



# BeyondTrust

## **Privileged Remote Access Aktualisierungshandbuch**

## Inhaltsverzeichnis

---

<b>Upgrade der BeyondTrust Privileged Remote Access-Software vornehmen</b> .....	<b>3</b>
<b>Ein einziges BeyondTrust-Gerät mithilfe der automatischen Aktualisierung upgraden</b> ..	<b>5</b>
<b>Upgrade eines einzigen BeyondTrust-Geräts mit manuellen Aktualisierungen</b> .....	<b>7</b>
<b>Zwei Geräte in einer Failover-Konfiguration upgraden</b> .....	<b>9</b>
<b>Synchrone Aktualisierung zweier BeyondTrust-Geräte in einer Failover-Beziehung</b> ....	<b>10</b>
Sicherung und Synchronisierung .....	10
Aktualisieren von Gerät A .....	10
Verifizieren und Testen .....	12
Aktualisieren von Gerät B .....	12
Wiederherstellen der Failover-Beziehung .....	12
<b>Asynchrone Aktualisierung zweier BeyondTrust-Geräte in einer Failover-Beziehung</b> ...	<b>14</b>
Sicherung und Synchronisierung .....	14
Aktualisieren von Gerät B .....	14
Verifizieren und Testen .....	16
Gerät B als primäres Gerät festlegen .....	16
Aktualisieren von Gerät A .....	17
Wiederherstellen der Failover-Beziehung .....	17
<b>Upgrade der BeyondTrust-Hardware vornehmen</b> .....	<b>19</b>
<b>Haftungsausschlüsse, Lizenzierungsbeschränkungen und Technischer Support</b> .....	<b>21</b>

# Upgrade der BeyondTrust Privileged Remote Access-Software vornehmen

Besuchen Sie das [Produktänderungsprotokoll](#), um Einzelheiten zu jeder Version der BeyondTrust Privileged Remote Access-Software einzusehen.

## Aktualisierungsvorbereitung

- Legen Sie vor der Aktualisierung stets eine Sicherungskopie Ihrer Einstellungen und Konfiguration über **/login > Verwaltung > Softwareverwaltung** an. Es wird empfohlen, ebenfalls eine Kopie Ihrer SSL-Zertifikate und Ihres privaten Schlüssels zu kopieren und diese lokal zu speichern, um im Falle eines fehlerhaften Upgrades Kontinuität zu gewährleisten.
- Um wichtige Softwareversionen zu erhalten werden Kunden mit einem aktuellen Wartungsvertrag in einen Rollout-Zeitplan eingetragen. Wenn die Aktualisierung verfügbar ist, wird BeyondTrust Sie per E-Mail darüber informieren und Sie dazu auffordern, die Aktualisierung vorzunehmen.
- Die Installation dauert in der Regel zwischen 15 Minuten und einer Stunde. Wenn Sie jedoch eine große Datenmenge auf Ihrem Gerät speichern (z. B. Aufnahmen von Sitzungen), kann die Installation deutlich länger dauern.
- BeyondTrust empfiehlt, Aktualisierungen innerhalb des angegebenen Wartungszeitraums vorzunehmen. Während der Aktualisierung ist Ihre BeyondTrust-Website kurzzeitig nicht verfügbar. Alle angemeldeten Benutzer werden abgemeldet und aktive Sitzungen werden beendet.
- BeyondTrust empfiehlt ebenfalls, vor der Bereitstellung in der Produktionsumgebung die Aktualisierung in einer kontrollierten Umgebung zu testen. Tests lassen sich am besten durchführen, wenn Sie zwei Geräte in einer Failover-Beziehung konfiguriert haben und asynchron aktualisieren. (Siehe „[Verifizieren und Testen](#)“ auf Seite 16).
- Sollten Sie während der Base-Aktualisierung auf Probleme stoßen, starten Sie das BeyondTrust-Gerät nicht neu. Wenden Sie sich bitte an den technischen BeyondTrust-Support.
- Wenn Sie zwei Geräte in einer Failover-Konfiguration eingerichtet haben, erwägen Sie, ob Sie synchron oder asynchron aktualisieren möchten.
  - Bei synchroner Aktualisierung wird das primäre Gerät zuerst aktualisiert und behält seine Rolle als primäres Gerät bei. Bei dieser Methode tritt eine Ausfallzeit auf. Sie empfiehlt sich für einfache Bereitstellungen und Szenarien, bei denen eine kurze Ausfallzeit während der Aktualisierung vertretbar ist.
  - Bei asynchroner Aktualisierung wird das Backup-Gerät zuerst aktualisiert und dieses übernimmt dann die Rolle des primären Gerätes. Mit dieser Methode wird die Ausfallzeit gering gehalten. Sie empfiehlt sich für größere Bereitstellungen und Szenarien, in denen eine unterbrechungsfreie Betriebszeit von großer Bedeutung ist. Eine zusätzliche Konfiguration kann vonnöten sein, da das Netzwerk möglicherweise modifiziert werden muss, damit das Backup-Gerät als Failover festgelegt werden kann.

## Client-Upgrades

Nur bestimmte Upgrades erfordern eine Aktualisierung der Client-Software. Die Base-Aktualisierungen und Lizenz-Add-ons erfordern keine Aktualisierung der Client-Software. Aktualisierungen der Website-Version erfordern jedoch Client-Aktualisierungen. Die meisten Client-Aktualisierungen erfolgen automatisch. Die für jeden Client-Typ zu erwartende Aktualisierungsprozedur ist jedoch unten aufgeführt.

- Nachdem das Seiten-Upgrade durchgeführt wurde, müssen Ihre installierten Zugriffskonsolen ebenfalls aktualisiert werden. Normalerweise geschieht dies automatisch, wenn der Benutzer das nächste Mal die Zugriffskonsole startet.

**WICHTIG!**

*Stellen Sie beim Upgraden auf ein neu kompiliertes Site-Softwarepaket sicher, dass alle Zertifikatspeicher ordnungsgemäß verwaltet und aktuell sind, bevor auf die neue BeyondTrust-Version upgegradet wird. Andernfalls kann der Großteil Ihrer bestehenden Jump Clients als offline erscheinen.*

- Zuvor mithilfe eines **MSI** auf gesperrten Computern bereitgestellte Zugriffskonsolen müssen nach dem Upgrade möglicherweise erneut bereitgestellt werden.
- Wenn die Funktion für die extrahierbare Zugriffskonsole oder den extrahierbaren Jump Client vom technischen BeyondTrust-Support für Ihre Website aktiviert wurde, können Sie ein MSI-Installationsprogramm herunterladen, um Zugriffskonsolen vor dem Upgrade des Geräts zu aktualisieren. Prüfen Sie dafür entweder manuell oder automatisch auf die neue Aktualisierung. Beachten Sie, dass die aktualisierten Clients erst online gehen, wenn das Gerät aktualisiert wurde. Es ist nicht notwendig, den ursprünglichen Client vor der Bereitstellung des neuen zu deinstallieren, da die neue Installation automatisch die alte ersetzen müsste. Als beste Vorgehensweise gilt jedoch, eine Kopie der alten MSI-Datei aufzubewahren, um die veralteten Installationen der Zugriffskonsolen zu entfernen, nachdem das Gerät aktualisiert wurde (sofern diese Entfernung notwendig ist). Die neue MSI-Datei ist dazu nicht in der Lage.
- Nach einem Upgrade aktualisieren sich bereitgestellte Jump Clients automatisch.
  - Wenn eine große Anzahl von Jump Clients gleichzeitig versucht, zu aktualisieren, können sie das Gerät überlasten und die Leistung sowohl auf Geräte- wie auch Netzwerkseite beeinträchtigen, abhängig von der verfügbaren Bandbreite und Hardware. Um die Menge der Bandbreite und Ressourcen einzuschränken, die von den Jump Client-Aktualisierungen verwendet werden soll, gehen Sie zu **/login > Jump > Jump Clients** und legen Sie die **Maximale Anzahl gleichzeitiger Jump Client-Aktualisierungen** fest.
  - Aktive und passive Jump Clients warten nach dem ersten Check-In bei dem Gerät nach der Aktualisierung des Geräts auf das Update. Diese Check-In-Ereignisse erfolgen in regelmäßigen Abständen ausgehend vom Jump Client-Host über den TCP-Port 443 zum Gerät. Aktive Jump Clients führen den Check-In sofort nach dem Abschluss eines Upgrades auf dem Gerät durch. Passive Jump Clients führen den Check-In beim Starten durch, nachdem eine Verbindung von der Zugriffskonsole hergestellt wurde, nachdem der Check-In-Befehl über das Infobereich-Symbol gewählt wurde und mindestens einmal alle 24 Stunden.
  - Falls ein Jump Client noch nicht aktualisiert wurde, wird er als **Upgrade ausstehend** markiert und eine Versions- und Revisionsnummer erscheinen im Detailfenster. Sie können einen veralteten Jump Client modifizieren, aber keinen Jump zu ihm durchführen. Der Versuch eines Jumps verschiebt diesen Jump Client jedoch an die Spitze der Upgrade-Warteschlange.
- Nach einer Aktualisierung werden bereitgestellte Jumpoints automatisch aktualisiert.



**Hinweis:** Haben Sie beim Upgrade auf eine neue Softwareversion etwas Geduld, bis alle Jump Clients wieder online kommen, bevor Sie mit weiteren Upgrade-Schritten fortfahren.

- BeyondTrust Verbindungs-Agenten werden nach der Aktualisierung der Site automatisch aktualisiert.
- BeyondTrust Integration-Clients werden nach Aktualisierung der Site nicht automatisch aktualisiert. Integration-Clients müssen manuell neu installiert werden. Installationsprogramme für den Integration-Client sind über die Seite **Downloads** auf [beyondtrustcorp.service-now.com/csm](https://beyondtrustcorp.service-now.com/csm) verfügbar.
- Bei Aktualisierungen ist es notwendig, jegliche für Jump Clients und Zugriffskonsolen zuvor erstellten Installationspakete erneut zu generieren. Die Clients selbst werden wie oben beschrieben aktualisiert. Ihre Installationsdateien werden jedoch ungültig, sobald das Gerät, das diese erzeugt hat, aktualisiert wird.

## Ein einziges BeyondTrust-Gerät mithilfe der automatischen Aktualisierung upgraden

In den meisten Fällen können BeyondTrust-Kunden Aktualisierungen ohne Hilfe des technischen BeyondTrust-Supports herunterladen und installieren. Um zu prüfen, ob eine Aktualisierung verfügbar ist, melden Sie sich über Ihr BeyondTrust-Gerät an (/appliance). Klicken Sie auf der Seite **Aktualisierungen** auf **Auf Aktualisierungen prüfen**.



Wenn eine Software-Aktualisierung verfügbar ist, erscheint diese unter **Verfügbare Aktualisierungen**. Wenn Sie **Diese Aktualisierung installieren** auswählen, lädt das Gerät die neue Version der BeyondTrust-Software herunter und installiert sie automatisch.

### **WICHTIG!**

*Stellen Sie beim Upgraden auf ein neu kompiliertes Site-Softwarepaket sicher, dass alle Zertifikatspeicher ordnungsgemäß verwaltet und aktuell sind, bevor auf die neue BeyondTrust-Version upgegradet wird. Andernfalls kann der Großteil Ihrer bestehenden Jump Clients als offline erscheinen.*

### Updates :: Check

When Bomgar releases updates to your software periodically, use this interface to view available updates and install select updates.

There are updates available to be installed

– Available Updates

**Base Software 3.3.2** Install This Update

---

**Bomgar-12.2.0**

*3.2.4 does not satisfy 12.2.0's requirements. Please install any other available package by clicking "Install this Update".*

- Primary Hostname: support.example.com
- Licenses: 15
- Expires: Never



**Hinweis:** Einige Pakete können erst nach der Installation anderer Pakete installiert werden. Installieren Sie das verfügbare Paket, um das davon abhängige Paket zu aktivieren.

Sollte die automatische Aktualisierung unerwartet fehlschlagen, lesen Sie bitte das Problemlösungs-FAQ zur Prüfung auf Aktualisierungen unter [beyondtrustcorp.service-now.com/csm/SSC/SolutionFAQ.aspx?id=1594](http://beyondtrustcorp.service-now.com/csm/SSC/SolutionFAQ.aspx?id=1594). Sollten Sie weiterhin nicht in der Lage sein, automatische Aktualisierungen durchzuführen, finden Sie weitere Informationen unter „Upgrade eines einzigen BeyondTrust-Geräts mit manuellen Aktualisierungen“ auf Seite 7.

## Upgrade eines einzigen BeyondTrust-Geräts mit manuellen Aktualisierungen

Wenn Sie automatische Aktualisierungen nicht verwenden können (wenn Ihr Gerät bspw. auf einem eingeschränkten Netzwerk betrieben wird), können Sie manuelle Aktualisierungen vornehmen.

Melden Sie sich in Ihrem BeyondTrust-Gerät an und gehen Sie zur Seite **Aktualisierungen**. Klicken Sie auf den Link **Geräte-Download-Schlüssel**, um einen einzigartigen Geräteschlüssel zu erzeugen. Senden Sie diesen Schlüssel dann von einem nicht beschränkten System an den BeyondTrust-Aktualisierungsserver auf [update.bomgar.com](http://update.bomgar.com). Laden Sie alle verfügbaren Aktualisierungen auf einen Wechseldatenträger herunter, und übertragen Sie diese Aktualisierungen auf ein System, mit dem Sie Ihr Gerät verwalten können.

Navigieren Sie unter **Aktualisierungen** zur Datei aus dem Abschnitt **Manuelle Installation** und klicken dann auf die Schaltfläche **Software aktualisieren**, um die Installation abzuschließen. Das Gerät installiert die neue Version der BeyondTrust-Software.



### WICHTIG!

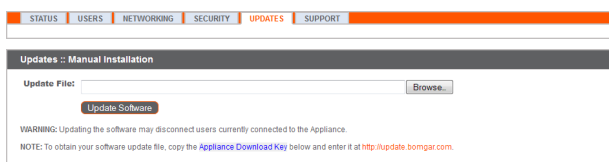
*Stellen Sie beim Upgraden auf ein neu kompiliertes Site-Softwarepaket sicher, dass alle Zertifikatspeicher ordnungsgemäß verwaltet und aktuell sind, bevor auf die neue BeyondTrust-Version upgegradet wird. Andernfalls kann der Großteil Ihrer bestehenden Jump Clients als offline erscheinen.*

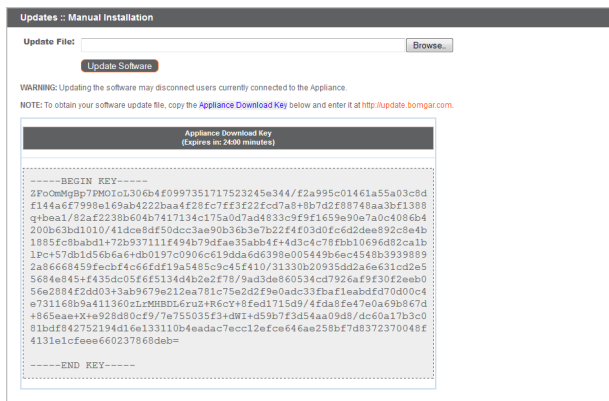


**Hinweis:** Bereiten Sie sich darauf vor, Softwareaktualisierungen direkt nach dem Download zu installieren. Wenn eine Aktualisierung heruntergeladen wurde, erscheint sie nicht länger in Ihrer Liste der verfügbaren Aktualisierungen. Sollten Sie eine Aktualisierung erneut herunterladen müssen, wenden Sie sich bitte an den technischen BeyondTrust-Support.



**Hinweis:** Wenn Sie eine Fehlermeldung erhalten, stellen Sie sicher, dass die auf der Seite **/appliance > Status > Basics** aufgeführte Zeit korrekt ist. Viele Funktionen des BeyondTrust-Geräts, darunter der Geräte-Download-Schlüssel, sind von einer korrekten Zeiteinstellung abhängig. Ist die Zeit nicht korrekt, überprüfen Sie die NTP-Einstellung auf der Seite **Netzwerk > IP-Konfiguration**.







## Zwei Geräte in einer Failover-Konfiguration upgraden

**WICHTIG!**

*BeyondTrust empfiehlt, Aktualisierungen zu Zeiten mit niedrigem Datenverkehr vorzunehmen.*

Es gibt zwei Methoden für Aktualisierungen in einer Failover-Umgebung: Synchrone Aktualisierung und asynchrone Aktualisierung.

### Synchrone Aktualisierung zweier BeyondTrust-Geräte in einer Failover-Beziehung

Bei synchroner Aktualisierung wird das primäre Gerät zuerst aktualisiert und behält seine Rolle als primäres Gerät bei. Bei dieser Methode tritt eine Ausfallzeit auf. Sie empfiehlt sich für einfache Bereitstellungen und Szenarien, bei denen eine kurze Ausfallzeit während der Aktualisierung vertretbar ist.

**Vorteil:** Kein Failover findet statt.

**Nachteil:** Längere Ausfallzeit am Produktionsort.

### Asynchrone Aktualisierung zweier BeyondTrust-Geräte in einer Failover-Beziehung

Bei asynchroner Aktualisierung wird das Backup-Gerät zuerst aktualisiert und dieses übernimmt dann die Rolle des primären Gerätes. Mit dieser Methode wird die Ausfallzeit gering gehalten. Sie empfiehlt sich für größere Bereitstellungen und Szenarien, in denen eine unterbrechungsfreie Betriebszeit von großer Bedeutung ist. Eine zusätzliche Konfiguration kann vonnöten sein, da das Netzwerk möglicherweise modifiziert werden muss, damit das Backup-Gerät als Failover festgelegt werden kann.

**Vorteil:** Minimale Produktionsausfallzeit.

**Nachteil:** Failover muss aktiviert sein.

## Erwägungen

1. Wählen Sie die Variante zur Failover-Aktualisierung, die am besten zu Ihrer Ausfallzeit und Ihren Kontinuitätsbedingungen passt.
2. Planen Sie zwei unterschiedliche Aktualisierungsfenster ein, in denen Sie die Aktualisierung vornehmen können.
3. Die Aktualisierung dauert auf beiden Geräten gleich lang.
4. Planen Sie eine Übergangszeit zwischen den beiden Aktualisierungsfenstern mit ein, die lang genug ist, um die neue Softwareversion in Ihrer Produktionsumgebung zu bestätigen, und kurz genug, um die Zeit, in der keine Failover-Konfiguration besteht, minimal zu halten.

## Synchrone Aktualisierung zweier BeyondTrust-Geräte in einer Failover-Beziehung

Bei synchroner Aktualisierung wird das primäre Gerät zuerst aktualisiert und behält seine Rolle als primäres Gerät bei. Bei dieser Methode tritt eine Ausfallzeit auf. Sie empfiehlt sich für einfache Bereitstellungen und Szenarien, bei denen eine kurze Ausfallzeit während der Aktualisierung vertretbar ist.

BeyondTrust empfiehlt, Aktualisierungen innerhalb des angegebenen Wartungszeitraums vorzunehmen. Während der Aktualisierung ist Ihre BeyondTrust-Website kurzzeitig nicht verfügbar. Alle angemeldeten Benutzer werden abgemeldet und aktive Sitzungen werden beendet. Sie müssen zwei unterschiedliche Aktualisierungsfenster einplanen, in denen Sie die Aktualisierung vornehmen. Die Installation dauert in der Regel zwischen 15 Minuten und einer Stunde. Wenn Sie jedoch eine große Datenmenge auf Ihrem Gerät speichern (z. B. Aufnahmen von Sitzungen), kann die Installation deutlich länger dauern. Planen Sie eine Übergangszeit zwischen den beiden Aktualisierungsfenstern mit ein, die lang genug ist, um die neue Softwareversion in Ihrer Produktionsumgebung zu bestätigen, und kurz genug, um die Zeit, in der keine Failover-Konfiguration besteht, minimal zu halten. BeyondTrust empfiehlt ebenfalls, vor der Bereitstellung in der Produktionsumgebung die Aktualisierung in einer kontrollierten Umgebung zu testen. Sollten Probleme bei der Basisaktualisierung auftreten, starten Sie das BeyondTrust-Gerät nicht neu. Wenden Sie sich bitte an den technischen BeyondTrust-Support.

In dieser Anleitung ist **Gerät A** das Hauptgerät (d.h. das Gerät, zu dem der primäre Hostname hin auflöst) und **Gerät B** das Backup-Gerät.

### Sicherung und Synchronisierung

Erstellen Sie vor der Aktualisierung eine Sicherungskopie Ihrer aktuellen BeyondTrust-Softwareeinstellungen. Gehen Sie auf **Gerät A** zu **/login > Verwaltung > Softwareverwaltung**.

	<b>STATUS</b>	<b>MY ACCOUNT</b>	<b>CONFIGURATION</b>	<b>JUMP™</b>	<b>ACCESS CONSOLE</b>	<b>USERS &amp; SECURITY</b>	<b>REPORTS</b>	<b>MANAGEMENT</b>
	SOFTWARE MANAGEMENT	SECURITY	SITE CONFIGURATION	EMAIL CONFIGURATION	OUTBOUND EVENTS	FAILOVER	API CONFIGURATION	SUPPORT

Klicken Sie auf die Schaltfläche **Sicherungskopie herunterladen** und speichern Sie die Sicherungsdatei an einem sicheren Ort.

Gehen Sie zu **/login > Verwaltung > Failover**, klicken Sie auf **Jetzt synchronisieren** und warten Sie bis zum Abschluss der Synchronisierung.

Sobald die Synchronisierung vorgenommen wurde, klicken Sie auf **Failover-Verbindungen trennen**.

### Aktualisieren von Gerät A

Aktualisieren Sie **Gerät A** entweder mittels der automatischen oder aber der manuellen Aktualisierungsmethode.

#### Automatisch

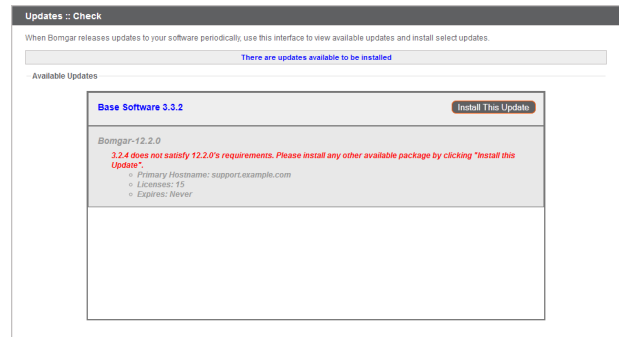
In den meisten Fällen können BeyondTrust-Kunden Aktualisierungen ohne Hilfe des technischen BeyondTrust-Supports herunterladen und installieren. Um zu prüfen, ob eine Aktualisierung verfügbar ist, gehen Sie zu **/appliance > Aktualisierungen**.



Klicken Sie auf **Auf Aktualisierungen prüfen**.



Wenn eine Software-Aktualisierung verfügbar ist, erscheint diese unter **Verfügbare Aktualisierungen**. Wenn Sie **Diese Aktualisierung installieren** auswählen, lädt das Gerät die neue Version der BeyondTrust-Software herunter und installiert sie automatisch.



**Hinweis:** „BeyondTrust“-Softwareaktualisierungen sind oft von einer oder mehreren „Basissoftware“-Aktualisierungen abhängig. Installieren Sie die verfügbaren Basissoftware-Aktualisierungen zur Aktivierung der davon abhängigen BeyondTrust-Aktualisierungen. Laden Sie dann eine Sicherungskopie herunter und installieren Sie die BeyondTrust-Softwareaktualisierungen umgehend vor jeglichen weiteren Schritten, wie etwa Failover oder der Installation von Aktualisierungen auf einem anderen Gerät.

Sollte die automatische Aktualisierung unerwartet fehlschlagen, lesen Sie bitte das Problemlösungs-FAQ zur Prüfung auf Aktualisierungen unter [beyondtrustcorp.service-now.com/csm/SSC/SolutionFAQ.aspx?id=1594](http://beyondtrustcorp.service-now.com/csm/SSC/SolutionFAQ.aspx?id=1594).

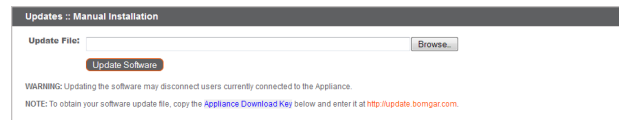
### Manuelle Installation

Wenn Sie automatische Aktualisierungen nicht verwenden können (wenn Ihr Gerät bspw. auf einem eingeschränkten Netzwerk betrieben wird), können Sie manuelle Aktualisierungen vornehmen.

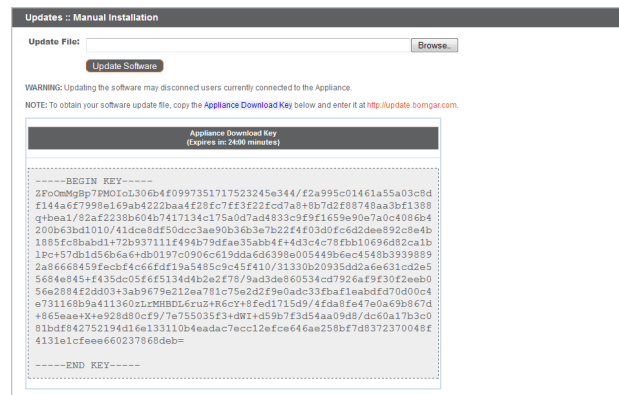
Gehen Sie zu **/appliance > Aktualisierungen**.



Klicken Sie auf den Link **Geräte-Download-Schlüssel**, um einen einzigartigen Geräteschlüssel zu erzeugen. Senden Sie diesen Schlüssel dann von einem nicht beschränkten System an den BeyondTrust-Aktualisierungsserver auf [update.bomgar.com](http://update.bomgar.com). Laden Sie alle verfügbaren Aktualisierungen auf einen Wechseldatenträger herunter, und übertragen Sie diese Aktualisierungen auf ein System, mit dem Sie Ihr Gerät verwalten können.



Navigieren Sie unter **Aktualisierungen** zur Datei aus dem Abschnitt **Manuelle Installation** und klicken dann auf die Schaltfläche **Software aktualisieren**, um die Installation abzuschließen. Das Gerät installiert die neue Version der BeyondTrust-Software.





**Hinweis:** Bereiten Sie sich darauf vor, Softwareaktualisierungen direkt nach dem Download zu installieren. Wenn eine Aktualisierung heruntergeladen wurde, erscheint sie nicht länger in Ihrer Liste der verfügbaren Aktualisierungen. Sollten Sie eine Aktualisierung erneut herunterladen müssen, wenden Sie sich bitte an den technischen BeyondTrust-Support.

## Verifizieren und Testen

Verifizieren Sie nach Abschluss des Aktualisierungsprozesses, dass die Aktualisierung erfolgreich abgeschlossen wurde und Ihre Software wie erwartet funktioniert. Nachdem das Seiten-Upgrade durchgeführt wurde, müssen Ihre installierten Zugriffskonsolen ebenfalls aktualisiert werden. Normalerweise geschieht dies automatisch, wenn der Benutzer das nächste Mal die Zugriffskonsole startet. Um den Software-Build zu überprüfen, den eine Konsole ausführt, melden Sie sich an der Konsole an und klicken Sie dann auf **Hilfe > Über**. Stellen Sie ebenfalls sicher, dass Sie über eine Sitzung eine Verbindung zu einem Remote-Computer herstellen können.



**Hinweis:** Zuvor mithilfe eines [MSI](#) auf gesperrten Computern bereitgestellte Zugriffskonsolen müssen nach dem Upgrade möglicherweise erneut bereitgestellt werden. Wenn die Funktion für die extrahierbare Zugriffskonsole oder den extrahierbaren Jump Client vom technischen BeyondTrust-Support für Ihre Website aktiviert wurde, können Sie ein MSI-Installationsprogramm herunterladen, um Zugriffskonsolen vor dem Upgrade des Geräts zu aktualisieren. Prüfen Sie dafür entweder manuell oder automatisch auf die neue Aktualisierung. Beachten Sie, dass die aktualisierten Clients erst online gehen, wenn das Gerät aktualisiert wurde. Es ist nicht notwendig, den ursprünglichen Client vor der Bereitstellung des neuen zu deinstallieren, da die neue Installation automatisch die alte ersetzen müsste. Als beste Vorgehensweise gilt jedoch, eine Kopie der alten MSI-Datei aufzubewahren, um die veralteten Installationen der Zugriffskonsolen zu entfernen, nachdem das Gerät aktualisiert wurde (sofern diese Entfernung notwendig ist). Die neue MSI-Datei ist dazu nicht in der Lage.

## Aktualisieren von Gerät B

Aktualisieren Sie **Gerät B** entweder mittels der automatischen oder aber der manuellen Aktualisierungsmethode, wie oben beschrieben. Verifizieren und testen Sie dann, ob die Aktualisierung erfolgreich abgeschlossen wurde.

## Wiederherstellen der Failover-Beziehung

Gehen Sie auf **Gerät A** zu **/login > Verwaltung > Failover**.

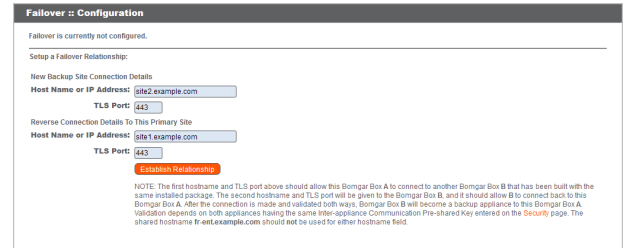
<b>STATUS</b>	<b>MY ACCOUNT</b>	<b>CONFIGURATION</b>	<b>JUMP™</b>	<b>ACCESS CONSOLE</b>	<b>USERS &amp; SECURITY</b>	<b>REPORTS</b>	<b>MANAGEMENT</b>
SOFTWARE MANAGEMENT	SECURITY	SITE CONFIGURATION	EMAIL CONFIGURATION	OUTBOUND EVENTS	FAILOVER	API CONFIGURATION	SUPPORT



**Hinweis:** Zur Konfiguration einer gültigen Verbindung müssen beide Geräte über identische Schlüssel zur Kommunikation zwischen Geräten verfügen. Gehen Sie zur Seite **/login > Verwaltung > Sicherheit** um den Schlüssel für jedes Gerät zu überprüfen.

Stellen Sie die Failover-Verbindung mit dem Backup-Gerät her, wobei **Gerät B** als Backup-Gerät und **Gerät A** als primäres Gerät beibehalten wird.

Das Herstellen der Verbindung zwischen den beiden Geräten geschieht auf der **Failover**-Seite des Geräts, das als primäres Gerät vorgesehen ist. Die hier eingegebenen Adressen stellen die Verbindung her und gestatten es beiden Geräten, sich jederzeit mit dem jeweils anderen zu verbinden. Die Felder unter **Verbindungsdetails zu neuem Backup-Standort** teilen dem primären Gerät mit, wie es sich mit dem Gerät verbinden kann, das zum Backup-Gerät wird. Die Felder unter **Umgekehrte Verbindungsdetails zu diesem primären Standort** werden dem Backup-Gerät übergeben und teilen ihm mit, wie es sich wieder mit diesem primären Gerät verbinden kann. Sie müssen einen gültigen Hostnamen bzw. eine gültige IP-Adresse und die TLS-Portnummer für diese Felder verwenden. Wenn alle Felder ausgefüllt sind, klicken Sie auf die Schaltfläche **Verbindung herstellen**, um die Verbindung herzustellen.




**Hinweis:** Wann immer dies möglich ist, empfiehlt BeyondTrust die Verwendung der einzigartigen IP-Adresse jedes Geräts bei der Konfiguration dieser Einstellungen.

Sobald die Beziehung hergestellt wurde, werden überflüssige Registerkarten von dem Backup-Standort entfernt. Die Einleitung der ersten Datensynchronisierung dauert etwa 60 Sekunden, aber Sie können auf die Schaltfläche **Jetzt synchronisieren** klicken, um die Synchronisierung zu erzwingen und die aktuellsten Informationen vom primären Gerät in den Speicher des Backup-Geräts zu übertragen. Die Synchronisierung selbst kann einige Sekunden bis hin zu mehreren Stunden dauern, abhängig von der zu synchronisierenden Datenmenge. Die Seite **Failover** listet den letzten Zeitpunkt der Datensynchronisierung auf, wenn die Synchronisierung abgeschlossen ist.

## Asynchrone Aktualisierung zweier BeyondTrust-Geräte in einer Failover-Beziehung

Bei asynchroner Aktualisierung wird das Backup-Gerät zuerst aktualisiert und dieses übernimmt dann die Rolle des primären Gerätes. Mit dieser Methode wird die Ausfallzeit gering gehalten. Sie empfiehlt sich für größere Bereitstellungen und Szenarien, in denen eine unterbrechungsfreie Betriebszeit von großer Bedeutung ist. Eine zusätzliche Konfiguration kann vonnöten sein, da das Netzwerk möglicherweise modifiziert werden muss, damit das Backup-Gerät als Failover festgelegt werden kann.

BeyondTrust empfiehlt, Aktualisierungen innerhalb des angegebenen Wartungszeitraums vorzunehmen. Während der Aktualisierung ist Ihre BeyondTrust-Website kurzzeitig nicht verfügbar. Alle angemeldeten Benutzer werden abgemeldet und aktive Sitzungen werden beendet. Sie müssen zwei unterschiedliche Aktualisierungsfenster einplanen, in denen Sie die Aktualisierung vornehmen. Die Installation dauert in der Regel zwischen 15 Minuten und einer Stunde. Wenn Sie jedoch eine große Datenmenge auf Ihrem Gerät speichern (z. B. Aufnahmen von Sitzungen), kann die Installation deutlich länger dauern. Planen Sie eine Übergangszeit zwischen den beiden Aktualisierungsfenstern mit ein, die lang genug ist, um die neue Softwareversion in Ihrer Produktionsumgebung zu bestätigen, und kurz genug, um die Zeit, in der keine Failover-Konfiguration besteht, minimal zu halten. BeyondTrust empfiehlt ebenfalls, vor der Bereitstellung in der Produktionsumgebung die Aktualisierung in einer kontrollierten Umgebung zu testen. Sollten Probleme bei der Basisaktualisierung auftreten, starten Sie das BeyondTrust-Gerät nicht neu. Wenden Sie sich bitte an den technischen BeyondTrust-Support.

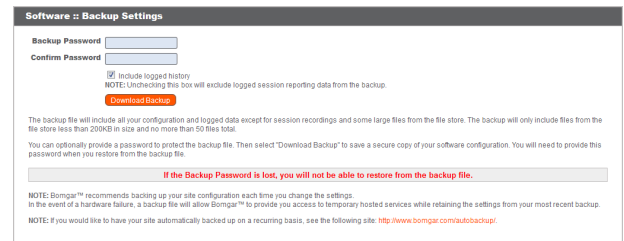
In dieser Anleitung ist **Gerät A** das Hauptgerät (d.h. das Gerät, zu dem der primäre Hostname hin auflöst) und **Gerät B** das Backup-Gerät.

### Sicherung und Synchronisierung

Erstellen Sie vor der Aktualisierung eine Sicherungskopie Ihrer aktuellen BeyondTrust-Softwareeinstellungen. Gehen Sie auf **Gerät A** zu **/login > Verwaltung > Softwareverwaltung**.

	<b>STATUS</b>	<b>MY ACCOUNT</b>	<b>CONFIGURATION</b>	<b>JUMP™</b>	<b>ACCESS CONSOLE</b>	<b>USERS &amp; SECURITY</b>	<b>REPORTS</b>	<b>MANAGEMENT</b>
	SOFTWARE MANAGEMENT	SECURITY	SITE CONFIGURATION	EMAIL CONFIGURATION	OUTBOUND EVENTS	FAILOVER	API CONFIGURATION	SUPPORT

Klicken Sie auf die Schaltfläche **Sicherungskopie herunterladen** und speichern Sie die Sicherungsdatei an einem sicheren Ort.



Gehen Sie zu **/login > Verwaltung > Failover**, klicken Sie auf **Jetzt synchronisieren** und warten Sie bis zum Abschluss der Synchronisierung.

Sobald die Synchronisierung vorgenommen wurde, klicken Sie auf **Failover-Verbindungen trennen**.



### Aktualisieren von Gerät B

Aktualisieren Sie **Gerät B** entweder mittels der automatischen oder aber der manuellen Aktualisierungsmethode.


#### Automatisch

In den meisten Fällen können BeyondTrust-Kunden Aktualisierungen ohne Hilfe des technischen BeyondTrust-Supports herunterladen und installieren. Um zu prüfen, ob eine Aktualisierung verfügbar ist, gehen Sie zu **/appliance > Aktualisierungen**.



Klicken Sie auf **Auf Aktualisierungen prüfen**.

Wenn eine Software-Aktualisierung verfügbar ist, erscheint diese unter **Verfügbare Aktualisierungen**. Wenn Sie **Diese Aktualisierung installieren** auswählen, lädt das Gerät die neue Version der BeyondTrust-Software herunter und installiert sie automatisch.



**Hinweis:** „BeyondTrust“-Softwareaktualisierungen sind oft von einer oder mehreren „Basissoftware“-Aktualisierungen abhängig. Installieren Sie die verfügbaren Basissoftware-Aktualisierungen zur Aktivierung der davon abhängigen BeyondTrust-Aktualisierungen. Laden Sie dann eine Sicherungskopie herunter und installieren Sie die BeyondTrust-Softwareaktualisierungen umgehend vor jeglichen weiteren Schritten, wie etwa Failover oder der Installation von Aktualisierungen auf einem anderen Gerät.

Sollte die automatische Aktualisierung unerwartet fehlschlagen, lesen Sie bitte das Problemlösungs-FAQ zur Prüfung auf Aktualisierungen unter [beyondtrustcorp.service-now.com/csm/SSC/SolutionFAQ.aspx?id=1594](http://beyondtrustcorp.service-now.com/csm/SSC/SolutionFAQ.aspx?id=1594).

### Manuelle Installation

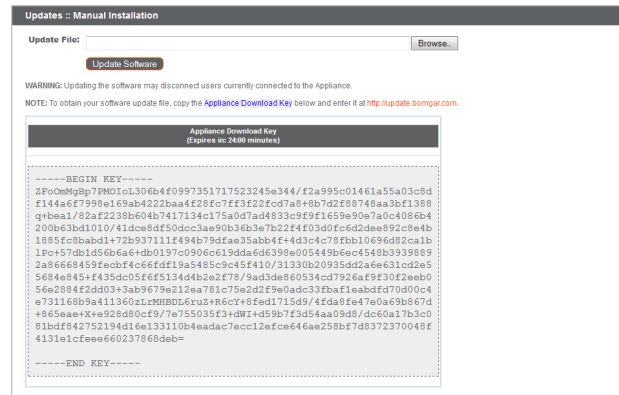
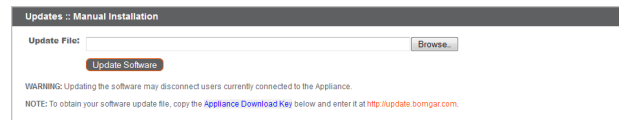
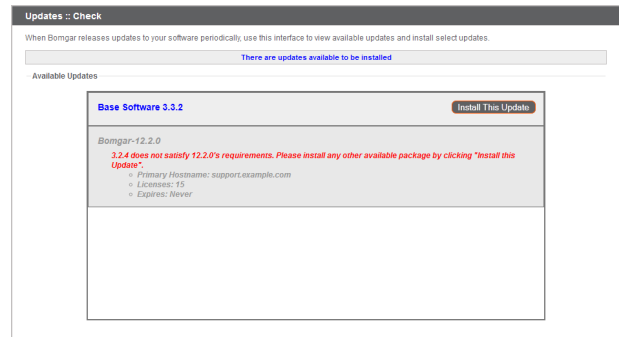
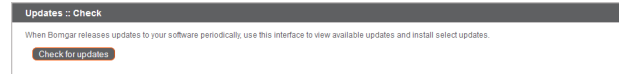
Wenn Sie automatische Aktualisierungen nicht verwenden können (wenn Ihr Gerät bspw. auf einem eingeschränkten Netzwerk betrieben wird), können Sie manuelle Aktualisierungen vornehmen.

Gehen Sie zu **/appliance > Aktualisierungen**.



Klicken Sie auf den Link **Geräte-Download-Schlüssel**, um einen einzigartigen Geräteschlüssel zu erzeugen. Senden Sie diesen Schlüssel dann von einem nicht beschränkten System an den BeyondTrust-Aktualisierungsserver auf [update.bomgar.com](http://update.bomgar.com). Laden Sie alle verfügbaren Aktualisierungen auf einen Wechseldatenträger herunter, und übertragen Sie diese Aktualisierungen auf ein System, mit dem Sie Ihr Gerät verwalten können.

Navigieren Sie unter **Aktualisierungen** zur Datei aus dem Abschnitt **Manuelle Installation** und klicken dann auf die Schaltfläche **Software aktualisieren**, um die Installation abzuschließen. Das Gerät installiert die neue Version der BeyondTrust-Software.





**Hinweis:** Bereiten Sie sich darauf vor, Softwareaktualisierungen direkt nach dem Download zu installieren. Wenn eine Aktualisierung heruntergeladen wurde, erscheint sie nicht länger in Ihrer Liste der verfügbaren Aktualisierungen. Sollten Sie eine Aktualisierung erneut herunterladen müssen, wenden Sie sich bitte an den technischen BeyondTrust-Support.

## Verifizieren und Testen

Verifizieren Sie nach Abschluss des Aktualisierungsprozesses, dass die Aktualisierung erfolgreich abgeschlossen wurde und Ihre Software wie erwartet funktioniert.

Bearbeiten Sie auf mindestens zwei lokalen Rechnern, welche auf **Gerät B** zugreifen können, die **Hosts-Datei**, damit der Hostname Ihrer Website zur IP-Adresse von **Gerät B** aufgelöst wird. Führen Sie auf einem Computer die Zugriffskonsole aus. Nachdem das Seiten-Upgrade durchgeführt wurde, müssen Ihre installierten Zugriffskonsolen ebenfalls aktualisiert werden. Normalerweise geschieht dies automatisch, wenn der Benutzer das nächste Mal die Zugriffskonsole startet. Um den Software-Build zu überprüfen, den eine Konsole ausführt, melden Sie sich an der Konsole an und klicken Sie dann auf **Hilfe > Über**. Stellen Sie ebenfalls sicher, dass Sie über eine Sitzung eine Verbindung zu einem Remote-Computer herstellen können.



**Hinweis:** Zuvor mithilfe eines **MSI** auf gesperrten Computern bereitgestellte Zugriffskonsolen müssen nach dem Upgrade möglicherweise erneut bereitgestellt werden. Wenn die Funktion für die extrahierbare Zugriffskonsole oder den extrahierbaren Jump Client vom technischen BeyondTrust-Support für Ihre Website aktiviert wurde, können Sie ein MSI-Installationsprogramm herunterladen, um Zugriffskonsolen vor dem Upgrade des Geräts zu aktualisieren. Prüfen Sie dafür entweder manuell oder automatisch auf die neue Aktualisierung. Beachten Sie, dass die aktualisierten Clients erst online gehen, wenn das Gerät aktualisiert wurde. Es ist nicht notwendig, den ursprünglichen Client vor der Bereitstellung des neuen zu deinstallieren, da die neue Installation automatisch die alte ersetzen müsste. Als beste Vorgehensweise gilt jedoch, eine Kopie der alten MSI-Datei aufzubewahren, um die veralteten Installationen der Zugriffskonsolen zu entfernen, nachdem das Gerät aktualisiert wurde (sofern diese Entfernung notwendig ist). Die neue MSI-Datei ist dazu nicht in der Lage.

## Gerät B als primäres Gerät festlegen

Legen Sie **Gerät B** als primäres Gerät fest und folgen Sie dabei den zuvor in Ihrem Failover-Plan definierten Schritten: Wechsel der freigegebenen IP-Adresse, DNS Swing oder NAT Swing.



**Hinweis:** Wenn Sie den BeyondTrust Integration-Client verwenden und ihn anhand der IP-Adresse anstatt des Hostnamen konfiguriert haben, vergewissern Sie sich, dass Sie Daten aus **Gerät B** extrahieren können, nachdem Sie **Gerät B** als primäres Gerät definiert haben.



**Hinweis:** Daten von Sitzungen, die auf einem der Geräte beendet werden, während die Failover-Verbindung nicht steht, werden automatisch synchronisiert, sobald die Failover-Verbindung wieder hergestellt wurde.



## Wechsel von freigegebener IP

Gehen Sie auf **Gerät A**, zu **/appliance > Netzwerk > IP-Konfiguration**.



Klicken Sie auf die freigegebene IP-Adresse, um sie zu bearbeiten, und deaktivieren Sie das Kontrollkästchen **Aktiviert**. Klicken Sie dann auf **Änderungen speichern**.

Gehen Sie dann direkt zu **/appliance > Netzwerk > IP-Konfiguration** auf **Gerät B**. Es kann hilfreich sein, diese Seite bereits in einem separaten Browser-Tab geöffnet zu haben.

Klicken Sie auf die freigegebene IP-Adresse, um sie zu bearbeiten, und aktivieren Sie das Kontrollkästchen **Aktiviert**. Klicken Sie dann auf **Änderungen speichern**.

Sobald der Wechsel vollzogen wurde, können Sie die reguläre Aktivität fortsetzen. Alle Anfragen an Ihre Website werden von **Gerät B** bearbeitet.

## DNS Swing

Greifen Sie auf den DNS-Controller zu und machen Sie den DNS-Eintrag für Ihre BeyondTrust-Website ausfindig. Bearbeiten Sie den Eintrag so, dass er auf die IP-Adresse für **Gerät B** zeigt. Sobald der DNS-Eintrag propagiert wurde, können Sie die reguläre Aktivität fortsetzen. Alle Anfragen an Ihre Website werden von **Gerät B** bearbeitet.

## NAT Swing

Greifen Sie auf den NAT-Controller zu und machen Sie den NAT-Eintrag für Ihre BeyondTrust-Website ausfindig. Bearbeiten Sie den Eintrag so, dass er auf die IP-Adresse für **Gerät B** zeigt. Sobald die Änderung vorgenommen wurde, können Sie die reguläre Aktivität fortsetzen. Alle Anfragen an Ihre Website werden von **Gerät B** bearbeitet.

## Aktualisieren von Gerät A



**Hinweis:** Jede Kundenumgebung ist anders, und obwohl BeyondTrust jede Funktion testet, können wir nicht jedes mögliche Kundenszenario testen. Bitte vergewissern Sie sich, dass die BeyondTrust-Software in Ihrer Umgebung funktioniert, bevor Sie Gerät A aktualisieren.

Aktualisieren Sie **Gerät A** entweder mittels der automatischen oder aber der manuellen Aktualisierungsmethode, wie oben beschrieben. Verifizieren und testen Sie dann, ob die Aktualisierung erfolgreich abgeschlossen wurde.

## Wiederherstellen der Failover-Beziehung

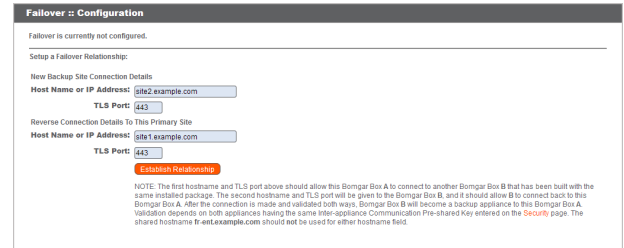
Gehen Sie auf **Gerät B** zu **/login > Verwaltung > Failover**.



**Hinweis:** Zur Konfiguration einer gültigen Verbindung müssen beide Geräte über identische Schlüssel zur Kommunikation zwischen Geräten verfügen. Gehen Sie zur Seite **/login > Verwaltung > Sicherheit** um den Schlüssel für jedes Gerät zu überprüfen.

Stellen Sie die Failover-Verbindung mit dem Backup-Gerät her, wobei **Gerät A** als Backup-Gerät und **Gerät B** als primäres Gerät festgelegt wird.

Das Herstellen der Verbindung zwischen den beiden Geräten geschieht auf der **Failover**-Seite des Geräts, das als primäres Gerät vorgesehen ist. Die hier eingegebenen Adressen stellen die Verbindung her und gestatten es beiden Geräten, sich jederzeit mit dem jeweils anderen zu verbinden. Die Felder unter **Verbindungsdetails zu neuem Backup-Standort** teilen dem primären Gerät mit, wie es sich mit dem Gerät verbinden kann, das zum Backup-Gerät wird. Die Felder unter **Umgekehrte Verbindungsdetails zu diesem primären Standort** werden dem Backup-Gerät übergeben und teilen ihm mit, wie es sich wieder mit diesem primären Gerät verbinden kann. Sie müssen einen gültigen Hostnamen bzw. eine gültige IP-Adresse und die TLS-Portnummer für diese Felder verwenden. Wenn alle Felder ausgefüllt sind, klicken Sie auf die Schaltfläche **Verbindung herstellen**, um die Verbindung herzustellen.



**Failover :: Configuration**

Failover is currently not configured.

Setup a Failover Relationship:

New Backup Site Connection Details

Host Name or IP Address:

TLS Port:

Reverse Connection Details To This Primary Site

Host Name or IP Address:

TLS Port:

**Finish**

NOTE: The first hostname and TLS port above should allow this Bomgar Box A to connect to another Bomgar Box B that has been built with the same installed package. The second hostname and TLS port will be given to the Bomgar Box B, and it should allow B to connect back to this Bomgar Box A. After the connection is made and validated both ways, Bomgar Box B will become a backup appliance to this Bomgar Box A. Validation depends on both appliances having the same file-appliance Communication Pre-shared key entered on the Security page. The shared hostname fr-ent.example.com should not be used for either hostname field.



**Hinweis:** Wann immer dies möglich ist, empfiehlt BeyondTrust die Verwendung der einzigartigen IP-Adresse jedes Geräts bei der Konfiguration dieser Einstellungen.

Sobald die Beziehung hergestellt wurde, werden überflüssige Registerkarten von dem Backup-Standort entfernt. Die Einleitung der ersten Datensynchronisierung dauert etwa 60 Sekunden, aber Sie können auf die Schaltfläche **Jetzt synchronisieren** klicken, um die Synchronisierung zu erzwingen und die aktuellsten Informationen vom primären Gerät in den Speicher des Backup-Geräts zu übertragen. Die Synchronisierung selbst kann einige Sekunden bis hin zu mehreren Stunden dauern, abhängig von der zu synchronisierenden Datenmenge. Die Seite **Failover** listet den letzten Zeitpunkt der Datensynchronisierung auf, wenn die Synchronisierung abgeschlossen ist.

## Upgrade der BeyondTrust-Hardware vornehmen

Wenn Sie ein Upgrade Ihres BeyondTrust-Geräts von einem physischen Gerät auf ein anderes durchführen oder zwischen einem physischen und einem virtuellen Gerät, müssen Sie sowohl das neue Gerät installieren wie auch Daten vom alten Gerät übertragen.

1. Installieren Sie das neue Gerät entsprechend des geeigneten Einrichtungshandbuchs.
  - Installation des virtuellen BeyondTrust-Geräts: [www.beyondtrust.com/docs/privileged-remote-access/getting-started/deployment/virtual/index.htm](http://www.beyondtrust.com/docs/privileged-remote-access/getting-started/deployment/virtual/index.htm)
  - Hardware-Installation des BeyondTrust-Geräts: [www.beyondtrust.com/docs/privileged-remote-access/getting-started/deployment/hardware/index.htm](http://www.beyondtrust.com/docs/privileged-remote-access/getting-started/deployment/hardware/index.htm)
2. Sichern Sie die Softwareeinstellungen Ihres aktuellen Geräts.
  - a. Gehen Sie auf Ihrem aktuellen Gerät zu **/login > Verwaltung > Softwareverwaltung**.
  - b. Klicken Sie im Abschnitt **Software :: Sicherungseinstellungen** auf die Schaltfläche **Sicherung herunterladen**.
  - c. Speichern Sie die Sicherungsdatei an einem sicheren Ort.
3. Importieren Sie Ihre bestehende SSL-Zertifikatskette in das neue Gerät.
  - a. Gehen Sie auf Ihrem aktuellen Gerät zu **/appliance > Sicherheit > Zertifikate**.
  - b. Markieren Sie im Abschnitt **Sicherheit :: Zertifikate** das Kästchen neben dem Zertifikat, das der aktiven IP-Adresse zugewiesen ist. Wählen Sie dann aus dem Dropdown-Menü überhalb dieses Abschnitts **Exportieren**.



**Hinweis:** Das Exportieren von Zertifikaten entfernt sie nicht vom Gerät.

- c. Wählen Sie auf der Seite **Sicherheit :: Zertifikate :: Exportieren** die Optionen zum Anfügen des Zertifikats, des privaten Schlüssels und der Zertifikatskette aus. Es wird empfohlen, dass Sie für den privaten Schlüssel eine Passphrase festlegen.
  - d. Gehen Sie auf Ihrem neuen Gerät zu **/appliance > Sicherheit > Zertifikate**.
  - e. Klicken Sie im Abschnitt **Sicherheit :: Zertifikat-Installation** auf die Schaltfläche **Importieren**.
  - f. Navigieren Sie zur Zertifikatsdatei, die Sie zuvor exportiert haben und klicken Sie auf **Hochladen**.
4. Weisen Sie dem Zertifikat eine IP-Adresse zu.
    - a. Gehen Sie auf Ihrem neuen Gerät zu **/appliance > Sicherheit > Zertifikate**.
    - b. Machen Sie im Abschnitt **Sicherheit :: Zertifikate** den Eintrag für Ihr SSL-Zertifikat ausfindig. Es enthält in der Regel ein Feld **Ausgestellt an**, das den vollständig qualifizierten Domännennamen Ihres Geräts enthält (z.B. `access.example.com`).
    - c. Vergewissern Sie sich, dass für das neue Zertifikat keine Warnungen aufgeführt werden. Sehen Sie im Falle von Warnungen unter FAQ 755 im BeyondTrust Technical Support Self Service Center nach, um Details zur Beseitigung der Warnung zu erhalten: <https://beyondtrustcorp.service-now.com/csm/SSC/SolutionFAQ.aspx?id=755>.
    - d. Klicken Sie nach Beseitigung aller Warnungen auf den Link **IP zuweisen** in der Zertifikatsreihe. Überprüfen Sie unten auf der Seite die IP-Adresse, die Sie zuweisen möchten, und klicken Sie dann auf die Schaltfläche **Konfiguration speichern**.
  5. Installieren Sie das neue Softwarepaket.
    - a. Gehen Sie auf Ihrem neuen Gerät zu **/appliance > Aktualisierungen**.
    - b. Klicken Sie entweder auf **Auf Aktualisierungen prüfen** oder verwenden Sie den **Geräte-Download-Schlüssel** gemäß der Bildschirmanweisungen.

- c. Klicken Sie auf **Diese Aktualisierung installieren**. Eine Endbenutzer-Lizenzvereinbarung muss vor der Installation unterzeichnet werden.
6. Importieren Sie Ihre Software-Konfigurationseinstellungen aus dem alten Gerät.
    - a. Melden Sie sich in der /login-Schnittstelle Ihres neuen Geräts an. Die Anmeldedaten für die erste Anmeldung lauten **admin** und **password**.
    - b. Gehen Sie zu **/login > Verwaltung > Softwareverwaltung**.
    - c. Navigieren Sie im Abschnitt **Software :: Einstellungen wiederherstellen** zur zuvor heruntergeladenen Sicherungsdatei und klicken Sie dann auf **Sicherung hochladen**, um die Sicherung auf dem neuen Gerät wiederherzustellen.

Jetzt können Sie Ihren DNS-Server aktualisieren, um Datenverkehr auf die IP-Adresse des neuen Geräts zu leiten und können mit dem Testen von Zugriffssitzungen auf Ihrem neuen Gerät beginnen. Sobald Sie sich vergewissert haben, dass dieses korrekt funktioniert, können Sie das alte Gerät zurücksenden (falls es sich um ein physisches Gerät handelt) oder es löschen (falls es sich um ein virtuelles Gerät handelt). Um ein physisches Gerät zurückzusenden, gehen Sie wie folgt vor:

1. Melden Sie sich in der **/appliance**-Webschnittstelle des alten Geräts an.
2. Navigieren Sie zur Seite **Status > Einfach** und klicken Sie auf **Gerät auf Originalstandards zurücksetzen**.
3. Warten Sie, bis die Zurücksetzung abgeschlossen ist, und klicken Sie dann auf **Dieses Gerät herunterfahren**.
4. Bereiten Sie das Gerät auf den Versand vor.
5. Kleben Sie das BeyondTrust-Retoureticket auf dem Paket auf und wenden Sie sich zur Abholung an Ihren Lieferdienst. Sollten Sie nicht über ein Lieferetikett verfügen, wenden Sie sich an den technischen BeyondTrust-Support.

# Haftungsausschlüsse, Lizenzierungsbeschränkungen und Technischer Support

## Haftungsausschlüsse

Dieses Dokument dient ausschließlich Informationszwecken. BeyondTrust Corporation kann die hierin enthaltenen Inhalte ohne Ankündigung ändern. Es kann weder die Fehlerfreiheit dieses Dokuments garantiert werden, noch unterliegt das Dokument irgendwelchen Garantien oder Gewährleistungen, weder in mündlicher Form noch in konkludenter rechtlicher Form, einschließlich konkludenten Garantien und Gewährleistungen der Marktgängigkeit oder Eignung für einen bestimmten Zweck. BeyondTrust Corporation lehnt jegliche Haftbarkeit in Bezug auf dieses Dokument ab, und es entstehen durch dieses Dokument keine direkten oder indirekten vertraglichen Verpflichtungen. Die hierin beschriebenen Technologien, Funktionen, Dienste und Prozesse können ohne Ankündigung geändert werden.

©2003-2019 BeyondTrust Corporation. Alle Rechte vorbehalten. BEYONDTRUST, sein Logo und JUMP sind Marken von BeyondTrust Corporation. Andere Marken sind Eigentum ihrer jeweiligen Inhaber.

## Lizenzierungsbeschränkungen

Mit einer BeyondTrust Privileged Remote Access-Lizenz kann jeweils ein Support-Techniker Probleme auf einer unbegrenzten Anzahl an Remote-Computern beheben. Dabei müssen die Benutzer nicht unbedingt am Computer sein. Obgleich mehrere Konten für die gleiche Lizenz eingerichtet sein können, sind zwei oder mehr Lizenzen (eine pro aktivem Support-Techniker) erforderlich, damit mehrere Support-Techniker gleichzeitig den Fehler beheben können.

Eine BeyondTrust Privileged Remote Access-Lizenz aktiviert den Zugriff auf ein Endpunkt-System. Obwohl diese Lizenz von einem System auf ein anderes übertragen werden kann, wenn der Zugriff auf das erste System nicht länger erforderlich ist, sind zwei oder mehr Lizenzen (eine pro Endpunkt) erforderlich, um den Zugriff auf mehrere Endpunkte gleichzeitig zu aktivieren.

## Technischer Support

Wir bei BeyondTrust fühlen uns verpflichtet, Service von höchster Qualität zu bieten, indem wir gewährleisten, dass unsere Kunden alles haben, was sie für einen Betrieb bei maximaler Produktivität benötigen. Sollten Sie Hilfe benötigen, wenden Sie sich an den technischen BeyondTrust-Support unter [beyondtrust.com/docs/index.htm#support](https://www.beyondtrust.com/docs/index.htm#support).

Technischen Support können Sie mit einem jährlichen Abonnement unseres Wartungsplans in Anspruch nehmen.