BeyondTrust

Remote Support
Hardware-Installation des Geräts

TC:22.04.2021

Table of Contents

Aufgabenliste zur Einrichtung des Geräts

Diese Aufgabenliste ist eine Kurzreferenz für die notwendigen Schritte zur Einrichtung Ihres Secure Remote Access Appliance. 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 Domänennamen (FQDN) Ihrer neuen Seite (z. B. support.beispiel.com).
    - Wenn sich Ihr Gerät in Ihrer DMZ oder in Ihrem internen Netzwerk befinden wird, wird ein interner A-Eintrag benötigt, der auf die interne IP-Adresse des Gerätes verweist.
    - Wenn Sie externe Kunden unterstützen möchtenSupport, muss ebenfalls ein öffentlicher DNS A-Eintrag für die externe IP-Adresse des Geräts registriert werden.
    - Detaillierte Informationen zu BeyondTrust-Netzwerkbereitstellungsszenarien finden Sie in Das Secure Remote Access Appliance im Netzwerk unter www.beyondtrust.com/docs/deployment/dmz/index.htm.

    WICHTIG!

    „BeyondTrust“ kann nicht im FQDN Ihrer Website verwendet werden.

2. Installieren Sie das Secure Remote Access Appliance entsprechend „Secure Remote Access Appliance – Installation“ auf Seite 7.
3. Beziehen Sie ein SSL-Zertifikat, das Ihrer FQDN-DNS entspricht (z. B. support.beispiel.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 Gerät und ordnen Sie dieser die IP-Adresse des Gerätes 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 Gerätes 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://support.beispiel.com/login).
    c. Verwenden Sie die standardmäßigen Administrator-Anmeldedaten **admin** und **password** zur erstmaligen Anmeldung.

BeyondTrust – Hardware-Voraussetzungen

Dieser Leitfaden führt Sie durch die Ersteinrichtung und Konfiguration Ihres virtuellen Secure Remote Access Appliance. Sollten Sie Hilfe benötigen, wenden Sie sich bitte an www.beyondtrust.com/support.

Voraussetzungen

Beachten Sie vor dem Beginnen: Erst wenn Sie die Voraussetzungen des Secure Remote Access Appliance erfüllt haben, können Sie das Gerät direkt über die IP-Adresse oder den Hostnamen erreichen oder auf Aktualisierungen prüfen oder darüber Remote-Support bereitstellen. Das Secure Remote Access Appliance erfordert mindestens Folgendes:

- Ein oder zwei freie Steckdosen, abhängig vom Gerät (eine beim B200, zwei beim B300 oder B400)
- Eine Hochgeschwindigkeits-Netzwerkverbindung
- Einen Netzwerkrouter oder -switch
- Eine eindeutige, statische IP-Adresse für das Secure Remote Access Appliance
- Einen privaten DNS A-Eintrag, der zur statischen IP Ihres Geräts hin auflöst. Ein öffentlicher A-Eintrag und eine öffentliche IP sind ebenfalls erforderlich, wenn externe Clients auf das Gerät zugreifen müssen.
- Ein SSL-Webserver-Zertifikat + intermediäre SSL-Zertifikat(e) und ein SSL-Root. ODER: 1 selbstsigniertes Zertifikat. (Siehe Leitfaden für SSL-Zertifikate und BeyondTrust.)
- Das BeyondTrust-Softwarelizenzpaket

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

- BeyondTrust Click-to-Chat- und mobile Clients erfordern ein SSL-Root- und SSL-Zwischenzertifikat(e).
- 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 Secure Remote Access Appliance über TCP-Port 443.

WICHTIG!

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

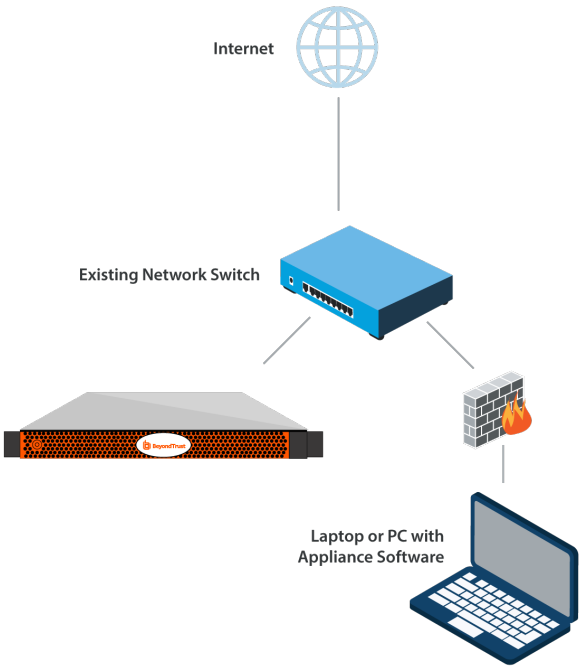
Erste Schritte

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

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

> ***Hinweis:*** *Ein privater DNS A-Eintrag, der zur statischen IP Ihres 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 Gerät zugreifen müssen.*

Obwohl ihr Gerät überall im Netzwerk betrieben werden kann, solange die richtigen Benutzer und Systeme es erreichen können, müssen Sie entscheiden, wo in Ihrem Netzwerk Sie das Gerät vor diesem Schritt installieren möchten. Wenn Sie jedoch auf Systeme außerhalb Ihres Netzwerks zugreifen wollen, empfiehlt BeyondTrust, das 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 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 Gerätes, bevor Sie das Secure Remote Access Appliance von der Stromquelle trennen. Wenn Sie das Gerät am neuen Standort wieder anschließen, müssen Sie es erneut einschalten.*

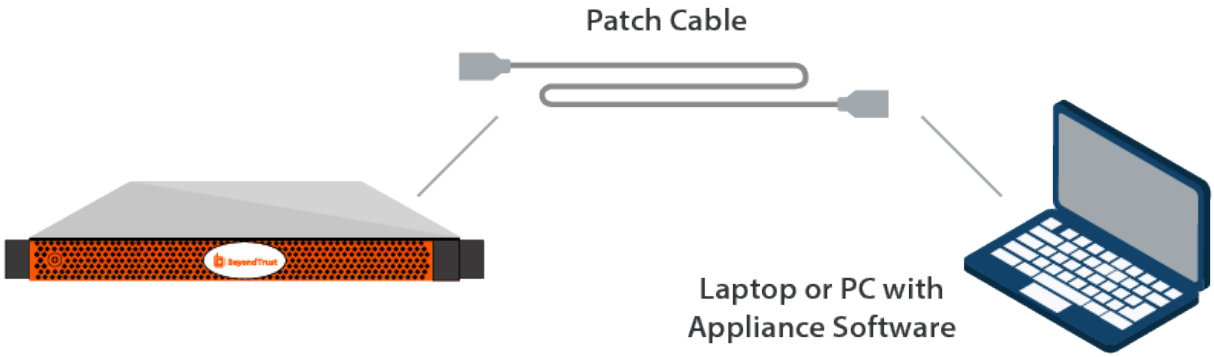
Erwägungen zum Netzwerkverzeichnis von Secure Remote Access Appliance

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 Clients und Konsolen des Support-Technikers als auch der Client des Kunden so konfiguriert sind, dass sie zu einer Ihrem 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.
Innerhalb Ihrer Firewall	Setzt die Port-Weiterleitung in Ihrer Firewall voraus und erfordert unter Umständen zusätzliche Konfigurationsschritte zu Ihrem NAT-Routing und internen DNS.

Secure Remote Access Appliance – Installation

Eine Installationsanleitung entnehmen Sie bitte den Ihrem Secure Remote Access Appliance beiliegenden Flyout-Anweisungen. Alternativ können Sie das Poweredge-Benutzerhandbuch unter www.beyondtrust.com/docs/remote-support/documents/infrastructure/rs-appliance-rail-installation.pdf konsultieren.

Hochfahren des Secure Remote Access Appliance



1. Verbinden Sie die Netzkabel des Secure Remote Access Appliance mit einer sicheren Stromquelle. Abhängig vom Gerätetyp gibt es möglicherweise zwei Netzkabel. Die Netzteile des Gerätes 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 Secure Remote Access Appliance. Sie können entweder Crossover- oder Straight-Through-Kabel verwenden. Wenn Sie DHCP verwenden, verbinden Sie das mitgelieferte Netzwerkkabel direkt mit dem Netzwerk. Das 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 Gerätes. 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 Secure Remote Access Appliance ist innerhalb etwa 60 Sekunden abgeschlossen.

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

Anfängliche Netzwerkkonfiguration während der Geräteeinrichtung

Vor der Bereitstellung des Secure Remote Access Appliance in Ihrem Netzwerk müssen Sie zunächst die Netzwerkkonfiguration einrichten. Dies erfolgt durch Zugriff auf die Secure Remote Access Appliance-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 Gerät ausgewählten Netzwerkstandort DHCP aktiviert ist, bezieht das Gerät 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 Kennwort.

Standardbenutzername: **admin**

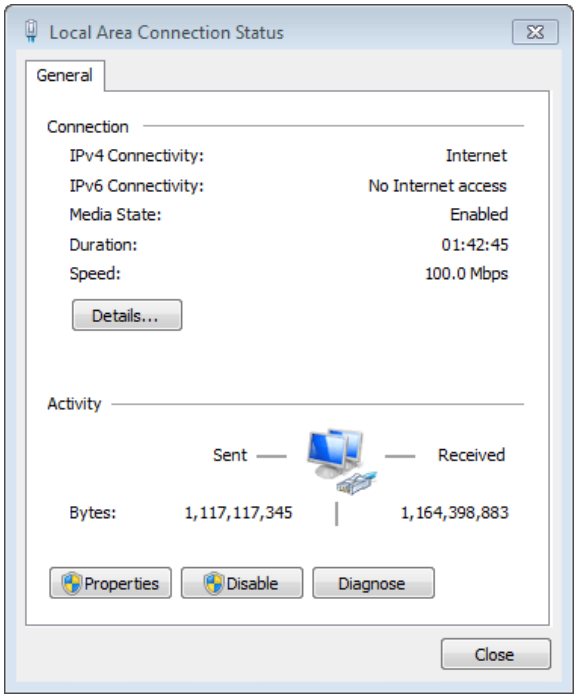
Standardkennwort: **password**

Bei der ersten Anmeldung werden Sie aufgefordert, Ihr Geräte-Verwaltungskennwort zu ändern.

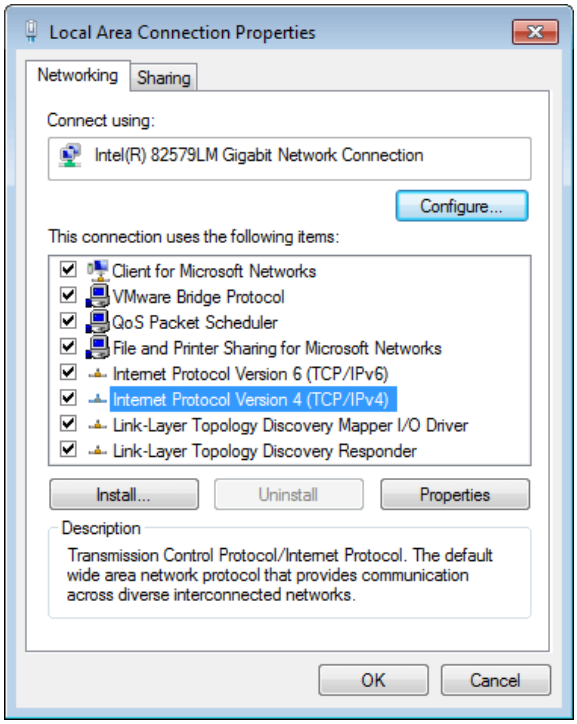
> ***Hinweis:*** *Wenn Sie DHCP verwenden, können Sie den Abschnitt zu den* ***Anweisungen für lokale Netzwerkverbindungen*** *überspringen und direkt im Bereich* ***/appliance-Konfiguration*** *fortfahren.*

Anweisungen für lokale Netzwerkverbindungen

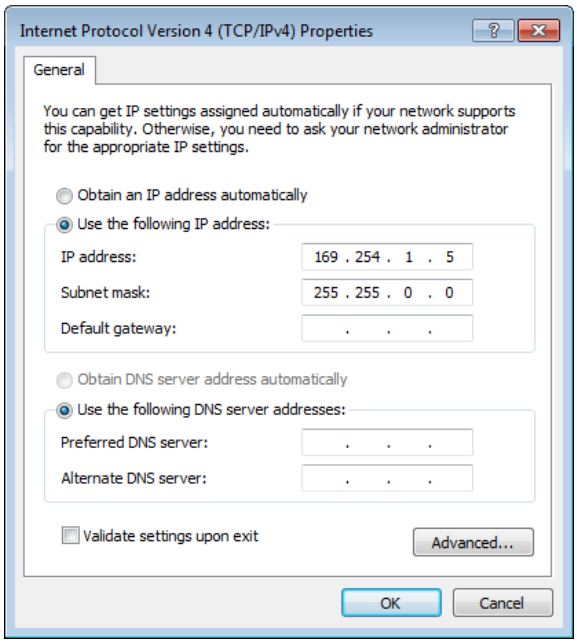
1. Navigieren Sie nach der externen Einrichtung Ihres Secure Remote Access Appliance zu **Lokale Netzwerkverbindung** auf Ihrem Computer und klicken Sie auf **Eigenschaften**.



2. Markieren Sie Internet Protocol Version 4 (IPv4) und klicken Sie auf die Schaltfläche **Eigenschaften**.



3. Geben Sie **169.254.1.5** als Ihre IP-Adresse und **255.255.0.0** als Subnetzmaske ein. Stellen Sie sicher, dass die Felder „Gateway“ und „DNS“ leer bleiben.

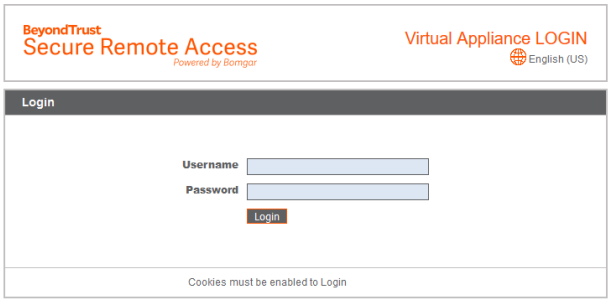


4. Öffnen Sie einen Webbrowser und geben Sie die Adresse **https://169.254.1.1/appliance/login.ns** im URL-Adressfeld ein. Versuchen Sie andernfalls, in der letzten Dezimalstelle der obigen Adresse den Wert durch „.2“, „.3“ oder „.4“ zu ersetzen. Laden Sie diese Adressen separat, bis Sie auf eine davon zugreifen könne. Geben Sie den standardmäßigen Benutzernamen und das dazugehörige Kennwort ein und klicken Sie auf **Anmelden**.

   Standardbenutzername: **admin**

   Standardkennwort: **password**

   Bei der ersten Anmeldung werden Sie aufgefordert, Ihr Geräte-Verwaltungskennwort zu ändern.

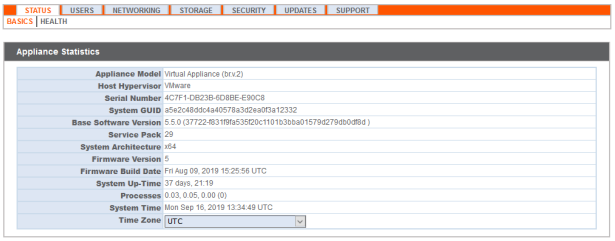


Hinweis: *Das Secure Remote Access Appliance verwendet zwei administrative Webschnittstellen,* ***/appliance*** *und* ***/login****, um die Hardware-Verwaltung von der Benutzerverwaltung zu trennen. Die* ***/appliance****-Schnittstelle wird verwendet, um Netzwerkeinstellungen zu konfigurieren und die BeyondTrust-Software zu aktualisieren. Sie das Secure Remote Access Appliance-Webschnittstelle-Handbuch unter www.beyondtrust.com/docs/remote-support/getting-started/deployment/web/index.htm.*

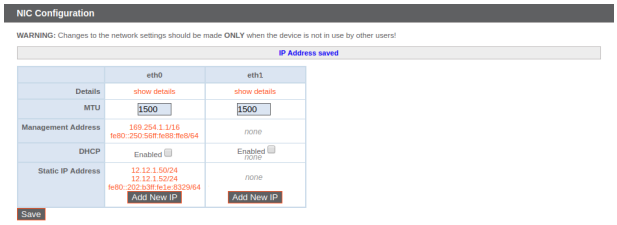
Die ***/login****-Schnittstelle ist erst verfügbar, wenn der BeyondTrust Technical Support das notwendige Softwarelizenzpaket kompiliert hat und dieses Paket über /appliance installiert wird. Nach der Installation wird* ***/login*** *zur Verwaltung von Benutzern und Workflows, zur Bereitstellung von Client-Software, für Berichte zur Zugriffsaktivität, zur Erstellung und Verwendung von Integrationen usw. verwendet. Siehe BeyondTrust-Verwaltungsschnittstelle unter www.beyondtrust.com/docs/remote-support/getting-started/admin/.*

/appliance-Konfiguration

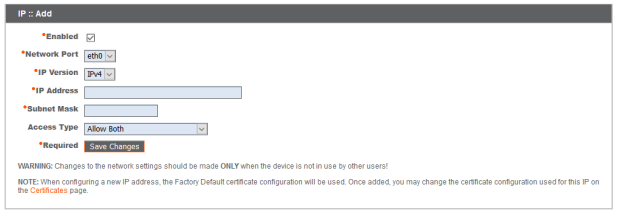
1. Nach der Anmeldung in der **/appliance**-Schnittstelle sehen Sie die Seite **Status > Einfach**. Diese Seite umfasst Informationen wie die Seriennummer, die der BeyondTrust Technical Support zur Registrierung des Gerätes in den BeyondTrust-Lizenzservern benötigt. Machen Sie eine Bildschirmaufnahme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



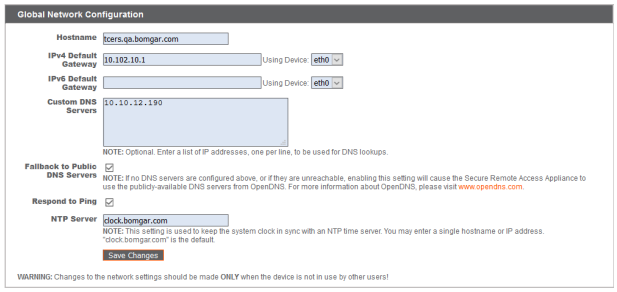
2. Gehen Sie als nächstes zu **Netzwerk > IP-Konfiguration**. Klicken Sie im Bereich **NIC-Konfiguration** auf **Neue IP**.



3. Geben Sie die statische IP-Adresse und Subnetzmaske für Ihr Secure Remote Access Appliance ein und klicken Sie dann auf **Änderungen speichern**. 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.



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**.

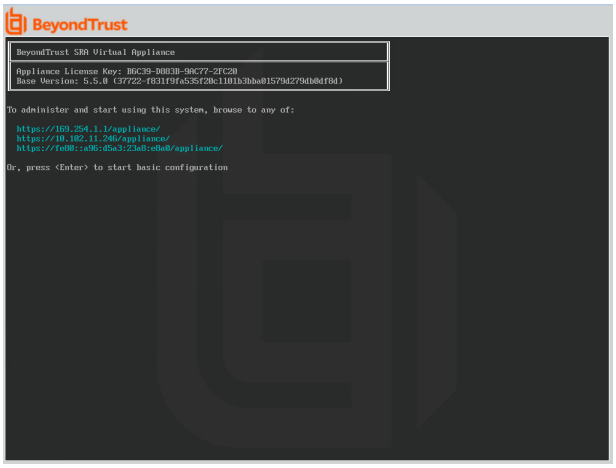


> ***Hinweis:*** *Damit Failover und automatische Updates ordnungsgemäß funktionieren, sind gültige DNS-Einstellungen erforderlich.*

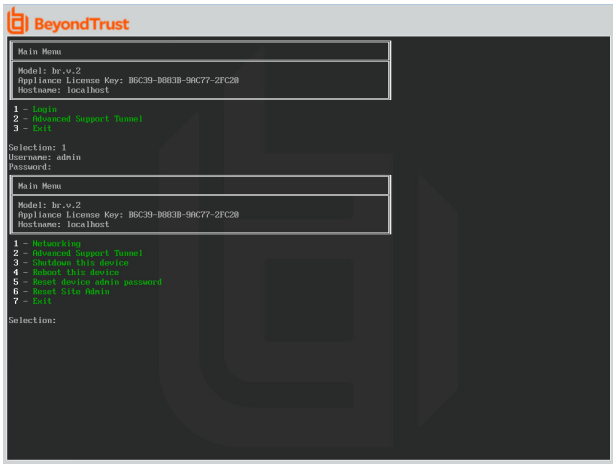
> *Detaillierte Informationen zur Netzwerkkonfiguration finden Sie in Das Secure Remote Access Appliance im Netzwerk unter www.beyondtrust.com/docs/remote-support/getting-started/deployment/dmz/index.htm.*
>
> *Verwaltungsfunktionen können auch durch den Anschluss eines Monitors und einer Tastatur und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

Konsolenverwaltung

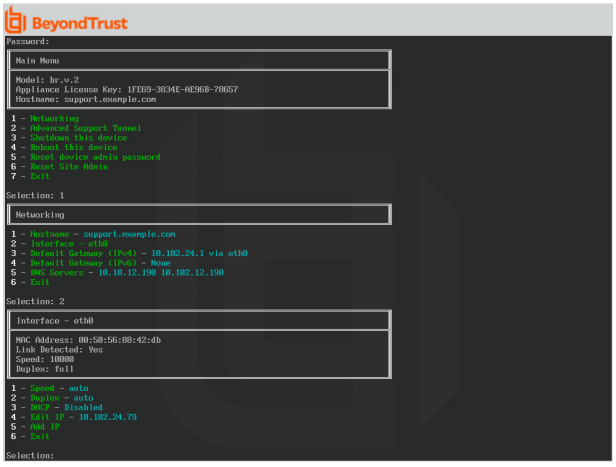
1. Wenn Sie die Bereitstellung Ihres Secure Remote Access Appliance abgeschlossen haben, können Sie einen Monitor und eine Tastatur anschließen und die Konsole der virtuellen Maschine nutzen, um auf bestimmte Verwaltungsfunktionen zuzugreifen.
2. Auf dem ersten Bildschirm der Konsole der Maschine sind die Hostnamen und IP-Adressen des Secure Remote Access Appliance 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 Secure Remote Access Appliance herunterfahren oder neu starten oder das Kennwort des Geräts oder das Administratorkennwort einer Website zurücksetzen.



5. Wählen Sie **Netzwerk** aus, um den Hostnamen, die IP-Adressen, das Standard-Gateway 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.



> *Verwaltungsfunktionen können auch durch Zugriff auf die Secure Remote Access Appliance-Verwaltungsschnittstelle über einen Webbrowser auf Ihrem Computer ausgeführt werden. Für den Zugriff auf diese Schnittstelle und für weitere Informationen zu Einstellungen der Netzwerkkonfiguration finden Sie in „Anfängliche Netzwerkkonfiguration während der Geräteeinrichtung“ auf Seite 8.*

SSL-Zertifikatsanforderungen

Alle BeyondTrust-Softwarekommunikation erfolgt über sichere, verschlüsselte Verbindungen. Diese basieren auf dem branchenerprobten SSL-Standard und der DNS-Adresse des Geräts. Secure Remote Access Appliance werden mit einem Standard-Zertifikat ausgeliefert, das die anfängliche Verbindung mit der Verwaltungsadresse 169.254.1.x 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 Secure Remote Access Appliance zunächst die Installation eines gültigen SSL-Zertifikats, das dem DNS A-Eintrag entspricht, den Sie für Ihr 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 Secure Remote Access Appliance 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 unter www.beyondtrust.com/docs/remote-support/how-to/sslcertificates/create-ca-signed.htm*
- *Erstellen eines selbstsignierten Zertifikats unter www.beyondtrust.com/docs/remote-support/how-to/sslcertificates/create-self-signed.htm*
- *Zertifikate: Erstellen und Verwalten von SSL-Zertifikaten unter 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 unter www.beyondtrust.com/docs/remote-support/how-to/sslcertificates/index.htm.

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

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

***Hinweis:** Wenn das Secure Remote Access Appliance eine Kopie des Zertifikats eines anderen Secure Remote Access Appliance 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 Secure Remote Access Appliance.*

Weitere Einzelheiten finden Sie im Abschnitt SSL-Zertifikat im Failover und in Atlas-Geräten replizieren im Leitfaden für SSL-Zertifikate.

- Senden Sie BeyondTrust Technical Support eine Kopie des SSL-Root-Zertifikates oder der Geräte-DNS-Adresse. Lassen Sie ihm außerdem eine Bildschirmaufnahme der Seite **/appliance > Status > Grundlagen** zukommen.

***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 www.beyondtrust.com/support Artikel, die beim Bezug Ihres Root-Zertifikats nützlich sein könnten. In jedem Fall braucht der BeyondTrust Technical Support die DNS-Adresse des 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. Wenn Sie das SSL-Zertifikat senden, achten Sie darauf, dass es das Format PKCS#7 (.p7b) oder DER (.cer) aufweist. Senden Sie **nicht** im Format PKCS#12 (.p12 und .pfx).*

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 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 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) des Geräts (z. B. support.beispiel.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 -Software

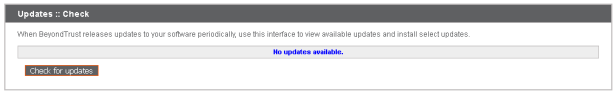
Aktualisierungen des Secure Remote Access Appliance werden über die /appliance-Webschnittstelle auf der Seite **Aktualisierungen** installiert. Jede Aktualisierung muss von BeyondTrust kompiliert werden und wird spezifisch für die Seriennummer des Gerätes erstellt. Aus diesem Grund muss das Gerät registriert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

1. Hat BeyondTrust eine Aktualisierung für Ihr 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 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 Geräts 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**)

   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.

   Wenn für Ihr Secure Remote Access Appliance 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 Gerät auftritt, wird eine weitere Meldung wie „Ein Fehler ist beim Kompilieren Ihrer Aktualisierung aufgetreten. Weitere Informationen finden Sie unter www.beyondtrust.com/docs/index.htm#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. *Vollqualifizierter Domänenname des Geräts*
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 Secure Remote Access Appliance für den Remote-Support verwendet werden. Um die Bereitschaft Ihres Geräts zu überprüfen, melden Sie sich in der /login-Schnittstelle an, indem Sie zur Geräte-URL gefolgt von /login navigieren (z. B. support.beispiel.com/login).

   Standardbenutzername: **admin**

   Standardkennwort: **password**

5. Sie werden bei der ersten Anmeldung aufgefordert, Ihr Kennwort 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 Remote Support von mehreren Benutzern gleichzeitig lizenziert wird, können Sie beliebig viele Konten mit jeweils eindeutigen Benutzernamen und Kennwörtern einrichten.

Aus Sicherheitsgründen unterscheiden sich der Administrator-Benutzername und das für die Schnittstelle /appliance verwendete Kennwort 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 Konsole d. Support-Technikers-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/index.htm. Die Gerätehandbücher und Support-Verwaltungshandbücher erläutern die unterschiedlichen Administrationsoptionen Ihrer /appliance- und /login-Webschnittstellen. Die Support-Techniker-Benutzerhandbücher erläutern die Verwendung der Client-Software von BeyondTrust.

Eigentumshinweise zu quelloffener Software

Informationen zum Urheberrecht und Eigentumshinweise zu quelloffener Software, die in den Hardware- und Software-Produkten von BeyondTrust verwendet wird, finden Sie im Attributionsindex unter www.beyondtrust.com/docs/remote-support/updates/attributions.