BeyondTrust

Privileged Remote Access
B-serie apparaatinterface 6.1
(/appliance)

TC:11/17/2022

Table of Contents

Web-interface van BeyondTrust Appliance B Series

Deze gids is speciaal ontworpen om u te helpen bij het configureren en beheren van de B Series Appliance via de **/appliance**-web-interface. De B Series Appliance dient als centraal punt voor de administratie en het beheer van uw BeyondTrust-site.

Gebruik deze gids pas nadat een beheerder de initiële installatie en configuratie van de B Series Appliance heeft uitgevoerd zoals beschreven in de BeyondTrust Appliance B Series Hardware-installatiegids op www.beyondtrust.com/docs/privileged-remote-access/getting-started/deployment/hardware-sra/. Nadat BeyondTrust correct is geïnstalleerd, kunt u direct toegang krijgen tot uw eindpunten. Neem contact op met BeyondTrust Technical Support via www.beyondtrust.com/support als u ondersteuning nodig hebt.

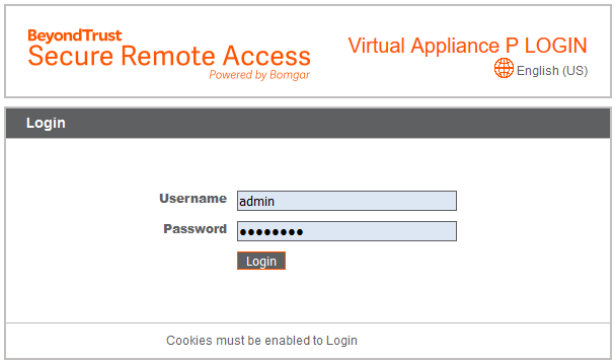
Log in bij de beheerinterface van de BeyondTrust Appliance B Series

Log na de installatie van het B Series Appliance in bij de beheerinterface van het B Series Appliance. Ga daarvoor naar de openbare URL van uw B Series Appliance, gevolgd door **/appliance** (bijv. http://toegang.voorbeeld.nl/appliance).

Standaard gebruikersnaam: **admin**

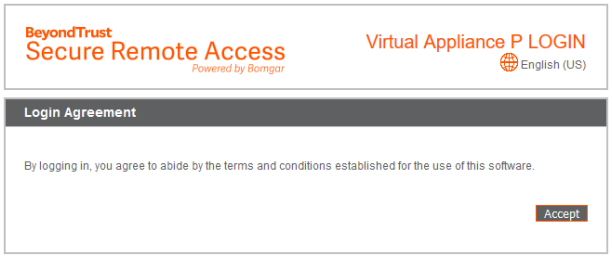
Standaard wachtwoord: **password**

Wanneer u voor de eerste keer inlogt, ziet u de vraag om het beheerderswachtwoord te wijzigen.[1]



Opmerking: *Om veiligheidsredenen zijn de gebruikersnaam en het wachtwoord voor het beheer via het **/appliance**-scherm anders dan de inloggegevens die voor het **/login**-scherm worden gebruikt. Beide moeten afzonderlijk worden beheerd.*

U kunt de toegang tot het aanmeldscherm beperken door een vereiste aanmeldovereenkomst in te schakelen die moet worden bevestigd voordat het aanmeldscherm wordt weergegeven.

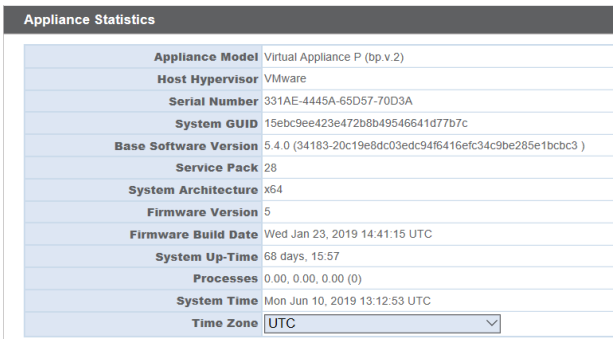


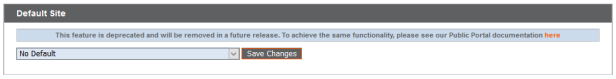
Raadpleeg als u de verplichte aanmeldovereenkomst wilt inschakelen: "Apparaatbeheer: Accounts, netwerken en poorten beperken, een STUN-server inschakelen, syslog instellen, inlogovereenkomst inschakelen, beheerdersaccount resetten" op pagina 26.

[1]Wachtwoorden moeten uit minimaal 8 tekens bestaan en aan de volgende voorwaarden voldoen: een hoofdletter, een kleine letter, een cijfer en een speciaal teken.

Status Basisinstellingen: Details van B Series Appliance tonen

De pagina **Basisinstellingen** bevat informatie over uw B Series Appliance en stelt u in de gelegenheid om uw systeem te bewaken. Ook kunt u uw lokale tijd instellen op elke geldige tijdzone. De systeemtijd wordt standaard weergegeven in UTC.

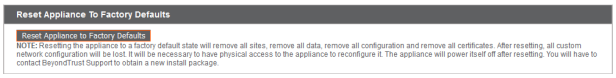




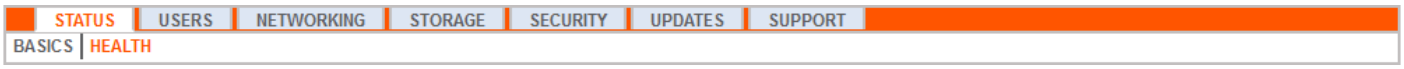
Deze instelling kan in vrijwel alle scenario's ongewijzigd blijven. BeyondTrust raadt af om meerdere sites op één B Series Appliance te hebben. Mocht het voor uw setup echter noodzakelijk zijn om meerder websites op één IP-adres te hebben, selecteer dan een standaard-website die moet reageren, mocht iemand het IP-adres invoeren in plaats van de domeinnaam. Als meer dan één DNS naar dit IP-adres wijst en u hebt **Geen standaard** geselecteerd, dan verschijnt er een foutmelding als iemand uw website probeert te bereiken via het IP-adres.

Op deze pagina kunt u uw B Series Appliance ook opnieuw opstarten of uitschakelen. Hoewel opnieuw opstarten van uw B Series Appliance niet vereist is, is het verstandig om maandelijks opnieuw opstarten van het apparaat op te nemen in uw routine-onderhoud. U hoeft geen fysieke toegang tot uw B Series Appliance te hebben om het opnieuw op te starten.

Doe het volgende uitsluitend als u dit door BeyondTrust Technical Support wordt gevraagd: Door op de knop **Fabrieksinstellingen van apparaat opnieuw instellen** te klikken, worden de fabrieksinstellingen van uw B Series Appliance opnieuw ingesteld. Hierdoor worden alle gegevens, configuratie-instellingen, websites en certificaten van uw B Series Appliance gewist. Als het B Series Appliance eenmaal is gereset, schakelt het apparaat ook vanzelf uit.



Status Conditie: Conditie van PRA Virtual Appliance weergeven



Opmerking: *Het tabblad* ***Conditie*** *is alleen zichtbaar voor sites die worden ondersteund door een PRA Virtual Appliance of Cloud Appliance.*

Op de pagina **Conditie** kunt u de status van uw virtuele of Cloud Appliance bekijken. U ziet hier hoeveel CPU's in gebruik zijn, hoeveel geheugen en opslagruimte wordt gebruikt. De kolommen **Status** en **Opmerkingen** geven suggesties over hoe u de conditie van uw B Series Appliance kunt verbeteren.

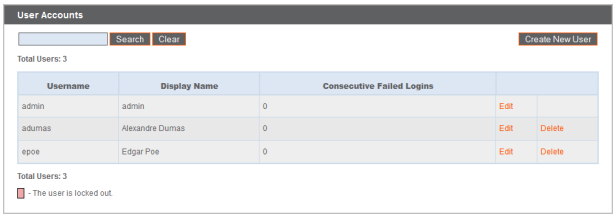
Hardware Health

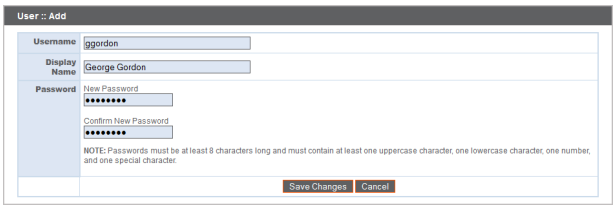
	Value	Status	Notes
CPU	Count: 8 Model: Intel(R) Xeon(R) CPU E5-2697 v3 @ 2.60GHz Speed: 2593.993 MHz Reservation: 0 MHz Limit: Unlimited		• Consider allocating a CPU Reservation to this VM of at least 500 MHz to help maintain functionality when the host's CPUs are under contention.
Memory	Physical: 16051 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		

Gebruikers: Gebruikersnaam of wachtwoord wijzigen, gebruiker toevoegen, gebruiker verwijderen

Op de pagina **Gebruikers** kunt u gebruikers met beheerdersrechten voor de /appliance-interface toevoegen, bewerken of verwijderen. U kunt ook de gebruikersnaam, de weergavenaam of het wachtwoord van een beheerder wijzigen. BeyondTrust adviseert u om uw wachtwoord regelmatig te wijzigen om u te beschermen tegen onbevoegde toegang.

Opmerking: *Er moet minstens één gebruikersaccount gedefinieerd zijn. Het BeyondTrust Appliance B Series bevat één vooraf gedefinieerd account, het beheerdersaccount. U kunt alleen het beheerdersaccount houden, extra accounts aanmaken of het beheerdersaccount vervangen.*





Meer informatie over het instellen van regels voor accountbeperking, inclusief de vervaldatum voor wachtwoorden en de geschiedenis, vindt u in *"Apparaatbeheer: Accounts, netwerken en poorten beperken, een STUN-server inschakelen, syslog instellen, inlogovereenkomst inschakelen, beheerdersaccount resetten" op pagina 26*.

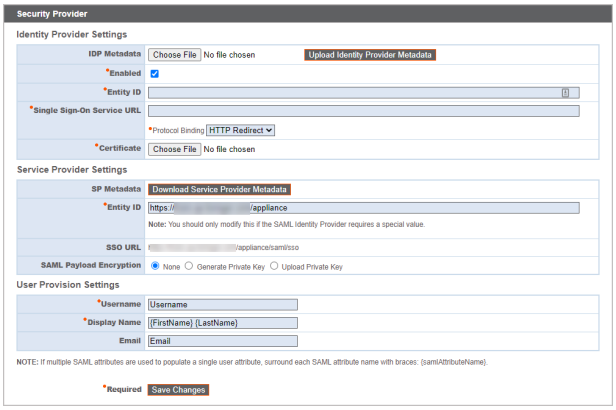
SAML: Gebruikersverificatie instellen via een SAML-identiteitsprovider

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

Configureer uw B Series Appliance om gebruikers toe te staan om naar de /appliance interface te verifiëren met behulp van SAML.

> ***Opmerking:*** *Om SAML-verificatie te gebruiken, moet u een identiteitsprovider hebben zoals Okta, OneLogin, Azure AD of ADFS.*

Om de verbinding op te zetten, begint u met de sectie **Instellingen serviceprovider**. Als uw identiteitsprovider (IDP) u toestaat om metagegevens van de serviceprovider (SP) te uploaden, klikt u op **Metagegevens van serviceprovider downloaden**. Dit levert u een XML-bestand op dat u tijdens het aanmaken van de toepassing kunt uploaden naar uw IDP. U kunt er ook voor kiezen om de **Entiteit-ID** en **SSO-URL** te kopiëren en in uw IDP te plakken.



> ***Tip:*** *De **Entiteit-ID** kan ook **Doelgroep-URI** heten in uw identiteitsprovider.*

Versleuteling van SAML-nettolading staat standaard uitgeschakeld, maar u kunt een privésleutel genereren of uploaden om dit in te schakelen. Om het B Series Appliance een privésleutel en certificaat te laten genereren, selecteert u **Privésleutel genereren** en klikt u op **Veranderingen opslaan**. Klik vervolgens op **SP-certificaat downloaden** en upload het gegenereerde certificaat naar uw identiteitsprovider. Als u zelf de privésleutel en het certificaat wilt opgegeven, selecteert u **Privésleutel uploaden**, kiest u het certificaatbestand en voert zo nodig u het wachtwoord in. U moet hetzelfde certificaatbestand uploaden naar uw identiteitsprovider.

Nadat u de toepassing hebt opgeslagen in uw identiteitsprovider, krijgt u mogelijk de optie om de metagegevens te downloaden. Als dat het geval is, upload dat bestand dan naar uw B Series Appliance middels de knop **Metagegevens van identiteitsprovider uploaden**. U kunt er ook voor kiezen om de **Entiteit-ID** en **URL voor service voor eenmalige aanmelding** te kopiëren en in de sectie **Instellingen identiteitsprovider** van uw B Series Appliance te plakken.

> ***Tip:*** *De **Entiteit-ID** kan ook **Identiteitsprovideruitgever** of **URL-verlener** genoemd worden en de **URL voor service voor eenmalige aanmelding** kan ook **SAML 2.0 Eindpunt** heten.*

Protocolbinding bepaalt of er een HTTP POST plaatsvindt of dat de gebruiker wordt doorgestuurd naar de aanmeld-URL. Laat dit ingesteld staan op **HTTP-omleiding**, tenzij uw identiteitsprovider dit anders wil hebben. U moet ook het IDP-**certificaat** verstrekken; u kunt dit downloaden van de IDP.

Wijs onder **Instellingen voor gebruikersprovisionering**, de **Gebruikersnaam**, **Schermnaam** en **E-mail** toe aan de bijbehorende kenmerken in uw identiteitsprovider.

Klik op **Wijzigingen opslaan** om de SAML-configuratie op te slaan.

Op de inlogpagina van /appliance zien gebruikers nu een koppeling naar **SAML-verificatie gebruiken** onder de knop **Inloggen**. Gebruikers die aan de in uw IDP aangemaakte toepassing zijn toegewezen kunnen op deze koppeling klikken om in te loggen. Als ze nog niet zijn aangemeld bij de IDP, worden ze doorverwezen naar de IDP om in te loggen voordat ze terug worden geleid naar /appliance.

Netwerken

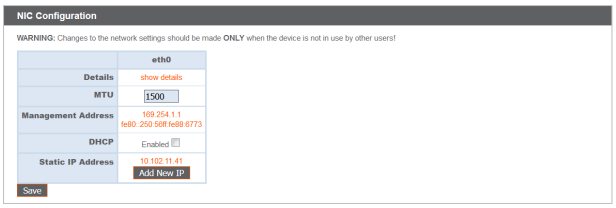
IP-configuratie: Configureer IP-adressen en netwerkinstellingen

Bedrijven met uitgebreide netwerkconfiguraties kunnen meerdere IP-adressen configureren op de ethernetpoorten van de B Series Appliance. Gebruik van meerdere poorten kan uw veiligheid verbeteren en biedt de mogelijkheid tot het maken van verbindingen over niet-standaard netwerken. Zo kunnen medewerkers die geen toegang hebben tot het internet maar off-netwerk ondersteuning moeten bieden, één poort gebruiken voor uw interne privénetwerk en een andere voor internetgebruik. Op deze manier hebben zij toegang tot alle systemen wereldwijd zonder uw beleid voor netwerkbeveiliging te schenden.

NIC-teaming combineert uw fysieke netwerk-interfacecontrollers (NIC's) in één enkele logische interface. NIC-teaming werkt als actieve back-up. Een van de NIC's wordt gebruikt voor al het netwerkverkeer. Als de koppeling naar deze NIC om welke reden dan ook verloren gaat, wordt de andere NIC actief. Controleer, voordat u NIC-teaming activeert, of beide NIC's met hetzelfde netwerksegment (subnet) verbonden zijn en of u IP-adressen op slechts een van de bestaande NIC's geconfigureerd hebt.

> ***Opmerking:*** *Als u een virtuele of cloudomgeving voor uw Cloud Appliance gebruikt, is de optie* ***NIC-teaming inschakelen*** *niet beschikbaar.*

Hoewel aan elke netwerk-interfacecontroller (NIC) meerdere IP-adressen kunnen worden toegewezen, moet u de NIC niet configureren met een IP-adres in hetzelfde subnet als een IP-adres op de andere NIC. In dat geval is er sprake van pakketverlies van pakketten die afkomstig zijn van het IP-adres op de NIC die geen standaardgateway heeft. Hier volgt een voorbeeldconfiguratie:



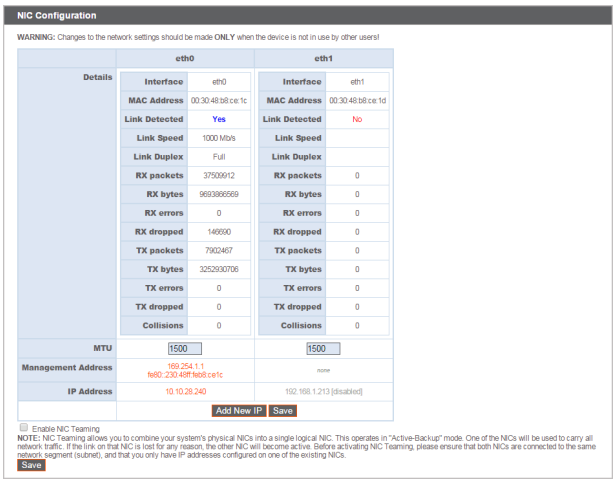
- eth0 is geconfigureerd met 192.168.1.1 als de standaard gateway
- eth0 heeft 192.168.1.5 toegewezen gekregen
- eth1 heeft 192.168.1.10 toegewezen gekregen
- Zowel eth0 als eth1 zijn verbonden met dezelfde subnetswitch

Met deze configuratie wordt verkeer van beide NIC's naar de standaard gateway (192.168.1.1) verzonden, ongeacht welke NIC het verkeer ontvangt. Switches die geconfigureerd zijn met dynamisch Address Resolution Protocol (ARP) sturen pakketten willekeurig naar eth0 (192.168.1.5) of eth1 (192.168.1.10), maar niet naar beide. Wanneer eth0 deze pakketten van de switch ontvangt die bestemd zijn voor eth1, laat eth0 de pakketten vallen. Sommige switches zijn geconfigureerd met statische ARP. Deze switch laat alle pakketten van eth1 vallen omdat deze NIC niet de standaard gateway heeft en niet in de statische ARP-tabel van de gateway aanwezig is. Als u overbodige NIC's op hetzelfde subnet wilt configureren, gebruikt u NIC-teaming.

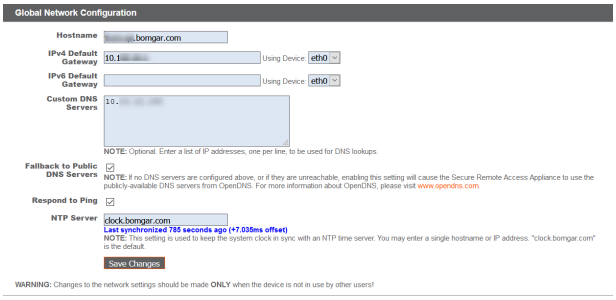
Standaard is het Dynamic Host Configuration Protocol (DHCP) ingeschakeld voor uw B Series Appliance. DHCP is een netwerkprotocol dat een DHCP-server gebruikt om de distributie van netwerkparameters beheert, zoals IP-adressen, zodat systemen automatisch deze parameters kunnen opvragen. Hierdoor is het niet meer nodig om de instellingen handmatig te configureren. In dit geval, als het vakje is aangevinkt, wordt een IP-adres verkregen van de DHCP-server en verwijderd uit de pool met beschikbare IP-adressen.

> *Raadpleeg Wat is DHCP? op docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/dd145320(v=ws.10) voor meer informatie over DHCP.*

Klik op **Details tonen** om voor elke ethernetpoort op het B Series Appliance statistieken over de transmissie en ontvangst weer te geven.



Configureer onder **Algemene netwerkconfiguratie** de hostnaam voor uw B Series Appliance.

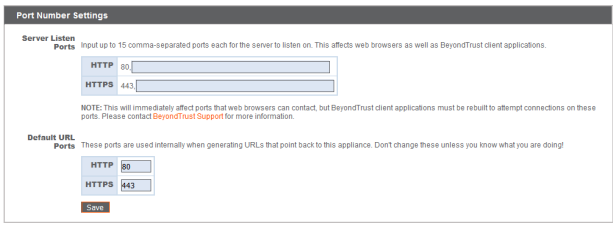


> ***Opmerking:*** *Er zijn geen technische vereisten voor het veld* ***Hostnaam****. Het maakt niet uit met welke hostnaam clientsoftware of externe gebruikers verbinding maken. Als de hostnaam die door de clientsoftware wordt geprobeerd moet worden gewijzigd, dient u BeyondTrust Technical Support te informeren over de benodigde wijzigingen, zodat ondersteuning een software-update kan samenstellen. Het veld* ***Hostnaam*** *is voornamelijk bedoeld om onderscheid te kunnen maken tussen meerdere B Series Appliances. Hij wordt ook gebruikt als lokale serveridentificatie bij SMTP-verbindingen om e-mailwaarschuwingen te verzenden. Dit is handig als de* ***SMTP-relayserver*** *gespecificeerd op* ***/appliance > Beveiliging > E-mailconfiguratie*** *vergrendeld is. In dat geval moet de geconfigureerde hostnaam wellicht overeenkomen met het resultaat van de omgekeerde DNS-zoekactie naar het IP-adres van het B Series Appliance.*

Wijs een standaard gateway toe en selecteer welke ethernetpoort moet worden gebruikt. Voer een IP-adres in voor één of meer DNS-servers. Als DHCP is ingeschakeld, verschaft de DHCP-lease u een standaardgateway en een lijst met DNS-servers in volgorde van voorkeur. Eventuele statisch geconfigureerde DNS-servers in het veld **Aangepaste DNS-servers** worden eerst benaderd, gevolgd door de DNS-servers ontvangen van de DHCP. Als deze lokale DNS-servers niet beschikbaar zijn, zorgt de optie **Op OpenDNS-servers terugvallen** ervoor dat het B Series Appliance openbaar beschikbare DNS-servers van OpenDNS kan gebruiken.

> *Raadpleeg www.opendns.com voor meer informatie over OpenDNS.*

Sta uw B Series Appliance toe om te reageren op pings als u wilt kunnen testen of de host functioneert. Stel de hostnaam of het IP-adres in voor een Network Time Protocol-server (NTP) waarmee u uw B Series Appliance wilt synchroniseren.

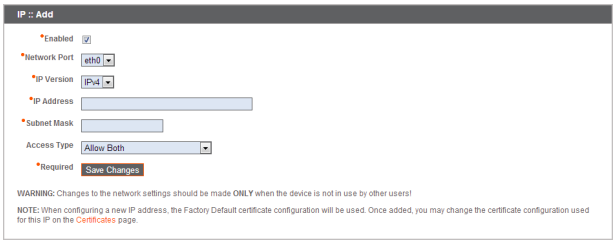


Er zijn twee instellingen beschikbaar in het gedeelte **Poortnummerinstellingen**: **Luisterpoorten server** en **Standaard URL-poorten**. Houd er wel rekening mee dat, wanneer u deze configuraties instelt, verbindingen naar geldige poorten geweigerd kunnen worden als gevolg van netwerkbeperkingen die zijn ingesteld in **/appliance > Beveiliging > Apparaatbeheer** en in **/login > Beheer > Beveiliging**. Het omgekeerde geldt ook: verbindingen naar ongeldige poorten kunnen worden geweigerd zelfs als dergelijke verbindingen aan de netbeperkingen voldoen.

In het gedeelte **Luisterpoorten server** kunt u poorten configureren waar het B Series Appliance op luistert. U kunt maximaal 15 door komma's gescheiden poorten voor HTTP en 15 door komma's gescheiden poorten voor HTTPS specificeren. Elke poort mag maar één keer in een veld voorkomen en mag maar in één veld tegelijk voorkomen, niet in beide. Het B Series Appliance reageert op HTTP-verbindingen naar elke willekeurige poort vermeld in het HTTP-veld en het B Series Appliance reageert op HTTPS-verbindingen naar elke willekeurige poort die staat vermeld in het HTTPS-veld. U kunt de ingebouwde luisterpoorten (80 en 443) niet wijzigen.

U kunt toegang tot uw B Series Appliance verkrijgen via een bepaalde poort door het poortnummer in de adresbalk van de browser in te voeren (bijv. support.example.com:8200). Clients die gedownload zijn van het B Series Appliance proberen verbinding te maken met poorten die staan weergegeven op de pagina **/login > Status > Informatie** onder **Clientsoftware is gemaakt om te proberen**. Deze poorten kunnen niet vanaf /login of /appliance worden geconfigureerd. Neem contact op met de ondersteuning van BeyondTrust voor een nieuwe update voor uw B Series Appliance om dit te wijzigen. Na de installatie stelt de update de poorten voor **Poging** in volgens de door de ondersteuning van BeyondTrust gespecificeerde parameters.

Als URL's worden gegenereerd die terugwijzen naar het B Series Appliance, zoals sessiesleutels die door de access console worden gegenereerd, worden **Standaard URL-poorten** gebruikt. Mochten de standaard poorten op het netwerk worden geblokkeerd (of om een andere reden niet goed functioneren), dan kunt u de standaard URL-poort wijzigen en gegenereerde URL's aan laten roepen met de door u gespecificeerde poorten. De poorten die u invoert, moeten ook vermeld zijn in de **Luisterpoorten server**, anders kunnen de standaard poorten geen verbinding maken. Als u bijvoorbeeld **8080** invoert in het veld **Standaard URL-poort**, moet u ervoor zorgen dat **8080** ook is opgenomen in de luisterpoortvelden **HTTP** of **HTTPS**. In tegenstelling tot de luisterpoorten, kunnen de velden voor URL-poorten maar één poort bevatten. Ook mag u niet dezelfde poort in beide velden invoeren.



Wanneer u een IP-adres toevoegt of bewerkt, moet u kiezen of dat IP-adres is in- of uitgeschakeld. Selecteer de netwerkpoort waarop u dit IP-adres wilt laten werken. Het veld **IP-adres** stelt een adres in waarnaar uw B Series Appliance kan reageren; **Subnetmasker** stelt BeyondTrust in staat om te communiceren met andere apparaten.

Wanneer u een IP-adres bewerkt dat zich op hetzelfde subnet bevindt als een ander IP-adres voor het B Series Appliance, moet u kiezen of u dit IP-adres **Primair** wilt maken. Als dit vakje is aangevinkt, wordt dit IP-adres door het B Series Appliance aangewezen als het primaire of oorspronkelijke IP-adres voor het subnet. Dit kan handig zijn als u bijvoorbeeld zeker wilt zijn dat netwerkverkeer afkomstig van het B Series Appliance op dat subnet overeenkomt met en voldoet aan de gedefinieerde regels voor firewalls.

Vanaf **Toegangstype** kunt u toegang via dit IP-adres naar de publieke website of klant-client beperken. Selecteer **Beide toestaan** om toegang voor zowel de publieke website als de klant-client toe te staan.

> ***Opmerking:*** *U kunt toegang tot de **/login**-interface beperken door netwerkbeperkingen in te stellen onder **/login > Beheer > Beveiliging**. U kunt toegang tot de **/appliance**-interface beperken door netwerkbeperkingen in te stellen onder **/appliance > Beveiliging > Apparaatbeheer**.*

Wanneer het IP-adres voor beheer[1] wordt weergegeven, biedt het vervolgkeuzemenu **Telnet-server** drie instellingen: **Volledig**, **Vereenvoudigd** en **Uitgeschakeld**, zoals hieronder wordt uitgelegd. Deze instellingen veranderen de menu-opties van de Telnet-server die alleen op dit privé-IP-adres beschikbaar is en die kan worden gebruikt in geval van noodherstel. Aangezien de Telnet-functie specifiek verbonden is aan het ingebouwde privé-IP-adres, maakt hij geen onderdeel uit van andere geconfigureerde IP-adressen.

Instelling	Functie
Volledig	Schakelt de Telnet-server in met volledige functionaliteit
Vereenvoudigd	Biedt vier opties: **FIPS-fout weergeven**, **Op fabrieksinstellingen resetten**, **Afsluiten** en **Opnieuw opstarten**
Uitgeschakeld	Schakelt de Telnet-server volledig uit

[1]Verwijder of wijzig het IP-adres voor beheer niet.

SNMP: Simple Network Management Protocol inschakelen

Het BeyondTrust Appliance B Series ondersteunt Simple Network Management Protocol (SNMP). SNMP is een internet-standaardprotocol dat wordt gebruikt voor het bewaken en beheren van apparaten binnen een netwerk.

Hiermee kunnen hulpmiddelen die beschikbaarheid en andere statistieken via het SNMP-protocol verzamelen een query naar het B Series Appliance sturen voor controledoeleinden.

U kunt SNMP voor dit B Series Appliance inschakelen door **SNMPv2 inschakelen** of **SNMPv3 inschakelen** aan te vinken. Hierdoor kan een SNMPv2- of SNMPv3-server op SNMP-queries reageren. Voer een waarde in voor de **Alleen-lezen community-naam**, de **Systeemlocatie** en de **IP-beperkingen**, oftewel IP-adressen die queries naar dit B Series Appliance mogen sturen met behulp van SNMP.

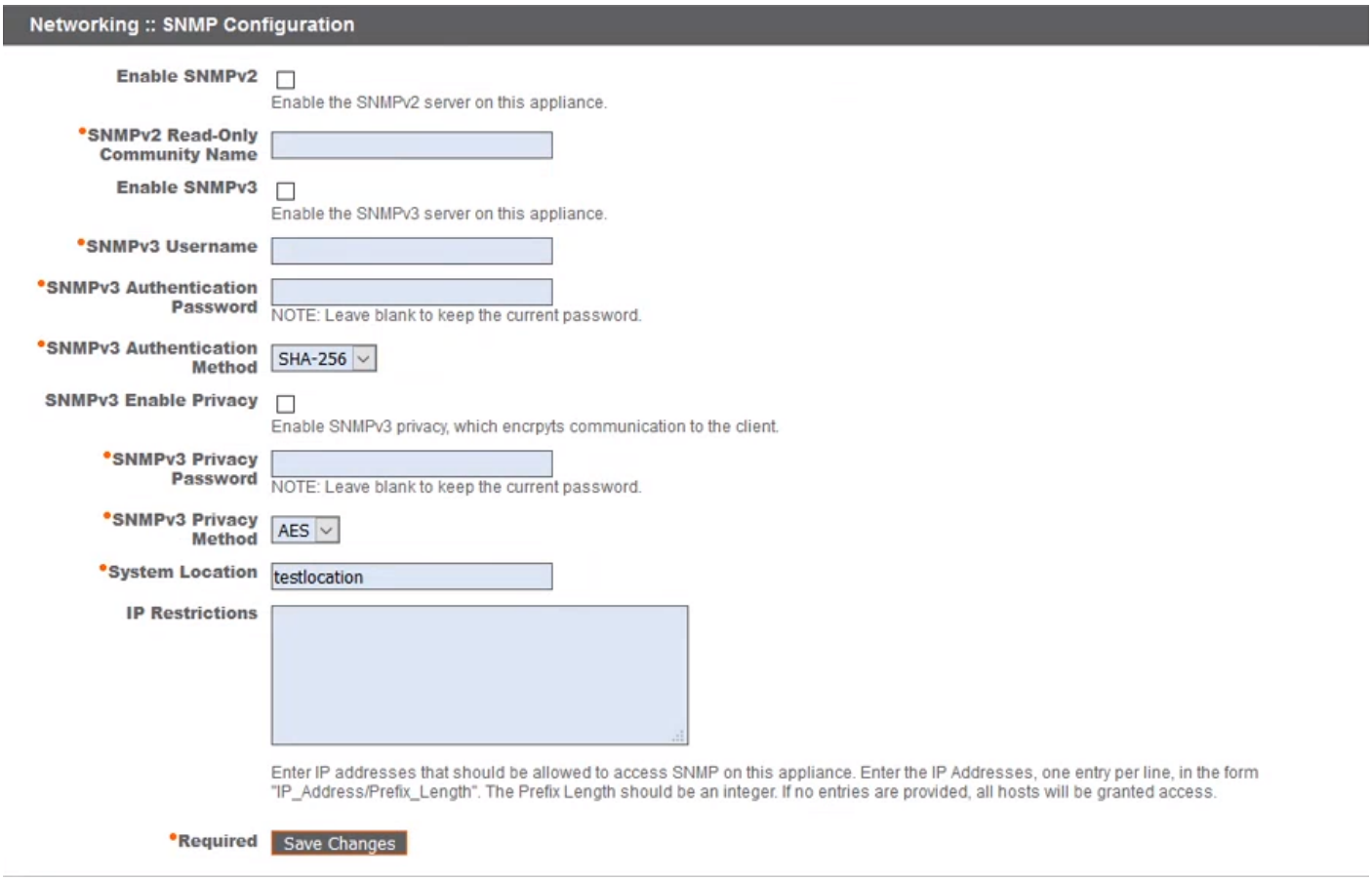
> ***Opmerking:*** *Als er geen IP-adressen worden ingevoerd in het veld* ***IP-beperkingen****, hebben alle hosts toegang.*

Als u SNMPv3 selecteert:

1. Vul een **gebruikersnaam** en **wachtwoord** in.
2. Selecteer de gewenste **Verificatiemethode** uit het vervolgkeuzemenu.
3. Vink **Privacy inschakelen op SNMPv3** als u communicatie met de client wilt versleutelen.
4. Voer een **Privacy-wachtwoord** in en selecteer een **Privacymethode**.

Klik op **Veranderingen opslaan** als u klaar bent.

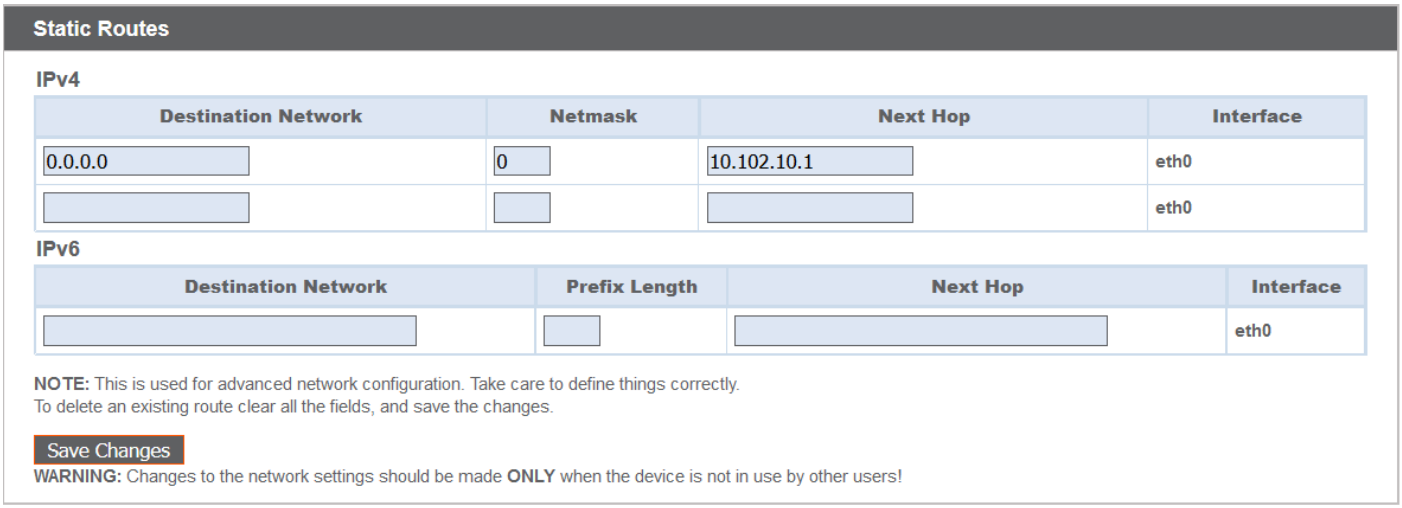
> *Ga naar Simple Network Management Protocol op wikipedia.org/wiki/Simple_Network_Management_Protocol voor meer informatie over SNMP.*



Statische routes: Statische routes voor netwerkcommunicatie instellen

Mocht zich een situatie voordoen waarbij twee netwerken niet met elkaar kunnen communiceren, dan kunt u een statische route maken zodat een beheerder met een computer op één netwerk via het B Series Appliance verbinding kan maken met een computer op het andere netwerk – mits het B Series Appliance zich ergens bevindt waar beide netwerken individueel met het apparaat kunnen communiceren.

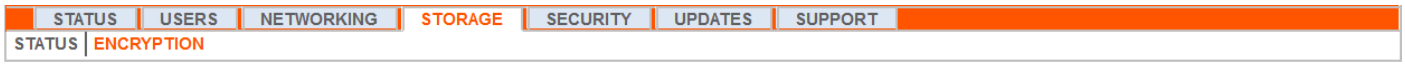
Het maken van statische routes is alleen geschikt voor gevorderde beheerders.



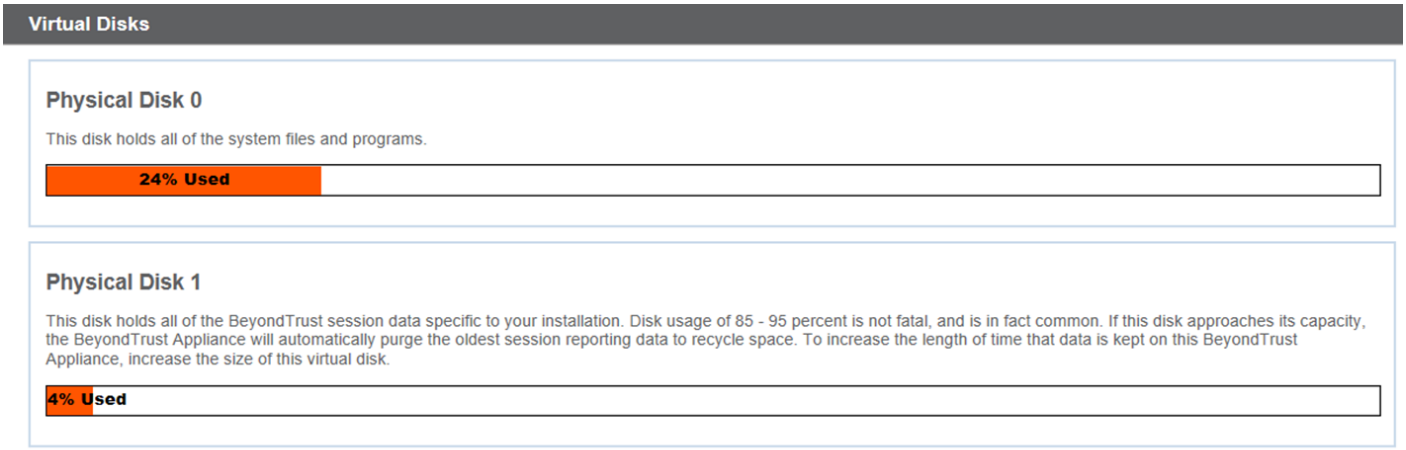
Opmerking: *Er kunnen ook statische routes worden gemaakt in de console. Zie voor meer informatie Configuratie van console voor veilige externe toegang op https://www.beyondtrust.com/nl/docs/privileged-remote-access/getting-started/deployment/hardware-sra/console.htm.*

Opslag

Status: Schijfruimte en status van harde schijf



De pagina **Status** geeft aan hoeveel procent van de harde schijf in uw B Series Appliance wordt gebruikt.



Als u alle opnamefunctie op uw website (sessies, protocol tunnelen en externe shell) hebt ingeschakeld of als u in het algemeen veel sessies hebt, ziet u gewoonlijk een hoger schijfgebruik. Let wel dat een schijfgebruik van 85-95% GEEN reden voor alarm is. Het B Series Appliance is zo geconfigureerd dat, mocht de beschikbare ruimte op uw harde schijf te laag zijn, de oudste sessiegegevens automatisch van het apparaat worden verwijderd en deze vrije ruimte opnieuw wordt gebruikt.

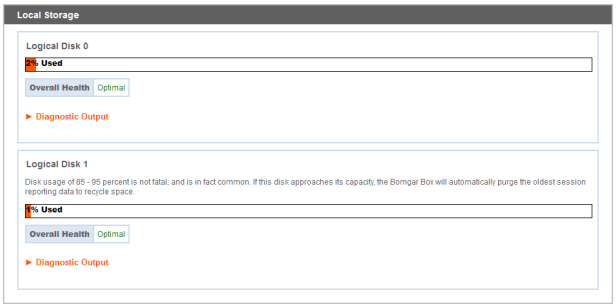
Specifiek voor de BeyondTrust B300P B Series Appliance

De B300P gebruikt een zogenaamd Redundant Array of Independent Disks (RAID) om uw gegevens op te slaan. Met RAID 6 kunnen maximaal 2 van de 4 schijven op uw B Series Appliance defect raken zonder verlies van gegevens. Als u een defecte schijf hebt, moet u deze verwijderen en contact met BeyondTrust opnemen voor een retourautorisatie voor reparatie of vervanging van de schijf. Nadat u de defecte schijf hebt vervangen, wordt de RAID automatisch met de nieuwe schijf herbouwd door het B Series Appliance. Wanneer u schijven vervangt, hoeft u het B Series Appliance niet uit te zetten.

Specifiek voor het BeyondTrust B400P B Series Appliance

De B400P bevat twee sets Redundant Array of Independent Disks (RAID) schijven. Deze RAID-configuratie bevat acht fysieke schijven geconfigureerd in twee logische RAID-schijven: Een RAID 1-configuratie die logische schijf 0 is en een RAID 6-configuratie die logische schijf 1 is.

Als een van de fysieke RAID 1- of RAID 6-schijven defect raakt, heeft dit geen invloed op de prestaties en is er geen gegevensverlies. Een tweede defecte schijf in de RAID 6-configuratie kan de prestaties echter negatief beïnvloeden, hoewel er geen gegevensverlies is.



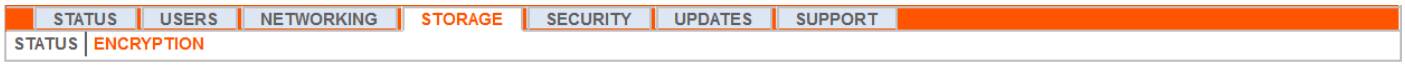
Waarschuwing defecte hardware (alleen B300P en B400P)

De LEDs op uw B Series Appliance geven tevens de status van uw harde schijf weer. In een normale situatie knipperen de LED's en geven daarmee de activiteit van de schijf aan. Als een schijf defect raakt, wordt de LED rood en klinkt er een waarschuwingsalarm. U kunt het alarm afzetten voordat het systeem wordt hersteld door op de knop **Alarm dempen** op deze web-interface te klikken.

Opmerking: *De knop **Alarm dempen** is beschikbaar ongeacht of er op dat moment een alarm klinkt. De knop kan niet worden gebruikt als indicator voor een actief alarm.*

Opmerking: *U kunt controleren of er een alarm klinkt door de **Conditie** aan te vinken direct boven de knop **Alarm dempen**. Als er een alarm klinkt in dezelfde ruimte als het B Series Appliance en u wilt uitsluiten dat het B Series Appliance de oorzaak is, kunt u een paar keer op de knop **Alarm dempen** klikken om alle mogelijke actieve alarmen uit te schakelen.*

Versleuteling: Sessiegegevens versleutelen

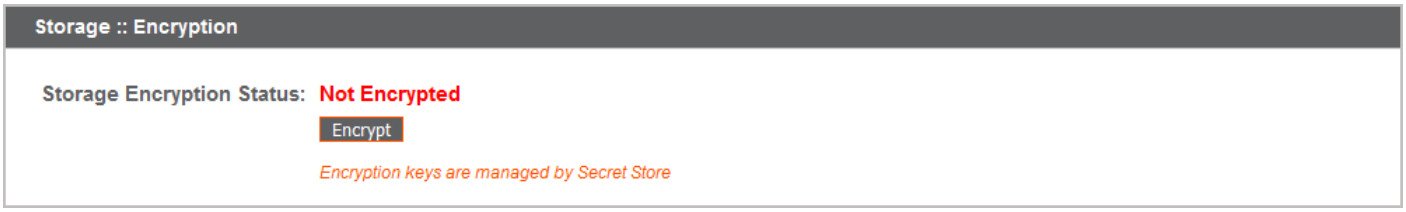


In het gedeelte **Versleuteling** kunt u sessiegegevens versleutelen die zijn opgeslagen op uw B Series Appliance. De eerste keer dat u uw gegevens versleutelt, kunt u maximaal 4 GB gegevens versleutelen, maar daarna is die beperking van 4 GB niet meer van toepassing.

Als u nog geen Secret Store hebt toegevoegd, ga dan naar **Beveiliging > Secret Store** om er een toe te voegen.

Ga voor meer informatie naar Secret Store.

***Opmerking:** Als u aan het begin meer dan 4 GB gegevens wilt versleutelen, neem dan contact op met BeyondTrust Technical Support www.beyondtrust.com/support.*



Beveiliging

Certificaten: TLS-certificaten maken en beheren

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

Beheer TLS-certificaten, maak zelf-ondertekende certificaten en certificaataanvragen en importeer certificaten die door een certificeringsautoriteit zijn ondertekend.

Installatie van certificaat

Het BeyondTrust Appliance B Series wordt geleverd met een zelf-ondertekend certificaat vooraf geïnstalleerd. Om uw B Series Appliance effectief te gebruiken, moet u echter ten minste een zelf-ondertekend certificaat aanmaken en bij voorkeur een door een certificeringsautoriteit ondertekend certificaat aanvragen en uploaden. Naast de functie voor een CA-certificaataanvraag bevat BeyondTrust een functie om eigen TLS-certificaten te verkrijgen en automatisch te verlengen via de open certificaatautoriteit Let's Encrypt.

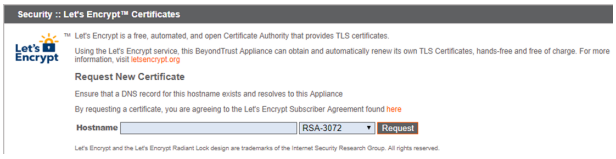
Let's Encrypt

Let's Encrypt geeft ondertekende certificaten af die 90 dagen geldig zijn en zichzelf automatisch oneindig kunnen verlengen. U moet aan de volgende vereisten voldoen om een Let's Encrypt-certificaat aan te vragen of om deze in de toekomst te verlengen:

- De DNS voor de hostnaam die u aanvraagt, moet uitkomen op het B Series Appliance.
- Het B Series Appliance moet toegang tot Let's Encrypt hebben via TCP-poort 443.
- Let's Encrypt moet toegang tot het B Series Appliance hebben via TCP-poort 80.

> *Ga voor meer informatie naar letsencrypt.org.*

Ga in het gedeelte **Beveiliging :: Let's Encrypt™-certificaten** als volgt te werk om een Let's Encrypt-certificaat te implementeren:



- Voer in het veld **Hostnaam** de volledig gekwalificeerde domeinnaam (FQDN) van het B Series Appliance in.
- Gebruik de vervolgkeuzelijst om het type certificaatsleutel te kiezen.
- Klik op **Aanvragen**.

Zolang aan bovenstaande vereisten wordt voldaan, resulteert dit in een certificaat dat automatisch elke 90 dagen zal worden verlengd nadat de geldigheidscontrole bij Let's Encrypt is uitgevoerd.

> ***Opmerking:*** *Het B Series Appliance start het proces voor het verlengen van het certificaat 30 dagen voordat het certificaat zal vervallen en vereist hetzelfde proces als voor de oorspronkelijke aanvraag. Als het proces 25 dagen voor het vervallen mislukt, stuurt het B Series Appliance dagelijks meldingen via e-mail naar de beheerder (als e-mailmeldingen zijn ingeschakeld). Het apparaat zal een foutmelding voor het certificaat weergeven.*

BELANGRIJK!

Omdat DNS slechts op één B Series Appliance apparaat tegelijk van toepassing kan zijn en omdat een B Series Appliance apparaat de DNS-hostnaam toegewezen moet krijgen waarvoor een certificaat- of verlengingsaanvraag wordt uitgevoerd, adviseren we u om geen Let's Encrypt-certificaten te gebruiken voor B Series Appliance twee apparaten waarvoor automatische omschakeling is geconfigureerd.

***Opmerking:** Als het aangevraagde certificaat een vervanging is, moet u de bestaande sleutel van het te vervangen certificaat selecteren.*

*Als het aangevraagde certificaat een vervangende sleutel moet krijgen, dan moet u de **Nieuwe sleutel** voor het certificaat selecteren.*

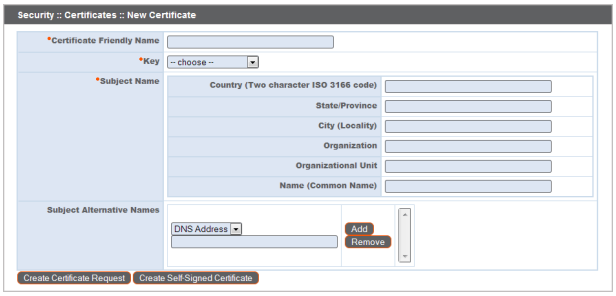
*Voor een vervangende sleutel moet alle informatie in de sectie **Beveiliging :: Certificaten :: Nieuw certificaat** gelijk zijn aan het certificaat waar u een vervangende sleutel voor aanvraagt. U moet een nieuwe vriendelijke naam voor het certificaat gebruiken zodat u het certificaat eenvoudig in de sectie **Beveiliging :: Certificaten** kunt terugvinden.*

*U kunt de vereiste informatie voor de vervangende sleutel verkrijgen door op het eerdere certificaat in de lijst in de sectie **Beveiliging :: Certificaten** te klikken.*

Voor een nieuwe sleutel of een vervangende sleutel zijn de stappen voor het importeren gelijk.

Overige certificaten die door een CA zijn uitgegeven

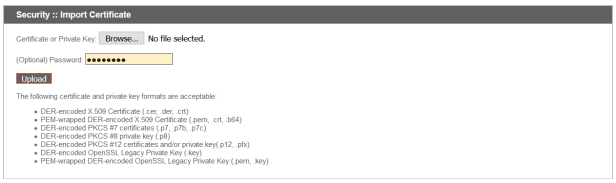
Ga als volgt te werk om een certificaataanvraag te maken:



- Ga naar **Beveiliging :: Overige certificaten** en klik op **Maken**.
- Voer bij **Beschrijvende naam van certificaat** een naam in die u gebruikt om dit certificaat te herkennen.
- Kies in het vervolgkeuzemenu **Sleutel** de optie **Bestaande sleutel** of uw *.beyondtrustcloud.com-certificaat.
- Voer de overige informatie over uw organisatie in.
- Voer in het veld **Naam (algemene naam)** een beschrijvende titel in voor uw BeyondTrust-site.
- Voer onder **Alternatieve namen voor onderwerp** de hostnaam van uw BeyondTrust-site in en klik op **Toevoegen**. Voeg een SAN toe voor alle DNS-namen of IP-adressen die door dit SSL-certificaat moeten worden beveiligd.

***Opmerking:** DNS-adressen kunnen worden ingevoerd als volledig gekwalificeerde domeinnamen, zoals toegang.voorbeeld.nl, of als domeinnaam met jokertekens, zoals *.voorbeeld.nl. Een domeinnaam met jokertekens beslaat meerdere subdomeinen, zoals toegang.voorbeeld.nl, extern.voorbeeld.nl, enzovoorts.*

Klik op **Certificaataanvraag aanmaken**.



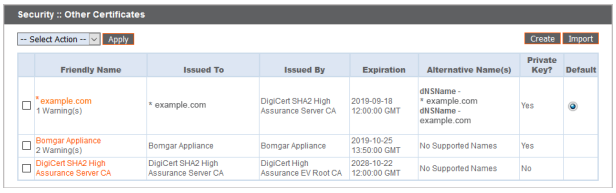
Om een door een CA ondertekend certificaat te gebruiken, moet u contact opnemen met een certificeringsautoriteit naar keuze en een nieuw certificaat kopen met behulp van het CSR dat u in BeyondTrust hebt gemaakt. De CA stuurt na aankoop een of meer nieuwe certificaatbestanden toe, die u op het B Series Appliance moet installeren.

Klik op **Importeren** om uw nieuwe certificaatbestanden te uploaden. Blader naar het eerste bestand en begin met uploaden. Herhaal dit voor alle certificaten die u van uw CA hebt ontvangen. Vaak stuurt een CA niet het basiscertificaat, dat wel op uw B Series Appliance moet worden geïnstalleerd. Als het basiscertificaat ontbreekt verschijnt de volgende waarschuwing onder uw nieuwe certificaat: 'Er ontbreken een of meer certificeringsautoriteiten in de certificaatketen en deze lijkt niet te eindigen in een zelf-ondertekend certificaat'.

Controleer of de informatie die u van uw certificaatautoriteit hebt ontvangen een koppeling bevat om het basiscertificaat voor uw B Series Appliance te downloaden. Als er geen is, moet u contact opnemen met de CA en er een aanvragen. Als dit niet praktisch is, ga dan naar hun website en zoek naar hun archief met basiscertificaten. Hier zijn alle basiscertificaten van de CA opgeslagen; alle belangrijke CA's publiceren hun basisarchief online.

Meestal kunt u de juiste hoofdmap voor uw certificaat het gemakkelijkst vinden door het certificaatbestand op uw lokale systeem te openen en **Certificaatpad** of **Certificaathiërarchie** te bekijken. De basis van deze hiërarchie of dit pad is meestal boven aan de boom weergegeven. Zoek naar dit basiscertificaat. Daarna kunt u het downloaden uit het basisarchief van de CA en in uw B Series Appliance importeren volgens de methode die hierboven is beschreven.

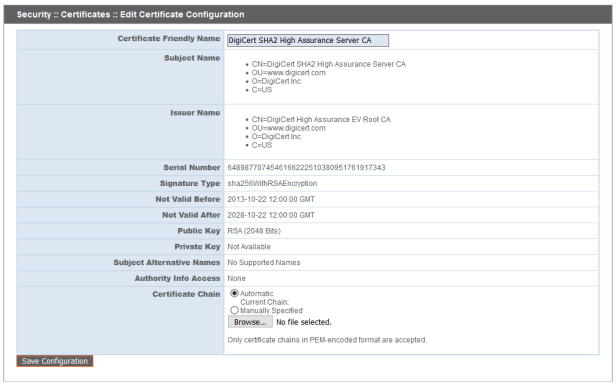
Certificaten



Geef een tabel weer van de SSL-certificaten die beschikbaar zijn op uw B Series Appliance.

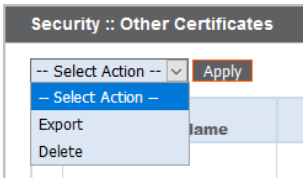
Voor verbindingen die geen Server Name Indication (SNI) of een onjuiste SNI opgeven, kunt u een standaard SSL-certificaat uit de lijst selecteren om deze verbindingen te maken door op de knop in de kolom **Standaard** te klikken. Het standaard SSL-certificaat kan geen zelf-ondertekend certificaat zijn –en evenmin het standaard B Series Appliance-certificaat dat voor de oorspronkelijke installatie is verstrekt.

> *Raadpleeg Server Name Indication op https://cio.gov/sni/ voor meer informatie over SNI.*

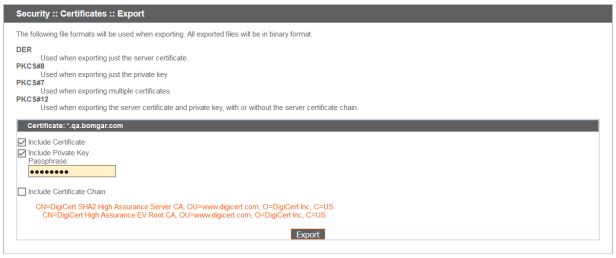


Klik op de naam van een certificaat om details weer te geven en de certificaatketen te beheren.

U kunt een of meer certificaten exporteren door de vakjes voor de betreffende certificaten aan te vinken. Selecteer vervolgens **Exporteren** in het vervolgkeuzemenu bovenaan de tabel en klik op **Toepassen**.

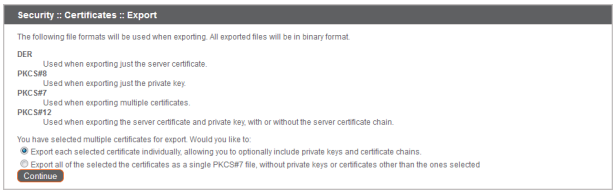


Als u maar één certificaat wilt downloaden, kunt u onmiddellijk kiezen om het certificaat en/of de certificaatketen op te nemen, als deze beschikbaar is. Klik op **Exporteren** om met downloaden te beginnen.

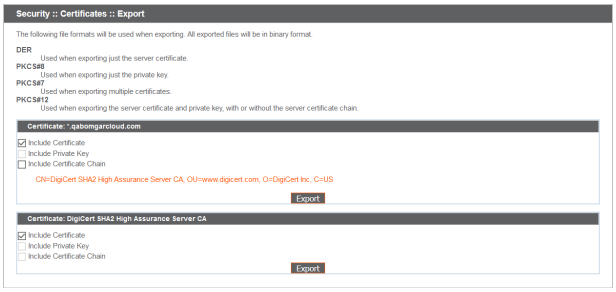


Als u meerdere certificaten wilt downloaden, kunt u of de individuele certificaten downloaden of alle certificaten samen in een PKCS#7=bestand.

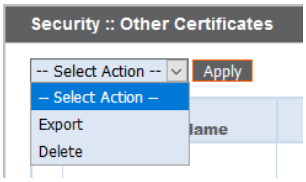
Wanneer u ervoor kiest meerdere certificaten als één bestand te downloaden, klikt u op **Doorgaan** om met downloaden te beginnen. Met deze optie worden alleen de certificaatbestanden zelf geëxporteerd –niet de certificaatketens.



Om ook de certificaatketens te exporteren, selecteert u individuele export en klikt u op **Doorgaan** om alle geselecteerde certificaten weer te geven. Voor elk certificaat op uw lijst, kunt u apart selecteren of u het certificaat en/of de certificaatketen, als deze beschikbaar is, wilt exporteren. Klik op **Exporteren** om met downloaden te beginnen.



U kunt een of meer certificaten verwijderen door voor elk gewenst certificaat het vakje aan te vinken en in het vervolgkeuzemenu bovenaan de tabel **Verwijderen** te selecteren. Klik vervolgens op **Toepassen**.

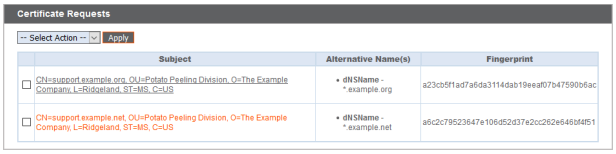


> ***Opmerking:*** *Onder normale omstandigheden worden certificaten nooit verwijderd, tenzij ze worden vervangen door een ander functionerend certificaat.*

Controleer of u de certificaten die u hebt aangevinkt, inderdaad wilt verwijderen en klik dan op **Verwijderen.**

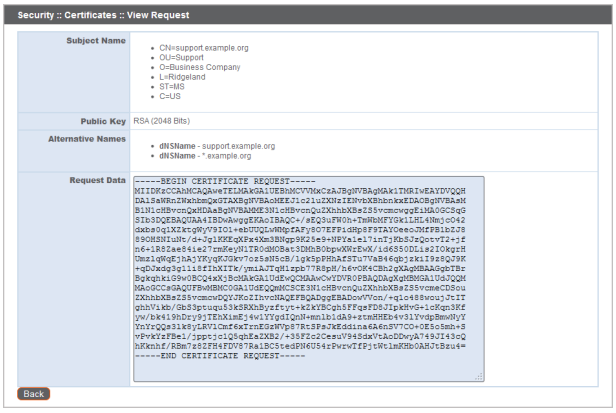
Certificaataanvragen

Geef een tabel weer van de aanvragen voor certificaten van derden die in behandeling zijn. Klik op de naam van een certificaataanvraag om details weer te geven.

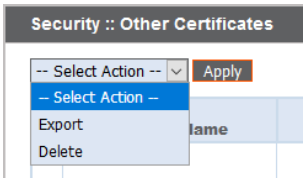


In de detailsweergave ziet u ook de aanvraaggegevens die u aan uw certificeringsautoriteit stuurt om een ondertekend certificaat aan te vragen.

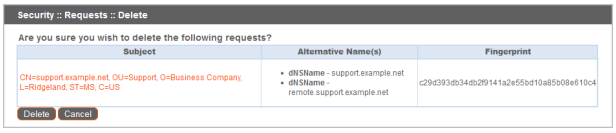
> ***Opmerking:*** *Als u een certificaat vernieuwt, gebruikt u dezelfde aanvraaggegevens als voor het oorspronkelijke certificaat.*



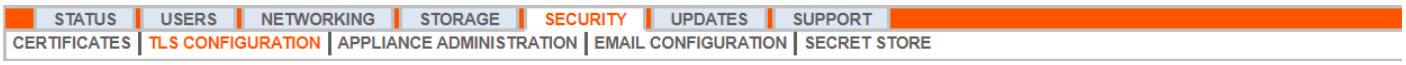
Om een of meer certificaataanvragen te verwijderen, vinkt u het vakje voor het gewenste certificaat aan en selecteert u **Verwijderen** in het vervolgkeuzemenu bovenaan de tabel. Daarna klikt u op **Toepassen**.



Controleer of u de certificaataanvragen die u hebt aangevinkt, inderdaad wilt verwijderen en klik dan op **Verwijderen**.



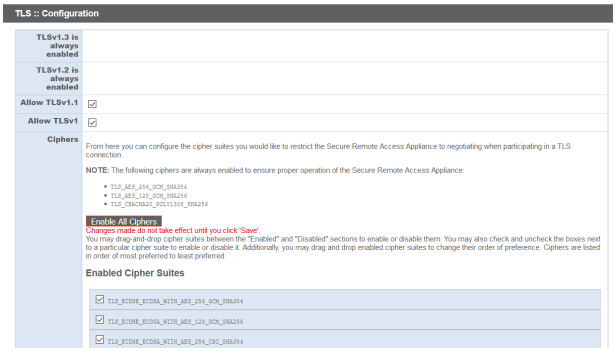
TLS-configuratie: Kies de TLS-coderingssuites en -versies



Let wel op dat sommige oudere browsers TLSv1.2 en TLSv1.3 niet ondersteunen. BeyondTrust staat u niet toe om zich aan te melden als u een of meer oudere beveiligingsprotocollen hebt uitgeschakeld en uw beheerinterface wilt openen via een oudere browser die de beveiligingsprotocollen die u hebt ingeschakeld niet ondersteunt.

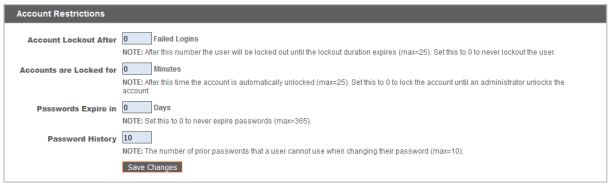
Deze instelling is voornamelijk van invloed op verbindingen met de web-interface van uw B Series Appliance. De tunnel voor ondersteuning tussen uw computer en die van uw klant gebruikt standaard TLSv1.2 ongeacht of u andere beveiligingsprotocollen hebt ingeschakeld.

Selecteer welke coderingspakketten op uw B Series Appliance moeten worden ingeschakeld of uitgeschakeld. Sleep de coderingsspakketten naar de gewenste plek om de voorkeursvolgorde te wijzigen. Wijzigingen in coderingspakketten worden pas van kracht nadat op **Opslaan** is geklikt.



Apparaatbeheer: Accounts, netwerken en poorten beperken, een STUN-server inschakelen, syslog instellen, inlogovereenkomst inschakelen, beheerdersaccount resetten

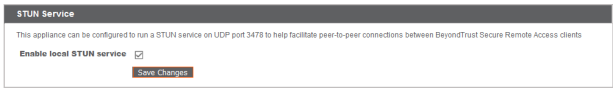
Beheer toegang tot de beheerinterface-accounts van /appliance door in te stellen hoeveel mislukte inlogpogingen toegestaan zijn. Stel in hoelang een account wordt geblokkeerd nadat de limiet voor mislukte inlogpogingen is overschreden. Stel het aantal dagen in dat een wachtwoord mag worden gebruikt voordat het vervalt en beperk het opnieuw gebruiken van eerdere wachtwoorden.



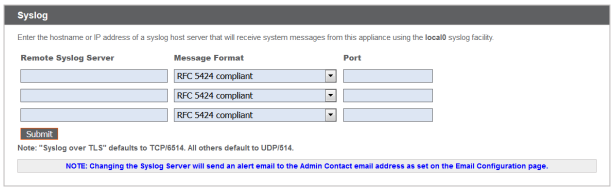
U kunt toegang tot de beheerinterface van uw B Series Appliance beperken door netwerkadressen in te stellen die wel en niet zijn toegestaan. Ook kunt u de poorten selecteren waardoor toegang kan worden verkregen tot deze interface.

In het veld **Geaccepteerde adressen** definieert u IP-adressen of netwerken die altijd toegang tot het /appliance hebben. In **Verworpen adressen** geeft u IP-adressen of netwerken op die altijd toegang tot de /appliance wordt geweigerd. Gebruik het vervolgkeuzemenu **Standaardactie** om aan te geven of u IP-adressen en netwerken die in geen van bovenstaande velden zijn vermeld, accepteert of weigert. In geval dat ze overlappen, krijgt de meest specifieke overeenkomst voorrang boven de andere.

Als u bijvoorbeeld toegang tot 10.10.0.0/16 wilt accepteren, maar toegang tot 10.10.16.0/24 weigert en toegang vanaf alle andere locaties afkeurt, moet u **10.10.0.0/16** in het veld **Geaccepteerde adressen** en **10.10.16.0/24** in het veld **Geweigerde adressen** invoeren en de **Standaardactie** instellen op **Weigeren**.



Het BeyondTrust Appliance B Series kan worden geconfigureerd om een STUN-service uit te voeren op UDP-poort 3478 om peer-to-peerconnecties tussen BeyondTrust-clients te faciliteren. Schakel het selectievakje **Lokale STUN-service inschakelen** in om deze functie te gebruiken.



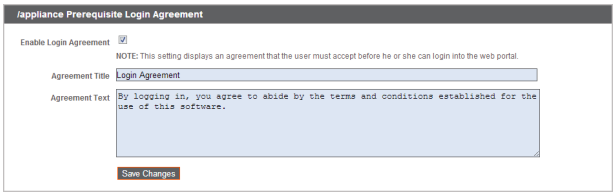
U kunt uw B Series Appliance zo configureren dat het logberichten verzendt naar maximaal drie syslog-servers. Voer in het veld **Externe Syslog-server** de hostnaam of het IP-adres in van de syslog-hostserver die systeemberichten van dit B Series Appliance ontvangt. Selecteer de gegevensindeling voor de gebeurteniswaarschuwingsberichten. Kies uit de standaardspecificatie **RFC 5424**, een van de legacy **BSD-indelingen** of **Syslog over TLS**. Syslog over TLS gebruikt standaard TCP-poort 6514. Alle andere indelingen maken standaard gebruik van UDP 514. De standaardinstellingen kunnen echter worden gewijzigd. B Series Appliance-logbestanden worden verzonden met behulp van de faciliteit **local0**.

Meer informatie over specifieke instellingen voor de cloud is te vinden in B Series Appliance-beheer: Syslog instellen via TLS op https://www.beyondtrust.com/docs/privileged-remote-access/getting-started/deployment/cloud/syslog-over-tls.htm.

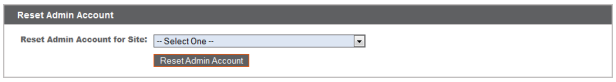
***Opmerking:** Wanneer een syslog-server wordt gewijzigd of toegevoegd, wordt er een waarschuwing naar het e-mailadres van de beheerder verzonden. De informatie over de beheerder wordt geconfigureerd via **Beveiliging > E-mailconfiguratie > Beveiliging :: Contactpersoon Admin**.*

Raadpleeg Naslag voor Syslog-berichten op www.beyondtrust.com/docs/privileged-remote-access/how-to/integrations/syslog/ voor een uitgebreide naslag van syslog-berichten.

U kunt een inlogovereenkomst activeren die gebruikers moeten accepteren voordat zij toegang krijgen tot het beheerinterface van /appliance. Met de overeenkomst, die u aan kunt passen, kunt u beperkingen en interne beleidsregels specificeren voordat gebruikers mogen inloggen.



U kunt een site selecteren en op **Beheerdersaccount opnieuw instellen** klikken als de gebruikersnaam is vergeten of moet worden vervangen. Daarmee worden de gebruikersnaam en het wachtwoord van de beheerder opnieuw ingesteld.



E-mailconfiguratie: B Series Appliance configureren om e-mailwaarschuwingen te verzenden

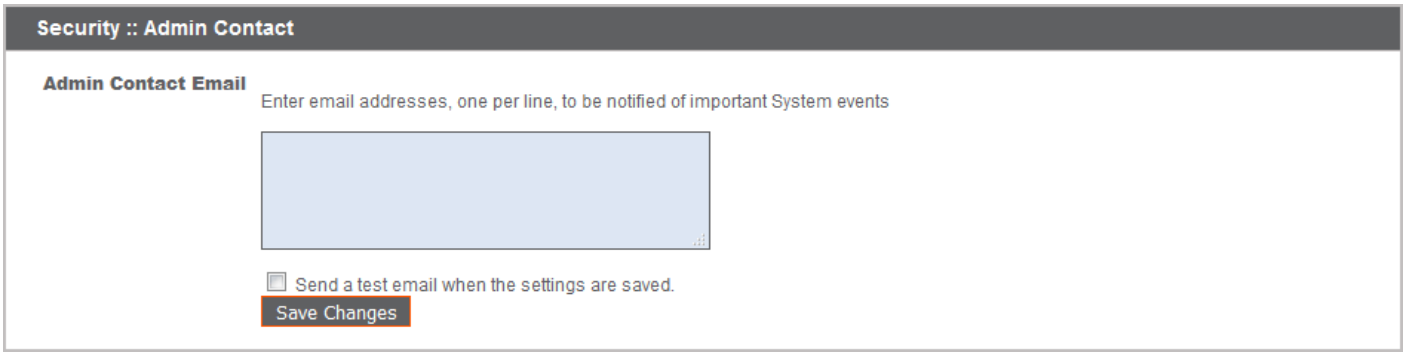
Uw B Series Appliance kan automatisch e-mailmeldingen naar u verzenden. E-mails worden verzonden bij de volgende gebeurtenissen:

- **Syslog-server is gewijzigd**: Een gebruiker op /appliance heeft de parameter voor de syslog-server gewijzigd.
- **RAID-gebeurtenis**: Een of meer logische RAID-stations is/zijn niet in optimale staat (achteruitgegaan of gedeeltelijk achteruitgegaan).
- **Kennisgeving van verlopen van SSL-certificaat**: Een SSL-certificaat dat in gebruik is (betreft identiteitscertificaten of een CA-certificaat in de keten) verloopt binnen 90 dagen.

Configureren via SMTP

> ***Opmerking:*** *Deze methode werkt niet voor bepaalde e-maildiensten. Bekijk* *"Configureren via OAuth2 voor Microsoft Azure AD" op pagina 28* *of* *"Configureren via OAuth2 voor Google" op pagina 30* *voor alternatieve configuraties.*

Nadat u de e-mailadressen van de admin-contactpersonen hebt ingevoerd, kunt u uw instellingen opslaan en een testmail verzenden om te controleren of alles naar behoren werkt.



Configureren via OAuth2 voor Microsoft Azure AD

Configuratie vereist dat instellingen worden gewijzigd op het BeyondTrust-apparaat en in het Microsoft 365-abonnement met Azure AD.

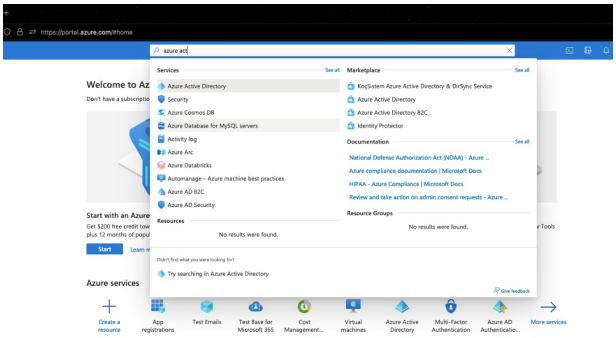
Begin met de instellingen te wijzigen op het BeyondTrust-apparaat:

1. Ga naar **Apparaat**, klik op het tabblad **Beveiliging** en klik vervolgens op **E-mailconfiguratie**.
2. Wijzig de **Verificatiemethode** in OAuth2
3. Noteer de **URI van autorisatie-omleiding**. Deze hebt u later nodig.

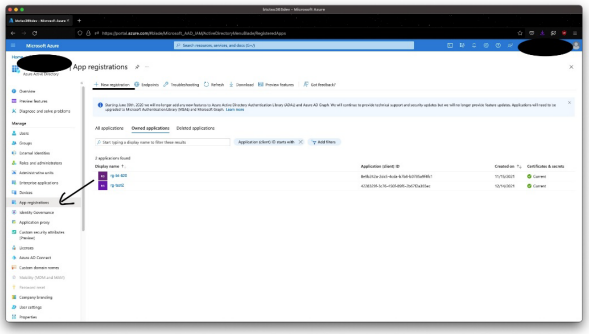
Voordat er gestart kan worden met de configuratie op de Azure Active Directory, moet een Azure/Office 365-beheerder geverifieerde SMTP inschakelen voor elke account op Exchange online. U doet dit door naar **Office 365-beheerportal (admin.microsoft.com) > Actieve gebruikers > E-mail > E-mailtoepassingen beheren** te gaan en **Geverifieerde SMTP** aan te vinken.

Nadat **Geverifieerde SMTP** is ingeschakeld, voert u de volgende stappen uit in de Azure-console:

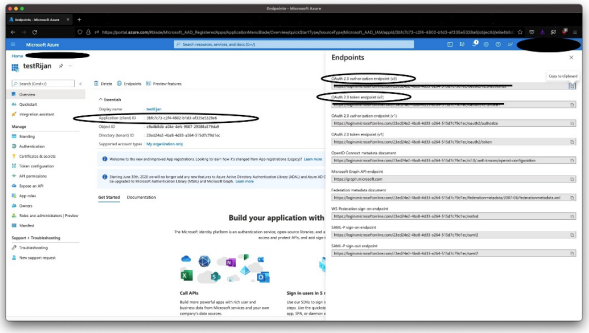
4. Log in op uw Azure-console (portal.Azure.com).
5. Ga naar **Azure Active Directory**.



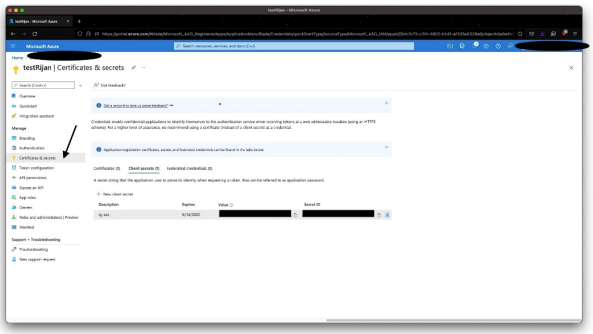
6. Ga naar **App-registraties** en selecteer **Nieuwe registratie**.
7. Voer een naam, bijv. Appliance-OAuth2.
8. Selecteer de accountsoorten die u wilt toestaan om zich aan te melden bij de toepassing via OAuth2. Selecteer **Eén tenant** alleen voor intern.
9. Voer de **Omleidings-URI** in. Dit is de **URI van autorisatie-omleiding** die verkregen is vanuit het BeyondTrust-apparaat aan het begin van dit proces.
10. Klik op **Registreren**.
11. Op de **Overzichtspagina** (geselecteerd uit het linker menu) staat de **Toepassing (client) ID**. Noteer deze. Deze hebt u later nodig.



12. Klik op **Eindpunten** (boven de **Toepassing (client) ID**).
13. Noteer het **OAuth2.0 autorisatie-eindpunt (v2)** URI en het **OAuth token-eindpunt (v2)** URI. Deze hebt u later nodig.



14. Op de pagina **Certificaten & geheimen** (geselecteerd uit het linker menu) staat het **Clientgeheim**. Noteer dit. Deze hebt u later nodig. Als u geen **Clientgeheim** hebt, klikt u op **Nieuw clientgeheim** om er één aan te maken.



De resterende stappen worden uitgevoerd op het BeyondTrust-apparaat.

15. Ga naar **Apparaat**, klik op het tabblad **Beveiliging** en klik vervolgens op **E-mailconfiguratie**.
16. Vul de volgende informatie in die u eerder hebt genoteerd:
    - **Eindpunt-autorisatie**
    - **Eindpunt-token**
    - **Client-ID**
    - **Clientgeheim**
17. Voer het e-mailadres voor deze service in als **Verzenden vanaf e-mailadres** en de **E-mail van de gebruiker**.

> ***Opmerking:*** *Deze adressen moeten overeenkomen en een geldige account voor Azure zijn. Als u Anonieme e-mail (E-mail verzenden vanaf willekeurig adres) hebt ingeschakeld voor de Azure Tenant, kunt u een willekeurig adres invullen in het e-mailveld. Zo niet, gebruik dan de gebruikersnaam van de eigenaar van de toepassing en de Toegestane gebruikers.*

18. Voer gegevens in bij de velden **Host**, **Versleuteling** en **Poort**.
    - **Host**: smtp.office365.com
    - **Versleuteling**: STARTTLS
    - **Poort**: 587

> ***Opmerking:*** *Standaardgegevens voor Azure worden weergegeven, maar het kan zijn dat uw installatie een andere host of versleutelingsmethode gebruikt. De poort is van toepassing voor STARTTLS, andere versleutelingsmethodes maken wellicht gebruik van een andere poort.*

19. Voer uw TLS-certificaat in, als u hierover beschikt. Zo niet, vink dan **TLS-certificaatfouten negeren** aan.
20. Voer bij **Bereiken** het volgende in: https://outlook.office.com/SMTP.Send offline_access
21. Klik op **Veranderingen opslaan**.
22. Klik op **Autoriseren**. Accepteer het verzoek voor machtigingen op de aanmeldpagina die wordt weergegeven. De pagina met e-mailinstellingen wordt opnieuw geladen en de autorisatie-knop wordt vervangen door het bericht 'geautoriseerd'.
23. Zo kunt u de configuratie testen:
    - Voeg een **E-mail van beheerdercontactpersoon** toe.
    - Vink **Teste-mail verzenden** aan.
    - Klik op **Veranderingen opslaan**.

Configureren via OAuth2 voor Google

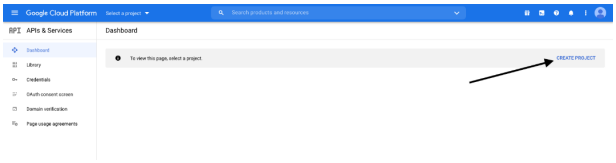
Configuratie vereist dat instellingen worden gewijzigd op het BeyondTrust-apparaat en in het Google Cloud Platform.

Begin met de instellingen te wijzigen op het BeyondTrust-apparaat:

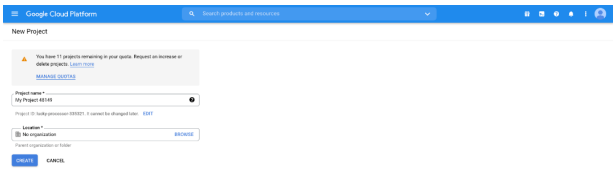
1. Ga naar **Apparaat**, klik op het tabblad **Beveiliging** en klik vervolgens op **E-mailconfiguratie**.
2. Wijzig de **Verificatiemethode** in OAuth2
3. Noteer de **URI van autorisatie-omleiding**. Deze hebt u later nodig.

Meld u aan bij uw Google Cloud Platform-console (Google Dev-console) (console.cloud.google.com). Let erop dat u het juiste Gmail-account gebruikt, want alleen de eigenaar van het project kan met het project werken. Als u nog niet over een betaalde account beschikt, kunt u ervoor kiezen om een account aan te schaffen door in de banner bovenaan te klikken op **Activeren**. BeyondTrust kan geen hulp bieden bij het aanschaffen van een account. Klik op **Meer informatie** in de banner bovenaan voor informatie over de beperkingen van gratis accounts.

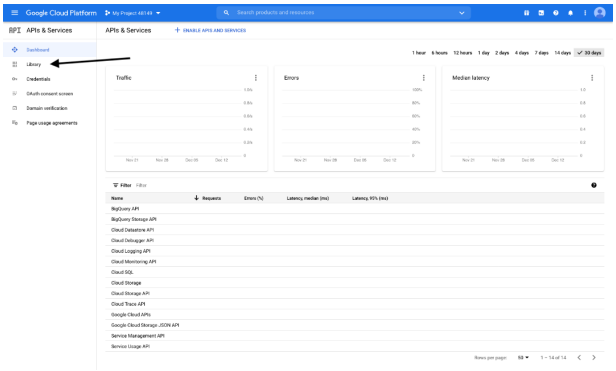
4. Klik op **PROJECT MAKEN**. U kunt ook een bestaand project gebruiken.



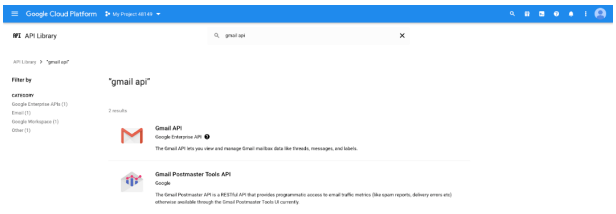
5. Accepteer de standaard **Projectnaam** of vul een naam in.
6. Accepteer de standaard **Locatie** of selecteer een map uit de mappen die voor uw organisatie beschikbaar zijn.
7. Klik op **MAKEN**.



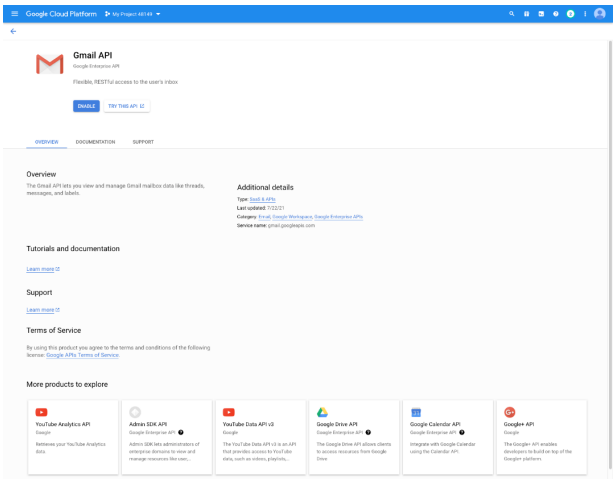
8. De pagina **API's en services** verschijnt. Klik op **Bibliotheek** in het linker menu.



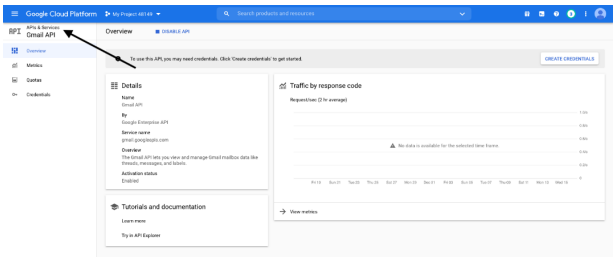
9. Zoek of blader naar de **Gmail API** in de bibliotheek en klik erop.



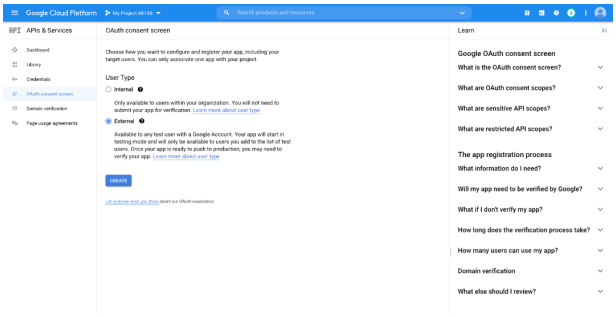
10. De **Gmail API** verschijnt op een eigen pagina. Klik op **INSCHAKELEN**.



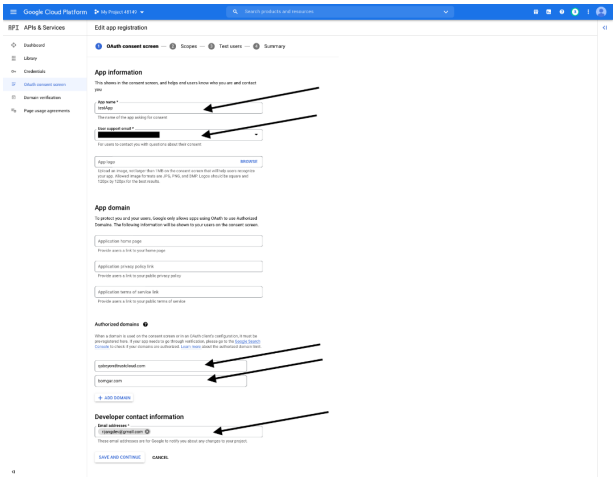
11. The pagina **Gmail API-overzicht** verschijnt. Klik op **API's & services** links bovenaan.
12. De pagina **API's en services** verschijnt opnieuw. Klik op het **OAuth-instemmingsscherm** in het linker menu.



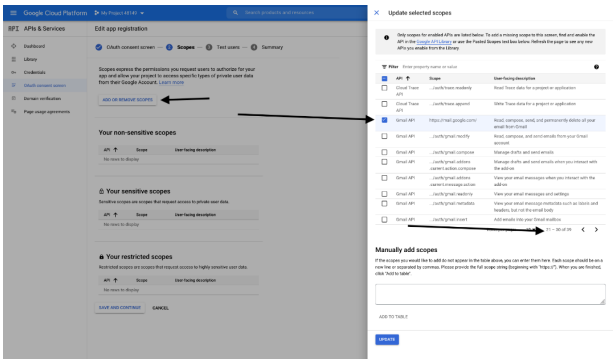
13. Selecteer het **Gebruikerstype**. Intern staat alleen gebruikers van binnen de organisatie toe, maar vereist wel een Google Workspace-account.
14. Klik op **MAKEN**.



15. Voer de **App-naam** in.
16. Voer een **E-mailadres voor gebruikersondersteuning** in. Dit kan het standaard e-mailadres zijn dat u gebruikt om het project aan te maken.
17. Voer desgewenst een logo voor de app in. Het onderdeel **App-domein** is ook optioneel.
18. Voeg de **Geautoriseerde domeinen** toe. Voor BeyondTrust-testapparaten zijn dit:
    - qabeyondtrustcloud.com
    - bomgar.com
19. Voer de **Contactgegevens van de ontwikkelaar** in. Dit is het e-mailadres dat u gebruikt om het project aan te maken.
20. Klik op **OPSLAAN EN DOORGAAN**.

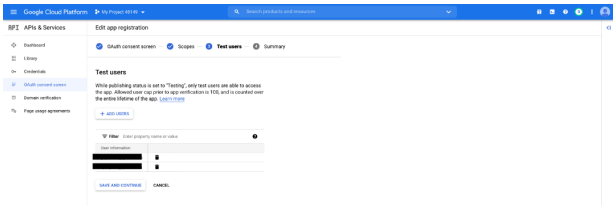


21. Klik onder het tabblad **Bereiken** op **BEREIKEN TOEVOEGEN OF VERWIJDEREN**. Hierdoor wordt het venster **Geselecteerde bereiken bijwerken** geopend.
22. Zoek het bereik **https://mail.google.com/** voor de Gmail API en vink het aan.

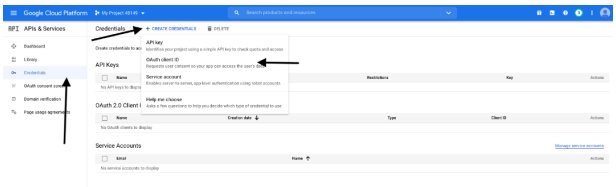


> ***Opmerking:*** *De API wordt niet weergegeven, als deze niet is ingeschakeld.*

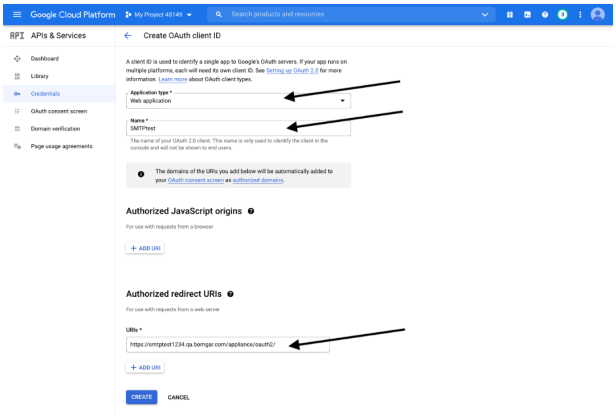
23. Klik op **BIJWERKEN**. Het venster **Geselecteerde bereiken bijwerken** wordt gesloten.
24. Klik op **OPSLAAN EN DOORGAAN**.
25. Klik onder het tabblad **Testgebruikers** op **GEBRUIKERS TOEVOEGEN**. Hierdoor wordt het venster **Gebruikers toevoegen** geopend. Voeg de gebruikers toe die toegang hebben tot de toepassing en klik op **TOEVOEGEN**. Let op de limieten voor testgebruikerstoegang en bijbehorende beperkingen.
26. Klik op **OPSLAAN EN DOORGAAN**.
27. Bekijk het overzicht en breng waar nodig wijzigingen of correcties aan.
28. Klik op **TERUG NAAR DASHBOARD**.



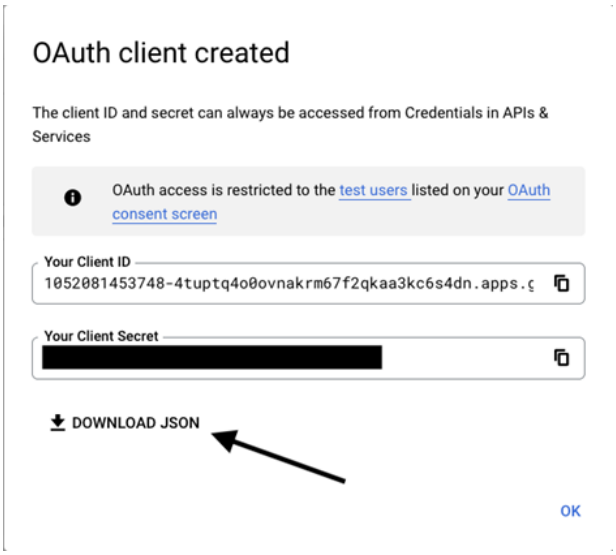
29. Klik op **Inloggegevens** in hert linker menu.
30. Klik op **INLOGGEGEVENS MAKEN** in de banner bovenaan en selecteer **OAuth client-ID**.



31. Op de pagina Inloggegevens maken selecteert u **Webtoepassing** voor het **Type toepassing**. Er worden extra velden weergegeven als dit is geselecteerd.
32. Voer een naam in voor de toepassing.
33. Scroll omlaag naar **Geautoriseerde omleiding-URI's** en klik op **URI TOEVOEGEN**.
34. Voer de **URI van autorisatie-omleiding** in die verkregen is vanuit het BeyondTrust-apparaat aan het begin van dit proces.
35. Klik op **MAKEN**.



36. Een venster bevestigt het aanmaken van de OAuth-client en geeft de **Client-ID** en het **Clientgeheim** weer. Klik om een JSON-bestand te downloaden. Het bestand bevat informatie die nodig is bij de volgende stappen.
37. Klik op **OK** om terug te keren naar de pagina API's en services.



De resterende stappen worden uitgevoerd op het BeyondTrust-apparaat.

38. Ga naar **Apparaat**, klik op het tabblad **Beveiliging** en klik vervolgens op **E-mailconfiguratie**.
39. Voer de volgende informatie in, die in het gedownloade JSON-bestand is gevonden:
    - **Eindpunt-autorisatie**
    - **Eindpunt-token**
    - **Client-ID**
    - **Clientgeheim**
40. Voer een e-mailadres in voor deze service als het **Verzenden vanaf e-mailadres**.
41. Voer **E-mailadres van de gebruiker** in. Dit moet een e-mailadres zijn dat is ingevoerd als **Testgebruiker** met toegang tot de toepassing, toen u de OAuth-instemmingspagina's hebt doorlopen.
42. Voer gegevens in bij de velden **Host**, **Versleuteling** en **Poort**.
    - **Host**: smtp.gmail.com
    - **Versleuteling**: TLS
    - **Poort**: 465

> ***Opmerking:*** *Standaardgegevens voor Google worden weergegeven, maar het kan zijn dat uw installatie een andere host of versleutelingsmethode gebruikt. De poort is van toepassing voor TLS, andere versleutelingsmethodes maken wellicht gebruik van een andere poort.*

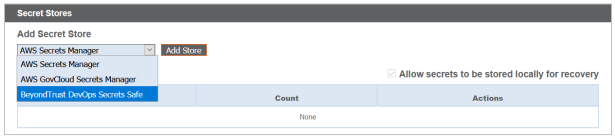
43. Voer uw TLS-certificaat in, als een dergelijk certificaat verstrekt is door Google. Zo niet, vink dan **TLS-certificaatfouten negeren** aan.
44. Voer bij **Bereiken** het volgende in: https://mail.google.com
45. Klik op **Veranderingen opslaan**.
46. Klik op **Autoriseren**. Nadat de aanmeldingspagina wordt weergegeven, krijgt u wellicht de waarschuwing **Google heeft dit bericht niet gecontroleerd**, als u de toepassing niet gepubliceerd hebt. De instemmingspagina wordt opnieuw geladen en de autorisatie-knop wordt vervangen door een bericht dat het geautoriseerd is.

47. Zo kunt u de configuratie testen:
    - Voeg een **E-mail van beheerdercontactpersoon** toe.
    - Vink **Teste-mail verzenden** aan.
    - Klik op **Veranderingen opslaan**.

Geheimenarchief: Opslag van en toegang tot geheimen

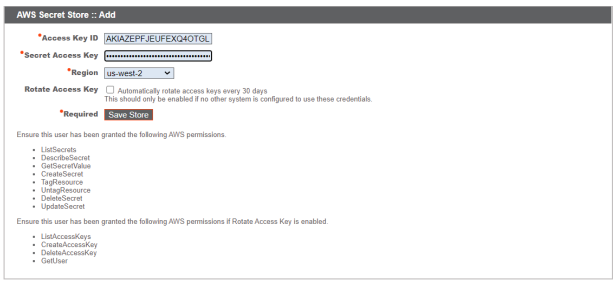
STATUS | USERS | NETWORKING | STORAGE | SECURITY | UPDATES | SUPPORT
CERTIFICATES | TLS CONFIGURATION | APPLIANCE ADMINISTRATION | EMAIL CONFIGURATION | SECRET STORE

Geheime codes aanmaken en beheren in AWS en BeyondTrust DevOps Secrets Safe (DSS) om versleutelde codes en sitegegevens veilig op te slaan. Om een geheimenarchief toe te voegen, selecteert u het archief uit het vervolgkeuzemenu en vervolgens klikt u op **Archief toevoegen**. Volg onderstaande stappen om de informatie voor het archief in te vullen en op te slaan.



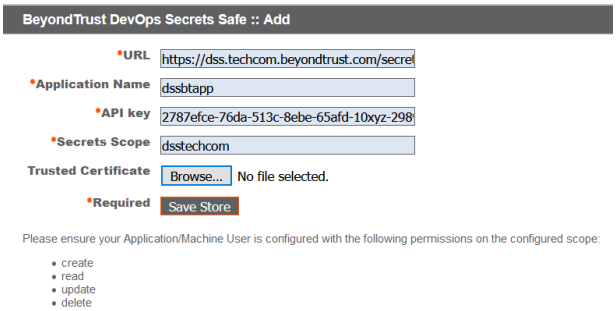
AWS-geheimenarchief toevoegen

1. Vul de **Toegangscode-ID**, **Geheime toegangscode** en **Regio** in.
2. Vink het vakje **Toegangscode roteren** alleen dan aan als u de inloggegevens niet in een ander systeem gebruikt.
3. Klik op **Archief opslaan**.



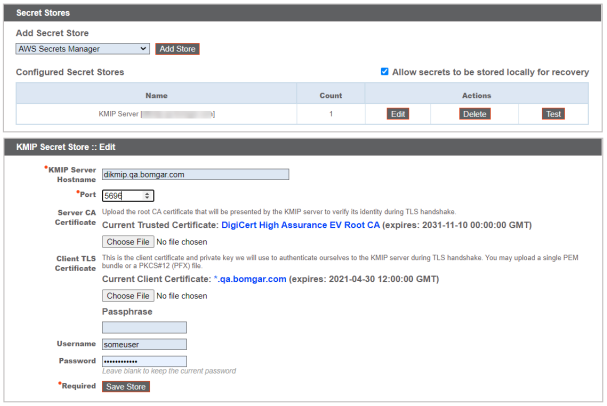
BeyondTrust DevOps Secrets Safe-archief toevoegen

1. Voer de **URL** voor uw DSS-exemplaar in.
2. Geef de **Toepassingsnaam** op die u binnen DSS hebt geconfigureerd.
3. Geef de **API-sleutel** op die binnen DSS is gegenereerd voor de toepassing.
4. Voer het **Geheimen-bereik** in dat u met machtigingen binnen DSS hebt geconfigureerd.
5. Als u een zelf ondertekend certificaat gebruikt in DSS, voeg dan het **Vertrouwd certificaat** toe. Als u een CA-certificaat gebruikt, hoeft u geen vertrouwd certificaat te verstrekken.
6. Klik op **Archief opslaan**.



Nadat een geheimenarchief is toegevoegd, klikt u op **Testen** om de connectiviteit met de server van het geheimenarchief te controleren en om u ervan te verzekeren dat de juiste machtigingen voor de inloggegevens van kracht zijn om toegang tot de server van het geheimenarchief te kunnen krijgen.

Opmerking: *Het configureren van een KMIP-server voor een versleuteld archief wordt niet meer ondersteund in versie 6.0 en latere versies. Als u een KMIP-server geconfigureerd hebt voor uw versleuteling vóór versie 6.0, wordt uw KMIP-server verplaatst naar de lijst met het Geheimenarchief; daar kunt u het archief bewerken, verwijderen en testen.*



Opmerking: *Voor extra veiligheid kunt u uw AWS Identity and Access Management (IAM)-beleid configureren om toegang te beperken tot hulpbronnen die overeenkomen met* ***BeyondTrust-**** *wat betreft de volgende machtigingen:*

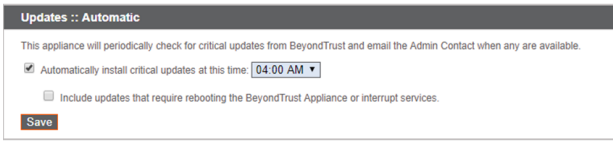
- *DescribeSecret*
- *GetSecretValue*
- *TagResource*
- *UntagResource*
- *CreateSecret*
- *DeleteSecret*
- *UpdateSecret*

Meer informatie over he beheren van AWS IAM-beleid vindt u onder IAM-beleid beheren op https://docs.aws.amazon.com/IAM/latest/UserGuide/access_policies_manage.html.

Opmerking: *Als u het laatste externe archief verwijdert, verschijnt er een bericht met de mededeling dat geheimen naar lokaal verplaatst zullen worden.*

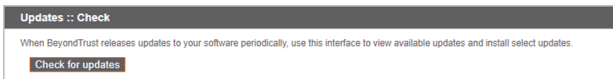
Updates: Op beschikbare updates controleren en software installeren op Privileged Remote Access

Het B Series Appliance controleert op gezette tijden op belangrijke updates en stuurt een e-mail naar de beheercontactpersoon wanneer updates beschikbaar zijn. U kunt kiezen of u de updates automatisch wilt installeren en het vervolgkeuzemenu gebruiken om een tijdstip voor de installatie te selecteren.



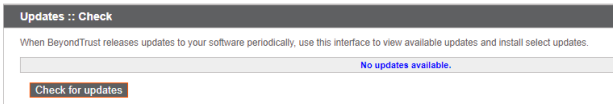
Updates waarbij een B Series Appliance opnieuw moet worden opgestart of waarbij een serviceonderbreking plaatsvindt, kunnen niet automatisch worden uitgevoerd, tenzij u het vakje aanvinkt dat ze wel uitgevoerd moeten worden.

BeyondTrust blijft u informerenu tevens over de meest recente builds wanneer deze beschikbaar zijn . Wanneer u een bericht ontvangt dat er nieuwe updatepakketten voor uw B Series Appliancebeschikbaar zijn, klikt u op de knop **Op updates controleren**, waarna de pakketten voor u worden klaargezet om te installeren.

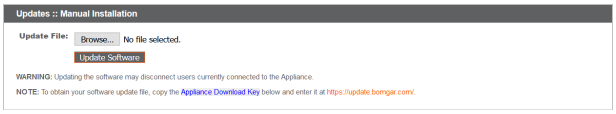


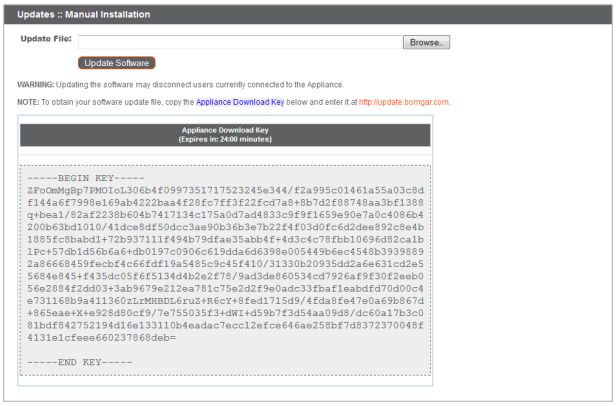
Als er meerdere softwarepakketten voor uw B Series Appliance beschikbaar zijn, wordt elk pakket apart vermeld in de lijst met beschikbare updates. Wanneer u op de betreffende knop **Deze update installeren** klikt, wordt uw nieuwe software wordt automatisch gedownload en geïnstalleerd.

Als er geen updatepakketten of patches voor uw B Series Appliance beschikbaar zijn, wordt het bericht 'Er zijn geen updates beschikbaar' weergegeven. Als een update beschikbaar is, maar er treedt een fout op tijdens het updaten van uw B Series Appliance, wordt er een aanvullend bericht weergegeven, zoals 'Er is een fout opgetreden tijdens het uitvoeren van uw update. Kijk op www.beyondtrust.com/support voor meer informatie.'



Het is niet verplicht om de functie **Op updates controleren** te gebruiken. Als het beveiligingsbeleid van uw organisatie automatische updates niet toestaat, kunt u handmatig op updates controleren. Klik op de koppeling **Downloadsleutel van een apparaat** om een unieke B Series Appliance-sleutel te genereren. Vervolgens kunt u die sleutel vanaf een systeem zonder restricties verzenden naar een updateserver van BeyondTrust op https://btupdate.com. Download eventuele beschikbare updates op een verwisselbaar opslagapparaat en breng die updates dan naar een systeem over waarvandaan u uw B Series Appliance kunt beheren.





Nadat u de software hebt gedownload, zoekt u vanuit het gedeelte **Handmatige installatie** naar het bestand en klikt u op de knop **Software bijwerken** om de installatie uit te voeren.

BELANGRIJK!

Wees erop voorbereid dat u de software-updates direct na het downloaden installeert. Als een update eenmaal is gedownload, dan verschijnt deze niet meer in uw lijst met beschikbare updates. Neem contact op met BeyondTrust Technical Support als u een software-update opnieuw moet downloaden.

Als het scherm met de Gebruiksrechtovereenkomst (EULA) van BeyondTrust wordt weergegeven, moet u de vereiste contactinformatie invullen en op de knop **Akkoord - Begin met downloaden** klikken om de EULA te accepteren en door te gaan met de installatie.

NB: Als u besluit om de Gebruiksrechtovereenkomst niet te accepteren, wordt er een foutmelding weergegeven en kunt u uw BeyondTrust-software niet bijwerken.

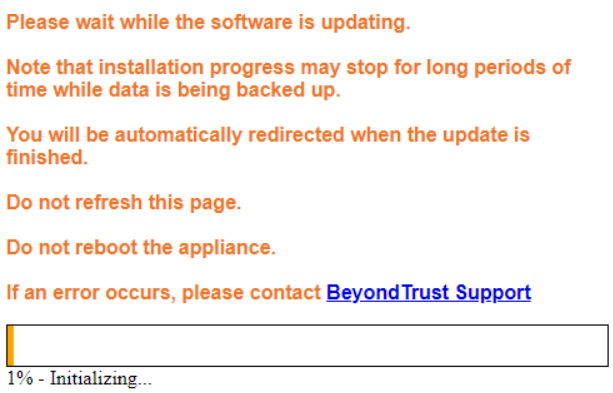
Neem contact op met BeyondTrust Technical Support via www.beyondtrust.com/support als u problemen ondervindt bij het bijwerken nadat u de Gebruiksrechtovereenkomst hebt geaccepteerd.

Tijdens het installeren, verschijnt op de pagina **Updates** een voortgangsbalk om u over het algehele installatieproces te informeren. Updates die hier worden toegepast, worden automatisch toegepast alle sites en licenties op uw B Series Appliance.

Als u een software-update installeert, kunnen ingelogde gebruikers tijdelijk te maken krijgen met een onderbreking van hun verbinding met access sessions en de toegangsconsole; plan uw updates daarom op een rustig moment. Als uw updatepakket echter alleen extra licenties bevat, kunt u de update installeren zonder de verbinding voor gebruikers hoeft te onderbreken.

Ga voor actuele informatie over de meest recente updates voor BeyondTrust naar https://www.beyondtrust.com/docs/release-notes/index.htm.

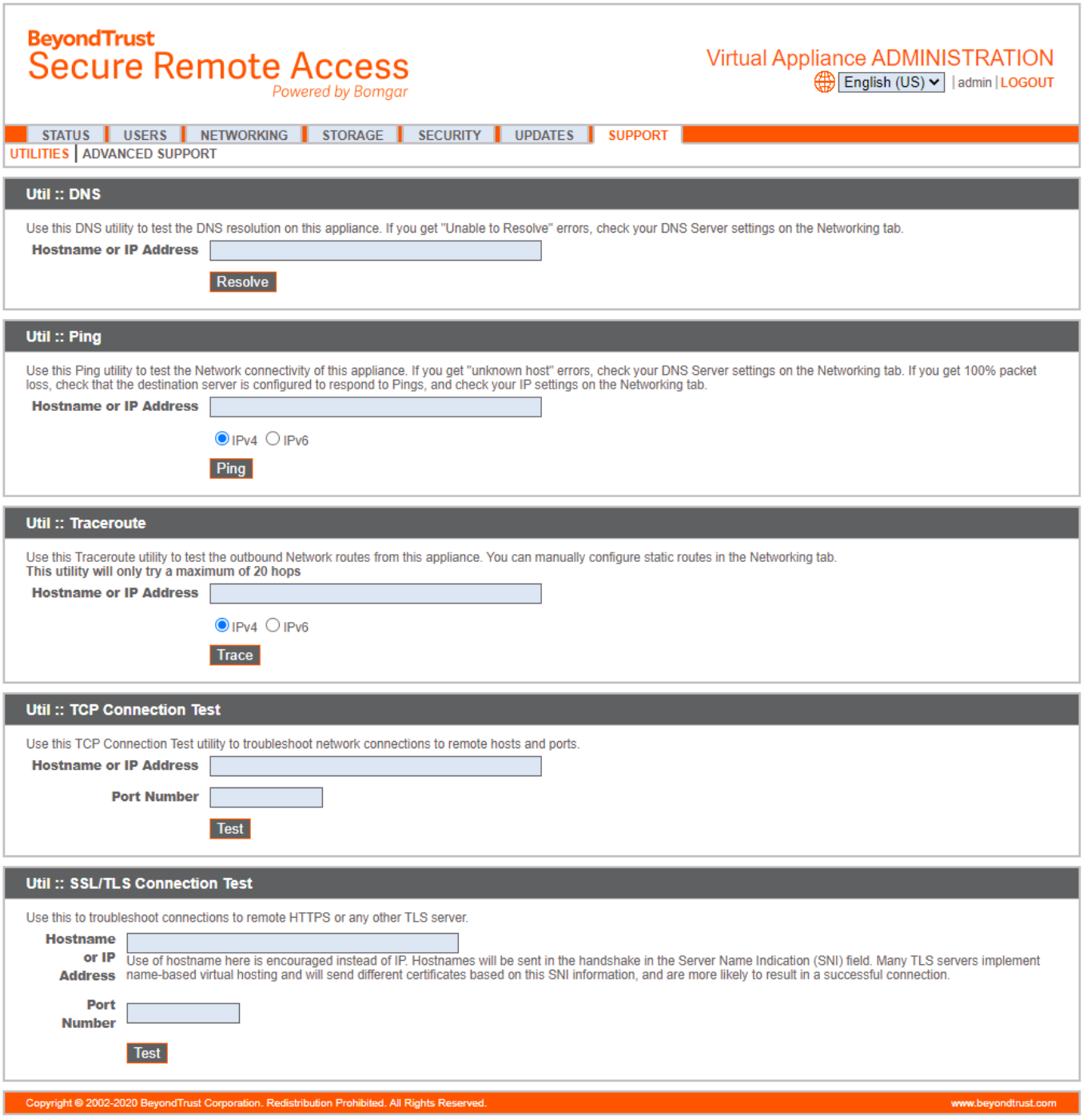
Om geïnstalleerde patches te bekijken, gaat u naar het tabblad **Updates** en selecteert u **Geïnstalleerde patches**. De tabel geeft alle geïnstalleerde firmwarepatches weer en wanneer deze zijn geïnstalleerd.



Ondersteuningshulpprogramma's: Netwerkproblemen opsporen

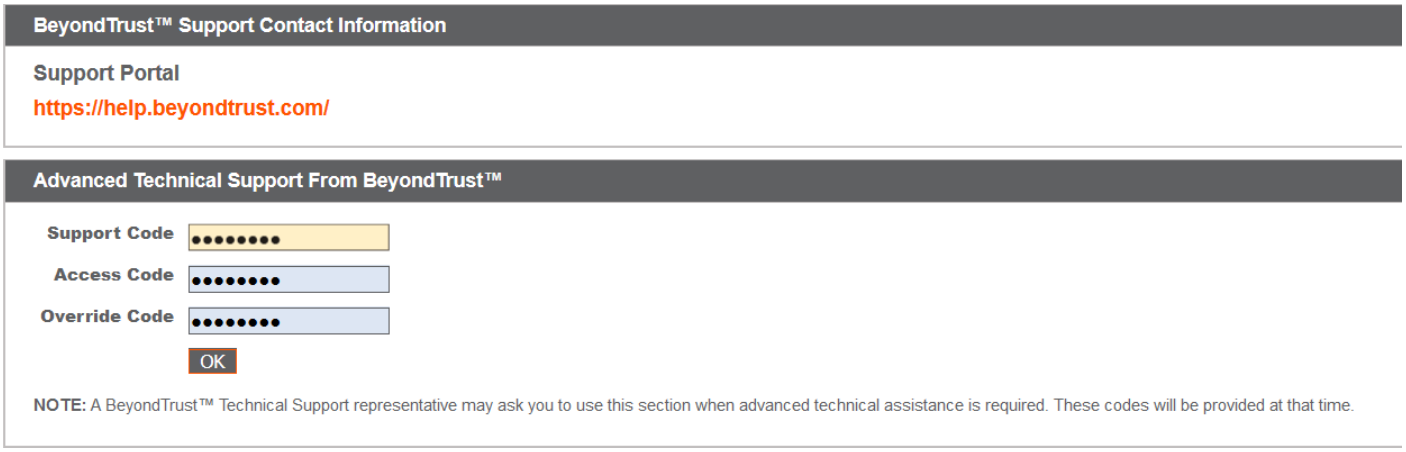
Het gedeelte **Hulpprogramma's** kan worden gebruikt om netwerkproblemen op te lossen. Als u geen verbinding kunt maken, kunt u met deze hulpprogramma's wellicht ontdekken wat de reden is:

- Test de **DNS**-naamomzetting van uw B Series Appliance door een hostnaam op te zoeken of door een omgekeerde zoekopdracht naar een IP-adres uit te voeren.
- **Ping** een hostnaam of IP-adres om de netwerkconnectiviteit van uw B Series Appliance te testen.
- Gebruik de **Traceroute** om het pad te zien waarop pakketten van het B Series Appliance naar een extern systeem reizen.
- Gebruik de **TCP-verbindingstest** om de verbinding van een specifieke poort op een doel-hostnaam of doel-IP-adres te controleren.
- Gebruik de **SSL/TLS-verbindingstest** om de connectiviteit met HTTPS of andere TLS externe servers te controleren.



Geavanceerde ondersteuning: Contact opnemen met BeyondTrust Technical Support

Het gedeelte **Uitgebreide ondersteuning** bevat contactinformatie voor uw BeyondTrust Technical Support-team en stelt u in staat om vanuit het apparaat een tunnel voor ondersteuning naar BeyondTrust Technical Support op te zetten om ingewikkelde problemen snel op te lossen.



Als het gedeelte **Er is een technische ondersteuningssessie met BeyondTrust Corporation actief** wordt weergegeven, heeft BeyondTrust Technical Support op dat moment een actieve sessie met uw B Series Appliance. De kolom **Duur** geeft aan hoelang de sessie van BeyondTrust Technical Support met uw B Series Appliance al duurt. Klik op **Beëindigen** om de sessie te stoppen. De tunnel tussen uw B Series Appliance en BeyondTrust Technical Support wordt dan gesloten.