
Bitdefender ENTERPRISE
BITDEFENDER
SMALL OFFICE
SECURITY
Schnellstart-Anleitung ››

Bitdefender Small Office Security
Schnellstart-Anleitung

Veröffentlicht 2014.06.10


Bitdefender

Inhaltsverzeichnis

1. Über Small Office Security

Mit Small Office Security-On-Premise können Unternehmen die Sicherheit auf ihrer eigenen Infrastruktur hosten und den Schutz für ihre PCs, Macs und Dateiserver selbst schnell und einfach bereitstellen, verwalten und überwachen. Dabei profitieren Sie von der führenden Malware-Erkennung und der neuesten Verwaltungskonsole aus dem Hause Bitdefender.

Anders als die Cloud-Version, die von Bitdefender gehostet wird und keine eigene Infrastruktur benötigt, wird diese Small Office Security-Version in der kundeneigenen Umgebung installiert.

Small Office Security besteht aus den folgenden Komponenten:

- Control Center
- Security for Endpoints
- Security for Mobile Devices

Control Center

Ein web-basiertes Dashboard und zentrale Verwaltungskonsole, die die Sicherheitslage im Unternehmen sowie allgemeine Sicherheitsrisiken transparent macht und dabei die Steuerung der Sicherheitsdienste erlaubt, die die virtuellen und physischeb Arbeitsplatzrechner, Server und Mobilgeräte schützen.

Control Center lässt sich mit den bestehenden Systemverwaltungs- und Überwachungssystemen integrieren und vereinfacht so die automatische Bereitstellung von Schutz auf nicht verwalteten Arbeitsplatzrechnern und Servern.

Security for Endpoints

Bitdefender Security for Endpoints Die Lösung schützt Computer im Hintergrund und setzt dabei auf vielfach ausgezeichnete Malware-Schutz-Technologien kombiniert mit einer Firewall, Angriffserkennung, der Steuerung und Filterung des Internet-Zugangs, dem Schutz von sensiblen Daten und einer Anwendungssteuerung. Security for Endpoints bietet Sicherheit für Computer mit Mac OS X oder Windows sowie für Windows-Server. Die Produktivität der Mitarbeiter wird durch effizienten Ressourceneinsatz, optimierte System-Scans und automatisierte Sicherheit, die ohne Eingriffe des Benutzers auskommt, sichergestellt.

Security for Mobile Devices

Verwaltet und steuert iPhones, iPads und Android-Geräte mit einem universellen auf den Einsatz in Unternehmen ausgelegten Ansatz, der die Geräte durch Echtzeit-Scans schützt

und die Sicherheitsrichtlinien des Unternehmens auf mobilen Geräten anwendet, so z. B. Bildschirmsperrung, Passwortschutz, Verschlüsselung von Wechseldatenträgern, Ortung verlorener Geräte und Zugriffsverweigerung für nicht konforme oder inoffiziell entsperrte Geräte.

2. Systemanforderungen

Alle Small Office Security-Lösungen werden über das Control Center installiert und verwaltet.

2.1. Anforderungen für die Small Office Security-Appliance

Small Office Security wird als virtuelle Appliance angeboten.Die Small Office Security-Appliance steht in den folgenden Formaten zur Verfügung:

- OVA (kompatibel mit VMware vSphere, View)
- XVA (kompatibel mit Citrix XenServer, XenDesktop, VDI-in-a-Box)
- VHD (kompatibel mit Microsoft Hyper-V)
- OVF (kompatibel mit Red Hat Enterprise Virtualization)*
- OVF (kompatibel mit Kernel-based Virtual Machine oder KVM)*
- RAW (kompatibel mit Oracle VM)*

*OVF- und RAW-Pakete sind im Format tar.bz2 gepackt.

Bitte wenden Sie sich an Bitdefender, falls Sie Unterstützung für weitere Formate oder Virtualisierungsplattformen wünschen.

2.1.1. Hardware-Anforderungen

Die folgende Tabelle enthält die Hardware-Anforderungen für die Small Office Security-Appliance je nach Anzahl der verwalteten Netzwerkobjekte.

Anzahl geschützter Objekte	RAM	HD	CPUs
1-250 Endpunkte 1-250 Mobilgeräte	4 GB	40 GB	2 virtuelle CPUs (mit je 2 GHz)
250-1000 Endpunkte 250-1000 Mobilgeräte	8 GB	60 GB	4 virtuelle CPUs (je 2GHz)

2.1.2. Internet-Verbindung

Die Small Office Security-Appliance benötigt eine aktive Internet-Verbindung.

2.1.3. Anforderungen Control Center-Web-Konsole

Folgendes wird benötigt, um die Control Center-Web-Konsole aufzurufen:

- Internet Explorer 9+, Mozilla Firefox 14+, Google Chrome 15+, Safari 5+
- Empfohlene Bildschirmauflösung: 1280x800 oder höher.
- Der Computer, von dem aus Sie eine Verbindung herstellen, muss im Netzwerk mit der Control Center-Appliance verbunden sein.

Warnung
Control Center funktioniert in der Kompatibilitätsansicht des Internet Explorer 9+ nicht bzw. wird nicht richtig angezeigt. Es ist, als würden Sie eine nicht unterstützte Browserversion benutzen.

2.2. Anforderungen für Security for Endpoints

2.2.1. 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 8.1 Industry
- Windows Embedded 8 Standard
- 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

2.2.2. 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.

2.2.3. Unterstützte Web-Browser

Security for Endpoints funktioniert mit folgenden Browsern:

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

2.3. Security for Mobile Devices-Anforderungen

2.3.1. Unterstützte Plattformen

Security for Mobile Devices unterstützt die folgenden Mobilgeräte und Betriebssysteme:

- Apple iPhones und iPads (iOS 5.1+)
- Smartphones und Tablets mit Google Android (2.3+)

2.3.2. Verbindunugngsanforderungen

Mobile Geräte müssen eine aktive und funktionierende Funk-Daten- oder WLAN-Verbindung mit dem Kommunikationsserver haben.

2.3.3. Push-Benachrichtigungen

Security for Mobile Devices verwendet Push-Benachrichtigungen, um Mobile Clients darauf hinzuweisen, dass Richtlinien-Updates oder Aufgaben bereit stehen. Push-Benachrichtigungen werden vom Kommunikationsserver über den Dienst gesendet, der vom Hersteller des Betriebssystems dafür vorgesehen ist:

- Google Cloud Messaging (GCM) bei Android-Geräten. Damit GCM funktioniert, müssen die folgenden Bedingungen erfüllt sein:
  - Google Play Store muss installiert sein.
  - Geräte, auf denen eine ältere Version als Android 4.0.4 läuft, müssen außerdem mindestens angemeldetes Google-Konto haben.
  - Um Push-Benachrichtigungen zu senden, müssen eine bestimmte Anzahl an Ports offen sein.
- Apple Push Notifications (APNs) bei iOS-Geräten. Weitere Informationen finden Sie in diesem Artikel der Wissensdatenbank.

Mehr über die Verwaltung von mobilen Gräten mit Small Office Security erfahren Sie in diesem Artikel.

2.3.4. Zertifikate für die iOS-Geräteverwaltung

Um die Infrastruktur zur Verwaltung von iOS-Mobilgeräten einzurichten, benötigen Sie bestimmte Zertifikate.

Weitere Informationen finden Sie unter Certificates.

2.4. Small Office Security-Kommunikations-Ports

In der folgenden Tabelle sind die Ports angegeben, die von den Small Office Security-Komponenten benutzt werden:

Schnittstelle	Nutzung
80 (HTTP) / 443 (HTTPS)	Port für den Zugriff auf Control Center.
8443 (HTTPS)	Port für die Verbindung der Client/Agend-Software mit dem Kommunikationsserver.
7074 (HTTP)	Update Server Port:
7075	Sorgt für die Kommunikation zwischen Small Office Security-Diensten und der Außenwelt.
4369 / 6150	Ports, die zur Sicherstellung der Kommunikation zwischen dem Control Center und dem Kommunikations-Server verwendet werden.
27017	Port, der standardmäßig vom Kommunikationsserver und Control Center zum Zugriff auf die Datenbank benutzt wird
5228, 5229, 5230	Ports für Google Cloud Messaging (GCM). Der Kommunikationsserver benutzt GCM, um Push-Benachrichtigungen an verwaltete Android-Geräte zu senden.
2195, 2196, 5223	Ports für den Dienst Apple Push Notification (APNs). Die Ports 2195 und 2196 werden vom Kommunikationsserver dazu benutzt, mit den APNs-Servern zu kommunizieren. Port 5223 wird unter bestimmten Umständen von verwalteten iOS-Geräten benutzt, um per WLAN mit den APNs-Servern zu kommunizieren. Weitere Informationen finden Sie in diesem Artikel der Wissensdatenbank.
123 (UDP)	Port für User Datagram Protocol (UDP), den Small Office Security-Appliances zur Zeitsynchronisation mit dem NTP-Server verwenden.

3. Small Office Security: Installation und Einrichtung

Führen Sie die folgenden Schritte aus, um die Installation möglichst reibungslos zu gestalten:

1. Installation vorbereiten.
2. Installieren Sie die Small Office Security-Virtual-Appliance, und richten Sie sie ein.
3. Verbindung zum Control Center herstellen und erstes Benutzerkonto einrichten.
4. Geben Sie Ihren Lizenzschlüssel ein.
5. Control Center-Einstellungen konfig.
6. Fügen Sie Control Center-Benutzer hinzu.

3.1. Installation vorbereiten

Zur Installation benötigen Sie ein Image der Small Office Security-Virtual-Appliance.Nachdem Sie die Small Office Security-Appliance installiert und eingerichtet haben, können Sie die nötigen Installationspakete für alle anderen Komponenten der Sicherheitsdienste aus der Ferne über die Oberfläche des Control Center installieren oder herunterladen.

Das Image der Small Office Security-Appliance steht in verschiedenen Formaten zur Verfügung, die mit den gängigsten Virtualisierungsplattformen kompatibel sind.Die Links zum Herunterladen erhalten Sie, wenn Sie sich auf der Bitdefender-Enterprise-Website für eine Testversion registrieren.

Für die Installation und Ersteinrichtungen sollten Sie die folgenden Dinge zur Hand haben:

- DNS-Namen oder festgelegte IP-Adressen (entweder durch statische Konfiguration oder über DHCP-Reservierung) für die Small Office Security-Appliance
- Benutzername und Passwort eines Domain-Administrators
- Lizenzschlüssel (siehe E-Mail zur Testversions-Registrierung oder zum Kauf)
- Server-Einstellungen für ausgehende E-Mails
- wenn nötig, Proxy-Server-Einstellungen
- Sicherheitszertifikate

Zur Installation der Dienste müssen zusätzliche Voraussetzungen erfüllt sein.

3.2. Installation und Einrichtung der Small Office Security-Appliance

Die Small Office Security-Appliance wird mit den folgenden vorkonfigurierten Rollen ausgeliefert:

- **Datenbank-Server**
- **Update Server**
- **Web-Konsole**
- **Kommunikations-Server**

Gehen Sie zur Installation und Einrichtung der Small Office Security-Appliance folgendermaßen vor:

1. Importieren Sie das Image der Small Office Security-Appliance in Ihre virtualisierte Umgebung.
2. Schalten Sie die Appliance an.
3. Greifen Sie von ihrem Virtualisierungsverwaltungsprogramm auf die Konsolenoberfläche der Small Office Security-Appliance zu.
4. Legen Sie ein Passwort für den eingebauten Systemadministrator `bdadmin` fest.
5. Drücken Sie die Enter-Taste, um die Konfigurationsoberfläche zu öffnen.
6. Richten Sie die Appliance über die Konfigurationsoberfläche wie folgt ein:
   a. Weisen Sie der Appliance einen DNS-Namen zu.
   b. Konfigurieren Sie die Netzwerkeinstellungen.
   c. Konfigurieren Sie, wenn nötig, die Proxy-Einstellungen.

   Die Small Office Security-Appliance hat eine schlichte Konfigurationsoberfläche.Mithilfe der Pfeiltasten und der `Tabulator`-Taste können Sie durch die Menüs und Optionen navigieren. Drücken Sie die `Enter`-Taste, um eine bestimmte Option auszuwählen.

3.2.1. Appliance-Hostname (DNS) konfigurieren

Die Kommunikation mit den Small Office Security-Rollen funktioniert über die IP-Adresse oder den DNS-Namen derjenigen Appliance, auf denen die jeweilige Rolle installiert ist.Standardmäßig kommunizieren die Small Office Security-Komponenten über IP-Adressen.Wenn Sie die Kommunikation über DNS-Namen ermöglichen möchten, müssen Sie den Small Office Security-Appliances DNS-Namen zuweisen und sicherstellen, dass diese Namen korrekt zu den konfigurierten IP-Adressen der Appliances aufgelöst werden.

So weisen Sie der Appliance einen DNS-Namen zu:

1. Wählen Sie aus dem Hauptmenü **Appliance-Hostname (DNS) konfigurieren**.
2. Wählen Sie **Appliance-Hostname (DNS) konfigurieren**.

3. Geben Sie den DNS-Namen ein.
4. Wählen Sie **OK**, um die Änderungen zu speichern.
5. Wählen Sie **Appliance-Hostname (DNS) anzeigen**, um sich zu vergewissern, dass der DNS-Name stimmt.

3.2.2. Netzwerkeinstellungen konfigurieren

Sie können die Appliance so einrichten, dass sie die Netzwerkeinstellungen automatisch vom DHCP-Server bezieht, oder Sie können sie manuell konfigurieren.Wenn Sie die DHCP-Methode wählen, müssen Sie den DHCP-Server so konfigurieren, dass er eine bestimmte IP-Adresse für die Appliance reserviert.

So konfigurieren Sie die Netzwerkeinstellungen:

1. Wählen Sie aus dem Hauptmenü **Netzwerkeinstellungen konfigurieren**.
2. Wählen Sie den Netzwerkadapter aus.
3. Wählen Sie die Konfigurationsmethode:
   - **Netzwerkeinstellungen manuell konfigurieren.** Sie müssen die IP-Adresse, die Netzwerkmaske, die Gateway-Adresse und die DNS-Server-Adressen angeben.
   - **Netzwerkeinstellungen automatisch über DHCP beziehen.** Wählen Sie diese Option nur, wenn Sie den DHCP-Server so konfiguriert haben, dass er eine bestimmte IP-Adresse für die Appliance reserviert.
4. Über die entsprechenden Optionen können Sie die aktuellen Details zur IP-Konfiguration bzw. den Link-Status überprüfen.

3.2.3. Proxy-Einstellgn. konf.

Wenn die Appliance über einen Proxy-Server mit dem Internet verbunden ist, müssen Sie die Proxy-Einstellungen konfigurieren.

So konfigurieren Sie die Proxy-Einstellungen:

1. Wählen Sie aus dem Hauptmenü **Proxy-Einstellungen konfigurieren**.
2. Wählen Sie **Proxy-Einstellungen konfigurieren**.
3. Geben Sie die Adresse des Proxy-Servers ein.
4. Wählen Sie **OK**, um die Änderungen zu speichern.

3.3. Control Center: Ersteinrichtung

Nach der Installation und Einrichtung der Small Office Security-Appliance müssen Sie die Web-Oberfläche des Control Center öffnen und Ihr Unternehmens-Administrator-Konto konfigurieren.

Beachten Sie
Weitere Informationen zu Control Center-Benutzern finden Sie unter „Benutzertypen in Control Center“ (S. 39).

1. Geben Sie in die Adressleiste ihres Browsers IP-Adresse oder den DNS-Hostnamen der Control Center-Appliance ein (mit dem Präfix `https://`). Ein Konfigurationsassistent wird geöffnet.
2. Zunächst müssen Sie Ihre Small Office Security-Installation bei einem Bitdefender-Konto registrieren.Geben Sie den Benutzernamen und das Passwort Ihres Bitdefender-Kontos ein.Wenn Sie noch kein Bitdefender-Konto haben, klicken Sie auf den entsprechenden Link, um eines zu erstellen.

   Klicken Sie auf **Weiter**.
3. Geben Sie den Lizenzschlüssel ein, der zur Validierung Small Office Security nötig ist. Sie finden Ihre Lizenzschlüssel in der E-Mail zur Testversions-Registrierung oder zum Kauf. Geben Sie den Lizenzschlüssel in das Feld **Schlüssel** ein, und klicken Sie auf die Schaltfläche + **Hinzufügen**. Warten Sie, bis der Lizenzschlüssel bestätigt wurde. In den entsprechenden Spalte sehen Sie auch das Ablaufdatum für Ihren Lizenzschlüssel.

   Klicken Sie auf **Weiter**.
4. Geben Sie die geforderten Informationen zu ihrem Unternehmens-Administrator-Konto an: Benutzername, E-Mail-Adresse und Passwort. Das Passwort muss mindestens einen Großbuchstaben, einen Kleinbuchstaben und eine Ziffer oder ein Sonderzeichen enthalten.
5. Klicken Sie **Konto erstellen**.

Das Unternehmens-Administrator-Konto wird erstellt, und Sie werden automatisch mit dem neuen Konto am Bitdefender Control Center angemeldet.

3.4. Lizenzschlüssel eingeben

Small Office Security wird mit einem einzigen Schlüssel für alle Sicherheitsdienste lizenziert.

Control Center wird kostenlos mit jedem Small Office Security-Sicherheitsdienst mitgeliefert.

Sie finden Ihre Lizenzschlüssel in der E-Mail zur Testversions-Registrierung oder zum Kauf.

So zeigen Sie bestehende Lizenzinformationen an und geben Ihre Lizenzschlüssel ein:

1. Stellen Sie eine Verbindung zum Control Center her und melden Sie sich mit einem Konto mit dem „Unternehmen verwalten“-Recht an.
2. Gehen Sie zur Seite **Konfiguration > Lizenz**
3. Jetzt können Sie die bestehenden Lizenzschlüssel, Status, Ablaufdaten und Benutzeranzahl der Lizenz sehen.

Wenn Sie den Lizenzschlüssel ändern möchten, geben Sie ihn in das Feld **Schlüssel** ein und klicken Sie auf die Schaltfläche **Hinzufügen**. Der eingegebene Lizenzschlüssel wird der Liste hinzugefügt, und gleichzeitig wird der bestehende Schlüssel ungültig.

3.5. Control Center-Einstellungen konfig.

So konfigurieren Sie die nötigen Control Center-Einstellungen:

1. Stellen Sie eine Verbindung zum Control Center her, und melden Sie sich mit einem Unternehmensadministrator-Konto an.
2. Gehen Sie zum Seite **Konfiguration**.
   - Wechseln Sie zum Reiter **Mail-Server**.

     Wenn Sie einrichten möchten, dass Control Center E-Mails versenden kann, markieren Sie das Kästchen **Mail-Server-Einstellungen**, und konfigurieren Sie die nötigen Einstellungen:

     – **Mail-Server (SMTP).** Geben Sie die IP-Adresse oder den Host-Namen des E-Mail-Servers ein, der die E-Mails versenden wird.

     – **Schnittstelle.** Geben Sie den Port ein, über den die Verbindung zum Mail Server hergestellt werden soll.

     – **Verschlüsselungstyp.** Wenn der Mail-Server eine verschlüsselte Verbindung erfordert, wählen Sie den passenden Typ aus dem Menü (SSL/TLS oder STRARTTLS).

     – **Absender-E-Mail-Adresse.** Geben Sie die E-Mail-Adresse ein, die im Absender-Feld der E-Mail (E-Mail-Adresse des Absenders) erscheinen soll.

     – **Authentifizierung verwenden.** Markieren Sie dieses Kästchen, wenn der Mail-Server eine Authentifizierung fordert.Sie müssen einen gültigen Benutzernamen/E-Mail-Adresse und ein gültiges Passwort angeben.

     Klicken Sie auf **Speichern**, um die Änderungen zu speichern.

   - Wechseln Sie zum Reiter **Proxy**.

     Wenn Ihr Computer über einen Proxy-Server mit dem Internet verbunden ist, wählen Sie **Proxy-Einstellungen verwenden** und konfigurieren Sie die erforderlichen Einstellungen:

     – **Adresse** - 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.

Klicken Sie auf **Speichern**, um die Änderungen zu speichern.

- Wählen Sie den Reiter **Verschiedenes**, um die folgenden Grundeinstellungen zu konfigurieren:
  - **Gleichzeitige Installationen.** Über Installationsaufgaben können Administratoren aus der Ferne Sicherheitskomponenten installieren.Wählen Sie diese Option, um die Höchstzahl der Installationen festzulegen, die gleichzeitig vorgenommen werden können.

    Wenn die Höchstzahl der gleichzeitigen Installationen zum Beispiel auf 10 gesetzt wurde und eine Ferninstallationsaufgabe 100 Computern zugewiesen wird, sendet Control Center zunächst 10 Installationspakete durch das Netzwerk.In diesem Fall wird die Installation gleichzeitig auf höchstens 10 Computern durchgeführt, während alle anderen Teilaufgaben zunächst den Zustand ausstehend erhalten.Sobald eine Teilaufgabe abgeschlossen ist, wird das nächste Installationspaket gesendet, usw.
  - **NTP-Server-Einstellungen**. Der NTP-Server dient zur Synchronisation der Zeit zwischen allen Small Office Security-Appliances. Eine Standardadresse ist voreingestellt. Im Feld **NTP-Server-Adresse** können Sie sie ändern.

    Beachten Sie
    Damit die Small Office Security-Appliances mit dem NTP-Server kommunizieren können, muss Port 123 (UDP) offen sein.

  Klicken Sie auf **Speichern**, um die Änderungen zu speichern.
- Wählen Sie im Reiter **Active Directory** den Punkt **Mit Active Directory synchronisieren** um Control Center mit einer Active-Directory-Domain zu integrieren und zu synchronisieren.Sie müssen Folgendes angeben:
  - Synchronisationsintervall (in Stunden)
  - Active-Directory-Domain-Name (inkl. Domain-Endung)
  - Benutzername und Passwort eines Domain-Administrators

  Klicken Sie auf **Speichern**, um die Änderungen zu speichern.

  Warten Sie einige Sekunden, bis sich das Control Center mit Active Directory aus der angegebenen Domain synchronisiert hat. Nach Abschluss des Vorgangs können Sie im Feld **Synchronisationsstatus** weitere Details einsehen.
- Wählen Sie den Reiter **Zertifikate**.

  Besorgen Sie alle nötigen Sicherheitszertifikate und laden Sie sie hoch. Außer dem Control Center-Zertifikate werden alle anderen Sicherheitszertifikate ausschließlich für die Verwaltung von iOS-Mobilgeräten benötigt.
  - **Control Center-Sicherheit.** Sicherheitswarnungen Ihres Browsers können Sie verhindern, indem Sie ein SSL-Zertifikat hinzufügen, das entweder von Ihrem Unternehmen oder von einer externen Zertifizierungsstelle (CA) unterzeichnet ist.

- **Kommunikations-Server.** Das Kommunikationsserver-Zertifikat wird zur Sicherung der Kommunikation zwischen dem Kommunikationsserver und iOS-Mobilgeräten eingesetzt.Dieses SSL-Zertifikat kann entweder von Ihrem Unternehmen oder einer externen Zertifizierungsstelle unterzeichnet sein.Der Common Name des Zertifikats muss extrakt mit dem Domain-Namen oder der IP-Adresse übereinstimmen, die von mobilen Clients verwendet wird, um eine Verbindung zum Kommunikationsserver herzustellen.Er ist als externe MDM-Adresse in der Konfigurationsoberfläche der Small Office Security-Appliance-Konsole konfiguriert.
- **Apple Push (MDM).** Apple benötigt das Apple-MDM-Push-Zertifikat, um beim Versand von Push-Benachrichtigungen die Sicherheit der Kommunikation zwischen dem Kommunikationsserver und den Servern des Diensts "Apple Push Notifications" (APNs) sicherzustellen.Sie können Ihr Apple-MDM-Push-Zertifikat ganz leicht erhalten und importieren, indem Sie den Anweisungen auf der Seite **Apple-MDM-Push-Zertifikat hinzufügen** folgen.
- **iOS-MDM-Identitäts- und Profilunterzeichnung.** Das iOS-MDM-Identitäts- und -Profil-Signatur-Zertifikat wird vom Kommunikationsserver dazu benutzt, Identitätszertifikate und Konfigurationsprofile, die an mobile Geräte gesendet werden, zu unterzeichnen.Es muss ein Zwischen- oder Endentitätszertifikat sein, das entweder von Ihrem Unternehmen oder einer externen Zertifizierungsstelle unterzeichnet ist.
- **iOS-MDM-Vertrauenskette.** Die iOS-MDM-Vertrauenskette muss alle Zwischenzertifikate bis hin zum Root-Zertifikat Ihres Unternehmens oder bis zum von der externen Zertifizierungsstelle unterzeichneten Zwischenzertifikat enthalten.

3. Öffnen Sie das Menü **Konfiguration** und wählen Sie den Punkt **Update**.
   - Laden Sie im Reiter **Produkt-Update** alle nötigen Installationspakete herunter, oder aktualisieren Sie sie.
   - Im Reiter **Update-Server** können Sie die Bitdefender-Update-Einstellungen konfigurieren.Die Update-Einstellungen gelten für alle Small Office Security-Produkte und -Komponenten sowie für Produkt- und Signatur-Updates.
   - Wechseln Sie zum Reiter **Infrastruktur**, um einen kurzen Überblick über die installierten Small Office Security-Appliances und die auf ihnen laufenden Rollen zu erhalten.

3.6. Control Center-Benutzer hinzufügen

Sie können das erste Small Office Security-Benutzerkonto während der Ersteinrichtung des Control Center nach der Installation der Small Office Security-Appliance erstellen. Das erste Benutzerkonto für Control Center hat die Unternehmensadministrator-Rolle mit vollen Rechten über die Konfiguration des Control Center und die Netzwerkverwaltung. Von diesem Konto aus können Sie alle anderen Benutzerkonten erstellen, die Sie für die Verwaltung Ihres Unternehmensnetzwerks benötigen.

Benutzerkonten werden auf der Seite **Konten** im Control Center verwaltet.

Beachten Sie
Alle Benutzer mit dem „Benutzer verwalten"-Recht können auf die Seite **Konten** zugreifen.

So fügen Sie einen Control Center-Benutzer hinzu:

1. Stellen Sie eine Verbindung zum Control Center her, und melden Sie sich mit dem Unternehmensadministrator-Konto an.
2. Rufen Sie die Seite **Konten** auf.
3. Klicken Sie auf die Schaltfläche + **Hinzufügen** auf der rechten Seite der Tabelle.Eine Konfigurationsseite wird geöffnet.
4. Geben Sie im Bereich **Details** die Benutzerdetails an.Sie können entweder einen Benutzer aus Active Directory hinzufügen (vorausgesetzt, dass eine Active-Directory-Integration konfiguriert wurde) oder einen benutzerdefinierten Benutzer anlegen.
   - Um einen Benutzer aus Active Directory hinzuzufügen, klicken Sie auf **Import aus Active Directory**. Im Feld **Benutzername** können Sie dann das Benutzerkonto festlegen.

     Wenn Sie einen Benutzer aus Active Directory hinzufügen, werden die Benutzerinformationen aus Active Directoy importiert. Der Benutzer meldet sich an der Control Center mit dem Benutzerpasswort von Active Directory an.

     Beachten Sie
     Standardmäßig wird die Control Center in festgelegten Intervallen automatisch mit Active Directory synchronisiert. Um sicherzustellen, dass die neuesten Änderungen in Active Directory auch in die Control Center importiert werden, klicken Sie auf die Schaltfläche **Synchronisieren**.

   - Um einen benutzerdefinierten Benutzer anzulegen, deaktivieren Sie die Option **Import aus Active Directory** und geben Sie den Benutzernamen, die E-Mail-Adresse, den vollen Namen und das Passwort des Benutzers an.

     Beachten Sie
     – Das Passwort muss mindestens einen Großbuchstaben, einen Kleinbuchstaben und eine Ziffer oder ein Sonderzeichen enthalten.
     – Die E-Mail-Adresse darf nur einmal vergeben werden. Sie können keine weiteren Benutzerkonten mit der gleichen E-Mail-Adresse anlegen.

5. Konfigurieren Sie im Bereich **Einstellungen und Rechte** Folgendes:
   - **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 eine Rolle aus, die die Rechte des Benutzers festlegt:

  Unternehmensadministrator

  Unternehmensadministrator-Konten gewähren vollen Zugriff auf die Konfiguration des Control Center und alle Verwaltungsfunktionen der Small Office Security-Sicherheitsdienste.

  Administrator

  Administrator-Konten haben das Recht zur Verwaltung der Small Office Security-Sicherheitsdienste, zur Überwachung von Funktionen und Berichterstattung (Sicherheitsdienste installieren, Benutzerkonten erstellen, Berichte erstellen, Dashboard anpassen). Die Administratorrechte können auf bestimmte Bereiche des Netzwerks oder bestimmte Small Office Security-Sicherheitsdienste beschränkt werden. Administratoren können die Konfigurationseinstellungen des Control Center nicht anzeigen oder bearbeiten.

  Berichterstatter

  Berichterstatterkonten bieten nur Zugriff auf Überwachungs- und Berichterstattungsfunktionen. Die Berichterstatterrechte können auf bestimmte Bereiche des Netzwerks oder bestimmte Small Office Security-Sicherheitsdienste beschränkt werden.Berichterstatter können die Netzwerk- und Sicherheitskonfiguration nicht einsehen oder verändern.

  Benutzerdef.

  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.

- **Rechte.** Sie können Small Office Security-Benutzerkonten die folgenden Benutzerrechte zuweisen:
  - **Lösung verwalten**. Ermöglicht Ihnen die Konfiguration von Control Center-Einstellungen (Mail-Server- und Proxy-Einstellungen, Sicherheitszertifikate und Small Office Security-Updates). 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.
  - **Benutzer verwalten**. Benutzerkonten erstellen, bearbeiten oder löschen.

- **Eigenes Unternehmen verwalten**. Benutzer können ihren eigenen Small Office Security-Lizenzschlüssel verwalten und die Einstellungen für ihr Unternehmensprofil bearbeiten. Dieses Recht haben nur Unternehmensadministratoren.

- **Ziele wählen**. Scrollen Sie im Konfigurationsbereich nach unten, um den Ziele-Bereich anzuzeigen. Sie können den Zugriff eines Benutzers auf bestimmte Small Office Security-Sicherheitsdienste oder auf bestimmte Bereiche des Netzwerks beschränken. Wählen Sie für jeden verfügbaren Sicherheitsdienst die Netzwerkgruppen, auf die der Benutzer Zugriff haben soll.

  Beachten Sie
  Die Optionen für die Zielauswahl werden nicht für Benutzer mit dem Recht zur Lösungsverwaltung angezeigt. Diese haben standardmäßig Rechte für das gesamte Netzwerk und die Sicherheitsdienste.

  Wichtig
  Vergessen Sie nicht, jedes Mal, wenn Sie Änderungen an Ihrer Netzwerkstruktur vornehmen oder eine neue Integration mit einem anderen vCenter-Server- oder XenServer-System einrichten, die Zugriffsrechte bestehender Benutzer zu überprüfen und gegebenenfalls anzupassen.

6. Klicken Sie auf **Speichern**, um den Benutzer hinzuzufügen. Das neue Konto erscheint in der Liste der Benutzerkonten.

   Control Center sendet dem Benutzer automatisch eine E-Mail mit den Zugangsdaten, sofern die Mail-Server-Einstellungen korrekt konfiguriert wurden.

4. Sicherheitsdienste installieren

Um Ihr Netzwerk mit Bitdefender zu schützen, müssen Sie die Small Office Security-Sicherheitsdienste installieren. Um die Small Office Security-Sicherheitsdienste zu installieren, benötigen Sie einen Control Center-Benutzer mit Administratorrechten für alle Dienste und das gesamte Netzwerk. Sie benötigen zudem Administratorzugriff auf die Netzwerk-Computer.

Die folgende Tabelle zeigt die Arten von Netzwerkobjekten, die durch die einzelnen Dienste geschützt werden:

Dienestleistung	Netzwerkobjekte
Security for Endpoints	Computer (Arbeitsplatzrechner, Laptops und Server), auf denen Microsoft Windows läuft
Security for Mobile Devices	iPhones, iPads und Android-Geräten

4.1. Security for Endpoints installieren

Security for Endpoints eignet sich für Computer und Laptops auf Windows- und Mac-OS-X-Betriebssystemen sowie für Windows-Server. 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.

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).

4.1.1. Vor der Installation

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

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

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

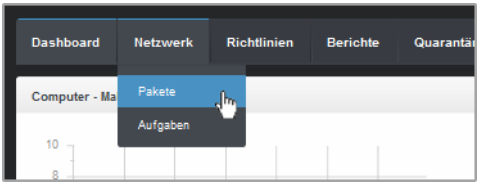
   Wichtig
   Um die Windows-Sicherheitsfunktionen (Windows Defender, Windows Firewall) müssen Sie sich nicht kümmern. Diese werden vor Beginn der Installation automatisch deaktiviert.

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

4.1.2. 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

Nach der Installation des ersten Clients wird dieser dazu verwendet, um andere Computer über den Netzwerkerkennungsmechanismus im gleichen Netzwerk zu erkennen. Weitere Informationen zur Netzwerkerkennung finden Sie unter „Wie die Netzwerkerkennung funktioniert“ (S. 29).

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

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

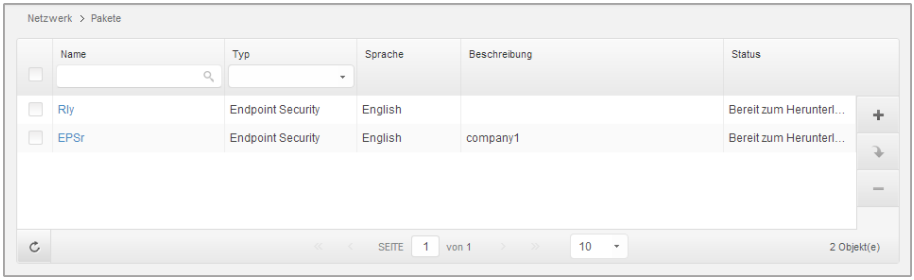
> **Beachten Sie**
> Dieser Schritt muss nicht durchgeführt werden, falls unter Ihrem Benutzerkonto bereits ein Installationspaket für das Netzwerk erstellt worden ist.

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

Endpoint Security Installationspakete erstellen

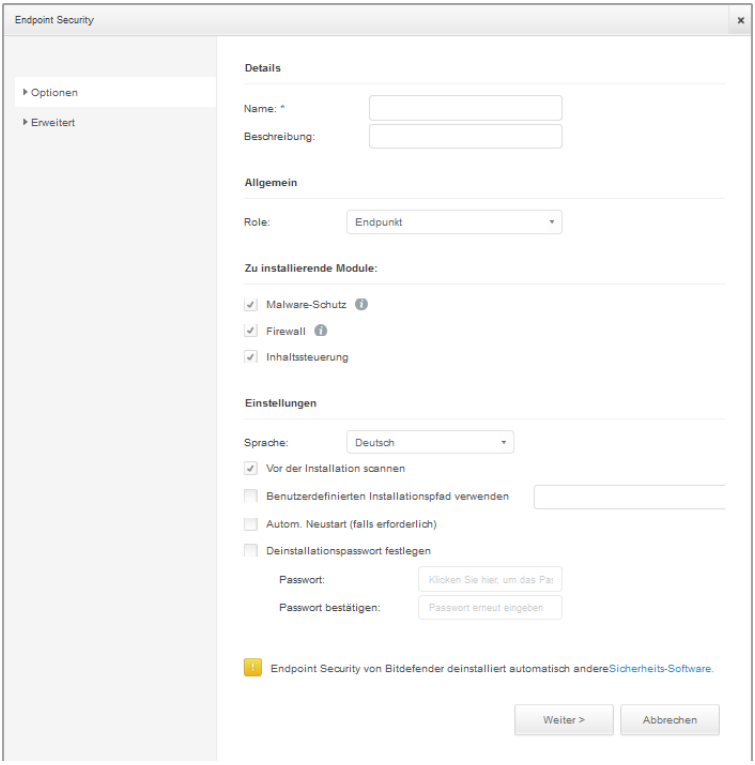
So erstellen Sie ein Installationspaket für Endpoint Security:

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, und wählen Sie **Endpoint Security** aus dem Menü. 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 Small Office Security-Appliance.
6. Wählen Sie die Schutzmodule aus, die Sie installieren möchten.
7. Wählen Sie aus dem Feld **Sprache** die gewünschte Sprache für die Client-Oberfläche.
8. 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.
9. 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.
10. 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.
11. Klicken Sie auf **Weiter**.
12. 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:
    - **Small Office Security-Appliance**, für beide Rollen verfügbar. Wenn nötig, können Sie auch die Adressen des Kommunikationsservers und der lokalen Update-Server in den folgenden Feldern konfigurieren.

      Wenn Sie die lokale Update-Adresse ändern, müssen Sie eine der folgenden Syntaxen verwenden:

      Beachten Sie

      Die hier festgelegte Update-Adresse wird nach der Installation vorübergehend genutzt. Sobald eine Richtlinie auf den Client angewendet wird, wird die Update-Adresse den

Richtlinieneinstellungen entsprechend angepasst. Um sicherzustellen, das der Client sich auch weiterhin über dieselbe Update-Adresse aktualisiert, müssen Sie sie in den Richtlinieneinstellungen entsprechend konfigurieren.

- `update_server_ip:port`
- `update_server_name:port`

- **Endpoint Security Relay** - wenn Sie die Endpunkte mit einem in Ihrem Netzwerk installierten Endpoint Security Relay verbinden möchten. Alle Computer mit der Rolle Endpoint Security Relay, die in Ihrem Netzwerk gefunden wurden, werden in der unten angezeigten Tabelle aufgeführt. Wählen Sie den gewünschten Endpoint Security Relay. Verbundene Endpunkte kommunizieren mit dem Control Center ausschließlich über den angegebenen Endpoint Security Relay.

Wichtig
Port 7074 muss offen sein, damit die Installation über einen Endpoint Security Relay funktioniert.

13. Klicken Sie auf **Speichern**.

Ab jetzt finden Sie das neue Installationspaket in der Liste der Pakete.

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 Installationskit von der Control Center-Appliance herunter und startet dann die 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).
   - **Installationspaket**. Die vollständigen Installationskits sind größer, und sie müssen auf einem Betriebssystem des entsprechenden Typs ausgeführt werden.

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.

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).

4.1.3. Remote-Installation

Mit Control Center können Sie Endpoint Security über Installationsaufgaben aus der Ferne auf Active-Directory-Computern und auf anderen Computern, die im Netzwerk gefunden wurden, installieren.

Nachdem Endpoint Security auf einem Computer installiert wurde, kann es einige Minuten dauern, bis die anderen Netzwerkcomputer in der Control Center angezeigt werden.

Endpoint Security verfügt über einen automatischen Netzwerkerkennungsmechanismus, mit dem Computer gefunden werden können, die nicht im Active Directory sind. Die gefundenen Computer werden als **nicht verwaltete Computer** auf der **Netzwerk**-Seite angezeigt (im Bereich **Computer** unter **Benutzerdefinierte Gruppen**). Control Center entfernt Active-Directory-Computer automatisch von der Liste der gefundenen Computer.

Damit die Netzwerkerkennung funktioniert, müssen Sie Endpoint Security bereits auf mindestens einem Computer im Netzwerk installiert haben. Dieser Computer wird dann eingesetzt, um das Netzwerk zu scannen und Endpoint Security auf den noch nicht geschützten Computern zu installieren.

Weitere Informationen zur Netzwerkerkennung finden Sie unter „Wie die Netzwerkerkennung funktioniert“ (S. 29).

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.

Durchführen von Endpoint Security-Ferninstallationsaufgaben

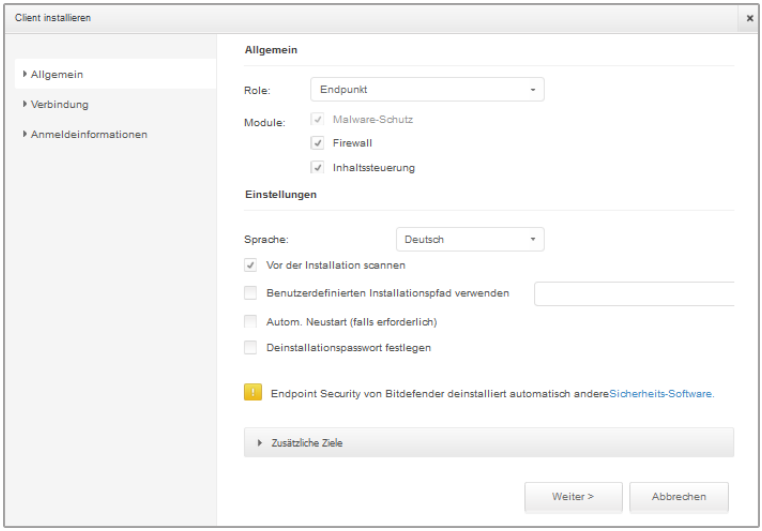
So führen Sie eine Ferninstallationsaufgabe aus:

1. Stellen Sie eine Verbindung zur Control Center her und melden Sie sich an.
2. Gehen Sie zur Seite **Netzwerk**.
3. Wählen Sie **Computer** aus der Dienstauswahl.
4. 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**.

5. Wählen Sie die Entitäten (Computer oder Gruppen von Computern) aus, auf denen Sie den Schutz installieren möchten.
6. 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

7. 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 Small Office Security-Appliance.
   - 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 **Zusätzliche Ziele**, wenn Sie den Client auf bestimmten Maschinen in Ihrem Netzwerk installieren möchten, die nicht im Netzwerkinventar angezeigt werden. Geben Sie die IP-Adressen oder die Hostnamen dieser Maschinen, durch Kommas getrennt, in das entsprechende Feld ein. Sie können so viele IP-Adressen wie nötig hinzufügen.

- Klicken Sie auf **Weiter**.

- Wählen Sie im Reiter **Verbindung** die Entität, über die die Clients kommunizieren sollen:

  – **Small Office Security-Appliance**. Wenn nötig, können Sie auch die Adressen des Kommunikationsservers und der lokalen Update-Server in den folgenden Feldern konfigurieren.

  Wenn Sie die lokale Update-Adresse ändern, müssen Sie eine der folgenden Syntaxen verwenden:
  - `update_server_ip:port`
  - `update_server_name:port`

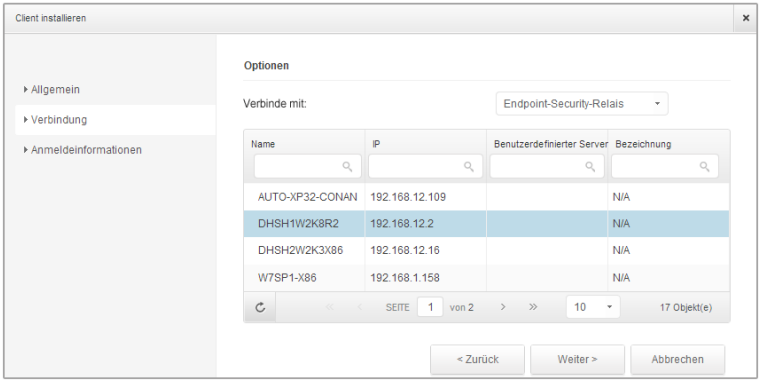
  

  Beachten Sie
  Die hier festgelegte Update-Adresse wird nach der Installation vorübergehend genutzt. Sobald eine Richtlinie auf den Client angewendet wird, wird die Update-Adresse den Richtlinieneinstellungen entsprechend angepasst. Um sicherzustellen, das der Client sich auch weiterhin über dieselbe Update-Adresse aktualisiert, müssen Sie sie in den Richtlinieneinstellungen entsprechend konfigurieren.

  – **Endpoint Security Relay** - wenn Sie die Endpunkte mit einem in Ihrem Netzwerk installierten Endpoint Security Relay verbinden möchten. Alle Computer mit der Rolle Endpoint Security Relay, die in Ihrem Netzwerk gefunden wurden, werden in der unten angezeigten Tabelle aufgeführt. Wählen Sie den gewünschten Endpoint

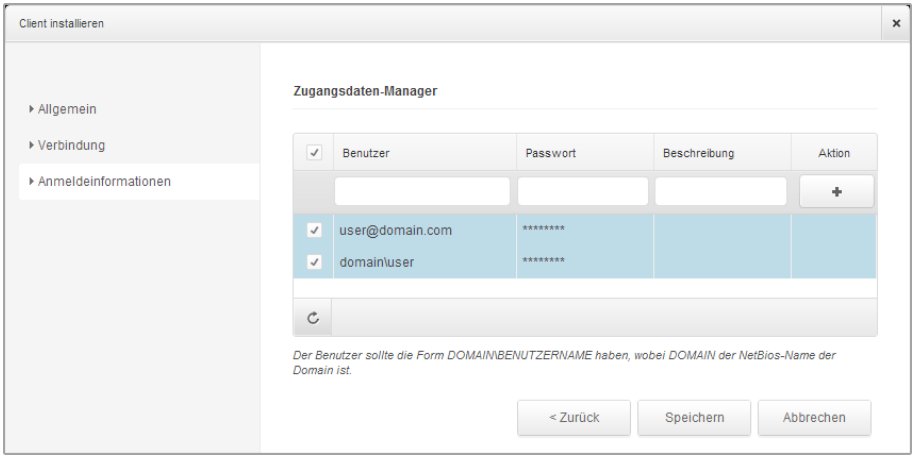
Security Relay. Verbundene Endpunkte kommunizieren mit dem Control Center ausschließlich über den angegebenen Endpoint Security Relay.

Wichtig
Port 7074 muss offen sein, damit die Installation über einen Endpoint Security Relay funktioniert.



8. Klicken Sie auf **Weiter**.
9. Geben Sie im Bereich **Zugangsdaten-Manager** die Administratorzugangsdaten an, die für die Fernauthentifizierung auf den ausgewählten Endpunkten benötigt werden. 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 Domain-Benutzerkontos eingeben, z. B. `user@domain.com` oder `domain\user`). Um sicherzugehen, dass die eingegebenen Zugangsdaten funktionieren, geben Sie sie in beiden Ausdrucksweisen ein (`user@domain.com` und `domain\user`).

   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.

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

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

4.1.4. Wie die Netzwerkerkennung funktioniert

Neben der Integration mit Active Directory verfügt Security for Endpoints über automatische Netzwerkerkennungsmechanismen 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.

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.

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.

4.2. Security for Mobile Devices installieren

Security for Mobile Devices ist eine Lösung zur Verwaltung mobiler Geräte für iPhones, iPads und Android-Geräte. Eine vollständige Liste der unterstützten Betriebssystemversionen finden Sie unter Systemanforderungen.

Security for Mobile Devices wird im Control Center verwaltet, indem mobile Geräte bestimmten Benutzern hinzugefügt werden und dann die Anwendung GravityZone Mobile Client auf den Geräten installiert wird. Sie können bestehenden Active-Directory-Benutzern mobile Geräte hinzufügen oder benutzerdefinierte Benutzer erstellen, um ihnen die Geräte hinzuzufügen.

Bevor Sie loslegen, sollten Sie eine öffentliche (externe) Adresse für den Kommunikationsserver konfigurieren.

So installieren Sie Security for Mobile Devices:

1. Wenn Sie die Integration mit Active Directory nicht benutzen, müssen Sie Benutzer für Eigentümer mobiler Geräte erstellen.
2. Benutzern Geräte hinzufügen.
3. GravityZone Mobile Client auf Geräten installieren und aktivieren.

4.2.1. Externe Adresse für den Kommunikationsserver konfigurieren

In der Standardeinrichtung von Small Office Security können mobile Geräte nur verwaltet werden, wenn sie direkt mit dem Unternehmensnetzwerk verbunden sind (über WLAN oder VPN). Der Grund dafür ist, dass mobile Geräte bei der Registrierungen so konfiguriert werden, dass sie eine Verbindung zur lokalen Adresse der Kommunikationsserver-Appliance herstellen.

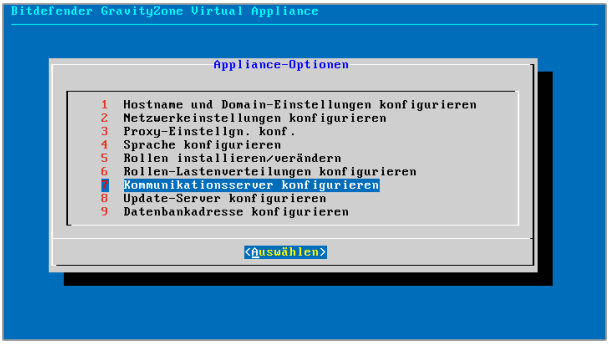
Um mobile Geräte an einem beliebigen Ort über das Internet zu verwalten, müssen Sie eine öffentlich erreichbare Adresse für den Kommunikationsserver konfigurieren.

Zur Verwaltung mobiler Geräte, die nicht mit dem Unternehmensnetzwerk verbunden sind, stehen Ihnen die folgenden Möglichkeiten zur Verfügung:

- Port-Weiterleitung im Unternehmens-Gateway für die Appliance konfigurieren, auf der die Kommunikationsserver-Rolle läuft.
- Einen zusätzlichen Netzwerkadapter zur Appliance, auf der die Kommunikationsserver-Rolle läuft, hinzufügen und ihm eine öffentliche IP-Adresse zuweisen.

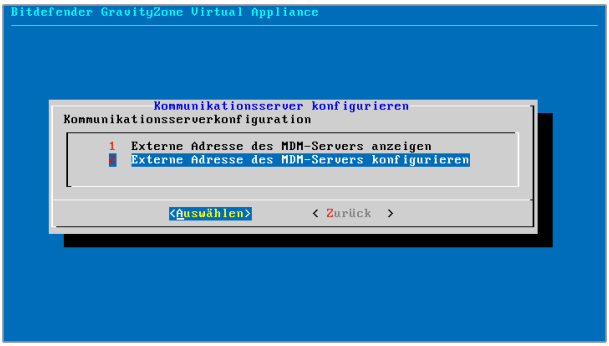
In beiden Fällen müssen Sie für den Kommunikationsserver die externe Adresse konfigurieren, die für die Verwaltung mobiler Geräte benutzt werden soll:

1. Greifen Sie über Ihre Virtualisierungsverwaltungs-Software (z. B. vSphere Client) auf die Appliance-Console zu.
2. Wählen Sie aus dem Hauptmenü **Kommunikationsserver konfigurieren**.



Fenster "Anwendungsoptionen"

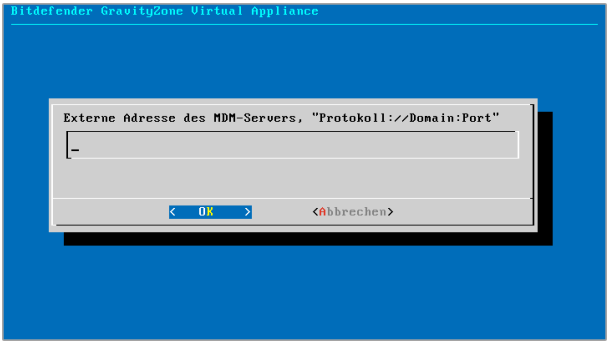
3. Wählen Sie **Externe Adresse des MDM-Servers konfigurieren**



Fenster "Kommunikationsserver konfigurieren"

4. Geben Sie die externe Adresse ein.

   Verwenden Sie die folgende Syntax: `https://<IP/Domain>:<Port>`.



Fenster für die Eingabe der externen Adresse des MDM-Servers

- Wenn Sie Port-Weiterleitung verwenden, müssen Sie erstens die öffentliche IP-Adresse oder den Domain-Namen und zweitens den auf dem Gateway offenen Port eingeben.
- Wenn Sie die öffentliche Adresse des Kommunikationsservers verwenden, müssen Sie erstens die öffentliche IP-Adresse oder oder den Domain-Namen und zweitens den Kommunikationsserver-Port angeben. Der Standard-Port ist `8443`.

5. Wählen Sie **OK**, um die Änderungen zu speichern.

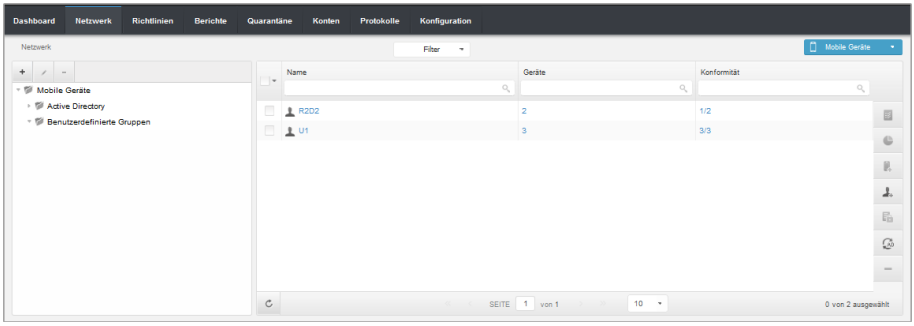
4.2.2. Benutzerdefinierte Benutzer erstellen und organisieren

In Situationen ohne Active Directory müssen Sie zunächst benutzerdefinierte Benutzer erstellen, um eine Möglichkeit zu haben, die Eigentümer mobiler Geräte zu identifizieren.Angegebene Benutzer mobiler Geräte werden in keiner Weise mit dem Active Directory oder mit anderen im Control Center definierten Benutzern verknüpft.

Benutzerdefinierte Benutzer erstellen

So erstellen Sie einen benutzerdefinierten Benutzer:

1. Gehen Sie zur Seite **Netzwerk**.
2. Wählen Sie aus dem Menü in der rechten oberen Ecke der Seite den Punkt **Mobile Geräte**.
3. Wählen Sie im linken Fenster **Benutzerdefinierte Gruppen**.



Netzwerk - Mobilgeräteübersicht - Benutzeransicht

4. Klicken Sie auf das Symbol **Benutzer hinzufügen** in der Symbolleiste. Ein Konfigurationsfenster wird sich öffnen.
5. Geben Sie die Informationen des gewünschten Benutzers an:
   - Einen aussagekräftigen Benutzernamen (z. B. den vollen Namen des Benutzers)
   - Die E-Mail-Adresse des Benutzers

   Wichtig
   Vergewissern Sie sich, dass die E-Mail-Adresse gültig ist. Wenn Sie ein Gerät hinzufügen, erhält der Benutzer eine E-Mail mit den Installationsanweisungen.

6. Klicken Sie auf **OK**.

Benutzerdefinierte Benutzer organisieren

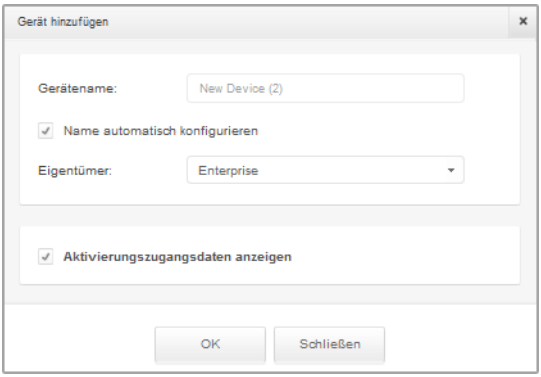
So organisieren Sie benutzerdefinierte Benutzer:

1. Erstellen Sie benutzerdefinierte Gruppen.
   a. Wählen Sie im linken Fenster **Benutzerdefinierte Gruppen**, und klicken Sie auf das Symbol **Gruppe hinzufügen** in der Symbolleiste (über dem Fenster).
   b. Geben Sie einen aussagekräftigen Namen für die Gruppe ein, und klicken Sie auf **OK** Die neue Gruppe wird jetzt unter **Benutzerdefinierte Gruppen** angezeigt.
2. Verschieben Sie benutzerdefinierte Benutzer in entsprechende benutzerdefinierte Gruppen.
   a. Wählen Sie im rechten Fenster die Benutzer.
   b. Verschieben Sie Ihre Auswahl per Drag und Drop in die gewünschte Gruppe im linken Fenster.

4.2.3. Benutzern Geräte hinzufügen

So fügen Sie einem Benutzer ein Gerät hinzu:

1. Gehen Sie zur Seite **Netzwerk**.
2. Wählen Sie aus dem Menü in der rechten oberen Ecke der Seite den Punkt **Mobile Geräte**.
3. Suchen Sie den Benutzer in den Active-Directory-Ordnern oder in benutzerdefinierten Gruppen.
4. Klicken Sie auf das Symbol **Gerät hinzufügen** in der Symbolleiste. Ein Konfigurationsfenster wird sich öffnen.



Ein Mobilgerät für einen Benutzer hinzufügen

5. Geben Sie einen aussagekräftigen Namen für das Gerät ein.
6. Mit der Option **Name automatisch konfigurieren** wird der Gerätename automatisch generiert. Nach Aktivierung dieser Option kann der Gerätename nicht geändert werden. Stattdessen wird ein Standardname automatisch zugewiesen.
7. Wählen Sie den Eigentümertyp des Geräts (geschäftlich/enterprise oder privat).
8. Wählen Sie die Option **Aktivierungszugangsdaten anzeigen** aus, nachdem Sie auf **OK** geklickt haben, wenn Sie den GravityZone Mobile Client auf dem Gerät des Benutzers installieren möchten.
9. Klicken Sie auf **OK**. Es wird sofort eine E-Mail an den Benutzer gesendet, die Installationsanweisungen und Aktivierungsdetails für das Gerät enthält. Die Aktivierungsdetails enthalten das Aktivierungs-Token und die Adresse des Kommunikationsservers (und den entsprechenden QR-Code).

Beachten Sie
Sie können die Aktivierungsdetails eines Geräts jederzeit einsehen, indem Sie im Control Center auf seinen Namen klicken.

Beachten Sie
I können auch einer Auswahl an Benutzern und Gruppen mobile Geräte hinzufügen. In diesem Fall können Sie im Konfigurationsfenster nur die Eigentümer der Geräte definieren. Mobile Geräte, die durch eine Mehrfachauswahl erstellt wurden, erhalten standardmäßig einen generischen Namen. Sobald ein Gerät registriert ist, ändert sich sein Name automatisch; ebenso die Hersteller- und Modell-Einträge.

4.2.4. GravityZone Mobile Client auf Geräten installieren

Die Anwendung GravityZone Mobile Client wird ausschließlich über den Apple App Store und Google Play vertrieben.

So installieren Sie GravityZone Mobile Client auf einem Gerät:

1. Suchen Sie die Anwendungen im offiziellen App-Store.
   - Link zu Google Play
   - Link zum Apple App Store
2. Laden Sie die Anwendung herunter, und installieren Sie sie auf dem Gerät.
3. Starten Sie die Anwendung, und nehmen Sie die nötige Konfiguration vor:
   a. Tippen Sie auf Android-Geräten auf **Aktivieren**, um GravityZone Mobile Client als Geräteadministrator zu aktivieren. Lesen Sie die Informationen gründlich durch.
   b. Geben Sie das Aktivierungs-Token und die Adresse des Kommunikationsservers ein, oder scannen Sie den QR-Code in der E-Mail ein.
   c. Tippen Sie auf **Aktivieren**.
   d. Auf iOS-Geräten werden Sie aufgefordert, das MDM-Profil zu installieren. Wenn ihr Gerät passwortgeschützt ist, werden Sie aufgefordert, das Passwort einzugeben. Folgen Sie den Anweisungen auf Ihrem Bildschirm, um die Profilinstallation abzuschließen.

5. Erste Schritte

Bitdefender Small Office Security-Lösungen 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.

5.1. Benutzertypen in Control Center

Control Center enthält mehrere vordefinierte Benutzerkontenrollen. Jede vordefinierte Rolle gewährt dem Benutzer bestimmte Rechte über das Control Center.

Die Rechte jedes Benutzerkontos können auf bestimmte Small Office Security-Sicherheitsdienste oder auf bestimmte Bereiche des Netzwerks beschränkt werden.

Unternehmensadministrator

Benutzer mit der Unternehmensadministrator-Rolle haben die vollen Rechte über die Einstellungen des Control Center und Netzwerksicherheitseinstellungen, darunter:

- Integration mit Active Directory
- Mail-Server-Einstellungen
- Update-Einstellungen für Small Office Security-Komponenten und Installationspakete
- Verwaltung von Sicherheitszertifikaten
- Verwaltung von Lizenzschlüsseln
- Benutzerverwaltung
- Netzwerksicherheitsverwaltung (Client-Installation, Richtlinien, Aufgaben, Quarantäne)
- Berichtverwaltung

Administrator

Administratorkonten gewähren vollen Zugriff auf alle Verwaltungsfunktionen für Small Office Security-Sicherheitsdienste, auch auf die Benutzerverwaltung. Administratoren können die Einstellungen des Control Center nicht anzeigen oder bearbeiten.

Berichterstatter

Berichterstatter haben nur Zugriff auf Überwachungs- und Berichterstattungsfunktionen. Berichterstatter können die Netzwerk- und Sicherheitskonfiguration nicht einsehen oder verändern.

5.2. 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.

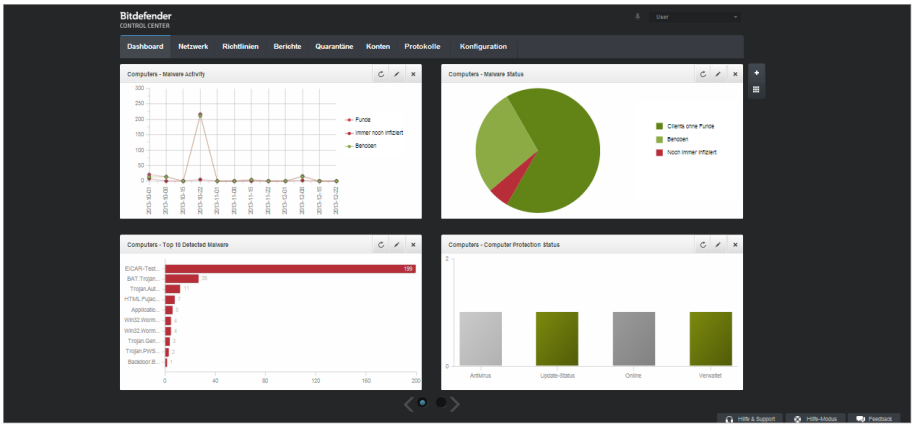
So stellen Sie eine Verbindung zum Control Center her:

1. Geben Sie in die Adressleiste ihres Browsers IP-Adresse oder den DNS-Hostnamen der Control Center-Appliance ein (mit dem Präfix `https://`).
2. Geben Sie Ihren Benutzernamen und Ihr Passwort ein.
3. 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.

5.3. 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

5.3.1. 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.

Konfiguration
Konfigurieren Sie die Control Center-Einstellungen, so zum Beispiel Mail-Server, Proxy-Einstellungen und Sicherheitszertifikate.

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

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.
- **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.

5.3.2. 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.

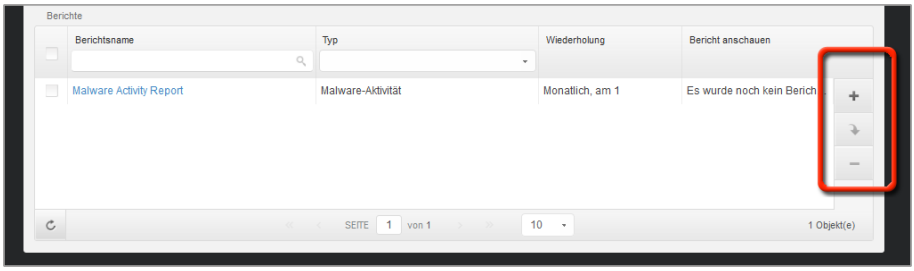
Tabellendaten aktualisieren

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

5.3.3. 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:

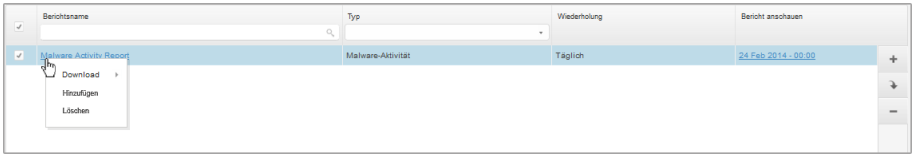
- Neuen Bericht erstellen.
- Geplant erstellte Berichte herunterladen.
- Einen geplanten Bericht löschen.



Die Berichtsübersicht - Symbolleisten

5.3.4. 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

5.3.5. Dienstauswahl

Als Administrator oder Berichterstatter können Sie die Control Center-Dienste einzeln verwalten.Wählen Sie den gewünschten Dienst aus dem **Dienstmenü** in der rechten oberen Ecke der Seite.

Beachten Sie
Das Dienstmenü ist nur auf denjenigen Seiten vorhanden, auf denen es einen Sinn hat, Daten nacht Diensttyp zu filtern.

Das Dienstmenü enthält die folgenden Optionen:

- **Computer** (Security for Endpoints)
- **Mobilgeräte** (Security for Mobile Devices)

Beachten Sie
Es werden Ihnen nur diejenigen Dienste angezeigt, für die Ihnen der Administrator, der Ihren Benutzer zum Control Center hinzugefügt hat, Rechte erteilt hat.

5.4. Sicherheitsrichtlinien anwenden

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 bestimmten Netzwerkinventarobjekten (Computern oder mobilen Geräten) angewendet werden sollen.

Direkt nach der Installation wird den Clients eine Standardrichtlinie zugewiesen, die mit den empfohlenen Schutzeinstellungen vorkonfiguriert ist.Sie können die Sicherheitseinstellungen nach Belieben ändern und/oder zusätzliche Sicherheitsfunktionen konfigurieren, indem Sie benutzerdefinierte Richtlinien erstellen und zuweisen.

5.4.1. Richtlinien erstellen und konfigurieren

Für jeden Small Office Security-Sicherheitsdienst gibt es eine eigene Richtlinienvorlage, in der die Sicherheitseinstellungen für den entsprechenden Typ von Netzwerkobjekten festgelegt sind.Für jeden Typ von Netzwerkobjekten müssen Sie mindestens eine benutzerdefinierte Richtlinie erstellen.

So erstellen und konfigurieren Sie eine neue Richtlinie:

1. Gehen Sie zur **Richtlinien**-Seite.
2. Wählen Sie aus dem Menü in der rechten oberen Ecke der Seite den Typ von Netzwerkobjekt (Computer oder mobile Geräte).
3. Klicken Sie auf die Schaltfläche **Hinzufügen** auf der rechten Seite der Tabelle.
4. Geben Sie einen eindeutigen Namen für die Richtlinie ein.Wenn Sie einen Namen festlegen, berücksichtigen Sie den Zweck und das Ziel der Richtlinie.
5. Konfigurieren Sie dann die Richtlinieneinstellungen.In den meisten Fällen empfiehlt sich die Nutzung der Standardsicherheitseinstellungen.
6. Klicken Sie auf **Speichern**.Die neue Richtlinie wird in der Tabelle **Richtlinien** angezeigt.

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

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.

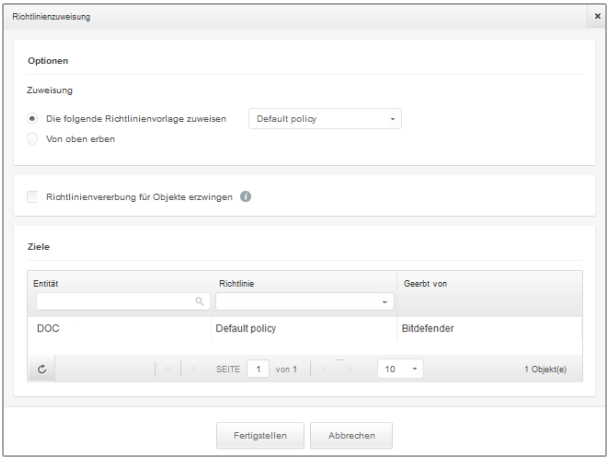
Beachten Sie

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. Wählen Sie eine Art von Netzwerkobjekt aus der Dienstauswahl.
3. Markieren Sie das Kästchen des gewünschten Netzwerkobjekts.Sie können ein oder mehrere Objekte auswählen, diese müssen jedoch von der selben Ebene sein.
4. Klicken Sie auf die Schaltfläche **Richtlinie zuweisen** auf der rechten Seite der Tabelle.

   Das Fenster **Richtlinienzuweisung** wird angezeigt:



Einstellungen für die Richtlinienzuweisung

5. 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.
6. 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.

5.5. Aufgaben verwenden

Control Center bietet eine Reihe administrativer Aufgaben, die Sie aus der Ferne auf Netzwerkobjekten (Computern oder mobilen Geräten) ausführen können. Aufgaben hängen mit den Small Office Security-Sicherheitsdiensten zusammen und unterscheiden sich je nach Typ des Netzwerkobjekts.

Sie können zum Beispiel einen Fern-Scan auf verwalteten Clients ausführen. Die Scan-Aufgabe steht für alle Arten von Netzwerkobjekten zur Verfügung.

So erstellen Sie eine Fern-Scan-Aufgabe und führen sie aus:

1. Gehen Sie zur Seite **Netzwerk**.
2. Wählen Sie aus dem Menü in der rechten oberen Ecke der Seite den Typ von Netzwerkobjekt (Computer oder mobile Geräte).
3. Finden Sie die einzelnen Netzwerkobjekte oder Gruppen, auf denen Sie die Aufgabe ausführen möchten, und wählen Sie sie aus.Sie können nur Objekte aus derselben übergeordneten Gruppe auswählen.
4. Klicken Sie auf die Schaltfläche **Aufgaben** auf der rechten Seite der Tabelle, und wählen Sie **Scan** aus dem Menü.Das Fenster **Scan-Aufgabe** wird angezeigt.
5. Konfigurieren Sie die Einstellungen nach Bedarf.
6. Klicken Sie auf **Speichern**.Die Aufgabe wird sofort auf Clients, die online sind, ausgeführt.Wenn ein Client offline ist, wird die Aufgabe ausgeführt, sobald er wieder online ist.

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

- Der Fortschritt der Aufgabe auf den einzelnen Clients wird angezeigt, wenn Sie auf den Link in der Spalte **Fortschritt** klicken.
- Wenn die Aufgabe abgeschlossen ist, können Sie auf das Symbol in der Spalte **Bericht** klicken, um einen detaillierten Aufgabenbericht anzuzeigen.
- Sie können eine fehlgeschlagene Installation, Deinstallation oder Update-Aufgabe erneut ausführen, ohne sie neu erstellen zu müssen. Wählen Sie sie dazu aus und klicken auf die Schaltfläche **Erneut ausführen** rechts neben der Tabelle.

5.6. Überwachung und Berichterstattung

Das Control Center bietet leistungsstarke Überwachungs- und Berichtfunktion.Das Control Center-Dashboard ist das zentrale Überwachungs-Tool inSmall Office Security.

- Dashboard
- Berichte

5.6.1. Verwendung des Dashboards

Das Dashboard des Control Centers ist eine anpassbare grafische Oberfläche, die einen Überblick über alle geschützten Netzwerkobjekte (Computer oder mobile Geräte) bietet.

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

Was Sie über Dashboard-Portlets wissen sollten:

- Die Control Center hat verschiedene vordefinierte Dashboard-Portlets für jeden Small Office Security-Sicherheitsdienst.
- 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. Die Portlet-Arten entsprechen den verfügbaren Berichtsarten.
- Die von den Portlets angezeigten Informationen beziehen sich ausschließlich auf die Netzwerkobjekte, die zu Ihrem Benutzerkonto gehören.
- Klicken Sie auf die einzelnen Einträge in der Diagrammlegende, um die entsprechende Variable, falls verfügbar, auf dem Graphen anzuzeigen bzw. auszublenden.
- 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.
- Die Portlets werden in Vierergruppen angezeigt. Verwenden Sie den Schieberegler unten auf der Seite, um zwischen den Portlet-Gruppen umzuschalten.

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.

Ein neues Portlet hinzufügen

Sie können weitere Portlets erstellen, um bestimmte Informationen angezeigt zu bekommen. Es können höchstens 36 Portlets gleichzeitig bestehen.

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 Portlet-Konfigurationsfenster wird angezeigt.
3. Im Reiter **Details** können Sie die Details des Portlets konfigurieren:
   - Sicherheitsdienst (**Computer** oder **Mobile Geräte**)
   - Art des Hintergrundberichts
   - Aussagekräftiger Portlet-Name
   - Update-Intervall
4. Wählen Sie im Reiter **Ziele** die Netzwerkobjekte und Gruppen, die Sie einbeziehen möchten.
5. Klicken Sie auf **Speichern**.

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.

Portlets im Dashboard 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**.

5.6.2. Berichte verwenden

Mit Control Center können Sie Berichte über den Sicherheitsstatus der verwalteten Clients 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.

Für jeden Small Office Security-Sicherheitsdienst stehen verschiedene Berichtsarten zur Verfügung, damit Sie einfachen Zugriff auf die von Ihnen benötigten Informationen erhalten.Diese Informationen werden in übersichtlichen Kreisdiagrammen, Tabellen und Grafiken dargestellt, so dass Sie schnell den Sicherheitsstatus des Netzwerkes überprüfen und eventuelle Sicherheitsprobleme erkennen können.

Einen Bericht erstellen

So erstellen Sie einen geplanten Bericht oder zeigen einen Sofortbericht an:

1. Gehen Sie zur Seite **Berichte**.
2. Wählen Sie aus dem Menü in der rechten oberen Ecke der Seite den Typ von Netzwerkobjekt (Computer oder mobile Geräte).
3. Klicken Sie auf die Schaltfläche + **Hinzufügen** auf der rechten Seite der Tabelle.Die Berichtskonfigurationsseite wird angezeigt.
4. Wählen Sie den gewünschten Berichtstyp aus dem Menü aus.
5. 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.
6. Konfigurieren Sie das Berichtsziel.Klicken Sie auf **Ziel ändern** und wählen Sie die Netzwerkobjekte oder Gruppen, die im Bericht vorkommen sollen.
7. Berichtwiederholung konfigurieren (Zeitplan).Sie haben die Wahl, ob Sie den Bericht sofort, täglich, wöchentlich (an einem bestimmten Tag der Woche) oder monatlich (an einem bestimmten Tag des Monats) erstellen möchten.

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

8. Konfigurieren Sie die Berichtsoptionen.
   a. Bei den meisten Berichtsarten müssen Sie für die Erstellung eines Sofortberichts einen Berichtszeitraum 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 Clients anzeigen, die im ausgewählten Zeitraum aktualisiert wurden (bzw. nicht aktualisiert wurden).
c. Um den Bericht als E-Mail zu versenden, wählen Sie die entsprechende Option aus.Sie müssen die E-Mail-Adressen der gewünschten Empfänger angeben.

9. Klicken Sie auf **Generieren/Speichern**, um einen Sofort- bzw. einen geplanten Bericht zu erstellen.
   - Wenn Sie einen Sofortbericht erstellt haben, wird dieser auf einer eigenen Seite angezeigt.Die Zeit, die bis zur Fertigstellung eines Berichts benötigt wird, hängt von der Anzahl der verwalteten Clients ab.Bitte warten Sie, bis der angeforderte Bericht erstellt wurde.Wenn Sie eine Kopie des Berichts speichern möchten, können Sie ihn herunterladen oder per E-Mail versenden.
   - Wenn Sie einen geplanten Bericht erstellt haben, wird dieser auf der Seite **Berichte** angezeigt.Sie können den geplanten Bericht jederzeit bearbeiten oder löschen.

6. Hilfe erhalten

Für weitere Informationen oder Hilfe direkt von Bitdefender:

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

Um ein Support-Ticket zu öffnen, füllen Sie bitte das Forumular aus, das Sie hier finden.