BeyondTrust

Sicherer Remote-Zugriff
Hardware-Installation

TC:15.07.2022

Table of Contents

BeyondTrust-Gerät B-Serie Aufgabenliste zur Einrichtung

Diese Aufgabenliste ist eine Kurzreferenz für die notwendigen Schritte zur Einrichtung Ihres B-Serien-Gerät. Die vollständigen Einzelheiten finden Sie weiter hinten in diesem Handbuch. Verwenden Sie diese Liste als Checkliste für die wichtigsten Schritte.

1. Konfigurieren Sie einen DNS-A-Eintrag für den vollständig qualifizierten Domain-Namen (FQDN) Ihrer neuen Site (z. B. appliance.example.com).
    - Wenn sich Ihr B-Serien-Gerät in Ihrer DMZ oder in Ihrem internen Netzwerk befinden wird, wird ein interner A-Eintrag benötigt, der auf die interne IP-Adresse des B-Serien-Geräts verweist.
    - Wenn Sie externe Kunden unterstützen möchten, muss ebenfalls ein öffentlicher DNS A-Eintrag für die externe IP-Adresse des B-Serien-Geräts registriert werden.
    - Detaillierte Informationen zu BeyondTrust-Netzwerkbereitstellungsszenarien finden Sie in Das BeyondTrust-Gerät B-Serie im Netzwerk auf www.beyondtrust.com/docs/deployment/dmz.
2. Installieren Sie das B-Serien-Gerät entsprechend „BeyondTrust-Gerät B-Serie-Voraussetzungen“ auf Seite 4.
3. Beziehen Sie ein SSL-Zertifikat, das Ihrer FQDN-DNS entspricht (z. B. appliance.example.com).
    a. Vollständige Einzelheiten finden Sie im SSL-Zertifikathandbuch unter www.beyondtrust.com/docs/remote-support/how-to/sslcertificates.
    b. Importieren Sie die Zertifikatkette in Ihr B-Serien-Gerät und ordnen Sie dieser die IP-Adresse des B-Serien-Gerät zu.
    c. Exportieren Sie den Root-Teil der Zertifikatkette (mit entsprechenden **Ausgestellt für** und **Ausgestellt von**-Werten) ohne private Schlüsselinformationen und speichern Sie das Root-Zertifikat für den nächsten Schritt.
4. Senden Sie dem BeyondTrust Technical Support die folgenden drei Dinge per E-Mail:
    - Den FQDN DNS-Hostnamen des B-Serien-Gerät aus Schritt 1.
    - Das Root-SSL-Zertifikatsegment, das Sie in Schritt 3c exportiert haben.
    - Eine Bildschirmaufnahme der Registerkarte **/appliance > Status > Einfach**.
5. Installieren Sie das neue Software-Lizenzpaket, das Ihnen das BeyondTrust Technical Support nach Abschluss der Schritte 1-4 senden wird.
    a. Sie werden per E-Mail benachrichtigt, wenn Sie das Softwarelizenzpaket mithilfe des Utilitys **Auf Aktualisierungen prüfen** installieren sollten.
    b. Navigieren Sie nach der Installation zur /login-Verwaltungsschnittstelle (z. B. https://appliance.example.com/login).
    c. Verwenden Sie die standardmäßigen Administrator-Anmeldedaten **admin** und **password** zur erstmaligen Anmeldung.

BeyondTrust-Gerät B-Serie-Voraussetzungen

Dieser Leitfaden führt Sie durch die Ersteinrichtung und Konfiguration Ihres virtuellen BeyondTrust-Gerät B-Serie. Sollten Sie Hilfe benötigen, wenden Sie sich bitte an www.beyondtrust.com/support.

Voraussetzungen

Beachten Sie vor dem Beginnen: Sie können das B-Serien-Gerät über die IP-Adresse oder den Hostnamen direkt erst dann erreichen, auf Aktualisierungen prüfen oder den berechtigten Zugriff bereitstellen, wenn Sie die Voraussetzungen des B-Serien-Geräts erfüllt haben. Das B-Serien-Gerät erfordert mindestens Folgendes:

- Zwei verfügbare Steckdosen
- Eine Hochgeschwindigkeits-Netzwerkverbindung
- Einen Netzwerkrouter oder -switch
- Eine eindeutige, statische IP-Adresse für das B-Serien-Gerät
- Einen privaten DNS A-Eintrag, der zur statischen IP Ihres B-Serien-Gerät hin auflöst. Ein öffentlicher A-Eintrag und eine öffentliche IP sind ebenfalls erforderlich, wenn externe Clients auf das B-Serien-Gerät zugreifen müssen.
- Ein SSL-Webserver-Zertifikat + intermediäre SSL-Zertifikat(e) und ein SSL-Root. ODER: 1 selbstsigniertes Zertifikat.

> *Weitere Informationen siehe SSL-Zertifikate und BeyondTrust-Handbuch.*

- Das BeyondTrust-Softwarelizenzpaket

Dies sind die Mindestvoraussetzungen, erweiterte Konfigurationen erfordern unter Umständen zusätzliche Komponenten. Beispiel:

- Mobile BeyondTrust-Clients erfordern ein SSL-Root und intermediäre SSL-Zertifikate.
- Der Zugriff von externen öffentlichen Netzwerken aus erfordert einen öffentlichen DNS A-Eintrag.
- Der Zugriff von mehreren DNS A-Einträgen erfordert entweder mehrere Webserver-Zertifikate und/oder SAN- oder Wildcard-Zertifikate.
- Die Isolierung von Client-Datenverkehr von mehreren Netzwerken erfordert mehrere statische IP-Adressen.
- Die automatische Aktualisierung und erweiterter technischer BeyondTrust-Support erfordern ausgehenden Zugriff auf das öffentliche Internet vom B-Serien-Gerät über TCP-Port 443.

WICHTIG!

Keine Client-Software (z. B. Konsolen, Jump-Clients, Jumpoints usw.) kann heruntergeladen, installiert oder verwendet werden, bis der BeyondTrust Technical Support ein Softwarelizenzpaket für Ihr B-Serien-Gerät kompiliert hat und Sie dieses entsprechend der Support-Anweisungen installiert haben. Da dieses Lizenzpaket mit dem DNS A-Eintrag des B-Serien-Geräts sowie mit seinem SSL-Zertifikat enkodiert wird, müssen diese Komponenten eingerichtet sein, bevor das Lizenzpaket bereitgestellt werden kann.

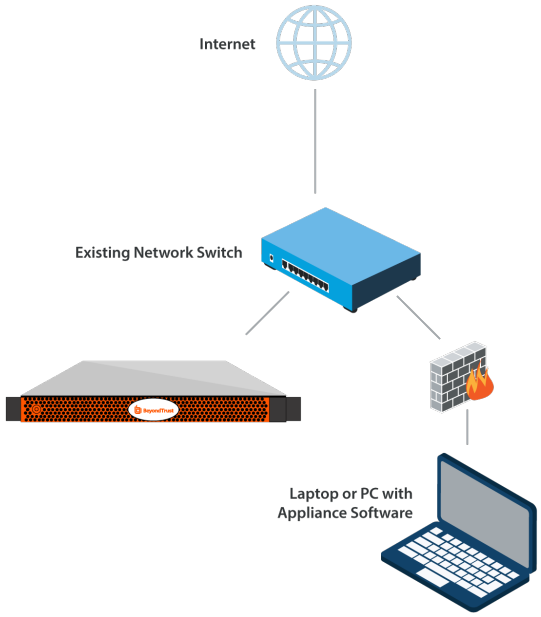
Erste Schritte

Mehrere Schritte sollten vor Lieferung und Installation der BeyondTrust-Hardware vorgenommen werden:

1. Sorgen Sie für ausreichend Rack-Platz für das B-Serien-Gerät. Stellen Sie sicher, dass die notwendige Stromversorgung und Netzwerkzugriff vorliegt.
2. Reservieren Sie eine statische IP-Adresse für das B-Serien-Gerät im Netzwerk. Beziehen Sie sich auf folgende Handbücher, um die richtige(n) IP-Adresse(n) zu reservieren:
    - BeyondTrust-Gerät B-Serie im Netzwerk – www.beyondtrust.com/docs/remote-support/getting-started/deployment/dmz
3. Konfigurieren Sie einen DNS-A-Eintrag für den vollständig qualifizierten Domain-Namen (FQDN) Ihrer neuen Site (z. B. appliance.example.com).

> ***Hinweis:*** *Ein privater DNS A-Eintrag, der zur statischen IP-Adresse Ihres B-Serien-Geräts hin auflöst, ist immer notwendig. Ein öffentlicher A-Eintrag und eine öffentliche IP sind ebenfalls erforderlich, wenn Clients in öffentlichen, externen Netzwerken auf das B-Serien-Gerät zugreifen müssen.*

Obwohl ihr B-Serien-Gerät überall im Netzwerk ausgeführt werden kann, wo Internetzugriff besteht, müssen Sie entscheiden, wo in Ihrem Netzwerk Sie das B-Serien-Gerät vor diesem Schritt installieren möchten. Wenn Sie jedoch auf Systeme außerhalb Ihres Netzwerks zugreifen wollen, empfiehlt BeyondTrust, das B-Serien-Gerät in einer DMZ oder außerhalb Ihrer internen Firewall zu platzieren. Detailliertere Informationen finden Sie in der untenstehenden Tabelle. Unterstützung für die Konfiguration der Firewall erhalten Sie beim Hersteller der Firewall-Software.



> ***Hinweis:*** *Wenn Sie das B-Serien-Gerät an einen anderen Ort bewegen müssen, um eine Internetverbindung herzustellen, müssen Sie es ausschalten und dann von der Stromquelle trennen. Wenn Sie sich in der /appliance-Verwaltungsschnittstelle anmelden können, navigieren Sie zur Seite* ***Status > Einfach*** *und klicken Sie auf* ***Dieses Gerät herunterfahren****. Das manuelle Herunterfahren ist möglich, wenn Sie die Netztaste einmal drücken und wieder loslassen. Warten Sie 60 Sekunden zum Herunterfahren des B-Serien-Geräts, bevor Sie das B-Serien-Gerät von der Stromquelle trennen. Wenn Sie das B-Serien-Gerät am neuen Standort wieder anschließen, müssen Sie es erneut einschalten.*

Erwägungen zum Netzwerkverzeichnis von B-Serien-Gerät

Netzwerkverzeichnis	Vor- und Nachteile
Außerhalb Ihrer Firewall	Setzt nicht voraus, dass die Ports 80 und 443 für eingehenden TCP-Verkehr in Ihrer Firewall offen sind. Macht den Einrichtungsvorgang wesentlich einfacher, da sowohl so konfiguriert sind, dass sie zu einer Ihrem B-Serien-Gerät direkt zugewiesenen öffentlichen IP-Adresse auflösen; es sind keine weiteren Konfigurationsschritte nötig, um eine Sitzung starten zu können.
DMZ	Erfordert je nach Ihrem Router oder Ihren Routern weitere Konfigurationsschritte.

Netzwerkverzeichnis	Vor- und Nachteile
Innerhalb Ihrer Firewall	Setzt die Port-Weiterleitung in Ihrer Firewall voraus und erfordert unter Umständen zusätzliche Konfigurationsschritte zu Ihrem NAT-Routing und internen DNS.

BeyondTrust-Gerät B-Serie – Installation

Eine Installationsanleitung entnehmen Sie bitte den Ihrem BeyondTrust-Gerät B-Serie beiliegenden Flyout-Anweisungen.

Hochfahren des BeyondTrust-Gerät B-Serie

1. Verbinden Sie die Netzkabel des B-Serien-Gerät mit einer sicheren Stromquelle. Abhängig vom B-Serien-Gerät-Typ gibt es möglicherweise zwei Netzkabel. Die Netzteile des B-Serien-Geräts wechseln automatisch zwischen 120 und 240 V, je nach Bedarf.
2. Verbinden Sie Ihren Computer mit einem der mitgelieferten Patch-Kabel mit NIC1 oder NIC2 auf der Rückseite des B-Serien-Gerät. Wenn Sie DHCP verwenden, verbinden Sie das mitgelieferte Netzwerkkabel direkt mit dem Netzwerk. Das B-Serien-Gerät erhält dann automatisch eine neue IP-Adresse.

   Hinweis: *BeyondTrust unterstützt das Platzieren beider NICs im gleichen Netzwerk zum Zwecke des NIC-Teamings. Gleichermaßen können NICs für segmentiertes Datenverkehrs-Routing auf separaten Netzwerk-Subnetzen platziert werden. Wenn Sie jedoch für NIC-Teaming die NICs auf dem gleichen Netzwerk platzieren, konfigurieren Sie nur einen der NICs. Wenn beide NICs über IP-Adressen des gleichen Subnetzes verfügen, kann es zu unerwartetem Verhalten kommen. Wenn mehrere IP-Adressen für ein einzelnes Subnetz erforderlich sind, sollten Sie alle IP-Adressen einem NIC zuordnen.*

3. Drücken Sie die Netztaste auf der Vorderseite des B-Serien-Geräts. Die Netz-LED rechts neben der Reset-Taste beginnt zu leuchten und die Festplattenaktivitäts-LED (rechts neben der Netz-LED) beginnt zu blinken. Die Initialisierung des B-Serien-Gerät ist innerhalb etwa 60 Sekunden abgeschlossen.

   Hinweis: *Die NIC1- und NIC2-LEDs können aufleuchten und Aktivität zeigen, auch wenn das B-Serien-Gerät nicht eingeschaltet ist. Daher sollten Sie auf die Netz- und Festplatten-LEDs achten um zu überprüfen, ob das B-Serien-Gerät eingeschaltet ist.*

Anfängliche Netzwerkkonfiguration während der BeyondTrust-Gerät B-Serie-Einrichtung

Vor der Bereitstellung des BeyondTrust-Gerät B-Serie in Ihrem Netzwerk müssen Sie zunächst die Netzwerkkonfiguration einrichten. Dies erfolgt durch Zugriff auf die B-Serien-Gerät-Verwaltungsschnittstelle über einen Webbrowser auf Ihrem Computer. Die untenstehenden Schritte leiten Sie durch diesen Prozess. Dieser kann abhängig von Ihrem Betriebssystem variieren.

DHCP-Anweisungen

Falls bei dem von Ihnen für Ihr B Series Appliance ausgewählten Netzwerkstandort DHCP aktiviert ist, bezieht das B Series Appliance eine IP-Adresse über das Netzwerk und ist unverzüglich über die jeweilige IP-Adresse unter **https://<ipaddress>/appliance** zugänglich. Sie finden diese IP-Adresse über die Konsole an der Videobuchse.

Verwenden zur Anmeldung den standardmäßigen Benutzernamen und das Passwort.

Standardbenutzername: **admin**

Standardpasswort: **password**

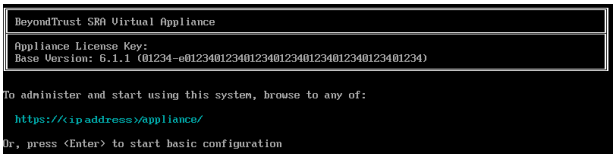
Bei der ersten Anmeldung werden Sie aufgefordert, Ihr B Series Appliance-Verwaltungspasswort zu ändern.

> ***Hinweis:*** *Wenn Sie DHCP verwenden, können Sie den Abschnitt zur* ***Konsolenkonfiguration*** *überspringen und direkt im Bereich /****appliance-Konfiguration*** *fortfahren.*

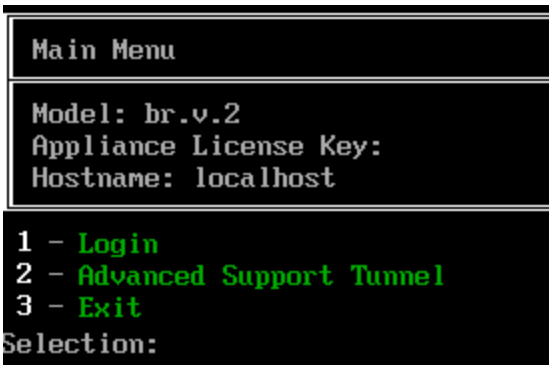
Konsolen-Konfiguration

Wenn an dem für Ihr Gerät gewählten Netzwerkstandort kein DHCP aktiviert ist, muss das Gerät über den Konsolenport mit einer statischen IP konfiguriert werden. Ein Bildschirm und eine Tastatur (über einen USB-Anschluss an der Vorder- oder Rückseite) müssen an das Gerät angeschlossen werden.

1. Drücken Sie **Eingabe**, um sich an der Konsole anzumelden.

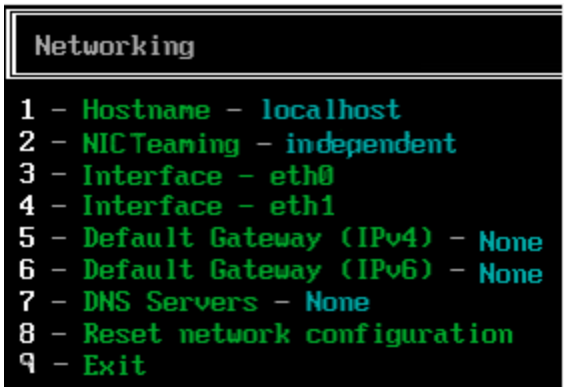


2. Geben Sie **1** ein, um **Login** zu wählen, und drücken Sie dann **Eingabe**.
   - Standardbenutzername: **admin**
   - Standardpasswort: **password**

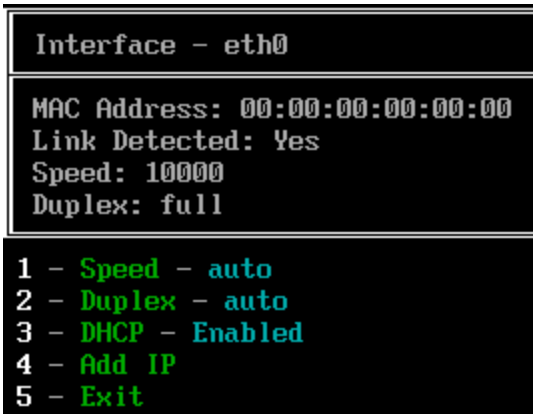


3. Geben Sie **1** ein, um das Menü **Netzwerke** zu wählen, und drücken Sie dann **Eingabe**.

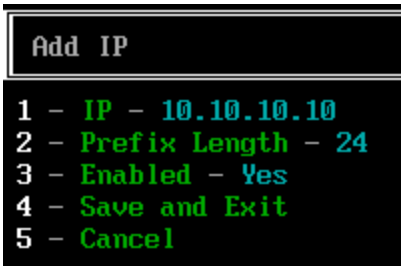
4. Geben Sie **3** ein, um das Menü **Schnittstelle - eth0** zu wählen, und drücken Sie dann **Eingabe**.



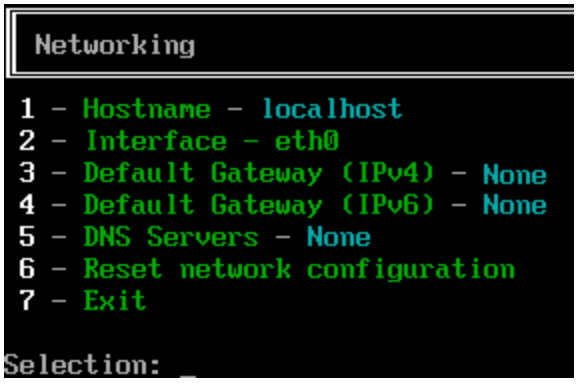
5. Geben Sie **4** ein, um **IP hinzufügen** zu wählen, und drücken Sie dann **Eingabe**.



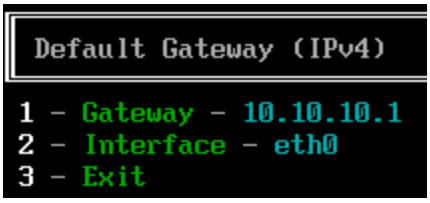
6. Geben Sie **1** ein, um **IP** auszuwählen, und geben Sie die gewünschte IP-Adresse ein. Drücken Sie **Eingabe**.



7. (Optional): Geben Sie **2** ein, um **Präfixlänge** zu wählen, wenn eine Änderung erforderlich ist, und geben Sie dann **4** ein, um **Speichern und Beenden** zu wählen.
8. (Optional): Geben Sie **3** ein, um **DHCP** auf dieser Schnittstelle zu deaktivieren.
9. Geben Sie **3** ein, um **Standardgateway (IPv4)** zu wählen, und drücken Sie dann **Eingabe**.



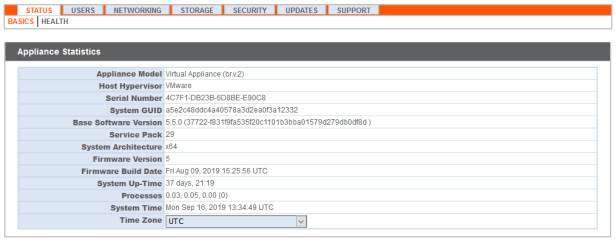
10. Geben Sie **1** ein, um **Gateway** auszuwählen, und geben Sie die gewünschte Standard-Gateway-Adresse ein. Drücken Sie **Eingabe**.



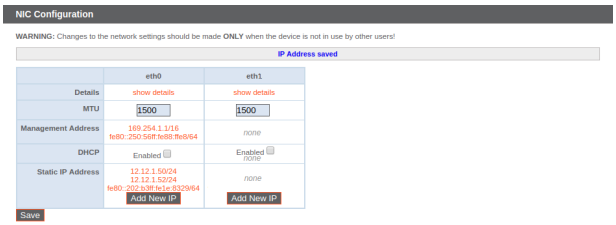
11. Wählen Sie **Speichern und Beenden**, und drücken Sie dann **Eingabe**.
12. Greifen Sie auf Ihr Gerät unter **https://<ipaddress>/appliance** zu.

/appliance-Konfiguration

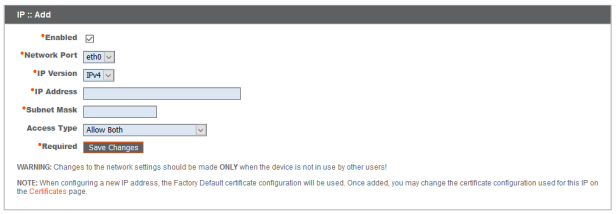
1. Nach der Anmeldung in der /appliance-Schnittstelle sehen Sie die Seite **Status > Einfach**. Diese Seite umfasst Informationen wie die Seriennummer, die der BeyondTrust Technical Support zur Registrierung des B-Serien-Geräts in den BeyondTrust-Lizenzservern benötigt. Machen Sie eine Bildschirmaufnahme dieser Seite und senden Sie sie an den BeyondTrust Technical Support, damit das Support-Team Ihr B-Serien-Gerät registrieren kann.



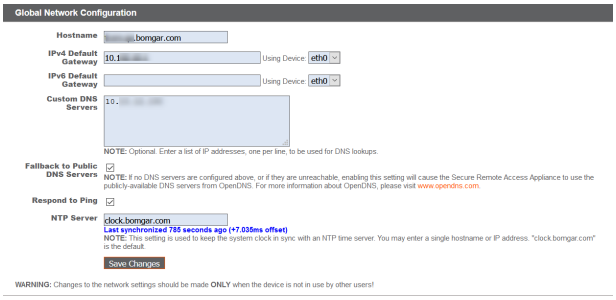
2. Gehen Sie als nächstes zu **Netzwerk > IP-Konfiguration**. Klicken Sie im Bereich **NIC-Konfiguration** auf **Neue IP**.



3. Geben Sie die statische IP-Adresse und Subnetzmaske für Ihr B-Serien-Gerät ein. In der Regel sollten Sie die Standardwerte für beide Felder unverändert lassen. Sie können entscheiden, ob diese IP-Adresse Support-Sitzungsdatenverkehr, Web-Datenverkehr oder beide Arten von Datenverkehr unterstützen soll. Klicken Sie dann auf **Änderungen speichern**.



4. Konfigurieren Sie im Abschnitt **Globale Netzwerkkonfiguration** Ihr Standard-Gateway. Geben Sie Ihre standardmäßigen Gateway- und DNS-Server-Adressen ein. Nachdem Sie die erforderlichen Informationen eingegeben haben, klicken Sie auf **Änderungen speichern**.

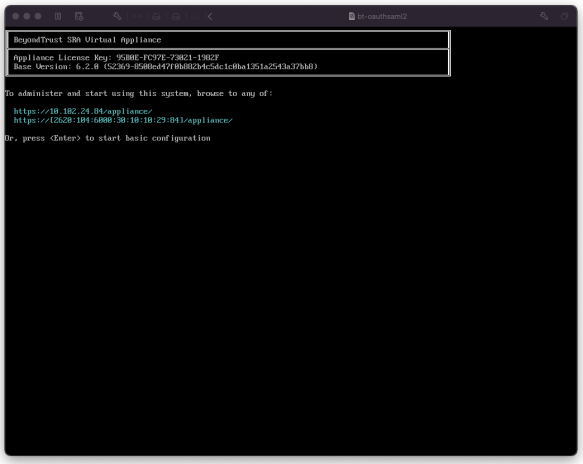


> ***Hinweis:*** *Damit Failover und automatische Updates ordnungsgemäß funktionieren, sind gültige DNS-Einstellungen erforderlich.*

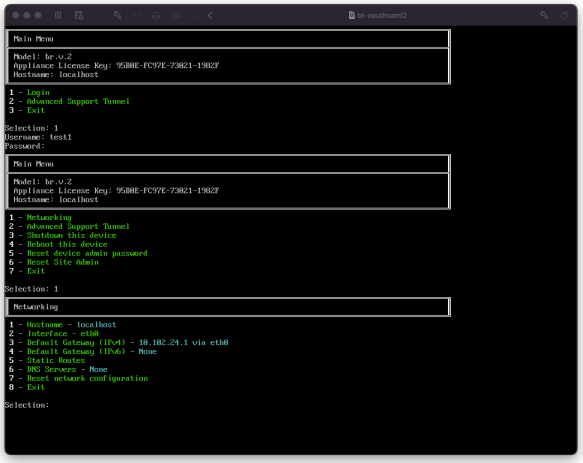
> *Weitere Informationen zur Netzwerkkonfiguration finden Sie unter Das BeyondTrust-Gerät B-Serie im Netzwerk auf https://www.beyondtrust.com/docs/remote-support/getting-started/deployment/dmz/index.htm.*
>
> *Verwaltungsfunktionen können auch durch den Anschluss eines Monitors und einer Tastatur und den Zugriff auf die Computer-Konsole ausgeführt werden. Weitere Informationen finden Sie in „Konsolenverwaltung für sicheren Remote-Zugriff“ auf Seite 12.*

Konsolenverwaltung für sicheren Remote-Zugriff

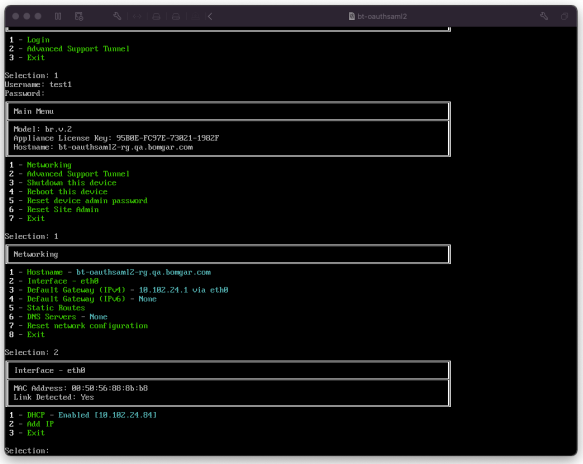
1. Wenn Sie die Bereitstellung Ihres B-Serien-Gerät abgeschlossen haben, können Sie einen Monitor und eine Tastatur anschließen und die Konsole der virtuellen Maschine nutzen, um auf bestimmte Verwaltungsfunktionen zuzugreifen.
2. Auf dem ersten Bildschirm der Konsole der Maschine sind die Hostnamen und IP-Adressen des B-Serien-Gerät aufgeführt. Um über dieses Fenster grundlegende Änderungen an der Konfiguration vorzunehmen, drücken Sie die **Eingabetaste**.



3. Treffen Sie im Menü eine Auswahl. Sie können sich anmelden, um Änderungen an der Konfiguration vorzunehmen. Außerdem können Sie Support-Codes eingeben, um einen vom Gerät initiierten Support-Tunnel zurück zum BeyondTrust Technical Support zu ermöglichen und so komplexe Probleme schnell zu lösen
4. Melden Sie sich an, um weitere Optionen zu erhalten. Sie können Netzwerke konfigurieren, einen erweiterten Support-Tunnel ermöglichen, das B-Serien-Gerät herunterfahren oder neu starten oder das B-Serien-Gerät-Passwort oder das Administratorpasswort einer Website zurücksetzen.



5. Wählen Sie **Netzwerk** aus, um den Hostnamen, die IP-Adressen, das Standard-Gateway, statische Routen und die DNS-Server zu verwalten.
6. Wählen Sie eine Netzwerkschnittstelle aus, um deren Geschwindigkeit oder Duplexkommunikation zu verwalten. Außerdem können Sie IP-Adressen hinzufügen oder bearbeiten.



> ***Hinweis:*** *Verwaltungsfunktionen können auch durch Zugriff auf die B-Serien-Gerät-Verwaltungsschnittstelle über einen Webbrowser auf Ihrem Computer ausgeführt werden. Für den Zugriff auf diese Schnittstelle und für weitere Informationen zu Einstellungen der Netzwerkkonfiguration konsultieren Sie „Anfängliche Netzwerkkonfiguration während der BeyondTrust-Gerät B-Serie-Einrichtung“ auf Seite 8.*

SSL-Zertifikatanforderung für das BeyondTrust-Gerät B-Serie

Alle BeyondTrust-Softwarekommunikation erfolgt über sichere, verschlüsselte Verbindungen. Diese basieren auf dem branchenerprobten SSL-Standard und der DNS-Adresse des B-Serien-Geräts. B-Serien-Geräte werden mit einem Standard-Zertifikat ausgeliefert, das alle Verbindungen auf allen IP-Adressen sichert. Dies erfüllt jedoch nicht die Anforderungen der BeyondTrust-Client-Software, welche strengere Validierungsprüfungen als Standardwebbrowser durchführt. Bevor Ihnen BeyondTrust daher ein voll funktionsfähiges Softwarelizenzpaket zur Verfügung stellen kann, erfordert Ihr B-Serien-Gerät zunächst die Installation eines gültigen SSL-Zertifikats, das dem DNS A-Eintrag entspricht, den Sie für Ihr B-Serien-Gerät registriert haben.

Ein gültiges SSL-Zertifikat kann entweder ein von einer Zertifizierungsstelle signiertes (CA-signiertes) SSL-Zertifikat oder ein selbstsigniertes SSL-Zertifikat sein. CA-signierte Zertifikate müssen alle BeyondTrust-Funktionen voll unterstützen (z. B. Click-to-Chat und mobile Clients), erfordern jedoch, dass Sie eine Anfrage zur Zertifikatsignierung (CSR) an die Zertifizierungsstelle senden. Die CSR-Anfrage ist ein Branchenstandard, der von allen Netzwerkgeräten und von Software mit SSL verwendet wird. Wenn statt eines selbstsignierten Zertifikats ein CSR/CA-signiertes Zertifikat verwendet wird, muss das CA-signierte Zertifikat von der Website der Zertifizierungsstelle (oder über die Zertifikat-Kauf-E-Mail) heruntergeladen und über die /appliance-Schnittstelle im B-Serien-Gerät importiert werden. Neben der Funktion zur Anforderung eines Zertifikats bei einer Zertifizierungsstelle bietet BeyondTrust Funktionen zum Abruf und automatischen Verlängern eigener TLS-Zertifikate über die offene Zertifizierungsstelle Let‘s Encrypt.

Weitere Informationen zum Erstellen und Verwalten von SSL-Zertifikaten in BeyondTrust RS finden Sie in den folgenden Artikeln:

- *Erstellen eines von einer Zertifizierungsstelle signierten SSL-Zertifikats für Ihr BeyondTrust-Gerät B-Serie auf www.beyondtrust.com/docs/remote-support/how-to/sslcertificates/create-ca-signed.htm*
- *Erstellen eines selbstsignierten Zertifikats für Ihr BeyondTrust-Gerät B-Serie auf www.beyondtrust.com/docs/remote-support/how-to/sslcertificates/create-self-signed.htm*
- *Zertifikate: Erstellen und Verwalten von SSL-Zertifikaten auf www.beyondtrust.com/docs/remote-support/getting-started/deployment/web/security-certificates.htm.*

Weitere Informationen dazu, wie BeyondTrust SSL-Zertifikate verwendet, sowie detaillierte Konfigurationsschritte zur Anforderung und Installation von Zertifikaten in BeyondTrust finden Sie im SSL-Zertifikatshandbuch auf www.beyondtrust.com/docs/remote-support/how-to/sslcertificates.

Der Abschnitt Ein SSL-Zertifikat erstellen beschreibt die nötigen Schritte für die Anfangskonfiguration im Detail. Nachfolgend finden Sie einen Überblick über das Verfahren.

1. Melden Sie sich in der BeyondTrust /appliance-Schnittstelle an und erstellen Sie eine Zertifikatsignierungsanfrage (CSR) oder ein selbstsigniertes Zertifikat.

   ***Hinweis:** Wenn das B-Serien-Gerät eine Kopie des Zertifikats eines anderen B-Serien-Gerät oder Server verwendet, ist kein CSR oder selbstsigniertes Zertifikat nötig. Exportieren Sie das Zertifikat stattdessen mit seinem privaten Schlüssel aus seinem aktuellen System und importieren Sie es in das B-Serien-Gerät. Weitere Einzelheiten finden Sie im Abschnitt SSL-Zertifikat im Failover und in Atlas-B-Serien-Geräte replizieren im Leitfaden für SSL-Zertifikate.*

2. Weisen Sie das neue Zertifikat der/den IP-Adresse(n) des B-Serien-Gerät zu.
3. Senden Sie dem BeyondTrust Technical Support eine Kopie des SSL-Root-Zertifikates und/oder der B-Serien-Gerät-DNS-Adresse.

> ***Hinweis:*** *Wird ein selbstsigniertes Zertifikat verwendet, dient das Zertifikat als sein eigenes Root-Zertifikat – aus diesem Grund sollte das selbstsignierte Zertifikat an das BeyondTrust Technical Support gesendet werden. Wird ein CA-signiertes Zertifikat verwendet, kontaktieren Sie CA, um eine Kopie des Root-Zertifikats anzufordern. Wenn Sie bei der Kontaktaufnahme mit der Zertifizierungsstelle Schwierigkeiten haben, finden Sie auf beyondtrustcorp.service-now.com/csm Artikel, die beim Bezug Ihres Root-Zertifikats nützlich sein könnten. In jedem Fall braucht der BeyondTrust Technical Support die DNS-Adresse des B-Serien-Geräts. Wenn Ihre DNS-Adresse öffentlich ist und das SSL-Zertifikat bereits installiert ist, kann der Support anhand der öffentlichen DNS-Adresse eine Kopie des Roots abrufen; in diesem Fall müssen Sie das Root-Zertifikat nicht manuell senden.*

Nach dem Abschluss der obigen Schritte enkodiert der BeyondTrust Technical Support den DNS-Hostnamen und das SSL-Root-Zertifikat in einem neuen Software-Lizenzpaket, sendet dies zur Kompilierung an die BeyondTrust-Lizenzserver und schickt Ihnen dann Anweisungen zur Installation des neu kompilierten Pakets.

Senden von B-Serien-Gerät Informationen an den technischen BeyondTrust-Support

Bei der Kompilierung Ihres Softwarepakets verschlüsselt der technische BeyondTrust Technical Support-Support den DNS-Hostnamen und das SSL-Root-Zertifikat Ihres B-Serien-Geräts in der Software. Bevor der technische BeyondTrust Technical Support-Support Ihre Software kompilieren kann, müssen Sie die folgenden Informationen angeben.

1. DNS-Hostname (vollqualifizierter Domänenname) von B-Serien-Gerät (z. B. appliance.example.com).
2. SSL-Root-Zertifikat oder selbstsigniertes SSL-Zertifikat. Dies erhalten Sie auf der Seite **/appliance > Sicherheit > Zertifikate**. Exportieren Sie den Zertifikatteil mit passenden Feldern für **Ausgestellt für** und **Ausgestellt von**.
3. Eine Bildschirmaufnahme der Seite **/appliance > Status > Einfach**.

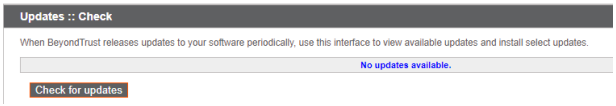
Suchen nach Aktualisierungen zur Installation der BeyondTrust SRA-Software

Aktualisierungen des BeyondTrust-Gerät B-Serie werden über die /appliance-Webschnittstelle auf der Seite **Aktualisierungen** installiert. Jede Aktualisierung muss von BeyondTrust kompiliert werden und wird spezifisch für die Seriennummer des B-Serien-Gerät erstellt. Aus diesem Grund muss das B-Serien-Gerät registriert werden, um auf Aktualisierungen prüfen zu können.

1. Hat BeyondTrust eine Aktualisierung für Ihr B-Serien-Gerät kompiliert, werden Sie per E-Mail benachrichtigt. Gehen Sie zu **/appliance > Aktualisierungen**. Rufen Sie die Aktualisierung entweder über **Aktualisierungen :: Prüfen > Auf Aktualisierungen prüfen** oder **Aktualisierungen :: Manuelle Installation > Geräte-Download-Schlüssel** ab.

   > ***Hinweis:*** *Die Option **Auf Aktualisierungen prüfen** kann nur verwendet werden, wenn das B-Serien-Gerät über einen ausgehenden Zugriff über TCP-Port 443 auf **btupdate.com** verfügt. Die manuelle Installation erfordert diese Verbindung nicht.*

2. Ist die Überprüfung abgeschlossen, werden alle verfügbaren Aktualisierungen, die mit der Seriennummer Ihres B-Serien-Gerät übereinstimmen, in der /appliance-Webschnittstelle aufgeführt. Es gibt zwei Aktualisierungstypen:
   - Aktualisierungen für die /login-Lizenzierung (stets im Format **BeyondTrust-x.x.x**)
   - Aktualisierungen für die /appliance-Basissoftware (stets im Format **Base Software x.x.x**)



   Wenn für Ihr B-Serien-Gerät keine Aktualisierungspakete oder Patches verfügbar sind, wird die Meldung „Keine Aktualisierungen verfügbar“ angezeigt. Wenn eine Aktualisierung verfügbar ist, aber ein Fehler beim Übertragen der Aktualisierung auf Ihr B-Serien-Gerät auftritt, wird eine weitere Meldung wie „Ein Fehler ist beim Kompilieren Ihrer Aktualisierung aufgetreten. Weitere Informationen finden Sie unter www.beyondtrust.com/support."

   Die Basissoftware umfasst Funktionen und Fehlerbehebungen für /appliance sowie den erforderlichen Code für die Installation von Lizenzaktualisierungen. Daher erfordern neue Lizenzierungsaktualisierungen in der Regel die Installation der benötigten Basissoftware-Aktualisierung. In diesem Fall weist die Aktualisierungsschnittstelle von BeyondTrust auf die korrekte Reihenfolge der Aktualisierungsinstallationen hin. Falls Sie sich dennoch nicht sicher sein sollten, machen Sie eine Bildschirmaufnahme Ihrer verfügbaren Aktualisierungen und senden Sie sie an BeyondTrust Technical Support.

WICHTIG!

Wir möchten Sie daran erinnern, dass Sie dem BeyondTrust Technical Support die folgenden Dinge zur Verfügung stellen müssen, bevor der Support Ihre Basissoftware- und/oder Softwarelizenzaktualisierungen bereitstellen kann:

1. *DNS-Hostname (vollqualifizierter Domänenname) des B-Serien-Gerät*
2. *SSL-Root-Zertifikat oder selbstsigniertes SSL-Zertifikat*
3. *Bildschirmaufnahme der Seite **/appliance > Status > Allgemein***

3. Sobald Sie dem BeyondTrust Technical Support Ihren Hostnamen, Ihr SSL-Zertifikat und eine Bildschirmaufnahme gesendet haben, kompiliert dieser die nötigen Aktualisierungen und sendet Ihnen detaillierte Installationsanweisungen.

4. Nach Abschluss der Installation kann das B-Serien-Gerät für den berechtigten Zugriff verwendet werden. Um die Bereitschaft Ihres B-Serien-Geräts zu überprüfen, melden Sie sich in der /login-Schnittstelle an, indem Sie zur B-Serien-Gerät-URL gefolgt von /login navigieren (z. B. appliance.example.com/login).

   Standardbenutzername: **admin**

   Standardpasswort: **password**

5. Sie werden bei der ersten Anmeldung aufgefordert, Ihr Passwort zu ändern.
6. Nach Abschluss der anfänglichen Anmeldung können Sie Ihre Softwarelizenzkonfiguration auf der Seite **Status > Informationen** validieren, Benutzerkonten unter **Benutzer und Sicherheit > Benutzer** hinzufügen und Client-Software über **Mein Konto** herunterladen. Weil BeyondTrust Sicherer Remote-Zugriff auf Basis der gestatteten Endpunkte lizenziert wird, können Sie so viele Konten wie benötigt hinzufügen, jeweils mit eigenen Benutzernamen und Kennwörtern.

Aus Sicherheitsgründen unterscheiden sich der Administrator-Benutzername und das für die Schnittstelle /appliance verwendete Passwort von den für die Schnittstelle /login verwendeten Anmeldedaten und müssen daher separat verwaltet werden. Benutzernamen und Kennwörter für /login gelten sowohl für die /login-Schnittstelle (wo Benutzer und die Konfiguration verwaltet werden) als auch für -Konsolen (wo Sitzungen ausgeführt werden). Die an beiden Orten verfügbaren Optionen sind von den Berechtigungen abhängig, die vom /login-Administrator für jedes Benutzerkonto festgelegt wurden.

Für Hilfe zur Verwendung der Client-Software von BeyondTrust siehe die Dokumentation unter www.beyondtrust.com/docs. Die B-Serien-Gerät-Handbücher und Sicherer Remote-Zugang-Verwaltungshandbücher erläutern die unterschiedlichen Administrationsoptionen Ihrer /appliance- und /login-Webschnittstellen. Die Zugriffs-Benutzerhandbücher erläutern die Verwendung der BeyondTrust-Client-Software.