



# BeyondTrust

## **Privileged Remote Access Schnittstelle des B Series Appliance 6.2 (/appliance)**

## Table of Contents

---

<b>BeyondTrust Appliance B Series Web-Schnittstelle</b> .....	4
<b>Anmeldung in der BeyondTrust Appliance B Series Verwaltungsschnittstelle</b> .....	5
<b>Status Einfach: B Series Appliance-Details einblenden</b> .....	6
<b>Status Systemzustand: Zustandsdetails zum PRA Virtual Appliance anzeigen</b> .....	7
<b>Benutzer: Passwort und Benutzername ändern, Benutzer hinzufügen, Benutzer löschen</b> .....	8
<b>SAML: Einrichten der Benutzer-Authentifizierung über einen SAML-Identitätsanbieter</b> ..	9
<b>Netzwerk</b> .....	11
IP-Konfiguration: Konfigurieren von IP-Adressen und Netzwerkeinstellungen .....	11
<b>SNMP: Simple Management Network Protocol aktivieren</b> .....	15
<b>Statische Routen: Einrichten von statischen Routen zur Netzwerkkommunikation</b> .....	17
<b>Speicher</b> .....	18
Status: Speicherplatz und Festplattenstatus .....	18
Spezifisch für das BeyondTrust B300P B Series Appliance .....	18
Spezifisch für das BeyondTrust B400P B Series Appliance .....	19
Benachrichtigung bei Hardware-Fehler (nur B300P und B400P) .....	19
<b>Verschlüsselung: Verschlüsseln von Sitzungsdaten</b> .....	20
<b>Sicherheit</b> .....	21
Zertifikate: Erstellen und Verwalten von TLS-Zertifikaten .....	21
Zertifikat-Installation .....	21
Zertifikate .....	23
Zertifikatsanfragen .....	24
<b>TLS-Konfiguration: Wählen Sie TLS-Codes und Versionen</b> .....	26
<b>Geräteverwaltung: Einschränken von Konten, Netzwerken und Ports, Aktivieren eines STUN-Servers, Einrichten von Syslogs, Aktivieren der Anmeldevereinbarung, Zurücksetzen des Administratorkontos</b> .....	27
<b>E-Mail-Konfiguration: Konfiguration des B Series Appliances für das Senden von E-Mail-Benachrichtigungen</b> .....	29
Konfigurieren über SMTP .....	29
Konfigurieren über OAuth2 für Microsoft Azure AD .....	29
Konfigurieren über OAuth2 für Google .....	32
<b>Geheimspeicher: Geheimnisse speichern und auf sie zugreifen</b> .....	37

---

<b>Aktualisierungen: Auf Aktualisierungen prüfen und Software auf Privileged Remote Access installieren .....</b>	<b>39</b>
<b>Support Dienstprogramme: Beseitigung von Netzwerkproblemen .....</b>	<b>41</b>
<b>Erweiterter Support: Kontakt mit BeyondTrust Technical Support .....</b>	<b>43</b>

# BeyondTrust Appliance B Series Web-Schnittstelle

Dieses Handbuch soll Ihnen bei der Konfiguration und Verwaltung des B Series Appliance über die **/appliance**-Webschnittstelle helfen. Das B Series Appliance dient als zentraler Administrations- und Verwaltungspunkt für Ihre BeyondTrust-Website.

Verwenden Sie dieses Handbuch erst, wenn die anfängliche Einrichtung und Konfiguration des B Series Appliance durch einen Administrator abgeschlossen wurde, entsprechend der Beschreibung im [BeyondTrust Appliance B Series-Installationshandbuch für Gerätehardware](#) unter [www.beyondtrust.com/docs/privileged-remote-access/getting-started/deployment/hardware-sra/](http://www.beyondtrust.com/docs/privileged-remote-access/getting-started/deployment/hardware-sra/). Ist BeyondTrust korrekt installiert, können Sie sofort mit dem Zugriff auf Ihre Endpunkte beginnen. Sollten Sie Hilfe benötigen, wenden Sie sich bitte an BeyondTrust Technical Support unter [www.beyondtrust.com/support](http://www.beyondtrust.com/support).

# Anmeldung in der BeyondTrust Appliance B Series Verwaltungsschnittstelle

Melden Sie sich nach der Installation des B Series Appliance bei der B Series Appliance Verwaltungsschnittstelle an. Dazu wechseln Sie zur öffentlichen URL Ihres B Series Appliance, gefolgt von **/appliance** (z. B. <http://access.example.com/appliance>).

Standardbenutzername: **admin**

Standardpasswort: **password**

Sie werden bei der ersten Anmeldung aufgefordert, das Administratorpasswort zu ändern.<sup>1</sup>

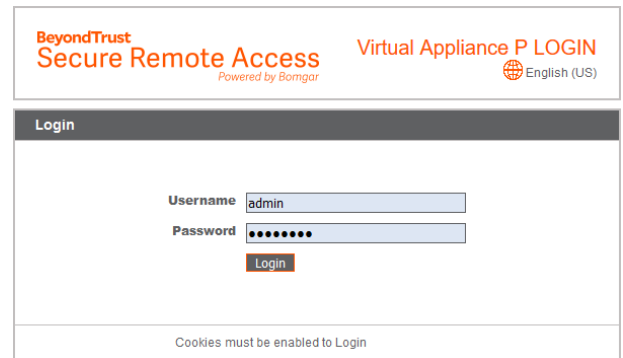


**Hinweis:** Aus Sicherheitsgründen unterscheiden sich der Administrator-Benutzername und das für die Schnittstelle **/appliance** verwendete Passwort von den für die Schnittstelle **/login** verwendeten Anmeldedaten und müssen daher separat verwaltet werden.

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



Wenn Sie die obligatorische Anmeldevereinbarung aktivieren möchten, schlagen Sie nach unter „Geräteverwaltung: **Einschränken von Konten, Netzwerken und Ports, Aktivieren eines STUN-Servers, Einrichten von Syslogs, Aktivieren der Anmeldevereinbarung, Zurücksetzen des Administratorkontos**“ auf Seite 27.



BeyondTrust Secure Remote Access Virtual Appliance P LOGIN  
Powered by Bomgar English (US)

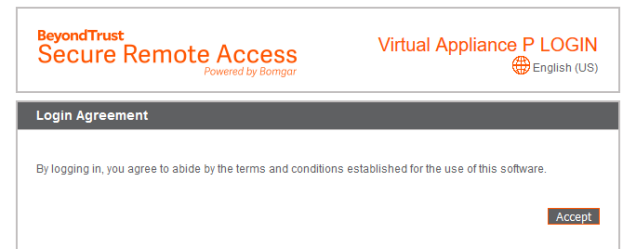
Login

Username

Password

Login

Cookies must be enabled to Login



BeyondTrust Secure Remote Access Virtual Appliance P LOGIN  
Powered by Bomgar English (US)

Login Agreement

By logging in, you agree to abide by the terms and conditions established for the use of this software.

Accept

<sup>1</sup>Passwörter müssen mindestens 8 Zeichen lang sein und folgendes enthalten: einen Großbuchstaben, einen Kleinbuchstaben, eine Zahl und ein Sonderzeichen.

## Status Einfach: B Series Appliance-Details einblenden

STATUS
USERS
NETWORKING
STORAGE
SECURITY
UPDATES
SUPPORT

BASICS | HEALTH

Die Seite **Einfach** enthält Informationen über Ihr B Series 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.

Appliance Statistics	
Appliance Model	Virtual Appliance P (bp.v.2)
Host Hypervisor	VMware
Serial Number	331AE-4445A-65D57-70D3A
System GUID	15ebc9ee423e472b8b49546641d77b7c
Base Software Version	5.4.0 (34183-20c19e8dc03edc94f6416efc34c9be285e1bc3)
Service Pack	28
System Architecture	x64
Firmware Version	5
Firmware Build Date	Wed Jan 23, 2019 14:41:15 UTC
System Up-Time	68 days, 15:57
Processes	0.00, 0.00, 0.00 (0)
System Time	Mon Jun 10, 2019 13:12:53 UTC
Time Zone	UTC <input type="text"/>

In fast allen Szenarien kann diese Einstellung unverändert belassen werden. BeyondTrust rät von mehreren Websites auf einem B Series Appliance 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 Domännennamen 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.

**Default Site**

This feature is deprecated and will be removed in a future release. To achieve the same functionality, please see our Public Portal documentation [here](#).

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

**Reboot | Shut Down**

**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 B Series Appliance auf die Werkseinstellungen zurückgesetzt. Hiermit werden alle Daten, Konfigurationseinstellungen, Sites und Zertifikate komplett von Ihrem B Series Appliance entfernt. Nachdem das B Series Appliance zurückgesetzt wurde, schaltet es sich selbst aus.

**Reset Appliance To Factory Defaults**

**Reset Appliance To Factory Defaults**

NOTE: Resetting the appliance to a factory default state will remove all sites, remove all data, remove all configuration and remove all certificates. After resetting, all custom network configuration will be lost. It will be necessary to have physical access to the appliance to reconfigure it. The appliance will power itself off after resetting. You will have to contact BeyondTrust Support to obtain a new install package.

## Status Systemzustand: Zustandsdetails zum PRA Virtual Appliance anzeigen




<b>STATUS</b>	USERS	NETWORKING	STORAGE	SECURITY	UPDATES	SUPPORT
BASICS	<b>HEALTH</b>					



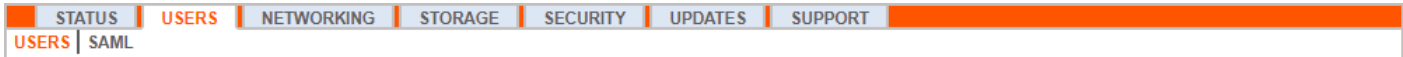
**Hinweis:** Die Registerkarte **Systemzustand** ist nur für Seiten sichtbar, die von einem PRA Virtual Appliance oder Cloud Appliance unterstützt werden.

Auf der Seite **Systemzustand** können Sie den Status Ihres virtuellen Geräts oder Cloud Appliance 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 B Series Appliance verbessern können.

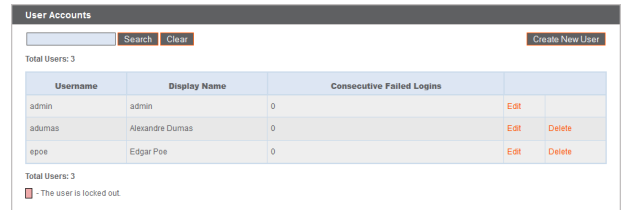
### Hardware Health

	Value	Status	Notes
<b>CPU</b>	Count: 8 Model: Intel(R) Xeon(R) CPU E5-2697 v3 @ 2.60GHz Speed: 2593.993 MHz Reservation: 0 MHz Limit: Unlimited		<ul style="list-style-type: none"> <li>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.</li> </ul>
<b>Memory</b>	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		<ul style="list-style-type: none"> <li>Memory swapping could indicate that this appliance is undersized for the current workload.</li> <li>Consider allocating a Memory Reservation to this VM for the full amount of physical memory to avoid host swapping, which is detrimental to performance.</li> </ul>
<b>Storage</b>	Total Space: 279.998 GiB		

# Benutzer: Passwort und Benutzername ändern, Benutzer hinzufügen, Benutzer löschen

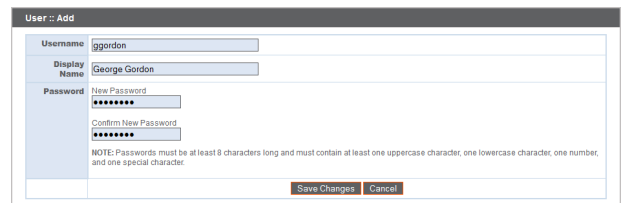


Auf der Seite **Benutzer** können Sie Administratoren für die /appliance-Schnittstelle hinzufügen, bearbeiten oder löschen. Auch können Sie den Benutzernamen, Anzeigenamen und das Passwort eines Administrators ändern. BeyondTrust empfiehlt, das Passwort regelmäßig zu ändern, um sich vor unberechtigtem Zugriff zu schützen.



Username	Display Name	Consecutive Failed Logins	
admin	admin	0	Edit
adumas	Alexandre Dumas	0	Edit Delete
epoe	Edgar Poe	0	Edit Delete

Total Users: 3  
 - The user is locked out.



**User:: Add**


Username:

Display Name:

Password:

Confirm New Password:

NOTE: Passwords must be at least 8 characters long and must contain at least one uppercase character, one lowercase character, one number, and one special character.

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


 Zum Festlegen von Konto einschränkungsregeln, einschließlich Passwort-Ablaufdatum und Verlauf, siehe „Geräteverwaltung: Einschränkungen von Konten, Netzwerken und Ports, Aktivieren eines STUN-Servers, Einrichten von Syslogs, Aktivieren der Anmeldevereinbarung, Zurücksetzen des Administratorkontos“ auf Seite 27.




# SAML: Einrichten der Benutzer-Authentifizierung über einen SAML-Identitätsanbieter



Konfigurieren Sie Ihr B Series Appliance 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.

 **Tip:** 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 B Series Appliance einen privaten Schlüssel und ein Zertifikat generiert, wählen Sie **Privaten Schlüssel generieren** und klicken Sie auf **Änderungen speichern**. Klicken Sie 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 Passwort ein. Sie müssen dasselbe Zertifikat auf Ihren Identitätsanbieter hochladen.

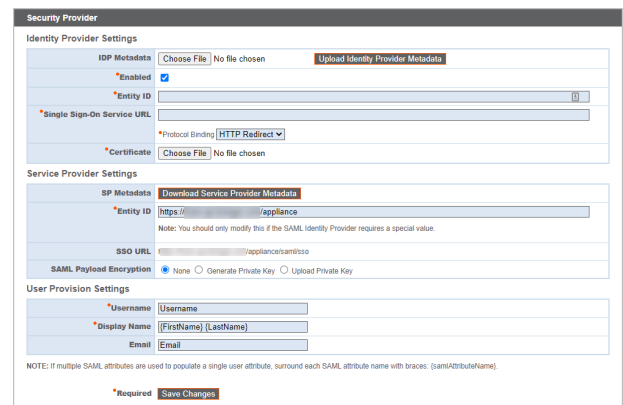
Nachdem Sie die Anwendung auf Ihrem Identitätsanbieter gespeichert haben, haben Sie vielleicht die Möglichkeit, deren Metadaten herunterzuladen. Ist dies der Fall, laden Sie diese Datei über die Schaltfläche **Identitätsanbieter-Metadaten hochladen** in Ihr B Series Appliance hoch. Kopieren Sie alternativ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

 **Tip:** 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 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 zugewiesen 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

STATUS	USERS	<b>NETWORKING</b>	STORAGE	SECURITY	UPDATES	SUPPORT
<b>IP CONFIGURATION</b>	STATIC ROUTES	SNMP				

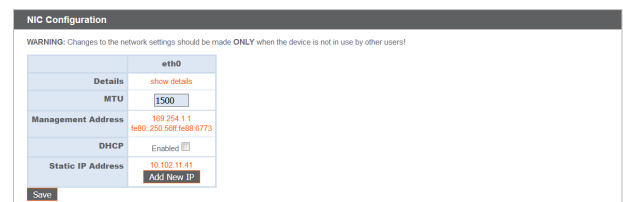
Unternehmen mit erweiterten Netzwerkkonfigurationen können mehrere IP-Adressen auf den Ethernet-Ports des B Series Appliances konfigurieren. Die Verwendung mehrerer Ports kann die Sicherheit verbessern oder Verbindungen über nicht standardmäßige Netzwerke ermöglichen. Wenn z. B. Mitarbeiter ohne Internet-Zugriff 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.

NIC-Teaming kombiniert die physischen NICs Ihres Systems in einer einzigen logischen Schnittstelle. NIC-Teaming wird im aktiven Backup-Modus durchgeführt. Eine der NICs wird für den gesamten Netzwerkverkehr verwendet. 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 Appliance-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 am gleichen Subnetz konfigurieren möchten, verwenden Sie NIC-Teaming.

Standardmäßig ist das Dynamische Hostkonfigurationsprotokoll (DHCP) für Ihr B Series Appliance 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.

 Um mehr über DHCP zu erfahren, lesen Sie weiter unter [Was ist DHCP?](https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/dd145320(v=ws.10)) unter [docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/dd145320\(v=ws.10\)](https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/dd145320(v=ws.10)).


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

NIC Configuration				
WARNING: Changes to the network settings should be made ONLY when the device is not in use by other users!				
eth0		eth1		
<b>Details</b>	Interface	eth0	Interface	eth1
	MAC Address	00:30:48:b8:ce:1c	MAC Address	00:30:48:b8:ce:1d
	Link Detected	Yes	Link Detected	No
	Link Speed	1000 Mbps	Link Speed	
	Link Duplex	Full	Link Duplex	
	RX packets	37500912	RX packets	0
	RX bytes	969386669	RX bytes	0
	RX errors	0	RX errors	0
	RX dropped	149950	RX dropped	0
	TX packets	7902467	TX packets	0
	TX bytes	3252030706	TX bytes	0
	TX errors	0	TX errors	0
	TX dropped	0	TX dropped	0
	Collisions	0	Collisions	0
	MTU	1500	MTU	1500
	Management Address	169.254.1.1 fe80::202:46f:b0b8:ce1c	Management Address	none
	IP Address	10.10.28.240	IP Address	192.168.1.213 [disabled]
		<a href="#">Add New IP</a> <a href="#">Save</a>		

Enable NIC Teaming  
 NOTE: NIC Teaming allows you to combine your system's physical NICs into a single logical NIC. This operates in "Active-Backup" mode. One of the NICs will be used to carry all network traffic. If the link on that NIC is lost for any reason, the other NIC will become active. Before activating NIC Teaming, please ensure that both NICs are connected to the same network segment (subnet), and that you only have IP addresses configured on one of the existing NICs.  
[Save](#)

Konfigurieren Sie im Abschnitt **Globale Netzwerkkonfiguration** den Hostnamen für Ihr B Series Appliance.

Global Network Configuration	
Hostname	<input type="text" value="bongmr.com"/>
IPv4 Default Gateway	<input type="text" value="0.0.0.0"/> Using Device: <input type="text" value="eth0"/>
IPv6 Default Gateway	<input type="text" value="::"/> Using Device: <input type="text" value="eth0"/>
Custom DNS Servers	<input type="text" value="::"/>
	<small>NOTE: Optional. Enter a list of IP addresses, one per line, to be used for DNS lookups.</small>
Fallback to Public DNS Servers	<input type="checkbox"/>
	<small>NOTE: If no DNS servers are configured above, or if they are unreachable, enabling this setting will cause the Secure Remote Access Appliance to use the publicly-available DNS servers from OpenDNS. For more information about OpenDNS, please visit <a href="http://www.opendns.com">www.opendns.com</a>.</small>
Respond to Ping	<input checked="" type="checkbox"/>
NTP Server	<input type="text" value="clock.bongmr.com"/>
	<small>Last synchronized 716 seconds ago (+7:03min offset) NOTE: This setting is used to keep the system clock in sync with an NTP time server. You may enter a single hostname or IP address. "clock.bongmr.com" is the default.</small>
	<a href="#">Save Changes</a>
<small>WARNING: Changes to the network settings should be made ONLY when the device is not in use by other users!</small>	

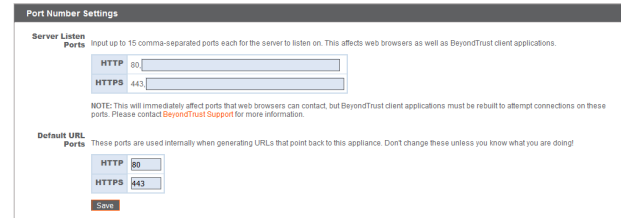
 **Hinweis:** Das Feld **Hostname** muss keine technischen Anforderungen erfüllen. Es hat keine Auswirkungen darauf, mit welchem Hostnamen Client-Anwendungen oder Remote-Benutzer sich verbinden. Wenn der von der Client-Software verwendete Hostname geändert werden muss, benachrichtigen Sie den BeyondTrust Technical Support über die benötigten Änderungen, damit der Support eine Softwareaktualisierung bereitstellen kann. Das Feld **Hostname** existiert hauptsächlich, damit Sie zwischen mehreren B Series Appliances 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 B Series Appliances 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 öffentliche DNS-Server zurück verschieben** des B Series Appliance die Möglichkeit geben, öffentlich verfügbare DNS-Server von OpenDNS zu verwenden.

 Besuchen Sie für weitere Informationen zu OpenDNS bitte [www.opendns.com](http://www.opendns.com).

Geben Sie Ihrem B Series Appliance 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 B Series 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.

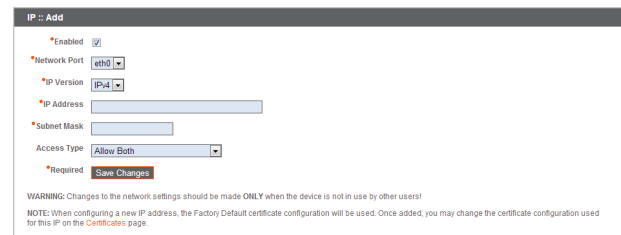


Der Bereich **Server-Listen-Ports** ermöglicht es Ihnen, Ports zu konfigurieren, die das B Series Appliance überprüft. Sie können bis zu 15 durch Komma getrennte Ports für HTTP und 15 durch Komma getrennte Ports für HTTPS angeben. Jeder Port darf nur einmal in maximal einem Feld erscheinen. Das B Series Appliance reagiert auf HTTP-Verbindungen zu einem der im HTTP-Feld aufgeführten Ports und das B Series Appliance reagiert 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 auf das B Series Appliance zuzugreifen, nutzen Sie einen Browser, der die Angabe des Ports in der URL zulässt (z. B. support.example.com:8200). Über das B Series Appliance 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 B Series Appliance 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 B Series Appliance zeigen, wie etwa über die access console 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 B Series Appliance 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 B Series Appliance sollten Sie festlegen, ob diese IP-Adresse als **Primär** festgelegt werden soll. Ist diese Option aktiviert, legt das B Series Appliance diese IP-Adresse als primäre oder ursprüngliche IP-Adresse für das Subnetz fest. Dies stellt beispielsweise sicher, dass jeglicher Netzwerkverkehr vom B Series Appliance 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<sup>1</sup>, 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: <b>FIPS-Fehler anzeigen</b> , <b>Gerät auf Originalstandards zurücksetzen</b> , <b>Herunterfahren</b> und <b>Neustart</b>
Deaktiviert	Deaktiviert den Telnet-Server vollständig

<sup>1</sup>Die Management-IP-Adresse darf nicht gelöscht oder modifiziert werden.

## SNMP: Simple Management Network Protocol aktivieren



Das BeyondTrust Appliance B Series unterstützt das Simple Network Management Protocol (SNMP). Das SNMP ist ein Internet-Standard-Protokoll, das zur Überwachung und Verwaltung von Netzwerkgeräten verwendet wird.

Hiermit können Tools, die Verfügbarkeitsdaten und andere Statistiken über das SNMP-Protokoll erfassen, das B Series Appliance zu Überwachungszwecken abfragen.

Um SNMP für dieses B Series Appliance zu aktivieren, wählen Sie **SNMPv2 aktivieren** oder **SNMPv3 aktivieren**. Hierdurch kann ein SNMPv2- oder v3-Server auf SNMP-Anfragen reagieren. Geben Sie einen Wert für **den schreibgeschützten Community-Namen**, den **Systemspeicherort** und die **IP-Beschränkungen** für IP-Adressen ein, die zur Abfrage dieses B Series Appliances mit SNMP berechtigt sind.



**Hinweis:** Allen Hosts wird Zugriff gewährt, wenn keine IP-Adressen im Feld **IP-Beschränkungen** eingegeben werden.

Bei der Auswahl von SNMPv3:

1. Geben Sie einen **Benutzernamen** und ein **Passwort** ein.
2. Wählen Sie im Dropdown-Menü die gewünschte **Authentifizierungsmethode** aus.
3. Aktivieren Sie **SNMPv3 Privatsphäre aktivieren**, wenn Sie die Kommunikation zum Client verschlüsseln möchten.
4. Geben Sie ein **Privatsphärenpasswort** ein und wählen Sie eine **Privatsphärenmethode**.

Wenn Sie fertig sind, klicken Sie auf **Änderungen speichern**.



Weitere Informationen zu SNMP finden Sie in [Simple Network Management Protocol](#) unter [wikipedia.org/wiki/Simple\\_Network\\_Management\\_Protocol](https://wikipedia.org/wiki/Simple_Network_Management_Protocol).

## Networking :: SNMP Configuration

**Enable SNMPv2**   
Enable the SNMPv2 server on this appliance.

• **SNMPv2 Read-Only Community Name**

**Enable SNMPv3**   
Enable the SNMPv3 server on this appliance.

• **SNMPv3 Username**

• **SNMPv3 Authentication Password**   
NOTE: Leave blank to keep the current password.

• **SNMPv3 Authentication Method**

**SNMPv3 Enable Privacy**   
Enable SNMPv3 privacy, which encrypts communication to the client.

• **SNMPv3 Privacy Password**   
NOTE: Leave blank to keep the current password.

• **SNMPv3 Privacy Method**

• **System Location**

**IP Restrictions**

Enter IP addresses that should be allowed to access SNMP on this appliance. Enter the IP Addresses, one entry per line, in the form "IP\_Address/Prefix\_Length". The Prefix Length should be an integer. If no entries are provided, all hosts will be granted access.

• **Required**



## Statische Routen: Einrichten von statischen Routen zur Netzwerkkommunikation

STATUS	USERS	<b>NETWORKING</b>	STORAGE	SECURITY	UPDATES	SUPPORT
IP CONFIGURATION	<b>STATIC ROUTES</b>	SNMP				

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 B Series Appliance mit einem Computer auf dem anderen Netzwerk verbinden kann, vorausgesetzt, das B Series Appliance befindet sich an einem Ort, an dem beide Netzwerke individuell mit ihm kommunizieren können.

Nur fortgeschrittene Administratoren sollten versuchen, statische Routen festzulegen.

**Static Routes**

**IPv4**

Destination Network	Netmask	Next Hop	Interface
<input type="text" value="0.0.0.0"/>	<input type="text" value="0"/>	<input type="text" value="10.102.10.1"/>	eth0
<input type="text"/>	<input type="text"/>	<input type="text"/>	eth0

**IPv6**

Destination Network	Prefix Length	Next Hop	Interface
<input type="text"/>	<input type="text"/>	<input type="text"/>	eth0

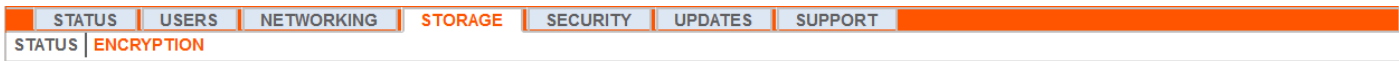
**NOTE:** This is used for advanced network configuration. Take care to define things correctly. To delete an existing route clear all the fields, and save the changes.

**WARNING:** Changes to the network settings should be made **ONLY** when the device is not in use by other users!

 **Hinweis:** Statische Routen können auch über die Konsole erstellt werden. Weitere Informationen finden Sie unter [Konsolen-Konfiguration für sicheren Remote-Zugriff auf https://www.beyondtrust.com/de/docs/privileged-remote-access/getting-started/deployment/hardware-sra/console.htm](https://www.beyondtrust.com/de/docs/privileged-remote-access/getting-started/deployment/hardware-sra/console.htm).

# Speicher

## Status: Speicherplatz und Festplattenstatus



Die Seite **Status** zeigt den Prozentsatz des belegten Festplattenspeichers Ihres B Series Appliance an.

**Virtual Disks**

**Physical Disk 0**

This disk holds all of the system files and programs.

24% Used

**Physical Disk 1**

This disk holds all of the BeyondTrust session data specific to your installation. Disk usage of 85 - 95 percent is not fatal, and is in fact common. If this disk approaches its capacity, the BeyondTrust Appliance will automatically purge the oldest session reporting data to recycle space. To increase the length of time that data is kept on this BeyondTrust Appliance, increase the size of this virtual disk.

4% Used

Wenn Sie alle Aufzeichnungsfunktionen auf Ihren Support-Sites (Sitzung, Protokoll-Tunneling 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 B Series Appliance ist so konfiguriert, dass bei Speicherknappheit auf der Festplatte automatisch die ältesten Sitzungsdaten gelöscht werden und der Speicher für neue Sitzungsdaten freigemacht wird.

## Spezifisch für das BeyondTrust B300P B Series Appliance

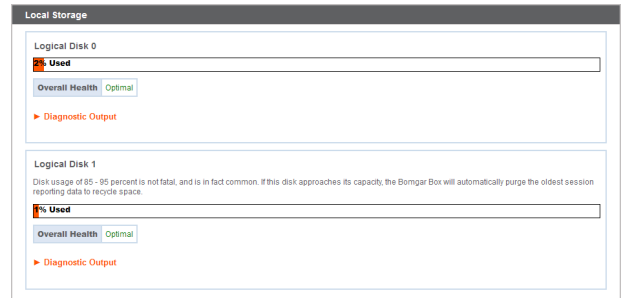
Das B300P verwendet ein RAID-System, um Ihre Daten zu sichern. RAID 6 wird verwendet, damit dem B Series Appliance selbst beim Verlust von 2 seiner 4 Laufwerke keine Daten verloren gehen. Entfernen Sie bei einem Ausfall die beschädigte Festplatte und wenden Sie sich an BeyondTrust, um eine Rücksendegenehmigung einzuholen und die Festplatte reparieren oder ersetzen zu lassen. Wenn Sie das beschädigte Laufwerk ersetzen, baut das B Series Appliance den RAID automatisch mithilfe des neuen Laufwerks erneut auf. Das Ausschalten des B Series Appliances beim Auswechseln der Festplatten ist nicht erforderlich.



## Spezifisch für das BeyondTrust B400P B Series Appliance

Das B400P 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 B300P und B400P)

Die LEDs auf Ihrem B Series Appliance 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.

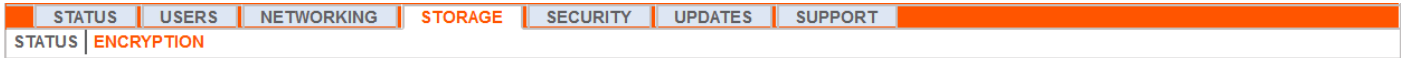


**Hinweis:** Die Schaltfläche **Alarm stumm schalten** ist unabhängig davon verfügbar, ob aktuell ein Alarm ertönt. Die Schaltfläche kennzeichnet nicht, ob aktuell ein Alarm aktiv ist.



**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 B Series Appliance ertönt und Sie das B Series Appliance als Quelle ausschließen möchten, klicken Sie mehrfach auf die Schaltfläche **Alarm stumm schalten**, um jegliche möglicherweise aktiven Alarmer zu deaktivieren.

## Verschlüsselung: Verschlüsseln von Sitzungsdaten



Im Bereich **Verschlüsselung** können Sie Sitzungsdaten auf Ihrem B Series 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 hinzugefügt 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 den BeyondTrust Technical Support unter [www.beyondtrust.com/support](http://www.beyondtrust.com/support).

### Storage :: Encryption

Storage Encryption Status: **Not Encrypted**

[Encrypt](#)

*Encryption keys are managed by Secret Store*

# Sicherheit

## Zertifikate: Erstellen und Verwalten von TLS-Zertifikaten

STATUS	USERS	NETWORKING	STORAGE	<b>SECURITY</b>	UPDATES	SUPPORT
<b>CERTIFICATES</b>	TLS CONFIGURATION	APPLIANCE ADMINISTRATION	EMAIL CONFIGURATION	SECRET STORE		

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

### Zertifikat-Installation

Das BeyondTrust Appliance B Series wird mit einem bereits installierten selbstsignierten Zertifikat geliefert. Um Ihr B Series 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

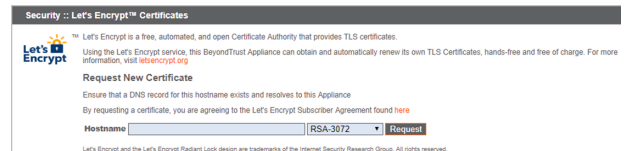
Let's Encrypt stellt signierte Zertifikate aus, die für 90 Tage gültig sind, aber die Fähigkeit haben, sich auf unbestimmte Zeit automatisch selbst zu verlängern. Um ein Let's Encrypt-Zertifikat anzufordern oder in Zukunft zu verlängern, müssen Sie folgende Anforderungen erfüllen:

- Der DNS für den angeforderten Hostnamen muss zum B Series Appliance aufgelöst werden.
- Das B Series Appliance muss Let's Encrypt auf TCP 443 erreichen können.
- Let's Encrypt muss das B Series Appliance auf TCP 80 erreichen können.


 Weitere Informationen finden Sie in [letsencrypt.org](https://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 Domännennamen (FQDN) des B Series Appliances 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 B Series Appliance startet den Zertifikatverlängerungsprozess 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 B Series Appliance 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 B Series Appliance gleichzeitig verwendet werden kann und da ein B Series Appliance 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-B Series Appliance-Paaren zu vermeiden.



**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, zertifikatfreundlicher Name 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 Domännennamen wie `access.example.com` oder als Platzhalterzeichen-Domännennamen wie `*.example.com`. Ein Platzhalterzeichen-Domänenname deckt mehrere Unterdomänen wie `access.example.com`, `remote.example.com` und so weiter ab.

Klicken Sie auf **Zertifikatanfrage 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 B Series Appliance installieren müssen.

Um Ihre neuen Zertifikatdateien 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 B Series 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.“

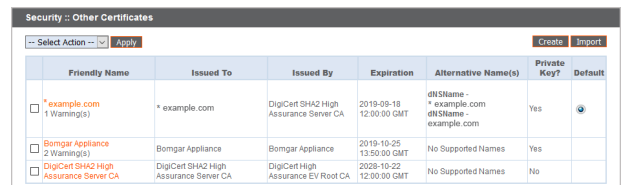
Um das Root-Zertifikat für Ihr B Series Appliance-Zertifikat herunterzuladen, überprüfen Sie die von der Zertifizierungsstelle gesandten Informationen auf einen Link zum entsprechenden Zertifikat. Sollte es nicht vorhanden sein, kontaktieren Sie die Zertifizierungsstelle. Sollte dies nicht möglich sein, suchen Sie auf der Website 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 ausfindig. Laden Sie es danach aus dem Root-Speicher der Zertifizierungsstelle herunter und importieren Sie es wie oben beschrieben in Ihrem B Series Appliance.

## Zertifikate

Zeigen Sie eine Tabelle der auf Ihrem B Series Appliance 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 B Series Appliance sein, das für die Erstinstallation bereitgestellt wurde.

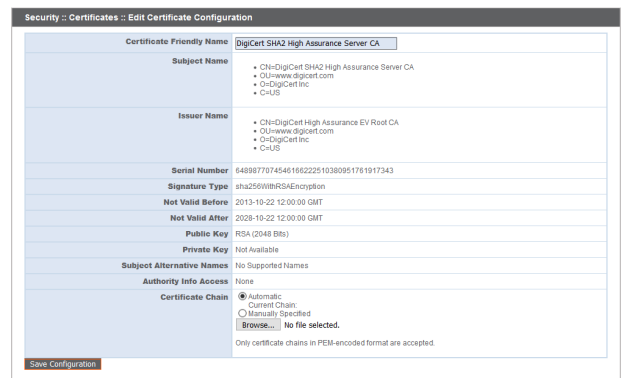


	Friendly Name	Issued To	Issued By	Expiration	Alternative Name(s)	Private Key?	Default
<input type="checkbox"/>	* example.com 1 Warning(s)	* example.com	DigiCert SHA2 High Assurance Server CA	2019-09-18 12:00:00 GMT	* example.com * example.com	Yes	<input checked="" type="radio"/>
<input type="checkbox"/>	Bomgar Appliance 2 Warning(s)	Bomgar Appliance	Bomgar Appliance	2019-10-25 13:50:00 GMT	No Supported Names	Yes	<input type="radio"/>
<input type="checkbox"/>	DigiCert SHA2 High Assurance Server CA	DigiCert SHA2 High Assurance Server CA	DigiCert High Assurance EV Root CA	2028-10-22 12:00:00 GMT	No Supported Names	No	<input type="radio"/>



Um mehr über SNI zu erfahren, lesen Sie weiter unter [Server Name Indication](https://cio.gov/sni/) unter <https://cio.gov/sni/>.

Klicken Sie auf einen Zertifikatnamen, um Einzelheiten dazu anzuzeigen und die Zertifikatkette zu verwalten.



Security :: Certificates - Edit Certificate Configuration

Certificate Friendly Name: DigiCert SHA2 High Assurance Server CA

Subject Name:

- CH=DigiCert SHA2 High Assurance Server CA
- O=www.digicert.com
- C=DigiCert Inc
- C=US

Issuer Name:

- CH=DigiCert High Assurance EV Root CA
- O=www.digicert.com
- C=DigiCert Inc
- C=US

Serial Number: 6488877074546166222510380951761917343

Signature Type: sha256WithRSAEncryption

Not Valid Before: 2013-10-22 12:00:00 GMT

Not Valid After: 2028-10-22 12:00:00 GMT

Public Key: RSA (2048 Bits)

Private Key: Not Available

Subject Alternative Names: No Supported Names

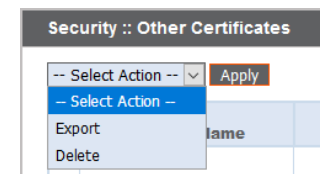
Authority Info Access: None

Certificate Chain:
 Automatic Current Chain  
 Manually Specified  
 No file selected.

Only certificate chains in PEM-encoded format are accepted.

Save Configuration

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**.



Security :: Other Certificates

-- Select Action -- Apply

-- Select Action --

Export

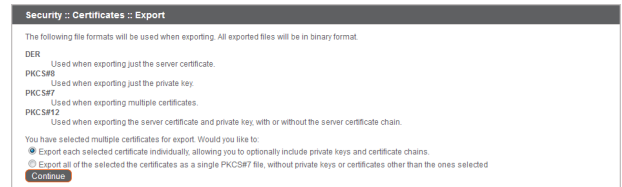
Delete

Wenn Sie nur ein Zertifikat exportieren, können Sie sofort auswählen, das Zertifikat oder die Zertifikatkette einzubeziehen, falls verfügbar. Klicken Sie auf **Exportieren**, um den Download zu starten.

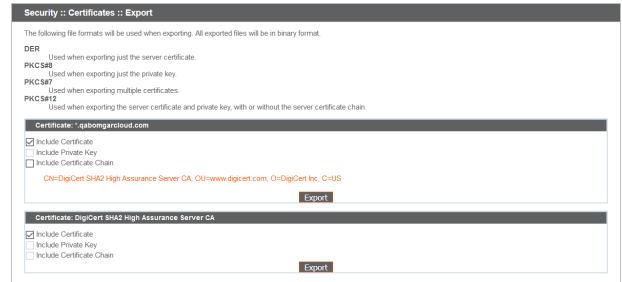


Wenn Sie mehrere Zertifikate exportieren, haben Sie die Möglichkeit, jedes Zertifikat einzeln oder in einer einzigen PKCS#7-Datei zu exportieren.

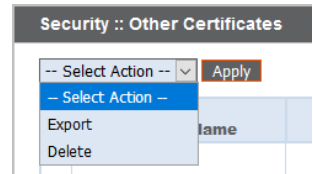
Wenn Sie auswählen, mehrere Zertifikate als eine Datei zu exportieren, klicken Sie auf **Weiter**, um den Download zu starten. Mit dieser Option werden nur die eigentlichen Zertifikatdateien ohne Zertifikatketten exportiert.




Um 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 und/oder die Zertifikatkette einzubeziehen, je nach Verfügbarkeit. Klicken Sie auf **Exportieren**, um den Download zu starten.



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

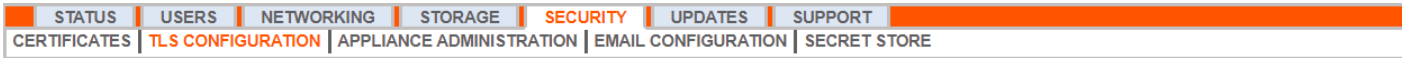
Zeigen Sie eine Tabelle der ausstehenden Anfragen für von Drittparteien signierte Zertifikate an. Klicken Sie auf den Namen der Zertifikatsanfrage, um die Details anzuzeigen.

Certificate Requests		
Subject	Alternative Name(s)	Fingerprint
<input type="checkbox"/> CN=Support example.org, OU=Potato Peeling Division, O=The Example Company, L=Ridgeland, ST=MS, C=US	• dNStName - *example.org	a23c05f1a7a6da31146a019ea07047590b6ac
<input type="checkbox"/> CN=Support example.net, OU=Potato Peeling Division, O=The Example Company, L=Ridgeland, ST=MS, C=US	• dNStName - *example.net	a6c2c79523647e106d52d37e2cc262e64805d51





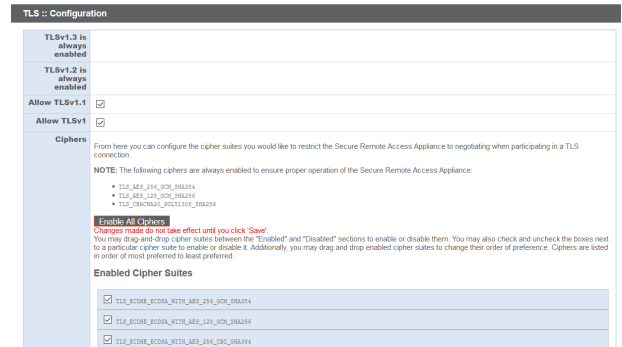
## TLS-Konfiguration: Wählen Sie TLS-Codes und Versionen



Beachten Sie, dass einige ältere Browser TLSv1.2 und TLSv1.3 nicht unterstützen. 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.

Diese Einstellungen beeinflussen hauptsächlich die Verbindungen mit der Webschnittstelle Ihres B Series Appliance. 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 B Series Appliance aktiviert bzw. deaktiviert werden sollen. Sie können die bevorzugte Reihenfolge der Ciphersuites mittels Ziehen und Ablegen ändern. Änderungen an den Ciphersuites werden erst wirksam, nachdem Sie auf die Schaltfläche **Speichern** geklickt haben.



# Geräteverwaltung: Einschränken von Konten, Netzwerken und Ports, Aktivieren eines STUN-Servers, Einrichten von Syslogs, Aktivieren der Anmeldevereinbarung, Zurücksetzen des Administratorkontos

STATUS	USERS	NETWORKING	STORAGE	SECURITY	UPDATES	SUPPORT
CERTIFICATES	TLS CONFIGURATION	APPLIANCE ADMINISTRATION	EMAIL CONFIGURATION	SECRET STORE		

Kontrollieren Sie den Zugriff auf die /appliance-Verwaltungsschnittstelle, indem Sie festlegen, wie viele fehlgeschlagenen Anmeldungen gestattet sind. Legen Sie fest, wie lange ein Konto nach Überschreitung dieser Zahl gesperrt wird. Legen Sie ebenfalls die Anzahl der Tage fest, für die ein Passwort vor Ablauf verwendet werden kann, und schränken Sie die Nutzung bereits verwendeter Passwörter ein.

Sie können den Zugriff auf die Verwaltungsschnittstelle Ihres B Series Appliances 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 aufgeführte 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 BeyondTrust Appliance B Series 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.

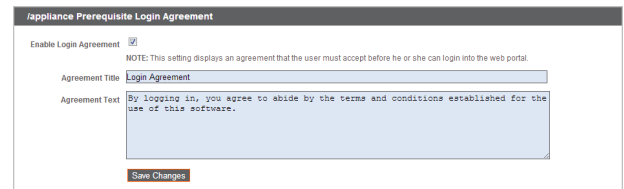
Sie können Ihr B Series Appliance zum Senden von Protokollnachrichten an bis zu drei Syslog-Server konfigurieren. Geben Sie den Hostnamen oder die IP-Adresse des Syslog-Hostservers, der Systemnachrichten von diesem B Series Appliance empfängt, im Feld **Remote-Syslog-Server** ein. Wählen Sie das Datenformat für die Ereignisbenachrichtigungsmeldungen. 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 Standardwerte können geändert werden. Die B Series Appliance-Protokolle werden mit Hilfe der Funktion **local0** versendet.

**i** Cloud-spezifische Einstellungen finden Sie in [B Series Appliance-Verwaltung: Syslog über TLS festlegen](https://www.beyondtrust.com/docs/privileged-remote-access/getting-started/deployment/cloud/syslog-over-tls.htm) unter <https://www.beyondtrust.com/docs/privileged-remote-access/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.

**i** Eine detaillierte Syslog-Nachrichtenreferenz finden Sie im [Syslog-Nachrichtenhandbuch](https://www.beyondtrust.com/docs/privileged-remote-access/how-to/integrations/syslog/) unter [www.beyondtrust.com/docs/privileged-remote-access/how-to/integrations/syslog/](https://www.beyondtrust.com/docs/privileged-remote-access/how-to/integrations/syslog/).

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



## E-Mail-Konfiguration: Konfiguration des B Series Appliances für das Senden von E-Mail-Benachrichtigungen

STATUS	USERS	NETWORKING	STORAGE	SECURITY	UPDATES	SUPPORT
CERTIFICATES	TLS CONFIGURATION	APPLIANCE ADMINISTRATION	EMAIL CONFIGURATION	SECRET STORE		

Ihr B Series Appliance kann Ihnen automatische E-Mail-Benachrichtigungen senden. 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.

### Konfigurieren über SMTP



**Hinweis:** Bei einigen E-Mail-Diensten funktioniert diese Methode nicht. Siehe „Konfigurieren über OAuth2 für Microsoft Azure AD“ auf Seite 29 oder „Konfigurieren über OAuth2 für Google“ auf Seite 32 für alternative Konfigurationen.

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.

**Security :: Admin Contact**

**Admin Contact Email** Enter email addresses, one per line, to be notified of important System events

Send a test email when the settings are saved.

**Save Changes**

### Konfigurieren über OAuth2 für Microsoft Azure AD

Die Konfiguration erfordert eine Änderung der Einstellungen auf der BeyondTrust Anwendung und dem Microsoft 365-Abonnement mit Azure AD.

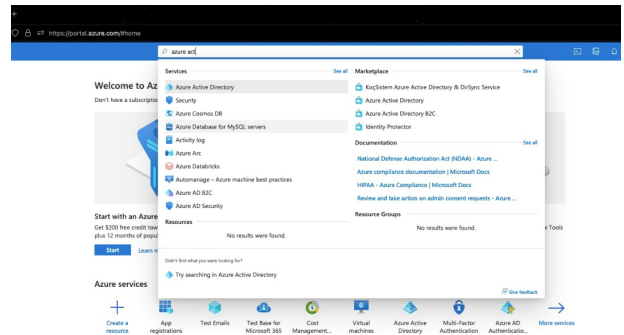
Ändern Sie zunächst die Einstellungen des BeyondTrust Geräts:

1. Gehen Sie zu **Gerät**, klicken Sie auf die Registerkarte **Sicherheit** und dann auf **E-Mail-Konfiguration**.
2. Ändern Sie die **Authentifizierungsmethode** in OAuth2
3. Beachten Sie den **Authorization Redirect URI**. Er wird später benötigt.

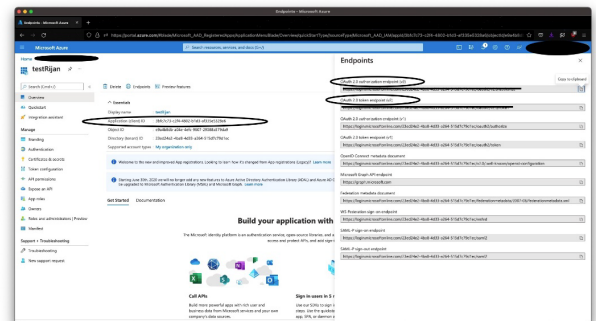
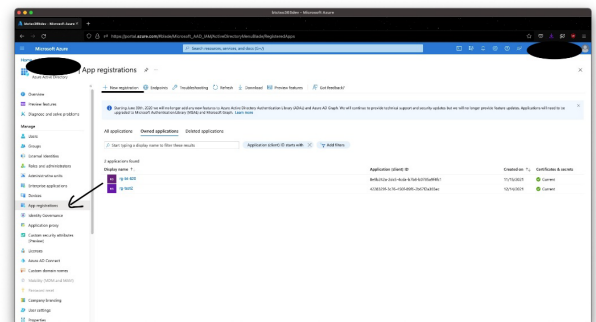
Bevor Sie mit der Konfiguration auf Azure Active Directory beginnen, muss ein Azure/Office 365-Administrator-authentifiziertes SMTP für jedes Konto auf Exchange online aktivieren. Gehen Sie dazu zu **Office 365 Admin Portal ([admin.microsoft.com](https://admin.microsoft.com)) > Aktive Benutzer > Mail > E-Mail-Anwendungen verwalten** und aktivieren Sie **Authentifiziertes SMTP**.

Sobald **Authentifiziertes SMTP** aktiviert ist, führen Sie die folgenden Schritte in der Azure-Konsole durch:

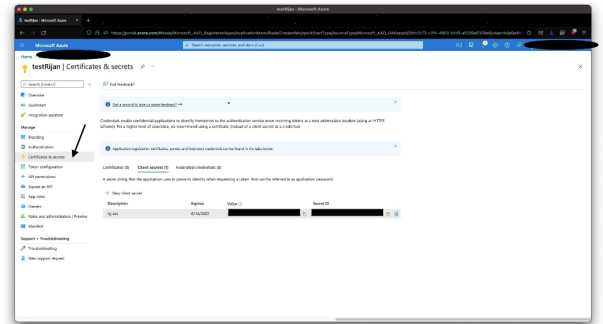
4. Melden Sie sich bei Ihrer Azure-Konsole an ([portal.azure.com](https://portal.azure.com)).
5. Gehen Sie zu **Azure Active Directory**.



6. Gehen Sie zu **App-Registrierungen** und wählen Sie **Neue Registrierung**.
7. Geben Sie einen Namen ein, z. B. **Gerät-OAuth2**.
8. Wählen Sie die Kontotypen aus, mit denen Sie sich über OAuth2 bei der Anwendung anmelden können möchten. Wählen Sie **Single Tenant** für nur intern.
9. Geben Sie den **URI Weiterleitung** ein. Dies ist der **Autorisierungsumleitungs-URI**, der zu Beginn dieses Prozesses von der BeyondTrust Gerätesoftware erhalten wurde.
10. Klicken Sie auf **Registrieren**.
11. Auf der **Übersichtsseite** (ausgewählt aus dem linken Menü) die **Anwendungs-(Client-)ID**. Er wird später benötigt.
12. Klicken Sie auf **Endpunkte** (oberhalb der **Anwendungs-(Client-)ID**).
13. Beachten Sie den **OAuth2.0 Autorisierungsendpunkt (v2) URI** und den **OAuth-Token-Endpunkt (v2) URI**. Diese werden später benötigt.




14. Beachten Sie auf der Seite **Zertifikate & Secrets** (aus dem linken Menü ausgewählt) das **Client-Secret**. Er wird später benötigt. Wenn Sie kein **Client-Secret** haben, klicken Sie auf **New Client-Secret**, um eines zu erstellen.




Die übrigen Schritte werden auf der BeyondTrust-Anwendung durchgeführt.

15. Gehen Sie zu **Gerät**, klicken Sie auf die Registerkarte **Sicherheit** und dann auf **E-Mail-Konfiguration**.
16. Geben Sie die folgenden, bereits erwähnten Informationen ein:
  - **Autorisierungsendpunkt**
  - **Token-Endpunkt**
  - **Client-ID**
  - **Client-Secret**
17. Geben Sie die E-Mail-Adresse für diesen Dienst als **Sende von E-Mail-Adresse** und die **Benutzer-E-Mail** ein.

 **Hinweis:** Diese Adressen müssen übereinstimmen und ein gültiges Konto für Azure sein. Wenn Sie für den Azure-Tenant die Option *Anonyme E-Mail (E-Mail als Jeder senden)* aktiviert haben, können Sie in das Feld *E-Mail* senden alles eingeben. Ist dies nicht der Fall, verwenden Sie den Benutzernamen des Anwendungseigentümers und die zulässigen Benutzer.

18. Geben Sie Daten für die Felder **Host**, **Verschlüsselung** und **Port** ein.
  - **Host:** smtp.office365.com
  - **Verschlüsselung:** STARTTLS
  - **Port:** 587

 **Hinweis:** Es werden Standarddaten für Azure angezeigt, aber Ihre Installation verwendet möglicherweise einen anderen Host oder eine andere Verschlüsselungsmethode. Der Port gilt für STARTTLS, aber andere Verschlüsselungsmethoden können einen anderen Port verwenden.

19. Geben Sie Ihr TLS-Zertifikat ein, wenn Sie eines haben. Wenn nicht, markieren Sie **TLS-Zertifikatsfehler ignorieren**.
20. Geben Sie für **Scopes** Folgendes ein: https://outlook.office.com/SMTP.Send offline\_access
21. Klicken Sie auf **Änderungen speichern**.
22. Klicken Sie auf **Autorisieren**. Akzeptieren Sie auf der daraufhin angezeigten Anmeldeseite die Berechtigungsanfrage. Die Seite mit den E-Mail-Einstellungen wird neu geladen, und die Schaltfläche zur Autorisierung wird durch eine autorisierte Nachricht ersetzt.
23. Zum Testen der Konfiguration:
  - Fügen Sie eine **Admin-Kontakt-E-Mail** hinzu.
  - Markieren Sie **Eine Test-E-Mail senden**.

- Klicken Sie auf **Änderungen speichern**.

## Konfigurieren über OAuth2 für Google

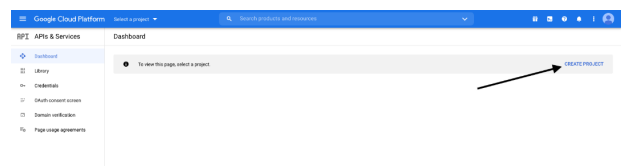
Die Konfiguration erfordert die Änderung von Einstellungen auf dem BeyondTrust Gerät und der Google Cloud Platform.

Ändern Sie zunächst die Einstellungen des BeyondTrust Geräts:

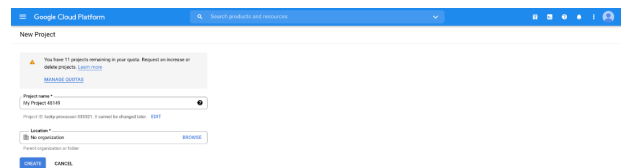
1. Gehen Sie zu **Gerät**, klicken Sie auf die Registerkarte **Sicherheit** und dann auf **E-Mail-Konfiguration**.
2. Ändern Sie die **Authentifizierungsmethode** in OAuth2
3. Beachten Sie den **Authorization Redirect URI**. Er wird später benötigt.

Melden Sie sich nun bei Ihrer Google Cloud Platform-Konsole (Google Dev Console) an ([console.cloud.google.com](https://console.cloud.google.com)). Verwenden Sie das richtige Gmail-Konto, da nur der Eigentümer des Projekts mit dem Projekt arbeiten kann. Wenn Sie noch kein bezahltes Konto haben, können Sie ein Konto erwerben, indem Sie auf **Aktivieren** im oberen Banner klicken. BeyondTrust kann Ihnen beim Kauf eines Kontos nicht behilflich sein. Klicken Sie auf **Mehr erfahren** im oberen Banner, um Informationen über die Einschränkungen der kostenlosen Konten zu erhalten.

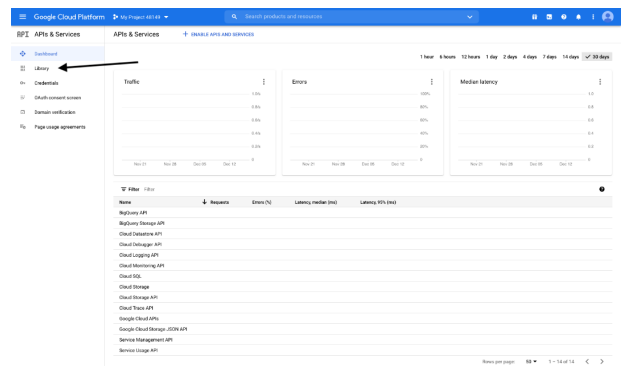
4. Klicken Sie auf **PROJEKT ERSTELLEN**. Sie können auch ein bestehendes Projekt verwenden.



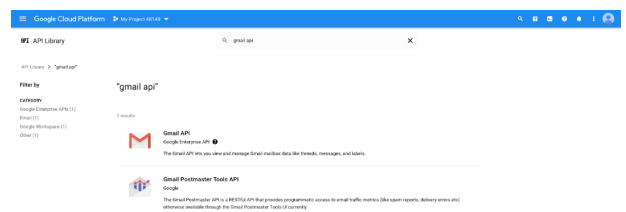
5. Akzeptieren Sie den Standard **Projektname** oder geben Sie einen Namen ein.
6. Akzeptieren Sie die Standardeinstellung **Speicherort** oder wählen Sie einen der für Ihr Unternehmen verfügbaren Ordner.
7. Klicken Sie auf **ERSTELLEN**.



8. Die Seite **APIs und Dienste** wird angezeigt. Klicken Sie im linken Menü auf **Bibliothek**.

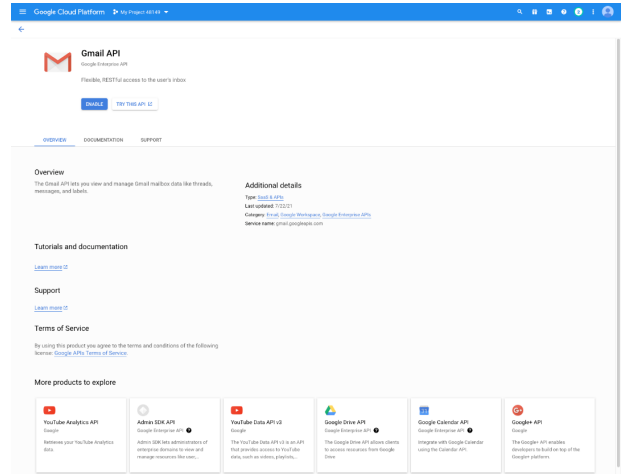


9. Suchen Sie in der Bibliothek nach der **Gmail-API** und klicken Sie darauf.



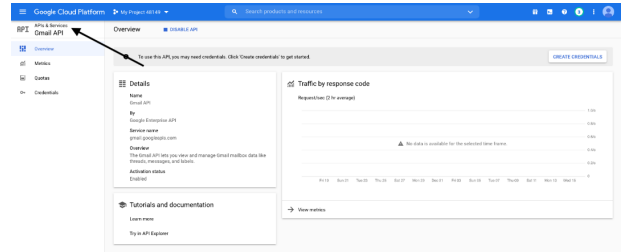


10. Die Gmail API erscheint auf einer eigenen Seite. Klicken Sie auf AKTIVIEREN.



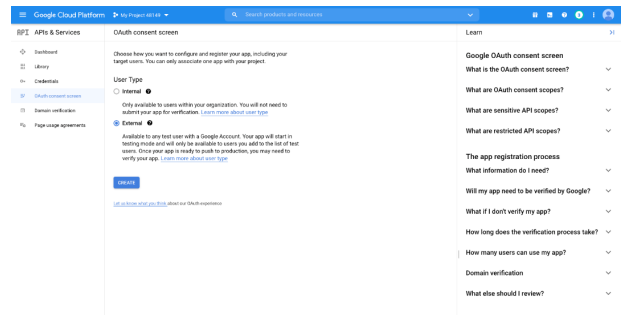
11. Die Seite Gmail API-Übersicht wird angezeigt. Klicken Sie oben links auf APIs & Dienste.

12. Die Seite APIs und Dienste wird wieder angezeigt. Klicken Sie im linken Menü auf OAuth-Zustimmungsbildschirm.



13. Wählen Sie den Benutzertyp. Intern erlaubt nur Benutzern innerhalb der Organisation, erfordert aber ein Google Workspace-Konto.

14. Klicken Sie auf ERSTELLEN.



15. Geben Sie den App-Namen ein.

16. Geben Sie eine Benutzer-Support-E-Mail-Adresse ein. Dies kann standardmäßig die Adresse sein, die Sie zum Erstellen des Projekts verwenden.

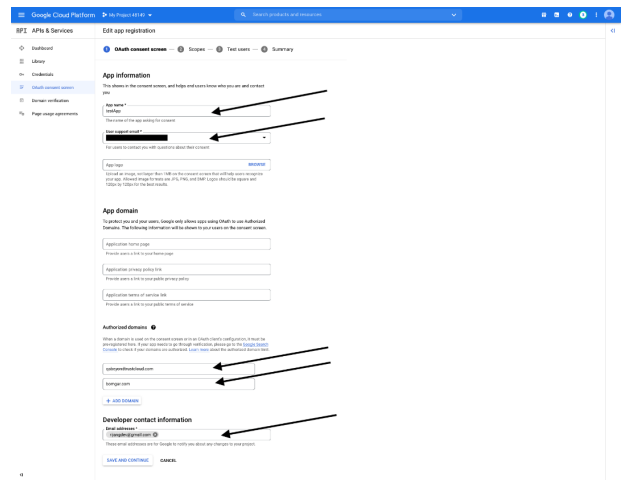
17. Geben Sie, falls gewünscht, ein Logo für die App ein. Der Abschnitt Anwendungsbereich ist ebenfalls optional.

18. Fügen Sie Zugelassene Domains hinzu. Für BeyondTrust Testgeräte sind das:

- qabeyondtrustcloud.com
bomgar.com

19. Geben Sie die Kontaktinformationen des Entwicklers ein. Dies ist die E-Mail-Adresse, die Sie zur Erstellung des Projekts verwenden.

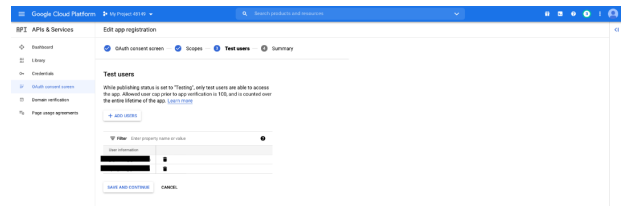
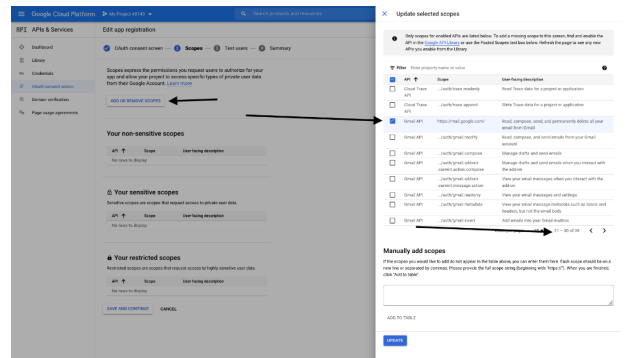
20. Klicken Sie auf SPEICHERN UND WEITER.



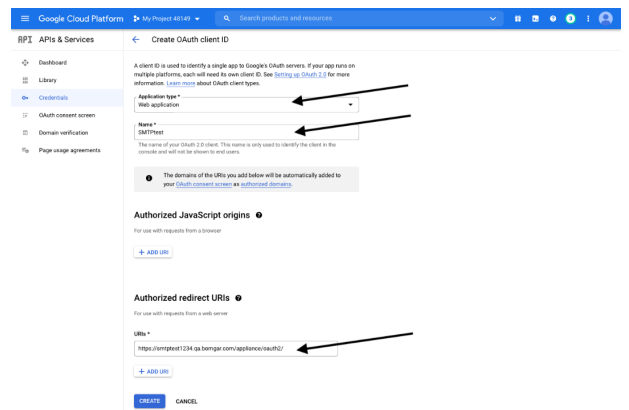
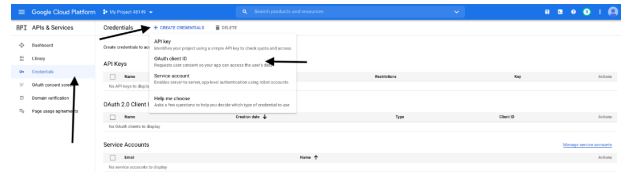
21. Klicken Sie auf der Registerkarte **Bereiche** auf **Bereiche hinzufügen oder entfernen**. Dies öffnet das Fenster **Ausgewählte Bereiche aktualisieren**.
22. Suchen Sie den Bereich **https://mail.google.com/** für die Gmail-API und überprüfen Sie ihn.

**Hinweis:** Die API wird nicht angezeigt, wenn sie nicht aktiviert wurde.

23. Klicken Sie **UPDATE**. Das Fenster **Ausgewählte Bereiche aktualisieren** wird geschlossen.
24. Klicken Sie auf **SPEICHERN UND WEITER**.
25. Klicken Sie auf der Registerkarte **Testbenutzer** auf **BENUTZER HINZUFÜGEN**. Dies öffnet das Fenster **Benutzer hinzufügen**. Fügen Sie die Benutzer hinzu, die Zugriff auf die Anwendung haben, und klicken Sie auf **ZUFÜGEN**. Beachten Sie die Zugriffsbeschränkungen für Testbenutzer und die damit verbundenen Einschränkungen.
26. Klicken Sie auf **SPEICHERN UND WEITER**.
27. Überprüfen Sie die Zusammenfassung und nehmen Sie gegebenenfalls Änderungen oder Korrekturen vor.
28. Klicken Sie auf **ZURÜCK ZUM DASHBOARD**.
29. Klicken Sie im linken Menü auf **Anmeldedaten**.
30. Klicken Sie auf **ANMELDEDATEN ERSTELLEN** im oberen Banner und wählen Sie **OAuth-Client-ID**.



31. Wählen Sie auf der Seite zum Erstellen von Anmeldedaten **Webanwendung** für den **Anwendungstyp**. Wenn diese Option ausgewählt ist, erscheinen zusätzliche Felder.
32. Geben Sie einen Namen für die Anwendung ein.
33. Scrollen Sie nach unten zu **Zugelassene Umleitungs-URIs** und klicken Sie auf **URI hinzufügen**.
34. Dies ist der **Autorisierungsumleitungs-URI**, der zu Beginn dieses Prozesses von der BeyondTrust Gerätesoftware erhalten wurde.
35. Klicken Sie auf **ERSTELLEN**.



36. Ein Fenster bestätigt die Erstellung des OAuth-Clients und zeigt die **Client ID** und **Client-Secret** an. Klicken Sie hier, um eine JSON-Datei herunterzuladen. Die Datei enthält Informationen, die für die nächsten Schritte benötigt werden.
37. Klicken Sie auf **OK**, um zur Seite "APIs und Dienste" zurückzukehren.

### OAuth client created

The client ID and secret can always be accessed from Credentials in APIs & Services

**i** OAuth access is restricted to the [test users](#) listed on your [OAuth consent screen](#)

Your Client ID  
1052081453748-4tuptq4o0ovnakrm67f2qkaa3kc6s4dn.apps.g

Your Client Secret  
[REDACTED]

↓ DOWNLOAD JSON

OK

Die übrigen Schritte werden auf der BeyondTrust-Anwendung durchgeführt.

38. Gehen Sie zu **Gerät**, klicken Sie auf die Registerkarte **Sicherheit** und dann auf **E-Mail-Konfiguration**.
39. Geben Sie die folgenden Informationen ein, die Sie in der heruntergeladenen JSON-Datei finden:
  - **Autorisierungsendpunkt**
  - **Token-Endpunkt**
  - **Client-ID**
  - **Client-Secret**
40. Geben Sie eine beliebige E-Mail-Adresse für diesen Dienst als **Senden von E-Mail-Adresse** ein.
41. Geben Sie die **Benutzer-E-Mail** ein. Dies muss eine E-Mail-Adresse sein, die als **Testbenutzer** mit Zugriff auf die Anwendung eingegeben wurde, als Sie die OAuth-Zustimmungsbildschirme ausgefüllt haben.
42. Geben Sie Daten für die Felder **Host**, **Verschlüsselung** und **Port** ein.
  - **Host:** smtp.gmail.com
  - **Verschlüsselung:** TLS
  - **Port:** 465



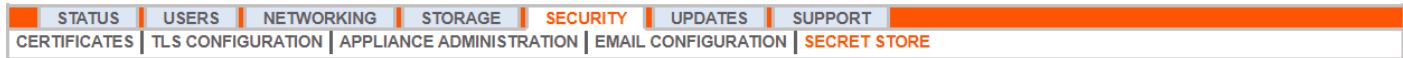
**Hinweis:** Es werden Standarddaten für Google angezeigt, aber Ihre Installation verwendet möglicherweise einen anderen Host oder eine andere Verschlüsselungsmethode. Der Port gilt für TLS, aber andere Verschlüsselungsmethoden können einen anderen Port verwenden.

43. Geben Sie Ihr TLS-Zertifikat ein, wenn es von Google angegeben wird. Wenn nicht, markieren Sie **TLS-Zertifikatsfehler ignorieren**.
44. Geben Sie für **Bereiche** Folgendes ein: https://mail.google.com
45. Klicken Sie auf **Änderungen speichern**.
46. Klicken Sie auf **Autorisieren**. Nach der Anmeldeseite, die angezeigt wird, erhalten Sie möglicherweise die Warnung **Google hat diese Nachricht nicht überprüft**, wenn Sie die Anwendung nicht veröffentlicht haben. Die Einwilligungsseite wird neu geladen, und die Schaltfläche zur Autorisierung wird durch eine autorisierte Nachricht ersetzt.

47. Zum Testen der Konfiguration:

- Fügen Sie eine **Admin-Kontakt-E-Mail** hinzu.
- Markieren Sie **Eine Test-E-Mail senden**.
- Klicken Sie auf **Änderungen speichern**.

# Geheimspeicher: Geheimnisse speichern und auf sie zugreifen



Erstellen und verwalten Sie in AWS und BeyondTrust DevOps Secrets Safe (DSS) gespeicherte geheime Schlüssel, um Verschlüsselungsschlüssel und Website-Daten sicher zu verwahren. Um einen Geheimpeicher hinzuzufügen, wählen Sie den Speicher aus der Dropdown-Liste aus und klicken Sie dann auf **Speicher hinzufügen**. Geben Sie die Informationen für den Speicher wie in den folgenden Schritten gezeigt ein und speichern Sie sie.

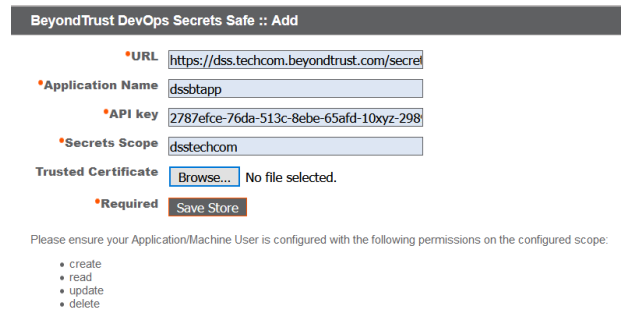
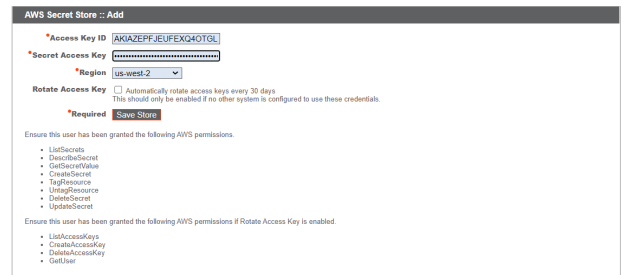
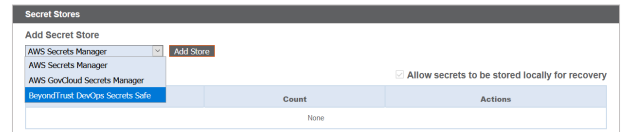
## AWS-Geheimspeicher hinzufügen

1. Geben Sie die **Zugriffsschlüssel-ID**, den **geheimen Zugriffsschlüssel** und die **Region** an.
2. Aktivieren Sie das Kontrollkästchen **Zugangsschlüssel rotieren** nur, wenn Sie die Anmeldedaten in keinem anderen System verwenden.
3. Klicken Sie auf **Speicher speichern**.

## BeyondTrust DevOps Secrets Safe Speicher hinzufügen

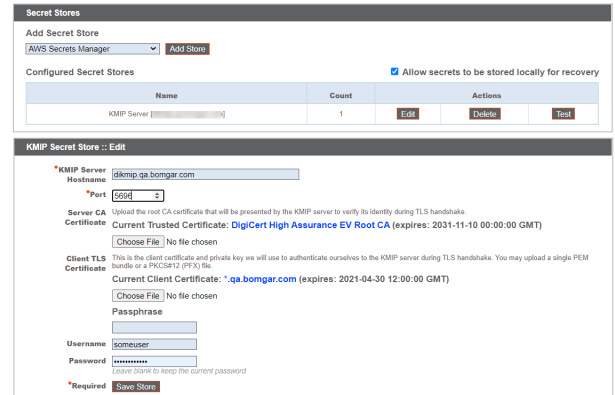
1. Geben Sie die **URL** für Ihre DSS-Instanz ein.
2. Geben Sie den **Anwendungsnamen** an, den Sie in DSS konfiguriert haben.
3. Geben Sie den in DSS generierten **API-Schlüssel** für die Anwendung an.
4. Geben Sie den **Secret-Scope** ein, den Sie mit Berechtigungen in DSS konfiguriert haben.
5. Wenn Sie ein selbstsigniertes Zertifikat in DSS verwenden, fügen Sie das **vertrauenswürdige Zertifikat** hinzu. Wenn Sie ein CA-Zertifikat verwenden, müssen Sie kein vertrauenswürdige Zertifikat bereitstellen.
6. Klicken Sie auf **Speicher speichern**.

Wenn Sie einen Geheimpeicher hinzugefügt haben, klicken Sie auf **Testen**, um die Verbindung mit dem Geheimpeicher-Server zu überprüfen und sicherzustellen, dass die richtigen Berechtigungen vorliegen, damit mit den Anmeldedaten auf den Geheimpeicher-Server zugegriffen werden kann.





**Hinweis:** Das Konfigurieren eines KMIP-Servers für einen Verschlüsselungsspeicher wird in Version 6.0 und höher 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.




**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-Richtlinien](https://docs.aws.amazon.com/IAM/latest/UserGuide/access_policies_manage.html) unter [https://docs.aws.amazon.com/IAM/latest/UserGuide/access\\_policies\\_manage.html](https://docs.aws.amazon.com/IAM/latest/UserGuide/access_policies_manage.html).

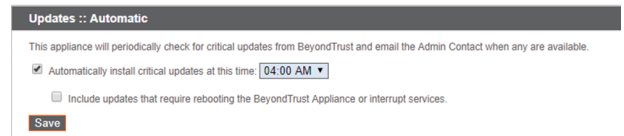


**Hinweis:** Wenn Sie den letzten Remote-Speicher löschen, wird eine Meldung angezeigt, dass die Secrets lokal verschoben werden.

# Aktualisierungen: Auf Aktualisierungen prüfen und Software auf Privileged Remote Access installieren



Das B Series Appliance 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 B Series Appliance-Neustart oder die Unterbrechung von Diensten erfordern, sind vom automatischen Aktualisierungsprozess ausgeschlossen, es sei denn, Sie aktivieren die entsprechende Option.

BeyondTrust, benachrichtigt Sie weiterhin Sie auch über die neuesten Builds, sobald diese verfügbar sind. Wenn Sie eine Benachrichtigung erhalten, dass neue Aktualisierungspakete für Ihr B Series Appliance verfügbar sind und auf die Schaltfläche **Auf Aktualisierungen prüfen** klicken, werden die Pakete gesucht und zur Installation für Sie verfügbar gemacht.

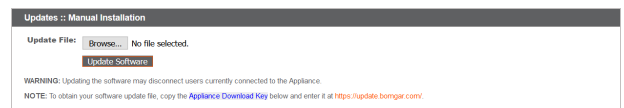


Falls mehrere Softwarepakete für Ihr B Series Appliance erstellt wurden, wird jedes einzeln in der Liste der verfügbaren Aktualisierungen aufgelistet. Ihre neue Software wird automatisch heruntergeladen und installiert, wenn Sie auf die entsprechende Schaltfläche **Diese Aktualisierung installieren**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

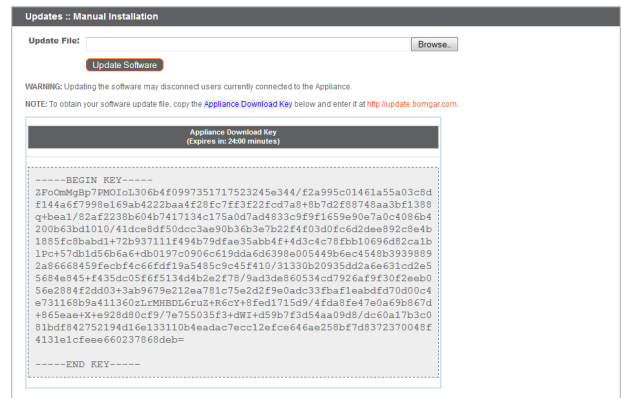
Wenn für Ihr B Series Appliance keine Aktualisierungspakete oder Patches verfügbar sind, wird die Meldung „Keine Aktualisierungen verfügbar“ angezeigt. Wenn eine Aktualisierung verfügbar ist, aber ein Fehler beim Übertragen der Aktualisierung auf Ihr B Series Appliance auftritt, wird eine weitere Meldung wie „Ein Fehler ist beim Kompilieren Ihrer Aktualisierung aufgetreten. Weitere Informationen finden Sie unter [www.beyondtrust.com/support](http://www.beyondtrust.com/support).“



Die Verwendung der Funktion **Auf Aktualisierungen prüfen** ist nicht zwingend erforderlich. Wenn 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 B Series Appliance-Schlüssel 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 B Series Appliance 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.



**WICHTIG!**

*Bitte bereiten Sie sich darauf vor, die Aktualisierungen direkt nach dem Herunterladen zu installieren. Wenn 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 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](http://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 aktualisieren automatisch alle Websites und Lizenzen in Ihrem B Series Appliance.

Wenn Sie eine Software-Aktualisierung installieren, verlieren angemeldete Benutzer vorübergehend die Verbindung zu sämtlichen access session und der Zugriffskonsole; 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 Benutzer installiert werden.

Aktuelle Informationen über die neuesten BeyondTrust Updates finden Sie unter <https://www.beyondtrust.com/docs/release-notes/index.htm>.

Um installierte Patches anzuzeigen, wählen Sie auf der Registerkarte **Updates** die Option **Installierte Patches**. Die Tabelle zeigt alle installierten Firmware-Patches und wann sie installiert wurden.

**Please wait while the software is updating.**

**Note that installation progress may stop for long periods of time while data is being backed up.**

**You will be automatically redirected when the update is finished.**

**Do not refresh this page.**

**Do not reboot the appliance.**

**If an error occurs, please contact [BeyondTrust Support](#)**

1% - Initializing...



## Support Dienstprogramme: Beseitigung von Netzwerkproblemen

STATUS	USERS	NETWORKING	STORAGE	SECURITY	UPDATES	SUPPORT	
UTILITIES	ADVANCED SUPPORT						

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 B Series Appliances, 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 B Series Appliances zu testen.
- Sie können **Traceroute** verwenden, um den Pfad anzuzeigen, den die Pakete auf ihrem Weg vom B Series Appliance 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.

# BeyondTrust Secure Remote Access

Powered by Bomgar

Virtual Appliance ADMINISTRATION

 English (US) | admin | LOGOUT

STATUS | USERS | NETWORKING | STORAGE | SECURITY | UPDATES | SUPPORT

UTILITIES | ADVANCED SUPPORT

## Util :: DNS

Use this DNS utility to test the DNS resolution on this appliance. If you get "Unable to Resolve" errors, check your DNS Server settings on the Networking tab.

Hostname or IP Address

Resolve

## Util :: Ping

Use this Ping utility to test the Network connectivity of this appliance. If you get "unknown host" errors, check your DNS Server settings on the Networking tab. If you get 100% packet loss, check that the destination server is configured to respond to Pings, and check your IP settings on the Networking tab.

Hostname or IP Address

IPv4  IPv6

Ping

## Util :: Traceroute

Use this Traceroute utility to test the outbound Network routes from this appliance. You can manually configure static routes in the Networking tab.  
This utility will only try a maximum of 20 hops

Hostname or IP Address

IPv4  IPv6

Trace

## Util :: TCP Connection Test

Use this TCP Connection Test utility to troubleshoot network connections to remote hosts and ports.

Hostname or IP Address

Port Number

Test

## Util :: SSL/TLS Connection Test

Use this to troubleshoot connections to remote HTTPS or any other TLS server.

Hostname

or IP

Address

Use of hostname here is encouraged instead of IP. Hostnames will be sent in the handshake in the Server Name Indication (SNI) field. Many TLS servers implement name-based virtual hosting and will send different certificates based on this SNI information, and are more likely to result in a successful connection.

Port  
Number

Test

# Erweiterter Support: Kontakt mit BeyondTrust Technical Support

STATUS | USERS | NETWORKING | STORAGE | SECURITY | UPDATES | SUPPORT

UTILITIES | ADVANCED SUPPORT

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

## BeyondTrust™ Support Contact Information

### Support Portal

<https://help.beyondtrust.com/>

## Advanced Technical Support From BeyondTrust™

Support Code

Access Code

Override Code

OK

NOTE: A BeyondTrust™ Technical Support representative may ask you to use this section when advanced technical assistance is required. These codes will be provided at that time.

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

## Advanced Technical Support From BeyondTrust™

Support Session Initiated to BeyondTrust

Support Code

Access Code

Override Code

OK

NOTE: A BeyondTrust™ Technical Support representative may ask you to use this section when advanced technical assistance is required. These codes will be provided at that time.

## Current Support Session

	Start Time	Duration	Terminate Connection
A Support Session with BeyondTrust Corporation is in progress.	06/13/2019 03:45 PM UTC		<b>Terminate</b>