



BeyondTrust

Remote Support Aktualisierungshandbuch für das Gerät

Table of Contents

Upgrade der BeyondTrust -Software	3
Sicherung des Vault-Schlüssels	4
Upgraden eines einzelnen Secure Remote Access Appliance mit automatischen Aktualisierungen	7
Upgrade eines einzelnen Secure Remote Access Appliance mit manuellen Aktualisierungen	8
Zwei Secure Remote Access Appliances in einer Failover-Konfiguration upgraden	9
Synchrone Aktualisierung zweier Geräte in einer Failover-Beziehung	10
Sicherung und Synchronisierung	10
Aktualisieren von Gerät A	10
Verifizieren und testen	12
Aktualisieren von Gerät B	12
Wiederherstellen der Failover-Beziehung	12
Asynchrone Aktualisierung zweier Geräte in einer Failover-Beziehung	14
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
Upgrade mehrerer Secure Remote Access Appliance in einem Atlas-Cluster	19
Mit konfiguriertem Failover	19
Ohne konfiguriertes Failover	21
Upgrade von BeyondTrust-Hardware	23
Haftungsausschlüsse, Lizenzierungsbeschränkungen und Technischer Support	25

Upgrade der BeyondTrust -Software

Genauere Informationen über jede Version von BeyondTrust Remote-Support-Software finden Sie im [Produktänderungsprotokoll](#).



Hinweis: Wenn Ihre BeyondTrust-Software schon seit längerer Zeit nicht mehr aktualisiert wurde und über mehrere Versionen hinweg veraltet ist, müssen Sie wahrscheinlich mehrere Versionen als Zwischenschritte installieren, bevor Sie die neueste Version installieren können. Bitte beachten Sie den dritten Punkt unten für Einzelheiten.

Aktualisierungsvorbereitung

- Legen Sie vor der Aktualisierung stets eine Sicherungskopie Ihrer Einstellungen und Konfiguration über **/login > Verwaltung > Softwareverwaltung** an.
- Es wird empfohlen, eine Kopie Ihrer SSL-Zertifikate und Ihres privaten Schlüssels zu kopieren und diese lokal zu speichern, um im Falle eines Fehlers während des 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, informiert Sie BeyondTrust per E-Mail darüber und fordert Sie dazu auf, die Aktualisierung vorzunehmen.
- Ist Ihr Gerät mehrere Monate oder Jahre veraltet, können Sie es wahrscheinlich nicht direkt in einer einzigen Installation auf die neueste BeyondTrust-Version aktualisieren. In diesem Fall werden einige Upgrade-Pakete in der Aktualisierungsliste möglicherweise nicht verfügbar sein und erfordern, dass zunächst ein anderes Paket installiert wird. Wählen Sie **Diese Aktualisierung installieren** bei verfügbaren Paketen aus, um die von ihnen abhängigen Pakete zu aktivieren.
 - Kontaktieren Sie den BeyondTrust Technical Support unter www.beyondtrust.com/support mit einer Bildschirmaufnahme der Seite **/appliance > Status > Einfach**, damit bestimmt werden kann, welche Aktualisierungen Sie für Ihr Gerät benötigen.
 - In Fällen, in denen BeyondTrust-Aktualisierungen als Zwischenschritte vor der neuesten Version installiert werden müssen, schlägt die automatische Aktualisierung von BeyondTrust-Software-Clients in der Regel fehl, es sei denn, sie erhalten ausreichend Zeit zum Abruf der Zwischenschritt-Pakete. Daher empfiehlt Ihnen BeyondTrust, nach jeder Installation eines Pakets mit dem Präfix *BeyondTrust* mindestens 24 Stunden zu warten.
 - Basisaktualisierungen erfordern keine Wartezeit, sind jedoch meist eine Voraussetzung für *BeyondTrust*-Pakete. Daher werden Basisaktualisierungen normalerweise direkt vor *BeyondTrust*-Paketen installiert.
 - Falls es nicht möglich ist, 24 Stunden bis zum Abschluss der automatischen Client-Upgrades zu warten, besteht die Alternative zur automatischen Aktualisierung darin, zunächst alle bestehende Client-Software zu deinstallieren, darunter die Konsole d. Support-Technikers, Jump-Clients, Jumpoints, Support Button, Verbindungsagenten usw. Installieren Sie jedes *BeyondTrust*- und Basis-Upgrade in der richtigen Reihenfolge, bis Sie die aktuellste Version erreicht haben. Installieren Sie dann manuell die gesamte Client-Software neu.
- 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.
- Wir empfehlen, Aktualisierungen innerhalb des angegebenen Wartungszeitraums vorzunehmen. Während des Upgrades ist Ihre BeyondTrust-Website kurzzeitig nicht erreichbar. Alle angemeldeten Benutzer werden abgemeldet und aktive Sitzungen werden beendet.
- Darüber hinaus empfehlen wir, 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.



Weitere Informationen finden Sie unter „[Verifizieren und testen](#)“ auf Seite 16.

- Sollten Sie während der Basis-Aktualisierung auf Probleme stoßen, starten Sie das Secure Remote Access Appliance nicht neu. Wenden Sie sich bitte an BeyondTrust Technical 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; wir empfehlen synchrone Aktualisierungen für einfache Bereitstellungen und Szenarien, bei denen eine kurze Ausfallzeit während der Aktualisierung vertretbar ist.
 - Bei asynchroner Aktualisierung wird das Sicherungsgerät zuerst aktualisiert und übernimmt dann die Rolle des primären Gerätes. Mit dieser Methode wird die Ausfallzeit gering gehalten; wir empfehlen asynchrone Aktualisierungen für größere Bereitstellungen und Szenarien, in denen eine unterbrechungsfreie Betriebszeit von großer Bedeutung ist. Womöglich ist eine weitere Konfiguration erforderlich, da das Netzwerk möglicherweise modifiziert werden muss, damit das Sicherungsgerät als Failover festgelegt werden kann.

Sicherung des Vault-Schlüssels

Der Vault-Verschlüsselungsschlüssel wird zur Ver- und Entschlüsselung aller Vault-Anmeldedaten verwendet, die auf Ihrem Secure Remote Access Appliance gespeichert sind. Falls Sie Konfigurationsdaten von einem Sicherungs- auf ein neues Gerät übertragen müssen, müssen Sie auch den Vault-Verschlüsselungsschlüssel von einem Backup wiederherstellen, um die verschlüsselten Vault-Anmeldedaten der Konfigurationssicherungskopie nutzen zu können.

Sicherungskennwort

Um Ihre Softwaresicherungsdatei mit einem Kennwort zu schützen, erstellen Sie ein Kennwort. Wenn Sie sich entscheiden, ein Kennwort festzulegen, können Sie nicht wieder auf die Sicherungskopie zurücksetzen, ohne das Kennwort anzugeben.

Vault-Verschlüsselungsschlüssel herunterladen

Klicken Sie auf die Schaltfläche **Vault-Verschlüsselungsschlüssel herunterladen**, um den Vault-Verschlüsselungsschlüssel zur späteren Verwendung herunterzuladen.



Hinweis: Der Vault-Verschlüsselungsschlüssel muss kennwortgeschützt sein.

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.

**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.

- Nachdem die Website aktualisiert wurde, müssen Ihre installierten Konsole d. Support-Technikers ebenfalls aktualisiert werden. Normalerweise geschieht dies automatisch, wenn der Support-Techniker das nächste Mal die Konsole d. Support-Technikers startet.
 - Konsolen der Support-Techniker, die zuvor auf zugriffsgesicherten Computern mit MSI bereitgestellt wurden, müssen, sobald die Aktualisierung beendet wurde, wieder bereitgestellt werden.



Weitere Informationen finden Sie in [Mein Konto: Kennwort und Benutzername ändern, die Konsole des Support-Technikers und andere Software herunterladen](#) unter <https://www.beyondtrust.com/docs/remote-support/getting-started/admin/my-account.htm>.

- Wenn die Funktion für die extrahierbare Konsole d. Support-Technikers oder den extrahierbaren Jump-Client vom BeyondTrust Technical Support für Ihre Website aktiviert wurde, können Sie ein MSI-Installationsprogramm herunterladen, um Konsole d. Support-Technikers oder Jump-Clients vor dem Upgrade des Geräts zu aktualisieren. Prüfen Sie dafür entweder manuell oder automatisch auf die neue Aktualisierung. Klicken Sie auf den Link **Installationsprogramme für die Konsole des Support-Technikers** oder **Installationsprogramme für Jump-Clients**, um die MSI-Datei für die Weiterverteilung herunterzuladen. 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 Netzwerkebene 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 einen niedrigeren Wert für **Maximale Anzahl gleichzeitiger Jump-Client-Aktualisierungen** und/oder **Maximale Bandbreite gleichzeitiger Jump-Client-Aktualisierungen** fest.
 - Nach der Aktualisierung des Geräts werden aktive und passive Jump-Clients beim ersten Check-in in die Aktualisierungswarteschlange gestellt. 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 Konsole d. Support-Technikers 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.
- Wenn Ihr Secure Remote Access Appliance veraltet ist, müssen möglicherweise mehrere Versionen installiert werden, um die aktuelle Version zu erreichen. In diesem Fall empfiehlt BeyondTrust, zwischen Aktualisierungen mindestens 24 Stunden zu

warten, damit Jump-Clients Gelegenheit zum Upgrade haben. Passive Jump-Clients können abhängig davon, wie lange ihre Host-Systeme offline verbleiben, noch länger brauchen.



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.

- Sobald ein Jump-Client in der Konsole d. Support-Technikers oder unter **/login > Status > Informationen** als online angezeigt wird, wurde er erfolgreich aktualisiert. Sie können die Aktualisierung aller Jump-Clients bestätigen, wenn Sie sich in der Konsole d. Support-Technikers als Administrator mit Berechtigung zur Modifizierung aller Jump-Clients im System anmelden. Die Liste der Jump-Clients exportieren. Sortieren Sie im erscheinenden Bericht die Jump-Clients nach **Statusdetails** und vergewissern Sie sich, dass alle aufgeführten Daten aktueller sind als das Datum des letzten Upgrades des Secure Remote Access Appliance.
- Wenn zu viele Versionen hintereinander installiert werden, ohne Jump-Clients die Möglichkeit zum Upgrade zu geben, müssen diese möglicherweise manuell erneut bereitgestellt werden.
- Nach einer Aktualisierung werden Support Button automatisch aktualisiert, sobald sie nach einer Aktualisierung das erste Mal verwendet werden.
- Nach einer Aktualisierung werden bereitgestellte Jumpoints automatisch aktualisiert.
- BeyondTrust Verbindungsagenten werden nach dem Upgrade der Website automatisch aktualisiert.
- BeyondTrust Integrationsclients werden nach dem Upgrade der Website nicht automatisch aktualisiert. Integration-Clients müssen manuell neu installiert werden.



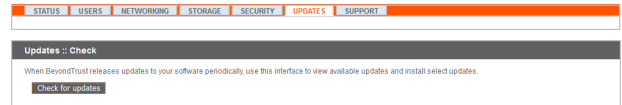
Hinweis: Installationsprogramme für den Integration-Client sind über die Seite **Downloads** von www.beyondtrust.com/support verfügbar.

- Bei Upgrades ist es notwendig, jegliche für Support Button, Jump-Clients und Konsole d. Support-Technikers 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.

Upgraden eines einzelnen Secure Remote Access Appliance mit automatischen Aktualisierungen

In den meisten Fällen können BeyondTrust-Kunden Aktualisierungen ohne Hilfe des BeyondTrust Technical Support herunterladen und installieren. Um zu prüfen, ob eine Aktualisierung verfügbar ist, melden Sie sich über Ihr Secure Remote Access Appliance 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.



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, rufen Sie bitte die Wissensdatenbank auf unter www.beyondtrust.com/support.

Sollten Sie weiterhin nicht in der Lage sein, automatische Aktualisierungen durchzuführen, finden Sie weitere Informationen unter „Upgrade eines einzelnen Secure Remote Access Appliance mit manuellen Aktualisierungen“ auf Seite 8.

Upgrade eines einzelnen Secure Remote Access Appliance 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 Secure Remote Access Appliance an und gehen Sie zur Seite Aktualisierungen. Beginnend mit Base 3.3.2 können Sie auf den Link Geräte-Download-Schlüssel klicken, um einen eindeutigen Geräte-Schlüssel zu generieren. Vor Base 3.3.2 müssen Sie den BeyondTrust Technical Support kontaktieren, um diesen Schlüssel anzufordern. Senden Sie diesen Schlüssel dann von einem nicht beschränkten System an den Aktualisierungsserver von BeyondTrust unter https://btupdate.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 BeyondTrust Technical Support unter www.beyondtrust.com/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 Secure Remote Access Appliance, 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.

Screenshot of the BeyondTrust appliance interface showing the 'Updates' section. It includes a navigation bar with 'STATUS', 'USERS', 'NETWORKING', 'STORAGE', 'SECURITY', 'UPDATES', and 'SUPPORT'. The 'Updates' section has a sub-header 'Manual Installation' and contains a file selection area with a 'Browse...' button and an 'Update Software' button. Below this, there are warning messages and a section for the 'Appliance Download Key' with a large text area containing a long alphanumeric key.

Zwei Secure Remote Access Appliances in einer Failover-Konfiguration upgraden

**WICHTIG!**

BeyondTrust empfiehlt, Aktualisierungen zu Zeiten mit geringem Datenverkehr vorzunehmen.

Es gibt zwei Methoden für Aktualisierungen in einer Failover-Umgebung: Synchroner Aktualisierung und asynchroner Aktualisierung.

Synchrone Aktualisierung zweier 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; wir empfehlen synchrone Aktualisierungen 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 Geräte in einer Failover-Beziehung

Bei asynchroner Aktualisierung wird das Sicherungsgerät zuerst aktualisiert und übernimmt dann die Rolle des primären Gerätes. Mit dieser Methode wird die Ausfallzeit gering gehalten; wir empfehlen asynchrone Aktualisierungen für größere Bereitstellungen und Szenarien, in denen eine unterbrechungsfreie Betriebszeit von großer Bedeutung ist. Womöglich ist eine weitere Konfiguration erforderlich, da das Netzwerk möglicherweise modifiziert werden muss, damit das Sicherungsgerät 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 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; wir empfehlen synchrone Aktualisierungen für einfache Bereitstellungen und Szenarien, bei denen eine kurze Ausfallzeit während der Aktualisierung vertretbar ist.

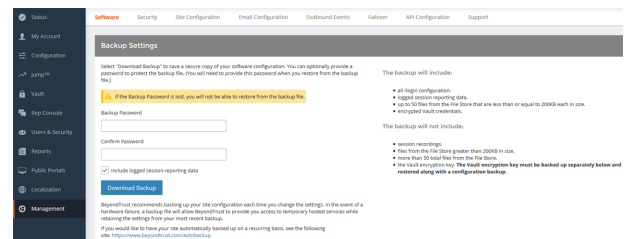
Wir empfehlen, Aktualisierungen innerhalb des angegebenen Wartungszeitraums vorzunehmen. Während des Upgrades ist Ihre BeyondTrust-Website kurzzeitig nicht erreichbar. Alle angemeldeten Benutzer werden abgemeldet und aktive Sitzungen werden beendet. Sie müssen zwei unterschiedliche Aktualisierungsfenster 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. Darüber hinaus empfehlen wir, vor der Bereitstellung in der Produktionsumgebung die Aktualisierung in einer kontrollierten Umgebung zu testen. Sollten Sie während der Basis-Aktualisierung auf Probleme stoßen, starten Sie das Secure Remote Access Appliance nicht neu. Wenden Sie sich bitte an BeyondTrust Technical Support.

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

Sicherung und Synchronisierung

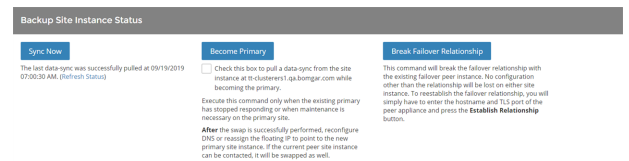
Erstellen Sie vor dem Upgrade eine Sicherungskopie Ihrer aktuellen BeyondTrust-Softwareeinstellungen. Gehen Sie unter **Gerät A** zu **/login > Verwaltung > Software**.

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**.



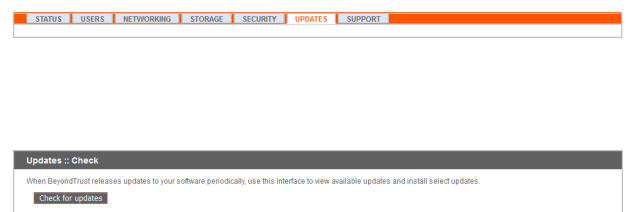
Aktualisieren von Gerät A

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 BeyondTrust Technical Support 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, rufen Sie bitte die Wissensdatenbank auf unter
www.beyondtrust.com/support.

Manuelle Installation

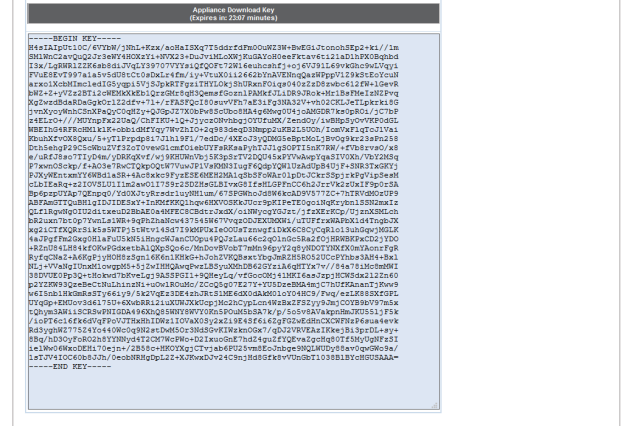
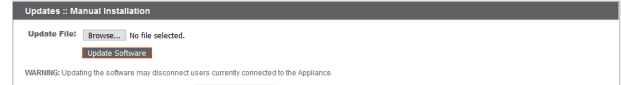
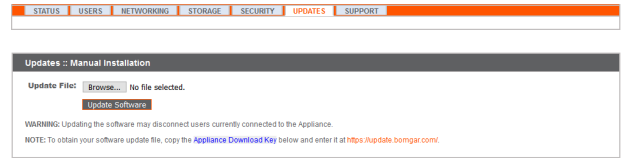
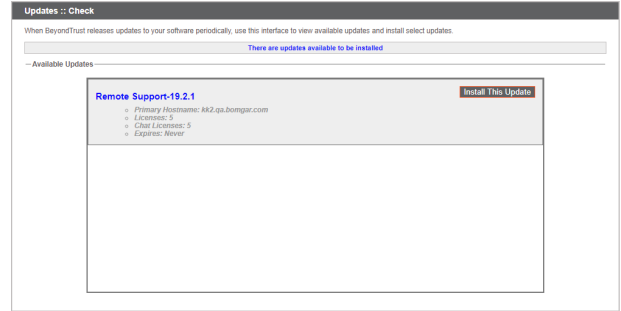
Wenn Sie automatische Aktualisierungen nicht verwenden können (wenn Ihr Gerät bspw. auf einem eingeschränkten Netzwerk betrieben
wird), können Sie manuelle Aktualisierungen vornehmen.

Gehen Sie zu /appliance > Aktualisierungen.

Beginnend mit Base 3.3.2 können Sie auf den Link Geräte-Download-
Schlüssel klicken, um einen eindeutigen Geräte-Schlüssel zu generieren.
Vor Base 3.3.2 müssen Sie den BeyondTrust Technical Support
kontaktieren, um diesen Schlüssel anzufordern. Senden Sie diesen
Schlüssel dann von einem nicht beschränkten System an den
Aktualisierungsserver von BeyondTrust unter https://btupdate.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 BeyondTrust Technical Support unter
www.beyondtrust.com/support.



Verifizieren und testen

Verifizieren Sie nach Abschluss des Aktualisierungsprozesses, dass die Aktualisierung erfolgreich abgeschlossen wurde und Ihre Software wie erwartet funktioniert. Nachdem die Website aktualisiert wurde, müssen Ihre installierten Konsole d. Support-Technikers ebenfalls aktualisiert werden. Normalerweise geschieht dies automatisch, wenn der Support-Techniker das nächste Mal die Konsole d. Support-Technikers 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 außerdem sicher, dass Sie über eine Sitzung eine Verbindung zu einem Remote-Computer herstellen können.



Hinweis: Konsolen der Support-Techniker, die zuvor auf zugriffsgesicherten Computern mit MSI bereitgestellt wurden, müssen, sobald die Aktualisierung beendet wurde, wieder bereitgestellt werden. Wenn die Funktion für die extrahierbare Konsole d. Support-Technikers oder den extrahierbaren Jump-Client vom BeyondTrust Technical Support für Ihre Website aktiviert wurde, können Sie ein MSI-Installationsprogramm herunterladen, um Konsole d. Support-Technikers oder Jump-Clients vor dem Upgrade des Geräts zu aktualisieren. Prüfen Sie dafür entweder manuell oder automatisch auf die neue Aktualisierung. Klicken Sie auf den Link **Installationsprogramme für die Konsole des Support-Technikers** oder **Installationsprogramme für Jump-Clients**, um die MSI-Datei für die Weiterverteilung herunterzuladen. 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

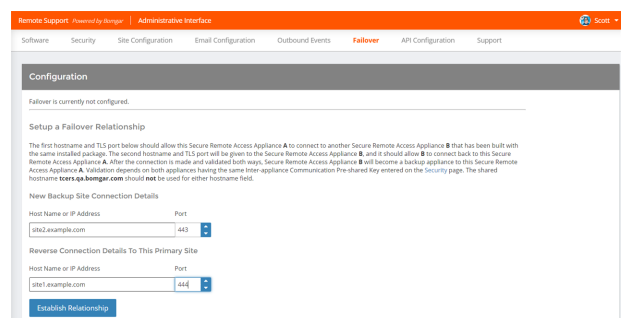
Gehen Sie auf **Gerät A** zu **/login > Verwaltung > Failover**.



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

Stellen Sie die Failover-Verbindung mit dem Sicherungsgerät her, wobei **Gerät B** als Sicherungsgerät 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 **Umgekehrten 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.



Remote Support **Admin/By Device** | Administrative Interface 🔍

Software Security Site Configuration Email Configuration Outbound Events **Failover** API Configuration Support

Configuration

Failover is currently not configured.

Setup a Failover Relationship

The first hostname and TLS port below should allow this Secure Remote Access Appliance A to connect to another Secure Remote Access Appliance B that has been built with the same installed package. The second hostname and TLS port will be given to the Secure Remote Access Appliance B, and it should allow B to connect back to this Secure Remote Access Appliance A. After the connection is made and validated both ways, Secure Remote Access Appliance B will become a backup appliance to the Secure Remote Access Appliance A. Validation depends on both appliances having the same Inter-appliance Communication Pre-shared Key entered on the Security page. The shared hostname help@beyondtrust.com should not be used for either hostname field.

New Backup Site Connection Details

Host Name or IP Address	Port
192.168.1.100	443

Reverse Connection Details To This Primary Site

Host Name or IP Address	Port
192.168.1.101	444

Establish Relationship



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 vom Sicherungsstandort 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 Sicherungsgeräts 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.

Die Failover-Synchronisierung synchronisiert alle Benutzerkonten, alle /login-Konfigurationseinstellungen, Dateien im Dateispeicher, Protokolle und Aufzeichnungen. All diese Informationen, die auf dem Sicherungsgerät vorliegen, werden von den Informationen auf dem primären Gerät überschrieben. Wenn das primäre Gerät der Hauptknoten in einem Atlas-Cluster ist, wird das Sicherungsgerät automatisch zum neuen Sicherungs-Hauptknoten in diesem Cluster.

Asynchrone Aktualisierung zweier Geräte in einer Failover-Beziehung

Bei asynchroner Aktualisierung wird das Sicherungsgerät zuerst aktualisiert und übernimmt dann die Rolle des primären Gerätes. Mit dieser Methode wird die Ausfallzeit gering gehalten; wir empfehlen asynchrone Aktualisierungen für größere Bereitstellungen und Szenarien, in denen eine unterbrechungsfreie Betriebszeit von großer Bedeutung ist. Womöglich ist eine weitere Konfiguration erforderlich, da das Netzwerk möglicherweise modifiziert werden muss, damit das Sicherungsgerät als Failover festgelegt werden kann.

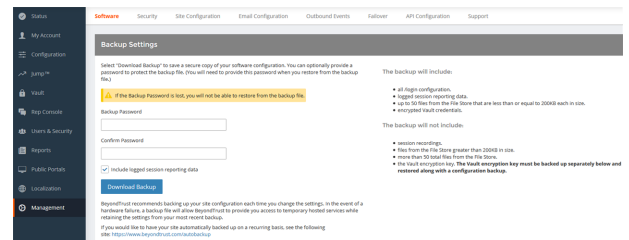
Wir empfehlen, Aktualisierungen innerhalb des angegebenen Wartungszeitraums vorzunehmen. Während des Upgrades ist Ihre BeyondTrust-Website kurzzeitig nicht erreichbar. Alle angemeldeten Benutzer werden abgemeldet und aktive Sitzungen werden beendet. Sie müssen zwei unterschiedliche Aktualisierungsfenster 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. Darüber hinaus empfehlen wir, vor der Bereitstellung in der Produktionsumgebung die Aktualisierung in einer kontrollierten Umgebung zu testen. Sollten Sie während der Basis-Aktualisierung auf Probleme stoßen, starten Sie das Secure Remote Access Appliance nicht neu. Wenden Sie sich bitte an BeyondTrust Technical Support.

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

Sicherung und Synchronisierung

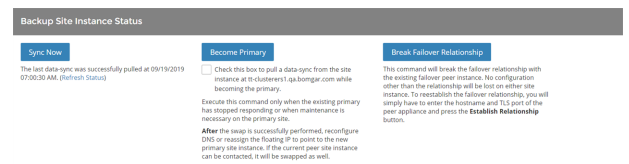
Erstellen Sie vor dem Upgrade eine Sicherungskopie Ihrer aktuellen BeyondTrust-Softwareeinstellungen. Gehen Sie unter **Gerät A** zu **/login > Verwaltung > Software**.

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**.



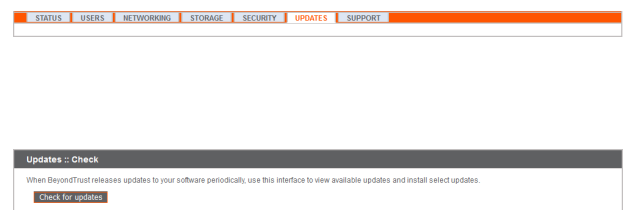
Aktualisieren von Gerät B

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 BeyondTrust Technical Support 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, rufen Sie bitte die Wissensdatenbank auf unter
www.beyondtrust.com/support.

Manuelle Installation

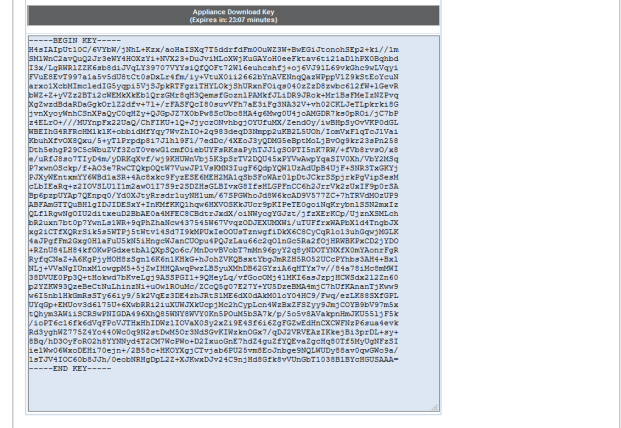
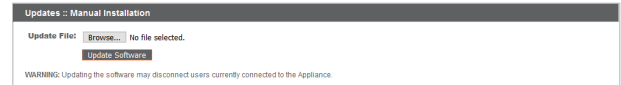
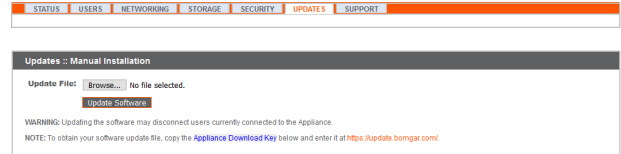
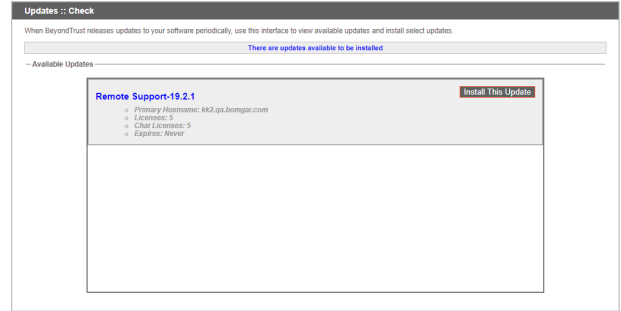
Wenn Sie automatische Aktualisierungen nicht verwenden können (wenn Ihr Gerät bspw. auf einem eingeschränkten Netzwerk betrieben
wird), können Sie manuelle Aktualisierungen vornehmen.

Gehen Sie zu /appliance > Aktualisierungen.

Beginnend mit Base 3.3.2 können Sie auf den Link Geräte-Download-
Schlüssel klicken, um einen eindeutigen Geräte-Schlüssel zu generieren.
Vor Base 3.3.2 müssen Sie den BeyondTrust Technical Support
kontaktieren, um diesen Schlüssel anzufordern. Senden Sie diesen
Schlüssel dann von einem nicht beschränkten System an den
Aktualisierungsserver von BeyondTrust unter https://btupdate.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 BeyondTrust Technical Support unter
www.beyondtrust.com/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 Host-Datei, damit der Hostname Ihrer Webseite zur IP-Adresse von **Gerät B** aufgelöst wird.


 Besuchen Sie für weitere Informationen zu Host-Dateien bitte [https://en.wikipedia.org/wiki/Hosts_\(file\)](https://en.wikipedia.org/wiki/Hosts_(file)).


Führen Sie die Konsole d. Support-Technikers auf einem Computer aus. Nachdem die Website aktualisiert wurde, müssen Ihre installierten Konsole d. Support-Technikers ebenfalls aktualisiert werden. Normalerweise geschieht dies automatisch, wenn der Support-Techniker das nächste Mal die Konsole d. Support-Technikers 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 außerdem sicher, dass Sie über eine Sitzung eine Verbindung zu einem Remote-Computer herstellen können.

 **Hinweis:** Konsolen der Support-Techniker, die zuvor auf zugriffsgesicherten Computern mit MSI bereitgestellt wurden, müssen, sobald die Aktualisierung beendet wurde, wieder bereitgestellt werden. Wenn die Funktion für die extrahierbare Konsole d. Support-Technikers oder den extrahierbaren Jump-Client vom BeyondTrust Technical Support für Ihre Website aktiviert wurde, können Sie ein MSI-Installationsprogramm herunterladen, um Konsole d. Support-Technikers oder Jump-Clients vor dem Upgrade des Geräts zu aktualisieren. Prüfen Sie dafür entweder manuell oder automatisch auf die neue Aktualisierung. Klicken Sie auf den Link **Installationsprogramme für die Konsole des Support-Technikers** oder **Installationsprogramme für Jump-Clients**, um die MSI-Datei für die Weiterverteilung herunterzuladen. 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 Hostnamens konfiguriert haben, vergewissern Sie sich, dass er Daten aus **Gerät B** extrahieren kann, nachdem Sie **Gerät B** als primäres Gerät definiert haben.

 **Hinweis:** Daten von Remote-Support-Sitzung Tech, 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 prüft, können wir nicht jedes mögliche Kundenszenario prüfen. 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

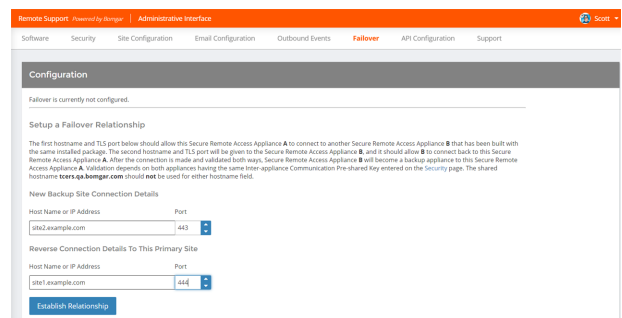
Gehen Sie auf **Gerät B** zu **/login > Verwaltung > Failover**.



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

Stellen Sie die Failover-Verbindung mit dem Sicherungsgerät her, wobei **Gerät A** als Sicherungsgerät 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 **Umgekehrten 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 vom Sicherungsstandort 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 Sicherungsgeräts 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.

Die Failover-Synchronisierung synchronisiert alle Benutzerkonten, alle /login-Konfigurationseinstellungen, Dateien im Dateispeicher, Protokolle und Aufzeichnungen. All diese Informationen, die auf dem Sicherungsgerät vorliegen, werden von den Informationen auf dem primären Gerät überschrieben. Wenn das primäre Gerät der Hauptknoten in einem Atlas-Cluster ist, wird das Sicherungsgerät automatisch zum neuen Sicherungs-Hauptknoten in diesem Cluster.

Upgrade mehrerer Secure Remote Access Appliance in einem Atlas-Cluster

Das Upgraden mehrerer BeyondTrust Atlas-Cluster ist aufwendiger als das Upgraden von Failover-Paaren oder einzelnen Geräten. Der folgende Abschnitt erklärt, wie Atlas-Cluster ordnungsgemäß upgegradet werden.



Weitere Informationen zur Einrichtung und Konfiguration von Atlas finden Sie im [Atlas-Konfigurationshandbuch](https://www.beyondtrust.com/docs/remote-support/how-to/atlas) unter www.beyondtrust.com/docs/remote-support/how-to/atlas.

Mit konfigurierterem Failover

Diese Schritte gehen davon aus, dass zwei Hauptknoten in einer Failover-Konfiguration vorliegen. Diese werden **Gerät A** (der primäre Hauptknoten im Failover-Paar) und **Gerät B** (Die Sicherungskopie des Hauptknotens) genannt. Ist kein Failover konfiguriert und existiert kein Sicherungs-Hauptknoten, springen Sie zum Abschnitt „[Ohne konfiguriertes Failover](#)“ auf Seite 21.



Hinweis: Der Failover-Prozess führt zu Ausfallzeiten. Bitte planen Sie entsprechend.

Vorbereitung

1. Gehen Sie in **Gerät A** zu **/appliance > Verwaltung > Softwareverwaltung**.
 - a. Laden Sie die verfügbaren Updates herunter, aber installieren Sie sie nicht.
 - b. Klicken Sie auf die Schaltfläche **An Cluster verteilen**, um das Paket zu allen anderen Knoten zu pushen.



Hinweis: Damit wird keine neue Software installiert, sondern dies nur vorbereitet.

2. Gehen Sie auf **Gerät A** zu **/login > Verwaltung > Cluster**.
 - a. Identifizieren Sie die Hälfte der Traffic-Knoten, die pro geografische Region vorübergehend deaktiviert werden.
 - b. Deaktivieren Sie bei den gewählten Knoten **Neue Client-Verbindungen annehmen**. Diese werden nun Offline-Traffic-Knoten genannt.
3. Gehen Sie bei jedem Offline-Traffic-Knoten zu **/login > Status > Informationen**.
4. Sehen Sie sich die Tabelle **Verbundene Clients** an und warten Sie, bis alle aktiven Kunden-Client- und Konsole d. Support-Technikers-Verbindungen beendet wurden. Die Wartezeit verhindert die Unterbrechung bestehender Sitzungen.

Upgrade der Sicherung

1. Gehen Sie auf **Gerät B** zu **/appliance > Updates**.
2. Klicken Sie auf die Schaltfläche **Installieren**, um die Software auf die aktuellste Version upzugraden. Installieren Sie die Updates dabei in der richtigen Reihenfolge.



WICHTIG!

Basissoftware-Updates werden in der Regel vor Lizenzsoftware-Updates installiert. Ist Ihnen die Reihenfolge nicht klar, kontaktieren Sie www.beyondtrust.com/support, bevor Sie Updates installieren. Das Gerät wird im Rahmen des Basissoftware-Updateprozesses

automatisch neu gestartet.

Wird die Software aktualisiert, markiert Gerät B automatisch alle Traffic-Knoten so in der Cluster-Konfiguration, dass keine neuen Client-Verbindungen akzeptiert werden.

Nehmen Sie während des Upgrade keine Änderungen an der Konfiguration von Gerät A vor. Solche Änderungen werden bei der ersten Datensynchronisierung nach dem Upgrade überschrieben.

3. Wiederholen Sie den obigen Upgrade-Prozess für jeden der Offline-Traffic-Knoten. Danach müssten Gerät A und die Hälfte der Traffic-Knoten die alte Version von BeyondTrust ausführen. Gerät B und die andere Hälfte der Traffic-Knoten sollten die neue Version ausführen.

Neues Primärgerät in die Produktionsrolle versetzen



Hinweis: Der Failover-Prozess führt zu Ausfallzeiten. Bitte planen Sie entsprechend.

1. Gehen Sie auf **Gerät A** zu **/login > Verwaltung > Failover**.
2. Aktivieren Sie **Sicherung werden, selbst wenn die Peer-Seite nicht kontaktiert werden kann**.
3. Klicken Sie auf die Schaltfläche **Als Sicherung festlegen**.



Hinweis: Dieser Prozess führt dazu, dass das Sicherungsgerät die Primärrolle im Failover-Paar übernimmt.

4. Falls nötig, wechseln Sie DNS und/oder NAT auf Gerät B. Ist ein Failover mit gemeinsamer IP konfiguriert, müssen keine DNS- oder NAT-Einstellungen geändert werden. Stattdessen wird die gemeinsame IP-Adresse automatisch auf Gerät A deaktiviert.
5. Gehen Sie auf **Gerät B** zu **/login > Verwaltung > Failover**.
6. Klicken Sie auf **Als Primär festlegen**.
7. Deaktivieren Sie das Kontrollkästchen **Sicherungsvorgänge aktivieren**.

Upgegradete Traffic-Knoten wieder online stellen

1. Gehen Sie auf **Gerät B** zu **/login > Verwaltung > Cluster**.
2. Aktivieren Sie bei jedem upgegradeten Traffic-Knoten das Kontrollkästchen **Neue Client-Verbindungen annehmen**.
3. Klicken Sie im Abschnitt **Cluster :: Status** auf **Jetzt synchronisieren**.

Upgraden der restlichen Bereitstellung

1. Gehen Sie bei jedem noch nicht upgegradeten Traffic-Knoten zu **/appliance > Updates**.
2. Klicken Sie auf **Installieren**, um auf die neue Version upzugraden. Stellen Sie sicher, dass Updates in der richtigen Reihenfolge installiert werden. Warten Sie, bis die Installation der Updates abgeschlossen ist.
3. Gehen Sie auf **Gerät B** zu **/login > Verwaltung > Cluster**.
4. Aktivieren Sie bei jedem im vorherigen Schritt upgegradeten Traffic-Knoten das Kontrollkästchen **Neue Client-Verbindungen annehmen**.

Upgraden von Gerät A

1. Gehen Sie auf **Gerät A** zu **/appliance > Aktualisierungen**.
2. Klicken Sie auf **Installieren**, um auf die neue Version upzugraden. Stellen Sie sicher, dass Updates in der richtigen Reihenfolge installiert werden.

Wiederherstellen der Cluster-Konfiguration

1. Gehen Sie auf **Gerät A** zu **/login > Verwaltung > Failover**.
2. Aktivieren Sie die Option **Sicherungsvorgänge aktivieren**.
3. Gehen Sie auf **Gerät B** zu **/login > Verwaltung > Cluster**.
4. Klicken Sie im Abschnitt **Cluster :: Status** auf **Jetzt synchronisieren**.

Ohne konfiguriertes Failover

Vorbereitung

1. Gehen Sie zu **/login > Verwaltung > Softwareverwaltung**.
 - a. Laden Sie die verfügbaren Updates wie in „[Upgrade eines einzelnen Secure Remote Access Appliance mit manuellen Aktualisierungen](#)“ auf Seite 8 beschrieben herunter, aber installieren Sie sie nicht.
 - b. Klicken Sie auf die Schaltfläche **An Cluster verteilen**, um das Paket zu allen anderen Knoten zu pushen.



Hinweis: *An Cluster verteilen* wird nur bei Geräten angezeigt, die Teil eines Atlas-Clusters sind.



Hinweis: *Damit wird keine neue Software installiert, sondern dies nur vorbereitet.*

2. Gehen Sie zu **/login > Verwaltung > Cluster**.
 - a. Identifizieren Sie die Hälfte der Traffic-Knoten, die pro geografische Region vorübergehend deaktiviert werden.
 - b. Deaktivieren Sie bei den gewählten Knoten **Neue Client-Verbindungen annehmen**. Diese werden nun Offline-Traffic-Knoten genannt.
3. Gehen Sie bei jedem Offline-Traffic-Knoten zu **/login > Status > Informationen**.
4. Sehen Sie sich die Tabelle **Verbundene Clients** an und warten Sie, bis alle aktiven Kunden-Client- und Konsole d. Support-Technikers-Verbindungen beendet wurden. Die Wartezeit verhindert die Unterbrechung bestehender Sitzungen.

Upgrade der Offline-Knoten

1. Gehen Sie bei jedem Offline-Traffic-Knoten zu **/appliance > Aktualisierungen**.
2. Klicken Sie auf die Schaltfläche **Installieren**, um die Software auf die aktuellste Version upzugraden. Installieren Sie die Updates dabei in der richtigen Reihenfolge.

**WICHTIG!**

Basissoftware-Updates werden in der Regel vor Lizenzsoftware-Updates installiert. Ist Ihnen die Reihenfolge nicht klar, kontaktieren Sie www.beyondtrust.com/support, bevor Sie Updates installieren. Das Gerät wird im Rahmen des Basissoftware-Updateprozesses automatisch neu gestartet.

Upgrade des Hauptknotens

1. Gehen Sie auf dem Hauptknoten zu **/appliance > Aktualisierungen**.
2. Klicken Sie auf die Schaltfläche **Installieren**, um die Software auf die aktuellste Version upzugraden. Installieren Sie die Updates dabei in der richtigen Reihenfolge. Beim Aktualisieren der Software markiert der Hauptknoten automatisch alle Traffic-Knoten so in der Cluster-Konfiguration, dass sie keine neue Client-Verbindungen annehmen.

Upgegradete Traffic-Knoten wieder online stellen

1. Gehen Sie auf dem Hauptknoten zu **/login > Verwaltung > Cluster**.
2. Aktivieren Sie bei jedem upgegradeten Traffic-Knoten das Kontrollkästchen **Neue Client-Verbindungen annehmen**.
3. Klicken Sie im Abschnitt **Status** auf **Jetzt synchronisieren**.

Upgraden der restlichen Bereitstellung

1. Gehen Sie bei jedem noch nicht upgegradeten Traffic-Knoten zu **/appliance > Updates**.
2. Klicken Sie auf **Installieren**, um auf die neue Version upzugraden. Stellen Sie sicher, dass Updates in der richtigen Reihenfolge installiert werden. Warten Sie, bis die Installation der Updates abgeschlossen ist.

Wiederherstellen der Cluster-Konfiguration

1. Gehen Sie auf dem Hauptknoten zu **/login > Verwaltung > Cluster**.
2. Aktivieren Sie bei jedem im vorherigen Schritt upgegradeten Traffic-Knoten das Kontrollkästchen **Neue Client-Verbindungen annehmen**.
3. Klicken Sie im Abschnitt **Status** auf **Jetzt synchronisieren**.

Upgrade von BeyondTrust-Hardware

Wenn Sie ein Upgrade Ihres Secure Remote Access Appliance von einem physischen Gerät auf ein anderes durchführen oder zwischen einem physischen und einem RS Virtual Appliance, müssen Sie sowohl das neue Gerät installieren wie auch Daten vom alten Gerät übertragen.

i *Vollständige Einzelheiten zu SSL-Zertifikaten und BeyondTrust finden Sie in [SSL-Zertifikate und BeyondTrust Remote Support](https://www.beyondtrust.com/docs/remote-support/how-to/sslcertificates/index.htm) unter <https://www.beyondtrust.com/docs/remote-support/how-to/sslcertificates/index.htm>.*

1. Wählen Sie das Standardzertifikat, das Sie Ihren Kunden präsentieren möchten.
 - a. Gehen Sie auf Ihrem neuen Gerät zu **/appliance > Sicherheit > Zertifikate**.
 - b. Machen Sie im Abschnitt **Sicherheit :: Andere 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. support.beispiel.com).
 - c. Vergewissern Sie sich, dass für das neue Zertifikat keine Warnungen aufgeführt werden.

i *Tritt eine Warnmeldung auf, beachten Sie die Wissensdatenbank unter www.beyondtrust.com/support.*

- d. Sobald alle Warnmeldungen bearbeitet sind, wählen Sie in der Spalte **Standard** den Auswahlknopf für das Zertifikat, das Sie als Standard festlegen möchten.
2. 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.
3. 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 > Software**.
 - c. Navigieren Sie im Abschnitt **Einstellungen wiederherstellen** zur zuvor heruntergeladenen Sicherungsdatei und klicken Sie dann auf **Sicherung hochladen**, um die Sicherung auf dem neuen Gerät wiederherzustellen.

Zu diesem Zeitpunkt können Sie Ihren DNS-Server aktualisieren, um Datenverkehr auf die IP-Adresse des neuen Geräts zu leiten und können mit dem Testen des Remote-Supports 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-Retouretikett auf das Paket und wenden Sie sich zur Abholung an Ihren Lieferdienst. Sollten Sie nicht über ein Lieferetikett verfügen, wenden Sie sich an den www.beyondtrust.com/support.

Haftungsausschlüsse, Lizenzierungsbeschränkungen und Technischer Support

Haftungsausschlüsse

Dieses Dokument dient ausschließlich Informationszwecken. BeyondTrust Corporation kann den Inhalt ohne Vorankündigung 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. Insbesondere lehnt BeyondTrust Corporation jedwede Haftung für den Inhalt des vorliegenden Dokuments ab, und durch dieses Dokument entstehen weder direkt noch indirekt irgendwelche vertraglichen Pflichten. Die hierin beschriebenen Technologien, Funktionen, Dienste und Prozesse können ohne Ankündigung geändert werden.

Alle Rechte vorbehalten. Andere Markenzeichen auf dieser Seite sind Eigentum der jeweiligen Inhaber. BeyondTrust ist keine gecharterte Bank oder Treuhandgesellschaft oder Hinterlegungsstelle. Sie ist nicht befugt, Geldeinlagen oder Treuhandkonten anzunehmen, und wird nicht von einem Staat oder einer Bundesbankbehörde lizenziert oder reguliert.

Lizenzierungsbeschränkungen

Mit einer BeyondTrust Remote Support-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.

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 bitte an www.beyondtrust.com/support.

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