anwendung blockiert werden soll. Sie können auf individuelle Zellen klicken oder eine Zelle anklicken und mit der Maus einen längeren Zeitraum definieren. Wenn Sie erneut auf die Zelle klicken, kehren Sie die Auswahl um.
   - Eine neue Auswahl starten Sie, indem Sie, je nach Wunsch, auf **Alle zulassen** oder **Alle blockieren** klicken.
   - Klicken Sie auf **Speichern**. Die neue Regel wird der Liste hinzugefügt.

Um eine Regel aus der Liste zu entfernen, klicken Sie auf die entsprechende Schaltfläche – **Löschen** auf der rechten Seite der Tabelle. Um eine bestehende Regel zu bearbeiten, klicken Sie auf den Namen der Anwendung.

8. Überwachungs-Dashboard

Das Control Center-Dashboard ist eine individuell anpassbare Anzeige, die Ihnen einen schnellen Überblick über die Sicherheitslage der geschützten Netzwerkobjekte verschafft.

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



Das Dashboard

Was Sie über Dashboard-Portlets wissen sollten:

- Die Control Center verfügt über verschiedene vordefinierte Dashboard-Portlets.
- Jedes Dashboard-Portlet enthält im Hintergrund einen detaillierten Bericht, der mit einem einfachen Klick auf das Diagramm abgerufen werden kann.
- Es gibt eine Reihe verschiedener Portlet-Arten, die unterschiedliche Informationen über den Schutz Ihrer Netzwerkobjekte enthalten, so zum Beispiel Update-Status, Malware-Status, Firewall-Aktivität usw. Weitere Informationen zu den verschiedenen Arten von Dashboard-Portlets finden Sie unter „Verfügbare Berichtstypen“ (S. 119).
- Die von den Portlets angezeigten Informationen beziehen sich ausschließlich auf die Netzwerkobjekte, die zu Ihrem Benutzerkonto gehören. Sie können mit dem **Portlet bearbeiten**-Befehl das Ziel für jedes Portlet individuell anpassen.

- Klicken Sie auf die einzelnen Einträge in der Diagrammlegende, um die entsprechende Variable, falls verfügbar, auf dem Graphen anzuzeigen bzw. auszublenden.
- Die Portlets werden in Vierergruppen angezeigt. Verwenden Sie den Schieberegler unten auf der Seite, um zwischen den Portlet-Gruppen umzuschalten.

Das Dashboard lässt sich nach individuellen Vorlieben leicht konfigurieren. Sie können Portlet-Einstellungen bearbeiten, neue Portlets hinzufügen, Portlets entfernen oder die bestehenden Portlets neu anordnen.

8.1. Portlet-Daten aktualisieren

Um sicherzustellen, dass das Portlet die aktuellsten Informationen anzeigt, klicken Sie auf das **Neu laden**-Symbol in der entsprechenden Titelleiste.

8.2. Portlet-Einstellungen bearbeiten

Einige der Portlets enthalten Statusinformationen, andere zeigen die Sicherheitsereignisse im letzten Berichtszeitraum an.Sie können den Berichtszeitraum eines Portlets anzeigen und konfigurieren, indem Sie auf die das Symbol **Portlet bearbeiten** in der entsprechenden Titelleiste klicken.

8.3. Ein neues Portlet hinzufügen

Sie können weitere Portlets hinzufügen, um bestimmte Informationen angezeigt zu bekommen.

So fügen Sie ein neues Portlet hinzu:

1. Gehen Sie zur Seite **Dashboard**.
2. Klicken Sie auf die Schaltfläche **Portlet hinzufügen** auf der rechten Seite des Dashboards.Das Konfigurationsfenster wird geöffnet.
3. Im Reiter **Details** können Sie die Details des Portlets konfigurieren:
   -
   - Art des Hintergrundberichts
   - Aussagekräftiger Portlet-Name
   - Update-Intervall

   Weitere Informationen zu verfügbaren Berichtstypen finden Sie unter „Verfügbare Berichtstypen“ (S. 119).
4. Wählen Sie im Reiter **Ziele** die Netzwerkobjekte und Gruppen, die sie einbeziehen möchten.
5. Klicken Sie auf **Speichern**.

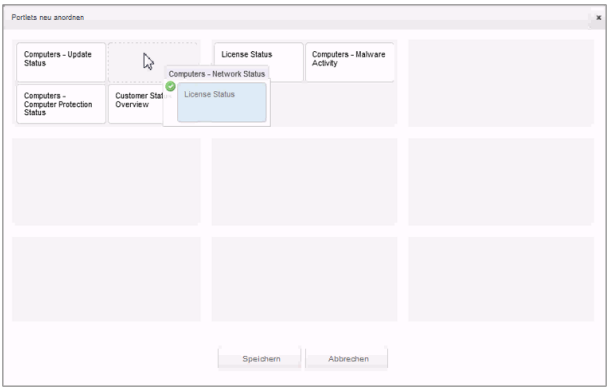
8.4. Ein Portlet entfernen

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.

8.5. Portlets neu anordnen

Sie können die Portlets im Dashboard ganz nach Ihren Bedürfnissen anordnen. So ordnen Sie die Portlets neu an:

1. Gehen Sie zur Seite **Dashboard**.
2. Klicken Sie auf die Schaltfläche **Portlets neu anordnen** auf der rechten Seite des Dashboards.Die Portlet-Übersicht wird angezeigt.
3. Ziehen Sie die einzelnen Portlets mit der Maus an die gewünschte Stelle.
4. Klicken Sie auf **Speichern**.



Portlets im Dashboard neu anordnen

9. Berichte verwenden

Mit Control Center können Sie Berichte über den Sicherheitsstatus der verwalteten Netzwerkobjekte zentral erstellen und anzeigen. Die Berichte können zu verschiedenen Zwecken eingesetzt werden, wie zum Beispiel:

- Einhaltung der Unternehmenssicherheitsrichtlinien überwachen und sicherstellen.
- Überprüfung und Bewertung des Netzwerksicherheitsstatus.
- Sicherheitsprobleme, Bedrohungen und Sicherheitslücken im Netzwerk erkennen.
- Sicherheitsvorfälle und Malware-Aktivität überwachen.
- Bereitstellung von übersichtlichen Daten zur Netzwerksicherheit für die Unternehmensführung.

Es stehen verschiedene Berichtstypen zur Verfügung, damit Sie einfachen Zugriff auf die von Ihnen benötigten Informationen erhalten. Diese Informationen werden in übersichtlichen interaktiven Diagrammen und Grafiken dargestellt, so dass Sie schnell den Sicherheitsstatus des Netzwerkes überprüfen und eventuelle Sicherheitsprobleme erkennen können.

Die Berichte können Daten vom gesamten Netzwerk der verwalteten Netzwerkobjekte beinhalten oder sich auf ausgewählte Gruppen konzentrieren. So können Sie mit einem einzigen Bericht folgendes erfahren:

- Statistische Daten zu allen oder Gruppen von verwalteten Netzwerkobjekten.
- Detailinformationen für jedes verwaltete Netzwerkobjekt.
- Die Liste von Computern, die bestimmte Kriterien erfüllen (zum Beispiel solche, deren Malware-Schutz deaktiviert ist).

Alle geplanten Berichte stehen im Control Center zur Verfügung, Sie können sie aber auch auf Ihrem Computer speichern oder per E-Mail versenden.

Verfügbare Formate sind u.a. Portable Document Format (PDF) und Comma-Separated Values (CSV).

9.1. Verfügbare Berichtstypen

Für Computer stehen die folgenden Berichtstypen zur Verfügung:

Update-Status

Zeigt Ihnen den Update-Status des auf den ausgewählten Computern installierten Endpoint Security an. Der Update-Status bezieht sich auf die Produktversion und die Version der Engines (Signaturen).

Über die verfügbaren Filter können Sie schnell feststellen, welche Clients über einen festgelegten Zeitraum aktualisiert oder nicht aktualisiert wurden.

Malware-Status

Hilft Ihnen dabei herauszufinden, wie viele und welche der ausgewählten Computer über einen bestimmten Zeitraum von Malware-Infektionen betroffen waren und wie mit der Bedrohung umgegangen wurde.

Computer werden nach diesen Kriterien in Gruppen aufgeteilt:

- Computer ohne Funde (über den festgelegten Zeitraum wurde keine Malware-Bedrohung gefunden).
- Computer mit behobener Malware (alle als infiziert erkannte Dateien wurden erfolgreich desinfiziert oder in die Quarantäne verschoben)
- Immer noch mit Malware infizierte Computer (der Zugriff auf einige der infizierten Dateien wurde verweigert)

Malware-Aktivität

Zeigt Ihnen übergreifende Informationen zu Malware-Bedrohungen, die über einen festgelegten Zeitraum auf den ausgewählten Computern gefunden wurden. Sie sehen:

- Anzahl der Funde (gefundene Dateien, die mit Malware infiziert sind)
- Anzahl der behobenen Infektionen (Dateien, die erfolgreich desinfiziert oder in die Quarantäne verschoben wurden)
- Anzahl der nicht behobenen Infektionen (Dateien, die nicht desinfiziert werden konnten, auf die der Zugriff aber verweigert wurde; so z. B. eine infizierte Datei, die mit einem proprietären Archivformat gespeichert wurde)

Netzwerkstatus

Zeigt Ihnen detaillierte Information zum allgemeinen Sicherheitsstatus der ausgewählten Computer. Computer werden nach diesen Kriterien in Gruppen aufgeteilt:

- Problemstatus
- Verwaltungsstatus
- Infektionsstatus
- Status des Malware-Schutzes
- Produktupdate Status
- Lizenzierungsstatus
- Der Netzwerkaktivitätsstatus jedes Computers (online/offline). Wenn der Computer zum Zeitpunkt der Berichtserstellung offline ist, werden Datum und Uhrzeit angezeigt, zu der er zuletzt vom Control Center gesehen wurde.

Computer-Schutzstatus

Liefert Ihnen verschiedene Statusinformationen zu ausgewählten Computern in Ihrem Netzwerk.

- Status des Malware-Schutzes
- Endpoint Security-Update-Status

- Status der Netzwerkaktivität (online/offline)
- Verwaltungsstatus

Sie können nach Sicherheitsaspekt und -status filtern, um die Informationen zu erhalten, nach denen Sie suchen.

Top-10 der infizierten Computer
Zeigt von den ausgewählten Computern die 10 Computer mit den meisten Infektionen an, sortiert nach der Anzahl der Funde während eines bestimmten Zeitraums.

Beachten Sie
In der Detailtabelle wird sämtliche Malware angezeigt, die auf den Top-10 der infizierten Computer gefunden wurde.

Top-10 der erkannten Malware
Zeigt Ihnen die 10 häufigsten Malware-Bedrohungen, die über einen bestimmten Zeitraum auf den ausgewählten Computern erkannt wurden.

Beachten Sie
In der Detailtabelle werden alle Computer angezeigt, die von einer der Top-10 der gefundenen Malware infiziert wurden.

Firewallaktivität
Informiert Sie über den Status des Firewall-Moduls von Endpoint Security. Hier sehen Sie die Anzahl der blockierten Verbindungsversuche und Port-Scans auf den ausgewählten Computern.

Blockierte Webseiten
Informiert Sie über den Status des Moduls Web-Steuerung von Endpoint Security. Hier sehen Sie die Anzahl der blockierten Websites auf den ausgewählten Computern.

Blockierte Anwendungen
Informiert Sie über den Status des Anwendungssteuerungsmoduls von Endpoint Security. Hier sehen Sie die Anzahl der blockierten Anwendungen auf den ausgewählten Computern.

Identitätsschutz
Informiert Sie über den Status des Identitätsschutzmoduls von Endpoint Security. Hier sehen Sie die Anzahl der blockierten E-Mails und Websites auf den ausgewählten Computern.

Phishing-Schutz-Aktivität
Informiert Sie über den Status des Phishing-Schutz-Moduls von Endpoint Security. Hier sehen Sie die Anzahl der blockierten Websites auf den ausgewählten Computern.

Vom Verhaltens-Scan blockierte Anwendungen
Informiert Sie über die von der Active Virus Control (AVC) / dem Angrifferkennungssystem (IDS) blockierte Anwendungen. Sie können die Anzahl der von AVC / IDS blockierten Anwendungen für jeden ausgewählten Computer einsehen. Klicken Sie auf die Anzahl

der blockierten Anwendungen für den gewünschten Computer, um die Liste der blockierten Anwendungen und die dazugehörigen Informationen anzuzeigen (Anwendungsname, der Blockierungsgrund, die Anzahl der blockierten Versuche sowie das Datum und der Zeitpunkt des zuletzt blockierten Versuchs).

9.2. Berichte erstellen

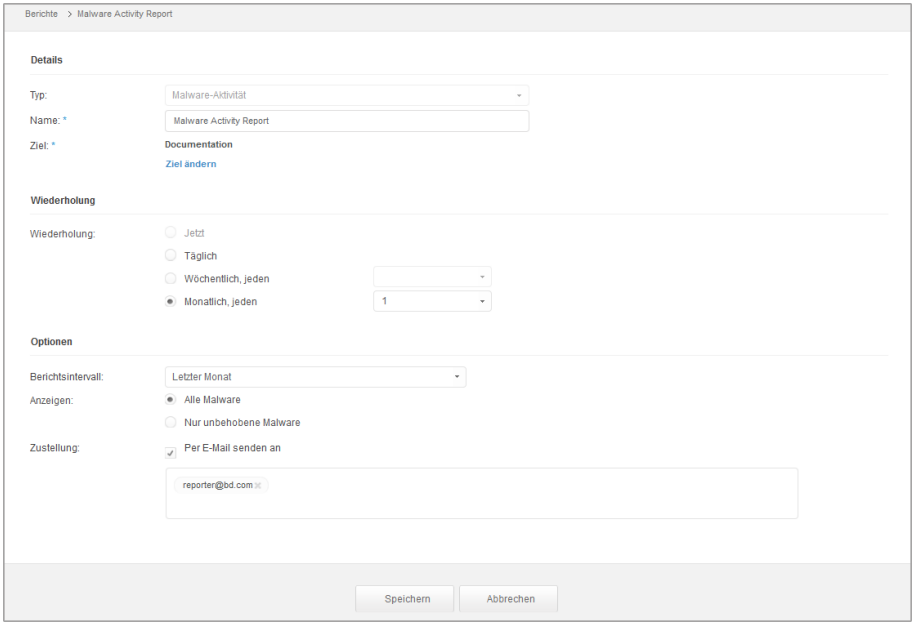
Sie können zwei verschiedene Kategorien von Berichten erstellen:

- **Sofortberichte.** Sofortberichte werden automatisch angezeigt, sobald sie erstellt wurden.
- **Geplante Berichte.** Geplante Berichte können so konfiguriert werden, dass sie zu einem bestimmten Zeitpunkt erstellt werden. Eine Liste aller geplanten Berichte finden Sie auf der Seite **Berichte**.

Wichtig
Sofortberichte werden automatisch gelöscht, wenn Sie die Berichtsseite schließen. Geplante Berichte werden auf der Seite **Berichte** gespeichert und angezeigt.

Um einen Bericht zu erstellen:

1. Gehen Sie zur Seite **Berichte**.



Optionen für Computer-Berichte

2. Klicken Sie auf die Schaltfläche + **Hinzufügen** auf der rechten Seite der Tabelle.
3. Wählen Sie den gewünschten Berichtstyp aus dem Menü aus. Weitere Informationen finden Sie unter „Verfügbare Berichtstypen“ (S. 119).
4. Geben Sie einen eindeutigen Namen für den Bericht ein. Wenn Sie einen Namen festlegen, berücksichtigen Sie den Berichtstyp, das Berichtsziel und unter Umständen auch die Berichtsoptionen.
5. Konfigurieren Sie das Berichtsziel, indem Sie auf den Link **Ziel ändern** klicken. Wählen Sie die Gruppe, zu der Sie den Bericht erstellen möchten.
6. Berichtwiederholung konfigurieren (Zeitplan). Sie haben die Wahl, ob Sie den Bericht sofort (Sofortbericht) erstellen oder so planen, dass er täglich, wöchentlich (an einem bestimmten Tag der Woche) oder monatlich (an einem bestimmten Tag des Monats) erstellt wird.

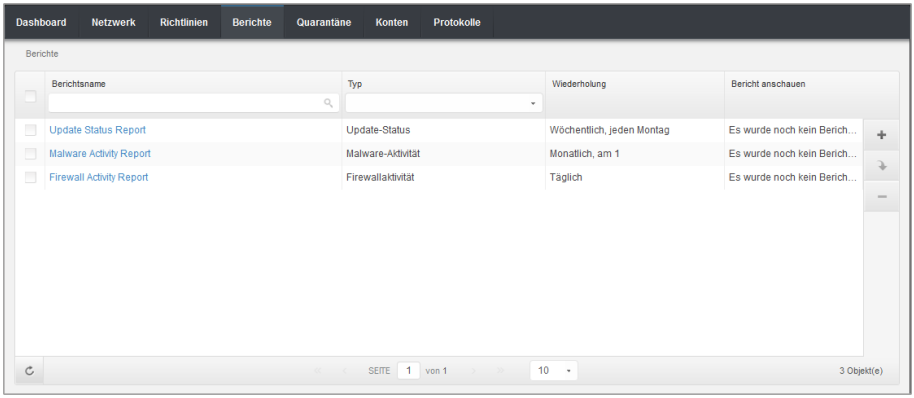
   Beachten Sie
   Geplante Berichte werden am geplanten Datum sofort nach 00:00 Uhr UTC (das ist die Standardzeitzone der GravityZone-Appliance) erstellt.

7. Konfigurieren Sie die Berichtsoptionen.
   a. Für die meisten Berichtstypen müssen Sie das Update-Intervall angeben. Der Bericht wird nur Daten für den ausgewählten Zeitraum enthalten.
   b. Viele Berichtsarten enthalten Filtermöglichkeiten, damit Sie die für Sie interessanten Informationen schnell finden können. Verwenden Sie die Filtermöglichkeiten, um nur die gewünschten Informationen abzurufen.

      Für Berichte über den **Update-Status** können Sie zum Beispiel auch nur die Computer anzeigen, die im ausgewählten Zeitraum aktualisiert wurden (bzw. nicht aktualisiert wurden) oder solche, die neu gestartet werden müssen, um ein Update abzuschließen.
   c. Um eingeplanten Bericht als E-Mail geschickt zu bekommen, wählen Sie die entsprechende Option.
8. Klicken Sie auf **Generieren**, um einen Sofortbericht zu erstellen, oder auf **Speichern**, um einen geplanten Bericht zu erstellen. Die Schaltfläche **Speichern** ändert sich automatisch zu **Generieren**, wenn Sie angegeben haben, einen Sofortbericht erstellen zu wollen.
   - Wenn Sie einen Sofortbericht erstellen, wird er sofort angezeigt, nachdem Sie auf **Generieren** geklickt haben. Die Zeit, die bis zur Fertigstellung eines Berichts benötigt wird, hängt von der Anzahl der verwalteten Computer ab. Bitte warten Sie, bis der angeforderte Bericht erstellt wurde.
   - Wenn Sie einen geplanten Bericht erstellt haben, wird dieser in der Liste auf der Seite **Berichte** angezeigt. Nachdem der Bericht erstellt wurde, können Sie ihn anzeigen, indem Sie auf den entsprechenden Link in der Spalte **Bericht anzeigen** auf der Seite **Berichte** klicken.

9.3. Geplante Berichte anzeigen und verwalten

Gehen Sie zum Anzeigen und Verwalten geplanter Berichte zur Seite **Berichte**.



Die Berichtsübersicht

Alle geplanten Berichte werden in einer Tabelle angezeigt. Sie können alle erstellten geplanten Berichte und nützliche Informationen dazu einsehen:

- Name und Art des Berichts.
- Den Zeitpunkt, zu dem der Bericht erstellt wird.

Beachten Sie
Geplante Berichte sind nur für den Benutzer verfügbar, der diese auch erstellt hat.

Um Berichte nach einer Spalte zu ordnen, klicken Sie einfach auf die Überschrift der jeweiligen Spalte. Mit einem erneuten Klick auf die Spaltenüberschrift können Sie die Sortierungsrichtung ändern

Die Berichtdetails werden in einer Tabelle angezeigt, die in mehreren Spalten verschiedene Informationen darstellt. Die Tabelle kann sich über mehrere Seiten erstrecken (standardmäßig werden pro Seite nur 10 Einträge angezeigt). Mit den Schaltflächen am unteren Rand der Tabelle können Sie durch die Detailseiten blättern.

Um die Suche nach Informationen zu beschleunigen, verwenden Sie die Suchfelder oder die Filtermöglichkeiten unter den Spaltenüberschriften.

Um die Berichtdetails nach einer bestimmten Spalte zu sortieren, klicken Sie einfach auf die entsprechend Spaltenüberschrift. Mit einem erneuten Klick auf die Spaltenüberschrift können Sie die Sortierungsrichtung ändern

Sie können das Suchfeld leeren, indem Sie mit dem Mauszeiger darüber fahren und auf das **Löschen**Symbol klicken.

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

9.3.1. Berichte betrachten

So zeigen Sie einen Bericht an:

1. Gehen Sie zur Seite **Berichte**.
2. Sortieren Sie die Berichte nach Namen, Typ oder Wiederholung, um den gewünschten Bericht leichter zu finden.
3. Klicken Sie in der Spalte **Bericht anschauen** auf den entsprechenden Link, um den Bericht anzuzeigen.

Alle Berichte haben eine Zusammenfassungsteil (die obere Hälfte der Berichtsseite) und einen Detailsteil (die untere Hälfte der Berichtsseite).

- Der Zusammenfassungsbereich enthält statistische Daten (Kuchendiagramme und Grafiken) für alle ausgewählten Netzwerkobjekte oder Gruppen sowie allgemeine Informationen über den Bericht wie den Berichtszeitraum (sofern anwendbar), Berichtsziel, usw.
- Der Detailbereich enthält detaillierte Informationen zu jedem verwalteten Netzwerkobjekt.

Beachten Sie

- Sie können die im Diagramm angezeigten Informationen anpassen, indem Sie auf die Einträge in der Legende klicken und damit die entsprechenden Daten anzeigen oder ausblenden.
- Klicken Sie auf den Bereich der Grafik, der Sie interessiert, um die dazugehörigen Details in der Tabelle unter dem Diagramm anzuzeigen.

9.3.2. Geplante Berichte bearbeiten

Beachten Sie

Wenn Sie einen geplanten Bericht bearbeiten, werden sämtliche Änderungen mit der nächsten Ausführung des Berichts wirksam. Zuvor erstellte Berichte sind von den Änderungen nicht betroffen.

Um die Einstellungen eines geplanten Berichts zu ändern:

1. Gehen Sie zur Seite **Berichte**.
2. Klicken Sie auf den Berichtnamen.

3. Ändern Sie die Berichtseinstellungen nach Bedarf. Sie können die folgenden Änderungen vornehmen:
   - **Berichtsname.** Geben Sie dem Bericht einen eindeutigen Namen, der seinen Inhalt widerspiegelt. Wenn Sie einen Namen festlegen, berücksichtigen Sie den Berichtstyp, das Berichtsziel und unter Umständen auch die Berichtsoptionen. Berichte die anhand eines geplanten Berichts erstellt werden, erhalten auch den entsprechenden Namen.
   - **Berichtsziel.** Die ausgewählte Option weist auf die Art des aktuellen Berichtsziels hin (entweder Gruppen oder einzelne Netzwerkobjekte). Klicken Sie auf den entsprechenden Link, um das aktuelle Berichtsziel anzuzeigen. Sie können das Berichtsziel ändern, indem Sie die Gruppen oder Netzwerkobjekte auswählen, die in dem Bericht eingeschlossen werden sollen.
   - **Berichtwiederholung (Planen).** Sie können festlegen, ob der Bericht täglich, wöchentlich (an einem bestimmten Tag der Woche) oder monatlich (an einem bestimmten Tag des Monats) automatisch erstellt werden soll. Abhängig von dem ausgewählten Zeitplan wird der Bericht nur Daten vom letzten Tag, aus der letzten Woche oder dem letzten Monat enthalten.
   - **Berichtsoptionen.** Der Bericht wird nur Daten aus dem ausgewählten Update-Intervall enthalten. Sie können das Intervall ab der nächsten Ausführung ändern. Sie können den Bericht auch per E-Mail erhalten. Die meisten Berichte enthalten Filtermöglichkeiten, damit Sie die für Sie interessanten Informationen schnell finden können. Wenn Sie den Bericht in der Konsole anzeigen, sind unabhängig von den gewählten Optionen immer alle Informationen verfügbar. Wenn Sie den Bericht herunterladen oder per E-Mail versenden, werden nur die Berichtszusammenfassung und die ausgewählten Informationen in der PDF-Datei enthalten sein. Die Berichtsdetails sind nur im CSV-Format verfügbar.
4. Klicken Sie auf **Speichern**, um die Änderungen zu speichern.

9.3.3. Geplante Berichte löschen

Wenn ein geplanter Bericht nicht mehr benötigt wird, empfiehlt es sich, diesen zu löschen. Durch das Löschen eines geplanten Berichts werden alle Berichte, die dieser bis zu diesem Zeitpunkt automatisch erstellt hat, gelöscht.

Um einen geplanten Bericht zu löschen:

1. Gehen Sie zur Seite **Berichte**.
2. Wählen Sie den Bericht, die Sie löschen möchten.
3. Klicken Sie auf die Schaltfläche − **Löschen** auf der rechten Seite der Tabelle.

9.4. Berichte speichern

Standardmäßig werden geplante Berichte automatisch im Control Center gespeichert.

Wenn Sie Berichte über einen längeren Zeitraum hin benötigen, können Sie sie auf Ihrem Computer abspeichern. Die Zusammenfassung des Berichts ist im PDF-Format verfügbar; die Berichtsdetails sind jedoch nur im CSV-Format verfügbar.

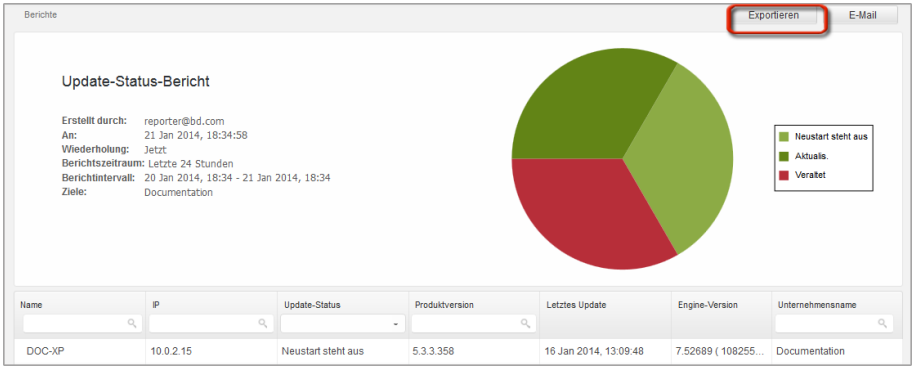
Sie können Berichte auf zweierlei Weise speichern:

- Exportieren
- Download

9.4.1. Berichte exportieren

So exportieren Sie den Bericht auf Ihren Computer:

1. Klicken Sie in der oberen rechten Ecke der Berichtseite auf **Exportieren**.



Berichte - Exportoption

2. Wählen Sie das gewünschte Format für den Bericht:
   - Portabeles Dokumentenformat (PDF) oder
   - Comma-separated values (CSV)
3. Je nach Ihren Browser-Einstellungen wird die Datei automatisch an einen Standard-Speicherort heruntergeladen, oder es wird ein Download-Fenster angezeigt, in dem Sie den Zielordner angeben können.

9.4.2. Berichte herunterladen

Einen Berichtsarchiv enthält sowohl die Zusammenfassung als auch die Details eines Berichts.

So laden Sie ein Berichtsarchiv herunter:

1. Gehen Sie zur Seite **Berichte**.
2. Wählen Sie den Bericht, den Sie speichern möchten.
3. Klicken Sie auf die Schaltfläche **Herunterladen** und wählen Sie entweder **Letzte Instanz**, um die zuletzt erstellte Instanz des Berichts herunterzuladen, oder **Vollständiges Archiv**, um ein Archiv herunterzuladen, das sämtliche Instanzen enthält.

   Je nach Ihren Browser-Einstellungen wird die Datei automatisch an einen Standard-Speicherort heruntergeladen, oder es wird ein Download-Fenster angezeigt, in dem Sie den Zielordner angeben können.

9.5. Berichte per E-Mail versenden

Sie können Berichte mit den folgenden Optionen per E-Mail versenden:

1. Um einen Bericht, den Sie gerade anzeigen, per E-Mail zu versenden, klicken Sie auf die Schaltfläche **E-Mail** in der rechten oberen Ecke der Berichtsseite. Der Bericht wird an die mit Ihrem Konto verknüpften E-Mail-Adresse gesendet.
2. So konfigurieren Sie den Versand geplanter Berichte per E-Mail:
   a. Gehen Sie zur Seite **Berichte**.
   b. Klicken Sie auf den gewünschten Berichtnamen.
   c. Wählen Sie unter **Optionen > Zustellung** den Punkt **Per E-Mail senden an**.
   d. Geben Sie die gewünschte E-Mail-Adresse im Feld darunter ein. Sie können beliebig viele E-Mail-Adressen hinzufügen.
   e. Klicken Sie auf **Speichern**.

Beachten Sie
In der PDF-Datei, die per E-Mail gesendet wird, sind nur die Berichtszusammenfassung und das Diagramm enthalten. Die Berichtsdetails sind in der CSV-Datei enthalten.

9.6. Berichte ausdrucken

Das Control Center verfügt derzeit über keine Druckoptionen.Um einen Bericht zu drucken, müssen Sie ihn zunächst auf Ihrem Computer speichern.

10. Quarantäne

Standardmäßig isoliert Endpoint Security verdächtige Dateien sowie mit Malware infizierte Dateien, die nicht desinfiziert werden können, in einem sicheren Bereich, der als Quarantäne bezeichnet wird. Die in der Quarantäne enthaltenen Dateien können weder ausgeführt noch geöffnet werden.

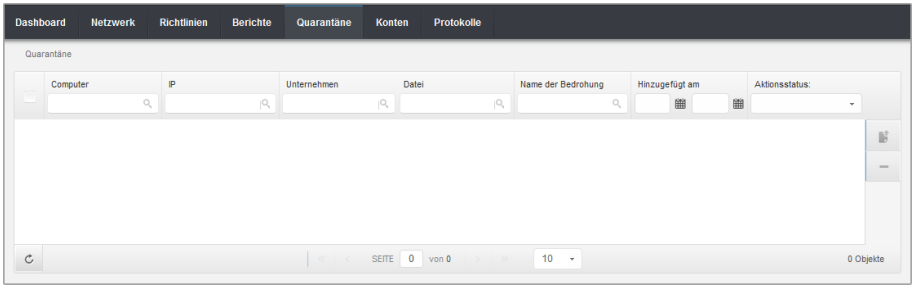
Security for Endpoints speichert die in die Quarantäne verschobenen Dateien auf jedem verwalteten Computer. Über das Control Center können Sie einzelne Dateien in der Quarantäne löschen oder wiederherstellen.

Dateien in Quarantäne werden standardmäßig an die Bitdefender-Labore geschickt, damit Sie dort von den Bitdefender-Malware-Forschern analysiert werden können. Sollten das Vorhandensein von Malware bestätigt werden, wird eine Signatur veröffentlicht, um das Entfernen der Malware zu ermöglichen.

Zudem werden die Dateien in Quarantäne nach jedem Update der Malware-Signaturen gescannt. Gesäuberte Dateien werden automatisch an ihren Ursprungsort zurück gelegt.

Über das Control Center erhalten Sie detaillierte Informationen über alle Dateien, die auf den über Ihr Konto verwalteten Netzwerkobjekten in die Quarantäne verschoben wurden.

Um Dateien in Quarantäne zu überprüfen und zu verwalten, gehen Sie zur **Quarantäne**-Seite.



Die Quarantäneübersicht

Informationen über Dateien in Quarantäne werden in einer Tabelle angezeigt.Sie erhalten die folgenden Informationen:

- Der Name des Netzwerkobjekts, auf dem die Bedrohung gefunden wurde.
- Die IP des Netzwerkobjekts, auf dem die Bedrohung gefunden wurde.
- Pfad zu der infizierten oder verdächtigen Datei auf dem Netzwerkobjekt, auf dem sie gefunden wurde.

- Der Name, den die Bitdefender-Sicherheitsexperten der Malware-Bedrohung gegeben haben.
- Zeitpunkt, zu dem die Datei in Quarantäne verschoben wurde.
- Ausstehende Aktion, die vom Administrator für die Datei in Quarantäne angefordert wurde.

Um sicherzustellen, dass die neuesten Informationen angezeigt werden, klicken Sie im unteren linken Bereich der Tabelle auf **Aktualisieren**.Dies könnte notwendig werden, wenn Sie mehr Zeit auf der Seite verbringen.

10.1. Navigation und Suche

Je nach der Anzahl der verwalteten Netzwerkobjekte und der Art der Infektion kann die Anzahl der Dateien in der Quarantäne manchmal sehr hoch sein.Die Tabelle kann sich über mehrere Seiten erstrecken (standardmäßig werden pro Seite nur 10 Einträge angezeigt).

Verwenden Sie die Navigationsschaltflächen am unteren Rand der Tabelle, um zwischen den Seiten zu wechseln.Um die Anzahl der Einträge zu ändern, die pro Seite angezeigt werden, wählen Sie die entsprechende Option aus dem Menü neben den Navigationsschaltflächen aus.

Sollten zu viele Einträge angezeigt werden, können Sie die Suchfelder unterhalb der Spaltenüberschriften verwenden, um die angezeigten Daten zu filtern.Sie können beispielsweise nach einer bestimmten Bedrohung suchen, die im Netzwerk gefunden wurde, oder nach einem bestimmten Netzwerkobjekt.Sie können auch auf die Spaltenüberschriften klicken, um Daten nach einer bestimmten Spalte zu ordnen.

10.2. Dateien aus der Quarantäne wiederherstellen

Es kann vorkommen, dass Sie Dateien in Quarantäne an ihrem Ursprungsort oder an anderer Stelle wiederherstellen müssen.So zum Beispiel, wenn Sie wichtige Dateien wiederherstellen möchten, die einem infizierten Archiv gespeichert sind, das in Quarantäne verschoben wurde.

Um eine oder mehrere Dateien in Quarantäne wiederherzustellen:

1. Öffnen Sie die **Quarantäne**-Seite.
2. Markieren Sie die Kästchen für die Dateien in Quarantäne, die Sie wiederherstellen möchten.
3. Klicken Sie auf die Schaltfläche **Wiederherstellen** auf der rechten Seite der Tabelle.
4. Wählen Sie den Speicherort aus, an dem Sie die ausgewählten Dateien wiederherstellen möchten (entweder der ursprüngliche Speicherort oder ein benutzerdefinierter Speicherort auf dem Ziel-Computer).

Wenn die Wiederherstellung an einem benutzerdefinierten Speicherort stattfinden soll, müssen Sie den Pfad in das entsprechende Feld eingeben.Es empfiehlt sich, (nach Möglichkeit) Systemvariablen zu verwenden, um sicherzustellen, dass der Pfad auf allen Computern gültig ist. Weitere Informationen finden Sie unter „Systemvariablen verwenden“ (S. 145).

5. Klicken Sie auf **Wiederherstellen**, um die Aktion zum Wiederherstellen einer Datei anzufordern.Die ausstehende Aktion können Sie in der Spalte **Aktion** sehen.
6. Die angeforderte Aktion wird sofort an die Ziel-Computer geschickt bzw. sobald diese wieder online sind.Sobald eine Datei wiederhergestellt ist, wird der entsprechende Eintrag in der Quarantäne-Tabelle nicht mehr auftauchen.

10.3. Dateien in der Quarantäne automatisch löschen

Standardmäßig werden Dateien in der Quarantäne, die älter als 30 Tage sind, automatisch gelöscht.Sie können diese Einstellung ändern, indem Sie die den verwalteten Netzwerkobjekten zugewiesene Richtlinie bearbeiten.

Um das Intervall für die automatische Löschung von Dateien in Quarantäne zu ändern:

1. Gehen Sie zur **Richtlinien**-Seite.
2. Lokalisieren Sie die Richtlinie, die den Netzwerkobjekten zugewiesen wurde, auf denen Sie die Einstellung ändern möchten, und klicken Sie auf ihren Namen.
3. Öffnen Sie den Bereich **Malware-Schutz > Quarantäne**.
4. Wählen Sie den gewünschten Zeitraum für das automatische Löschen aus dem Menü.
5. Klicken Sie auf **Speichern**, um die Änderungen zu speichern.

10.4. Dateien in der Quarantäne löschen

Wenn Sie Dateien in der Quarantäne von Hand löschen möchten, sollten Sie zunächst sicherstellen, dass die von Ihnen ausgewählten Dateien nicht mehr gebraucht werden.Denken Sie an diese Tipps, wenn Sie Dateien in Quarantäne löschen:

- Eine Datei kann unter Umständen auch selbst die Malware sein. Sollten Ihre Nachforschungen dies ergeben, können Sie die Quarantäne nach dieser speziellen Bedrohung durchsuchen und sie aus der Quarantäne löschen.
- Das Folgende können Sie bedenkenlos löschen:
  - Unwichtige Archivdateien.
  - Infizierte Setup-Dateien.

Um eine oder mehrere Dateien in Quarantäne zu löschen:

1. Öffnen Sie die **Quarantäne**-Seite.

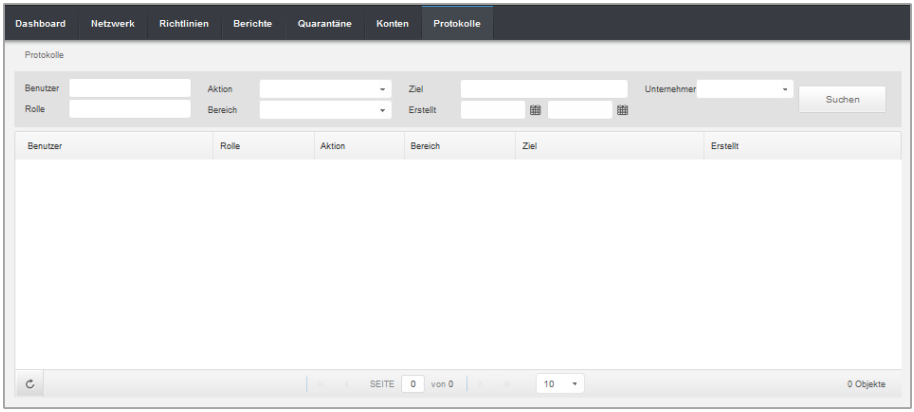
2. Überprüfen Sie die Liste der Dateien in Quarantäne und markieren Sie die Kästchen für die Einträge, die Sie löschen möchten.
3. Klicken Sie auf die Schaltfläche − **Löschen** auf der rechten Seite der Tabelle.Der Status "Ausstehend" wird in der Spalte **Aktion** angezeigt.
4. Die angeforderte Aktion wird sofort (bzw. sobald diese wieder online sind) an die entsprechenden Netzwerkobjekte geschickt.Sobald eine Datei gelöscht wurde, wird der entsprechende Eintrag in der Quarantäne-Tabelle nicht mehr auftauchen.

11. Benutzeraktivitätsprotokoll

Das Control Center protokolliert alle von Benutzer ausgeführten Operationen und Aktionen. Protokolllisten enthalten je nach Ihrem Administratorrechten die folgenden Ereignisse:

- Anmelden und Abmelden
- Berichte erstellen, bearbeiten, umbenennen und löschen
- Dashboard-Portlets hinzufügen und entfernen
- Zugangsdaten erstellen, bearbeiten und löschen
- Netzwerkpakete erstellen, modifizieren, herunterladen und löschen
- Netzwerkaufgaben erstellen
- Benutzerkonten erstellen, bearbeiten, umbenennen und löschen
- Computer löschen oder zwischen Gruppen verschieben
- Gruppen erstellen, verschieben, umbenennen und löschen
- Dateien aus der Quarantäne löschen oder wiederherstellen
- Benutzerkonten erstellen, bearbeiten und löschen
- Richtlinien erstellen, bearbeiten, umbenennen, zuweisen und löschen

Um die Aufzeichnungen über die Aktivitäten der Benutzer einzusehen, öffnen Sie die **Protokolle**übersicht.



Die Protokollübersicht

Um aufgezeichnete Ereignisse anzuzeigen, an denen Sie interessiert sind, müssen Sie eine Suche definieren. Geben Sie die Suchkriterien in die verfügbaren Felder ein und klicken Sie auf **Suchen**. Alle zu Ihren Kriterien passenden Einträge werden in der Tabelle angezeigt.

Die Spalten geben nützliche Informationen zu den aufgelisteten Ereignissen:

- Der Name des Benutzers, der die Aktion durchgeführt hat.
- Benutzerrolle.
- Aktion, die das Ereignis ausgelöst hat.
- Art des Konsolenobjekts, das von der Aktion betroffen ist.
- Bestimmtes Konsolenobjekt, das von der Aktion betroffen ist.
- Zeitpunkt, zu dem das Ereignis eingetreten ist.

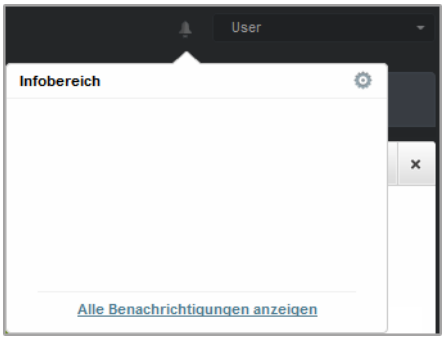
Um Ereignisse nach einer Spalte zu ordnen, klicken Sie einfach auf die Überschrift der jeweiligen Spalte. Klicken Sie erneut auf die Spaltenüberschrift, um die Sortierungsreihenfolge umzukehren.

Um Details zu einem Ereignis anzuzeigen, wählen Sie es aus und sehen Sie in den Abschnitt unter der Tabelle.

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

12. Benachrichtigungen

Je nach den Ereignissen, die in Ihrem Netzwerk auftreten, wird das Control Center verschiedene Benachrichtigungen anzeigen, die Sie über den Sicherheitsstatus Ihrer Umgebung auf dem Laufenden halten.Die Benachrichtigungen werden im **Benachrichtigungsbereich** in der oberen rechten Ecke des Control Center angezeigt.



Infobereich

Wenn ein neues Ereignis im Netzwerk gefunden wird, wird im Benachrichtigungsbereich ein rotes Symbol angezeigt, dass die Zahl der neu gefundenen Ereignisse angibt. Klicken Sie auf das Symbol, um eine Liste der gefundenen Ereignisse anzuzeigen.

12.1. Benachrichtigsarten

Hier eine Liste der verfügbaren Benachrichtigungstypen:

Malware-Ausbruch
Diese Benachrichtigung wird an Benutzer gesendet, die mindestens 5 % ihrer verwalteten Netzwerkobjekte mit derselben Malware infiziert haben.

Update verfügbar
Informiert Sie über ein neues zur Verfügung stehendes Small Office Security-Update.

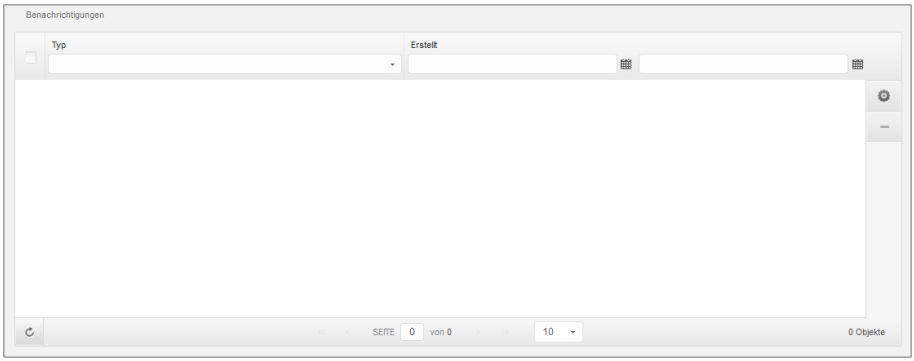
Lizenz läuft ab
Diese Benachrichtigung wird 30 und 7 Tage vor Ablauf der Lizenz sowie am Tag des Ablaufs selbst gesendet.

Benutzergrenze der Lizenz ist bald erreicht
Diese Benachrichtigung wird gesendet, wenn 90 % der verfügbaren Lizenzen vergeben sind.

Die Benutzergrenze der Lizenz ist erreicht
Diese Benachrichtigung wird gesendet, wenn alle verfügbaren Lizenzen vergeben sind.

12.2. Benachrichtigungen anzeigen

Sie können die Benachrichtigungen anzeigen, indem Sie auf die Schaltfläche **Benachrichtigungsbereich** und anschließend auf **Alle Benachrichtigungen anzeigen** klicken. Eine Tabelle mit allen Benachrichtigungen wird angezeigt.



Die Benachrichtigungsübersicht

Abhängig von der Anzahl der Benachrichtigungen kann sich die Benachrichtigungstabelle über mehrere Seiten erstrecken (standardmäßig werden nur 10 Einträge pro Seite angezeigt).

Verwenden Sie die Navigationsschaltflächen am unteren Rand der Tabelle, um zwischen den Seiten zu wechseln.

Um die Anzahl der Einträge zu ändern, die pro Seite angezeigt werden, wählen Sie die entsprechende Option aus dem Menü neben den Navigationsschaltflächen aus.

Sollten zu viele Einträge angezeigt werden, können Sie die Suchfelder unterhalb der Spaltenüberschriften oder das Filtermenü über der Tabelle verwenden, um die angezeigten Daten zu filtern.Sie können zum Beispiel nach einem bestimmten Typ von Benachrichtigung suchen oder nur die in einem bestimmten Zeitraum erstellten Benachrichtigungen anzeigen.

- Sie können die Benachrichtigungen Filtern, indem Sie den gewünschten Benachrichtigungstyp aus dem Menü **Typ** wählen. Optional können Sie auch den Zeitraum, in dem die Benachrichtigungen erstellt wurden, eingrenzen, um die Zahl der in der Tabelle angezeigten Einträge zu verringern, besonders wenn sehr viele Benachrichtigungen erstellt worden sind.

- Wenn Sie auf den Namen einer Benachrichtigung in der Tabelle klicken, werden weitere Details zu ihr angezeigt. Unter der Tabelle wird der Bereich **Details** angezeigt, in dem das Ereignis angezeigt wird, dass die Benachrichtigung verursacht hat.

12.3. Benachrichtigungen löschen

So löschen Sie Benachrichtigungen:

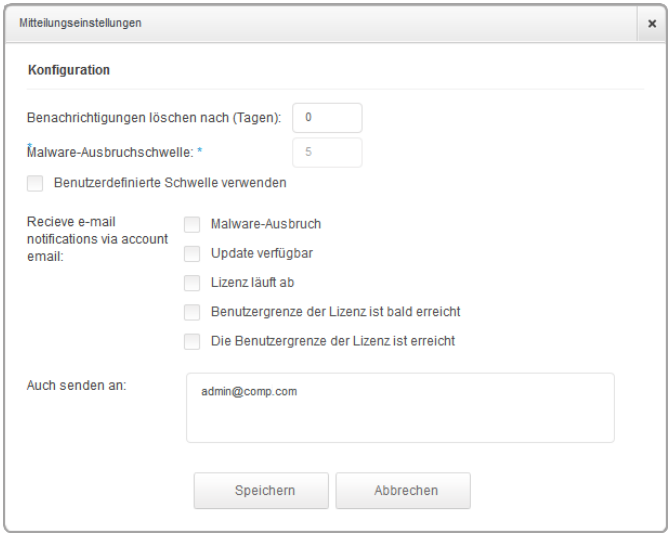
1. Klicken Sie auf die Schaltfläche **Benachrichtigungsbereich** auf der rechten Seite der Menüleiste und anschließend auf **Alle Benachrichtigungen anzeigen**. Eine Tabelle mit allen Benachrichtigungen wird angezeigt.
2. Wählen Sie die Benachrichtigungen, die Sie löschen möchten.
3. Klicken Sie auf die Schaltfläche **Löschen** auf der rechten Seite der Tabelle.

12.4. Benachrichtigungseinstellungen konfigurieren

Die Benachrichtigungstypen, die gesendet werden, sowie die E-Mail-Adresse, an die sie gesendet werden, können für jeden Benutzer einzeln festgelegt werden.

So konfigurieren Sie die Benachrichtigungseinstellungen:

1. Klicken Sie auf die Schaltfläche **Benachrichtigungsbereich** auf der rechten Seite der Menüleiste und anschließend auf **Alle Benachrichtigungen anzeigen**. Eine Tabelle mit allen Benachrichtigungen wird angezeigt.
2. Klicken Sie auf die Schaltfläche **Konfigurieren** auf der rechten Seite der Tabelle. Das Fenster **Benachrichtigungsseinstellungen** wird angezeigt.



Mitteilungseinstellungen

Beachten Sie

Sie können das Fenster für die **Benachrichtigungseinstellungen** auch direkt über das **Konfigurieren**-Symbol oben rechts im **Infobereich**-Fenster aufrufen.

3. Wählen Sie die gewünschten Benachrichtigungstypen aus der Liste.Weitere Informationen finden Sie unter „Benachrichtigsarten“ (S. 135)
4. Wenn Sie möchten, können Sie die Benachrichtigungen per E-Mail an eine bestimmte E-Mail-Adresse senden lassen. Geben Sie die E-Mail-Adressen in das dafür vorgesehene Feld ein; drücken Sie die Eingabetaste zwischen mehreren Adressen.
5. Klicken Sie auf **Speichern**.

13. Hilfe erhalten

Bitdefender hat es sich zur Aufgabe gemacht, seinen Kunden beispiellos schnellen und sorgfältigen Support zu bieten.Sollten Probleme im Zusammenhang mit Ihrem Bitdefender-Produkt auftreten oder Sie Fragen dazu haben, so wenden Sie sich bitte an unser Online-Support-Center. Dort gibt es verschiedene Ressourcen, mit deren Hilfe Sie schnell die richtige Lösung oder Antwort finden können.Sie können auch das Kundenbetreuungs-Team von Bitdefender kontaktieren. Unsere Kundenbetreuer beantworten Ihre Fragen zügig und bieten Ihnen die benötigte Unterstützung.

13.1. Bitdefender-Support-Center

Im Bitdefender-Support-Center unter http://enterprise.bitdefender.com/support unterstützen wir Sie in allen Belangen rund um Ihr Bitdefender-Produkt.

Dabei stehen Ihnen verschiedene Ressourcen zur Verfügung, um die richtige Lösung oder Antwort zu finden:

- Artikel in der Wissensdatenbank
- Bitdefender-Support-Forum
- Produktdokumentation

Zudem können Sie auch Ihre favorisierte Suchmaschine nutzen, um mehr zu erfahren über Computersicherheit, die Bitdefender-Produkte und das Unternehmen.

Artikel in der Wissensdatenbank

Die Bitdefender-Wissensdatenbank ist eine Online-Datenbank mit Informationen rund um die Bitdefender-Produkte. Hier sind in einem leicht zugänglichen Format Berichte zu den Ergebnissen des fortlaufenden technischen Supports sowie der Bugfix-Aktivitäten der Bitdefender-Support- und Entwicklungsteams gespeichert. Hinzu kommen Artikel zur Virenvorbeugung, detaillierte Erklärungen zur Verwaltung von Bitdefender-Lösungen und vieles mehr.

Die Bitdefender-Wissensdatenbank ist öffentlich zugänglich und komplett durchsuchbar. Die darin enthaltenen Informationen sind äußerst umfangreich und stellen eine weitere Methode dar, mit der Bitdefender-Kunden mit dem notwendigen technischen Wissen versorgt werden. Alle berechtigen Informationsanfragen oder Fehlermeldungen von Bitdefender-Kunden finden sich über kurz oder lang im Bitdefender-Wissensdatenbank wieder und dienen als Bugfix-Anleitungen, Umgehungslösungen oder Informationsartikel, die die Hilfedateien des Produkts ergänzen sollen.

Die Bitdefender-Wissensdatenbank für Unternehmensprodukte steht Ihnen jederzeit unter http://enterprise.bitdefender.com/support zur Verfügung.

Bitdefender-Support-Forum

Das Bitdefender-Support-Forum bietet Bitdefender-Anwendern eine Möglichkeit, schnelle Hilfe zu erhalten oder anderen Hilfestellung zu geben.Hier können Sie Ihre Probleme und Fragen rund um Ihr Bitdefender-Produkt posten.

Support-Techniker von Bitdefender überwachen neue Einträge in das Forum, um Ihnen helfen zu können. Außerdem können Sie eine Antwort auf Ihre Frage oder einen Lösungsvorschlag von einem bereits erfahrenen Bitdefender-Anwender erhalten.

Bevor Sie einen Eintrag ins Forum stellen, suchen Sie bitte im Forum nach einem ähnlichen oder verwandten Themenbereich.

Das Bitdefender Support-Forum finden Sie unter http://forum.bitdefender.com. Es steht in 5 verschiedenen Sprachen zur Verfügung: Englisch, Deutsch, Französisch, Spanisch und Rumänisch.Mit einem Klick auf **Business Protection** gelangen Sie in den Bereich Unternehmensprodukte.

Produktdokumentation

Die Produktdokumentation ist die umfassendste Informationsquelle rund um Ihr Produkt.

Die neuesten Versionen der Dokumentation für Bitdefender-Unternehmensprodukte finden Sie zum Lesen und Herunterladen unter Support Center > Dokumentation.

13.2. Hilfe anfordern

Nutzen Sie das Online-Support-Center, um Unterstützung anzufordern:

1. Gehen Sie zu http://www.bitdefender.de/support/contact-us.html.
2. Im Kontaktformular können Sie ein E-Mail-Support-Ticket eröffnen oder auf weitere Kontaktoptionen zugreifen.

13.3. Verwenden des Support-Tools

Das Support-Tool von Small Office Security ermöglicht Benutzern und Support-Mitarbeitern den schnellen Zugriff auf alle Informationen, die Sie zur Lösung von Problemen benötigen.Führen Sie das Support-Tool auf den betroffenen Computern aus und senden Sie das daraufhin erstellte Archiv mit den Informationen für die Fehlersuche an einen Bitdefender-Support-Mitarbeiter.

Um das Support-Tools zu verwenden:

1. Laden Sie das Support-Tool herunter und bringen Sie sie auf die betroffenen Computer aus.Um das Support-Tool herunterzuladen:
   a. Bauen Sie über Ihr Konto eine Verbindung mit der Control Center auf.
   b. Klicken Sie in der unteren rechten Bildschirmecke der Konsole auf **Hilfe und Support**.
   c. Die Download-Links finden Sie im **Support**-Bereich.Es stehen zwei Versionen zur Verfügung: eine für 32-Bit-Systeme und eine für 64-Bit-Systeme.Stellen Sie sicher, dass Sie die richtige Version verwenden, wenn Sie das Support-Tool auf einem Computer ausführen.
2. Führen Sie das Support-Tool lokal auf jedem der betroffenen Computer aus.
   a. Markieren Sie das Zustimmungskästchen und klicken Sie auf **Weiter**.
   b. Geben Sie in das Formular die nötigen Daten ein:
      i. Geben Sie Ihre E-Mail-Adresse ein.
      ii. Geben Sie Ihren Namen ein.
      iii. Wählen Sie Ihr Land aus dem entsprechenden Menü.
      iv. Beschreiben Sie im Textfeld das Problem, das aufgetreten ist.
      v. Sie können auch versuchen das Problem zu reproduzieren, bevor Sie mit der Datensammlung beginnen. Gehen Sie in diesem Fall folgendermaßen vor:
         A. Aktivieren Sie die Option **Versuchen Sie, das Problem vor der Übertragung zu reproduzieren**.
         B. Klicken Sie auf **Weiter**.
         C. Wählen Sie die Art des aufgetretenen Problems.
         D. Klicken Sie auf **Weiter**.
         E. Reproduzieren Sie das Problem auf Ihrem Computer. Kehren Sie danach zum Support-Tool zurück und wählen Sie die Option **Ich habe das Problem reproduziert**.
   c. Klicken Sie auf **Weiter**.Das Support Tool sammelt Produktinformationen, Informationen zu anderen Anwendungen, die auf ihrem System installiert sind sowie die Software und Hardware Konfiguration.
   d. Warten Sie, bis der Vorgang beendet ist.
   e. Klicken Sie auf **Beenden**, um das Fenster zu schließen.Es wurde ein ZIP-Archiv auf Ihrem Desktop erstellt.

      Schicken Sie das ZIP-Archiv gemeinsam mit Ihrer Anfrage an einen Bitdefender-Support-Mitarbeiter. Verwenden Sie dafür das E-Mail-Support-Ticket-Formular auf der **Hilfe und Support**-Seite der Konsole.

13.4. Kontaktinformation

Effiziente Kommunikation ist der Schlüssel zu einem erfolgreichen Unternehmen. Seit mehr als 10 Jahren überbietet Bitdefender konstant die bereits hochgesteckten Erwartungen seiner Kunden und Partner und diese Tradition wollen wir auch in Zukunft fortführen. Für jedwede Fragen stehen wir Ihnen gerne zur Verfügung.

13.4.1. Kontaktadressen

Vertrieb: enterprisesales@bitdefender.com
Support-Center:http://enterprise.bitdefender.com/support
Dokumentation: documentation@bitdefender.com
Lokale Vertriebspartner:http://www.bitdefender.de/partners
Partnerprogramm: partners@bitdefender.com
Presse: presse@bitdefender.de
Jobs: jobs@bitdefender.de
Virus-Einsendungen: virus_submission@bitdefender.com
Spam-Einsendungen: spam_submission@bitdefender.com
Report Abuse: abuse@bitdefender.com
Website:http://enterprise.bitdefender.com/de

13.4.2. Bitdefender-Niederlassungen

Bitdefender-Niederlassungen stehen Ihnen für betriebliche und allgemeine Fragen und Informationen in ihren jeweiligen Bereichen jederzeit zur Verfügung. Die genauen Kontaktdaten und Adressen finden Sie in der unten stehenden Auflistung.

Spain

Bitdefender España, S.L.U.
Avda. Diagonal, 357, 1º 1ª
08037 Barcelona
España
Fax: (+34) 93 217 91 28
Telefon (Geschäftsstelle&Vertrieb): (+34) 93 218 96 15
Telefon (Technischer Support): (+34) 93 502 69 10
Vertrieb: comercial@bitdefender.es
Webseite: http://www.bitdefender.es
Support-Center: http://www.bitdefender.es/businesshelp

USA

Bitdefender, LLC

PO Box 667588
Pompano Beach, Fl 33066
United States
Telefon (Vertrieb&Technischer Support): 1-954-776-6262
Vertrieb: sales@bitdefender.com
Web: http://www.bitdefender.com
Support-Center: http://www.bitdefender.com/businesshelp

Deutschland

Bitdefender GmbH
Airport Office Center
Robert-Bosch-Straße 2
59439 Holzwickede
Deutschland
Telefon (Geschäftsstelle&Vertrieb): +49 (0)2301 91 84 222
Telefon (Technischer Support): +49 (0)2301 91 84 444
Vertrieb: vertrieb@bitdefender.de
Webseite: http://www.bitdefender.de
Support-Center: http://www.bitdefender.de/businesshelp

Großbritannien und Irland

Genesis Centre Innovation Way
Stoke-on-Trent, Staffordshire
ST6 4BF
UK
Telefon (Vertrieb&Technischer Support): +44 (0) 8451-305096
E-Mail: info@bitdefender.co.uk
Vertrieb: sales@bitdefender.co.uk
Webseite: http://www.bitdefender.co.uk
Support-Center: http://www.bitdefender.co.uk/businesshelp

Rumänien

BITDEFENDER SRL
DV24 Offices, Building A
24 Delea Veche Street
024102 Bucharest, Sector 2
Fax: +40 21 2641799
Telefon (Vertrieb&Technischer Support): +40 21 2063470
Vertrieb: sales@bitdefender.ro
Webseite: http://www.bitdefender.ro
Support-Center: http://www.bitdefender.ro/businesshelp

Vereinigte Arabische Emirate

Bitdefender FZ-LLC
Dubai Internet City, Building 17
Office # 160
Dubai, UAE
Telefon (Vertrieb&Technischer Support): 00971-4-4588935 / 00971-4-4589186
Fax: 00971-4-44565047
Vertrieb: sales@bitdefender.com
Web: http://www.bitdefender.com/world
Support-Center: http://www.bitdefender.com/businesshelp

A. Anhänge

A.1. Liste der Anwendungsdateitypen

Die Malware-Prüf-Engines von Bitdefender-Sicherheitslösungen können so eingerichtet werden, dass nur Anwendungsdateien geprüft werden. Anwendungsdateien sind weitaus anfälliger für Malware-Angriffe als andere Dateitypen.

Diese Kategorie beinhaltet Dateien mit folgenden Erweiterungen:

```
386; a6p; ac; accda; accdb; accdc; accde; accdp; accdr; accdt; accdu;
acl; acr; action; ade; adp; air; app; as; asd; asp; awk; bas; bat;
bin; cgi; chm; cla; class; cmd; cnv; com; cpl; csc; csh; dat; dek;
dld; dll; doc; docm; docx; dot; dotm; dotx; drv; ds; ebm; esh; exe;
ezs; fky; frs; fxp; gadget; grv; hlp; hms; hta; htm; html; iaf; icd;
ini; inx; ipf; isu; jar; js; jse; jsx; kix; laccdb; lnk; maf; mam;
maq; mar; mat; mcr; mda; mdb; mde; mdt; mdw; mem; mhtml; mpp; mpt;
mpx; ms; msg; msi; msp; mst; msu; oab; obi; obs; ocx; oft; ole; one;
onepkg; ost; ovl; pa; paf; pex; pfd; php; pif; pip; pot; potm; potx;
ppa; ppam; pps; ppsm; ppsx; ppt; pptm; pptx; prc; prf; prg; pst; pub;
puz; pvd; pwc; py; pyc; pyo; qpx; rbx; rgs; rox; rpj; rtf; scar; scr;
script; sct; shb; shs; sldm; sldx; smm; snp; spr; svd; sys; thmx;
tlb; tms; u3p; udf; url; vb; vbe; vbs; vbscript; vxd; wbk; wcm; wdm;
wiz; wll; wpk; ws; wsf; xar; xl; xla; xlam; xlb; xlc; xll; xlm; xls;
xlsb; xlsm; xlsx; xlt; xltm; xltx; xlw; xml; xqt; xsf; xsn; xtp
```

A.2. Systemvariablen verwenden

Für einige der in der Konsole verfügbaren Einstellungen müssen Sie zunächst den Pfad auf dem Ziel-Computern angeben.Es empfiehlt sich, (nach Möglichkeit) Systemvariablen zu verwenden, um sicherzustellen, dass der Pfad auf allen Computern gültig ist.

Im Folgenden finden Sie eine Liste der vordefinierten Systemvariablen:

`%ALLUSERSPROFILE%`
Der Profilordner für alle Benutzer.Typischer Pfad:

`C:\Dokumente und Einstellungen\Alle Benutzer`

`%APPDATA%`
Der Anwendungsdatenordner des angemeldeten Benutzers.Typischer Pfad:

- Windows XP:

`C:\Dokumente und Einstellungen\{username}\Anwendungsdaten`

- Windows Vista/7:

  `C:\Benutzer\{username}\AppData\Roaming`

`%HOMEPATH%`
Die Benutzerordner.Typischer Pfad:

- Windows XP:

  `Dokumente und Einstellungen\{username}`

- Windows Vista/7:

  `\Benutzer\{username}`

`%LOCALAPPDATA%`
Temporäre Dateien von Anwendungen.Typischer Pfad:

`C:\Benutzer\{username}\AppData\Lokal`

`%PROGRAMMDATEIEN%`
Der Programmdateienordner. Meist zu finden unter `C:\Programmdateien`.

`%PROGRAMFILES(X86)%`
Der Programme-Ordner für 32-Bit-Anwendungen (auf 64-Bit-Systemen).Typischer Pfad:

`C:\Programmdateien (x86)`

`%COMMONPROGRAMFILES%`
Der Ordner Gemeinsame Dateien.Typischer Pfad:

`C:\Programmdateien\Gemeinsame Dateien`

`%COMMONPROGRAMFILES(X86)%`
Der Ordner Gemeinsame Dateien für 32-Bit-Anwendungen (auf 64-Bit-Systemen).Typischer Pfad:

`C:\Programmdateien (x86)\Gemeinsame Dateien`

`%WINDIR%`
Der Windows SDatenverzeichnis oder SYSROOT. Meist zu finden unter `C:\Windows`.

Glossar

Adware

Adware wird häufig mit einer anderen Anwendung kombiniert, die kostenlos ist, solange der Nutzer die Adware akzeptiert. Adware-Anwendungen werden in der Regel installiert, nachdem der Nutzer einer Lizenzvereinbarung zugestimmt hat. In der Lizenzvereinbarung wird auch der Zweck der Anwendung genannt, und somit liegt keine Rechtswidrigkeit vor.

Allerdings können Popup-Anzeigen mit der Zeit sehr lästig werden und in manchen Fällen die Systemperformance beeinträchtigen. Zudem kann aufgrund der Daten, die manche dieser Programme sammeln, die Privatsphäre von Nutzern verletzt werden, die sich über die Bedingungen in der Lizenzvereinbarung nicht völlig im Klaren waren.

Archive

Ein Datenträger, ein Magnetband oder ein Ordner mit Dateien, die von einer Datensicherung/BackUp erzeugt wurden.

Eine Datei, die eine oder mehrere Dateien in einem komprimierten Format enthält.

Backdoor (Hintertür)

Eine Sicherheitslücke eines Systems, die der Entwickler oder Administrator absichtlich hinterlässt. Der Grund dafür muss nicht immer bösartig sein. Manche Betriebssysteme haben schon standardmäßig privilegierte Konten eingerichtet, damit diese von den Kundendienst-Technikern oder Programmierern der Hersteller benutzt werden können.

Befehlszeile

Die Befehlszeile ist eine zeichenorientierte Benutzerschnittstelle. Die Kommunikation zwischen Benutzer und Computer findet ausschließlich durch die Eingabe von bestimmten Befehlen statt, die sich aus einzelnen Buchstabenfolgen zusammensetzen. Als Eingabegerät wird eine Tastatur benutzt. Die Verwendung einer Maus ist nicht möglich. Auf der Befehlszeile werden die einzelnen Anweisungen in einer bestimmten Befehlssprache eingegeben, die vom Computer und seiner Software ausgewertet und mit den entsprechenden Ergebnissen auf dem Ausgabegerät (meistens ein Monitor) wieder an den Benutzer übergeben werden.

Bootsektor

Der erste Sektor einer Festplatte oder Diskette. Hier liegen Daten, die das Betriebssystem zum Booten (Starten) braucht.

Bootvirus

Ein Virus, der den Bootsektor einer Festplatte oder eines Diskettenlaufwerks infiziert. Beim Versuch von einer Diskette, die mit einem Bootvirus infiziert ist, zu booten wird dieser im Arbeitsspeicher aktiviert. Bei jedem Neustart wird der Virus so im Arbeitsspeicher aktiviert und überträgt sich auf eingelegte Wechselmedien.

Cookie

In der Internetbranche werden mit Cookies kleine Dateien bezeichnet, die Daten über einzelne Computer enthalten und die von den Werbetreibenden analysiert und verwendet werden, um die Interessen und Vorlieben der Benutzer herauszufinden. Die Cookie-Technologie wird stetig weiterentwickelt mit dem Ziel Benutzern nur noch solche Werbung anzuzeigen, die ihren Interessen entspricht. Für viele ist dies ein zweischneidiges Schwert. Einerseits ist es praktisch, nur Anzeigen zu sehen, an denen man interessiert ist. Anderseits bedeutet es, dass Online-Aktivitäten der Benutzer gewissermaßen auf Schritt und "Klick" verfolgt werden. Es ist also verständlich, dass in diesem Zusammenhang Datenschutz ein umstrittenes Thema ist und viele sich unwohl fühlen, quasi als SKU-Nummer (die Strichcodes auf den Packungen, die im Geschäft an der Theke gescannt werden) betrachtet zu werden. Auch wenn diese Sicht etwas extrem erscheint, ist sie doch manchmal korrekt.

Dateierweiterung

Der Teil hinter dem Punkt im Dateinamen. Die Erweiterung oder Extension beschreibt die Art der Daten, die in einer Datei gespeichert sind.

Viele Betriebssysteme benutzen Dateierweiterungen, z.B. Unix, VMS, MS-DOS. Sie sind gewöhnlich ein bis drei Buchstaben lange (alte Betriebssysteme können oft nicht mehr als drei Buchstaben unterstützen). Beispiele sind "exe" ausführbare Dateien, "ps" für PostScript oder "txt" für Text-Dateien.

Durchsuchen

Kurzform für Web-Browser, ein Programm, mit dem Internetseiten aufgerufen und angezeigt werden können. Die bekanntesten Browser sind Mozilla Firefox und Microsoft Internet Explorer. Beide sind graphische Browser, was bedeutet, dass sie sowohl Grafiken als auch Texte anzeigen können. Weiterhin können die meisten Browser Multimedia-Daten wie Klang- und Videodateien anzeigen, wobei sie für diverse Formate Plug-Ins (zusätzliche Softwarekomponenten) benutzen.

Ereignisanzeige

Ereignisse oder Erscheinungen, die in einem Programm vorkommen. Ereignisse können Benutzeraktionen, wie zum Beispiel Mausklicks oder Tastatureingaben, oder Systemereignisse, wie zum Beispiel ungenügender Speicher, sein.

Fehlalarm

Erscheint, wenn ein Virenscanner eine Datei als infiziert erkennt, obwohl dies nicht der Fall ist.

Heuristik

Eine Methode, um neue Viren zu identifizieren. Diese Scan-Methode benötigt keine spezifischen Virussignaturen. Der Vorteil eines heuristischen Scans ist, dass man nicht von einer neuen Variante eines alten Virus getäuscht werden kann. Manchmal kann jedoch auch ein verdächtiger Code in einem normalen Programm gemeldet werden, ein sogenannter Fehlalarm oder "falsch-positive Meldung" wird angezeigt.

IP

Internet Protocol - Das TCP/IP Protokoll ist verantwortlich für die korrekte IP Adressierung und die korrekte Zustellung der Datenpakete.

Keylogger

Ein Keylogger ist eine Anwendung, die alles aufzeichnet, was Sie tippen.

Keylogger sind an sich nicht schädlich. Sie können auch legitim eingesetzt werden, um beispielsweise die Aktivitäten von Angestellten oder Kindern zu überwachen. Sie werden jedoch zunehmend von Cyber-Kriminellen mit bösartiger Absicht eingesetzt (um beispielsweise private Daten wie Benutzernamen oder Passwörter zu sammeln).

Logdatei (Berichtsdatei)

Eine Datei, die stattgefundene Aktivitäten aufzeichnet. Zum Beispiel speichert Bitdefender eine Prokolldatei mit den gescannten Pfaden, Ordnern, der Anzahl der gescannten Archive und Dateien sowie der Anzahl der gefundenen infizierten oder verdächtigen Dateien.

Makrovirus

Eine Virusform, die in einem Dokument als eingebettetes Makro verschlüsselt wird. Viele Anwendungen, wie Microsoft Word und Excel, unterstützen leistungsstarke Makrosprachen.

Diese Anwendungen ermöglichen das Einbetten eines Makros in ein Dokument, welches dann bei jedem Öffnen des Dokuments ausgeführt wird.Ein Makro ist eine Aufzeichnung des Ablaufs von Routineaufgaben innerhalb des makrofähigen Programms, das dann immer wieder verwendet werden kann.

Malware

Malware ist der Sammelbegriff für alle Software-Arten, die darauf ausgelegt sind, Schaden zu verursachen - das Wort setzt sich zusammen aus den englischen Begriffen malicious und software, also bösartige Software. Der Begriff hat sich noch nicht vollständig durchgesetzt, wird aber immer häufiger als Oberbegriff gebraucht, wenn von Viren, Trojanern, Würmern und Malicious Mobile Code die Rede ist.

Malware-Signatur

Malware-Signaturen sind Codebruchstücke, die aus aktuellen Malware-Beispielen extrahiert werden. Diese werden von Antiviren-Programmen zum Musterabgleich und

zur Aufspürung von Malware verwendet.Signaturen werden auch genutzt, um den Malware-Code aus infizierten Dateien zu entfernen.
Die Bitdefender Malware-Signatur-Datenbank ist eine Sammlung von stündlich durch Bitdefender-Mitarbeiter upgedateten Malware-Signaturen.

Nicht heuristisch

Diese Scan-Methode beruht auf spezifischen Virussignaturen. Der Vorteil eines nicht-heuristischen Scans ist, dass er nicht von einem Scheinvirus getäuscht werden kann und so Fehlalarme verhindert.

Phishing

Das Senden einer E-Mail an einen Benutzer, in der der Sender sich als Vertreter eines legitimen Unternehmens ausgibt und versucht, den Empfänger so zu manipulieren, dass er persönliche Informationen preisgibt, die dann zum Diebstahl der Identität verwendet werden können. Die E-Mail leitet den Benutzer dann auf eine Webseite, auf der er aufgefordert wird, vertrauliche Daten wie Kreditkartennummern, TANs oder PINs preiszugeben. Es wird oft vorgegeben, dass dies aus Gründen der Aktualisierung geschehen soll. Diese Webseiten sind jedoch gefälscht und wurden eigens für den Diebstahl dieser Daten eingerichtet.

Polymorpher Virus

Ein Virus, der seine Form mit jeder Datei, die er infiziert, ändert. Da diese Viren kein beständiges binäres Muster haben, sind sie sehr schwer zu erkennen.

Rootkit

Bei einem Rootkit handelt es sich um eine Sammlung von Software-Tools, mit denen auf ein System mit Administratorrechten zugegriffen werden kann. Der Begriff wurde ursprünglich nur für UNIX-Systeme verwendet und beschrieb rekompilierte Tools, mit denen sich Angreifer Administratorrechte verschaffen und so ihre Anwesenheit vor den tatsächlichen Administratoren verbergen konnten.

Die Hauptaufgabe eines Rootkits besteht darin, Prozesse, Dateien und Protokolle zu verstecken. Sie können auch Daten von Terminals, Netzwerkverbindungen oder Peripheriegeräten abfangen, falls Sie eine entsprechende Software eingebaut haben.

Rootkits sind nicht grundsätzlich schädlich. Einige Systeme und Anwendungen verstecken z. B. wichtige Dateien mithilfe von Rootkits. Sie werden jedoch oft dazu missbraucht, Malware zu verbergen oder unbemerkt einen Eindringling einzuschleusen. In Kombination mit Malware stellen sie eine große Gefahr für Ihr System dar. Denn sie können den Datenverkehr abhören, Sicherheitslücken in Ihrem System schaffen, Dateien und Zugangsdaten verändern, und das alles, ohne entdeckt zu werden.

Schnittstelle

Stelle eines Rechners, an die ein Gerät angeschlossen werden kann. Rechner haben verschiedenartige Schnittstellen. Im Inneren gibt es Schnittstellen zum Anschluss von

Festplatten, Grafikkarten und Tastaturen. Extern haben Rechner Schnittstellen zum Anschluss von Modems, Druckern und anderen Peripheriegeräten.

In TCP/IP und UDP Netzwerken, ein Endpunkt zu logischen Verbindungen. Die Schnittstellennummer gibt die Art der Schnittstelle an. Zum Beispiel, Schnittstelle 80 wird für HTTP Traffic verwendet.

Script

Ein anderer Begriff für Makro- oder Batchdatei. Ein Skript ist eine Befehlsliste, die ohne Benutzereingriff ausgeführt werden kann.

Spam

Junk-E-Mail oder Junk-Postings in Newsgroups. Im Allgemeinen versteht man darunter jede Art von unerwünschter E-Mail.

Spyware

Software, die unentdeckt vom Nutzer private und geheime Anwenderdaten über seine Internetverbindung abgreift. Dies geschieht in der Regel zu Werbezwecken. Typischerweise sind Spyware-Anwendungen als verborgene Komponenten in Freeware- oder Shareware-Programmen enthalten, die aus dem Internet heruntergeladen werden können. Die große Mehrzahl von Shareware- und Freeware-Anwendungen ist natürlich frei von Spyware. Ist die Spyware einmal installiert, überwacht sie die Nutzeraktivitäten und überträgt diese Daten im Hintergrund an einen Dritten. Spyware kann auch Informationen über E-Mail-Adressen und sogar Passwörter und Kreditkartennummern sammeln.

Einem Trojanischen Pferd ähnelt Spyware darin, dass die Anwender das Produkt unwissentlich gemeinsam mit etwas anderem installieren. Opfer von Spyware wird man oft dann, wenn man sich bestimmte Peer-to-Peer-Dateiaustauschprogramme herunterlädt.

Ganz abgesehen von den Fragen der Ethik und des Datenschutzes belegt Spyware auch unnötig Systemressourcen und Bandbreite, indem über die Internetverbindung des Nutzers Informationen an den Spyware-Heimatserver gesendet werden. Da Spyware Speicher und Systemressourcen verbraucht, können die im Hintergrund laufenden Anwendungen zu Systemabstürzen oder allgemeiner Systeminstabilität führen.

Symbolleiste

Die Symbolleiste wurde mit Windows 95 eingeführt und befindet sich auf der Windows Task-Leiste (gewöhnlich unten rechts, dort wo sich auch die Uhrzeit befindet). Sie enthält kleine Symbole zur Information und zum leichteren Zugriff auf Systemfunktionen wie Drucker, Modems, Lautstärke und anderes. Um auf die Details und Optionen dieser Funktionen zuzugreifen, ist ein Doppelklick oder ein Klick mit der rechten Maustaste erforderlich.

TCP/IP

Transmission Control Protocol/Internet Protocol – im Internet weit verbreiteter Netzwerkprotokollsatz, der die Kommunikation zwischen verbundenen Computernetzwerken mit verschiedenen Hardware-Architekturen und Betriebssystemen ermöglicht. TCP/IP bietet eine Möglichkeit, all diese unterschiedlichen Komponenten zu Kommunikationszwecken miteinander zu verbinden.

Trojaner

Ein bösartiges Programm, das sich als eine legitime Anwendung ausgibt. Im Unterschied zu Viren vervielfältigen sich die Trojaner (auch "trojanische Pferde" genannt) nicht, aber sie können ebenso schädlich sein. Einer der heimtückischsten Trojaner ist ein Programm, das behauptet Ihren Rechner von Viren zu befreien, stattdessen aber den Rechner infiziert.

Der Begriff entstammt einer Geschichte in Homers "Ilias", in der die Griechen ihren Feinden, den Trojanern, angeblich als Sühnegabe ein riesiges hölzernes Pferd schenkten. Aber nachdem die Trojaner das Pferd in die Stadt gebracht hatten, schlichen sich die im Bauch des hölzernen Pferdes versteckten Soldaten bei Nacht heraus, öffneten die Tore der Stadt und ermöglichten somit ihren Landsleuten, in die Stadt einzudringen und auf diese Weise Troja zu besetzen.

Update

Eine neue Software- oder Hardwareversion, die eine ältere Version desselben Produkts ersetzt. Die Update-Installationsroutine eines Programms prüft oft, ob eine ältere Versionen auf dem Rechner installiert ist, da sonst kein Update installiert werden kann.

Bitdefender verfügt über ein eigenes Update-Modul, das die manuelle oder automatische Suche nach Updates ermöglicht.

Virus

Ein Programm oder ein Stück Code, das auf einen Rechner kopiert wird und sich allein ausführt, ohne dass es der Besitzer des Rechners will oder merkt. Die meisten Viren können sich auch selbst vervielfältigen. Alle Computerviren wurden von Menschen programmiert. Ein Virus, der sich immer wieder vervielfältigen kann, ist sehr einfach zu programmieren. Sogar ein solch einfacher Virus kann gefährlich sein, da er im Handumdrehen sämtlichen Arbeitsspeicher belegen und so das System lahmlegen kann. Noch gefährlicher sind Viren, die sich über Netzwerke selbst weiterversenden und Sicherheitssysteme umgehen.

Wurm

Ein Programm, das sich selbst kopiert und über ein Netzwerk verbreitet. Es kann sich nicht an andere Programme anhängen.