BeyondTrust

Remote Support
Schnittstelle des Geräts 6.1
(/appliance)

TC:22.04.2021

Table of Contents

Secure Remote Access Appliance – Übersicht

BeyondTrust hat als erstes Unternehmen einen gerätebasierten Ansatz für den Remote-Support auf den Markt gebracht. Unser patentiertes Bereitstellungsmodell – das Secure Remote Access Appliance – ist eine äußerst sichere Option zur Bereitstellung von Remote-Support.

Das Secure Remote Access Appliance (ob physisch oder virtuell) befindet sich in Ihrer Einrichtung oder Ihrem Datenzentrum und unterliegt Ihren eigenen Sicherheitsmaßnahmen. Dieses Bereitstellungsmodell sorgt für mehr Kontrolle über Sicherheit und stellt eine sichere Methode zur Integration von Remote-Support mit Identitätsverwaltung dar, was den Export von Berichtsdaten und Videos für einen vollständigen Prüfpfad erleichtert.

Anatomie der Secure Remote Access Appliance

Das Secure Remote Access Appliance verwendet zwei administrative Webschnittstellen, **/appliance** und **/login**, um die Hardware-Verwaltung von der Benutzerverwaltung zu trennen.

Abbildung: Das BeyondTrust B400-Gerät

Geräteverwaltung

Webschnittstelle **/appliance**
Belegt für:

- Installieren und Konfigurieren von Hardware
- Aktualisieren der BeyondTrust-Software

Ressource
Das Secure Remote Access Appliance Benutzerhandbuch für Administratoren

Benutzerverwaltung

Webschnittstelle **/login**
Belegt für:

- Verwaltung von Benutzern und Workflows
- Berichte zur Support-Aktivität
- Erstellen und Verwenden von Integrationen

Ressource
Das BeyondTrust Benutzerhandbuch für Administratoren

Verwenden dieses Handbuchs

Aus Sicherheitsgründen hat BeyondTrust die Geräteverwaltung von der Benutzerverwaltung getrennt.

Dementsprechend konzentriert sich dieses Handbuch ausschließlich auf die Verwaltung des Secure Remote Access Appliance. Informationen zur Benutzerverwaltung (die /login-Webschnittstelle) finden Sie in der BeyondTrust Verwaltungsschnittstelle.

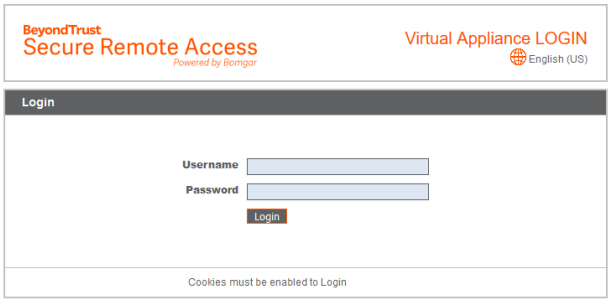
Secure Remote Access Appliance Web-Schnittstelle

Dieses Handbuch soll Ihnen bei der Verwaltung des Secure Remote Access Appliance über die **/appliance**-Webschnittstelle helfen. Das Gerät dient als zentraler Administrations- und Verwaltungspunkt für Ihre BeyondTrust-Websites.

Verwenden Sie dieses Handbuch erst, wenn die anfängliche Einrichtung und Konfiguration des Secure Remote Access Appliance durch einen Administrator abgeschlossen wurde, entsprechend der Beschreibung im Secure Remote Access Appliance-Installationshandbuch für Gerätehardware unter www.beyondtrust.com/docs/remote-support/getting-started/deployment/hardware/. Sobald BeyondTrust korrekt installiert ist, können Sie Kunden sofort unterstützen. Sollten Sie Hilfe benötigen, wenden Sie sich bitte an www.beyondtrust.com/support.

Anmelden in der Geräte-Verwaltungsschnittstelle

Melden Sie sich nach der Installation des Geräts bei der Secure Remote Access Appliance Verwaltungsschnittstelle an. Dazu wechseln Sie zur öffentlichen URL Ihres Geräts gefolgt von **/appliance** (z. B. http://support.beispiel.com/appliance).



Standardbenutzername: **admin**

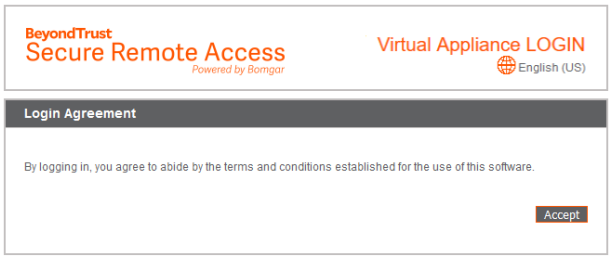
Standardkennwort: **password**

Bei der ersten Anmeldung werden Sie aufgefordert, das Administratorkennwort zu ändern.[1]

Sie können den Zugriff auf den Anmeldebildschirm einschränken, indem Sie eine erforderliche Anmeldungsvereinbarung aktivieren, die bestätigt werden muss, bevor der Anmeldebildschirm angezeigt wird.

Wenn Sie die obligatorische Anmeldungsvereinbarung aktivieren möchten, schlagen Sie nach unter „Geräteverwaltung: Konten, Netzwerke und Ports einschränken, Syslog einrichten, Anmeldungsvereinbarung aktivieren, Administratorkonto zurücksetzen“ auf Seite 27.

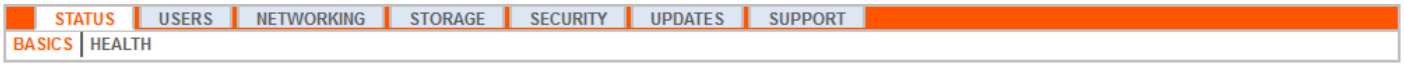
***Hinweis:** Aus Sicherheitsgründen unterscheiden sich der Administrator-Benutzername und das für die Schnittstelle /appliance verwendete Kennwort von den für die Schnittstelle /login verwendeten Anmeldedaten und müssen daher separat verwaltet werden.*



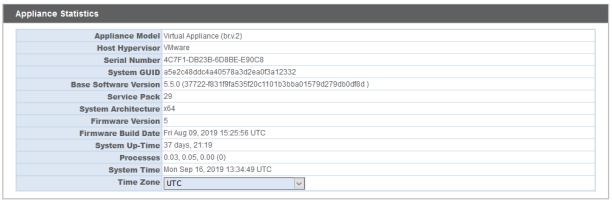
[1]Kennwörter müssen mindestens 8 Zeichen lang sein und jeweils eines der folgenden Zeichen enthalten: einen Großbuchstaben, einen Kleinbuchstaben, eine Zahl und ein Sonderzeichen.

Status

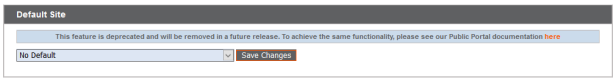
Einfach: Details zum Gerät anzeigen



Die Seite **Einfach** enthält Informationen über Ihr Secure Remote Access Appliance und ermöglicht Ihnen die Überwachung Ihres Systems. Außerdem können Sie die Ortszeit auf eine beliebige Zeitzone der Welt einstellen. Die Systemzeit wird immer in UTC (koordinierte Weltzeit) angezeigt.

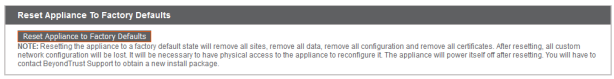


In fast allen Szenarien kann diese Einstellung unverändert belassen werden. BeyondTrust rät von mehreren Websites auf einem Gerät ab. Wenn Ihr Szenario jedoch erfordert, dass mehr als eine Site auf die IP-Adresse reagiert, wählen Sie eine Standard-Site für die Beantwortung, für den Fall, dass Personen die IP-Adresse direkt und nicht den Domänennamen eingeben. Falls mehr ein DNS-Eintrag zu dieser IP-Adresse geleitet wird und Sie **Ohne Standard** wählen, erscheint eine Fehlermeldung, wenn Personen versuchen, durch Eingabe der IP-Adresse auf die Site zuzugreifen.

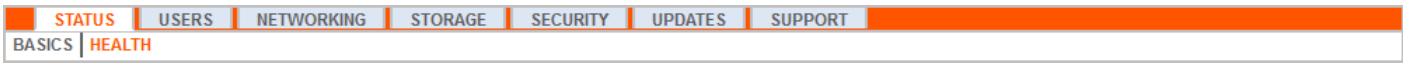


Auf dieser Seite können Sie Ihr Secure Remote Access Appliance auch neu starten oder herunterfahren. Zwar ist der Neustart des Geräts nicht erforderlich, es wird jedoch empfohlen, das Gerät im Rahmen der monatlichen Wartung neu zu starten. Ein physikalischer Zugriff auf das Gerät ist nicht erforderlich, um diesen Neustart durchzuführen.

Die folgenden Schritte dürfen nur bei entsprechender Aufforderung durch den BeyondTrust Technical Support durchgeführt werden: Durch Klicken auf die Schaltfläche **Gerät auf Standardeinstellungen zurücksetzen** wird Ihr Secure Remote Access Appliance auf die Werkseinstellungen zurückgesetzt. Hiermit werden alle Daten, Konfigurationseinstellungen, Sites und Zertifikate komplett von Ihrem Gerät entfernt. Nachdem das Gerät zurückgesetzt wurde, schaltet es sich selbst aus.



Status: Zustandsdetails zum RS Virtual Appliance anzeigen



> ***Hinweis:*** *Die Registerkarte* ***Status*** *ist nur für Seiten sichtbar, die von einem RS Virtual Appliance oder Cloud-Gerät unterstützt werden.*

Auf der Seite **Systemzustand** können Sie den Status Ihres virtuellen oder Cloud-Geräts überwachen. Es werden Informationen dazu angezeigt, wie viele CPUs genutzt werden und wie hoch der Arbeits- und Festplattenspeicherverbrauch ist. Sie können die Spalten **Status** und **Hinweise** aufrufen, um Ratschläge zu erhalten, wie Sie den Status Ihres Geräts verbessern können.

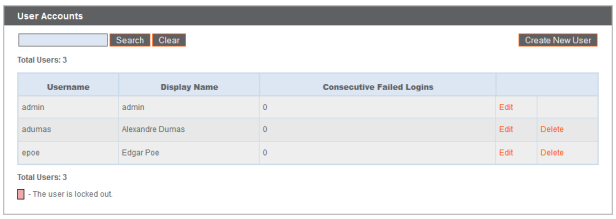
Hardware Health

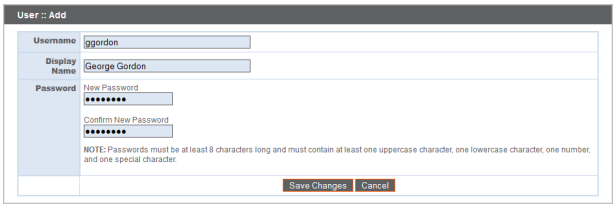
	Value	Status	Notes
CPU	Count: 8 Model: Intel(R) Xeon(R) CPU E5-2697 v3 @ 2.60GHz Speed: 2593.993 MHz Reservation: 0 MHz Limit: Unlimited		• Consider allocating a CPU Reservation to this VM of at least 500 MHz to help maintain functionality when the host's CPUs are under contention.
Memory	Physical: 16051 MiB Used: 15342 MiB Swap Used: 1187.33203125 MiB Reservation: 0 MiB Limit: 3145727 MiB Host Ballooning: 0 MiB Host Swapping: 0 MiB		• Memory swapping could indicate that this appliance is undersized for the current workload. • Consider allocating a Memory Reservation to this VM for the full amount of physical memory to avoid host swapping, which is detrimental to performance.
Storage	Total Space: 279.998 GiB		

Benutzer

Kennwort und Benutzername ändern, Benutzer hinzufügen

Hier können Sie Administratorbenutzer für die /appliance-Schnittstelle hinzufügen, bearbeiten oder löschen. Auch können Sie den Benutzernamen, Anzeigenamen und das Kennwort eines Administrators ändern. BeyondTrust empfiehlt, das Passwort regelmäßig zu ändern, um den Schutz vor unberechtigtem Zugriff zu gewährleisten.





Siehe „Geräteverwaltung: Konten, Netzwerke und Ports einschränken, Syslog einrichten, Anmeldungsvereinbarung aktivieren, Administratorkonto zurücksetzen“ auf Seite 27, um Kontoeinschränkungsregeln, darunter Kennwortablauf und Verlauf, festzulegen.

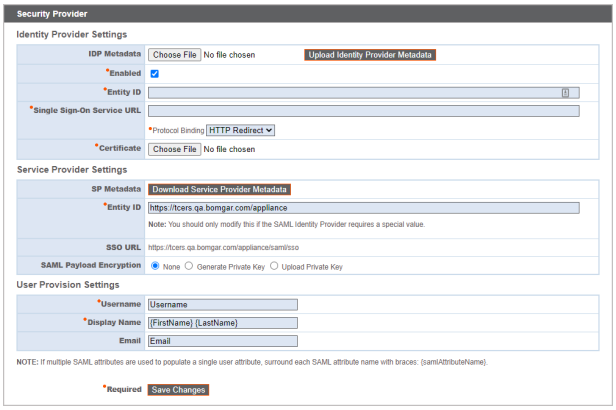
***Hinweis:** Sie müssen über mindestens ein definiertes Benutzerkonto verfügen. Das Secure Remote Access Appliance wird mit einem vordefinierten Konto geliefert, dem Administratorkonto. Sie können das Admin-Konto einfach beibehalten, zusätzliche Konten erstellen oder das Admin-Konto ersetzen.*

SAML: Einrichten der Authentifizierung über einen SAML-Identitätsanbieter

Konfigurieren Sie Ihr Gerät so, dass sich Benutzer über SAML an der /appliance-Schnittstelle authentifizieren können.

> ***Hinweis:*** *Um die SAML-Authentifizierung verwenden zu können, brauchen Sie einen Identitätsanbieter wie Okta, OneLogin, Azure AD oder ADFS.*

Beginnen Sie beim Einrichten der Verbindung mit dem Abschnitt **Serviceanbieter-Einstellungen**. Wenn Ihr Identitätsanbieter (IDP) Ihnen das Hochladen von Metadaten des Serviceanbieters (SP) erlaubt, klicken Sie auf **Metadaten des Serviceanbieters herunterladen**. Dann erhalten Sie eine XML-Datei, die Sie beim Erstellen der Anwendung auf Ihren IDP hochladen können. Kopieren Sie alternativ die **Entitäts-ID** und **SSO-URL** und fügen Sie sie in Ihrem IDP ein.



> ***Tipp:*** *Die **Entitäts-ID** heißt in Ihrem Identitätsanbieter womöglich **Zielgruppen-URI**.*

SAML-Payload-Verschlüsselung ist standardmäßig deaktiviert, Sie können jedoch einen privaten Schlüssel generieren oder hochladen, um sie zu aktivieren. Damit das Gerät einen privaten Schlüssel und ein Zertifikat generiert, wählen Sie **Privaten Schlüssel generieren** und klicken Sie auf **Änderungen speichern**. Klicken Sie auf auf **SP-Zertifikat herunterladen** und laden Sie das generierte Zertifikat auf Ihren Identitätsanbieter hoch. Um den privaten Schlüssel und das Zertifikat selbst bereitzustellen, wählen Sie **Privaten Schlüssel hochladen**, wählen Sie die Zertifikatdatei und geben Sie bei Bedarf deren Kennwort ein. Sie müssen dasselbe Zertifikat auf Ihren Identitätsanbieter hochladen.

Nachdem Sie die Anwendung auf Ihrem Identitätsanbieter gespeichert haben, haben Sie vielleicht die Möglichkeit, deren Metadaten herunterzuladen. Ist dies der Fall, laden Sie diese Datei über die Schaltfläche **Identitätsanbieter-Metadaten hochladen** in Ihr Gerät hoch. Kopieren Sie alternativ die **Entitäts-ID** und **Einzelanmeldungsdienst-URL** im Abschnitt **Identitätsanbieter-Einstellungen** in Ihrem Gerät ein.

> ***Tipp:*** *Die **Entitäts-ID** heißt womöglich **Identitätsanbieter-Aussteller** oder **Aussteller-URL**, und die **Einzelanmeldungsdienst-URL** heißt womöglich **SAML 2.0-Endpunkt**.*

Über die **Protokoll-Bindung** wird festgelegt, ob ein HTTP-POST erfolgt oder oder der Benutzer an die Anmelde-URL weitergeleitet wird. Belassen Sie dies auf **HTTP-Weiterleitung**, sofern Ihr Identitätsanbieter nicht anderes erfordert. Außerdem müssen Sie das **Zertifikat** des Identitätsanbieters angeben, das Sie bei diesem herunterladen können.

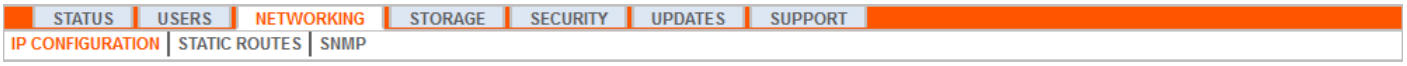
Ordnen Sie unter **Benutzerbereitstellungseinstellungen** den **Benutzernamen**, den **Anzeigenamen** und die **E-Mail-Adresse** den jeweiligen Attributen auf Ihrem Identitätsanbieter zu.

Klicken Sie auf **Änderungen speichern**, um die SAML-Konfiguration zu übernehmen.

Nun sehen Benutzer auf der /appliance-Anmeldeseite unter der Schaltfläche **Anmelden** den Link **SAML-Authentifizierung verwenden**. Benutzer, die der auf Ihrem Identitätsanbieter erstellten Anwendung zugewieseb wurden, können sich über diesen Link anmelden. Wenn sie noch nicht auf dem Identitätsanbieter angemeldet sind, werden sie zur Anmelden auf dem Identitätsanbieter weitergeleitet, ehe sie wieder zum /appliance zurückgeleitet werden.

Netzwerk

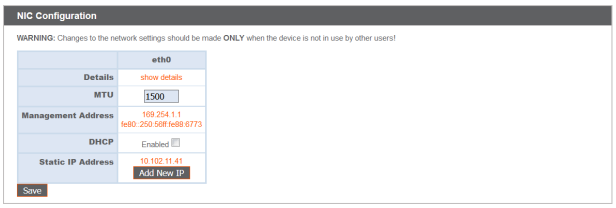
IP-Konfiguration: Konfigurieren von IP-Adressen und Netzwerkeinstellungen



Unternehmen mit erweiterten Netzwerkkonfigurationen können mehrere IP-Adressen auf den Ethernet-Ports des Geräts konfigurieren. Die Verwendung mehrerer Ports kann die Sicherheit verbessern oder Verbindungen über nicht standardmäßige Netzwerke ermöglichen. Wenn z. B. Mitarbeiter ohne Internet-Zugriff netzwerkferne Unterstützung benötigen, verwenden Sie einen Port für Ihr internes privates Netzwerk und einen anderen für das öffentliche Internet. Hiermit geben Sie den weltweiten Benutzern die Möglichkeit, auf Systeme zuzugreifen, ohne gegen Ihre Netzwerksicherheitsrichtlinien zu verstoßen.

Damit kombinieren Sie die physischen Netzwerk-Interface-Controller (NICs) Ihres Sytems in einer einzigen logischen Schnittstelle. Das NIC-Teaming wird im „Aktiv-Backup"-Modus durchgeführt. Einer der NICs übernimmt den gesamten Netzwerkverkehr. Wird die Verbindung zu dieser NIC abgebrochen, wird der andere NIC aktiv. Vor der Aktivierung von NIC-Teaming sollten Sie sicherstellen, dass beide NICs zum gleichen Netzwerksegment verbunden sind (Subnetz), und dass IP-Adressen nur unter einer der bestehenden NICs konfiguriert wurden.

> ***Hinweis:*** *Wenn Sie eine virtuelle oder Cloud-Geräte-Umgebung verwenden, ist die Option* ***NIC-Teaming aktivieren*** *nicht verfügbar.*



Obwohl jedem Network Interface Controller (NIC) mehrere IP-Adressen zugewiesen werden können, sollten Sie NICs nicht so konfigurieren, dass sie eine IP-Adresse im selben Subnetz wie die andere NIC aufweisen. In diesem Szenario kommt es zu Paketverlusten bei Paketen von der IP an der NIC, die nicht das Standard-Gateway besitzt. Erwägen Sie folgende Beispielkonfiguration:

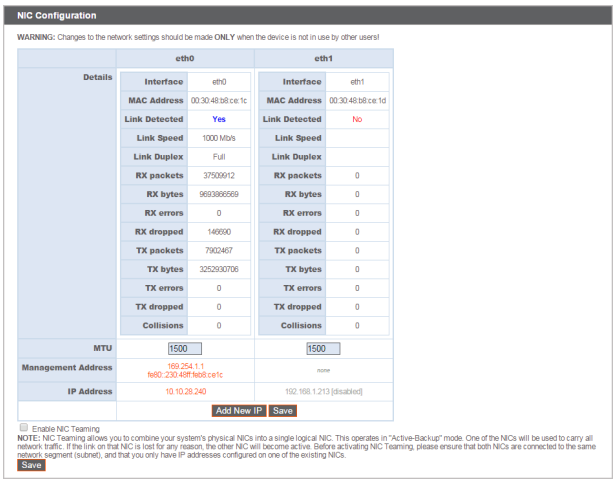
- eth0 ist mit dem Standard-Gateway 192.168.1.1 konfiguriert
- eth0 ist mit 192.168.1.5 konfiguriert
- eth1 ist mit 192.168.1.10 konfiguriert
- Sowohl eth0 als auch eth1 sind mit dem gleichen Subnetz-Switch verbunden

In dieser Konfiguration wird Verkehr beider NICs an das Standard-Gateway (192.168.1.1) gesandt, unabhängig davon, welche NIC Verkehr erhalten hat. Mit dem dynamischen Adressauflösungsprotokoll (ARP) konfigurierte Switches senden Pakete zufällig entweder an eth0 (192.168.1.5) oder eth1 (192.168.1.10), nicht aber an beide. Wenn eth0 diese Pakete vom für eth1 zugewiesenen Switch erhält, verwirft eth0 die Pakete. Einige Switches sind mit einem statischen ARP konfiguriert. Diese Switches verwerfen alle von eth1 erhaltenen Pakete, da diese NIC das Standard-Gateway aufweist und nicht in der statischen ARP-Tabelle des Gateways aufgeführt ist. Wenn Sie redundante NICs im gleichen Subnetz konfigurieren möchten, verwenden Sie NIC-Teaming.

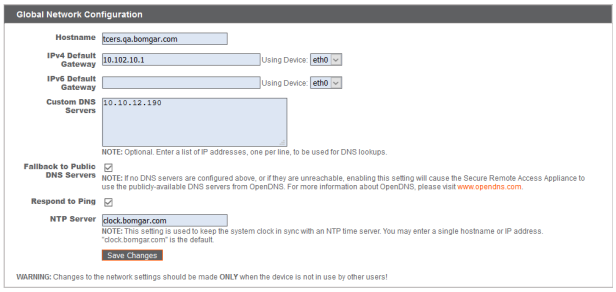
Standardmäßig ist das dynamische Hostkonfigurationsprotokoll (DHCP) für Ihr Gerät aktiviert. DHCP ist ein Netzwerkprotokoll, das einen DHCP-server nutzt, um die Verteilung von Netzwerkparametern wie IP-Adressen zu steuern. So können Systeme diese Parameter automatisch anfordern. Dies reduziert den manuellen Konfigurationsaufwand. Ist diese Option aktiviert, wird eine IP-Adresse vom DHCP-Server zugewiesen, die dann vom Pool verfügbarer IP-Adressen entfernt wird.

> ***Hinweis:*** *Um mehr über DHCP zu erfahren, lesen Sie weiter in Dynamisches Hostkonfigurationsprotokoll (DHCP) unter https://docs.microsoft.com/en-us/windows-server/networking/technologies/dhcp/dhcp-top.*

Klicken Sie auf **Details einblenden**, um die Übertragungs- und Empfangsdaten für jeden Ethernet-Port auf dem Gerät anzuzeigen und zu prüfen.



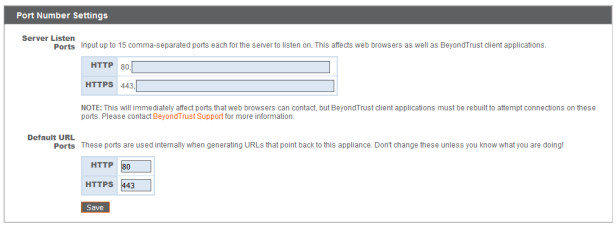
Konfigurieren Sie im Abschnitt **Globale Netzwerkkonfiguration** den Hostnamen für Ihr Secure Remote Access Appliance.



> ***Hinweis:*** *Das Hostnamensfeld muss keine technischen Anforderungen erfüllen. Es hat keine Auswirkungen darauf, mit welchem Hostnamen Client-Anwendungen oder Remote-Benutzer sich verbinden. (Um diese Änderungen vorzunehmen, siehe* ***/login > Status > Informationen > Client-Software verwendet standardmäßig zuerst****. Wenn der von der Client-Software verwendete Hostname geändert werden muss, benachrichtigen Sie den BeyondTrust Technical Support über die benötigten Änderungen, damit der Support eine Softwareaktualisierung bereitstellen kann.) Das Hostnamensfeld existiert hauptsächlich, damit Sie zwischen mehreren Secure Remote Access Appliance unterscheiden können. Ebenfalls wird es als lokale Serverkennung verwendet, wenn SMTP-Verbindungen zum Versenden von E-Mail-Benachrichtigungen aufgebaut werden. Dies ist nützlich, wenn der* ***SMTP-Relay-Server*** *unter* ***/appliance > Sicherheit > E-Mail-Konfiguration*** *nicht zugänglich ist. In diesem Fall muss der konfigurierte Hostname möglicherweise mit der Reverse-DNS-Abfrage der IP-Adresse des Geräts übereinstimmen.*

Konfigurieren Sie ein Standard-Gateway und wählen Sie, welcher Ethernet-Port genutzt werden sollen. Geben Sie eine IP-Adresse für einen oder mehrere DNS-Server ein. Wenn DHCP aktiviert ist, bietet Ihnen der DHCP-Lease ein Standard-Gateway und eine Liste von DNS-Servern in bevorzugter Reihenfolge. Jegliche statisch konfigurierte DNS-Server aus dem Feld **Benutzerdefinierte DNS-Server** werden zuerst kontaktiert, gefolgt von über DHCP erhaltenen DNS-Servern. Falls diese lokalen DNS-Server nicht verfügbar sind, können Sie mit der Option **Auf offene DNS-Server zurück verschieben** des Secure Remote Access Appliance die Möglichkeit geben, öffentlich verfügbare DNS-Server von OpenDNS zu verwenden. Für weitere Informationen über OpenDNS gehen Sie bitte zu www.opendns.com.

Geben Sie Ihrem Gerät die Möglichkeit, auf Pings zu antworten, wenn Sie in der Lage sein möchten zu testen, ob der Host funktioniert. Legen Sie den Hostnamen oder die IP-Adresse für einen NTP-Server (Network Time Protocol) fest, mit dem Ihr Secure Remote Access Appliance synchronisiert werden soll.

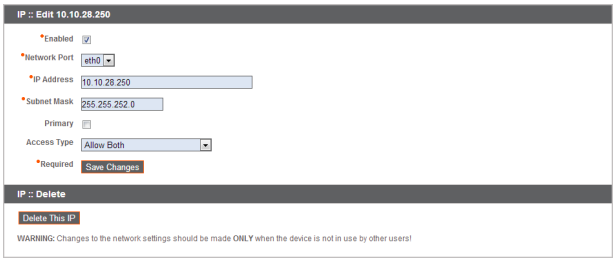


Zwei Einstellungen sind im Bereich **Portnummer-Einstellungen** verfügbar: **Server-Listen-Ports** und **Standard-URL-Ports**. Beachten Sie bei deren Konfiguration, dass Verbindungen zu gültigen Ports aufgrund der unter **/appliance > Sicherheit > Geräteverwaltung** und **/login > Verwaltung > Sicherheit** vorgenommenen Netzwerkeinschränkungen abgelehnt werden können. Auch das Gegenteil gilt: Verbindungen zu ungültigen Ports werden abgelehnt, auch wenn diese Verbindungen die Netzwerkeinschränkungen erfüllen.

Der Bereich **Server-Listen-Ports** ermöglicht es Ihnen, Ports zu konfigurieren, die das Gerät überprüft. Sie können bis zu 15 durch Komma getrennte Ports für HTTP und 15 durch Komma getrennte Ports für HTTPS angeben. Jeder Port darf nur einmal in maximal einem Feld erscheinen. Das Gerät reagiert auf HTTP-Verbindungen zu einem der im HTTP-Feld aufgeführten Ports sowie auf HTTPS-Verbindungen zu einem der im HTTPS-Feld aufgeführten Ports. Sie können die integrierten Listen-Ports (80 und 443) nicht ändern.

Um über einen bestimmten Port mit einem Browser auf das Gerät zuzugreifen, müssen Sie den Port in der URL des Browsers angeben (z. B. support.example.com:8200). Über das Gerät heruntergeladene Clients versuchen, über die auf der Seite **/login > Status > Informationen** unter **Client-Software verwendet standardmäßig zuerst** angegebenen Ports Verbindungen aufzubauen. Diese Ports sind nicht über /login oder /appliance konfigurierbar. Um sie zu ändern, müssen Sie den BeyondTrust-Support kontaktieren und eine neue Aktualisierung für Ihr Gerät kompilieren lassen. Nach der Installation legt die Aktualisierung die **Standard**-Ports fest, die vom BeyondTrust-Support als Parameter für die Aktualisierung konfiguriert wurden.

Standard-URL-Ports werden bei der Erzeugung von URLs verwendet, die zurück auf das Gerät zeigen, wie etwa über die Konsole d. Support-Technikers generierte Sitzungsschlüssel. Wenn die Standardports am Netzwerk gesperrt sind (oder aus anderen Gründen nicht verwendet werden können), können Sie die Standard-URL-Ports ändern, damit URLs mit den benutzerdefinierten Ports generiert werden. Eingegebene Ports sollten ebenfalls als **Server-Listen-Ports** konfiguriert sein. Andernfalls kann keine Verbindung über die Standardports hergestellt werden. Wenn Sie zum Beispiel **8080** im Feld **Standard-URL-Port** eingeben, geben Sie **8080** auch im Feld **HTTP**- oder **HTTPS-Listen-Port** ein. Anders als die Listen-Port-Felder können Sie nicht mehr als einen Port in einem der URL-Port-Felder eingeben. Sie können den gleichen Port nicht in beiden Feldern eingeben.



Wählen Sie beim Hinzufügen oder Bearbeiten einer IP-Adresse aus, ob diese IP aktiviert oder deaktiviert werden soll. Wählen Sie den Netzwerk-Port aus, auf dem diese IP funktionieren soll. Im Feld **IP-Adresse** wird die Adresse festgelegt, der Ihr Gerät antworten kann, während **Subnetzmaske** BeyondTrust die Kommunikation mit anderen Geräten ermöglicht.

Beim Bearbeiten einer IP-Adresse im gleichen Subnetz wie eine andere IP-Adresse für dieses Gerät sollten Sie festlegen, ob diese IP-Adresse als **Primär** festgelegt werden soll. Ist diese Option aktiviert, legt das Gerät diese IP-Adresse als primäre oder ursprüngliche IP-Adresse für das Subnetz fest. Dies stellt beispielsweise sicher, dass jeglicher Netzwerkverkehr vom Gerät dieses Subnetzes mit den definierten Firewall-Regeln übereinstimmt.

Über **Zugriffstyp** können Sie den Zugriff auf diese IP auf die öffentliche Website oder den Kunden-Client einschränken. Nutzen Sie **Beide zulassen**, damit der Zugriff sowohl über die öffentliche Website als auch über den Kunden-Client möglich ist.

> ***Hinweis:*** *Um den Zugriff auf die **/login**-Schnittstelle einzuschränken, legen Sie Netzwerkeinschränkungen unter **/login > Verwaltung > Sicherheit** fest. Um den Zugriff auf die **/appliance**-Schnittstelle einzuschränken, legen Sie Netzwerkeinschränkungen unter **/appliance > Sicherheit > Geräteverwaltung** fest.*

Bei Anzeige der Verwaltungs-IP-Adresse[1], bietet das **Telnet-Server**-Dropdownmenü drei Einstellungen: **Vollständig**, **Vereinfacht** und **Deaktiviert**, wie unten erläutert. Diese Einstellungen ändern die Menüoptionen für den Telnet-Server, der nur auf dieser privaten IP verfügbar ist und in Wiederherstellungssituationen nach einem Notfall verwendet werden kann. Da die Telnet-Funktion speziell mit der integrierten privaten IP verbunden ist, erscheint sie nicht unter den anderen konfigurierten IP-Adressen.

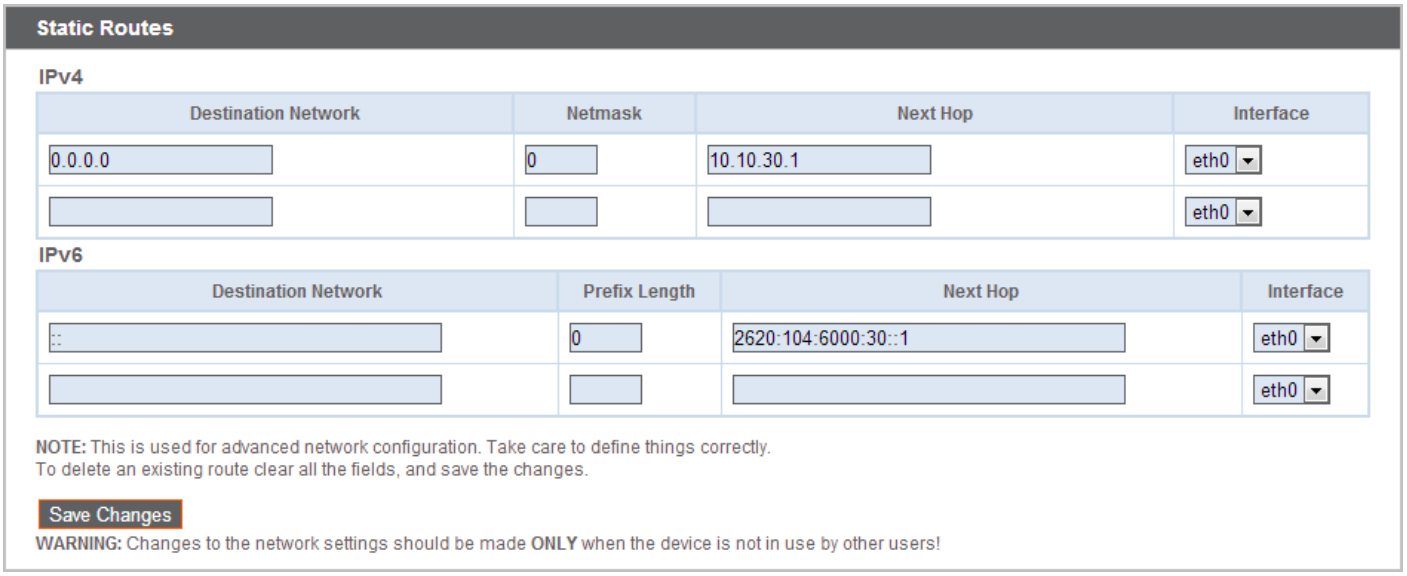
Einstellung	Funktion
Vollständig	Aktiviert den Telnet-Server mit vollständiger Funktionalität
Vereinfacht	Ermöglicht vier Optionen: **FIPS-Fehler anzeigen**, **Gerät auf Originalstandards zurücksetzen**, **Herunterfahren** und **Neustart**
Deaktiviert	Deaktiviert den Telnet-Server vollständig

[1]Die Management-IP-Adresse darf nicht gelöscht oder modifiziert werden.

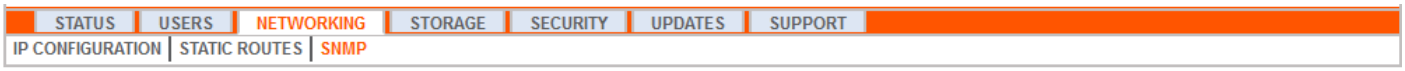
Statische Routen: Einrichten von statischen Routen zur Netzwerkkommunikation

Sollte eine Situation eintreten, bei der zwei Netzwerke nicht miteinander kommunizieren können, können Sie eine statische Route erstellen, damit sich ein Administrator mit einem Computer auf einem Netzwerk über das Secure Remote Access Appliance mit einem Computer auf dem anderen Netzwerk verbinden kann, vorausgesetzt, das Gerät befindet sich an einem Ort, an dem beide Netzwerke individuell mit ihm kommunizieren können.

Nur fortgeschrittene Administratoren sollten versuchen, statische Routen festzulegen.

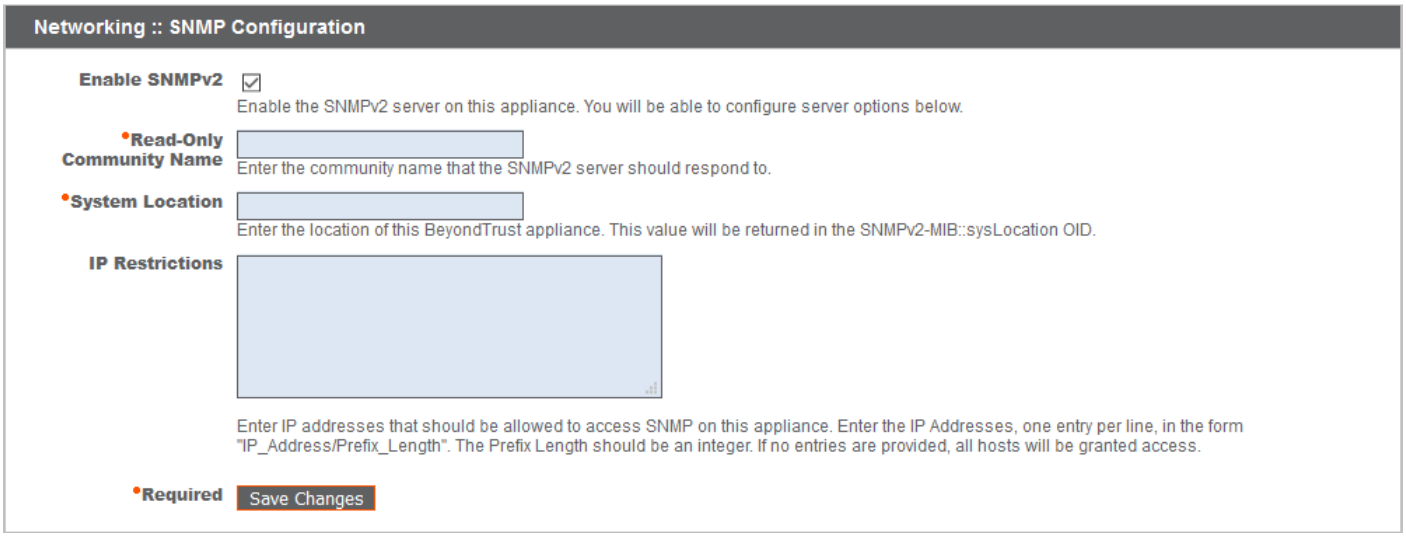


SNMP: Simple Management Network Protocol aktivieren



Das Secure Remote Access Appliance unterstützt das Simple Network Management Protocol (SNMP)[1] zur Überwachung von Statistiken für Netzwerk, Festplatte(n), Speicher und CPU. Hiermit können Tools, die Verfügbarkeitsdaten und andere Statistiken über das SNMP-Protokoll erfassen, das Secure Remote Access Appliance zu Überwachungszwecken abfragen.

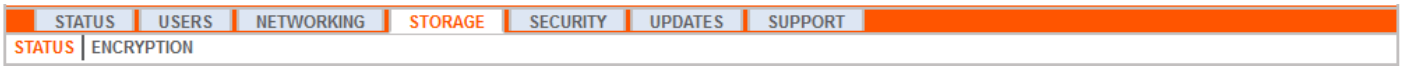
Um SNMP für dieses Gerät zu aktivieren, wählen Sie **SNMPv2 aktivieren**. Hierdurch kann ein SNMPv2-Server auf SNMP-Anfragen reagieren. Geben Sie einen Wert für den **Systemspeicherort**, den **schreibgeschützten Community-Namen** und die **IP-Beschränkungen** oder IP-Adressen ein, die zur Abfrage dieses Geräts mit SNMP berechtigt sind. Bitte beachten Sie, dass allen Hosts der Zugriff gewährt wird, wenn keine IP-Adressen eingegeben werden.



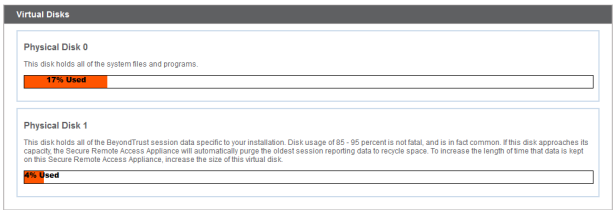
[1]Das Simple Network Management Protocol (SNMP) ist ein Internetstandardprotokoll, das zur Überwachung und Verwaltung von Netzwerkgeräten verwendet wird (siehe Simple Network Management Protocol).

Speicher

Status: Speicherplatz und Festplattenstatus



Die Seite **Status** zeigt den Prozentsatz des belegten Festplattenspeichers Ihres Secure Remote Access Appliance an.

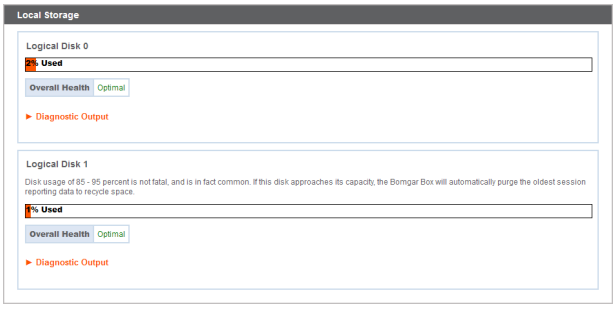


Wenn Sie alle Aufzeichnungsfunktionen auf Ihren Zugangs-Sites (Sitzung und Remote-Shell-Aufzeichnungen) aktivieren oder wenn die Gesamtanzahl Ihrer Sitzungen hoch ist, ist eine höhere Festplattenbelegung normal. Bitte beachten Sie, dass eine Festplattenbelegung von 85-95 % KEIN Grund zur Besorgnis ist. Das Gerät ist so konfiguriert, dass bei Speicherknappheit auf der Festplatte automatisch die ältesten Sitzungsdaten gelöscht werden und der Speicher für neue Sitzungsdaten freigemacht wird.

Spezifische Informationen zum BeyondTrust B300P-Gerät

Das B300 verwendet ein RAID-System, um Ihre Daten zu sichern. RAID 6 wird verwendet, damit dem Gerät selbst beim Verlust von 2 seiner 4 Laufwerke keine Daten verloren gehen. Entfernen Sie bei einem Ausfall die beschädigte Festplatte und wenden Sie sich an BeyondTrust, um eine Rücksendegenehmigung einzuholen und die Festplatte reparieren oder ersetzen zu lassen. Wenn Sie das beschädigte Laufwerk ersetzen, baut das Gerät den RAID automatisch mithilfe des neuen Laufwerks erneut auf. Das Ausschalten des Geräts beim Auswechseln der Festplatten ist nicht erforderlich.

Spezifische Informationen zum BeyondTrust B400P-Gerät



Das B400 enthält zwei Sätze logischer RAID- (Redundant Array of Independent Disks) Laufwerke. Diese RAID-Konfiguration beinhaltet acht physikalische Festplatten, die in zwei logischen RAID-Laufwerken konfiguriert sind: Eine RAID 1-Konfiguration, die das logische Laufwerk 0 darstellt, und eine RAID 6-Konfiguration, die das logische Laufwerk 1 darstellt.

Wenn eines der physikalischen Laufwerke RAID 1 oder RAID 6 fehlschlägt, wird weder die Leistung beeinträchtigt, noch gehen Daten verloren. Bei einem zweiten Laufwerksfehler in der RAID 6-Konfiguration wird zwar die Leistung beeinträchtigt. Es gehen jedoch keine Daten verloren.

Benachrichtigung bei Hardware-Fehler (nur B300 und B400)

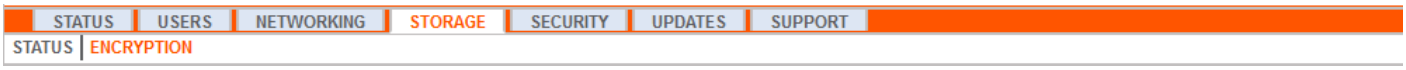
Die LEDs auf Ihrem Gerät geben außerdem den Status Ihrer Festplatten an. Normalerweise blinken die LEDs, um auf die Aktivität der Festplatte

hinzuweisen. Sollte eine Festplatte ausfallen, leuchtet die LED rot, und ein Alarmton weist auf einen Ausfall hin. Um den Alarm auszuschalten, bevor das System wiederhergestellt wird, klicken Sie auf die Schaltfläche **Alarm stummschalten** auf dieser Webschnittstelle.

> ***Hinweis:*** *Die Schaltfläche* ***Alarm stummschalten*** *ist unabhängig davon verfügbar, ob aktuell ein Alarm erklingt. Die Schaltfläche kennzeichnet nicht, ob aktuell ein Alarm aktiv ist.*

> ***Hinweis:*** *Um festzustellen, ob ein Alarm ertönt, überprüfen Sie den* ***Systemzustand*** *direkt über der Schaltfläche* ***Alarm stummschalten****. Wenn ein Alarm im gleichen Raum wie das Secure Remote Access Appliance ertönt und Sie das Gerät als Quelle ausschließen möchten, klicken Sie mehrfach auf die Schaltfläche* ***Alarm stumm schalten****, um jegliche möglicherweise aktiven Alarme zu deaktivieren.*

Verschlüsselung: Verschlüsseln von Sitzungsdaten

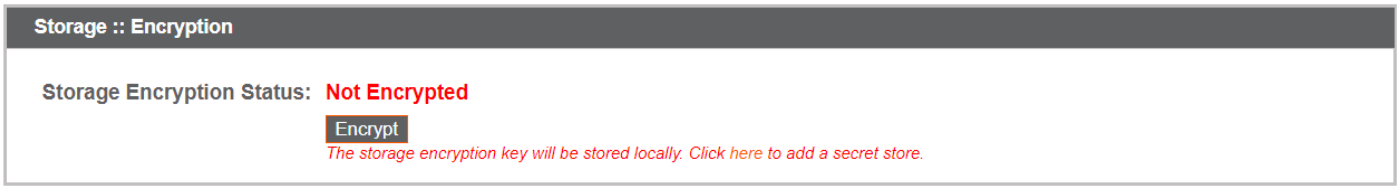


Im Bereich **Verschlüsselung** können Sie Sitzungsdaten auf Ihrem Secure Remote Access Appliance verschlüsseln. Bei der erstmaligen Datenverschlüsselung sind Sie auf 4 GB Daten beschränkt. Nach der Erstverschlüsselung gilt diese Begrenzung jedoch nicht mehr.

Wenn Sie noch keinen Geheimspeicher erstellt haben, gehen Sie zu **Sicherheit > Geheimspeicher**, um einen hinzuzufügen.

Weitere Informationen finden Sie unter Geheimspeicher.

***Hinweis:** Wenn Sie mehr als 4 GB Daten zur erstmaligen Verschlüsselung haben, kontaktieren Sie bitte das BeyondTrust Technical Support unter www.beyondtrust.com/support.*



Sicherheit

Zertifikate: Erstellen und Verwalten von SSL-Zertifikaten

Verwalten von SSL-Zertifikaten, Erstellen von selbstsignierten Zertifikaten und Zertifikatanforderungen und Importieren von Zertifikaten, die von einer Zertifizierungsstelle signiert sind.

Zertifikat-Installation

Das Secure Remote Access Appliance wird mit einem bereits installierten selbstsignierten Zertifikat geliefert. Um Ihr Secure Remote Access Appliance jedoch effektiv nutzen zu können, müssen Sie außerdem zumindest ein selbstsigniertes Zertifikat erstellen; es wird jedoch empfohlen, ein von einer Zertifizierungsstelle signiertes Zertifikat anzufordern und hochzuladen.Neben der Funktion zur Anforderung eines Zertifikats bei einer Zertifizierungsstelle bietet BeyondTrust Funktionen zum Abruf und automatischen Verlängern eigener TLS-Zertifikate über die offene Zertifizierungsstelle Let‘s Encrypt.

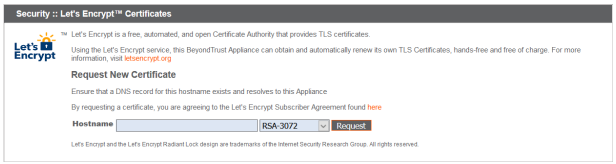
Let's Encrypt

Let's Encrypt stellt signierte Zertifikate aus, die für 90 Tage gültig sind, aber die Fähigkeit haben, sich auf unbestimmte Zeit automatisch selbst zu verlängern. Um ein Let‘s Encrypt-Zertifikat anzufordern oder in Zukunft zu verlängern, müssen Sie folgende Anforderungen erfüllen:

- Der DNS für den angeforderten Hostnamen muss zum Gerät aufgelöst werden.
- Das Gerät muss Let‘s Encrypt auf TCP 443 erreichen können.
- Let‘s Encrypt muss das Gerät auf TCP 80 erreichen können.

Weitere Informationen finden Sie in letsencrypt.org.

Um ein Let‘s Encrypt-Zertifikat zu implementieren, geben Sie im Bereich **Security :: Let's Encrypt™-Zertifikate** Folgendes an:



- Geben Sie im Feld **Hostname** den voll qualifizierten Domänennamen (FQDN) des Geräts ein.
- Wählen Sie im Dropdown-Menü die Art des Zertifikatschlüssels aus.
- Klicken Sie auf **Anfordern**.

Solange die obigen Anforderungen erfüllt sind, erhalten Sie ein Zertifikat, das sich alle 90 Tage automatisch verlängert, sobald die Validitätsprüfung bei Let‘s Encrypt abgeschlossen ist.

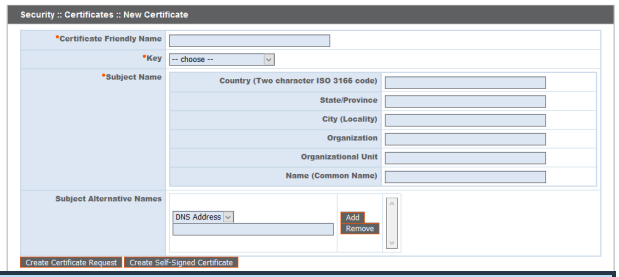
***Hinweis:** Das Gerät startet den Zertifikatvelrängerungsprozess 30 Tage vor Ablauf des Zertifikats und erfordert den gleichen Vorgang wie beim ursprünglichen Anforderungsvorgang. Wenn der Vorgang 25 Tage vor Ablauf noch immer erfolglos ist, sendet das Gerät tägliche Administrator-E-Mail-Warnungen (falls E-Mail-Benachrichtigungen aktiviert sind). Der Status zeigt das Zertifikat in einem Fehlerzustand.*

WICHTIG!

Da der DNS nur für ein Gerät gleichzeitig verwendet werden kann und da ein Gerät dem DNS-Hostnamen zugewiesen werden muss, für den es eine Zertifikat- oder Verlängerungsanforderung versendet, empfehlen wir, die Verwendung von Let's Encrypt-Zertifikaten bei Failover-Gerätepaaren zu vermeiden.

Andere von Zertifizierungsstellen ausgestellte Zertifikate

Um ein selbstsigniertes Zertifikat oder eine Zertifikatanforderung eines anderen Ausstellers zu erstellen, navigieren Sie zum Bereich **Sicherheit :: Andere Zertifikate** und klicken Sie auf **Erstellen**. Geben Sie in **Aussagekräftiger Zertifikatname** den Namen ein, den Sie zur Kennzeichnung dieses Zertifikats verwenden möchten. Wählen Sie im Dropdown-Menü **Schlüssel** aus, einen neuen Schlüssel zu erstellen, oder wählen Sie einen vorhandenen Schlüssel aus. Geben Sie die restlichen Informationen über Ihre Organisation ein.



Hinweis:
Wenn das angeforderte Zertifikat eine Erneuerung ist, sollten Sie den bestehenden Schlüssel des Zertifikats wählen, das ersetzt wird.

*Wenn das angeforderte Zertifikat ein Re-Key ist, sollten Sie **Neuer Schlüssel** für das Zertifikat auswählen.*

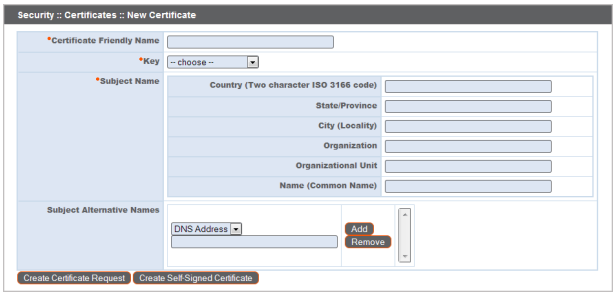
*Bei einem Re-Key sollten alle Informationen des Abschnitts **Sicherheit :: Zertifikate :: Neues Zertifikat** mit dem Zertifikat übereinstimmen, für das der Re-Key angefordert wird. Es sollte ein neuer, aussagekräftiger Zertifikatname verwendet werden, damit das Zertifikat leicht im Abschnitt **Sicherheit :: Zertifikate** identifiziert werden kann.*

*Die für den Re-Key erforderlichen Informationen können angefordert werden, indem Sie auf das ältere Zertifikat auf der Liste klicken, die im Abschnitt **Sicherheit :: Zertifikate** angezeigt wird.*

Die Schritte zum Import sind bei neuen Schlüsseln und Re-Key-Zertifikaten identisch.

Andere von Zertifizierungsstellen ausgestellte Zertifikate

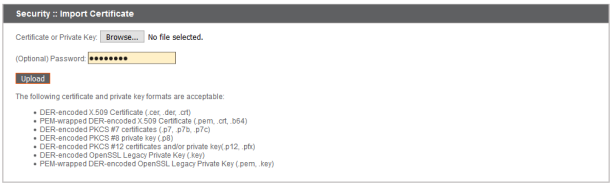
Um eine Zertifikatanforderung zu erstellen:



- Navigieren Sie zum Bereich **Sicherheit :: Andere Zertifikate** und klicken Sie auf **Erstellen**.
- Geben Sie in **Zertifikatsanzeigename** den Namen ein, den Sie zur Kennzeichnung dieses Zertifikats verwenden werden.
- Wählen Sie im Dropdown **Schlüssel** den **bestehenden Schlüssel** Ihres *.beyondtrustcloud.com-Zertifikats.
- Geben Sie die restlichen Informationen über Ihre Organisation ein.
- Geben Sie im Feld **Name (allgemeiner Name)** eine Beschreibung für Ihre BeyondTrust-Website ein.
- Geben Sie im Abschnitt **Betreff-Alternativnamen** den Hostnamen Ihrer BeyondTrust-Website ein und klicken Sie auf **Hinzufügen**. Fügen Sie einen SAN für jede benötigte DNS oder IP-Adresse hinzu, die von diesem SSL-Zertifikat geschützt wird.

> ***Hinweis:*** *DNS-Adressen können eingegeben werden als voll qualifizierte Domänennamen wie zugang.beispiel.com oder als Platzhalterzeichen-Domänennamen wie *.example.com. Ein Platzhalterzeichen-Domänenname deckt mehrere Unterdomämen wie access.example.com und so weiter ab.*

Wenn Sie beabsichtigen, ein signiertes Zertifikat von einer Zertifizierungsstelle anzufordern, klicken Sie auf **Zertifikatsanfrage erstellen**. Andernfalls klicken Sie auf **Selbstsigniertes Zertifikat erstellen**.



Um ein von einer Zertifizierungsstelle signiertes Zertifikat zu verwenden, kontaktieren Sie eine Zertifizierungsstelle Ihrer Wahl und erwerben Sie mit dem in BeyondTrust erstellten CSR ein neues Zertifikat. Nach dem Kauf sendet Ihnen die Zertifizierungsstelle eine oder mehrere Zertifikatsdateien, die Sie auf dem Secure Remote Access Appliance installieren müssen.

Um Zertifikate oder private Schlüssel hochzuladen, klicken Sie auf **Importieren**. Navigieren Sie zur ersten Datei und laden Sie sie hoch. Wiederholen Sie dies für jedes Zertifikat, das Sie von der Zertifizierungsstelle erhalten haben. Oft sendet eine Zertifizierungsstelle nicht ihr Root-Zertifikat, das auf Ihrem Secure Remote Access Appliance installiert werden muss. Sollte das Root-Zertifikat fehlen, erscheint eine Warnung unter Ihrem neuen Zertifikat: „In der Zertifizierungskette fehlen offenbar Zertifizierungsstellen und die Kette endet nicht mit einem selbstsignierten Zertifikat.“

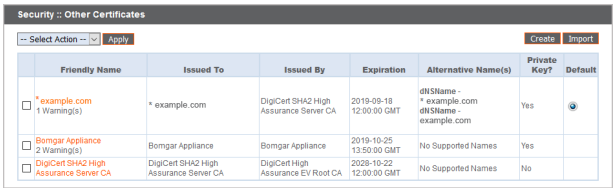
Um das Root-Zertifikat für Ihr Gerätezertifikat herunterzuladen, überprüfen Sie die von der Zertifizierungsstelle gesandten Informationen auf einen Link zum entsprechenden Zertifikat. Sollte es nicht vorhanden sein, kontaktieren Sie die Zertifizierungsstelle. Sollte dies nicht möglich sein, suchen Sie auf der Webseite nach dem Root-Zertifikatspeicher. Diese enthält alle Root-Zertifikate der Zertifizierungsstelle und alle großen Zertifizierungsstellen veröffentlichen ihren Root-Speicher online.

Das richtige Root-Zertifikat finden Sie in der Regel, indem Sie die Zertifikatdatei auf Ihrem lokalen System öffnen und den „Zertifizierungspfad“ bzw. die „Zertifizierungshierarchie“ überprüfen. Das übergeordneteste Zertifikat dieser Hierarchie bzw. dieses Pfads wird in der Regel ganz oben im Baum angezeigt. Machen Sie dieses Root-Zertifikat im Root-Speicher des Online-Root-Speichers Ihrer Zertifizierungsstelle ausfindig. Laden Sie es danach aus dem Root-Speicher der Zertifizierungsstelle herunter und importieren Sie es wie oben beschrieben in Ihrem Secure Remote Access Appliance.

Wenn das Zwischen- und/oder Root-Zertifikat von den aktuell verwendeten Zertifikaten abweicht (oder wenn ein selbstsigniertes Zertifikat verwendet wurde), fordern Sie bitte ein Update von BeyondTrust Technical Support an. BeyondTrust Technical Support wird eine Kopie des neuen Zertifikats und der Zwischen- und Root-Zertifikate benötigen.

Zertifikate

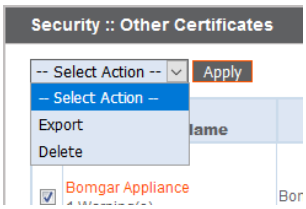
Zeigen Sie eine Tabelle der auf Ihrem Gerät verfügbaren SSL-Zertifikate an.



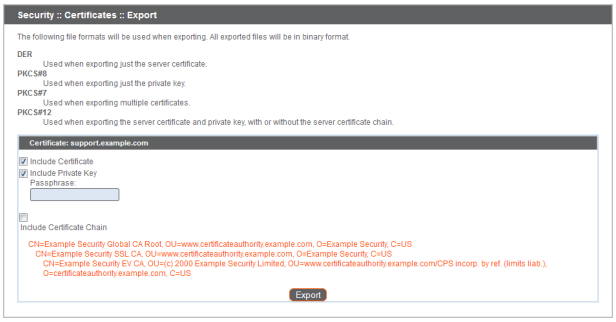
Für Verbindungen, die keine Server Name Indication (SNI) oder eine falsche SNI bereitstellen, wählen Sie ein SSL-Standardzertifikat aus der Liste für diese Verbindungen, indem Sie auf die Schaltfläche unterhalb der Spalte **Standard** klicken. Das SSL-Standardzertifikat darf kein selbstsigniertes Zertifikat und auch nicht das Standardzertifikat des Secure Remote Access Appliance sein, das für die Erstinstallation bereitgestellt wurde.

> ***Hinweis:*** *Um mehr über SNI zu erfahren, lesen Sie weiter unter Server Name Indicationunter https://cio.gov/sni/.*

Um eine oder mehrere Zertifikate zu exportieren, markieren Sie das Kästchen für jedes gewünschte Zertifikat, wählen Sie **Exportieren** im Dropdown-Menü oben in der Tabelle, und klicken Sie auf **Anwenden**.

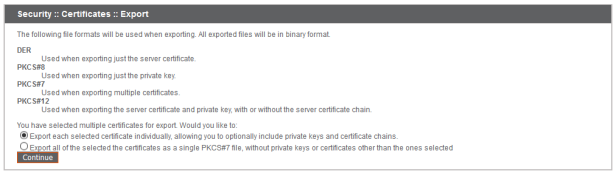


Wenn Sie nur ein Zertifikat exportieren, können Sie sofort auswählen, das Zertifikat, den privaten Schlüssel (optional durch eine Passphrase gesichert) und/oder die Zertifikatkette einzubeziehen, je nach Verfügbarkeit des einzelnen Objekts. Klicken Sie auf **Exportieren**, um den Download zu starten.

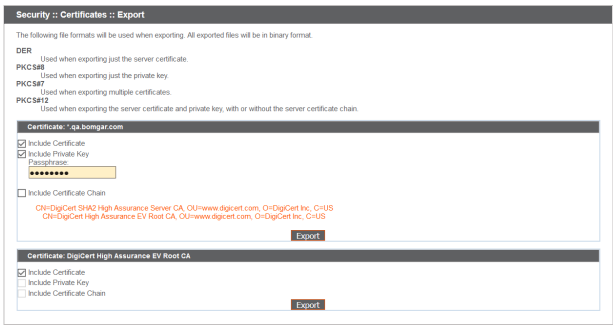


Wenn Sie mehrere Zertifikate exportieren, haben Sie die Möglichkeit, jedes Zertifikat einzeln oder die Zertifikate in einer einzigen PKCS#7-Datei zu exportieren.

Wenn Sie auswählen, mehrere Zertifikate als eine Datei zu exportieren, klicken Sie auf **Weiter**, um den Download zu starten. Mit dieser Option werden nur die eigentlichen Zertifikatdateien ohne private Schlüssel oder Zertifikatketten exportiert.

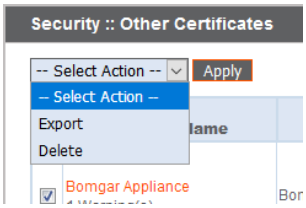


Um private Schlüssel und/oder Zertifikatketten in den Export einzubeziehen, wählen Sie den individuellen Export, und klicken Sie auf **Weiter**, um alle ausgewählten Zertifikate anzuzeigen. Wählen Sie für jede Auflistung aus, das Zertifikat, den privaten Schlüssel (optional durch eine Passphrase gesichert) und/oder die Zertifikatkette einzubeziehen, je nach Verfügbarkeit des einzelnen Objekts. Klicken Sie auf **Exportieren**, um den Download zu starten.



> ***Hinweis:*** *Der private Schlüssel sollte nie oder nur selten von einem Gerät exportiert werden. Wird er gestohlen, könnte sich ein Angreifer leicht Zugriff zur BeyondTrust-Website verschaffen, die den Schlüssel erzeugt hat. Sollte der Schlüssel doch exportiert werden müssen, weisen Sie dem privaten Schlüssel unbedingt ein starkes Kennwort zu.*

Um ein oder mehrere Zertifikate zu löschen, markieren Sie das Kästchen für jedes gewünschte Zertifikat, wählen Sie **Löschen** im Dropdown-Menü oben in der Tabelle, und klicken Sie auf **Anwenden**.

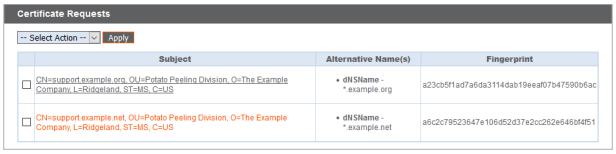


> ***Hinweis:*** *Unter normalen Umständen sollte ein Zertifikat nie gelöscht werden, es sei denn, es wurde bereits durch einen einsatzfähigen Ersatz ausgetauscht.*

Um die Richtigkeit zu bestätigen, prüfen Sie die Zertifikate, die gelöscht werden sollen, und klicken Sie auf **Löschen**.

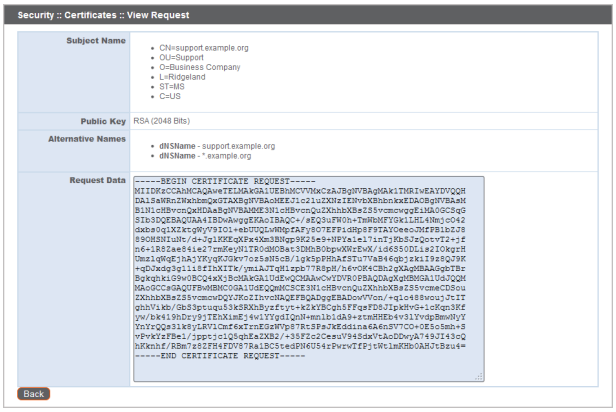
Zertifikatsanfragen

Zeigen Sie eine Tabelle der ausstehenden Anfragen für von Drittparteien signierte Zertifikate an. Klicken Sie auf den Namen der Zertifikatsanfrage, um die Details anzuzeigen.

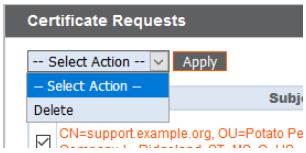


Die Detailansicht liefert außerdem die Anfragedaten, die Sie Ihrer bevorzugten Zertifizierungsstelle übermitteln, wenn Sie ein signiertes Zertifikat anfordern.

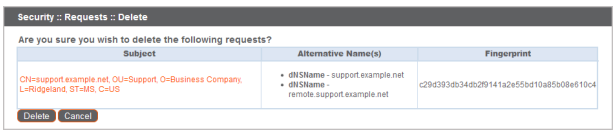
> ***Hinweis:*** *Wenn Sie ein Zertifikat erneuen, nutzen Sie die gleichen Zertifikatanfragedaten, die für das ursprüngliche Zertifikat verwendet wurden.*



Um eine oder mehrere Zertifikatsanfragen zu löschen, markieren Sie das Kästchen für jede gewünschte Anfrage, wählen Sie **Löschen** im Dropdown-Menü oben in der Tabelle, und klicken Sie auf **Anwenden**.



Um die Richtigkeit zu bestätigen, prüfen Sie die Zertifikatsanfragen, die gelöscht werden sollen, und klicken Sie auf **Löschen**.



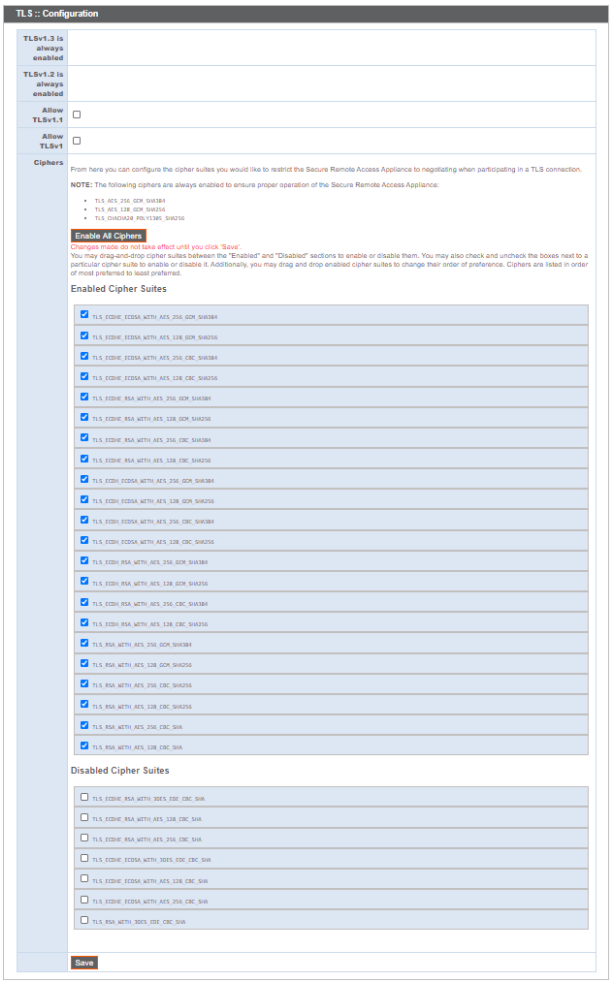
TLS-Konfiguration: Wählen Sie TLS-Codes und Versionen

Wählen Sie, ob TLSv1.3, TLSv1.1, TLSv1 und/oder SSLv3 aktiviert oder deaktiviert werden soll. Für optimale Sicherheit kehrt die BeyondTrust-Webschnittstelle immer zum Standard TLSv1.2 zurück, bevor zu TLSv1.1, TLS1.0 oder SSLv3 gewechselt wird.

Einige ältere Browser unterstützen TLSv1.2 unter Umständen jedoch nicht. Wenn Sie eines oder mehrere ältere Sicherheitsprotokolle deaktivieren und versuchen, von einem älteren Browser, der die aktivierten Sicherheitsprotokolle nicht unterstützt, auf die Verwaltungsschnittstelle zuzugreifen, erlaubt BeyondTrust Ihnen nicht, sich anzumelden. Durch Aktivierung von TLSv1.1, TLSv1.0 und SSLv3 können Sie sich von jedem Computer, unabhängig von der Browser-Version, bei Ihrer Webschnittstelle anmelden.

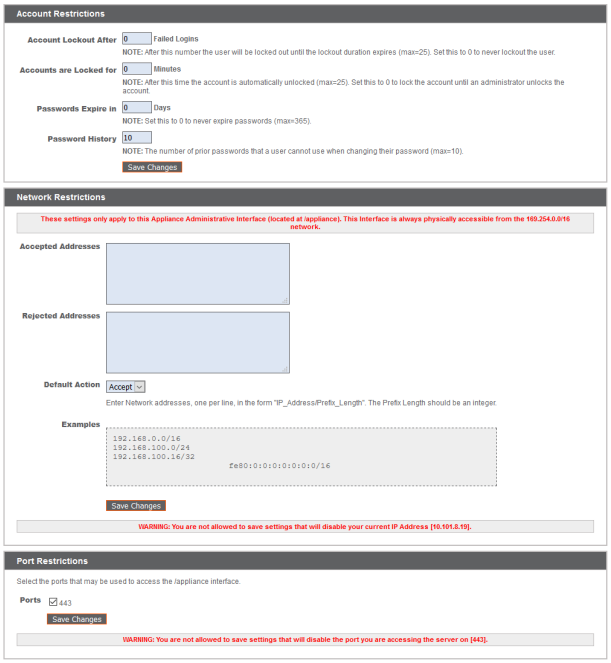
Beachten Sie, dass diese Einstellung hauptsächlich die Verbindungen mit der Webschnittstelle Ihres Secure Remote Access Appliance beeinflusst. Der Support-Tunnel zwischen Ihrem Computer und dem Computer Ihres Kunden ist standardmäßig immer mit TLSv1.2 verschlüsselt ist, unabhängig von anderen aktivierten Sicherheitsprotokollen.

Wählen Sie aus, welche Ciphersuites auf Ihrem Gerät aktiviert bzw. deaktiviert werden sollen. Sie können die bevorzugte Reihenfolge der Ciphersuites mittels Ziehen und Ablegen ändern. Beachten Sie, dass die Änderungen der Ciphersuites erst wirksam werden, nachdem Sie auf die Schaltfläche **Speichern** geklickt haben.



Geräteverwaltung: Konten, Netzwerke und Ports einschränken, Syslog einrichten, Anmeldungsvereinbarung aktivieren, Administratorkonto zurücksetzen

Kontrollieren Sie den Zugriff auf die /appliance-Verwaltungsschnittstelle, indem Sie festlegen, wie viele fehlgeschlagenen Anmeldungen gestattet sind. Legen Sie fest, wie lange ein Konto gesperrt wird, nachdem das Limit für fehlgeschlagene Anmeldungen überschritten wurde. Legen Sie ebenfalls die Anzahl von Tagen fest, die ein Kennwort vor dem Ablauf verwendet werden kann und schränken Sie die Wiederverwendung zuvor verwendeter Kennwörter ein.

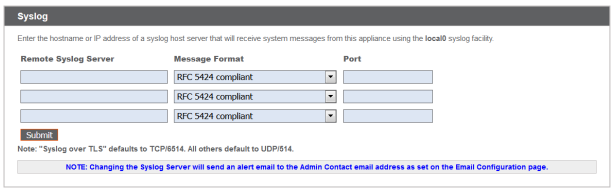


Sie können den Zugriff auf die Verwaltungsschnittstelle Ihres Geräts beschränken, indem Sie Netzwerkadressen festlegen, die erlaubt bzw. nicht erlaubt sind, und indem Sie die Ports auswählen, über die Sie auf diese Schnittstelle zugreifen können.

Definieren Sie im Feld **Akzeptierte Adressen** die IP-Adressen oder Netzwerke, deren Zugriff auf /appliance stets gewährt werden soll. Definieren Sie im Feld **Abgelehnte Adressen** die IP-Adressen oder Netzwerke, deren Zugriff auf /appliance stets abgelehnt werden soll. Verwenden Sie die Dropdown-Option **Standardaktion** um zu bestimmen, ob nicht in den obigen Feldern angeführte IP-Adressen und Netzwerke akzeptiert oder abgelehnt werden sollen. Bei einer Überschneidung gilt die genauere Angabe.

Wenn Sie zum Beispiel den Zugriff für 10.10.0.0/16 gewähren, den Zugriff für 10.10.16.0/24 aber ablehnen und den Zugriff von allen anderen Adressen aus ablehnen möchten, geben Sie 10.10.0.0/16 im Feld **Akzeptierte Adressen** ein, geben 10.10.16.0/24 im Feld **Abgelehnte Adressen** ein und setzen **Standardaktion** auf **Ablehnen**.

Das Secure Remote Access Appliance kann darauf konfiguriert werden, einen STUN-Dienst auf dem UDP-Port 3478 laufen zu lassen, um Peer-to-Peer-Verbindungen zwischen BeyondTrust-Clients zu vereinfachen. Aktivieren Sie die Option **Lokalen STUN-Dienst aktivieren**, um diese Funktion zu nutzen.



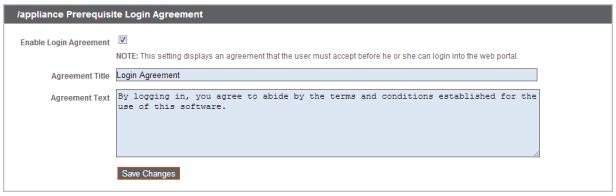
Sie können Ihr Gerät zum Senden von Protokollnachrichten an bis zu drei Syslog-Server konfigurieren. Geben Sie den Hostnamen oder die IP-Adresse des Syslog-Hostservers, der Systemnachrichten von diesem Gerät empfängt, im Feld **Remote-Syslog-Server** ein. Wählen Sie das Nachrichtenformat für die Ereignisbenachrichtigungen. Wählen Sie aus der Standardspezifikation **RFC 5424**, einem der veralteten **BSD-Formate** oder **Syslog over TLS**. Syslog over TLS verwendet standardmäßig den TCP-Port 6514. Alle anderen Formate verwenden standardmäßig UDP 514. Die Standardeinstellungen können jedoch geändert werden. Secure Remote Access Appliance-Protokolle werden mithilfe der Funktion **local0** versendet.

Cloud-spezifische Einstellungen finden Sie in Geräteverwaltung: Syslog über TLS festlegen unter https://www.beyondtrust.com/docs/remote-support/getting-started/deployment/cloud/syslog-over-tls.htm.

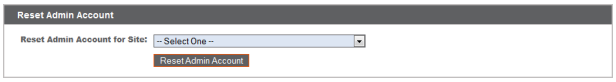
***Hinweis:** Beim Ändern oder Hinzufügen eines Syslog-Servers wird eine Warnung an die E-Mail-Adresse des Administrators gesandt. Die Administratorinformationen werden unter **Sicherheit > E-Mail-Konfiguration > Sicherheit :: Administratorkontakt** konfiguriert.*

Eine detaillierte Syslog-Nachrichtenreferenz finden Sie im Syslog-Nachrichtenreferenzhandbuch in Syslog-Nachrichtenreferenzhandbuch unter www.beyondtrust.com/docs/remote-support/how-to/integrations/syslog/index.

Sie können eine Anmeldungsvereinbarung aktivieren, die Benutzer annehmen müssen, bevor Sie auf die /appliance-Verwaltungsschnittstelle zugreifen können. Die konfigurierbare Vereinbarung gestattet Ihnen die Angabe von Einschränkungen und internen Richtlinien, bevor sich Benutzer anmelden dürfen.

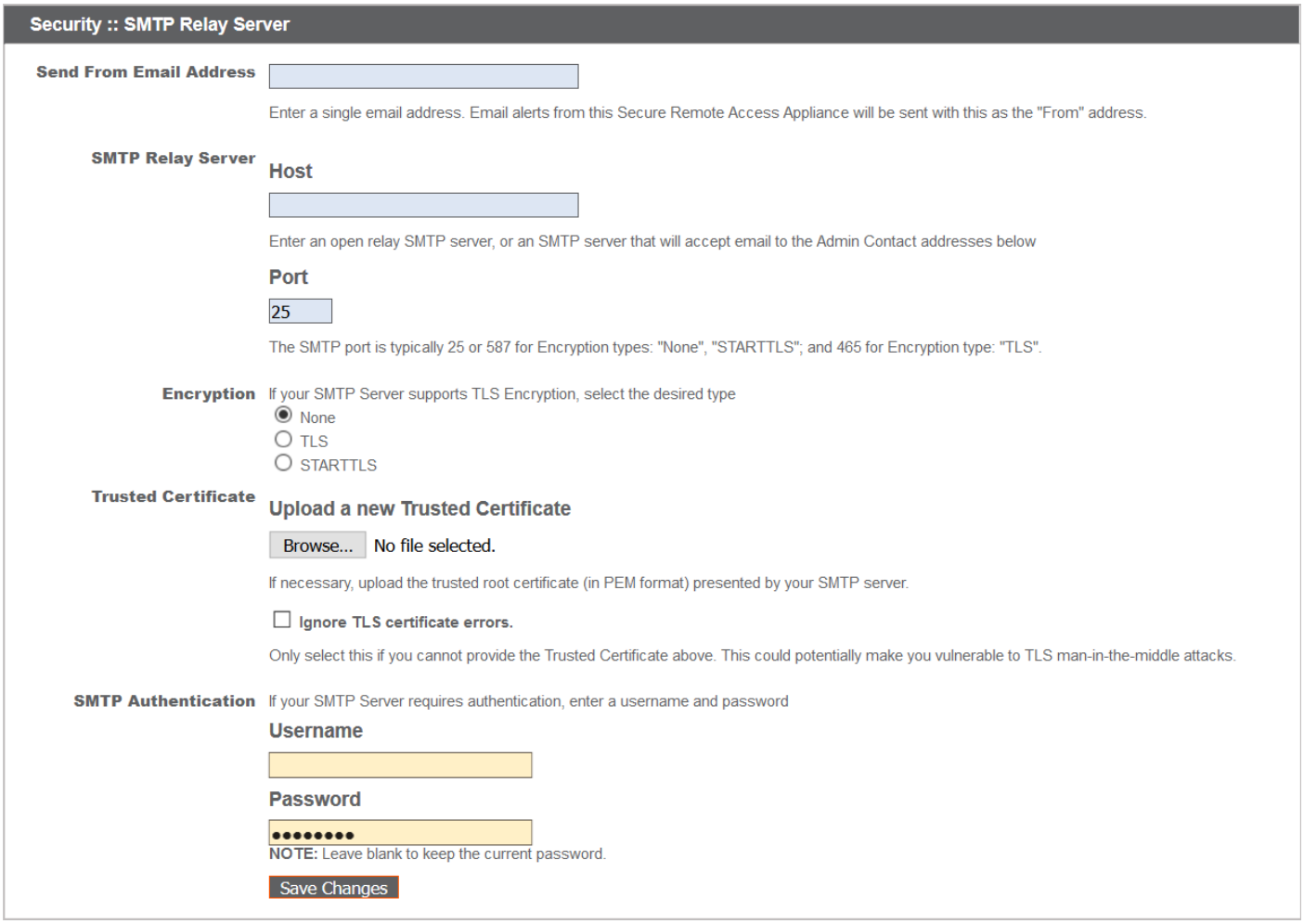


Sie können **Admin-Konto zurücksetzen** auswählen; hierdurch werden der administrative Benutzername und das Kennwort einer Site auf den Standard zurückgesetzt, falls Sie die Anmeldeinformationen vergessen haben oder sie ersetzen müssen.

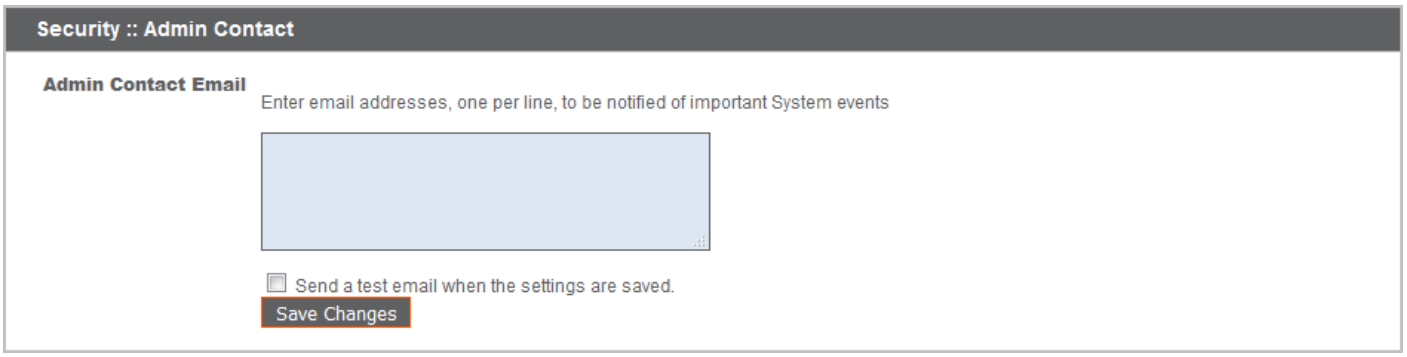


E-Mail-Konfiguration: Konfiguration des Geräts für das Senden von E-Mail-Benachrichtigungen

Konfigurieren Sie Ihren SMTP-Relay-Server und legen Sie einen oder mehrere administrative Kontakte fest, damit Ihr Secure Remote Access Appliance Ihnen automatische E-Mail-Benachrichtigungen senden kann.



Speichern Sie nach der Eingabe der E-Mail-Adressen für die Administratorenkontakte Ihre Einstellungen und senden Sie eine Test-E-Mail, um sicherzustellen, dass alles richtig funktioniert.

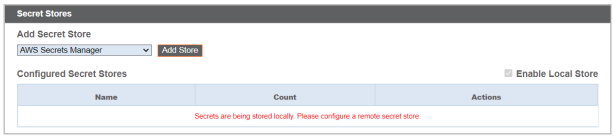


E-Mails werden für folgende Ereignisse versendet:

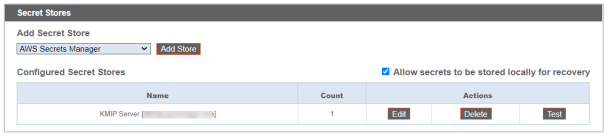
- **Syslog-Server wurde geändert**: Ein Benutzer auf /appliance hat den Syslog-Server-Parameter geändert.
- **RAID-Ereignis**: Eines oder mehrere logische RAID-Laufwerke sind nicht in optimalem Zustand (heruntergestuft oder teilweise heruntergestuft).
- **Ablaufhinweis für ein SSL-Zertifikat**: Ein verwendetes SSL-Zertifikat (schließt entweder End-Entity-Zertifikate oder jegliche CA-Zertifikate in der Kette ein) läuft in 90 Tagen oder weniger ab.

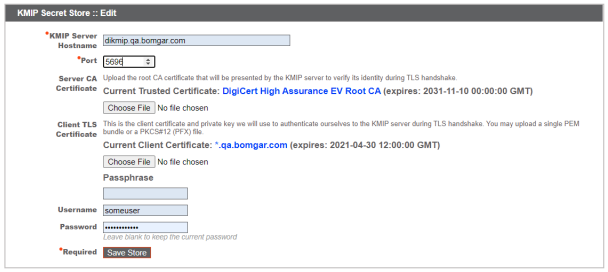
Geheimspeicher: Geheimnisse speichern und auf sie zugreifen

Erstellen und verwalten Sie geheime AWS-Schlüssel, um Verschlüsselungsschlüssel und Website-Daten sicher zu verwahren.



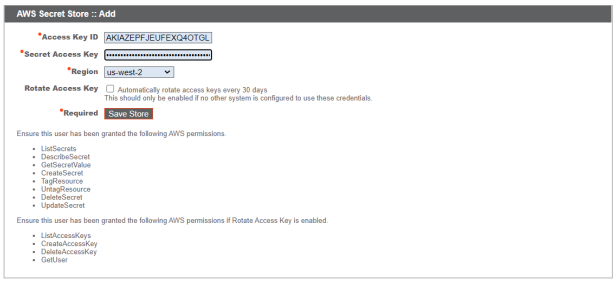
> ***Hinweis:*** *Das Konfigurieren eines KMIP-Servers für einen Verschlüsselungsspeicher wird in Version 6.0 nicht mehr unterstützt. Wenn Sie vor Version 6.0 einen KMIP-Server zur Verschlüsselung konfiguriert haben, wird Ihr KMIP-Server in die Liste der Geheimspeicher migriert. Dort können Sie ihn bearbeiten, löschen, und testen.*





Um einen Speicher hinzuzufügen, klicken Sie auf **Speicher hinzufügen**, füllen Sie die AWS-Geheimspeicher-Daten aus und klicken Sie dann auf **Speicher speichern**.

Aktivieren Sie das Kontrollkästchen **Zugangsschlüssel rotieren** nur, wenn Sie die Anmeldedaten in keinem anderen System verwenden.



Wenn Sie einen Geheimspeicher hinzugefügt haben, klicken Sie auf **Testen**, um die Verbindung mit dem AWS-Server zu überprüfen, sicherzustellen, dass das Benutzerkonto über die richtigen Berechtigungen verfügt und dass mit den Anmeldedaten auf den AWS-Server zugegriffen werden kann.

> ***Hinweis:***
> *Konfigurieren Sie für zusätzliche Sicherheit Ihre AWS-Identitäts- und Zugriffsverwaltungsrichtlinie (IAM), um den Zugriff auf Ressourcen, die **BeyondTrust-*** entsprechen, bei folgenden Berechtigungen zu begrenzen:*
>
> - *DescribeSecret*
> - *GetSecretValue*
> - *TagResource*

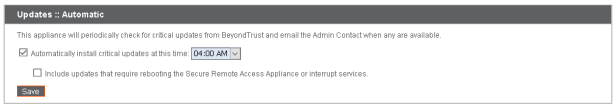
- *UntagResource*
- *CreateSecret*
- *DeleteSecret*
- *UpdateSecret*

Weitere Informationen zur Verwaltung von AWS IAM-Richtlinien finden Sie in Verwalten von IAM-Richtlinienhttps://docs.aws.amazon.com/IAM/latest/UserGuide/access_policies_manage.html.

***Hinweis:** Wenn Sie den letzten Remote-Speicher löschen, wird eine Meldung angezeigt, dass die Secrets lokal verschoben werden.*

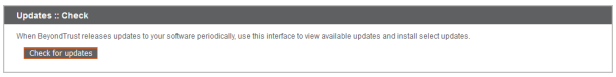
Aktualisierungen: Auf Aktualisierungen prüfen und Software installieren

Das Gerät sucht regelmäßig nach wichtigen Aktualisierungen und sendet eine E-Mail an den Administrator, wenn Aktualisierungen verfügbar sind. Sie können wählen, ob die Aktualisierungen automatisch installiert werden sollen und können das Dropdown-Menü nutzen, um einen Installationszeitpunkt zu wählen.

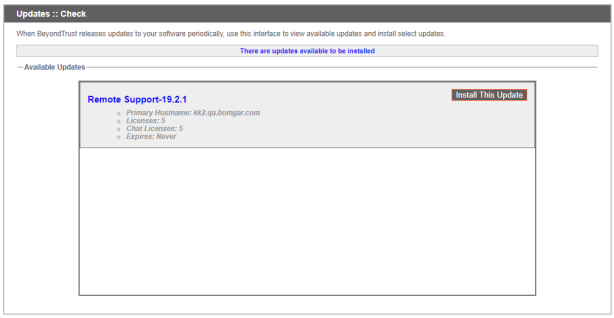


Aktualisierungen, die einen Geräteneustart oder die Unterbrechung von Diensten erfordern, sind vom automatischen Aktualisierungsprozess ausgeschlossen, es sei denn, Sie aktivieren die entsprechende Option.

BeyondTrust benachrichtigt Sie weiterhin über die neuesten Versionen, sobald sie verfügbar sind. Wenn Sie eine Benachrichtigung erhalten, dass neue Aktualisierungspakete für Ihr Gerät verfügbar sind und auf die Schaltfläche **Auf Aktualisierungen prüfen** klicken, werden die Pakete gesucht und zur Installation für Sie verfügbar gemacht.

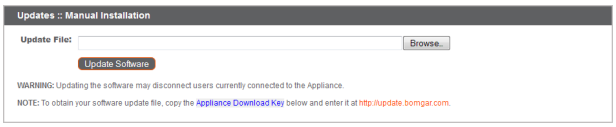


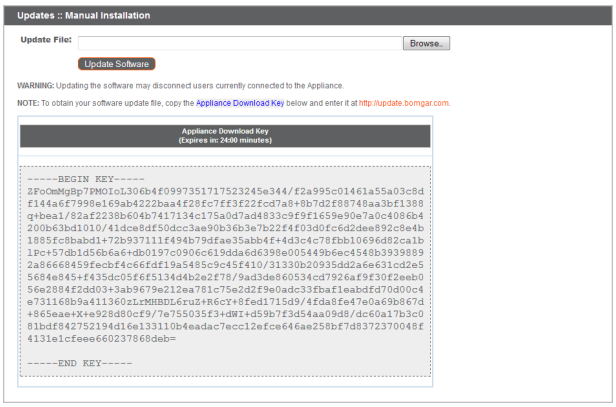
Falls mehrere Softwarepakete für Ihr Gerät erstellt wurden, wird jedes einzeln in der Liste der verfügbaren Aktualisierungen aufgelistet. Ihre neue Software wird automatisch heruntergeladen und installiert, wenn Sie auf die entsprechende Schaltfläche **Diese Aktualisierung installieren** klicken.



Wenn für Ihr Secure Remote Access Appliance keine Aktualisierungspakete oder Patches verfügbar sind, wird die Meldung „Keine Aktualisierungen verfügbar“ angezeigt. Wenn eine Aktualisierung verfügbar ist, aber ein Fehler beim Übertragen der Aktualisierung auf Ihr Gerät auftritt, wird eine weitere Meldung wie „Ein Fehler ist beim Kompilieren Ihrer Aktualisierung aufgetreten. Weitere Informationen finden Sie unter www.beyondtrust.com/docs/index.htm#support.“

Die Verwendung der Funktion **Auf Aktualisierungen prüfen** ist nicht zwingend erforderlich. Falls Ihr Gerät nicht mit dem Internet verbunden ist oder die Sicherheitsrichtlinien Ihrer Organisation keine automatische Aktualisierungsfunktion zulassen, können Sie manuell nach Aktualisierungen suchen. Klicken Sie auf den Link **Geräte-Download-Schlüssel**, um einen eindeutigen Geräteschlüssel zu generieren. Senden Sie diesen Schlüssel dann von einem nicht beschränkten System an den BeyondTrust-Aktualisierungsserver auf 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.





Nach dem Herunterladen eines Softwarepakets navigieren Sie im Abschnitt **Manuelle Installation** zur Datei und klicken dann auf die Schaltfläche **Software aktualisieren**, um die Installation abzuschließen.

> ***Hinweis:*** *Bitte bereiten Sie sich darauf vor, die Aktualisierungen direkt nach dem Herunterladen zu installieren. Nachdem eine Aktualisierung heruntergeladen wurde, erscheint sie nicht länger in Ihrer Liste der verfügbaren Aktualisierungen. Sollten Sie eine Software-Aktualisierung erneut herunterladen müssen, wenden Sie sich bitte an BeyondTrust Technical Support.*

Wenn der Bildschirm für die BeyondTrust-Endbenutzerlizenzvereinbarung (End User License Agreement (EULA)) erscheint, geben Sie die erforderlichen Kontaktinformationen ein, und klicken Sie auf die Schaltfläche **Stimme zu – Download starten**, um die EULA zu akzeptieren und die Installation fortzusetzen. Wenn Sie mehrere Geräte mit derselben Website-Konfiguration (entweder für Failover oder für ATLAS) haben, brauchen Sie die EULA nur einmal zu akzeptieren.

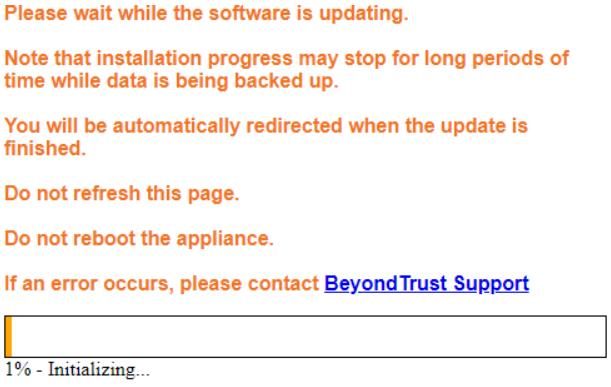
Wenn Sie die EULA nicht akzeptieren, wird eine Fehlermeldung angezeigt, und Sie können Ihre BeyondTrust-Software nicht aktualisieren.

Falls Sie nach dem Akzeptieren der EULA Probleme mit der Aktualisierung haben, wenden Sie sich bitte an BeyondTrust Technical Support unter www.beyondtrust.com/support.

Während der Installation wird auf der Seite **Aktualisierungen** eine Statusleiste angezeigt, die Sie über den Fortschritt der Aktualisierung informiert. Hier vorgenommene Aktualisierungen werden automatisch auf alle Websites und Lizenzen auf Ihrem Secure Remote Access Appliance angewandt.

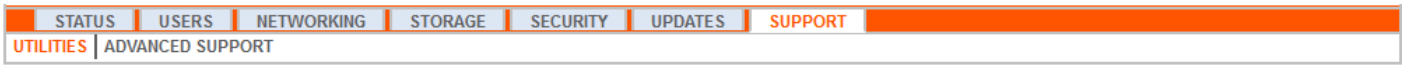
Wenn Sie eine Software-Aktualisierung installieren, verlieren angemeldete Support-Techniker vorübergehend die Verbindung mit ihren Support-Sitzung Tech und der Konsole d. Support-Technikers; daher wird empfohlen, die Software-Aktualisierungen außerhalb der Hauptgeschäftszeiten durchzuführen. Wenn Ihr Aktualisierungspaket jedoch lediglich zusätzliche Lizenzen beinhaltet, kann die Aktualisierung ohne Unterbrechung der Verbindungen der Support-Techniker installiert werden.

Unter https://www.beyondtrust.com/support/changelog finden Sie aktuelle Informationen über die neuesten BeyondTrust-Aktualisierungen.



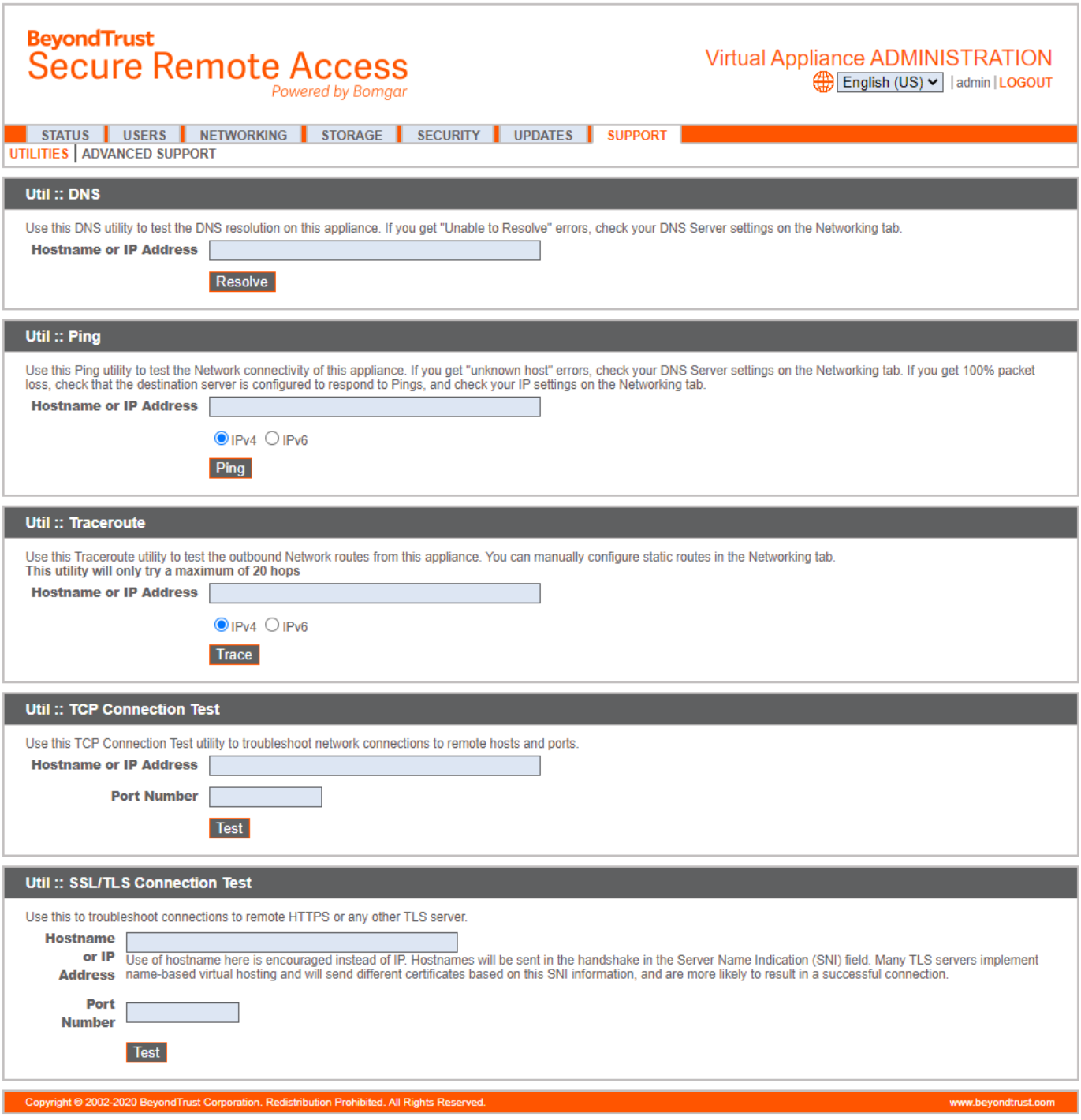
Support

Dienstprogramme: Beseitigung von Netzwerkproblemen

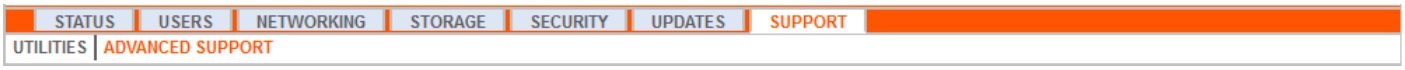


Der Abschnitt **Dienstprogramme** kann zur Beseitigung von Netzwerkproblemen verwendet werden. Falls Sie keine Verbindung aufbauen können, helfen diese Dienstprogramme, den Grund zu bestimmen.

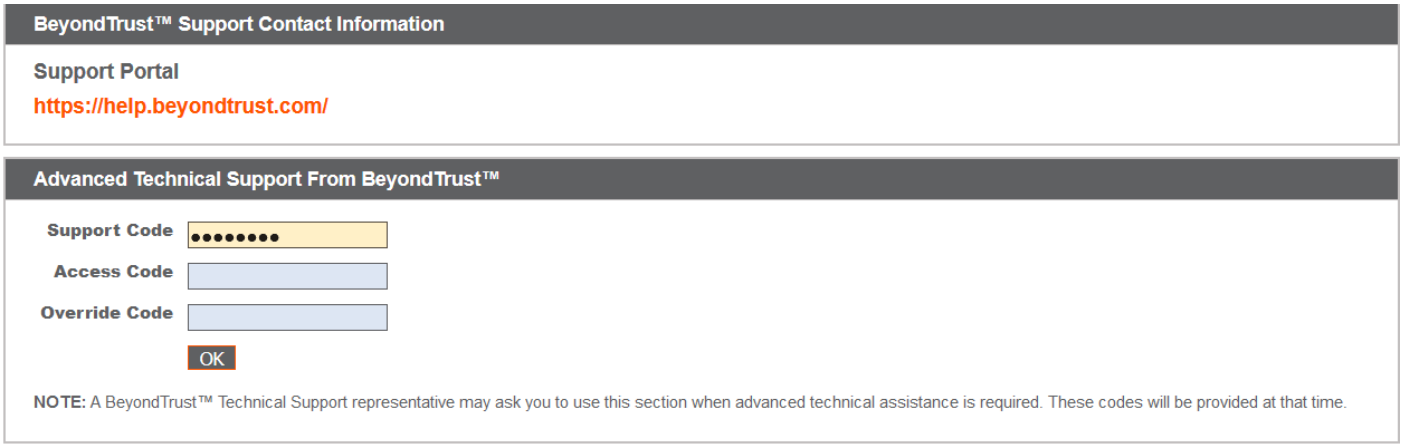
- Testen Sie die **DNS**-Auflösung Ihres Geräts, indem Sie einen Abruf eines Hostnamens oder einen umgekehrten Abruf einer IP-Adresse durchführen.
- **Pingen** Sie einen Hostnamen oder eine IP-Adresse an, um die Netzwerkkonnektivität Ihres Geräts zu testen.
- Sie können **Traceroute** verwenden, um den Pfad anzuzeigen, den die Pakete auf ihrem Weg vom Gerät zu externen Systemen einschlagen.
- Verwenden Sie den **TCP-Verbindungstest**, um die Verbindung zu einem bestimmten Port einer Ziel-IP-Adresse oder eines Hostnamens zu überprüfen.
- Verwenden Sie den **SSL/TLS-Verbindungstest**, um die Verbindung zu HTTPS- oder anderen TLS-Remote-Servern zu prüfen.



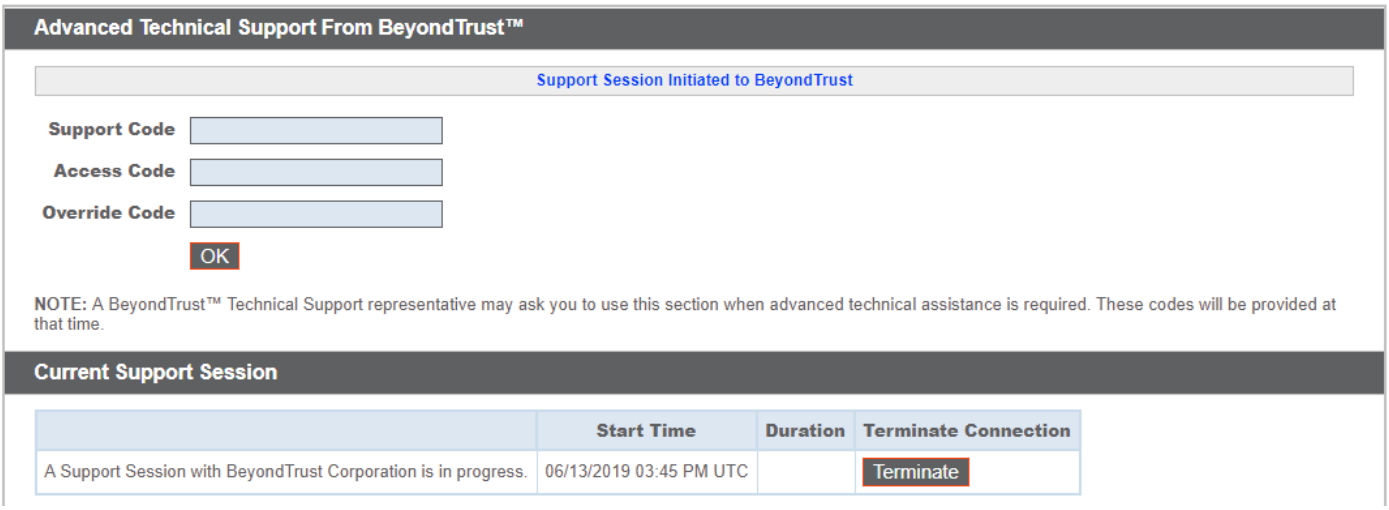
Erweiteter Support: Kontakt mit BeyondTrust Technical Support



Der Abschnitt **Erweiterter Support** enthält Kontaktinformationen für Ihr BeyondTrust Technical Support-Team und ermöglicht auch einen vom Gerät initiierten Support-Tunnel zurück zum BeyondTrust Technical Support, wodurch komplexe Probleme schnell behoben werden können.



Wenn **Eine Support-Sitzung mit BeyondTrust Corporation läuft** sichtbar ist, führt der BeyondTrust Technical Support eine aktive Sitzung mit Ihrem Secure Remote Access Appliance durch. Die Spalte **Dauer** zeigt an, wie lange der BeyondTrust Technical Support bereits in einer Sitzung mit Ihrem Gerät ist. Um die Sitzung zu stoppen, klicken Sie auf **Beenden**, und der Tunnel zwischen Ihrem Gerät und dem BeyondTrust Technical Support wird geschlossen.



Secure Remote Access Appliance-Vergleich

	B400	B300	B200
Support-Techniker-Kapazität	Bis zu 1200 gleichzeitige Techniker	Bis zu 300 gleichzeitige Techniker	Bis zu 20 gleichzeitige Techniker, die jeweils maximal drei Sitzungen ausführen
Jump	Bis zu 25.000 aktive Jump-Clients	Bis zu 10.000 aktive Jump-Clients	Bis zu 1.000 aktive Jump-Clients
Bereitstellung	1U rackmontierbarer Server Kompatibel mit Atlas-Bereitstellungen	1U rackmontierbarer Server Kompatibel mit Atlas-Bereitstellungen	1U rackmontierbarer Server