



BeyondTrust

Bevoorrechte toegang op afstand 21.1 **Handleiding voor beheerders**

Inhoudsopgave

BeyondTrust Privileged Remote Access-beheerinterface	4
Log in bij de PRA-beheerinterface	5
Beheer van Privileged Remote Access: Status	6
Informatie: Informatie over BeyondTrust Privileged Remote Access-software weergeven	6
Gebruikers: Ingelogde gebruikers bekijken en berichten verzenden	8
Wat is er nieuw: Zie release-informatie van Privileged Remote Access-software	9
Mijn account: Wachtwoord en gebruikersnaam wijzigen, de Access Console en andere software downloaden	10
Configuratie	13
Opties: Verbindingsopties beheren, sessies opnemen, sessies versnellen	13
Teams: Gebruikers in teams groeperen	17
Aanpasbare velden: Aangepaste API-velden maken, bewerken en verwijderen	19
Jump	20
Jump-clients: Instellingen van Jump-clients voor toegang tot eindpunten beheren en installeren	20
Jumpgroepen: Configureer welke gebruikers toegang hebben tot welke Jumpitems	26
Jump-beleidslijnen: Roosters, kennisgevingen en toestemmingen voor Jumpitems instellen	28
Jumpitem-rollen: Machtigingen aanmaken voor Jumpitems	33
Jumpoint: Toegang zonder toezicht naar een netwerk instellen	36
Jumpitems: Bulkimport van snelkoppelingen naar Jumps en beheren van instellingen voor Jumpitems	39
Vault voor Privileged Remote Access	48
Accounts: Vault-accounts beheren	48
Accountgroepen: accountgroepen toevoegen en beheren	55
Eindpunten: Gedetecteerde systemen weergeven en beheren	58
Domeinen: Domeinen toevoegen en beheren	59
Detectie: Domeinen, accounts en eindpunten detecteren	60
Opties: Wachtwoordrotatie plannen	62
Toegangsconsole	63
Instellingen van toegangsconsole: Standaard instellingen van toegangsconsole beheren ...	63
Aangepaste koppelingen: URL-snelkoppelingen toevoegen aan de Access Console	67
Standaard scripts: Scripts aanmaken voor sessies met scherm delen of met opdrachtshell ..	68

Speciale acties: Aangepaste speciale acties aanmaken	70
Gebruikers en beveiliging	72
Gebruikers: Accountmachtigingen toevoegen voor een gebruiker of beheerder	72
Gebruikersaccounts om wachtwoorden opnieuw in te stellen: Gebruikers toestaan om wachtwoorden te beheren	83
Toegangsuitnodiging: Profielen aanmaken om externe gebruikers in sessies uit te nodigen	85
Beveiligingsproviders: Inloggen via LDAP, Active Directory, RADIUS en Kerberos activeren	86
Leveranciersgroepen	102
Sessiebeleidslijnen: Sessiemachtigingen en prompt-regels instellen	105
Groepsbeleidslijnen: Gebruikersmachtigingen op groepen gebruikers toepassen	111
Kerberos Keytab: De Kerberos Keytab beheren	123
Rapporten	124
Toegang: Rapport over sessie-activiteit	124
Vault: Rapport over Vault-account en gebruikersactiviteit	127
Leveranciers: Rapport over Leverancier-accounts en gebruikersactiviteit	128
Naleving: Gegevens uit Privileged Remote Access anonimiseren om aan compliance-normen te voldoen	129
Beheer	131
Software: Een back-up downloaden, software bijwerken	131
Beveiliging: Beveiligingsinstellingen beheren	133
Websiteconfiguratie: HTTP-poorten instellen, vereiste inlogovereenkomst inschakelen	138
E-mailconfiguratie: Software configureren om e-mails te verzenden	139
Uitgaande gebeurtenissen: Gebeurtenissen instellen om berichten uit te laten gaan	141
Cluster: Atlas-clustertechnologie configureren voor loadbalancing	144
Automatische omschakeling: Een back-up B Series Appliance instellen voor automatische omschakeling	147
API-configuratie: De XML API inschakelen en aangepaste velden configureren	150
Ondersteuning: Contact opnemen met BeyondTrust Technical Support	153
Poorten en firewalls	154
Vrijwaringen, beperkingen voor licenties en technische ondersteuning	155

BeyondTrust Privileged Remote Access-beheerinterface

In deze gids staat een gedetailleerd overzicht van **/login**. De gids is bedoeld om u te helpen BeyondTrust-gebruikers en uw BeyondTrust-software te beheren. Het BeyondTrust Appliance B Series dient als het centrale punt voor administratie en beheer van uw BeyondTrust-software en stelt u in staat om in te loggen van elke plaats met internettoegang om de access console te downloaden.

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](http://www.beyondtrust.com/docs/privileged-remote-access/getting-started/deployment/hardware/) op www.beyondtrust.com/docs/privileged-remote-access/getting-started/deployment/hardware/. 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 PRA-beheerinterface

Inloggen

Meld u aan bij de beheerinterface door naar de URL van uw B Series Appliance te gaan, gevolgd door **/login**. Beheerders kunnen met de gebruikersbeheer-interface gebruikersaccounts aanmaken en software-instellingen configureren.

Hoewel de URL van uw B Series Appliance elke geregistreerde DNS kan zijn, is dit hoogstwaarschijnlijk een subdomein van het primaire domein van uw bedrijf (bijv. [toegang.voorbeeld.nl/login](#)).

Standaard gebruikersnaam: **admin**

Standaard wachtwoord: **password**



Opmerking: Om beveiligingsredenen zijn de administratieve gebruikersnaam en het wachtwoord voor de /appliance-interface anders dan die gebruikt worden voor de /login-interface. Beide moeten afzonderlijk worden beheerd.

Als verificatie in twee stappen voor uw account is ingeschakeld, voert u de code van de verificatie-app in.



Opmerking: Gebruikers die al inlogcodes ontvingen, worden automatisch geüpgraded naar 2FA, hoewel ze e-mailcodes mogen blijven gebruiken tot ze hun app hebben geregistreerd. Op het moment dat ze 2FA gaan gebruiken, wordt de optie voor e-mailcodes permanent uitgeschakeld.



Raadpleeg [Inloggen bij de PRA-toegangsconsole](https://www.beyondtrust.com/docs/privileged-remote-access/getting-started/access-console/login-to-the-access-console.htm) op <https://www.beyondtrust.com/docs/privileged-remote-access/getting-started/access-console/login-to-the-access-console.htm> voor meer informatie.

Gebruik geïntegreerde browserverificatie

Als Kerberos juist is geconfigureerd voor eenmalige aanmelding, dan kunt u op de koppeling klikken om geïntegreerde browserverificatie te gebruiken zodat u direct in de web-interface kunt komen zonder uw inloggegevens in te moeten voeren.

Uw wachtwoord vergeten?

Als op de pagina **/login > Beheer > Beveiliging** wachtwoord resetten is ingeschakeld en de SMTP-server is ingesteld voor uw site, dan is deze koppeling zichtbaar. U kunt uw wachtwoord resetten door op de koppeling te klikken en uw e-mailadres in te voeren en te bevestigen. Klik vervolgens op **Verzenden**. Als meerdere gebruikers hetzelfde e-mailadres delen, moet u uw gebruikersnaam bevestigen. U ontvangt een e-mailbericht met een koppeling terug naar de inlogpagina. Op het inlogscherm wordt u gevraagd een nieuw wachtwoord in te voeren en te bevestigen. Vervolgens klikt u op **Wachtwoord veranderen**.

Inlogovereenkomst

Beheerders kunnen de toegang tot het inlogscherm beperken door een vereiste inlogovereenkomst in te schakelen die moet worden bevestigd voordat het inlogscherm wordt weergegeven. U kunt de inlogovereenkomst inschakelen en aanpassen op de pagina **/login > Beheer > Websiteconfiguratie**.

Beheer van Privileged Remote Access: Status

Informatie: Informatie over BeyondTrust Privileged Remote Access-software weergeven

 Status

Informatie

Sitestatus

De hoofdpagina van de /login-interface voor BeyondTrust Privileged Remote Access bevat een overzicht van de statistieken voor uw B Series Appliance. Als u contact met BeyondTrust Technical Support opneemt voor software-updates of voor het oplossen van problemen, kan u worden gevraagd per e-mail een schermopname van deze pagina te verzenden.

Privileged Remote Access-software opnieuw starten

U kunt de BeyondTrust-software op afstand opnieuw opstarten. Start uw software alleen opnieuw op als u daar opdracht toe krijgt van BeyondTrust Technical Support.

Tijdzone

Een beheerder kan uit een vervolgkeuzemenu de juiste tijdzone selecteren en daarmee de juiste datum en tijd van het B Series Appliance instellen voor de geselecteerde regio.

Rapport van licentiegebruik downloaden

Download een zip-bestand met gedetailleerde informatie (alleen in het Engels) over het gebruik van uw BeyondTrust-licentie. Dit bestand bevat een lijst met alle Jumpitems (exclusief de niet-geïnstalleerde Jump-clients), dagtellingen voor bewerkingen op Jumpitems en licentiegebruik en een samenvatting van de B Series Appliance en het eindpuntlicentiegebruik en het verloop ervan.

Clientsoftware

Dit is de hostnaam waarmee de BeyondTrust-clientsoftware verbinding maakt. 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 voorbereiden.

Verbonden clients

Bekijk het aantal en type BeyondTrust-softwareclients dat een verbinding met uw B Series Appliance heeft.



Ga voor meer informatie over de BeyondTrust Appliance B Series naar het [B Series Appliance-overzicht](https://www.beyondtrust.com/docs/privileged-remote-access/getting-started/deployment/index.htm) op <https://www.beyondtrust.com/docs/privileged-remote-access/getting-started/deployment/index.htm>.

ECM-clients

Bekijk het aantal BeyondTrustEndpoint Credential Managers (ECM) dat een verbinding met uw B Series Appliance-apparaat heeft. Bekijk ook informatie over de locatie en verbindingstijd voor elke ECM, alsmede de groep waartoe de ECM behoort.



Opmerking: Om optimale up-time te waarborgen, kunnen beheerders maximaal drie ECM's op verschillende Windows-systemen installeren om met dezelfde inloggegevensopslag te communiceren. Een lijst met de ECM's die met het apparaat verbonden zijn, is te vinden op **/login > Status > Informatie > ECM-clients**.



Opmerking: Als er meerdere ECM's in een configuratie met hoge beschikbaarheid zijn verbonden, stuurt het BeyondTrust Appliance B Series verzoeken naar de ECM in de ECM-groep die het langst met het apparaat is verbonden.



Zie voor meer informatie [Inloggen bij eindpunten met gebruik van inloggegevensinjectie](https://www.beyondtrust.com/docs/privileged-remote-access/getting-started/access-console/web-access/credential-injection.htm) op <https://www.beyondtrust.com/docs/privileged-remote-access/getting-started/access-console/web-access/credential-injection.htm>.

Gebruikers: Ingelogde gebruikers bekijken en berichten verzenden

 Status	Gebruikers
--	-------------------

Ingelogde gebruikers

Geef een lijst weer van gebruikers die bij de access console zijn ingelogd, inclusief het tijdstip van inloggen en of ze sessies uitvoeren.

Beëindigen

U kunt de verbinding van een gebruiker met de access console beëindigen.

Bericht naar gebruikers sturen

Verzend een bericht naar alle ingelogde gebruikers via een pop-upvenster in de access console.

Gebruikers Uitgebreide beschikbaarheid

Bekijk gebruikers waarvoor de uitgebreide beschikbaarheid-modus is ingeschakeld.

Uitschakelen

U kunt de uitgebreide beschikbaarheid van een gebruiker uitschakelen.

Wat is er nieuw: Zie release-informatie van Privileged Remote Access-software



Status

Wat is er nieuw

Wat is er nieuw

Neem eenvoudig de functies en mogelijkheden in BeyondTrust door die beschikbaar zijn in elke nieuwe release. Lees alles over hoe u de nieuwste functies kunt gebruiken om maximaal te profiteren van uw BeyondTrust-implementatie.

De eerste keer wanneer u zich na een upgrade van de BeyondTrust-software bij de beheerinterface aanmeldt, informeert de pagina **Wat is er nieuw** u over nieuwe functies die beschikbaar zijn op uw site. Alleen beheerders hebben toegang tot dit tabblad.

De informatie die op de pagina **Wat is er nieuw** wordt weergegeven, is ook beschikbaar voor gebruikers in de access console via het menu **Help > Over**.



Raadpleeg [BeyondTrust Privileged Remote Access-updatedocumentatie](https://www.beyondtrust.com/docs/privileged-remote-access/updates/index.htm) op <https://www.beyondtrust.com/docs/privileged-remote-access/updates/index.htm> voor meer informatie.

Mijn account: Wachtwoord en gebruikersnaam wijzigen, de Access Console en andere software downloaden



Mijn account

BeyondTrust Privileged Web-toegangconsole

Open de privileged web access console, een online access console. Open externe systemen vanuit uw browser zonder de volledige access console te hoeven downloaden en installeren.

BeyondTrust Access Console

Kies platform

Kies het besturingssysteem waarop u deze software wilt installeren. Deze vervolgkeuzelijst heeft als standaard het juiste installatieprogramma voor het gedetecteerde besturingssysteem.

i Zie voor meer informatie de [Privileged Web Access Console-gids](https://www.beyondtrust.com/docs/privileged-remote-access/getting-started/access-console/web-access/index.htm) op <https://www.beyondtrust.com/docs/privileged-remote-access/getting-started/access-console/web-access/index.htm>.

Download BeyondTrust Access Console

Download het installatieprogramma voor de BeyondTrust-access console.

Als een systeembeheerder het console-installatieprogramma op een groot aantal systemen moet implementeren, dan kan hij of zij het Microsoft installatieprogramma in combinatie met een willekeurig beheerdershulpmiddel gebruiken. Op de commandoregel moet u bij het samenstellen van de opdracht om de console met een MSI te installeren naar de map gaan waar de MSI was gedownload en de opdracht invoeren zoals die op de pagina **Mijn account** staat.

U kunt voor uw MSI-installatie optionele parameters meegeven.

- Met **INSTALLDIR=** kunt u elk geldig pad opgeven naar de map waar u de console wilt installeren.
- Voor **RUNATSTARTUP=** kunt u **0** (standaard) of **1** opgeven. Als u **1** invoert, dan wordt de console telkens opgestart als de computer opstart.
- **ALLUSERS=** accepteert **""** of **1** (standaard). Als u **1** invoert, dan wordt de console voor alle gebruikers van de computer geïnstalleerd, anders alleen voor de huidige gebruiker.
- **SHOULD AUTOUPDATE=1** Als u alleen voor de huidige gebruiker installeert, dan kunt u kiezen of de console automatisch moet worden bijgewerkt telkens wanneer de site wordt bijgewerkt door de waarde **1** in te voeren. Bij **0** (standaard) wordt niet automatisch bijgewerkt maar moet de console handmatig opnieuw worden geïnstalleerd als de site wordt bijgewerkt. Als u de console voor alle gebruikers installeert, dan wordt deze niet automatisch bijgewerkt.

Uw wachtwoord veranderen

BeyondTrust adviseert u om uw wachtwoord regelmatig te wijzigen.

Gebruikersnaam, huidig wachtwoord, nieuw wachtwoord

Controleer of u bent ingelogd op de account waarvoor u het wachtwoord wilt wijzigen en voer vervolgens uw huidige wachtwoord in. Maak een nieuw wachtwoord voor uw account en bevestig dit. U kunt het wachtwoord net zo instellen als u wilt, als de tekenreeks maar voldoet aan het beleid zoals het gedefinieerd is op de pagina **/login > Beheer > Beveiliging**.

Verander uw e-mailinstellingen

E-mailadres

Stel het e-mailadres in waarnaar e-mailkennisgevingen moeten worden verzonden, zoals het opnieuw instellen van het wachtwoord of waarschuwingen over uitgebreide beschikbaarheid-modus.

Wachtwoord

Voer het wachtwoord voor uw /login-account in, niet het wachtwoord voor uw e-mailaccount.

Verificatie in twee stappen

Verificatie in twee stappen activeren

Activeer verificatie in twee stappen (2FA) om het beveiligingsniveau te verhogen voor gebruikers die toegang hebben tot /login en de BeyondTrust-access console. Klik op **Verificatie in twee stappen activeren** en gebruik vervolgens een verificator-app naar keuze, zoals Google Authenticator, om de QR-code die op de pagina wordt weergegeven te scannen. U kunt ook de alfanumerieke code onder de QR-code handmatig in uw verificator-app invoeren.

De app registreert automatisch het account en voorziet u van codes. Voer uw wachtwoord in en de code die de door u geselecteerde app heeft gegenereerd en klik vervolgens op **Activeren**. Let wel dat de code 60 seconden geldig is. Hierna wordt een nieuwe code gegenereerd. Nadat u hebt ingelogd, hebt u de keuze om naar een andere verificator-app over te schakelen of om 2FA uit te schakelen.



Opmerking: Als uw beheerder u dwingt 2FA te gebruiken, kunt u de functie niet uitschakelen.

Uitgebreide beschikbaarheid-modus

Activeren of uitschakelen

Activeer de modus uitgebreide beschikbaarheid of schakel deze uit door op de knop **Activeren of uitschakelen** te klikken. In de modus uitgebreide beschikbaarheid kunt u, als u niet op de console bent ingelogd, e-mailuitnodigingen van andere gebruikers ontvangen met het verzoek een sessie te delen.

Agent voor Bureaublad op afstand

Installatieprogramma voor agent voor extern bureaublad downloaden

De agent voor extern bureaublad moet worden geïnstalleerd op 64-bits Windows-servers waarop Extern bureaublad-services zijn ingeschakeld en waarop door beheerders gedefinieerde toepassingen moeten worden gestart en van inloggegevens moeten worden voorzien

Virtuele smartcard

De BeyondTrust-gebruiker moet een stuurprogramma voor de virtuele smartcard van BeyondTrust hebben geïnstalleerd om verificatie via virtuele smartcard te kunnen uitvoeren. De computer waar toegang toe wordt verkregen, moet actief zijn in opgewaardeerde modus. Ook moet er ofwel het stuurprogramma voor de virtuele smartcard van BeyondTrust voor een eindpunt zijn geïnstalleerd of er moet toegang mogelijk zijn via de functie 'Jump naar' van de access console.



Raadpleeg [Smartcards voor verificatie op afstand](https://www.beyondtrust.com/docs/privileged-remote-access/how-to/smart-card/index.htm) op <https://www.beyondtrust.com/docs/privileged-remote-access/how-to/smart-card/index.htm> voor meer informatie en vereisten.

Windows architectuur selecteren

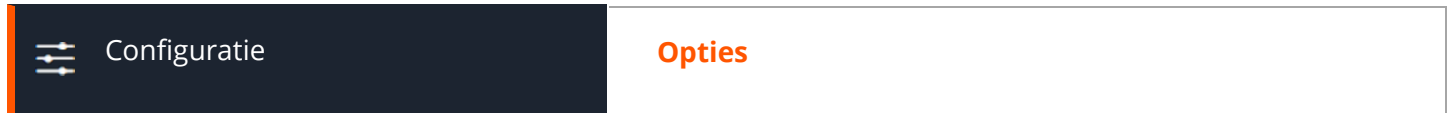
Kies of u het installatieprogramma voor de virtuele smartcard wilt downloaden voor het systeem van de BeyondTrust-gebruiker of voor het eindpuntsysteem.

Installatieprogramma voor Virtuele Smartcard downloaden

Download het hierboven geselecteerde installatieprogramma voor de virtuele smartcard. Met een virtuele smartcard kunt u op een extern systeem worden geverifieerd via een smartcard op uw lokale systeem.

Configuratie

Opties: Verbindingsopties beheren, sessies opnemen, sessies versnellen



Sessieopties

Afgesloten sessies bij Uitloggen of Afsluiten vereisen

Als u **Afgesloten sessies bij Uitloggen of Afsluiten vereisen** aanvinkt, kunnen gebruikers van de console niet uitloggen als ze op dat moment nog sessietabbladen open hebben staan.

Verbindingsopties

Time-out voor nieuwe verbinding

Bepaal hoe lang een endpoint client waarvan de verbinding is verbroken, moet proberen opnieuw verbinding te krijgen.

Beperk de fysieke toegang tot het eindpunt als de verbinding met het eindpunt wordt verbroken of als de verbinding met alle gebruikers die bij de sessie aanwezig zijn verbroken is

Als de verbinding met de sessie verloren is gegaan, dan kan de invoer van de muis en het toetsenbord op het externe systeem tijdelijk uitgeschakeld zijn. Beide komen weer beschikbaar als de verbinding is hersteld of als de sessie wordt beëindigd.

Gedrag voor beëindigen van sessie

U kunt kiezen wat er moet worden gedaan als u binnen de in **Time-out voor nieuwe verbinding** ingestelde periode niet opnieuw verbinding kunt krijgen. Om ervoor te zorgen dat de eindgebruiker niet-geautoriseerde rechten krijgt na een opgewaardeerde sessie, moet u de client zo instellen dat bij het beëindigen van een sessie met een externe Windows computer de eindgebruiker automatisch wordt uitgelogd, de externe computer op slot gaat of dat er niets gebeurt. Deze regels gelden niet voor sessies waarin de browser wordt gedeeld.

Hiermee kunnen gebruikers deze instelling per sessie overschrijven

U kunt tijdens een sessie vanaf het tabblad **Samenvatting** in de console een gebruiker toestaan de instelling voor het afsluiten van de sessie te overschrijven.

Inlogopties voor toegangssessies

Opnemen van Scherm delen inschakelen

Kies of sessies met scherm delen automatisch als video's moeten worden opgenomen.

Resolutie van de 'Scherm delen'-opname

Stel de resolutie in waarmee u het terugspelen van de sessie wilt bekijken.



Opmerking: Alle opnames worden in ruwe opmaak opgeslagen, de resolutie heeft alleen gevolgen voor het afspelen.

Gebruikersopname voor Jump via tunnelprotocol inschakelen

Kies of sessies met Jump via tunnelprotocol automatisch als video's moeten worden opgenomen. Omdat voor Jumps via tunnelprotocol een toepassing naar keuze van derden vereist is, wordt de volledige desktop van de gebruiker vastgelegd, inclusief alle beeldschermen.

Resolutie van opname van de gebruiker

Stel de resolutie in waarmee u het terugspelen van de sessie wilt bekijken.



Opmerking: Alle opnames worden in ruwe opmaak opgeslagen, de resolutie heeft alleen gevolgen voor het afspelen.

Toestemming van de gebruiker vragen voordat de opname start

Kies of gebruikers een prompt moeten krijgen die hen informeert dat de desktop wordt opgenomen bij het starten van een Jump via tunnelprotocol. Let wel dat als de gebruiker geen toestemming geeft, de Jump via tunnelprotocol niet doorgaat.

Opnemen van Oprachtshells inschakelen

Kies of sessies met opdrachtshell automatisch als video's moeten worden opgenomen. Als u opnames van sessies met opdrachtshell inschakelt, komen ook sessies met opdrachtshell als tekst beschikbaar.

Resolutie van de Oprachtshellopname

Stel de resolutie in waarmee u het terugspelen van de sessie wilt bekijken.



Opmerking: Alle opnames worden in ruwe opmaak opgeslagen, de resolutie heeft alleen gevolgen voor het afspelen.



BELANGRIJK!

De opname-instellingen op deze pagina kunnen worden overschreven door een Jumpbeleid met **Sessieopnames uitschakelen** ingesteld. Dit is van toepassing op scherm delen, opnames voor Jump via tunnelprotocol en opdrachtshellopnames.

Automatische registratie van systeeminformatie activeren

Kies of systeeminformatie automatisch aan het begin van de sessie van het externe systeem moet worden opgehaald zodat deze informatie later in de rapporten over de sessie beschikbaar is.

Forensische gegevens van sessies inschakelen

Kies of u de extra mogelijkheid wilt om over alle sessies heen te zoeken op basis van sessie-gebeurtenissen. Dit omvat chatberichten, bestandsoverdracht, gebeurtenissen in de register-editor en gebeurtenissen waardoor het voorgrond-venster van de sessie wijzigt. Deze functie is standaard ingeschakeld.



Opmerking: Als opdrachtshell is ingeschakeld, dan kunt u met Forensische gegevens van sessies uitgebreid in shell-opnames zoeken. Als u op een zoekterm zoekt en deze wordt gevonden in een opgeslagen shell-opname, dan wordt de video automatisch op dat tijdstip in de opname gepositioneerd. Er worden geen uitvoer van opdrachten en geen wachtwoorden opgenomen.

Peer-to-peer opties

Uitgeschakeld

Dit is de standaard instelling. Hiermee worden peer-to-peer-verbindingen uitgeschakeld. Om deze functie in te schakelen, moet u een server kiezen om de sessie te onderhandelen. Als scherm delen, bestand overdragen of opdrachtshell wordt gedetecteerd, wordt een peer-to-peer-verbinding geprobeerd. Als dit lukt, wordt een directe verbinding tussen de gebruiker en de clientsystemen aangemaakt, terwijl nog steeds een tweede datastream naar het B Series Appliance wordt verzonden voor controledoeleinden. Als om welke reden dan ook een peer-to-peer-verbinding niet kan worden ingesteld, wordt het sessieverkeer naar de standaard door het B Series Appliance bemiddelde verbinding geleid.

Gebruik BeyondTrust gehoste peer-to-peer-server

BeyondTrust-clients proberen om een peer-to-peer-verbinding te bereiken via de server die door BeyondTrust gehost wordt. Hiervoor is vereist dat uw BeyondTrust-clients uitgaande UDP 3478-verbindingsverzoeken kunnen maken naar stun.bomgar.com. Deze instelling zou in de meeste gevallen moeten werken.

B Series Appliance gebruiken als peer-to-peer-server

Als uw organisatie specifieke beveiligingsinstellingen vereist voor verkeer, kunt u het B Series Appliance gebruiken als een peer-to-peer-server. Hiervoor is vereist dat uw B Series Appliance inkomende UDP 3478-verbindingsverzoeken kan ontvangen van uw BeyondTrust-clients. Er moeten aanvullende instellingen op de firewall worden geconfigureerd.



Ga voor meer informatie naar [BeyondTrust Appliance B Series Beheer: Accounts, netwerken en poorten beperken, een STUN-server inschakelen, syslog instellen, inlogovereenkomst inschakelen, beheerdersaccount resetten](https://www.beyondtrust.com/docs/privileged-remote-access/getting-started/deployment/web/security-appliance-administration.htm) op <https://www.beyondtrust.com/docs/privileged-remote-access/getting-started/deployment/web/security-appliance-administration.htm>.

Logo van toegangsportaal

Beheerders kunnen een eigen logo uploaden dat wordt weergegeven op voor publiek toegankelijke webpagina's. Hieraan kunnen externe gebruikers zien dat ze op de website van uw organisatie zijn. Bovendien wordt het toegangsportaal verfraaid met de naam van uw organisatie.

Uw logoafbeelding wordt op de volgende voor publiek toegankelijke webpagina's weergegeven:

- Downloadpagina voor toegangsuitnodiging (de pagina die wordt weergegeven nadat op een koppeling in een uitnodigingse-mail voor toegang wordt geklikt)
- URL's met publieke opnames (bekijken en downloaden)
- Reacties op uitgebreide beschikbaarheid (de pagina die wordt weergegeven nadat op een koppeling in een uitnodigingse-mail voor uitgebreide beschikbaarheid wordt geklikt)
- Authorisatie voor Jump-goedkeuring (de pagina die wordt weergegeven nadat op een koppeling in een Jump-goedkeuringse-mail wordt geklikt)



Opmerking: Logoafbeeldingen kunnen in alle standaard afbeeldingsindelingen worden geüpload. De logische afbeeldingsgrootte is maximaal 250 pixels breed en 64 pixels hoog. Maar BeyondTrust ondersteunt ook hogere resoluties met een fysieke afmeting van maximaal 500 pixels breed en 128 pixels hoog.

Teams: Gebruikers in teams groeperen

 Configuratie

Teams

Teams beheren

Gebruikers in teams groeperen draagt bij aan de efficiëntie door het toewijzen van leiderschap binnen groepen gebruikers. In de access console wordt elk team weergegeven als een aparte wachtrij voor sessies.

Nieuw team toevoegen, bewerken, verwijderen

Maak een nieuw team aan, wijzig een bestaand team of verwijder een bestaand team. Als een team wordt verwijderd, worden de bijbehorende gebruikersaccounts niet verwijderd, alleen het team waartoe ze behoren wordt verwijderd.

Team toevoegen of bewerken

Teamnaam

Maak een unieke naam aan om dit team te identificeren.

Codenaam

Stel een codenaam in voor integratiedoeleinden. Als u geen codenaam instelt, maakt PRA er automatisch een aan.

Opmerkingen

Voeg commentaar toe om aan te geven wat het doel is van dit object.

Groepsbeleidslijnen

Let op eventuele groepsbeleidslijnen waardoor leden aan dit team worden toegewezen. Klik op de koppeling om naar de pagina **Groepsbeleidslijnen** te gaan om beleidsleden te verifiëren of toe te wijzen.

Teamleden

Zoek naar gebruikers om aan dit team toe te voegen. U kunt de rol van elk lid instellen op **Teamlid**, **Teamleider** of **Teammanager**. Deze rollen spelen een belangrijke rol in de **Dashboard**-functie van de access console.

Geef de bestaande teamleden in de onderstaande tabel weer. U kunt de weergave filteren door een gebruikersnaam in het filtervak in te voeren. Ook kunt u de rol van een lid bewerken of een lid uit het team verwijderen.

Ga naar **Gebruikers en beveiliging > Groepsbeleidslijnen** om een groep gebruikers aan een team toe te voegen en die groep een of meer teams toe te wijzen in een bepaalde rol.



Opmerking: U kunt sommige teamleden mogelijk niet bewerken of verwijderen. Dit gebeurt wanneer een gebruiker via een groepsbeleid wordt toegevoegd.

Klik op de koppeling voor het groepsbeleid om het beleid als geheel te wijzigen. Alle wijzigingen aan het groepsbeleid gelden voor alle leden van dat groepsbeleid.

U kunt ook individuen aan een team toevoegen en hun instellingen die ergens anders zijn gedefinieerd, overschrijven.

Dashboard-instellingen

Een gebruiker kan binnen een team alleen andere gebruikers beheren die een lagere rol hebben dan hij of zij zelf heeft. Let er echter op dat rollen strikt binnen een bepaald team gelden, zodat een gebruiker in het ene team een andere gebruiker kan beheren, maar diezelfde gebruiker in een ander team niet kan beheren.

Meekijken met teamleden vanaf het Dashboard

Als dit is ingeschakeld, dan kan een teamleider vanaf het dashboard met teamleden meekijken. Kies voor het **Uitschakelen** van de mogelijkheid om mee te kijken of kies **Alleen Access Console** om een teamleider of beheerder toe te staan om de access console van een teamlid te controleren. Meekijken is van toepassing op alle teamleiders en beheerders voor alle teams op de site.

Deelname aan een sessie en overname ervan via het dashboard inschakelen

Als deze optie is aangevinkt, kan een teamleider sessies van een teamlid bijwonen of overnemen. Ook kan een teammanager zowel teamleden als teamleiders beheren. De teamleider moet startsessie-toegang hebben tot het Jumpitem dat gebruikt is om de sessie aan te maken, tenzij de onderstaande optie eveneens is aangevinkt.

Teammanagers/-leiders toestaan om 'Overdracht', 'Overnemen' en 'Deelnemen aan sessie' te gebruiken voor sessies die gestart zijn vanuit Jumpitems waarvoor ze geen toegang hebben tot 'Sessie starten'.

Als deze optie is aangevinkt, kan een teamleider sessies van een teamlid bijwonen of overnemen, zelfs als de teamleider geen startsessie-toegang heeft tot het Jumpitem dat gebruikt is om de sessie aan te maken.

Aanpasbare velden: Aangepaste API-velden maken, bewerken en verwijderen



Configuratie

Aanpasbare velden

Maak aangepaste API-velden om informatie over uw klant te verzamelen, waardoor u BeyondTrust nog dieper kunt integreren in uw bestaande programma's. Aangepaste velden moeten worden gebruikt in combinatie met de BeyondTrust-API. Maak een nieuw veld aan, wijzig een bestaand veld of verwijder een bestaand veld.

Aangepast API-veld toevoegen of bewerken

Scherмнаam

Maak een unieke naam aan om dit aangepaste veld te identificeren. De naam wordt in de access console weergegeven als onderdeel van de sessiegegevens.

Codenaam

Stel een codenaam in voor integratiedoeleinden. Als u geen codenaam instelt, maakt PRA er automatisch een aan.

Weergeven in Access Console

Als u **Weergeven in Access Console** inschakelt, zullen dit veld en de waarden ervan zichtbaar zijn als de gegevens van de aangepaste sessie in de access console worden weergegeven.

Jump

Jump-clients: Instellingen van Jump-clients voor toegang tot eindpunten beheren en installeren

 Jump

Jump-clients

Wizard voor massa-implementatie van Jump-clients

Beheerders en bevoorrechte gebruikers kunnen de wizard voor massa-implementatie gebruiken om Jump-clients op een of meer externe computers te installeren om later toegang zonder toezicht tot deze computers te krijgen.

i Meer informatie is te vinden in [Privileged Remote Access Handleiding voor Jump-client: Onbewaakte toegang tot systemen in elk netwerk](https://www.beyondtrust.com/docs/privileged-remote-access/how-to/jump-clients/index.htm) op <https://www.beyondtrust.com/docs/privileged-remote-access/how-to/jump-clients/index.htm>.

Jumpgroep

Selecteer uit het vervolgkeuzemenu **Jumpgroep** of de Jump-client moet worden vastgespeld aan uw persoonlijke lijst met Jumpitems of aan een Jumpgroep die door anderen wordt gedeeld. Als de Jump-client is vastgespeld aan uw persoonlijke met Jumpitems, dan bent u de enige die via deze Jump-client toegang tot deze externe computer kan krijgen. Door hem vast te spelden aan een Jumpgroep is deze Jump-client beschikbaar voor alle leden van die Jumpgroep.

Naam

Voer een naam in voor de Jump-client.

Bepaalde instellingen voor de wizard voor massa-implementatie kunnen worden overschreven, zodat u de opdrachtregel kunt gebruiken om vóór de installatie parameters in te stellen die specifiek zijn voor uw implementatie.

Jump-beleid

U kunt op deze Jump-client een Jump-beleid toepassen. Jump-beleidslijnen worden op de pagina **Jump > Jump-beleidslijnen** geconfigureerd en bepalen gedurende welke periodes een gebruiker toegang tot deze Jump-client kan krijgen. Er kan ook een kennisgeving worden verzonden als het Jumpbeleid wordt benaderd of er kan toestemming moeten worden gevraagd om het te benaderen. Als er geen Jumpbeleid is toegepast, dan kan zonder beperking toegang tot deze Jump-client worden verkregen.

Verbindingstype

Stel het **Type verbinding** in op **Actief** of **Passief** voor de Jump-clients die worden geïmplementeerd. Een actieve Jump-client behoudt een voortdurende verbinding met het B Series Appliance, terwijl een passieve Jump-client op connectieverzoeken wacht.

Probeer een opgevaardeerde installatie als de client dit ondersteunt

Als **Probeer een opgevaardeerde installatie als de client dit ondersteunt** is geselecteerd, dan probeert het installatieprogramma met beheerdersrechten te starten om de Jump-client als een systeemservice te installeren. Als de poging tot een opgevaardeerde

installatie niet slaagt of als deze optie niet is geselecteerd, dan start het installatieprogramma met gebruikersrechten en wordt de Jump-client als een toepassing geïnstalleerd. Deze opties is alleen van toepassing op Windows- en Mac-besturingssystemen.



Opmerking: Een Jump-client die in gebruikersmodus is vastgespeld is alleen beschikbaar als die gebruiker ingelogd is. Daar staat tegenover dat een Jump-client die in servicemodus is vastgespeld, met opgewaardeerde rechten, toestaat dat het systeem altijd beschikbaar is, ongeacht of de gebruiker ingelogd is of niet.

Dit installeerprogramma is geldig gedurende

Het installatieprogramma blijft te gebruiken gedurende de periode die gespecificeerd is in de vervolgkeuzelijst **Dit installatieprogramma is geldig gedurende**. Zorg dat u voldoende tijd reserveert voor het installeren. Mocht iemand proberen na deze periode het installatieprogramma voor de Jump-client uit te voeren, dan mislukt de installatie en moet een nieuw installatieprogramma voor de Jump-client worden aangemaakt. Ook als het installatieprogramma wordt uitgevoerd binnen de toegewezen periode, maar de Jump-client binnen die tijd geen verbinding kan maken met het B Series Appliance, wordt de Jump-client verwijderd en moet een nieuw installatieprogramma worden geïmplementeerd. De geldigheidsperiode kan op een willekeurige waarde van 10 minuten tot 1 jaar worden ingesteld. Deze periode heeft GEEN invloed op hoe lang de Jump-client actief blijft.

Naast het verlopen na de periode die door de optie **Dit installatieprogramma is geldig gedurende** is ingesteld, worden Jump-client massa-implementatiepakketten ongeldig als het B Series Appliance waarop ze waren aangemaakt wordt bijgewerkt. De enige uitzondering op deze regel zijn live updates die het licentienummer of de licentieverloopdatum wijzigen. Eventuele overige updates, zelfs als deze het versienummer van het B Series Appliance niet wijzigen, maken Jump-client installatieprogramma's van voor de upgrade ongeldig. Als deze installatieprogramma's MSI-pakketten zijn, kunnen ze nog steeds worden gebruikt om Jump-clients te deïnstalleren indien nodig.

Nadat een Jump-client is geïnstalleerd, blijft deze online en actief totdat de installatie wordt verwijderd van het lokale systeem, ofwel door een ingelogde gebruiker, een BeyondTrust-gebruiker vanaf de Jump-interface van de access console of door een script voor verwijderen van de installatie. Een BeyondTrust-gebruiker kan geen Jump-client verwijderen tenzij de gebruiker daartoe machtigingen heeft gekregen van diens beheerder in de /login-interface.

Opmerkingen

Voeg **Opmerkingen** toe die handig kunnen zijn bij het zoeken naar en identificeren van externe computers. Bedenk dat alle Jump-clients die via dit installatieprogramma zijn geïmplementeerd in eerste instantie dezelfde opmerkingen hebben, tenzij u **Overschrijven toestaan tijdens installatie** aanvinkt en de individuele parameters gebruikt om het installatieprogramma voor individuele programma's aan te passen.

Sessiebeleid

U kunt een **Sessiebeleid** kiezen om aan deze Jump-client toe te kennen. Sessiebeleidlijnen worden geconfigureerd op de pagina **Gebruikers en beveiliging > Sessiebeleidlijnen**. Het aan deze Jump-client toegekende sessiebeleid heeft de hoogste prioriteit bij het instellen van sessiemachtigingen.

Proxy voor Jumpoint

Als u een of meer Jumpoints als proxy hebt ingesteld, dan kunt u een Jumpoint selecteren om als proxy op te treden voor verbindingen naar deze Jump-clients. Op die manier kunnen deze Jump-clients, als deze op computers zonder eigen internetverbinding zijn geïnstalleerd, het Jumpoint gebruiken om een verbinding terug naar uw B Series Appliance te maken. De Jump-clients moeten op hetzelfde netwerk zijn geïnstalleerd als het Jumpoint dat geselecteerd is om voor de verbindingen als proxy op te treden.

Prompt voor inloggegevens voor opwaardering indien nodig

Als **Prompt voor inloggegevens voor opwaardering, indien nodig** is geselecteerd, dan vraagt het installatieprogramma de gebruiker om beheerders-inloggegevens in te voeren als het systeem vereist dat deze inloggegevens onafhankelijk worden ingevoerd, anders wordt de Jump-client met gebruikersrechten geïnstalleerd. Dit is alleen van toepassing als de gebruiker een opgewaardeerde installatie probeert uit te voeren.

Tag

Door een **Label** toe te voegen, kunt u uw Jump-clients in de access console ordenen in categorieën.

Overschrijven tijdens installatie toestaan

Bepaalde instellingen voor de wizard voor massa-implementatie kunnen worden overschreven, zodat u de opdrachtregel kunt gebruiken om vóór de installatie parameters in te stellen die specifiek zijn voor uw implementatie.

Hulp bij massa-implementatie

Systeembeheerders die het installatieprogramma voor de Jump-client op een groot aantal systeem moeten implementeren kunnen het uitvoerbare Windows MSI installatieprogramma voor Windows, Mac of Linux gebruiken samen met een willekeurig beheerderhulpmiddel. U kunt een geldig pad opgeven naar de map waar u de Jump-client wilt installeren.



Opmerking: Het kan voorkomen dat u tijdens het installeren een foutbericht krijgt over een probleem met de lay-out of vormgeving. Dergelijke berichten kunt u negeren.

U kunt, al naar gelang uw wensen, bepaalde installatieparameters ook overschrijven. Als u bepaalde installatie-opties markeert om tijdens installatie te worden overschreven, dan kunt u de volgende parameters gebruiken om het installatieprogramma voor de Jump-client voor individuele installaties aan te passen. Denk eraan dat als u een parameter op de opdrachtregel ingeeft, maar deze in de /login-beheerinterface niet is gemarkeerd voor overschrijven, dat de installatie dan mislukt. Als de installatie mislukt, kunt u in het gebeurtenislogboek van het besturingssysteem de installatiefouten bekijken.

Opdrachtregel-parameter	Waarde	Beschrijving
--install-dir	<directory_path>	Hier specificeert u een nieuwe schrijfbaar map waaronder u de Jump-client wilt installeren. Dit wordt alleen op Windows en Linux ondersteund. Als u een aangepaste map voor installatie wilt definiëren, dan moet u controleren of de map die u wilt aanmaken niet al bestaat en op een locatie is waar u mag schrijven.
--jc-name	<name...>	Als overschrijven is toegestaan, dan zal deze opdrachtregel-parameter de naam van de Jump-client instellen.
--jc-jump-group	user:<username>jumpgroep:<jumpgroup-code-name>	Als overschrijven is toegestaan, dan wordt met deze opdrachtregel-parameter de in de Wizard voor massa-implementatie gespecificeerde Jumpgroep overschreven.

<code>--jc-session-policy</code>	<code><session-policy-code-name></code>	Als overschrijven is toegestaan, dan wordt met deze opdrachtregel-parameter het sessiebeleid van de Jump-client ingesteld waarmee het machtigingsbeleid tijdens een access session wordt bepaald.
<code>--jc-jump-policy</code>	<code><jump-policy-code-name></code>	Als overschrijven is toegestaan, dan wordt met deze opdrachtregel-parameter het Jumpbeleid ingesteld dat regelt hoe gebruikers een Jump naar de Jump-client kunnen uitvoeren.
<code>--jc-tag</code>	<code><tag-name></code>	Als overschrijven is toegestaan, dan wordt met deze opdrachtregel-parameter de tag van de Jump-client ingesteld.
<code>--jc-comments</code>	<code><comments ... ></code>	Als overschrijven is toegestaan, dan worden met deze opdrachtregel-parameter de opmerkingen van de Jump-client ingesteld.
<code>--silent</code>		Als dit wordt gebruikt, vertoont het installatieprogramma geen vensters, spinners, fouten of andere zichtbare waarschuwingen.



Opmerking: Als een MSI-installatieprogramma geïmplementeerd wordt in Windows met gebruik van de `msiexec`-opdracht, dan kunnen de bovenstaande parameters worden gespecificeerd door:

1. Voorafgaande streepjes (`--`) te verwijderen
2. Overgebleven streepjes naar onderstrepingstekens (`_`) te converteren
3. Met een gelijkteken (`=`) een waarde toe te kennen

MSI-voorbeeld:

```
msiexec /i bomgar-scc-win32.msi KEY_INFO=w0dc3056g7ff8d1j68ee6wi6dhwzfefgggyezh7c40jc90
jc_jump_group=jumpgroup:server_support jc_tag=servers
```

Tijdens de implementatie van een `.EXE`-installatieprogramma kunnen de bovenstaande parameters worden gespecificeerd door:

- koppeltekens toe te voegen
- een spatie tussen de parameter en de waarde toe te voegen

EXE-voorbeeld:

```
bomgar-scc-[unique id].exe --jc-jump-group jumpgroup:servers --jc-tag servers
```

Andere regels waarmee rekening moet worden gehouden:

- `installdir` bevat een streepje in de EXE-versie, maar niet in de MSI-versie.
- `/quiet` wordt gebruikt voor de MSI-versie in plaats van `--silent` in de EXE-versie.

Statistieken voor Jump-Clients

Een beheerder kan kiezen welke statistieken voor alle Jump-clients hij of zij bekijkt voor een gehele site. Deze statistieken worden in de access console weergegeven en bevatten informatie over statistieken, de consolegebruiker, het schijfgebruik, een miniatuurweergave van het externe scherm en de bedrijfstijd.

Upgraden

Maximale bandbreedte voor gelijktijdige upgrades van Jump-clients

U kunt de tijdens het bijwerken gebruikte bandbreedte verder regelen met de instelling **Maximale bandbreedte voor gelijktijdige upgrades van Jump-clients**.

Maximaal aantal gelijktijdige upgrades van Jump-clients

Stel ook het maximale aantal Jump-clients in dat tegelijkertijd mag worden bijgewerkt. Bedenk dat als u een groot aantal Jump-clients geïmplementeerd hebt, u dit aantal mogelijk moet beperken om de hoeveelheid gebruikte bandbreedte te regelen.



Opmerking: Deze instelling heeft geen invloed op upgrades van de access console.

Algemene verbindingssnelheid voor Jump-clients

De instelling van de globale verbindingssnelheid wordt door ontkoppelde Jump-clients gebruikt als aanwijzing hoe sterk ze moeten proberen opnieuw te verbinden.

Onderhoud

Aantal dagen voordat Jump-clients die geen verbinding hebben gemaakt automatisch worden verwijderd

Als een Jump-client offline gaat en geen verbinding met het B Series Appliance maakt gedurende het aantal dagen dat in de instelling **Aantal dagen voordat Jump-clients die geen verbinding hebben gemaakt automatisch worden verwijderd** is opgegeven, wordt deze automatisch verwijderd op de doelcomputer en in de Jump-interface van de access console.



Opmerking: Deze instelling wordt gedeeld met de Jump-client tijdens normale activiteiten, zodat deze zichzelf zelfs op de geconfigureerde tijd kan verwijderen als er geen communicatie met de site mogelijk is. Als deze instelling wordt gewijzigd nadat de verbinding tussen de Jump-client en het B Series Appliance wordt verbroken, zal deze zichzelf op het eerder geconfigureerde tijdstip deïnstalleren.

Aantal dagen voordat Jump-clients die geen verbinding hebben gemaakt als 'verloren' worden beschouwd

Als een Jump-client offline gaat en geen verbinding met de B Series Appliance maakt tijdens het aantal dagen dat in de instelling **Aantal dagen voordat Jump-clients die geen verbinding hebben gemaakt automatisch worden verwijderd** is opgegeven, wordt deze in de access console aangemerkt als verloren. Er wordt op dit moment geen specifieke actie voor de Jump-client uitgevoerd. Deze wordt alleen als 'Verloren' aangemerkt ter identificatie, zodat een beheerder de reden voor de verbroken verbinding kan diagnosticeren en actie kan ondernemen om de situatie te corrigeren.



Opmerking: Er moet een kleinere waarde voor dit veld worden ingesteld dan voor het veld 'Verwijdering' hierboven, zodat u verloren Jump-clients kunt identificeren voordat ze automatisch worden verwijderd.

Gedrag verwijderende Jump-client

Gedrag verwijderende Jump-client bepaalt wat de access console met een Jump-client doet die door een eindgebruiker is verwijderd. Afhankelijk van de optie uit het vervolkeuzemenu, kan het verwijderde item als verwijderd worden gemarkeerd, maar op de lijst blijven, of van de lijst met Jumpitems in de access console worden verwijderd. Als de Jump-client op het moment van verwijderen geen contact met het B Series Appliance kan maken, blijft het item offline.

Overig

Standaard verbindingstype voor Jump-client

Stel in of het standaard type Jump-client-verbinding actief of passief moet zijn.

Poort voor passieve Jump-client

Met **Poort voor passieve Jump-client** kunt u specificeren welke poort een passieve Jump-client gebruikt om naar een opdracht 'uit slaapmodus halen' van het B Series Appliance te luisteren. De standaardpoort is **5832**. Controleer of de instellingen van de firewall inkomend verkeer via deze poort toestaan voor uw hosts met passieve Jump-clients. Nadat een Jump-client actief is geworden, maakt deze altijd een verbinding met het B Series Appliance via poort 80 of 443 uitgaand.

Gebruikers toestaan om te proberen Jump-clients uit de slaapstand te halen

Gebruikers toestaan om te proberen Jump-clients uit de slaapstand te halen biedt de mogelijkheid om een geselecteerde Jump-client uit slaapmodus te halen door Wake-on-LAN (WOL) pakketten via een andere Jump-client op hetzelfde netwerk te sturen. Als een poging tot WOL is uitgevoerd, dan is deze optie gedurende 30 seconden niet beschikbaar. Pas daarna kan een volgende poging worden ondernomen. WOL moet op de doelcomputer en het netwerk zijn ingeschakeld om deze functie te kunnen gebruiken. De standaard gateway-informatie van de Jump-client wordt gebruikt om te bepalen of andere Jump-clients zich op hetzelfde netwerk bevinden. Bij het verzenden van een WOL-pakket heeft de gebruiker een geavanceerde optie om een wachtwoord mee te geven voor WOL-omgevingen waar zo'n WOL-wachtwoord vereist is.



Opmerking: U kunt Jump-clients zo configureren dat ze gelijktijdige Jumps vanuit het gedeelte **Jump > Jumpitems > Jumpinstellingen** al dan niet toestaan. Indien toegestaan, kunnen meerdere gebruikers toegang tot dezelfde Jump-client verkrijgen zonder uitnodiging van een andere gebruiker om aan een actieve sessie deel te nemen. Indien niet toegestaan, kan maar één Jump-client tegelijk een Jump uitvoeren. Alleen een uitnodiging van de gebruiker die de sessie startte kan een tweede gebruiker toestaan een sessie bij te wonen.



Raadpleeg [Instellingen voor Jump-clients beheren](https://www.beyondtrust.com/docs/privileged-remote-access/how-to/jump-clients/settings.htm) op <https://www.beyondtrust.com/docs/privileged-remote-access/how-to/jump-clients/settings.htm> voor meer informatie.

Jumpgroepen: Configureer welke gebruikers toegang hebben tot welke Jumpitems

 Jump

Jumpgroepen

Jumpgroepen

Een Jumpgroep is een manier om Jumpitems te organiseren en om leden verschillende toegangsniveaus tot deze Jumpitems te bieden. Gebruikers worden aan Jumpgroepen toegewezen ofwel via deze pagina of via de pagina **Gebruikers en beveiliging > Groepsbeleidslijnen**.

[Nieuwe Jumpgroep toevoegen, bewerken, verwijderen](#)

Maak een nieuwe groep aan, wijzig een bestaande groep of verwijder een bestaande groep.

Groep toevoegen of bewerken

Naam

Maak een unieke naam aan om deze groep te identificeren. Deze naam is handig wanneer Jumpitems aan een groep worden toegevoegd en wanneer wordt bepaald welke gebruikers en groepsbeleidslijnen lid zijn van een Jumpgroep.

Codenaam

Stel een codenaam in voor integratiedoeleinden. Als u geen codenaam instelt, maakt PRA er automatisch een aan.

ECM-groep

Selecteer welke ECM-groep aan de Jumpgroep moet worden gekoppeld. Het vervolgkeuzemenu toont ECM-groepen die op de site zijn aangemaakt. Als er geen aangepaste ECM-groepen zijn, is **Standaard** de enige beschikbare optie. Verzoeken om inloggegevens die afkomstig zijn van Jumpitems in een Persoonlijke Jumpgroep worden naar de Standaard ECM-groep geleid.



Opmerking: Deze functie is alleen beschikbaar als de functie is ingeschakeld toen uw site werd gebouwd. Neem contact op met uw sitebeheerder als de functie niet beschikbaar is.



Opmerking: De ECM-groepen moeten bestaan om aan een Jumpgroep gekoppeld te kunnen worden, maar ze moeten ook nog aan een API-account worden gekoppeld om ze door te kunnen leiden. Ga voor meer informatie naar "[API-configuratie: De XML API inschakelen en aangepaste velden configureren](#)" op pagina 150.

Opmerkingen

Voeg een korte beschrijving toe om het doel van deze Jumpgroep samen te vatten.

Groepsbeleidslijnen

Hier wordt een lijst met groepbeleidslijnen weergegeven die gebruikers aan deze Jumpgroep toewijzen.

Toegestane gebruikers

Zoek naar gebruikers om aan deze Jumpgroep toe te voegen. U kunt voor elke gebruiker de **Jumpitem-rol** instellen om de specifieke machtigingen voor Jumpitems in deze Jumpgroep in te stellen. U kunt ook de standaard Jumpitem-rollen van de gebruiker gebruiken die op de pagina **Gebruikers en beveiliging > Groepsbeleidslijnen** of **Gebruikers en beveiliging > Gebruikers** zijn ingesteld. Een Jumpitem-rol is een van te voren gedefinieerde reeks machtigingen voor het beheer en gebruik van Jumpitems.

U kunt ook op elke gebruiker een **Jumpbeleid** toepassen om diens toegang tot de Jumpitems in deze Jumpgroep te beheren. Als u in plaats hiervan **Op Jumpitem ingesteld** selecteert, wordt het Jumpbeleid toegepast op het Jumpitem zelf. Jump-beleidslijnen worden op de pagina **Jump > Jump-beleidslijnen** geconfigureerd en bepalen welke periodes een gebruiker toegang heeft tot dit Jumpitem. Er kan ook een kennisgeving worden verzonden als het Jumpbeleid wordt benaderd of er kan toestemming moeten worden gevraagd om het te benaderen. Als er op de gebruiker of het Jumpitem geen Jumpbeleid is toegepast, is de toegang tot dit Jumpitem onbeperkt.

De bestaande Jumpgroepgebruikers worden in een tabel weergegeven. U kunt gebruikerslijst filteren door een gebruikersnaam in te voeren in het vak **Filteren**. Ook kunt u de instellingen van een gebruiker bewerken of de gebruiker van de Jumpgroep verwijderen.

Ga naar **Gebruikers en beveiliging > Groepsbeleidslijnen** om groepen gebruikers aan een Jumpgroep toe te voegen en wijs die groep aan een of meer Jumpgroepen toe.



Opmerking: Bewerken en verwijderen van functionaliteit kan voor sommige gebruikers zijn uitgeschakeld. Dit gebeurt wanneer een gebruiker via een groepsbeleid is toegevoegd of wanneer de Jumpitem-rol van het systeem van een gebruiker ingesteld is op iets anders dan **Geen toegang**.

Klik op de koppeling voor het groepsbeleid om het beleid als geheel te wijzigen. Alle wijzigingen aan het groepsbeleid gelden voor alle leden van dat groepsbeleid.

Klik op de koppeling voor de gebruiker om Jumpitem-rol van het systeem van die gebruiker te wijzigen. Alle wijzigingen aan de Jumpitem-rol van het systeem van de gebruiker gelden voor alle Jumpgroepen waarvan de gebruiker een niet-toegewezen lid is.

U kunt ook de individuen aan de groep toevoegen en hiermee hun instellingen die ergens anders zijn gedefinieerd, overschrijven.



Raadpleeg [Jumpgroepen gebruiken om te configureren welke gebruikers toegang tot bepaalde Jumpitems hebben](https://www.beyondtrust.com/docs/privileged-remote-access/how-to/jumpoint/jump-groups.htm) op <https://www.beyondtrust.com/docs/privileged-remote-access/how-to/jumpoint/jump-groups.htm> voor meer informatie.

Jump-beleidslijnen: Roosters, kennisgevingen en toestemmingen voor Jumpitems instellen

 Jump**Jump-beleidslijnen**

Jump-beleidslijnen

Jump-beleidslijnen worden gebruikt om te bepalen wanneer toegang tot bepaalde Jumpitems kan worden gekregen door roosters te implementeren, e-mailmeldingen te versturen bij toegang tot een Jumpitem, of door goedkeuring te vereisen of door te vereisen dat een gebruiker een ticketsysteemnummer invult voordat deze toegang krijgt tot een Jumpitem.

Nieuwe Jump-beleidslijn toevoegen, bewerken, verwijderen

Maak een nieuw beleid aan, wijzig een bestaand beleid of verwijder een bestaand beleid.

Een beleid toevoegen of bewerken

Scherмнаam

Maak een unieke naam aan om dit beleid te identificeren. Gebruikers kunnen dit beleid aan deze naam herkennen als het aan Jumpitems wordt toegekend.

Codenaam

Stel een codenaam in voor integratiedoeleinden. Als u geen codenaam instelt, maakt PRA er automatisch een aan.

Beschrijving

Voeg een korte beschrijving toe om het doel van dit beleid samen te vatten.

Jump-rooster

Ingeschakeld

Stel een schema in om te bepalen wanneer Jumpitems waarop dit beleid van toepassing is toegankelijk zijn. Stel de tijdzone in die u voor dit rooster wilt gebruiken en voeg vervolgens een of meer roostervermeldingen toe. Stel voor elke vermelding de startdatum en -tijd en de einddatum en -tijd in.

Als de begintijd bijvoorbeeld is ingesteld op 08.00 uur en de eindtijd op 17.00 uur, dan kan een gebruiker een sessie met dit Jumpitem op elk willekeurig tijdstip binnen deze periode starten en blijven doorwerken tot na de eindtijd. Een poging om na 17.00 uur opnieuw toegang tot dit Jumpitem te krijgen, resulteert echter in een melding dat het schema geen toestemming geeft om een sessie te starten. De gebruiker kan zo nodig kiezen om de schemabeperking te negeren en de sessie toch te starten.

Forceer beëindiging van sessie als het rooster toegang niet toestaat

Als strikter toegangsbeheer noodzakelijk is, moet u het veld **Beëindiging van sessie forceren** aanvinken. Hierdoor wordt afgedwongen dat de verbinding met de sessie op het geplande eindtijdstip wordt verbroken. In dit geval ontvangt de gebruiker herhaalde berichten vanaf 15 minuten voordat de sessie wordt beëindigd.

Jump-mededeling

Geadresseerden berichten wanneer een sessie start

Als deze optie is aangevinkt, wordt een kennisgeving per e-mail naar de aangegeven geadresseerden verzonden wanneer een sessie met een Jumpitem die dit Jumpbeleid gebruikt wordt gestart. Als een gebruiker probeert een sessie te starten met een Jumpitem dat beleid gebruikt, verschijnt een prompt dat er een e-mailmelding wordt verzonden waarin wordt gevraagd of de gebruiker de sessie toch wil starten.

Geadresseerden berichten wanneer een sessie stopt

Als deze optie is aangevinkt, wordt er een kennisgeving per e-mail naar de aangegeven geadresseerden verzonden wanneer een sessie met een Jumpitem die dit Jumpbeleid gebruikt wordt beëindigd. Als gebruikers proberen een sessie te starten met een Jumpitem dat dit beleid gebruikt, krijgen zij een prompt waarin staat dat aan het eind van de sessie een e-mailmelding wordt verzonden waarin wordt gevraagd of de gebruiker de sessie toch wil starten.

E-mailadres(sen)

Voer een of meer e-mailadressen in waar e-mails naartoe moeten worden verzonden. De adressen moeten door een spatie worden gescheiden. Voor deze functie is een geldige [SMTP](#)-configuratie voor uw B Series Appliance vereist. U kunt deze instellen op de pagina [/login > Beheer > E-mailconfiguratie](#).

Schermnaam

Voer de naam van de e-mailgeadresseerde in. Deze naam verschijnt bij de prompt die de gebruiker ziet vóór een sessie met een Jumpitem dat deze beleidslijn gebruikt.

Regio

Als er op deze site meerdere talen zijn ingeschakeld, dan moet u de taal instellen waarin e-mails worden verzonden.

Jump-goedkeuring

Ticket-ID vereist voordat een sessie start

Als deze optie is aangevinkt, dan moet de gebruiker een geldig ticket-ID invoeren voordat een toegangssessie kan starten. Als een gebruiker probeert toegang tot een eindpunt te krijgen wanneer dit Jumpbeleid van toepassing is, dan moet de gebruiker een ticket-ID van uw bestaande ITSM of goedkeuringsproces voor een ticket-ID invoeren voordat toegang wordt verleend. Configureer de integratie met de ITSM of het ticketsysteem vanuit de sectie **Jump-beleidslijnen :: Ticketsysteem**.

Toestemming vereisen voordat een sessie start.

Als deze optie is aangevinkt, wordt er een kennisgeving per e-mail naar de aangegeven geadresseerden verzonden wanneer een sessie met een Jumpitem die dit Jumpbeleid gebruikt wordt gestart. Als een gebruiker probeert een sessie te starten met een Jumpitem dat dit beleid gebruikt, dan verschijnt een dialoog waarin de gebruiker wordt gevraagd een reden voor het verzoek in te voeren evenals het tijdstip en de duur van het verzoek.

Maximale toegangsduur

Stel de maximale tijdsduur in waarvoor een gebruiker toegang kan aanvragen tot een Jumpitem dat dit beleid gebruikt. De gebruiker kan een kortere tijdsduur aanvragen, maar geen langere dan hier is ingesteld.

Toestemming voor toegang geldt voor

Wanneer goedkeuring voor een Jumpitem is verleend, komt dat Jumpitem beschikbaar ofwel voor elke gebruiker die het betreffende Jumpitem kan zien en er toegang toe kan aanvragen of alleen voor de gebruiker die toestemming heeft aangevraagd.

E-mailadres(sen)

Voer een of meer e-mailadressen in waar e-mails naartoe moeten worden verzonden. De adressen moeten door een spatie worden gescheiden. Voor deze functie is een geldige [SMTP](#)-configuratie voor uw B Series Appliance vereist. U kunt deze instellen op de pagina [/login > Beheer > E-mailconfiguratie](#).

Scherмнаam

Voer de naam van de e-mailgeadresseerde in. Deze naam verschijnt bij de prompt die de gebruiker ziet vóór een sessie met een Jumpitem dat deze beleidslijn gebruikt.

Regio

Als er op deze site meerdere talen zijn ingeschakeld, dan moet u de taal instellen waarin e-mails worden verzonden.

Opnamen uitschakelen

Opnamen uitschakelen

Als deze optie is aangevinkt, worden sessies met dit Jumpbeleid niet opgenomen, zelfs als opnames zijn ingeschakeld op de pagina [Configuratie > Opties](#). Dit is van toepassing op scherm delen, gebruikeropnames voor Jump via tunnelprotocol en opdrachtshellopnames.

Sjabloon voor e-mail met mededelingen

Onderwerp

Pas het onderwerp van deze e-mail aan. Klik op de koppeling onder het veld **Body** om de macro's weer te geven die kunnen worden gebruikt om de tekst in uw e-mails voor uw doeleinden aan te passen.

Bericht

Pas de inhoud van deze e-mail aan. Klik op de koppeling onder het veld **Body** om de macro's weer te geven die kunnen worden gebruikt om de tekst in uw e-mails voor uw doeleinden aan te passen.

Sjabloon voor e-mail met goedkeuring

Onderwerp

Pas het onderwerp van deze e-mail aan. Klik op de koppeling onder het veld **Body** om de macro's weer te geven die kunnen worden gebruikt om de tekst in uw e-mails voor uw doeleinden aan te passen.

Bericht

Pas de inhoud van deze e-mail aan. Klik op de koppeling onder het veld **Body** om de macro's weer te geven die kunnen worden gebruikt om de tekst in uw e-mails voor uw doeleinden aan te passen.

Ticketsysteem

URL van ticketsysteem

Voer in **URL van ticketsysteem** de URL in voor uw externe ticketsysteem. Het B Series Appliance verzendt een uitgaand verzoek naar uw externe ticketsysteem. De URL moet de juiste opmaak hebben voor HTTP of HTTPS. Als u een HTTPS-URL invoert, dan moet het certificaat van de site geverifieerd zijn om een geldige verbinding te maken. Als er een Jumpbeleid bestaat waarvoor een ticket-ID vereist is, dan moet een URL voor het ticketsysteem zijn ingevoerd, anders ontvangt u een waarschuwing.

Een certificaat voor HTTPS-verbindingen uploaden

Klik op **Certificaat kiezen** om het certificaat voor de verbinding van het HTTPS-ticketsysteem naar het B Series Appliance te uploaden. Als het certificaat is geüpload, gebruikt het B Series Appliance dit wanneer het apparaat met het externe systeem contact maakt. Als u geen certificaat uploadt en het selectievakje **SSL-certificaatfouten negeren** inschakelt, valt het B Series Appliance eventueel terug op het ingebouwde certificaatarchief als het verzoek wordt verzonden.

Gebruikersprompt

Voer bij **Gebruikersprompt** de tekst voor het dialoogvenster in die gebruikers van access console moeten zien als hun wordt gevraagd het ticket-ID in te voeren om toegang te krijgen.

Ticket-ID behandelen als gevoelige informatie

Als dit selectievakje is ingeschakeld, wordt de ticket-ID beschouwd als gevoelige informatie en worden in plaats van tekst sterretjes weergegeven. U moet een HTTPS-URL voor het ticketsysteem gebruiken. Als een adres met HTTP wordt ingevoerd, verschijnt er een foutmelding dat u HTTPS moet gebruiken.

Wanneer deze functie is ingeschakeld, kunt u problemen met SSL-certificaten niet omzeilen door het vakje **SSL-certificaatfouten negeren** aan te vinken. Dit betekent dat u een geldig SSL-certificaat moet hebben. Als u het vakje **SSL-certificaatfouten negeren** probeert aan te vinken, verschijnt er een melding dat u SSL-certificaatfouten niet kunt negeren.

Als de ticket-ID gevoelig is, gelden de volgende regels:

- De toegangsconsoles van zowel het bureaublad als de web geven sterretjes weer in plaats van tekst.
- Het ticket wordt nergens gelogd door de toegangsconsole of op het B Series Appliance.



Raadpleeg [Jump-beleidslijnen maken om toegang tot Jumpitems te beheren](https://www.beyondtrust.com/docs/privileged-remote-access/how-to/jumpoint/policies.htm) op <https://www.beyondtrust.com/docs/privileged-remote-access/how-to/jumpoint/policies.htm> voor meer informatie.

SSL-certificaatfouten negeren

Als deze optie is aangevinkt, neemt de B Series Appliance **niet** de informatie om het certificaat te valideren op als het met het externe ticketsysteem contact maakt. Zorg dat deze optie niet is aangevinkt als u een certificaat voor een beveiligde HTTPS-verbinding uploadt.

Jumpitem-rollen: Machtigingen aanmaken voor Jumpitems



Jump

Jumpitem-rollen

Jumpitem-rollen

Een jumpsnelkoppelingsrol is een van te voren gedefinieerde reeks machtigingen voor het beheer en gebruik van jumpsnelkoppelingen. Jumpsnelkoppelingsrollen zijn van toepassing op gebruikers van de pagina **Jump > Jumpgroepen** of van de pagina **Gebruikers en beveiliging > Groepsbeleidslijnen**.

Als meerdere rollen aan een gebruiker zijn toegewezen, dan wordt altijd de meest specifieke rol voor een gebruiker gebruikt. De volgorde van specificiteit voor jumpsnelkoppelingsrollen is, van meest specifiek naar minst specifiek:

- De rol die is toegewezen aan de relatie tussen een gebruiker en een Jumpgroep op de pagina **Jump > Jumpgroepen**.
- De rol die is toegewezen aan de relatie tussen een gebruiker en een Jumpgroep op de pagina **Gebruikers en beveiliging > Groepsbeleidslijnen**.
- De **Jumpsnelkoppelingsrollen** die voor een gebruiker geconfigureerd zijn op de pagina **Gebruikers en beveiliging > Gebruikers** of op de pagina **Gebruikers en beveiliging > Groepsbeleidslijnen**.

Nieuwe Jumpitem-rol toevoegen, bewerken, verwijderen

Maak een nieuwe rol aan, wijzig een bestaande rol of verwijder een bestaande rol.

Jumpitemrol toevoegen of bewerken

Naam

Maak een unieke naam aan om deze rol te identificeren. Deze naam is handig wanneer een Jumpitemrol met een gebruiker of groep gebruikers in een jumpgroep wordt gekoppeld.

Beschrijving

Voeg een korte beschrijving toe om het doel van deze rol samen te vatten.

Machtigingen

Jumpgroep of persoonlijke Jumpitems

Nieuwe Jumpitems aanmaken en implementeren

Hiermee kunnen gebruikers Jumpitems aanmaken en deze op externe systemen installeren.

Jumpitems verplaatsen en kopiëren

Hiermee kan de gebruiker Jumpitems verplaatsen van de ene Jumpgroep naar een andere Jumpgroep. Deze machtiging moet voor beide Jumpgroepen zijn ingeschakeld. Gekopieerde Jumpitems kunnen bewerkt worden.



Ga voor meer informatie over het kopiëren van Jumpitems naar [Jump-interface: Jumpitems gebruiken voor toegang tot externe systemen](#) op <https://www.beyondtrust.com/docs/privileged-remote-access/getting-started/access-console/jump-interface.htm>.

Bestaande Jumpitems verwijderen

Hiermee kunnen gebruikers Jumpitems verwijderen.

Jumpitem

Sessies starten

Hiermee kan de gebruiker een Jump uitvoeren naar externe systemen.

Tag bewerken

Hiermee kan de gebruiker een tag-veld van een Jumpitem bewerken.

Opmerkingen bewerken

Hiermee kan de gebruiker een opmerkingenveld van een Jumpitem bewerken.

Jump-beleid bewerken

Hiermee kan de gebruiker instellen welk Jumpbeleid op een Jumpitem wordt toegepast.

Sessiebeleid bewerken

Hiermee kan de gebruiker instellen welk sessiebeleid een Jumpitem moet gebruiken. Het wijzigen van het sessiebeleid kan van invloed zijn op de machtigingen in de sessie.

Connectiviteit en verificatie bewerken

Hiermee kan de gebruiker de verbinding en verificatiegegevens van een Jumpitem wijzigen. Denk hierbij onder andere aan velden zoals hostnaam, Jumpoint, poort en gebruikersnaam.

Gedrag en ervaring bewerken

Hiermee kan de gebruiker het gedrag van Jumpitems wijzigen. Denk hierbij onder andere aan velden zoals verbindingstype, weergavegrootte en terminal-type.



Raadpleeg [Jump-itemrollen gebruiken om machtigingssets te configureren voor Jump-items](https://www.beyondtrust.com/docs/privileged-remote-access/how-to/jumpoint/jump-item-roles.htm) op <https://www.beyondtrust.com/docs/privileged-remote-access/how-to/jumpoint/jump-item-roles.htm> voor meer informatie.

Jumpoint: Toegang zonder toezicht naar een netwerk instellen



Jump

Jumpoint

Jumpoint beheer

Met de Jump-technologie van BeyondTrust kan een gebruiker toegang krijgen tot computers op een extern netwerk zonder vooraf op elke machine software te moeten installeren. Er hoeft alleen een enkele Jumpoint-agent op een willekeurige netwerklocatie te zijn geïnstalleerd om zonder toezicht toegang tot elke pc in dat netwerk te krijgen.

Nieuw Jumpoint toevoegen, bewerken, verwijderen

Maak een nieuw Jumpoint aan, wijzig een bestaand Jumpoint of verwijder een bestaand Jumpoint.

Opnieuw implementeren

Verwijder de installatie van een Jumpoint en download een installatieprogramma om het bestaande Jumpoint door een nieuw te vervangen. Snelkoppelingen voor een Jump met het bestaande Jumpoint zullen het nieuwe Jumpoint gebruiken als dat geïnstalleerd is.



Opmerking: Als een bestaand Jumpoint wordt vervangen, dan wordt de configuratie ervan niet opgeslagen. Het nieuwe Jumpoint moet opnieuw worden geconfigureerd.

Jumpoint toevoegen of bewerken

Naam

Maak een unieke naam aan om dit Jumpoint te identificeren. Deze naam helpt gebruikers om dit Jumpoint te lokaliseren als zij een sessie met een computer op hetzelfde netwerk moeten opstarten.

Codenaam

Stel een codenaam in voor integratiedoeleinden. Als u geen codenaam instelt, maakt PRA er automatisch een aan.

Opmerkingen

Voeg een korte beschrijving toe om het doel van dit Jumpoint samen te vatten. Dit is handig bij het beheren van Jumpoints.

Uitgeschakeld

Als dit is aangevinkt, dan kan het Jumpoint geen Jump-verbindingen maken.

Geclusterd

Als dit is aangevinkt, dan kunt u meerdere, redundante nodes van hetzelfde Jumpoint op verschillende hostsystemen toevoegen. Zo zorgt u ervoor dat het Jumpoint beschikbaar blijft zolang er ten minste één node online blijft.

Shell Jump activeren

Als u gebruikers wilt toestaan om via dit Jumpoint verbinding te maken met netwerkapparaten met SSH of Telnet, moet u **Toegang tot Shell Jump-methode activeren** aanvinken. Opdrachtfiltering kan worden geconfigureerd om het per ongeluk gebruiken van opdrachten die schadelijk kunnen zijn voor de eindpuntsystemen te voorkomen.

i Raadpleeg [Shell-jump gebruiken om toegang tot een apparaat in een extern netwerk te krijgen](https://www.beyondtrust.com/docs/privileged-remote-access/getting-started/access-console/shell-jump.htm) op www.beyondtrust.com/docs/privileged-remote-access/getting-started/access-console/shell-jump.htm voor meer informatie over het filteren van opdrachten.

Methode voor Jump via tunnelprotocol inschakelen

Als **Methode voor Jump via tunnelprotocol inschakelen** is geselecteerd, kunnen gebruikers TCP-verbindingen maken vanaf hun systemen naar externe eindpunten via dit Jumpoint.

RDP-serviceaccount

Selecteer de account die door een Jumpoint moet worden gebruikt voor het uitvoeren van een door de gebruiker geïnitieerde client op de RPD-server. Dit maakt het mogelijk om aanvullende gebeurtenisinformatie te verzamelen van een RPD-sessie die met dit Jumpoint is gestart. Deze account wordt alleen gebruikt als het Remote RPD Jumpitem is geconfigureerd om de functionaliteit voor **Forensische gegevens van sessies** te kunnen inschakelen.

i Lees voor meer informatie over het instellen van de functionaliteit voor **Forensische gegevens** in de access console [RDP gebruiken om toegang tot een extern Windows-eindpunt te krijgen](https://www.beyondtrust.com/docs/privileged-remote-access/getting-started/access-console/rdp.htm) op <https://www.beyondtrust.com/docs/privileged-remote-access/getting-started/access-console/rdp.htm>.

Groepsbeleidslijnen

Geeft de groepsbeleidslijnen weer die gebruikers toestemming verlenen tot deze Jumpoint.

Toegestane gebruikers

Naam nieuw lid

Zoek naar gebruikers om aan dit Jumpoint toe te voegen. Gebruikers die dit Jumpoint mogen gebruiken, kunnen sessies starten met Jumpitems of Jumpitems maken die via dit Jumpoint verbinding maken, op voorwaarde dat zij daarvoor zijn gemachtigd.

De onderstaande tabel geeft de bestaande Jumpoint-gebruikers weer. U kunt de weergave filteren door een tekenreeks in te voeren in het tekstvak **Filteren op naam**. Ook kunt u vanaf het Jumpoint gebruikers verwijderen.

Ga naar **Gebruikers en beveiliging > Groepsbeleidslijnen** om een groep gebruikers aan een Jumpoint toe te voegen en wijs die groep aan een of meer Jumpoints toe.



Opmerking: Voor sommige gebruikers zijn de opties **Verwijderen** uitgeschakeld. Dit gebeurt wanneer een gebruiker via een groepsbeleid wordt toegevoegd.

Klik op de koppeling voor het groepsbeleid om het beleid als geheel te wijzigen. Alle wijzigingen aan het groepsbeleid gelden voor alle leden van dat groepsbeleid.

U kunt ook de individuen aan het Jumpoint toevoegen en hiermee hun instellingen die ergens anders zijn gedefinieerd, overschrijven.



Zie voor meer informatie over configuratie van een Jumpoints [Een PRA Jumpoint configureren en installeren](https://www.beyondtrust.com/docs/privileged-remote-access/how-to/jumpoint/installation.htm) op www.beyondtrust.com/docs/privileged-remote-access/how-to/jumpoint/installation.htm.

Jumpitems: Bulkimport van snelkoppelingen naar Jumps en beheren van instellingen voor Jumpitems

 Jump

Jumpitems

Wizard voor bulkimport van snelkoppelingen naar Jumps

Via een Jumpoint kunnen Jumpsnelkoppelingen gemaakt worden om het volgende te doen:

- een standaard toegangssessie starten
- een sessie via Remote Desktop Protocol starten met een Windows- of Linux-systeem
- een Jump naar een website op een externe browser maken
- een Shell Jump te maken naar een netwerkapparaat met SSH of Telnet
- verbinden met een VNC-server
- een Jump via tunnelprotocol gebruiken om een TCP-verbinding te maken



Opmerking: Linux Jumpoints kunnen alleen worden gebruikt voor RDP en SSH/Telnet-sessies. Dit maakt inloggegevensinjectie van de gebruiker of vanuit vault mogelijk; ook de functie Externe app en het filteren van Shell Jumps is hierdoor mogelijk. Geclusterde Jumpoints kunnen alleen nieuwe nodes van hetzelfde besturingssysteem toevoegen. U kunt Windows- en Linux-nodes niet door elkaar gebruiken.

Als u een groot aantal snelkoppelingen naar Jumps maakt, is het mogelijk eenvoudiger om deze uit een werkblad te importeren dan om ze een voor een toe te voegen in de access console.



Zie voor meer informatie [Een Jumpitem gebruiken voor het uitvoeren van een Jump naar een extern systeem](https://www.beyondtrust.com/docs/privileged-remote-access/how-to/jumpoint/jump-shortcuts.htm) op <https://www.beyondtrust.com/docs/privileged-remote-access/how-to/jumpoint/jump-shortcuts.htm>.


Sjabloon downloaden

Selecteer in het vervolgkeuzemenu in het gedeelte **Wizard voor bulkimport van snelkoppelingen voor Jumps** in de /login-interface het type Jumpitem dat u wilt toevoegen en klik daarna op **Sjabloon downloaden**. Gebruik de tekst uit de CSV-sjabloon als kolomkoppen en voeg de informatie toe voor elke snelkoppeling naar een Jump die u wilt importeren. Het importeren mislukt als er verplichte velden ontbreken. Optionele velden kunnen worden ingevuld of leeg blijven.

Snelkoppelingen naar Jumps importeren

Nadat u de sjabloon helemaal hebt ingevuld, kunt u **Snelkoppelingen naar Jumps importeren** gebruiken om het CSV-bestand met de informatie over de Jumpitems te uploaden. De maximale bestandsgrootte die in één keer kan worden geüpload is 5 MB. Elk CSV-bestand kan maar één type Jumpitem bevatten. De opmaak van het CSV-bestand moet aan de beschrijving in de onderstaande tabellen voldoen.

Lokale jumpsnelkoppeling

Veld	Beschrijving
Hostnaam	De hostnaam van het eindpunt dat toegankelijk moet zijn voor dit Jumpitem. Deze tekenreeks mag maximaal 128 tekens lang zijn.
Naam	De naam van het eindpunt waarop toegang kan worden verkregen door dit Jumpitem. Het item is onder deze naam te vinden in de sessietabbladen. Deze tekenreeks mag maximaal 128 tekens lang zijn.
Jumpgroep	De codenaam van de Jumpgroep waarmee dit Jumpitem moet worden geassocieerd. <div style="border: 1px solid black; padding: 5px; margin-top: 10px;">  Opmerking: Bij gebruik van de importmethode kan een Jumpitem niet met een persoonlijke lijst met Jumpitems worden geassocieerd. </div>
Tag (optioneel)	U kunt uw Jumpitems in categorieën onderverdelen door een tag toe te voegen. Deze tekenreeks mag maximaal 1024 tekens lang zijn.
Opmerkingen (optioneel)	U kunt commentaar aan uw Jumpitems toevoegen. Deze tekenreeks mag maximaal 1024 tekens lang zijn.
Jumpbeleid (optioneel)	De codenaam van een Jump-beleid. U kunt een Jump-beleid opgeven om de toegang tot dit Jumpitem te beheren.
Sessiebeleid (optioneel)	De codenaam van een sessiebeleid. U kunt een sessiebeleid specificeren om de machtigingen te beheren die op dit Jumpitem beschikbaar zijn.
Beleid voor eindpuntovereenkomst (optioneel)	Met de waarde Accepteren wordt de eindpuntovereenkomst automatisch geaccepteerd als er een time-out optreedt en kan de sessie starten. Met de waarde Weigeren wordt de eindpuntovereenkomst automatisch geweigerd en kan de sessie niet starten. Met de waarde Niet_vragen wordt geen eindpuntovereenkomst getoond, ook al is de functie geconfigureerd. Dit veld heeft geen invloed op de algemene eindpuntovereenkomst als het niet is ingeschakeld.

i Zie voor meer informatie over de algemene instelling [Jumpitems: Bulkimport van Jumpsnelkoppelingen en beheren van instellingen voor Jumpitems](https://www.beyondtrust.com/docs/privileged-remote-access/getting-started/admin/jump-items.htm) op <https://www.beyondtrust.com/docs/privileged-remote-access/getting-started/admin/jump-items.htm>.

Externe jumpsnelkoppeling

Veld	Beschrijving
Hostnaam	De hostnaam van het eindpunt dat toegankelijk moet zijn voor dit Jumpitem. Deze tekenreeks mag maximaal 128 tekens lang zijn.
Jumpoint	De codenaam van het Jumpoint waarmee toegang tot het eindpunt wordt verkregen.
Naam	De naam van het eindpunt waarop toegang kan worden verkregen door dit Jumpitem. Het item is onder deze naam te vinden in de sessietabbladen. Deze tekenreeks mag maximaal 128 tekens lang zijn.
Jumpgroep	De codenaam van de Jumpgroep waarmee dit Jumpitem moet worden geassocieerd.

Veld	Beschrijving
	 Opmerking: Bij gebruik van de importmethode kan een Jumpitem niet met een persoonlijke lijst met Jumpitems worden geassocieerd.
Tag (optioneel)	U kunt uw Jumpitems in categorieën onderverdelen door een tag toe te voegen. Deze tekenreeks mag maximaal 1024 tekens lang zijn.
Opmerkingen (optioneel)	U kunt commentaar aan uw Jumpitems toevoegen. Deze tekenreeks mag maximaal 1024 tekens lang zijn.
Jump-beleid (optioneel)	De codenaam van een Jump-beleid. U kunt een Jump-beleid opgeven om de toegang tot dit Jumpitem te beheren.
Sessiebeleid (optioneel)	De codenaam van een sessiebeleid. U kunt een sessiebeleid specificeren om de machtigingen te beheren die op dit Jumpitem beschikbaar zijn.
Beleid voor eindpuntovereenkomst (optioneel)	Met de waarde Accepteren wordt de eindpuntovereenkomst automatisch geaccepteerd als er een time-out optreedt en kan de sessie starten. Met de waarde Weigeren wordt de eindpuntovereenkomst automatisch geweigerd en kan de sessie niet starten. Met de waarde Niet_vragen wordt geen eindpuntovereenkomst getoond, ook al is de functie geconfigureerd. Dit veld heeft geen invloed op de algemene eindpuntovereenkomst als het niet is ingeschakeld.

i Zie voor meer informatie over de algemene instelling *Jumpitems: Bulkimport van Jumpsnelkoppelingen en beheren van instellingen voor Jumpitems* op <https://www.beyondtrust.com/docs/privileged-remote-access/getting-started/admin/jump-items.htm>.

Externe VNC-jumpsnelkoppeling

Veld	Beschrijving
Hostnaam	De hostnaam van het eindpunt dat toegankelijk moet zijn voor dit Jumpitem. Deze tekenreeks mag maximaal 128 tekens lang zijn.
Jumpoint	De codenaam van het Jumpoint waarmee toegang tot het eindpunt wordt verkregen.
Poort (optioneel)	Een geldig poortnummer tussen 100 en 65535 . De standaard poort is 5900 .
Naam	De naam van het eindpunt waarop toegang kan worden verkregen door dit Jumpitem. Het item is onder deze naam te vinden in de sessietabbladen. Deze tekenreeks mag maximaal 128 tekens lang zijn.
Jumpgroep	De codenaam van de Jumpgroep waarmee dit Jumpitem moet worden geassocieerd.  Opmerking: Bij gebruik van de importmethode kan een Jumpitem niet met een persoonlijke lijst met Jumpitems worden geassocieerd.
Tag (optioneel)	U kunt uw Jumpitems in categorieën onderverdelen door een tag toe te voegen. Deze tekenreeks mag maximaal 1024 tekens lang zijn.

Veld	Beschrijving
Opmerkingen (optioneel)	U kunt commentaar aan uw Jumpitems toevoegen. Deze tekenreeks mag maximaal 1024 tekens lang zijn.
Jump-beleid (optioneel)	De codenaam van een Jump-beleid. U kunt een Jump-beleid opgeven om de toegang tot dit Jumpitem te beheren.

Externe RDP-snelkoppeling

Veld	Beschrijving
Hostnaam	De hostnaam van het eindpunt dat toegankelijk moet zijn voor dit Jumpitem. Deze tekenreeks mag maximaal 128 tekens lang zijn.
Jumpoint	De codenaam van het Jumpoint waarmee toegang tot het eindpunt wordt verkregen.
Gebruikersnaam (optioneel)	De gebruikersnaam om u mee aan te melden.
Domein (optioneel)	Het domein waarin het eindpunt zich bevindt.
Kwaliteit (optioneel)	De kwaliteit waarmee u het externe systeem wilt bekijken. Dit kan low zijn (zwart-wit voor het laagste gebruik van bandbreedte), best_perf (standaard, 8-bits kleur voor snelle prestaties), perf_and_qual (16 bit voor gemiddelde kwaliteit en prestaties), best_qual (32-bits voor de hoogste beeldresolutie) of video_opt (VP9-code voor vloeiende videobeeld). Dit kan tijdens de sessie met bureaublad op afstand (RDP) niet worden gewijzigd.
Consolesessie	1: Hiermee start een consolesessie. 0: Hiermee start een nieuwe sessie (standaard).
Onbetrouwbaar certificaat negeren (optioneel)	1: Negeert certificaatwaarschuwingen. 0: Toont een waarschuwing als het certificaat van de server niet kan worden geverifieerd.
SecureApp-type	De SecureApp opstartmethode. Kan zijn 'none', 'remote_app' (om de ingebouwde externe app-functionaliteit van RDP te gebruiken), 'remote_desktop_agent' (om de agent voor extern bureaublad in BeyondTrust te gebruiken), of 'remote_desktop_agent_credentials' (om in BeyondTrust de agent voor extern bureaublad met inloggegevensinjectie te gebruiken). Als 'remote_desktop_agent' of 'remote_desktop_agent_credentials' wordt gekozen, moet de agent voor extern bureaublad in BeyondTrust op het externe systeem worden geïnstalleerd.>
Naam van externe toepassing	De naam van de externe app. Deze tekenreeks mag maximaal 520 tekens lang zijn.
Parameters van externe toepassing	Een door spaties gescheiden lijst met parameters om toegang te krijgen tot de externe app. Voor parameters met spaties moet u dubbele aanhalingstekens gebruiken. Deze tekenreeks mag maximaal 16000 tekens lang zijn.
Parameters voor uitvoerbaar bestand op afstand	Een door spaties gescheiden lijst met parameters om door te geven aan het externe uitvoerbare bestand dat zal worden opgestart met de BeyondTrust-agent voor toegang tot extern bureaublad. Voor parameters met spaties moet u dubbele aanhalingstekens gebruiken. Deze kan alleen worden gebruikt als het type SecureApp de BeyondTrust-agent voor toegang tot extern bureaublad gebruikt.
Parameters voor uitvoerbaar bestand op	Een door spaties gescheiden lijst met parameters om door te geven aan het externe uitvoerbare bestand dat zal worden opgestart met de BeyondTrust-agent voor toegang tot extern bureaublad. Voor parameters

Veld	Beschrijving
afstand	met spaties moet u dubbele aanhalingstekens gebruiken. Deze kan alleen worden gebruikt als het type SecureApp de BeyondTrust-agent voor toegang tot extern bureaublad gebruikt.
Doelsysteem	De naam van het doelsysteem dat door de externe toepassing wordt benaderd. Deze waarde wordt gebruikt om de lijst met geïnjecteerde inloggegevens te beperken tot de inloggegevens die geldig zijn voor het doelsysteem. Deze waarde kan alleen worden gebruikt als het SecureApp-type de BeyondTrust-agent voor toegang tot extern bureaublad met inloggegevensinjectie gebruikt.
Type inloggegevens	Het type inloggegevens dat in de externe toepassing wordt geïnjecteerd. Deze waarde is afhankelijk van de wachtwoordkluis waar de inloggegevens uit worden verkregen. Deze waarde kan alleen worden gebruikt als het SecureApp-type de BeyondTrust-agent voor toegang tot extern bureaublad met inloggegevensinjectie gebruikt.
Naam	De naam van het eindpunt waarop toegang kan worden verkregen door dit Jumpitem. Het item is onder deze naam te vinden in de sessietabbladen. Deze tekenreeks mag maximaal 128 tekens lang zijn.
Jumpgroep	De codenaam van de Jumpgroep waarmee dit Jumpitem moet worden geassocieerd. <div style="border: 1px solid black; padding: 5px; margin-top: 10px;">  Opmerking: Bij gebruik van de importmethode kan een Jumpitem niet met een persoonlijke lijst met Jumpitems worden geassocieerd. </div>
Tag (optioneel)	U kunt uw Jumpitems in categorieën onderverdelen door een tag toe te voegen. Deze tekenreeks mag maximaal 1024 tekens lang zijn.
Opmerkingen (optioneel)	U kunt commentaar aan uw Jumpitems toevoegen. Deze tekenreeks mag maximaal 1024 tekens lang zijn.
Jump-beleid (optioneel)	De codenaam van een Jump-beleid. U kunt een Jump-beleid opgeven om de toegang tot dit Jumpitem te beheren.

Shell Jump-snelkoppeling

Veld	Beschrijving
Hostnaam	De hostnaam van het eindpunt dat toegankelijk moet zijn voor dit Jumpitem. Deze tekenreeks mag maximaal 128 tekens lang zijn.
Jumpoint	De codenaam van het Jumpoint waarmee toegang tot het eindpunt wordt verkregen.
Gebruikersnaam (optioneel)	De gebruikersnaam om u mee aan te melden.
Protocol	Mag SSH of Telnet zijn.
Poort (optioneel)	Een geldig poortnummer van 1 tot 65535 . Het standaard poortnummer is 22 als het protocol ssh is, of 23 als het protocol telnet is.
Terminal-type (optioneel)	Dit kan xterm zijn (standaard) of VT100 .
Keepalive (optioneel)	Het aantal seconden tussen ieder verzonden pakket om te voorkomen dat een niet-actieve sessie wordt gestopt. Dit kan elk getal zijn tussen 0 en 300 . Met 0 wordt het actief houden uitgeschakeld (standaard).


Veld	Beschrijving
Naam	De naam van het eindpunt waarop toegang kan worden verkregen door dit Jumpitem. Het item is onder deze naam te vinden in de sessietabbladen. Deze tekenreeks mag maximaal 128 tekens lang zijn.
Jumpgroep	De codenaam van de Jumpgroep waarmee dit Jumpitem moet worden geassocieerd. <div style="border: 1px solid black; padding: 5px; margin-top: 10px;">  Opmerking: Bij gebruik van de importmethode kan een Jumpitem niet met een persoonlijke lijst met Jumpitems worden geassocieerd. </div>
Tag (optioneel)	U kunt uw Jumpitems in categorieën onderverdelen door een tag toe te voegen. Deze tekenreeks mag maximaal 1024 tekens lang zijn.
Opmerkingen (optioneel)	U kunt commentaar aan uw Jumpitems toevoegen. Deze tekenreeks mag maximaal 1024 tekens lang zijn.
Jumpbeleid (optioneel)	De codenaam van een Jump-beleid. U kunt een Jump-beleid opgeven om de toegang tot dit Jumpitem te beheren.
Sessiebeleid (optioneel)	De codenaam van een sessiebeleid. U kunt een sessiebeleid specificeren om de machtigingen te beheren die op dit Jumpitem beschikbaar zijn.

Protocoltunnel-jumpsnelkoppeling

Veld	Beschrijving
Hostnaam	De hostnaam van het eindpunt dat toegankelijk moet zijn voor dit Jumpitem. Deze tekenreeks mag maximaal 128 tekens lang zijn.
Jumpoint	De codenaam van het Jumpoint waarmee toegang tot het eindpunt wordt verkregen.
TCP-tunnels	De lijst van een of meer tunneldefinities. Een tunneldefinitie is een toewijzing van een TCP-poort op het systeem van de lokale gebruiker aan een TCP-poort op het externe eindpunt. Elke verbinding die naar de lokale poort wordt gemaakt, zorgt ervoor dat er een verbinding naar de externe poort wordt gemaakt, zodat gegevens lussen lokale en externe systemen kunnen worden getunneld. Meerdere toewijzingen moeten door een puntkomma worden gescheiden. <div style="border: 1px solid black; padding: 5px; margin-top: 10px;">  auto->22;3306->3306 </div> <p>In dit voorbeeld wordt een willekeurige lokale poort op externe poort 22 toegewezen, terwijl lokale poort 3306 op externe poort 3306 wordt toegewezen.</p>
Lokaal adres (optioneel)	Het adres vanwaar de verbinding moet worden gemaakt. Dit kan elk willekeurig adres zijn met sub-bereik 127.x.x.x. Het standaard adres is 127.0.0.1.
Naam	De naam van het eindpunt waarop toegang kan worden verkregen door dit Jumpitem. Het item is onder deze naam te vinden in de sessietabbladen. Deze tekenreeks mag maximaal 128 tekens lang zijn.
Jumpgroep	De codenaam van de Jumpgroep waarmee dit Jumpitem moet worden geassocieerd. <div style="border: 1px solid black; padding: 5px; margin-top: 10px;">  Opmerking: Bij gebruik van de importmethode kan een Jumpitem niet met een persoonlijke lijst met Jumpitems worden geassocieerd. </div>

Veld	Beschrijving
Tag (optioneel)	U kunt uw Jumpitems in categorieën onderverdelen door een tag toe te voegen. Deze tekenreeks mag maximaal 1024 tekens lang zijn.
Opmerkingen (optioneel)	U kunt commentaar aan uw Jumpitems toevoegen. Deze tekenreeks mag maximaal 1024 tekens lang zijn.
Jump-beleid (optioneel)	De codenaam van een Jump-beleid. U kunt een Jump-beleid opgeven om de toegang tot dit Jumpitem te beheren.

Snelkoppeling naar Web Jump

Veld	Beschrijving
Naam	De naam van het eindpunt waarop toegang kan worden verkregen door dit Jumpitem. Het item is onder deze naam te vinden in de sessietabbladen. Deze tekenreeks mag maximaal 128 tekens lang zijn.
Jumpoint	De codenaam van het Jumpoint waarmee toegang tot het eindpunt wordt verkregen.
Jumpgroep	De codenaam van de Jumpgroep waarmee dit Jumpitem moet worden geassocieerd. <div style="border: 1px solid black; background-color: #e1f5fe; padding: 5px; margin-top: 10px;">  Opmerking: Bij gebruik van de importmethode kan een Jumpitem niet met een persoonlijke lijst met Jumpitems worden geassocieerd. </div>
Tag (optioneel)	U kunt uw Jumpitems in categorieën onderverdelen door een tag toe te voegen. Deze tekenreeks mag maximaal 1024 tekens lang zijn.
Opmerkingen (optioneel)	U kunt commentaar aan uw Jumpitems toevoegen. Deze tekenreeks mag maximaal 1024 tekens lang zijn.
Jump-beleid (optioneel)	De codenaam van een Jump-beleid. U kunt een Jump-beleid opgeven om de toegang tot dit Jumpitem te beheren.
Sessiebeleid (optioneel)	De codenaam van een sessiebeleid. U kunt een sessiebeleid specificeren om de machtigingen te beheren die op dit Jumpitem beschikbaar zijn.
URL	De URL van de website. De URL moet beginnen met http of https .
Certificaat verifiëren (optioneel)	1: Het certificaat voor de website wordt vóór het begin van de sessie gevalideerd. Als er problemen zijn, gaat de sessie niet van start. 0: Het certificaat voor de website is niet gevalideerd.
Opmaak gebruikersnaam	passthru: Voer de gebruikersnaam rechtstreeks door van de provider van de inloggegevens. username_only: Als de gebruikersnaam in UPN-indeling (Gebruikersnaam@Domein) of DLLN-indeling (DOMEIN\Gebruikersnaam) is, wordt het domein verwijderd. Alleen de gebruikersnaam wordt dan geïnjecteerd.
Hint veld Gebruikersnaam	Een selectiefunctie voor query's in CSS-stijl die het gebruikersnaamveld identificeert om te helpen bij de initiële inloggegevensinjectie. Als deze waarde wordt verstrekt en er geen overeenkomend element wordt gevonden, zal de inloggegevensinjectie mislukken.
Hint veld Wachtwoord	Een selectiefunctie voor query's in CSS-stijl die het wachtwoordveld identificeert om te helpen bij de initiële inloggegevensinjectie. Als deze waarde wordt verstrekt en er geen overeenkomend element wordt gevonden, zal de inloggegevensinjectie mislukken.

Veld	Beschrijving
Hint knop Verzenden	Een selectiefunctie voor query's in CSS-stijl die de knop Verzenden identificeert om te helpen bij de initiële inloggegevensinjectie. Als deze waarde wordt verstrekt en er geen overeenkomend element wordt gevonden, zal de inloggegevensinjectie mislukken.
Time-out verificatie	De tijd die de webjumpclient moet wachten voor een geslaagde verificatie voor een time-out. Geldige waarden zijn 1, 2, 3, 5, 10, 15, 30



Zie voor meer informatie [Een Jumpitem gebruiken voor het uitvoeren van een Jump naar een extern systeem](https://www.beyondtrust.com/docs/privileged-remote-access/how-to/jumpoint/jump-shortcuts.htm) op <https://www.beyondtrust.com/docs/privileged-remote-access/how-to/jumpoint/jump-shortcuts.htm>.

Eindpuntgebruikerscontract

Schakel de configuratie van toestemming van eindpuntgebruikers in voor toepasselijke Jumpitems

Schakel een vervolgkeuzelijst in de toegangsconsole in, waarmee opties voor overeenkomsten voor eindpuntgebruikers kunnen worden geconfigureerd voor afzonderlijke Jumpitems.

Titel

Pas de titel van de overeenkomst aan. De eindgebruiker ziet deze in de titelbalk van de melding. U kunt deze tekst vertalen voor elke taal die u hebt ingeschakeld. Om de standaard tekst terug te zetten, moet u de tekst in het veld verwijderen en daarna het lege veld opslaan.

Tekst

Geef de tekst op voor de overeenkomst. U kunt deze tekst vertalen voor elke taal die u hebt ingeschakeld. Om de standaard tekst terug te zetten, moet u de tekst in het veld verwijderen en daarna het lege veld opslaan.

Time-out voor accepteren

Als de gebruiker de overeenkomst niet binnen de ingestelde **Time-out voor accepteren** accepteert, wordt de overeenkomst aanvaard of geweigerd overeenkomstig de eigenschappen van het Jumpitem.

Automatisch gedrag

Kies **Automatisch accepteren** of **Automatisch weigeren**. Met de waarde **Automatisch accepteren** wordt de eindpuntovereenkomst automatisch geaccepteerd als er een time-out optreedt en kan de sessie starten. Met de waarde **Automatisch weigeren** wordt de eindpuntovereenkomst automatisch geweigerd en kan de sessie niet starten.

Instellingen voor Jumpitems

Gelijktijdige jumps

Voor Jump-client, lokale Jump, externe Jump, VNC op afstand en Shell Jump

Stel deze optie in op **Deelnemen aan bestaande sessie** om meerdere gebruikers toegang tot hetzelfde Jumpitem te verlenen zonder uitnodiging van een andere gebruiker om aan een actieve sessie deel te nemen. De eerste gebruiker die toegang krijgt tot het Jumpitem, blijft eigenaar van de sessie. Gebruikers in een gedeelde Jump-sessie kunnen elkaar zien en met elkaar chatten.

Stel deze optie in op **Jump niet toestaan** om ervoor te zorgen dat maar één gebruiker tegelijk een Jump naar een Jumpitem kan uitvoeren. Alleen een uitnodiging van de gebruiker die de sessie startte kan een tweede gebruiker toestaan een sessie bij te wonen.

Deze instelling geldt voor de volgende typen Jumpitems: Jump-client, lokale Jump, externe Jump, VNC op afstand en Shell Jump.

Voor externe RDP

Stel deze optie in op **Nieuwe sessie starten** om meerdere gebruikers toegang tot hetzelfde Jumpitem te verlenen zonder uitnodiging van een andere gebruiker om aan een actieve sessie deel te nemen. Voor bureaublad op afstand (RDP), hebben meerdere gebruikers toegang tot een Jumpitem, maar elke gebruiker start een eigen sessie.

Stel deze optie in op **Jump niet toestaan** om ervoor te zorgen dat maar één gebruiker tegelijk een Jump naar een Jumpitem kan uitvoeren. Alleen een uitnodiging van de gebruiker die de sessie startte kan een tweede gebruiker toestaan een sessie bij te wonen.

Deze instelling geldt alleen voor Jumpitems van het type bureaublad op afstand (RDP).

Externe hulpprogramma's

Gebruikers toestaan om externe RDP-Jumpsnelkoppelingen met een extern hulpprogramma te openen

Als dit is ingeschakeld, kunt u uw eigen RDP-hulpprogramma gebruiken voor externe RDP-Jumpsnelkoppelingen.

Shell Jumpfiltering

Herkende shell-prompts

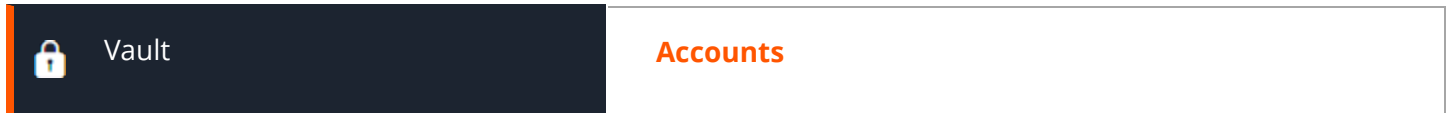
Voer reguliere expressies in, één per regel, waarvoor een overeenkomst wordt gezocht met de opdrachtshell-prompts op uw eindpuntstelsel. Voor een reguliere expressie mag alleen een overeenkomst worden gezocht op de laatste regel van een prompt die uit meerdere regels bestaat.

Validatie van overeenkomende shell-prompts

Voer een bestaande eindpuntshell-prompt in, waarna in de uitvoer wordt aangegeven of deze met een van de reguliere expressies in de lijst overeenkomt. Met deze functionaliteit worden uw reguliere expressies getest zonder een sessie te starten.

Vault voor Privileged Remote Access

Accounts: Vault-accounts beheren



Informatie over alle gedetecteerde en handmatig toegevoegde accounts bekijken en beheren.

Beschikbare informatie voor gedeelde accounts bevat onder meer:

- **Type:** Het type account, specifiek of het een domeinaccount of een lokaal account is, of een algemeen account met een wachtwoord.
- **Name:** De naam van het account.
- **Groep:** De naam van de accountgroep waartoe het account behoort.
- **Eindpunt:** Het eindpunt dat aan het account is gekoppeld.
- **Beschrijving:** Korte beschrijving van het account.
- **Laatst uitgecheckt:** De laatste keer dat het account is uitgecheckt.
- **Wachtwoordleeftijd:** De leeftijd van het wachtwoord.



*Tip: U kunt de weergegeven lijst met gedeelde accounts aanpassen met behulp van de filters voor **Groep** en **Wachtwoordleeftijd**.*

Op basis van deze informatie kunt u diverse acties uitvoeren, waaronder inchecken/uitchecken van inloggegevens en rotatie van inloggegevens.

Beschikbare informatie voor persoonlijke accounts bevat onder meer:

- **Type:** Het type account, specifiek of het een domeinaccount of een lokaal account is, of een algemeen account met een wachtwoord.
- **Name:** De naam van het account.
- **Eigenaar:** De naam van de persoon die het account heeft aangemaakt en de eigenaar ervan is.
- **Beschrijving:** Korte beschrijving van het account.
- **Wachtwoordleeftijd:** De leeftijd van het wachtwoord.



*Tip: U kunt de weergegeven lijst met persoonlijke accounts filteren op **Eigenaar** en **Wachtwoordleeftijd**.*

Accounts

Account toevoegen

Klik op **Toevoegen** om handmatig gedeelde of persoonlijke algemene accounts toe te voegen aan de BeyondTrust-Vault.

Gedeelde accounts zoeken

Zoeken naar een specifieke gedeelde account of een groep accounts op basis van **Naam**, **Eindpuntnaam** en **Beschrijving**.

Inchecken en uitchecken bij een gedeeld account

Klik op **Uitchecken** om inloggegevens van een gedeeld account weer te geven en te gebruiken. Wanneer het is geselecteerd verschijnt de prompt **Accountwachtwoord**, waarin de inloggegevens 60 seconden lang worden getoond zodat u het wachtwoord kunt kopiëren. Wanneer de prompt wordt gesloten, komt de optie **Inchecken** beschikbaar. Klik wanneer u klaar bent met het gebruik van het account op **Inchecken** om het wachtwoord terug in het systeem in te checken.



Zie voor meer informatie [Inloggegevens uitchecken uit de PRA /login-interface](https://www.beyondtrust.com/docs/privileged-remote-access/how-to/vault/check-out.htm) op <https://www.beyondtrust.com/docs/privileged-remote-access/how-to/vault/check-out.htm>.

Ellipsis-menu voor gedeelde accounts

Klik op **Ellipsis (...)** om meer acties te bekijken, zoals **Wachtwoord roteren**, **Bewerken** en **Verwijderen**. Wanneer **Wachtwoord roteren** is geselecteerd, roteert of wijzigt het systeem automatisch het wachtwoord. Als **Bewerken** is geselecteerd, kunt u de informatie van het account aanpassen. Met de optie **Verwijderen** wordt het account verwijderd uit de lijst **Accounts**.



Raadpleeg [Bevoorrechte inloggegevens wisselen met BeyondTrust Vault](https://www.beyondtrust.com/docs/privileged-remote-access/how-to/vault/rotation.htm) op <https://www.beyondtrust.com/docs/privileged-remote-access/how-to/vault/rotation.htm> voor meer informatie.

In persoonlijke accounts zoeken

Zoeken naar een specifiek account of een groep accounts op basis van **Naam** en **Beschrijving**.

Wachtwoord voor persoonlijk account bekijken

Klik op **Wachtwoord bekijken** om inloggegevens weer te geven en te gebruiken. Wanneer het is geselecteerd verschijnt de prompt **Accountwachtwoord**, waarin de inloggegevens 60 seconden lang worden getoond zodat u het wachtwoord kunt kopiëren.

Persoonlijk account bewerken

Klik op **Account bewerken** om de accountgegevens aan te passen, specifiek de **Naam**, **Beschrijving**, **Gebruikersnaam** en het **Wachtwoord**.

Gedeeld algemeen account toevoegen

Met de optie **Toevoegen > Gedeeld algemeen account** kunt u accounts toevoegen zonder een detectietaak uit te moeten voeren. In plaats daarvan kunt u handmatig informatie over het account invoeren. Deze optie is handig in situaties waar een gedeeld account of een combinatie gebruikersnaam/wachtwoord kan worden gebruikt om toegang te krijgen tot veel verschillende systemen.

Naam

Voer een naam in voor het account.

Beschrijving

Voer een korte en makkelijk te onthouden beschrijving van het account in.

Gebruikersnaam

Geef de gebruikersnaam voor het account op.

Verificatie

Selecteer de verificatiemethode voor het account: **Wachtwoord** of **SSH-privésleutel**.



Opmerking: Als u een privé SSH-sleutel gebruikt voor de verificatie, moet u een privésleutel opgeven voor het account in OpenSSH-indeling. Optioneel kunt u de wachtwoordzin die bij de privésleutel hoort bijvoegen.

Wachtwoord en Wachtwoord bevestigen

Wanneer **Wachtwoord** is geselecteerd voor verificatie moet u het wachtwoord voor het account invoeren en het wachtwoord bevestigen.

SSH-privésleutel

Wanneer **SSH-privésleutel** is geselecteerd voor verificatie moet u de SSH-privésleutel voor het account invoeren.

SSH-privésleutel

De informatie voor de SSH-privésleutel opgeven.

SSH-code wachtwoordzin

Voer de wachtwoordzin van de SSH-privésleutel in indien van toepassing.

Simultaan uitchecken toestaan

Selecteer deze optie als het account uitgecheckt en gebruikt kan worden door meerdere gebruikers of sessies tegelijk.

Accountgroep

Selecteer een groep uit de lijst om het gedeelde account toe te voegen aan een accountgroep. Als er geen groep wordt geselecteerd, wordt het account toegevoegd aan de systeemgroep **Geen**.

Accountgebruikers

Nieuwe gebruikersnaam

Gebruikers selecteren die toegang tot dit account hebben.

Nieuwe rol voor leden

Selecteer de Vault-accountrol voor de nieuwe gebruiker en klik vervolgens op **Toevoegen**. Er kan een van de volgende twee rollen aan gebruikers worden toegewezen:

- **Injecteren** (standaardwaarde): Gebruikers met deze rol kunnen dit account gebruiken in Privileged Remote Access-sessies.
- **Injecteren en uitschrijven**: Gebruikers met deze rol kunnen dit account gebruiken in Privileged Remote Access-sessies en het account uitschrijven op /login. De machtiging **Uitschrijven** heeft geen invloed op generieke SSH-accounts.



Opmerking: De **Vault account-rol** is zichtbaar in de lijst met gebruikers die aan het Vault-account zijn toegevoegd.



Opmerking: Als er een BeyondTrust Privileged Remote Access-installatie wordt geüpgraded met de functie Configureerbare Vault uitschrijven zal de **Vault-accountrol** na de upgrade standaard op **Injecteren en uitschrijven** worden ingesteld voor alle bestaande **Vault-accountlidmaatschappen** die voorafgaand aan de upgrade in Groepsbeleidslijnen werden geconfigureerd.



BELANGRIJK!

Voorrang voor Vault-accountrol: Vault-accountrollen kunnen aan zowel gebruikers als groepsbeleidslijnen worden toegewezen. Dit betekent dat dezelfde gebruiker verschillende rollen kan hebben voor één Vault-account. Er kan een rol door de groepsbeleidslijnen van de gebruiker worden toegewezen, terwijl er een andere rol kan worden toegewezen op grond van de expliciete toegang van de gebruiker tot het Vault-account. Het systeem gebruikt in deze gevallen de meest specifieke rol voor die gebruiker. Het systeem zal de rol die op de pagina **Vault-account bewerken** is toegewezen dan prevaleren boven de rol die in het groepsbeleid van de gebruiker is toegewezen. Als de rol op deze manier wordt overschreven, wordt het woord overschreven weergegeven op de pagina **Vault-account bewerken** voor het lidmaatschap van de gebruiker voor het groepsbeleid. Dit gedrag is consistent met de volgorde van voorrang voor Jumpitem-rollen.



Opmerking: Gebruikersaccounts met de machtiging **Toestemming voor het beheer van Vault** hebben impliciet toestemming om toegang te krijgen tot elk Vault-account.

Persoonlijk account toevoegen

Met de optie **Toevoegen > Persoonlijk algemeen account** kunt u accounts toevoegen.

Naam

Voer een naam in voor het account.

Beschrijving

Voer een korte en makkelijk te onthouden beschrijving van het account in.

Gebruikersnaam

Geef de gebruikersnaam voor het account op.

Verificatie

Selecteer de verificatiemethode voor het account: **Wachtwoord** of **SSH-privésleutel**.



Opmerking: Als u een SSH-sleutel selecteert voor de verificatie moet u een privésleutel opgeven voor het account in OpenSSH-indeling. Optioneel kunt u de wachtwoordzin die bij de privésleutel hoort bijvoegen.

Wachtwoord en Wachtwoord bevestigen

Wanneer **Wachtwoord** is geselecteerd voor verificatie moet u het wachtwoord voor het account invoeren en het wachtwoord bevestigen.

SSH-privésleutel

Wanneer **SSH-privésleutel** is geselecteerd voor verificatie moet u de SSH-privésleutel voor het account invoeren.

SSH-privésleutel

De informatie voor de SSH-privésleutel opgeven.

SSH-code wachtwoordzin

Voer de wachtwoordzin van de SSH-privésleutel in indien van toepassing.

Lokaal account bewerken

Naam

De naam die gebruikt wordt voor het account weergeven of bewerken.

Beschrijving

De beschrijving van het account weergeven of bewerken.

Gebruikersnaam

De gebruikersnaam die bij het account hoort weergeven.

Wachtwoord

Voer een nieuw wachtwoord in voor het account, of laat het veld leeg om het bestaande wachtwoord te houden. Bevestig het ingevoerde wachtwoord.

Wachtwoordleeftijd

De leeftijd van het bestaande wachtwoord weergeven.

Inloggegevens automatisch roteren na inchecken

Lokale accounts zo instellen dat ze automatisch wisselen na gebruik.

Simultaan uitchecken toestaan

Selecteer deze optie als het account uitgecheckt en gebruikt kan worden door meerdere gebruikers of sessies tegelijk.

Accountgroep

Selecteer een groep uit de lijst om het gedeelde account toe te voegen aan een accountgroep. Als er geen groep wordt geselecteerd, wordt het account toegevoegd aan de systeemgroep **Geen**.

Naam van eindpunt

Weergeven welk(e) eindpunt(en) bij het account horen.

Hostnaam van eindpunt

De hostnaam van de bijbehorende eindpunten weergeven.

Accountgebruikers

Selecteer gebruikers die toegang tot dit account hebben, samen met hun vault-accountrol en klik vervolgens op **Toevoegen**.



Opmerking: Gebruikersaccounts met de machtiging **Toestemming voor het beheer van Vault** hebben impliciet toestemming om toegang te krijgen tot elk Vault-account.

Domeinaccount bewerken

Naam

De naam die gebruikt wordt voor het account weergeven of bewerken.

Beschrijving

De beschrijving van het account weergeven of bewerken.

Gebruikersnaam

De gebruikersnaam die bij het account hoort weergeven.

Wachtwoord

Voer een nieuw wachtwoord in voor het account, of laat het veld leeg om het bestaande wachtwoord te houden. Bevestig het ingevoerde wachtwoord.

Wachtwoordleeftijd

De leeftijd van het bestaande wachtwoord weergeven.

Inloggegevens automatisch roteren na inchecken

Selecteer deze optie als u wilt dat de inloggegevens automatisch worden geroteerd nadat deze zijn ingecheckt.

Simultaan uitchecken toestaan

Selecteer deze optie als het account uitgecheckt en gebruikt kan worden door meerdere gebruikers of sessies tegelijk.

Distinguished Name

De DN-naam voor het account weergeven.

Accountgroep

Selecteer een groep uit de lijst om het gedeelde account toe te voegen aan een accountgroep. Als er geen groep wordt geselecteerd, wordt het account toegevoegd aan de systeemgroep **Geen**.

Accountgebruikers

Selecteer gebruikers die toegang tot dit account hebben, samen met hun vault-accountrol en klik vervolgens op **Toevoegen**.



Opmerking: *Gebruikersaccounts met de machtiging **Toestemming voor het beheer van Vault** hebben impliciet toestemming om toegang te krijgen tot elk Vault-account.*

Persoonlijk algemeen (wachtwoord) account bewerken

Naam

Voer een naam in voor het account.

Beschrijving

Voer een korte en makkelijk te onthouden beschrijving van het account in.

Gebruikersnaam

Geef de gebruikersnaam voor het account op.

Wachtwoord en Wachtwoord bevestigen

Wanneer **Wachtwoord** is geselecteerd voor verificatie moet u het wachtwoord voor het account invoeren en het wachtwoord bevestigen.

Accountgroepen: accountgroepen toevoegen en beheren

 Vault

Accountgroepen

Gedeelde Vault-accounts kunnen worden toegevoegd aan een accountgroep, zodat Vault-beheerders gebruikers op een efficiëntere manier toegang kunnen verlenen tot meerdere gedeelde Vault-accounts. Accountgroepen kunnen ook worden gebruikt om een groep met gedeelde Vault-accounts te koppelen aan een groepsbeleid.



Opmerking: Een gedeeld Vault-account kan slechts tot één groep tegelijkertijd behoren en persoonlijke Vault-accounts kunnen niet worden toegevoegd aan een accountgroep.

Accountgroepen

Accountgroepen toevoegen, weergeven en beheren.

Accountgroep toevoegen

Klik op **Toevoegen** om een accountgroep toe te voegen, Vault-accounts toe te voegen aan de groep en gebruikers toegang te verlenen tot de groep met gedeelde Vault-accounts.

Accountgroepen zoeken

Zoek naar specifieke accountgroepen op basis van **naam** of **beschrijving**.

Accountgroep toevoegen

Via de optie **Accountgroep toevoegen** kunt u accountgroepen toevoegen om gebruikers in één keer toegang te verlenen tot meerdere Vault-accounts.

Naam

Voer een naam in voor de accountgroep.

Beschrijving

Voer een korte en makkelijk te onthouden beschrijving van de accountgroep in.

Groepsbeleidlijnen

Als de accountgroep is toegevoegd aan een of meerdere groepsbeleidsregels, dan staan die hier vermeld met de bijbehorende de Vault-accountrollen.

Accounts

Bronaccountgroep

Filter de lijst met beschikbare accounts die aan de groep kunnen worden toegevoegd door een groep te kiezen uit de lijst **Bronaccountgroep**.

In geselecteerde accountgroep zoeken

Filter de lijst met beschikbare accounts die aan de groep kunnen worden toegevoegd door te zoeken naar een accountgroep. U kunt zoeken op **naam**, **eindpunt** en **beschrijving**.

Accounts die zich niet in een groep bevinden

Lijst met beschikbare Vault-accounts die aan de accountgroep kunnen worden toegevoegd.

Toevoegen

Selecteer accounts uit de lijst met beschikbare groepen en klik vervolgens op **Toevoegen** om ze toe te voegen aan de lijst **Accounts in deze groep**.

Verwijderen

Selecteer accounts uit de lijst met **Accounts in deze groep** en klik vervolgens op **Verwijderen** om ze te verwijderen uit de accountgroep te verwijderen.

In deze accountgroep zoeken

Filter de lijst met **Accounts in deze groep** door naar een accountgroep te zoeken op basis van **Naam**, **Eindpunt** en **Beschrijving**.

Accounts in deze groep

Lijst met Vault-accounts die in deze accountgroep voorkomen.

Toegestane gebruikers

Nieuwe gebruikersnaam

Gebruikers selecteren die toegang tot dit account hebben.

Rol nieuw lid

Selecteer de Vault-accountrol voor de nieuwe gebruiker en klik vervolgens op **Toevoegen**. Er kan een van de volgende twee rollen aan gebruikers worden toegewezen:

- **Injecteren** (standaardwaarde): Gebruikers met deze rol kunnen dit account gebruiken in Privileged Remote Access-sessies.
- **Injecteren en uitchecken**: Gebruikers met deze rol kunnen dit account gebruiken in Privileged Remote Access-sessies en het account uitchecken op **/login**. De machtiging **Uitchecken** heeft geen invloed op generieke SSH-accounts.



Opmerking: De Vault account-rol is zichtbaar in de lijst met gebruikers die aan het Vault-account zijn toegevoegd.

Eindpunten: Gedetecteerde systemen weergeven en beheren



Vault

Eindpunten

Eindpunten

Informatie weergeven over alle gedetecteerde eindpunten, zoals de naam en de hostnaam van het systeem, samen met informatie over de accounts die bij deze systemen horen.

Naar eindpunten zoeken

Zoeken naar een specifiek eindpunt of een groep eindpunten op basis van **Naam**, **Hostnaam**, **Beschrijving** of **Domeinnaam**.

Accounts

Het aantal accounts weergeven dat gevonden is tijdens de detectie, alsmede de eindpunten waar deze bij horen. Klik op de link **Accounts** om de accounts te bekijken die aan het systeem gekoppeld zijn.

Jumpitems

Bekijk het aantal Jumpitems dat aan elk eindpunt is gekoppeld. Klik op de optie **Jumpitems** om de accounts te bekijken die aan het systeem gekoppeld zijn.

Bewerken

Wijzig de informatie van het eindpunt, met name **Naam**, **Beschrijving** en **Hostnaam**.

Verwijderen

Het eindpunt verwijderen uit de lijst met **Eindpunten**.

Domeinen: Domeinen toevoegen en beheren



Vault

Domeinen

Informatie over uw domeinen toevoegen, weergeven en beheren.

Domeinen

Domein toevoegen

Klik op **Toevoegen** om handmatig een nieuw domein toe te voegen aan de lijst **Domeinen**.

Domeinnaam

De naam van het domein weergeven.

Jumpoint

Het Jumpoint dat gebruikt wordt voor de detectie van accounts en eindpunten op het domein weergeven.

Beheeraccount

Het beheerderaccount dat bij het Jumpoint en het domein hoort weergeven.

Detecteren

Klik op **Detecteren** om het Jumpoint te laten starten met het scannen en detecteren van eindpunten en accounts op het domein.

Bewerken

Klik op **Bewerken** om domeininformatie aan te passen.

Verwijderen

Klik op **Verwijderen** om dit domein te verwijderen uit de lijst met **Domeinen**.

Domein toevoegen

DNS-naam

Voer de **DNS-naam** van het domein in.

Jumpoint

Kies een bestaand Jumpoint dat zich bevindt in de omgeving waar u accounts wilt detecteren.

Beheeraccount

Selecteer het beheerderaccount dat nodig is om een detectietaak voor dit domein te starten. Kies een nieuw account, dat een **Gebruikersnaam**, **Wachtwoord** en **Wachtwoordbevestiging** nodig heeft. Of kies er voor om een bestaand account te gebruiken dat bij een eerdere taak gedetecteerd is of handmatig is toegevoegd in de sectie **Accounts**.

Domein bewerken

DNS-naam

De **DNS-naam** van het account weergeven of bewerken.

Jumpoint

De informatie over het Jumpoint voor het domein weergeven of bewerken.

Beheeraccount

Het beheerderaccount dat nodig is voor het starten van een detectietaak voor dit domein weergeven of bewerken. Kies een nieuw account, dat een **Gebruikersnaam**, **Wachtwoord** en **Wachtwoordbevestiging** nodig heeft. Of kies er voor om een bestaand account te gebruiken dat bij een eerdere taak gedetecteerd is of handmatig is toegevoegd in de sectie **Accounts**.

Detectie: Domeinen, accounts en eindpunten detecteren



Vault

Detecteren

BeyondTrust Vault is een inloggegevensopslag op het apparaat, waarmee detectie van en toegang tot bevoorrechte inloggegevens mogelijk is. U kunt bevoorrechte inloggegevens handmatig toevoegen, of u kunt de ingebouwde detectietool gebruiken om Active Directory en lokale accounts te scannen en in BeyondTrust Vault te importeren.

i Zie voor meer informatie [Technisch Whitepaper BeyondTrust Vault](https://www.beyondtrust.com/docs/privileged-remote-access/how-to/vault/index.htm) op <https://www.beyondtrust.com/docs/privileged-remote-access/how-to/vault/index.htm>.

Domeinaccounts detecteren

Met de Vault-invoegtoepassing voor BeyondTrust kunt u Active Directory-accounts, lokale accounts en eindpunten detecteren. Jumpoints worden gebruikt om eindpunten te scannen en de accounts die bij deze eindpunten horen te detecteren.

i Raadpleeg de [BeyondTrust Privileged Remote Access Jumpoint-handleiding](https://www.beyondtrust.com/docs/privileged-remote-access/how-to/jumpoint/index.htm) op <https://www.beyondtrust.com/docs/privileged-remote-access/how-to/jumpoint/index.htm> voor meer informatie over Jumpoints.

DNS-naam

Voer de DNS-naam in voor uw omgeving.

Jumpoint

Kies een bestaand Jumpoint dat zich bevindt in de omgeving waar u accounts wilt detecteren.

Beheeraccount

Selecteer het beheerderaccount dat nodig is om de detectiestaat te starten. Kies een nieuw account, waarvoor een **Gebruikersnaam**, **Wachtwoord**, en **Wachtwoordbevestiging** ingevoerd moeten worden. Of kies er voor om een bestaand account te gebruiken dat bij een eerdere taak gedetecteerd is of handmatig is toegevoegd in de sectie **Accounts**. Klik, nadat een account is geselecteerd, op **Detecteren** om de detectietaak te starten.

Gebruikersnaam

Voer een geldige gebruikersnaam in die voor detectie moet worden gebruikt (gebruikersnaam@domein).

Wachtwoord

Voer een geldig wachtwoord in om te gebruiken voor detectie.

Wachtwoord bevestigen

Voer het wachtwoord in ter bevestiging.



Opmerking: U kunt opgeven welke delen van een domein een **detectie-/importtaak** moeten uitvoeren. Nadat u de verplichte velden voor een **detectietaak** hebt geselecteerd, kunt u de zoekopdracht verfijnen door op te geven welke organisatie-eenheden als doel fungeren of door LDAP-query's in te voeren.


Detectietaken

Geef detectietaken weer die in uitvoering zijn voor een specifiek domein, of vernieuw de resultaten van detectietaken die gelukt of mislukt zijn.

Resultaten weergeven

Bekijk de resultaten van de detectietaak in de sectie **Detectieresultaten**, waaronder gedetecteerde eindpunten, gedetecteerde plaatselijke accounts en gedetecteerde domeinaccounts die op het domein gevonden zijn. Voor elk gedetecteerd item wordt een **Naam** en een **Beschrijving** gegeven. U kunt selecteren welke eindpunten en accounts u wilt importeren en opslaan in uw BeyondTrust Vault-exemplaar. Schakel het selectievakje in naast elk lijstitem dat u wilt importeren en klik op **Selectie importeren**.

Opties: Wachtwoordrotatie plannen

 Vault	Opties
---	---------------

Automatisch wachtwoordbeheer

Geplande wachtwoordrotatie inschakelen

Vink de optie **Geplande wachtwoordrotatie inschakelen** in om wachtwoorden automatisch te roteren voor Vault-accounts wanneer het wachtwoord een bepaalde tijd in gebruik is.

Maximale wachtwoordleeftijd

Specificeer het maximum aantal dagen dat een wachtwoord kan worden gebruikt voor Vault-accounts voordat het automatisch wordt geroteerd.

Toegangsconsole

Instellingen van toegangsconsole: Standaard instellingen van toegangsconsole beheren



Toegangsconsole

Instellingen van toegangsconsole

Access Console-instellingen beheren

U kunt de standaard instellingen van de access console voor al uw gebruikers instellen en zo een consistente gebruikerservaring voor de access console toepassen en teams efficiënter maken. U kunt instellingen afdwingen, toestaan dat de instellingen door de gebruiker worden overschreven of de instellingen onbeheerd laten. Als u **Onbeheerd** selecteert, dan wordt de standaard BeyondTrust-instelling ernaast weergegeven zodat u kunt afwegen of u het echt wilt.

Bij elke instelling waarvoor u **Inschakelen** of **Uitschakelen** selecteert, wordt een keuzevakje weergegeven waarmee u kunt aangeven of de instelling wordt afgedwongen. Afgedwongen instellingen worden effectief als de gebruiker de volgende keer inlogt. Ze kunnen niet in de console worden geconfigureerd. Een afgedwongen instelling kan alleen worden overschreven als de beheerder in de /login-beheerinterface het vinkje in het keuzevakje **Geforceerd** voor die instelling weghaalt.



Zie [Instellingen en voorkeuren in de toegangsconsole wijzigen](https://www.beyondtrust.com/docs/privileged-remote-access/getting-started/access-console/settings.htm) op <https://www.beyondtrust.com/docs/privileged-remote-access/getting-started/access-console/settings.htm> voor meer informatie over hoe een gebruiker instellingen in de access console naar eigen voorkeur kan configureren.

Kies de instellingen die u als standaard voor uw gebruikers wilt en klik op de knop **Opslaan** bovenaan de pagina.

NB: opgeslagen instellingen worden pas effectief als op de console wordt ingelogd. Zelfs als u de instellingen opslaat en toepast door op de knop **Nu toepassen** onderaan de pagina te klikken, waarover later meer, gebruikt de gebruiker de nieuwe instellingen pas als hij of zij inlogt.

Als u bijvoorbeeld standaard instellingen voor nieuwe gebruikers wilt instellen maar de instellingen voor bestaande gebruikers ongewijzigd wilt laten, dan kunt u uw beheerde instellingen opslaan maar niet toepassen. Op deze manier worden bij iedere nieuwe sessie waarbij op de access console wordt ingelogd, uw nieuwe beheerde standaard instellingen van kracht. Voor bestaande gebruikers worden de afgedwongen instellingen de volgende keer dat zij inloggen van kracht, maar alle andere instellingen blijven ongewijzigd.

Algemene instellingen

Spellingcontrole ingeschakeld

Vanuit de sectie **Algemene instellingen** kunt u kiezen om voor chat de spellingcontrole aan of uit te zetten. Momenteel is spellingcontrole alleen beschikbaar voor Amerikaans Engels.

Instelbaar kantlijnartikel voor sessie

Kies of u wilt dat het pictogram voor het sessiemenu wordt weergegeven, of het kantlijnartikel kan worden losgekoppeld en of de widgets op het kantlijnartikel voor de sessie een andere volgorde en grootte kunnen krijgen.

Waarschuwingen - Chat-waarschuwingen

Hoorbare waarschuwingen - laat een geluid horen als een chatbericht wordt ontvangen

Kies of er een geluid moet worden afgespeeld als de gebruiker een chatbericht ontvangt. Als een gebruiker niet beheerd is of als deze ingeschakeld en niet geforceerd is, dan mag hij of zij een aangepast geluid in WAV-formaat aanwijzen met een maximale grootte van 1 MB.

Visuele waarschuwingen - laat het toepassing-pictogram knipperen als een chatbericht wordt ontvangen

Kies of het pictogram voor de toepassing moet knipperen als de gebruiker een chatbericht ontvangt.

Statusberichten in chat-vensters van team weergeven

Kies of statusberichten in de teamchat worden meegenomen, zoals het in- of uitloggen van gebruikers, of alleen de tussen teamleden verzonden chats.

Popup-meldingen

Teamchat

Kies of een gebruiker een popup-melding moet ontvangen voor in een teamchat ontvangen chatberichten.

Access Sessions

Kies of een gebruiker een popup-melding moet ontvangen voor chatberichten die binnenkomen in een access session.

Waarschuwingen - Wachtrij-waarschuwingen

Hoorbare waarschuwingen - laat een geluid horen als een sessie een wachtrij binnenkomt

Kies of een geluid moet worden afgespeeld als er een sessie in een van de wachtrijen van de gebruiker komt.

Popup-meldingen

Popup-meldingen verschijnen onafhankelijk van de access console en bovenop andere vensters. Als de popup-melding is ingeschakeld en niet afgedwongen is of onbeheerd wordt gelaten, dan kan de gebruiker kiezen hoe hij of zij popup-meldingen wil ontvangen.

Persoonlijke wachtrij - gedeelde sessies

Kies of een gebruiker een popup-melding moet ontvangen voor gedeelde sessies in deze wachtrij.

Teamchat - Gedeelde sessies

Kies of een gebruiker een popup-melding moet ontvangen voor gedeelde sessies in deze wachtrij.

Popup-gedrag - locatie en duur

Stel de standaard locatie en duur in voor popup-meldingen.

Access Sessions

Automatische aanvraag Scherm delen

Kies of u wilt dat in de sessies van uw gebruikers scherm delen actief is bij het begin.

Automatisch loskoppelen

Kies of u sessies als tabbladen in de access console wilt openen of automatisch sessies los wilt koppelen en in nieuwe vensters wilt weergeven.

Standaardkwaliteit

Stel de standaard kwaliteit in voor sessies met scherm delen.

Standaardschaal

Stel de standaard afmetingen in voor sessies met scherm delen.

Automatisch naar volledig scherm wanneer scherm delen begint

Als scherm delen begint, dan kan de gebruiker automatisch naar volledig scherm gaan.

Beperk de zichtbaarheid van het eindpunt automatisch als het scherm wordt gedeeld

Als het scherm wordt gedeeld, kan het externe systeem het scherm, de muis en de toetsenbord invoer automatisch beperken en een privacy scherm weergeven.

Opdrachtshell

Aantal regels beschikbaar in opdrachtgeschiedenis

U kunt het aantal regels instellen dat in de historie van de opdrachtshell wordt opgeslagen. De standaard waarde is 500 regels.

Opslaan

Klik op **Opslaan** om alle profielinstellingen op te slaan die u hebt geconfigureerd. Het bevestigingsbericht **Opslaan instellingenprofiel geslaagd** verschijnt bovenaan de pagina. Alle gebruikers die op de access console inloggen nadat u een nieuw profiel hebt opgeslagen, krijgen de nieuwe instellingen als standaard instellingen.

Access Console-instellingen toepassen

Nu toepassen

Als u de standaard instellingen op al uw gebruikers van toepassing wilt laten zijn, klik dan op **Nu toepassen**. Er verschijnt bovenaan de pagina een bevestigingsbericht **Opslaan instellingenprofiel geslaagd**.

Nadat u de nieuwe instellingen op alle gebruikers van toepassing hebt gemaakt, krijgen de gebruikers een waarschuwing dialoogvenster om te bevestigen dat de nieuwe instellingen van toepassing zijn de eerstvolgende keer dat zij op de access console inloggen nadat u de instellingen van toepassing hebt gemaakt. Dit dialoogvenster waarschuwt hen dat de instellingen zijn gewijzigd en ze krijgen een prompt met de optie het dialoogvenster te bevestigen of hun access console-instellingenvenster te openen om de wijzigingen te bekijken.

Aangepaste koppelingen: URL-snelkoppelingen toevoegen aan de Access Console



Toegangsconsole

Aanpasbare koppelingen

Aanpasbare koppelingen

Maak koppelingen naar sites aan waar gebruikers tijdens sessies toegang toe kunnen hebben. Voorbeelden zijn een koppeling naar een kennisbank met zoekmogelijkheden (zodat gebruikers de mogelijkheid hebben om een oplossing voor een probleem op het eindpuntsysteem op te zoeken) of een CRM-systeem.

Koppelingen die hier worden aangemaakt, worden via de knop **Koppelingen** in de access console beschikbaar gesteld.

Aangepaste koppeling toevoegen, bewerken, verwijderen

Voeg een nieuwe koppeling toe of wijzig of verwijder een bestaande koppeling.

Een aangepaste koppeling toevoegen of bewerken

Naam

Maak een unieke naam aan om deze koppeling te identificeren.

URL

Voeg de URL toe waarnaar deze aangepaste koppeling moet verwijzen. Klik op de koppeling onder het veld **Body** om de macro's weer te geven die kunnen worden gebruikt om de tekst in uw e-mails voor uw doeleinden aan te passen.



Raadpleeg [Overzicht en hulpmiddelen voor toegangssessies](https://www.beyondtrust.com/docs/privileged-remote-access/getting-started/access-console/session-overview.htm) op <https://www.beyondtrust.com/docs/privileged-remote-access/getting-started/access-console/session-overview.htm> voor meer informatie.

Standaard scripts: Scripts aanmaken voor sessies met scherm delen of met opdrachtshell



Toegangsconsole

Standaard scripts

Standaard scripts

Maak aangepaste scripts aan om te gebruiken in sessies met scherm delen en opdrachtshell. Het script wordt in de interface van scherm delen of opdrachtshell weergegeven terwijl het wordt uitgevoerd. Als u een script in de interface voor scherm delen uitvoert, dan wordt het uitgevoerde script op het externe beeldscherm weergegeven.



Raadpleeg [Overzicht en hulpmiddelen voor toegangssessies](https://www.beyondtrust.com/docs/privileged-remote-access/getting-started/access-console/session-overview.htm) op <https://www.beyondtrust.com/docs/privileged-remote-access/getting-started/access-console/session-overview.htm> voor meer informatie.



Raadpleeg [De opdrachtshell op het externe eindpunt openen met behulp van de Access Console](https://www.beyondtrust.com/docs/privileged-remote-access/getting-started/access-console/command-shell.htm) op <https://www.beyondtrust.com/docs/privileged-remote-access/getting-started/access-console/command-shell.htm> voor meer informatie.

Filters voor beschikbaarheid van team en categorieën

Filter de weergave door in de vervolgkeuzelijst een team of categorie te selecteren.

Nieuw standaard script toevoegen, bewerken, verwijderen

Maak een nieuw script aan, wijzig een bestaand script of verwijder een bestaand script.

Standaard script toevoegen of bewerken

Scriptnaam

Maak een unieke naam aan om dit script te identificeren. Deze naam moet de gebruikers helpen het script te vinden dat zij willen uitvoeren.

Beschrijving

Voeg een korte beschrijving toe om het doel van dit script samen te vatten. De beschrijving wordt bij de prompt weergegeven om te bevestigen dat de gebruiker het geselecteerde script wil uitvoeren.

Opdrachtenreeks

Schrijf de serie opdrachten. Scripts moeten in opdrachtregel formaat worden geschreven, net zoals u een batchbestand of shellsript schrijft. Let op dat alleen de laatste regel interactief kan zijn: u kunt niet middenin een script om invoer vragen.

In het script kunt u aan een hulpbronbestand refereren door middel van '%RESOURCE_FILE%'. Let er daarbij op dat u de aanhalingstekens niet vergeet. Let op dat de opdrachtenreeks hoofdlettergevoelig is.

U kunt toegang krijgen tot de tijdelijke map van het hulpbronbestand door %RESOURCE_DIR% te gebruiken. Als u een script uitvoert met een bijbehorend hulpbronbestand, dan wordt dat bestand tijdelijk naar de computer van de klant geüpload.

Beschikbaarheid van team

Selecteer welke teams dit item moeten kunnen gebruiken.

Categorieën

Selecteer de categorie waaronder dit item in de lijst moet worden opgenomen.

Hulpbronbestand

U kunt een hulpbronbestand selecteren dat bij dit script hoort.

Categorieën

Categorie toevoegen, verwijderen

Maak een nieuwe categorie aan of verwijder een bestaande categorie.

Bronnen

Bron kiezen en uploaden

Voeg eventuele hulpbronbestanden toe waar u vanuit uw scripts toegang toe wilt hebben. U mag maximaal 100 MB naar uw map met hulpbronbestanden uploaden.

Verwijderen

Verwijder een bestaand hulpbronbestand.

Speciale acties: Aangepaste speciale acties aanmaken



Toegangsconsole

Speciale acties

Speciale acties

Maak speciale acties om uw processen sneller te laten verlopen. Er kunnen speciale acties worden gemaakt voor Windows-, Mac- en Linux-systemen.

Nieuwe speciale acties toevoegen, bewerken, verwijderen

Maak een nieuwe speciale actie aan, wijzig een bestaande speciale actie of verwijder een bestaande speciale actie.

Speciale actie toevoegen of bewerken

Naam actie

Maak een unieke naam aan om deze actie te identificeren. Een gebruiker kan tijdens een sessie deze naam in de vervolkeuzelijst speciale acties zien.

Opdracht

Voer in het veld **Opdracht** het volledige pad in van de toepassing die u wilt uitvoeren. Gebruik geen aanhalingstekens, deze worden automatisch toegevoegd indien nodig. Windows systemen maken gebruik van de opgegeven macro's. Als de opdracht op het externe systeem niet kan worden gevonden, dan verschijnt deze aangepaste speciale actie niet in de lijst speciale acties voor de gebruiker.

Argumenten

Als de opgegeven opdracht opdrachtregelargumenten accepteert, kunt u deze argumenten vervolgens invoeren. In argumenten mogen, indien nodig, aanhalingstekens worden gebruikt en in argumenten voor Windows-systemen mogen de geleverde macro's worden gebruikt.



Zoek naar 'opdrachtregelparameters' op docs.microsoft.com voor hulp bij Windows-argumenten.

Bevestigen

Als u het selectievakje **Bevestigen** inschakelt, moeten gebruikers bevestigen dat zij deze speciale actie willen uitvoeren voordat de speciale actie daadwerkelijk wordt uitgevoerd. Anders wordt de speciale actie direct uitgevoerd als de speciale actie tijdens een sessie in het menu wordt geselecteerd.

Instellingen speciale acties

Ingebouwde speciale acties weergeven

Schakel **Ingebouwde speciale acties weergeven** in om de standaard door BeyondTrust geboden speciale acties in te schakelen. Als u daarentegen alleen uw eigen speciale acties wilt inschakelen, dan mag u deze optie niet aanvinken.



Opmerking: De speciale actie **Windows beveiliging (Ctrl-Alt-Del)** kan niet worden uitgeschakeld.

Gebruikers en beveiliging

Gebruikers: Accountmachtigingen toevoegen voor een gebruiker of beheerder



Gebruikers en beveiliging

Gebruikers

Gebruikersaccounts

Bekijk informatie over alle gebruikers die toegang tot uw B Series Appliance hebben, inclusief alle lokale gebruikers en de gebruikers die toegang hebben via integratie met een beveiligingsprovider.

Gebruiker toevoegen, bewerken, verwijderen

Maak een nieuwe account aan, wijzig een bestaande account of verwijder een bestaande account. U kunt uw eigen account niet verwijderen.

Naar gebruikers zoeken

Zoek naar een specifiek gebruikersaccount op basis van gebruikersnaam, schermnaam of e-mailadres.

Beveiligingsprovider

Selecteer een type beveiligingsprovider in het vervolgkeuzemenu om de lijst met gebruikers te filteren op beveiligingsprovider.

Synchroniseren

Synchroniseer de gebruikers en groepen die met een externe beveiligingsprovider geassocieerd zijn. De synchronisatie wordt eenmaal per dag automatisch uitgevoerd. Als u op deze knop klikt, wordt de synchronisatie handmatig uitgevoerd.

Mislukte inlogpogingen opnieuw instellen en account deblokken

Als een gebruiker een of meer mislukte aanmeldpoging heeft gedaan, kunt u op de knop **Opnieuw instellen** naast het gebruikersaccount klikken om het aantal terug te zetten op 0.

Als een gebruiker vanwege te veel achtereenvolgende mislukte aanmeldpogingen wordt geblokkeerd, kunt u op de knop **Account deblokken** naast het gebruikersaccount klikken om het aantal terug te zetten op 0 en het account te deblokken.

Gebruiker toevoegen of bewerken

Gebruikersnaam

Unieke identificatie om in te loggen.

Scherмнаam

De naam van de gebruiker zoals deze in teamchats, rapporten e.d. wordt weergegeven.

E-mailadres

Stel het e-mailadres in waarnaar e-mailkennisgevingen moeten worden verzonden, zoals het opnieuw instellen van het wachtwoord of waarschuwingen over uitgebreide beschikbaarheid-modus.

Wachtwoord

Wachtwoord dat in combinatie met de gebruikersnaam wordt gebruikt om aan te melden. U kunt het wachtwoord net zo instellen als u wilt, als de tekenreeks maar voldoet aan het beleid zoals het gedefinieerd is op de pagina **/login > Beheer > Beveiliging**.

Moet wachtwoord opnieuw instellen bij volgende login

Als deze optie geselecteerd is, moet de gebruiker zijn of haar wachtwoord bij de volgende login opnieuw instellen.

Het wachtwoord vervalt nooit

Schakel dit selectievakje in om in te stellen dat het wachtwoord van de gebruiker nooit vervalt.

Verloopdatum wachtwoord

Stel een vervaldatum in voor het wachtwoord.

Lidmaatschappen



Opmerking: *Op het moment dat de nieuwe gebruiker wordt aangemaakt, wordt het gedeelte **Lidmaatschappen** nog niet weergegeven. Zodra de nieuwe gebruiker echter is opgeslagen, verschijnt er een nieuw gedeelte **Lidmaatschappen** met eventuele groepsbeleidslijnen of teams waar de gebruiker wellicht aan toegevoegd is.*

Lidmaatschappen van groepsbeleid

Overzicht van de groepsbeleidslijnen waar deze gebruiker toe behoort.

Teamlidmaatschappen

Overzicht van de teams waar de gebruiker toe behoort.

Jumpoint-lidmaatschappen

Overzicht van de Jumpoints waar de gebruiker toe behoort.

Lidmaatschappen van Jumpgroepen

Overzicht van de Jumpgroepen waar de gebruiker toe behoort.

Accountinstellingen

Verificatie in twee stappen

Bij verificatie in twee stappen (2FA) wordt gebruik gemaakt van een verificator-app waarmee een op tijd gebaseerde, eenmalig code wordt gegenereerd. Met deze code kunt u vervolgens bij de beheerinterface en de toegangsconsole inloggen. Als **Vereist** is geselecteerd, worden gebruikers gevraagd te registreren en de volgende keer dat ze inloggen 2FA te gebruiken. Als **Optioneel** is geselecteerd, krijgen gebruikers de keuze om 2FA te gebruiken, maar zijn ze dat niet verplicht. Klik op **Huidige verificator-app verwijderen** als u wilt dat een gebruiker een bepaalde verificator niet meer gebruikt.



Opmerking: Gebruikers die al inlogcodes ontvangen, worden automatisch geüpgraded naar 2FA, hoewel ze e-mailcodes mogen blijven gebruiken tot ze hun app hebben geregistreerd. Op het moment dat ze 2FA gaan gebruiken, wordt de optie voor e-mailcodes permanent uitgeschakeld.

Account vervalt nooit

Account vervalt nooit als dit is aangevinkt. Er moet een vervaldatum voor het account zijn ingesteld als dit niet is aangevinkt.

Verloopdatum account

Hierdoor vervalt het account na een ingestelde datum.

Account uitgeschakeld

Hiermee kunt u het account uitschakelen, zodat de gebruiker niet kan inloggen. Als een account wordt uitgeschakeld, wordt deze NIET verwijderd.

Opmerkingen

Voeg commentaar toe om aan te geven wat het doel is van dit object.

Algemene machtigingen

Beheer

Beheerdersrechten

Hierdoor krijgt de gebruiker volledige beheerdersrechten.

Mag Vault beheren

Stelt gebruikers in staat om toegang te krijgen tot de Vault.

Instelling voor wachtwoord

Hierdoor kan de gebruiker wachtwoorden instellen en accounts ontgrendelen voor lokale gebruikers die geen beheerder zijn.

Jumpoint bewerken

Hierdoor mogen gebruikers Jumpoints aanmaken of bewerken. Deze optie heeft geen invloed op de mogelijkheid voor de gebruikers om via Jumpoints toegang tot externe computers te krijgen. Dat wordt via beleid op Jumpoint- of groepsniveau geconfigureerd.

Bewerking van team

Hierdoor kunnen gebruikers teams aanmaken of bewerken.

Jumpgroep bewerken

Biedt gebruikers de mogelijkheid jumpgroepen aan te maken of te bewerken.

Standaard script bewerken

Hierdoor kan de gebruiker standaard scripts aanmaken of bewerken die worden gebruikt in sessies met scherm delen of met opdrachtshell.

Bewerking van aangepaste link

Hierdoor kan de gebruiker aangepaste koppelingen aanmaken of bewerken.

Mag rapporten van toegangssessies bekijken

Hierdoor kan de gebruiker rapporten maken over access session-activiteiten, alleen sessies weergeven waarvan hij of zij de primaire sessie-eigenaar is, alleen sessies weergeven voor eindpunten die tot een Jumpgroep behoren waarvan de gebruiker een lid is, of alle sessies weergeven.

Mag Access Session-opnamen bekijken

Hierdoor kan een gebruiker opnames bekijken van sessies met scherm delen en van sessies met opdrachtshell.

Mag Vault-rapporten zien

Stelt de gebruiker in staat om zijn of haar eigen vault- of alle vault-gebeurtenissen te bekijken.

Toegangsmachtigingen

Toegang

Mag eindpunten benaderen

Hierdoor mag de gebruiker de access console gebruiken om sessies uit te voeren. Als toegang tot een eindpunt is ingeschakeld, dan zijn er ook opties beschikbaar die betrekking hebben op toegang tot een eindpunt.

Sessiebeheer

Mag sessies delen met teams waarvan hij/zij geen deel uitmaakt

Hierdoor kan de gebruiker behalve zijn of haar teamleden ook een minder beperkte groep gebruikers uitnodigen om sessies te delen. Samen met de machtiging Uitgebreide beschikbaarheid vormt deze machtiging een uitbreiding van de mogelijkheden om sessies te delen.

i Raadpleeg [Het externe eindpunt beheren met scherm delen](https://www.beyondtrust.com/docs/privileged-remote-access/getting-started/access-console/screen-sharing.htm) op <https://www.beyondtrust.com/docs/privileged-remote-access/getting-started/access-console/screen-sharing.htm> voor meer informatie.

Mag externe gebruikers uitnodigen

Hierdoor kan de gebruiker een gebruiker van een derde partij uitnodigen eenmalig aan een sessie deel te nemen.

i Raadpleeg [Een externe gebruiker uitnodigen om een toegangssessie bij te wonen](https://www.beyondtrust.com/docs/privileged-remote-access/getting-started/access-console/access-invite.htm) op <https://www.beyondtrust.com/docs/privileged-remote-access/getting-started/access-console/access-invite.htm> voor meer informatie.

Toegestaan om uitgebreide beschikbaarheid-modus in te schakelen

Hierdoor kan de gebruiker e-mailuitnodigingen van andere gebruikers ontvangen met het verzoek een sessie te delen, ook als hij of zij niet bij de access console is ingelogd.

i Zie voor meer informatie [Uitgebreide beschikbaarheid gebruiken om beschikbaar te blijven als u niet bent ingelogd](https://www.beyondtrust.com/docs/remote-support/getting-started/rep-console/extended-availability.htm) op <https://www.beyondtrust.com/docs/remote-support/getting-started/rep-console/extended-availability.htm>.

Mag de externe code bewerken

Staat de gebruiker toe om de externe sleutel te wijzigen vanaf het informatievenster van een sessie binnen de access console.

i Raadpleeg [Overzicht en hulpmiddelen voor toegangssessies](https://www.beyondtrust.com/docs/privileged-remote-access/getting-started/access-console/session-overview.htm) op <https://www.beyondtrust.com/docs/privileged-remote-access/getting-started/access-console/session-overview.htm> voor meer informatie.

Scherm delen van gebruiker tot gebruiker

i Raadpleeg [Uw scherm delen met een andere gebruiker](https://www.beyondtrust.com/docs/privileged-remote-access/getting-started/access-console/user-screensharing.htm) op <https://www.beyondtrust.com/docs/privileged-remote-access/getting-started/access-console/user-screensharing.htm> voor meer informatie.

Mag scherm tonen aan andere gebruikers

Hierdoor kan een gebruiker zijn of haar scherm delen met een andere gebruiker zonder dat de ontvanger aan een sessie hoeft aan te melden. Deze optie is zelfs beschikbaar als de gebruiker niet in een sessie is.

Mag besturing geven tijdens tonen van scherm aan andere gebruikers

Hierdoor kan de gebruiker tijdens scherm delen de besturing over muis en toetsenbord aan de gebruiker geven die zijn of haar scherm bekijkt.

Jump-technologie

Toegestane Jumpitem-methodes

Hiermee kan de gebruiker een Jump uitvoeren naar computers via **Jump-clients**, **Lokale Jump op het lokale netwerk**, **Externe Jump via een Jumpoint**, **Externe VNC via een Jumpoint**, **Extern RDP via een Jumpoint**, **Web Jump via een Jumpoint**, **Shell Jump via een Jumpoint** en **Jump via tunnelprotocol via een Jumpoint**.

Jumpitem-rollen

Een Jumpitem-rol is een van te voren gedefinieerde reeks machtigingen voor het beheer en gebruik van Jumpitems. Klik voor elke optie op **Tonen** om de Jumpitem-rol in een nieuw tabblad te openen.

De **Standaard** rol wordt alleen gebruikt als **Standaard van gebruiker toepassen** is ingesteld voor een bepaalde gebruiker in een Jumpgroep.

De **Persoonlijke** rol is alleen van toepassing op Jumpitems die zijn vastgespeld aan de persoonlijke lijst met Jumpitems van de gebruiker.

De **Teams**-rol is van toepassing op Jumpitems die zijn vastgespeld aan de persoonlijke lijst met Jumpitems van een teamlid met een lagere rol. Een teammanager kan bijvoorbeeld de persoonlijke Jumpitems van teamleiders en teamleden bekijken. En een teamleader kan de persoonlijke Jumpitems van teamleden bekijken.

De **Systeem** rol is van toepassing op alle andere Jumpitems in het systeem. Voor de meeste gebruikers moet dit worden ingesteld op **Geen toegang**. Als een andere optie is ingesteld, worden gebruikers toegevoegd aan Jumpgroepen waar ze normaal niet aan zouden worden toegewezen. Ook kunnen zij in de access console de lijst met persoonlijke Jumpitems van niet-leden zien.



Raadpleeg [Jump-itemrollen gebruiken om machtigingssets te configureren voor Jump-items](https://www.beyondtrust.com/docs/privileged-remote-access/how-to/jumpoint/jump-item-roles.htm) op <https://www.beyondtrust.com/docs/privileged-remote-access/how-to/jumpoint/jump-item-roles.htm> voor meer informatie.

Sessietoestemmingen

Stel de prompts en de machtigingsregels in die voor de sessies van deze gebruiker moeten gelden. Kies een bestaand sessiebeleid of definieer aangepaste machtigingen voor deze gebruiker. Als u **Niet gedefinieerd** specificeert, dan wordt het algemene standaard beleid gebruikt. Deze machtigingen kunnen door een beleid met hogere prioriteit worden overschreven.

Beschrijving

Bekijk de omschrijving van een vooraf gedefinieerd beleid voor sessietoestemming.

Scherm delen

Regels voor scherm delen

Stel de gebruiker in staat om het externe scherm weer te geven of te beheren. Als deze optie **Niet gedefinieerd** is, dan wordt deze ingesteld op het beleid met de naastlagere prioriteit. Deze instelling kan worden overschreven door een beleid met hogere prioriteit.

i Raadpleeg [Het externe eindpunt beheren met scherm delen](https://www.beyondtrust.com/docs/privileged-remote-access/getting-started/access-console/screen-sharing.htm) op <https://www.beyondtrust.com/docs/privileged-remote-access/getting-started/access-console/screen-sharing.htm> voor meer informatie.

Klembordsynchronisatierichting

Selecteer hoe uitwisseling van klembordinhoud tussen ondersteuningstechnici en eindgebruikers verloopt. De opties zijn:

- **Niet toegestaan:** De ondersteuningstechnicus mag het klembord niet gebruiken, er worden geen klembordpictogrammen weergegeven in de access console, en knippen en plakken werkt niet.
- **Van ondersteuningstechnicus naar klant toegestaan:** De ondersteuningstechnicus kan klembordinhoud naar de klant versturen, maar kan geen klembordinhoud van de eindgebruiker kopiëren en plakken. Alleen het klembordpictogram **Verzenden** wordt weergegeven in de access console.
- **In beide richtingen toegestaan:** Klembordinhoud kan in beide richtingen worden verzonden. De klembordpictogrammen **Verzenden** en **Ontvangen** worden weergegeven in de access console.

i Ga voor meer informatie over de Klembordsynchronisatiemodus naar "[Beveiliging: Beveiligingsinstellingen beheren](#)" op pagina 133.

Beperkingen voor het delen van een toepassing

Hierdoor wordt de toegang tot bepaalde toepassingen op het externe systeem beperkt met ofwel **Alleen de uitvoerbare bestanden uit een lijst toestaan** ofwel **Alleen de uitvoerbare bestanden uit een lijst weigeren**. U kunt ook kiezen of u toegang tot het bureaublad wilt toestaan of weigeren.



Opmerking: Deze functie is alleen van toepassing op Windows-besturingssystemen.

Nieuwe uitvoerbare bestanden toevoegen

Als beperkingen op toepassingen delen worden afgedwongen, dan verschijnt een knop **Nieuwe uitvoerbare bestanden toevoegen**. Als u op deze knop klikt, dan verschijnt een dialoog waarin u uitvoerbare bestanden kunt specificeren die moeten worden geweigerd of toegestaan, in overeenstemming met uw bedoelingen.

Nadat u uitvoerbare bestanden hebt toegevoegd, worden de bestandsnamen die u als beperking hebt geselecteerd in één of twee tabellen weergegeven. U kunt beheerdersopmerkingen in een bewerkbaar veld invoeren.

Voer bestandsnamen of SHA-256 hashes in, één per regel

Als u aan uitvoerbare bestanden beperkingen stelt, dan kunt u handmatig de namen of hashes van de uitvoerbare bestanden invoeren die u wilt toestaan of weigeren. Klik op **Uitvoerbare bestanden toevoegen** als u klaar bent met het toevoegen van de gekozen bestanden aan uw configuratie.

U mag per dialoog maximaal 25 bestanden invoeren. Als u er meer moet toevoegen, moet u op **Uitvoerbare bestanden toevoegen** klikken en vervolgens de dialoog opnieuw openen.

Naar een of meer bestanden bladeren

Bij het beperken van uitvoerbare bestanden kunt u deze optie selecteren om op uw systeem te bladeren en uitvoerbare bestanden te selecteren om de namen en hashes ervan automatisch af te leiden. Als u op deze wijze bestanden op uw lokale platform en systeem selecteert, wees dan voorzichtig en let erop dat de bestanden inderdaad uitvoerbare bestanden zijn. Er wordt geen verificatie op browserniveau uitgevoerd.

Kies **Bestandsnaam gebruiken** of **Bestandshash gebruiken** om ervoor te zorgen dat de browser de namen of hashes van de uitvoerbare bestanden automatisch kan afleiden. Klik op **Uitvoerbare bestanden toevoegen** als u klaar bent en de gekozen bestanden aan uw configuratie wilt toevoegen.

U mag per dialoog maximaal 25 bestanden invoeren. Als u er meer moet toevoegen, moet u op **Uitvoerbare bestanden toevoegen** klikken en vervolgens de dialoog opnieuw openen.



Opmerking: Deze optie is alleen beschikbaar in moderne browsers, niet in oudere browsers.

Toegestane eindpuntbeperkingen

Stel in of de gebruiker invoer van de muis en het toetsenbord van het externe systeem kan opschorten. De gebruiker kan er ook voor zorgen dat het bureaublad op afstand niet wordt weergegeven.



Raadpleeg [Het externe eindpunt beheren met scherm delen](https://www.beyondtrust.com/docs/privileged-remote-access/getting-started/access-console/screen-sharing.htm) op <https://www.beyondtrust.com/docs/privileged-remote-access/getting-started/access-console/screen-sharing.htm> voor meer informatie.

Annotaties

Regels voor annotaties

Hierdoor kan de gebruiker hulpmiddelen voor annotaties gebruiken om op het externe scherm te tekenen. Als deze optie **Niet gedefinieerd** is, dan wordt deze ingesteld op het beleid met de naastlagere prioriteit. Deze instelling kan worden overschreven door een beleid met hogere prioriteit.



Zie voor meer informatie [Annotaties gebruiken om op het externe scherm van het eindpunt te tekenen](https://www.beyondtrust.com/docs/privileged-remote-access/getting-started/access-console/annotations.htm) op <https://www.beyondtrust.com/docs/privileged-remote-access/getting-started/access-console/annotations.htm>.

Bestandsoverdracht

Regels voor bestandsoverdracht

Hierdoor kan de gebruiker bestanden naar het externe systeem uploaden, van het externe systeem downloaden, of beide. Als deze optie **Niet gedefinieerd** is, dan wordt deze ingesteld op het beleid met de naastlagere prioriteit. Deze instelling kan worden overschreven door een beleid met hogere prioriteit.

Toegankelijke paden op het bestandssysteem van het eindpunt

Sta toe dat de gebruiker bestanden overdraagt naar of van alle mappen op het externe systeem of alleen naar of van gespecificeerde mappen.

Toegankelijke paden op het bestandssysteem van de gebruiker

Sta toe dat de gebruiker bestanden overdraagt naar of van alle mappen op zijn of haar lokale systeem of alleen naar of van gespecificeerde mappen.



Zie voor meer informatie [Bestandsoverdracht naar en van het externe eindpunt](https://www.beyondtrust.com/docs/privileged-remote-access/getting-started/access-console/file-transfer.htm) op <https://www.beyondtrust.com/docs/privileged-remote-access/getting-started/access-console/file-transfer.htm>.

Opdrachtshell

Regels voor opdrachtshell

Hiermee kan de gebruiker via een virtuele interface opdrachten op de opdrachtregel van de externe computer geven. Als deze optie **Niet gedefinieerd** is, dan wordt deze ingesteld op het beleid met de naastlagere prioriteit. Deze instelling kan worden overschreven door een beleid met hogere prioriteit.



Opmerking: Toegang tot de opdrachtshell kan niet worden beperkt voor Shell Jump-sessies.

Opdrachtfiltering configureren om het per ongeluk gebruiken van opdrachten die schadelijk kunnen zijn voor de eindpuntssystemen te voorkomen.



Raadpleeg [Shell-jump gebruiken om toegang tot een apparaat in een extern netwerk te krijgen](https://www.beyondtrust.com/docs/privileged-remote-access/getting-started/access-console/shell-jump.htm) op www.beyondtrust.com/docs/privileged-remote-access/getting-started/access-console/shell-jump.htm voor meer informatie over het filteren van opdrachten.



Zie voor meer informatie [De opdrachtshell op het externe eindpunt openen met behulp van de toegangsconsole](https://www.beyondtrust.com/docs/privileged-remote-access/getting-started/access-console/command-shell.htm) op <https://www.beyondtrust.com/docs/privileged-remote-access/getting-started/access-console/command-shell.htm>.

Systeeminformatie

Regels voor systeeminformatie

Hiermee kan de gebruiker systeeminformatie over de externe computer weergeven. Als deze optie **Niet gedefinieerd** is, dan wordt deze ingesteld op het beleid met de naastlagere prioriteit. Deze instelling kan worden overschreven door een beleid met hogere prioriteit.

Mag systeeminformatie-acties gebruiken

Hierdoor kan de gebruiker met processen en programma's op de externe computer communiceren zonder de noodzaak van scherm delen. Stop processen, start, stop, pauzeer, hervat services en start ze opnieuw; en maak de installatie van programma's ongedaan.

i Raadpleeg [Systeeminformatie bekijken op het externe eindpunt op https://www.beyondtrust.com/docs/privileged-remote-access/getting-started/access-console/system-info.htm](https://www.beyondtrust.com/docs/privileged-remote-access/getting-started/access-console/system-info.htm) voor meer informatie.

Register-toegang

Regels voor registertoegang

Hierdoor kan de gebruiker het register op een extern Windows-systeem benaderen zonder de noodzaak tot scherm delen. Bekijk sleutels, voeg ze toe en bewerk ze, zoek en importeer/exporteer sleutels.

i Zie voor meer informatie [Toegang tot de register-editor op het externe eindpunt op https://www.beyondtrust.com/docs/privileged-remote-access/getting-started/access-console/registry-editor.htm](https://www.beyondtrust.com/docs/privileged-remote-access/getting-started/access-console/registry-editor.htm).

Standaard scripts

Regels voor standaard scripts

Hierdoor kan de gebruiker standaardscripts uitvoeren die voor zijn of haar teams zijn aangemaakt. Als deze optie **Niet gedefinieerd** is, dan wordt deze ingesteld op het beleid met de naastlagere prioriteit. Deze instelling kan worden overschreven door een beleid met hogere prioriteit.

i Raadpleeg [De opdrachtshell op het externe eindpunt openen met behulp van de Access Console op https://www.beyondtrust.com/docs/privileged-remote-access/getting-started/access-console/command-shell.htm](https://www.beyondtrust.com/docs/privileged-remote-access/getting-started/access-console/command-shell.htm) voor meer informatie.

Beschikbaarheidsinstellingen

Inlogschema

Beperk inloggen van gebruiker aan de hand van het volgende rooster

Stel een schema in om te bepalen wanneer gebruikers kunnen inloggen bij de access console. Stel de tijdzone in die u voor dit rooster wilt gebruiken en voeg vervolgens een of meer roostervermeldingen toe. Stel voor elke vermelding de startdatum en -tijd en de einddatum en -tijd in.

Als bijvoorbeeld de begintijd is ingesteld op 08:00 uur en de eindtijd op 17:00 uur, dan kan een gebruiker op elk tijdstip in deze periode inloggen en kan blijven doorwerken tot na de eindtijd. De gebruiker kan echter na 17:00 uur niet opnieuw inloggen.

Forceer uitloggen als het schema inloggen niet toestaat

Als strengere toegangscontrole is vereist, dan moet u deze optie aanvinken. Hierdoor wordt de gebruiker geforceerd op de geplande eindtijd uit te loggen. In dit geval ontvangt de gebruiker herhaalde berichten vanaf 15 minuten voordat de sessie wordt beëindigd.

Wanneer de gebruiker uitgelogd wordt, volgen eventuele eigen sessies de sessieterugval-regels.

Rapport gebruikersaccount

Exporteer gedetailleerde informatie over uw gebruikers voor controledoeleinden. Verzamel gedetailleerde informatie over alle gebruikers, gebruikers van een bepaalde beveiligingsprovider of alleen lokale gebruikers. De verzamelde informatie bevat gegevens die onder de knop 'Gegevens weergeven' worden weergegeven, alsook groepsbeleid, teamlidmaatschappen en machtigingen.

Gebruikersaccounts om wachtwoorden opnieuw in te stellen: Gebruikers toestaan om wachtwoorden te beheren



Gebruikers en beveiliging

Gebruikers

Gebruikersaccounts

Beheerders kunnen via gebruikersmachtigingen de taak voor het opnieuw instellen van wachtwoorden van lokale gebruikers en vergrendelde gebruikersaccounts aan bevoorrechte gebruikers delegeren, zonder volledige beheerdersrechten toe te kennen. Gebruikers kunnen nog steeds hun eigen wachtwoord resetten.



Opmerking: *Beheerders met de machtiging **Mag wachtwoorden instellen** zien geen verschil in de gebruikersinterface.*

Als een bevoorrechte gebruiker zonder beheersrechten naar de pagina **Gebruikers en beveiliging > Gebruikers** in de //login-interface gaat, ziet hij of zij een beperkte weergave van het scherm **Gebruikers** met **Wachtwoord wijzigen**-knoppen voor niet-administratieve gebruikers. De bevoorrechte gebruiker kan geen gebruikersaccounts bewerken of verwijderen. Bevoorrechte gebruikers mogen geen wachtwoorden van beheerders of van gebruikers van beveiligingsproviders resetten.

Naar gebruikers zoeken

Zoek naar een specifiek gebruikersaccount op basis van gebruikersnaam, schermnaam of e-mailadres.

Mislukte inlogpogingen opnieuw instellen en account deblokkeren

Als een gebruiker een of meer mislukte aanmeldpoging heeft gedaan, kunt u op de knop **Opnieuw instellen** naast het gebruikersaccount klikken om het aantal terug te zetten op 0.

Als een gebruiker vanwege te veel achtereenvolgende mislukte aanmeldpogingen wordt geblokkeerd, kunt u op de knop **Account deblokkeren** naast het gebruikersaccount klikken om het aantal terug te zetten op 0 en het account te deblokkeren.

Wachtwoord veranderen

Wijzig het wachtwoord van een gebruiker die geen beheerder is.

Wachtwoord veranderen

Gebruikersnaam

Unieke identificatie om in te loggen. Dit veld kan niet worden bewerkt.

Schermnamen

De naam van de gebruiker zoals deze in teamchats, rapporten e.d. wordt weergegeven. Dit veld kan niet worden bewerkt.

E-mailadres

Het e-mailadres waar e-mails met meldingen naartoe worden verzonden, zoals voor het opnieuw instellen van wachtwoorden of waarschuwingen voor de uitgebreide beschikbaarheid-modus. Dit veld kan niet worden bewerkt.

Opmerkingen

Opmerkingen over het account. Dit veld kan niet worden bewerkt.

Wachtwoord

Het nieuwe wachtwoord dat aan dit gebruikersaccount wordt toegekend. U kunt het wachtwoord net zo instellen als u wilt, als de tekenreeks maar voldoet aan het beleid zoals het gedefinieerd is op de pagina **/login > Beheer > Beveiliging**.

E-mail voor het opnieuw instellen van het wachtwoord naar gebruiker verzenden

Stuur e-mailbericht naar de gebruiker met een koppeling om het wachtwoord van het account opnieuw in te stellen. Voor deze functie is een geldige **SMTP**-configuratie voor uw B Series Appliance vereist. U kunt deze instellen op de pagina **/login > Beheer > E-mailconfiguratie**.

Moet wachtwoord opnieuw instellen bij volgende login

Als deze optie geselecteerd is, moet de gebruiker zijn of haar wachtwoord bij de volgende login opnieuw instellen.

Toegangsuitnodiging: Profielen aanmaken om externe gebruikers in sessies uit te nodigen



Gebruikers en beveiliging

Toegangsuitnodiging

E-mailuitnodiging openen

Een bevoorrechte gebruiker kan met een toegangsuitnodiging een externe gebruiker uitnodigen om eenmalig een sessie bij te wonen. Als de gebruiker de uitnodiging maakt, dan moet hij of zij een beveiligingsprofiel selecteren om te bepalen welk niveau privileges de externe gebruiker moet krijgen. Beveiligingsprofielen voor toegangsuitnodigingen worden op de pagina **Gebruikers en beveiliging > Sessiebeleidslijnen** als sessiebeleidslijnen geconfigureerd en moeten worden ingeschakeld voor gebruik in toegangsuitnodigingen.

De e-mailuitnodiging wordt naar externe gebruikers verzonden als u hen uitnodigt een sessie bij te wonen.

Onderwerp

Pas het onderwerp van deze e-mail aan. Klik op de koppeling onder het veld **Body** om de macro's weer te geven die kunnen worden gebruikt om de tekst in uw e-mails voor uw doeleinden aan te passen.

Bericht

Pas de inhoud van deze e-mail aan. Klik op de koppeling onder het veld **Body** om de macro's weer te geven die kunnen worden gebruikt om de tekst in uw e-mails voor uw doeleinden aan te passen.

i Raadpleeg [Een externe gebruiker uitnodigen om een toegangssessie bij te wonen](https://www.beyondtrust.com/docs/privileged-remote-access/getting-started/access-console/access-invite.htm) op <https://www.beyondtrust.com/docs/privileged-remote-access/getting-started/access-console/access-invite.htm> voor meer informatie.

Beveiligingsproviders: Inloggen via LDAP, Active Directory, RADIUS en Kerberos activeren



Gebruikers en beveiliging

Beveiligingsproviders

Beveiligingsproviders

U kunt uw BeyondTrust Appliance B Series configureren om gebruikers tegen bestaande LDAP-, RADIUS- of Kerberos-servers te verifiëren en om machtigingen toe te kennen op basis van eerdere instellingen voor hiërarchie en groepen die al in uw servers zijn gespecificeerd. Kerberos ondersteunt eenmalige aanmelding, terwijl RSA en andere tweestapsverificatiemechanismes via RADIUS een extra beveiligingsniveau bieden.

Provider toevoegen

Selecteer in het vervolgkeuzemenu **Toevoegen** LDAP, RADIUS, Kerberos, SAML of SCIM om een nieuwe configuratie voor een beveiligingsprovider toe te voegen.

Volgorde veranderen

Klik op deze knop om beveiligingsproviders te slepen en neer te zetten om de prioriteiten ervan in te stellen. U kunt servers binnen een cluster slepen en neerzetten en clusters kunnen als geheel worden gesleept en neergezet. Klik op **Volgorde opslaan** om de wijzigingen in de prioriteiten te effectueren.

Uitschakelen

Schakel de verbinding met deze beveiligingsprovider uit. Dit is nuttig voor gepland onderhoud, als u wilt dat een server offline is maar niet verwijderd is.

Synchronisatie

Synchroniseer de gebruikers en groepen die met een externe beveiligingsprovider geassocieerd zijn. De synchronisatie wordt eenmaal per dag automatisch uitgevoerd. Als u op deze knop klikt, wordt de synchronisatie handmatig uitgevoerd.

Logboek bekijken

Bekijk de statushistorie voor een verbinding met een beveiligingsprovider.

Node dupliceren

Maak een kopie van een bestaande configuratie van een geclusterde beveiligingsprovider aan. Deze wordt als nieuwe node aan dezelfde cluster toegevoegd.

Tot cluster upgraden

Upgrade een beveiligingsprovider tot een geclusterde beveiligingsprovider. Kopieer een bestaande node om meer beveiligingsproviders aan deze cluster toe te voegen.

Kopiëren

Maak een kopie van een bestaande configuratie van een beveiligingsprovider aan. Deze wordt als een beveiligingsprovider op het hoogste niveau toegevoegd en niet als onderdeel van een cluster.

Bewerken, verwijderen

Wijzig een bestaand object of verwijder een bestaand object.



Opmerking: Als u de lokale beveiligingsprovider bewerkt en een standaard beleid selecteert dat geen beheerdersmachtigingen heeft, verschijnt er een waarschuwing. Zorg ervoor dat andere gebruikers beheerdersmachtigingen hebben voordat u verder gaat.

Beveiligingsprovider bewerken - LDAP

Algemene instellingen

Naam

Maak een unieke naam aan om deze provider te identificeren.

Ingeschakeld

Als deze optie is ingeschakeld, kan uw B Series Appliance naar deze beveiligingsprovider zoeken als een gebruiker zich probeert aan te melden. Als het niet is aangevinkt, wordt niet naar de provider gezocht.

Verificatie gebruiker

Kiezen of deze provider gebruikt moet worden voor gebruikersverificatie. Wanneer dit is gedeselecteerd, zijn opties specifiek voor gebruikersverificatie uitgeschakeld.

Gebruikersprovisioning

Standaard vindt gebruikersprovisioning plaats op deze provider. Als u een SCIM-provider heeft ingesteld, kunt u kiezen om gebruikers te provisioneren via die provider. Als deze provider niet wordt gebruikt voor gebruikersverificatie, is **Gebruikers niet provisioneren** geselecteerd.



Opmerking: Deze instelling kan niet worden aangepast nadat deze beveiligingsprovider de eerste keer wordt opgeslagen.

De gebruikersinformatie met de LDAP-server gesynchroniseerd houden

Met het aanvinken van deze optie blijft de schermnaam van een gebruiker ingesteld op de naam die is toegewezen op de beveiligingsprovider in plaats van toe te staan dat de schermnaam in BeyondTrust kan worden aangepast.

Autorisatie-instellingen

Synchronisatie: LDAP-objectcache inschakelen

Als deze optie is aangevinkt, dan worden LDAP-objecten die voor het B Series Appliance zichtbaar zijn, elke nacht of, indien gewenst handmatig, in de cache opgeslagen en gesynchroniseerd. Bij gebruik van deze optie worden er minder verbindingen met de LDAP-server voor beheerdoeleinden gemaakt zodat potentieel de snelheid en efficiency omhoog gaan.

Als deze optie niet is aangevinkt, dan komen wijzigingen op de LDAP-server direct beschikbaar zonder de noodzaak tot synchronisatie. Maar als u via de beheerinterface wijzigingen maakt in gebruikersbeleidslijnen, dan worden, voor zover noodzakelijk, enkele kortstondige verbindingen met de LDAP-server gemaakt.

Bij providers die voorheen de synchronisatie in hadden geschakeld en de synchronisatie uitschakelen door het vinkje bij de synchronisatie-optie weg te halen, worden alle gecachte records verwijderd die op dat moment niet in gebruik zijn.

Groep opzoeken

U kunt ervoor kiezen deze beveiligingsprovider alleen voor gebruikersverificatie te gebruiken, alleen voor het opzoeken van groepen of voor beide doeleinden. Als de optie **Gebruikersverificatie** hierboven niet is aangevinkt is **Groepen opzoeken met deze provider** geselecteerd. De optie om groepen op te zoeken met gebruik van een andere provider is alleen beschikbaar wanneer een andere provider die groepen kan opzoeken al is aangemaakt.

Standaard groepsbeleid *(Alleen zichtbaar als gebruikersverificatie is toegestaan)*

Elke gebruiker die tegen een externe server wordt geverifieerd, moet lid van ten minste één groepsbeleid zijn om op uw B Series Appliance te kunnen worden geverifieerd en in te kunnen loggen op ofwel de /login-interface ofwel de access console. U kunt een standaard groepsbeleid selecteren om op alle gebruikers toe te passen die toestemming hebben om tegen de geconfigureerde server te worden geverifieerd.

Bedenk dat als er een standaard beleid is gedefinieerd, dat dan elke toegestane gebruiker die tegen deze server wordt geverifieerd, potentieel toegang heeft op het niveau van dit standaard beleid. Daarom wordt aanbevolen dat u een beleid met minimale machtigingen als standaard instelt om te voorkomen dat gebruikers machtigingen krijgen die u niet wilt.



Opmerking: Als voor een gebruiker een standaard groepsbeleid geldt en vervolgens speciaal aan een ander groepsbeleid wordt toegevoegd, dan hebben de instellingen voor het speciale beleid altijd voorrang boven de instellingen voor het standaard beleid, zelfs als het speciale beleid een lagere prioriteit heeft dan het standaard beleid en zelfs als de instellingen van het standaard beleid zijn ingesteld op overschrijven.

Instellingen voor verbinding

Hostnaam

Voer de hostnaam in van de server waar uw externe adreslijstarchief staat.



Opmerking: Als u **LDAPS** of **LDAP met TLS** gebruikt, dan moet de hostnaam overeenkomen met de in het publieke SSL-certificaat van uw LDAP-server gebruikte onderwerpnaam of met de DNS-component van de alternatieve onderwerpnaam.

Poort

Specificeer de poort voor uw LDAP-server. Dit is meestal poort **389** voor LDAP of poort **636** voor LDAPS. BeyondTrust ondersteunt ook een globale catalogus via poort **3268** voor LDAP of **3269** voor LDAPS.

Versleuteling

Selecteer het type versleuteling dat moet worden gebruikt voor communicatie met de LDAP-server. Om beveiligingsredenen wordt **LDAPS** of **LDAP met TLS** aanbevolen.



Opmerking: Standaard LDAP verzendt en ontvangt gegevens ongecodeerd van de LDAP-server en stelt zo mogelijk vertrouwelijke informatie over de gebruikersaccount aan packet sniffing bloot. Zowel LDAPS als LDAP met TLS versleutelen de verzonden gegevens waardoor deze methodes aanbevolen worden boven standaard LDAP. LDAP met TLS gebruikt de functie StartTLS om een verbinding met LDAP ongecodeerd op te zetten maar waardeert deze verbinding vervolgens op tot een versleutelde verbinding. LDAPS zet de verbinding over een versleutelde verbinding op zonder enige tekst ongecodeerd te verzenden.

Als u **LDAPS** of **LDAP met TLS** selecteert, dan moet u het door uw LDAP-server gebruikte SSL-basiscertificaat uploaden. Dit is nodig om de geldigheid van de server en de beveiliging van de gegevens zeker te stellen. Het basiscertificaat moet de PEM-opmaak hebben.



Opmerking: Als de onderwerpnaam van het openbare SSL-certificaat van de LDAP-server of de DNS-component van de alternatieve onderwerpnaam niet met de waarde in het veld **Hostnaam** overeenkomt, dan wordt de provider als onbereikbaar behandeld. U kunt echter een wildcardcertificaat opgeven om meerdere subdomeinen op dezelfde site te certificeren. Zo certificeert bijvoorbeeld een certificaat voor ***.voorbeeld.nl** zowel **toegang.voorbeeld.nl** als **extern.voorbeeld.nl**.

Verificatiegegevens binden

Specificeer een gebruikersnaam en wachtwoord waarmee uw B Series Appliance kan binden met en kan zoeken in het LDAP-adreslijstarchief.

Als uw server anonieme binding ondersteunt, dan kunt u ervoor kiezen om een binding te maken zonder een gebruikersnaam en wachtwoord te specificeren. Anonieme binding wordt geacht onveilig te zijn en is op de meeste LDAP-servers standaard uitgeschakeld.

Verbindingsmethode

Als u een extern adreslijstarchief gebruikt in hetzelfde lokale netwerk als uw B Series Appliance, dan kunnen de twee systemen direct met elkaar communiceren. In dat geval hoeft u de optie **Proxy van apparaat via de verbindingagent** niet aan te vinken en kunt u verder gaan.

Als de twee systemen niet direct met elkaar kunnen communiceren, bijvoorbeeld als uw externe adreslijstserver achter een firewall staat, dan moet u een verbindingagent gebruiken. Als u de Win32-verbindingagent downloadt, dan kunnen uw adreslijstserver en uw B Series Appliance met elkaar communiceren via een uitgaande met SSL versleutelde verbinding zonder firewallconfiguratie. De verbindingagent kan ofwel direct naar de adreslijstserver worden gedownload, ofwel naar een aparte server op hetzelfde netwerk als uw adreslijstserver (aanbevolen).

In het bovenstaande geval moet u **Proxy van apparaat via de verbindingagent** aanvinken. Maak een **Wachtwoord verbindingagent** aan om tijdens de installatie van de verbindingagent te gebruiken. Klik vervolgens op **Verbindingagent downloaden**, voer het installatieprogramma uit en volg de instructies van de installatiewizard op. Tijdens installatie wordt u gevraagd om de naam van de beveiligingsprovider in te voeren evenals het hier hierboven aangemaakte wachtwoord voor de verbindingagent.



Opmerking: *BeyondTrust Cloud-klanten moeten de verbindingagent uitvoeren om een extern adreslijstarchief te gebruiken.*

Gebruikersnaam

Voer een gebruikersnaam in voor verificatiegegevens binden.

Wachtwoord en Wachtwoord bevestigen

Voer een wachtwoord voor verificatiegegevens binden in en bevestigen dit.

Type adressenlijst

Om u te helpen de netwerkverbinding tussen uw B Series Appliance en uw beveiligingsprovider te configureren, kunt u een type map als sjabloon selecteren. Zo worden onderstaande te configureren velden vooraf met standaard gegevens ingevuld, maar die gegevens moeten worden gewijzigd om ze in overeenstemming te brengen met de specifieke configuratie van uw beveiligingsprovider. Active Directory LDAP is het meest gebruikte type server, maar u kunt BeyondTrust zo configureren dat met de meeste typen beveiligingsproviders kan worden gecommuniceerd.

Instellingen voor cluster *(Alleen zichtbaar voor clusters)*

Selectie-algoritme voor leden

Selecteer de methode waarmee in deze cluster naar nodes wordt gezocht.

Bij **Van boven naar beneden** wordt eerst op de server met de hoogste prioriteit gezocht. Als die server niet beschikbaar is of als de account niet is gevonden, dan wordt op de server met de daarop volgende prioriteit gezocht. Vervolgens wordt in volgorde van aflopende prioriteit op de servers uit de lijst geclusterde servers gezocht tot de account is gevonden of blijkt dat de account niet op een van de gespecificeerde en beschikbare servers bestaat.

Round-robin is bedoeld om de belasting van de verschillende servers in balans te houden. Bij dit algoritme wordt de eerste server waarop wordt gezocht willekeurig gekozen. Als die server niet beschikbaar is of als de account niet is gevonden, dan wordt op een willekeurige andere server gezocht. Vervolgens wordt in willekeurige volgorde op de overige servers uit de lijst geclusterde servers gezocht tot de account is gevonden of blijkt dat de account niet op een van de gespecificeerde en beschikbare servers bestaat.

Wachttijd voor opnieuw proberen

Stel in hoe lang moet worden gewacht nadat een lid van een cluster niet beschikbaar is geworden voordat een nieuwe poging wordt gedaan voor dat lid van die cluster.

Instellingen gebruikersschema

Clusterwaarden overschrijven *(Alleen zichtbaar voor clusternodes)*

Als deze optie niet is aangevinkt, dan worden voor deze clusternode dezelfde schema-instellingen gebruikt als voor de cluster. Als deze optie niet is aangevinkt, dan kunt u hieronder de schema-instellingen wijzigingen.

Basis DN opzoeken

Bepaal het niveau in uw mappenhiërarchie, gespecificeerd door een onderscheiden naam, waar het B Series Appliance moet beginnen naar gebruikers te zoeken. Afhankelijk van de grootte van uw adreslijstarchief en de gebruikers die BeyondTrust-accounts nodig hebben, kunt u de prestaties verbeteren door de specifieke organisatorische eenheid in uw adreslijstarchief aan te wijzen waar toegang toe nodig is. Als u niet zeker weet of gebruikers binnen meerdere organisatorische eenheden actief zijn, kunt u mogelijk het beste de DN-naam (Distinguished Name) van uw adreslijstarchief op het hoogste niveau gebruiken.

Gebruikersquery

Specificeer de query-informatie die het B Series Appliance moet gebruiken bij het vinden van een LDAP-gebruiker wanneer de gebruiker probeert in te loggen. In het veld **Gebruikersquery** kunt u een standaard LDAP-query invoeren (RFC 2254: Representatie van de tekenreeks voor LDAP-zoekfilters). U kunt de voor de query te gebruiken tekenreeks aanpassen aan de manier waarop uw gebruikers inloggen en aan de methode waarop gebruikersnamen worden geaccepteerd. Om binnen de tekenreeks de waarde te specificeren die voor de gebruikersnaam wordt gebruikt, kunt u die waarde vervangen door een *.

Query bladeren

De zoekvraag bepaalt hoe resultaten worden weergegeven als via groepsbeleidslijnen wordt gezocht. Hiermee worden de resultaten gefilterd zodat alleen bepaalde resultaten in de vervolgreuzelijst om leden te kiezen worden weergegeven als leden aan een groepsbeleidslijn worden toegevoegd.

Objectklassen

Specificeer geldige objectklassen voor een gebruiker binnen uw adreslijstarchief. Alleen gebruikers die een of meer van deze objectklassen bezitten, mogen verifiëren. Deze objectklassen worden ook met de onderstaande attribuutnamen gebruikt om aan uw B Series Appliance het schema aan te geven dat de LDAP-server gebruikt om gebruikers te identificeren. U kunt meerdere gebruikersobjectklassen invoeren, één per regel.

Attribuutnamen

Specificeer welke velden moeten worden gebruikt als de unieke ID, schermnaam en e-mailadres van een gebruiker.

Unieke ID

In dit veld moet een unieke identificator voor het object worden ingevoerd. Hoewel de distinguished name (DN-naam) als deze identificator kan dienen, kan de distinguished name van een gebruiker gedurende de levensduur van de gebruiker vaak wijzigen, bijvoorbeeld bij een wijziging van de naam of van de locatie of als de naam van het LDAP-archief wordt gewijzigd. De meeste LDAP-servers beschikken daarom over een veld dat per object uniek is en gedurende de levensduur van de gebruiker niet wijzigt. Als u toch de onderscheiden naam als de unieke ID gebruikt en de onderscheiden naam van een gebruiker wijzigt, dan wordt die gebruiker als een nieuwe gebruiker beschouwd en worden eventuele wijzigingen specifiek voor de BeyondTrust-gebruikersaccount van die persoon niet naar de nieuwe gebruiker overgedragen. Als uw LDAP-server niet over een unieke identificator beschikt, dan kunt u een veld gebruiken waarvan de kans zo klein mogelijk is dat de waarde hiervan voor een andere gebruiker identiek is.

E-mailadres

Deze waarde bepaalt welk veld moet worden gebruikt als het e-mailadres van de gebruiker.

Schermnaam

Deze waarde bepaalt welk veld moet worden gebruikt als de schermnaam van de gebruiker.

Instellingen groepsschema *(Alleen zichtbaar tijdens het opzoeken van groepen)*

Type adressenlijst

Om u te helpen de netwerkverbinding tussen uw B Series Appliance en uw beveiligingsprovider te configureren, kunt u een type map als sjabloon selecteren. Zo worden onderstaande te configureren velden vooraf met standaard gegevens ingevuld, maar die gegevens moeten worden gewijzigd om ze in overeenstemming te brengen met de specifieke configuratie van uw beveiligingsprovider. Active Directory LDAP is het meest gebruikte type server, maar u kunt BeyondTrust zo configureren dat met de meeste typen beveiligingsproviders kan worden gecommuniceerd.

Basis DN opzoeken

Bepaal het niveau in uw mappenhiërarchie, gespecificeerd door een onderscheiden naam, waar het B Series Appliance moet beginnen naar groepen te zoeken. Afhankelijk van de grootte van het adreslijstarchief en de groepen die toegang tot het B Series Appliance nodig hebben, kunt u de prestaties verbeteren door de specifieke organisatorische eenheid in uw adreslijstarchief aan te wijzen waarvoor toegang nodig is. Als u niet zeker weet of groepen binnen meerdere organisatorische eenheden actief zijn, kunt u mogelijk het beste de DN-naam (Distinguished Name) van uw adreslijstarchief op het hoogste niveau gebruiken.

Query bladeren

De zoekvraag bepaalt hoe resultaten worden weergegeven als via groepsbeleidslijnen wordt gezocht. Hiermee worden de resultaten gefilterd zodat alleen bepaalde resultaten in de vervolgekeuzelijst om leden te kiezen worden weergegeven als leden aan een groepsbeleidslijn worden toegevoegd.

Objectklassen

Specificeer geldige objectklassen voor een groep binnen uw map-archieven. Alleen groepen die een of meer van deze objectklassen bezitten, worden geretourneerd. Deze objectklassen worden ook met de onderstaande attributnamen gebruikt om aan uw B Series Appliance het schema aan te geven dat de LDAP-server gebruikt om groepen te identificeren. U kunt meerdere groepsobjectklassen invoeren, op elke regel één.

Attribuutnamen

Specificeer welke velden moeten worden gebruikt als de unieke ID en schermnaam van een groep.

Unieke ID

In dit veld moet een unieke identificator voor het object worden ingevoerd. Hoewel de onderscheiden naam als deze identificator kan dienen, kan de onderscheiden naam van een groep gedurende de levensduur van een groep vaak wijzigen, bijvoorbeeld bij een locatiewijziging of als de naam van het LDAP-archief wordt gewijzigd. De meeste LDAP-servers beschikken daarom over een veld dat per object uniek is en gedurende de levensduur van de groep niet wijzigt. Als u toch de onderscheiden naam als de unieke identificator gebruikt en de onderscheiden naam van een groep wijzigt, dan wordt die groep als een nieuwe groep beschouwd en worden eventuele voor die groep gedefinieerde groepsbeleidslijnen niet naar de nieuwe groep overgedragen. Als uw LDAP-server niet over een unieke identificator beschikt, dan kunt u een veld gebruiken waarvan de kans zo klein mogelijk is dat de waarde hiervan voor een andere groep identiek is.

Scherмнаam

Deze waarde bepaalt welk veld moet worden gebruikt als de schermnaam van de groep.

Gebruiker naar groep relaties

U moet in dit veld een query invoeren om te bepalen welke gebruikers tot welke groepen behoren of, andersom, welke groepen welke gebruikers bevatten.

Rekursieve zoekopdracht uitvoeren voor groepen

U kunt recursief naar groepen zoeken. Er wordt dan een query naar een gebruiker uitgevoerd, vervolgens queries voor alle groepen waar die gebruiker toe behoort enzovoort totdat alle mogelijke groepen die met die gebruiker geassocieerd zijn, zijn gevonden.

Het uitvoeren van een recursieve zoekopdracht kan een grote invloed op de prestaties hebben, omdat de server voortdurend zoekopdrachten uitzet tot alle informatie over alle groepen gevonden is. Als dit te lang duurt, dan kan de gebruiker mogelijk niet inloggen.

Bij niet-recursief zoeken wordt er per gebruiker maar één query uitgevoerd. Als uw LDAP-server over een speciaal veld beschikt met alle groepen waar de gebruiker toe behoort, dan is recursief zoeken niet nodig. Recursief zoeken is ook niet nodig als het ontwerp van uw mapstructuur geen groepsleden van groepen ondersteunt.

Instellingen testen

Gebuikersnaam en wachtwoord

Voer een gebruikersnaam en wachtwoord in voor een account die op de door u te testen server bestaat. Deze account moet overeenkomen met de inlog-criteria die in bovenstaande configuratie zijn gespecificeerd.

Probeer de gebruikerskenmerken en groepslidmaatschappen te krijgen als de inloggegevens worden geaccepteerd

Als deze optie is aangevinkt en het testen van inloggegevens is geslaagd, dan wordt ook geprobeerd de gebruikersattributen te controleren en de groep op te zoeken. Let op: om de test van deze functies te laten slagen, moeten ze door uw beveiligingsprovider worden ondersteund en moeten ze daar geconfigureerd zijn.

Test starten

Als uw server juist is geconfigureerd en u voor de test een geldige gebruikersnaam en wachtwoord hebt ingevoerd, dan ontvangt u een bericht dat de test geslaagd is. Anders ziet u een foutmelding en een logboekvermelding waarmee u het probleem kunt onderzoeken.

Beveiligingsprovider bewerken - RADIUS

Algemene instellingen

Naam

Maak een unieke naam aan om deze provider te identificeren.

Ingeschakeld

Als deze optie is ingeschakeld, kan uw B Series Appliance naar deze beveiligingsprovider zoeken als een gebruiker zich probeert aan te melden. Als het niet is aangevinkt, wordt niet naar de provider gezocht.

Houd de schermnaam gesynchroniseerd met het systeem op afstand

Met het aanvinken van deze optie blijft de schermnaam van een gebruiker ingesteld op de naam die is toegewezen op de beveiligingsprovider in plaats van toe te staan dat de schermnaam in BeyondTrust kan worden aangepast.

Autorisatie-instellingen

Alleen de volgende gebruikers toelaten

U kunt ervoor kiezen alleen toegang toe te staan tot bepaalde gebruikers op uw RADIUS-server. Voer de gebruikersnamen op aparte regels in. Nadat de gebruikersnamen zijn toegevoegd, zijn de gebruikers beschikbaar vanaf de dialoog **Beleidslid toevoegen** wanneer u op de pagina **/login > Gebruikers en beveiliging > Groepsbeleidslijnen** groepsbeleidslijnen bewerkt.

Als u dit veld leeg laat, dan worden alle gebruikers toegestaan die tegen uw RADIUS-server worden geverifieerd. Als u iedereen toestaat, dan moet u ook een standaard groepsbeleid specificeren.

LDAP-groep opzoeken

Als u wilt dat gebruikers op deze beveiligingsprovider op een aparte LDAP-server met hun groepen worden geassocieerd, dan moet u een of meerdere LDAP-groepservers kiezen die bij het opzoeken van de groep moeten worden gebruikt.

Standaard groepsbeleid

Elke gebruiker die tegen een externe server wordt geverifieerd, moet lid van ten minste één groepsbeleid zijn om op uw B Series Appliance te kunnen worden geverifieerd en in te kunnen loggen op ofwel de /login-interface ofwel de access console. U kunt een standaard groepsbeleid selecteren om op alle gebruikers toe te passen die toestemming hebben om tegen de geconfigureerde server te worden geverifieerd.

Bedenk dat als er een standaard beleid is gedefinieerd, dat dan elke toegestane gebruiker die tegen deze server wordt geverifieerd, potentieel toegang heeft op het niveau van dit standaard beleid. Daarom wordt aanbevolen dat u een beleid met minimale machtigingen als standaard instelt om te voorkomen dat gebruikers machtigingen krijgen die u niet wilt.



Opmerking: Als voor een gebruiker een standaard groepsbeleid geldt en vervolgens speciaal aan een ander groepsbeleid wordt toegevoegd, dan hebben de instellingen voor het speciale beleid altijd voorrang boven de instellingen voor het standaard beleid, zelfs als het speciale beleid een lagere prioriteit heeft dan het standaard beleid en zelfs als de instellingen van het standaard beleid zijn ingesteld op overschrijven.

Instellingen voor verbinding

Hostnaam

Voer de hostnaam in van de server waar uw externe adreslijstarchief staat.

Poort

Specificeer de verificatiepoort voor uw RADIUS-server. Meestal is dit poort **1812**.

Verbindingsmethode

Als u een extern adreslijstarchief gebruikt in hetzelfde lokale netwerk als uw B Series Appliance, dan kunnen de twee systemen direct met elkaar communiceren. In dat geval hoeft u de optie **Proxy van apparaat via de verbindingagent** niet aan te vinken en kunt u verder gaan.

Als de twee systemen niet direct met elkaar kunnen communiceren, bijvoorbeeld als uw externe adreslijstserver achter een firewall staat, dan moet u een verbindingagent gebruiken. Als u de Win32-verbindingagent downloadt, dan kunnen uw adreslijstserver en uw B Series Appliance met elkaar communiceren via een uitgaande met SSL versleutelde verbinding zonder firewallconfiguratie. De verbindingagent kan ofwel direct naar de adreslijstserver worden gedownload, ofwel naar een aparte server op hetzelfde netwerk als uw adreslijstserver (aanbevolen).

In het bovenstaande geval moet u **Proxy van apparaat via de verbindingagent** aanvinken. Maak een **Wachtwoord verbindingagent** aan om tijdens de installatie van de verbindingagent te gebruiken. Klik vervolgens op **Verbindingagent downloaden**, voer het installatieprogramma uit en volg de instructies van de installatiewizard op. Tijdens installatie wordt u gevraagd om de naam van de beveiligingsprovider in te voeren evenals het hier hierboven aangemaakte wachtwoord voor de verbindingagent.

Gedeeld geheim

Geef een nieuw gedeeld geheim op om uw B Series Appliance en uw RADIUS-server met elkaar te laten communiceren.

Time-out (seconden)

Stel in hoe lang op antwoord van de server moet worden gewacht. Denk eraan dat als het antwoord **Antwoord-accepteren** of **Antwoord-uitdaging** is, dan wacht RADIUS gedurende de totale hier gedefinieerde tijd voordat de account wordt geverifieerd. Aanbevolen wordt daarom om deze waarde zo laag mogelijk in te stellen als uw netwerkinstellingen toestaan. De beste waarde is 3-5 seconden, de maximale waarde is drie minuten.

Instellingen voor cluster *(Alleen zichtbaar voor clusters)*

Selectie-algoritme voor leden

Selecteer de methode waarmee in deze cluster naar nodes wordt gezocht.

Bij **Van boven naar beneden** wordt eerst op de server met de hoogste prioriteit gezocht. Als die server niet beschikbaar is of als de account niet is gevonden, dan wordt op de server met de daarop volgende prioriteit gezocht. Vervolgens wordt in volgorde van aflopende prioriteit op de servers uit de lijst geclusterde servers gezocht tot de account is gevonden of blijkt dat de account niet op een van de gespecificeerde en beschikbare servers bestaat.

Round-robin is bedoeld om de belasting van de verschillende servers in balans te houden. Bij dit algoritme wordt de eerste server waarop wordt gezocht willekeurig gekozen. Als die server niet beschikbaar is of als de account niet is gevonden, dan wordt op een willekeurige andere server gezocht. Vervolgens wordt in willekeurige volgorde op de overige servers uit de lijst geclusterde servers gezocht tot de account is gevonden of blijkt dat de account niet op een van de gespecificeerde en beschikbare servers bestaat.

Wachttijd voor opnieuw proberen

Stel in hoe lang moet worden gewacht nadat een lid van een cluster niet beschikbaar is geworden voordat een nieuwe poging wordt gedaan voor dat lid van die cluster.

Instellingen testen

Gebruikersnaam en wachtwoord

Voer een gebruikersnaam en wachtwoord in voor een account die op de door u te testen server bestaat. Deze account moet overeenkomen met de inlog-criteria die in bovenstaande configuratie zijn gespecificeerd.

Probeer de gebruikerskenmerken en groepslidmaatschappen te krijgen als de inloggegevens worden geaccepteerd

Als deze optie is aangevinkt en het testen van inloggegevens is geslaagd, dan wordt ook geprobeerd de gebruikersattributen te controleren en de groep op te zoeken. Let op: om de test van deze functies te laten slagen, moeten ze door uw beveiligingsprovider worden ondersteund en moeten ze daar geconfigureerd zijn.

Test starten

Als uw server juist is geconfigureerd en u voor de test een geldige gebruikersnaam en wachtwoord hebt ingevoerd, dan ontvangt u een bericht dat de test geslaagd is. Anders ziet u een foutmelding en een logboekvermelding waarmee u het probleem kunt onderzoeken.

Beveiligingsprovider bewerken - Kerberos

Algemene instellingen

Naam

Maak een unieke naam aan om deze provider te identificeren.

Ingeschakeld

Als deze optie is ingeschakeld, kan uw B Series Appliance naar deze beveiligingsprovider zoeken als een gebruiker zich probeert aan te melden. Als het niet is aangevinkt, wordt niet naar de provider gezocht.

Houd de schermnaam gesynchroniseerd met het systeem op afstand

Met het aanvinken van deze optie blijft de schermnaam van een gebruiker ingesteld op de naam die is toegewezen op de beveiligingsprovider in plaats van toe te staan dat de schermnaam in BeyondTrust kan worden aangepast.

Ontdoe realm van principal-namen

Selecteer deze optie om bij het samenstellen van de BeyondTrust-gebruikersnaam het REALM-gedeelte van de Principal-naam van gebruiker te verwijderen.

Autorisatie-instellingen

Gebruikersafhandelingsmodus

Selecteer welke gebruikers op uw B Series Appliance kunnen worden geverifieerd. **Alle gebruikers toestaan** staat iedereen toe die momenteel via uw KDC wordt geverifieerd. **Alleen gebruikers-principals toelaten die op de lijst zijn gespecificeerd** staat alleen

gebruikers-principals toe die expliciet zijn vermeld. Met **Alleen gebruikers-principals toelaten die met de regex overeenkomen** worden alleen gebruikers-principals toegelaten die met een Perl-compatibele reguliere expressie (PCRE) overeenkomen.

SPN-afhandelingsmodus: Alleen SPN's toelaten die op de lijst zijn gespecificeerd

Als dit veld niet is aangevinkt, dan worden alle service-principal-namen (SPN's) voor deze beveiligingsprovider toegelaten. Als dit veld is aangevinkt, dan moet u specifieke SPN's uit een lijst van momenteel geconfigureerde SPN's selecteren.

LDAP-groep opzoeken

Als u wilt dat gebruikers op deze beveiligingsprovider op een aparte LDAP-server met hun groepen worden geassocieerd, dan moet u een of meerdere LDAP-groepservers kiezen die bij het opzoeken van de groep moeten worden gebruikt.

Standaard groepsbeleid

Elke gebruiker die tegen een externe server wordt geverifieerd, moet lid van ten minste één groepsbeleid zijn om op uw B Series Appliance te kunnen worden geverifieerd en in te kunnen loggen op ofwel de /login-interface ofwel de access console. U kunt een standaard groepsbeleid selecteren om op alle gebruikers toe te passen die toestemming hebben om tegen de geconfigureerde server te worden geverifieerd.

Bedenk dat als er een standaard beleid is gedefinieerd, dat dan elke toegestane gebruiker die tegen deze server wordt geverifieerd, potentieel toegang heeft op het niveau van dit standaard beleid. Daarom wordt aanbevolen dat u een beleid met minimale machtigingen als standaard instelt om te voorkomen dat gebruikers machtigingen krijgen die u niet wilt.



Opmerking: Als voor een gebruiker een standaard groepsbeleid geldt en vervolgens speciaal aan een ander groepsbeleid wordt toegevoegd, dan hebben de instellingen voor het speciale beleid altijd voorrang boven de instellingen voor het standaard beleid, zelfs als het speciale beleid een lagere prioriteit heeft dan het standaard beleid en zelfs als de instellingen van het standaard beleid zijn ingesteld op overschrijven.

Beveiligingsprovider bewerken - SAML

Algemene instellingen

Naam

Deze unieke naam helpt bij het identificeren van uw provider. De naam van uw SAML-provider wordt automatisch gegenereerd en kan nu niet worden bewerkt.

Ingeschakeld

Als deze optie is ingeschakeld, kan uw B Series Appliance naar deze beveiligingsprovider zoeken als een gebruiker zich probeert aan te melden. Als het niet is aangevinkt, wordt niet naar de provider gezocht.

Gebruikersprovisioning

Standaard vindt gebruikersprovisionering plaats op deze provider. Als u een SCIM-provider heeft ingesteld, kunt u kiezen om gebruikers te provisioneren via die provider.



Opmerking: Deze instelling kan niet worden aangepast nadat deze beveiligingsprovider de eerste keer wordt opgeslagen.

Instellingen identiteitsprovider

Metagegevens van identiteitsprovider

Het metagegevensbestand bevat alle informatie die nodig is voor de eerste instelling van uw SAML-provider en moet worden gedownload bij uw identiteitsprovider. Selecteer het XML-bestand en klik daarna op **Bestand kiezen** om te selecteren het geselecteerde bestand te uploaden.



Opmerking: De velden voor **Entiteit-ID**, **URL voor service met eenmalige aanmelding**, en **Certificaat** worden automatisch ingevuld uit het metagegevensbestand van de identiteitsprovider. Als u geen metagegevensbestand van uw provider kunt krijgen kan deze informatie handmatig worden ingevoerd.

Entiteit-ID

Dit is de unieke identicator voor de identiteitsprovider die u gebruikt.

URL voor service voor eenmalige aanmelding

Wanneer u bij BeyondTrust wilt inloggen met gebruik van SAML is dit de URL waar u automatisch naar wordt doorgestuurd zodat u kunt inloggen.

Protocolbinding SSO URL

Dit bepaalt of er een HTTP POST plaatsvindt of dat de gebruiker wordt doorgestuurd naar de aanmeld-URL. Dit moet 'redirect' (doorsturen) zijn tenzij anders vereist door de identiteitsprovider.

Servercertificaat

Dit certificaat wordt gebruikt om de handtekening van de assertie die gestuurd is vanaf de identiteitsprovider te verifiëren.

Instellingen serviceprovider

Metagegevens van serviceprovider

Download de metagegevens van BeyondTrust, die u vervolgens moet uploaden naar uw identiteitsprovider.

Entiteit-ID

Dit is uw BeyondTrust-URL. Het identificeert uw site bij de identiteitsprovider.

Privécode

Indien nodig kunt u berichten die gestuurd zijn door de identiteitsprovider ontsleutelen, wanneer deze versleuteling ondersteunen en vereisen. Klik op **Bestand kiezen** om de privé sleutel die nodig is voor het ontsleutelen van de berichten die gestuurd zijn door de identiteitsprovider te uploaden.

Instellingen voor gebruikersprovisionering *(Alleen zichtbaar als deze provider wordt gebruikt voor gebruikersprovisionering)*

SAML-attribuut van gebruiker

Deze kenmerken worden gebruikt om gebruikers in BeyondTrust in te richten. De standaardwaarden komen overeen met door BeyondTrust gecertificeerde toepassingen met verschillende identiteitsproviders. Als u uw eigen SAML-connector aanmaakt, moet u mogelijk de attributen aanpassen om deze overeen te laten komen met wat er wordt verstuurd door uw identiteitsprovider.

Instellingen voor verificatie *(Alleen zichtbaar als deze provider wordt gebruikt voor gebruikersprovisionering)*

Groep opzoeken

Dit is het SAML-attribuut dat de namen van de groepen bevat waar de gebruikers toe moeten behoren. De standaardnaam voor de BeyondTrust-toepassingen is 'Groepen'.



Opmerking: Als de attribuutwaarde meerdere groepsnamen bevat, specificeer dan het scheidingsteken dat u gebruikt om de namen te scheiden. Als u het scheidingsteken leeg laat, dan kan de attribuutwaarde meerdere XML-nodes bevatten die elk een andere naam bevatten.

Beschikbare groepen

Staat een voorgedefinieerde lijst van groepen toe die bij de beveiligingsprovider horen. Deze lijst kan vervolgens worden gebruikt om een groep te koppelen aan het juiste groepsbeleid.

Standaard groepsbeleid

Elke gebruiker die tegen een externe server wordt geverifieerd, moet lid van ten minste één groepsbeleid zijn om op uw B Series Appliance te kunnen worden geverifieerd en in te kunnen loggen op ofwel de /login-interface ofwel de access console. U kunt een standaard groepsbeleid selecteren om op alle gebruikers toe te passen die toestemming hebben om tegen de geconfigureerde server te worden geverifieerd.

Bedenk dat als er een standaard beleid is gedefinieerd, dat dan elke toegestane gebruiker die tegen deze server wordt geverifieerd, potentieel toegang heeft op het niveau van dit standaard beleid. Daarom wordt aanbevolen dat u een beleid met minimale machtigingen als standaard instelt om te voorkomen dat gebruikers machtigingen krijgen die u niet wilt.



Opmerking: Als voor een gebruiker een standaard groepsbeleid geldt en vervolgens speciaal aan een ander groepsbeleid wordt toegevoegd, dan hebben de instellingen voor het speciale beleid altijd voorrang boven de instellingen voor het standaard beleid, zelfs als het speciale beleid een lagere prioriteit heeft dan het standaard beleid en zelfs als de instellingen van het standaard beleid zijn ingesteld op overschrijven.

i Raadpleeg [SAML voor verificatie met eenmalige aanmelding](https://www.beyondtrust.com/docs/privileged-remote-access/how-to/integrations/security-providers/saml/index.htm) op <https://www.beyondtrust.com/docs/privileged-remote-access/how-to/integrations/security-providers/saml/index.htm> voor meer informatie.

Beveiligingsprovider bewerken - SCIM

Opmerking: Om SCIM te laten functioneren moet de SCIM-API ingeschakeld zijn op een API-account en moet de API geconfigureerd zijn op uw SCIM-provider. API-accounts worden beheerd op **/login > Beheer > API-configuratie**. Op dit moment kan er slechts één SCIM-provider worden aangemaakt. Nadat een SCIM-provider is aangemaakt is de optie SCIM niet langer beschikbaar in het vervolgkeuzemenu **Provider aanmaken**. SCIM gebruikersprovisionering gebruikt SCIM 2.0 gebruikers en groepsobjecten. Zie voor meer informatie over de SCIM 2.0-standaard <http://www.simplecloud.info/>.

Opmerking: Bevoorrechte toegang op afstand ondersteunt nu SCIM-API's voor groepen gebruikers. Nadat u een SCIM-provider hebt geconfigureerd in /login en gebruikers en groepen hebt geconfigureerd in uw SCIM-oplossing, geeft PRA dezelfde groepen weer als de groepen die aanwezig zijn in uw SCIM-oplossing, zodat u per SCIM-groep groepsbeleidslijnen kunt selecteren.

Algemene instellingen

Naam

Maak een unieke naam aan om deze provider te identificeren.

Ingeschakeld

Als deze optie is ingeschakeld, kan uw B Series Appliance naar deze beveiligingsprovider zoeken als een gebruiker zich probeert aan te melden. Als het niet is aangevinkt, wordt niet naar de provider gezocht.

SCIM-gebruikersquery-ID

Selecteer in het vervolgkeuzemenu het unieke ID dat de SCIM moet gebruiken voor uw queries.

SCIM-groepsquery-ID

Selecteer in het vervolgkeuzemenu het unieke ID dat de SCIM moet gebruiken voor uw groepsqueries.

Instellingen voor gebruikersprovisionering

Gebruikersattribuut

Deze kenmerken worden gebruikt om gebruikers in BeyondTrust in te richten. De standaardwaarden komen overeen met door BeyondTrust gecertificeerde toepassingen met verschillende identiteitsproviders.

Autorisatie-instellingen

Unieke ID

Voer het SCIM-attribuut in dat gebruikt moet worden als de unieke ID voor de gebruiker binnen BeyondTrust.

Standaard groepsbeleid

Elke gebruiker die tegen een externe server wordt geverifieerd, moet lid van ten minste één groepsbeleid zijn om op uw B Series Appliance te kunnen worden geverifieerd en in te kunnen loggen op ofwel de /login-interface ofwel de access console. U kunt een standaard groepsbeleid selecteren om op alle gebruikers toe te passen die toestemming hebben om tegen de geconfigureerde server te worden geverifieerd.

Bedenk dat als er een standaard beleid is gedefinieerd, dat dan elke toegestane gebruiker die tegen deze server wordt geverifieerd, potentieel toegang heeft op het niveau van dit standaard beleid. Daarom wordt aanbevolen dat u een beleid met minimale machtigingen als standaard instelt om te voorkomen dat gebruikers machtigingen krijgen die u niet wilt.



Opmerking: Als voor een gebruiker een standaard groepsbeleid geldt en vervolgens speciaal aan een ander groepsbeleid wordt toegevoegd, dan hebben de instellingen voor het speciale beleid altijd voorrang boven de instellingen voor het standaard beleid, zelfs als het speciale beleid een lagere prioriteit heeft dan het standaard beleid en zelfs als de instellingen van het standaard beleid zijn ingesteld op overschrijven.

Attribuutnaam

Voer de naam van het SCIM-attribuut in dat de gebruikers uniek identificeert.

Met SCIM geprovisioneerde groepen worden altijd voor het opzoeken van groepen via hun naam uniek geïdentificeerd. Deze identificatie is niet hoofdlettergevoelig.

Leveranciersgroepen



Gebruikers en beveiliging

Leveranciers

Maak leveranciersgroepen aan om externe gebruikers gecontroleerde toegang tot systemen te verlenen. Dit kan nodig zijn om ondersteuning of onderhoud te bieden, of voor een andere taak waarvoor toegang tot het systeem vereist is. U kunt maximaal 50 leveranciersgroepen configureren.

Nieuwe leveranciersgroep toevoegen

Naam

Voer een naam in voor deze leveranciersgroep.

Autorisatie-instellingen

Groepsbeleid

Het geselecteerde groepsbeleid bepaalt de machtigingen, lidmaatschappen en andere instellingen voor alle gebruikers die via deze leverancier verifiëren. Deze instellingen kunnen niet op een per-gebruiker-basis worden gewijzigd. Selecteer een beleid uit de beschikbare opties of ga naar **Gebruikers en beveiliging > Groepsbeleidslijnen** om een nieuw beleid aan te maken.



Opmerking: Groepsbeleidslijnen waarin beheerdersmachtigingen worden toegekend zijn voor leveranciers niet beschikbaar.

Account vervalt na

Stel het aantal dagen waarna het account zal worden gedeactiveerd.

Breng de PRA-beheerder op de hoogte als er een gebruiker aan deze leveranciersgroep wordt toegevoegd

Als dit hokje is aangevinkt, wordt er een e-mail verzonden naar de PRA-beheerder telkens wanneer er een nieuwe gebruiker wordt toegevoegd aan de groep. U kunt goedkeuring van de PRA-beheerder vereisen voor nieuwe leden. Als goedkeuring van de beheerder vereist is, wordt er in de lijst met groepsleden naast de naam van het lid het bericht weergegeven dat de gebruiker **Goedkeuring vereist**.

Vereis goedkeuring van de PRA-beheerder om gebruikers in deze leveranciersgroep te activeren

Als dit vakje is aangevinkt, moet een PRA-beheerder nieuwe leden goedkeuren.

PRA-beheerder

Klik het zoekveld aan om een beheerder te selecteren. Alle leveranciersgroepen moeten minstens één beheerder hebben. Leveranciersbeheerders kunnen geen andere leveranciersbeheerders toevoegen.

Netwerkbeperingen

Lijst met toegestane netwerkadressen

Voer netwerkadresvoorvoegsels in, één per regel, zoals in de onderstaande voorbeelden. Netmasks zijn optioneel en kunnen in punt-decimaalindeling worden gegeven of als een integer bitmask. Als netmask wordt weggelaten, dan zal er worden uitgegaan van één enkel IP-adres.

Instellingen van leveranciersportaal

U kunt het leveranciersportaal voor zelfregistratie aanpassen; dit is het portaal dat gebruikers zien wanneer ze zich registreren. Wijzigingen worden pas doorgevoerd, nadat de leveranciersgroep is opgeslagen.

Leveranciersportaal activeren

Vink het vakje aan om het leveranciersportaal in te schakelen. Deze functie kan alleen geactiveerd worden nadat een groepsbeleid is geselecteerd onder **Autorisatie-instellingen**.

Logo uploaden

Klik om een logo te uploaden. Dit kan uw eigen logo zijn of dat van de leverancier, afhankelijk van uw behoeften en voorkeuren. Gebruik voor het beste resultaat een afbeelding van 128 x 128 pixels. U kunt twee accentkleuren en één achtergrondkleur toepassen:

- **Accentkleur 1:** Bepaalt de achtergrondkleur, randkleur en donkere tekstkleur van de sectieheader.
- **Accentkleur 2:** Bepaalt de kleur van de link, de achtergrondkleur van de knop en de kleur van de taal-wereldbol.

Klik op **Terug naar standaard**, als u de door u aangebrachte wijzigingen niet wilt behouden.

Portaalinstructies

Voer de tekst in die gebruikers te zien krijgen, wanneer ze zich registreren in het portaal voor zelfregistratie.

Onderwerp van e-mail

Dit is het e-mailonderwerp dat gebruikers te zien krijgen wanneer ze de bevestigingsmail ontvangen, nadat ze zich hebben geregistreerd via het portaal voor zelfregistratie.

E-mailhoofdttekst

Voer de tekst in voor de bevestigingsmail die naar gebruikers wordt verzonden nadat ze het registratieformulier hebben ingediend.

URL van leveranciersportaal

Voer de URL in voor de website waar gebruikers zich kunnen registreren.

Emaildomein-acceptatielijst

U kunt e-mailadressen beperken tot de hier vermelde domeinen wanneer gebruikers zich registreren via het portaal. Voer één e-maildomein per regel in. Komma's en spaties zijn niet toegestaan. Als hier niets wordt ingevoerd, gelden er geen beperkingen ten aanzien van toegestane e-mailadressen.

Configureerbare slug

Voer de URL-slug voor uw website in.

Als u klaar bent, klikt u op **Voorbeeld van leveranciersportaal** om te kijken hoe het portaal eruit zal zien.

Sessiebeleidslijnen: Sessiemachtigingen en prompt-regels instellen



Gebruikers en beveiliging

Sessiebeleidslijnen

Sessiebeleidslijnen

Met sessiebeleidslijnen kunt u sessiebeveiligingsmachtigingen aan specifieke scenario's aanpassen. Sessiebeleidslijnen kunnen op gebruikers en Jump-clients worden toegepast.

In de sectie **Sessiebeleidslijnen** staat een lijst met beschikbare beleidslijnen. Klik op het pijltje naast een beleidsnaam om snel te zien waar dat beleid wordt gebruikt, of het voor gebruikers, toegangsuitnodigingen en Jump-clients beschikbaar is en welke hulpmiddelen zijn geconfigureerd.

Sessiebeleid toevoegen, bewerken of verwijderen

Maak een nieuw beleid aan, wijzig een bestaand beleid of verwijder een bestaand beleid.

Kopiëren

Om het aanmaken van gelijksoortige beleidslijnen te versnellen, kunt u op **Kopiëren** klikken om een nieuwe beleidslijn aan te maken met identieke instellingen. U kunt deze nieuwe beleidslijn dan bewerken om aan uw wensen te voldoen.

Sessiebeleid toevoegen of bewerken

Schermaam

Maak een unieke naam aan om dit beleid te identificeren. Deze naam helpt bij het toekennen van een sessiebeleid aan gebruikers en Jump-clients.

Codenaam

Stel een codenaam in voor integratiedoelinden. Als u geen codenaam instelt, maakt PRA er automatisch een aan.

Beschrijving

Voeg een korte beschrijving toe om het doel van dit beleid samen te vatten. U kunt de beschrijving zien als u een beleid op gebruikersaccounts, groepsbeleidslijnen en toegangsuitnodigingen toepast.

Beschikbaarheid

Gebruikers

Kies of dit beleid beschikbaar moet zijn om aan gebruikers toe te wijzen (gebruikersaccounts en groepsbeleidslijnen).

Toegangsuitnodiging

Kies of dit beleid beschikbaar moet zijn om gebruikers te selecteren die worden uitgenodigd om een sessie bij te wonen.

Jumpitems

Kies of dit beleid beschikbaar moet zijn om aan Jumpitems toe te wijzen.

Afhankelijk

Als dit sessiebeleid al in gebruik is, dan ziet u het aantal gebruikers en Jump-clients dat dit beleid gebruikt.

Machtigingen

U kunt voor alle volgende machtigingen ervoor kiezen deze te activeren of uit te schakelen of u kunt ervoor kiezen deze op **Niet gedefinieerd** in te stellen. Sessiebeleidslijnen worden hiërarchisch op een sessie toegepast, waarbij Jump-clients de hoogste prioriteit krijgen, dan gebruikers en dan de algemene standaard. Als er meerdere beleidslijnen op een sessie van toepassing zijn, dan krijgt het beleid met de hoogste prioriteit voorrang boven het andere. Als het op een Jump-client toegepaste beleid bijvoorbeeld een machtiging definieert, dan mogen gedurende de sessie geen andere beleidslijnen die machtiging wijzigen. Om ervoor te zorgen dat een machtiging door een beleid op een lager niveau kan worden gedefinieerd, dan moet die machtiging op **Niet gedefinieerd** zijn ingesteld.

Stel in welke hulpmiddelen met dit beleid moeten worden in- of uitgeschakeld.

Verhoogde toegang naar hulpmiddelen en speciale acties op het eindpunt toestaan

Als dit is ingeschakeld, zal toegang tot verhoogde functionaliteit geleverd worden in de access console voor deze sessie, zonder dat expliciete rechten van een ingelogde gebruiker op het externe eindpunt nodig zijn.

Als deze instelling is uitgeschakeld, krijgen gebruikers geen volledige toegang tot het bestandsoverdracht- en opdrachtshell-functies wanneer ze naar een verhoogd Jumpitem gaan maar geen verhoogde rechten hebben. Om dit te bereiken, zijn speciale acties en aan/uitschakelingsmogelijkheden verborgen en niet beschikbaar. Hiermee worden tevens **Bestandsoverdracht**, **Opdrachtshell** en **Register-toegang** beperkt, wanneer er geen gebruiker in de sessie aanwezig is. Deze instelling is van toepassing voor zover dit is toegestaan door het platform van het eindpunt.

Scherm delen

Regels voor scherm delen

Stel de gebruiker in staat om het externe scherm weer te geven of te beheren. Als deze optie **Niet gedefinieerd** is, dan wordt deze ingesteld op het beleid met de naastlagere prioriteit. Deze instelling kan worden overschreven door een beleid met hogere prioriteit.

Toegestane eindpuntbeperkingen

Stel in of de gebruiker invoer van de muis en het toetsenbord van het externe systeem kan opschorten. De gebruiker kan er ook voor zorgen dat het bureaublad op afstand niet wordt weergegeven.

Klembordsynchronisatierichting

Selecteer hoe uitwisseling van klembordinhoud tussen ondersteuningstechnici en eindgebruikers verloopt. De opties zijn:

- **Niet toegestaan:** De ondersteuningstechnicus mag het klembord niet gebruiken, er worden geen klembordpictogrammen weergegeven in de access console, en knippen en plakken werkt niet.
- **Van ondersteuningstechnicus naar klant toegestaan:** De ondersteuningstechnicus kan klembordinhoud naar de klant versturen, maar kan geen klembordinhoud van de eindgebruiker kopiëren en plakken. Alleen het klembordpictogram **Verzenden** wordt weergegeven in de access console.
- **In beide richtingen toegestaan:** Klembordinhoud kan in beide richtingen worden verzonden. De klembordpictogrammen Verzenden en Ontvangen worden weergegeven in de access console.



Ga voor meer informatie over de Klembordsynchronisatiemodus naar "*Beveiliging: Beveiligingsinstellingen beheren*" op pagina 133.

Beperkingen voor het delen van een toepassing

Hierdoor wordt de toegang tot bepaalde toepassingen op het externe systeem beperkt met ofwel **Alleen de uitvoerbare bestanden uit een lijst toestaan** ofwel **Alleen de uitvoerbare bestanden uit een lijst weigeren**. U kunt ook kiezen of u toegang tot het bureaublad wilt toestaan of weigeren.



Opmerking: Deze functie is alleen van toepassing op Windows-besturingssystemen.

Nieuwe uitvoerbare bestanden toevoegen

Als beperkingen op toepassingen delen worden afgedwongen, dan verschijnt een knop **Nieuwe uitvoerbare bestanden toevoegen**. Als u op deze knop klikt, dan verschijnt een dialoog waarin u uitvoerbare bestanden kunt specificeren die moeten worden geweigerd of toegestaan, in overeenstemming met uw bedoelingen.

Nadat u uitvoerbare bestanden hebt toegevoegd, worden de bestandsnamen die u als beperking hebt geselecteerd in één of twee tabellen weergegeven. U kunt beheerdersopmerkingen in een bewerkbaar veld invoeren.

Voer bestandsnamen of SHA-256 hashes in, één per regel

Als u aan uitvoerbare bestanden beperkingen stelt, dan kunt u handmatig de namen of hashes van de uitvoerbare bestanden invoeren die u wilt toestaan of weigeren. Klik op **Uitvoerbare bestanden toevoegen** als u klaar bent met het toevoegen van de gekozen bestanden aan uw configuratie.

U mag per dialoog maximaal 25 bestanden invoeren. Als u er meer moet toevoegen, moet u op **Uitvoerbare bestanden toevoegen** klikken en vervolgens de dialoog opnieuw openen.

Naar een of meer bestanden bladeren

Bij het beperken van uitvoerbare bestanden kunt u deze optie selecteren om op uw systeem te bladeren en uitvoerbare bestanden te selecteren om de namen en hashes ervan automatisch af te leiden. Als u op deze wijze bestanden op uw lokale platform en systeem selecteert, wees dan voorzichtig en let erop dat de bestanden inderdaad uitvoerbare bestanden zijn. Er wordt geen verificatie op browserniveau uitgevoerd.

Kies **Bestandsnaam gebruiken** of **Bestandshash gebruiken** om ervoor te zorgen dat de browser de namen of hashes van de uitvoerbare bestanden automatisch kan afleiden. Klik op **Uitvoerbare bestanden toevoegen** als u klaar bent en de gekozen bestanden aan uw configuratie wilt toevoegen.

U mag per dialoog maximaal 25 bestanden invoeren. Als u er meer moet toevoegen, moet u op **Uitvoerbare bestanden toevoegen** klikken en vervolgens de dialoog opnieuw openen.



Opmerking: Deze optie is alleen beschikbaar in moderne browsers, niet in oudere browsers.

Mag inloggen met inloggegevens van een Endpoint Credential Manager

Activeer een verbinding van een gebruiker naar uw Endpoint Credential Manager om inloggegevens te gebruiken vanaf uw bestaande wachtwoord-opslagplaatsen of -kluizen.

Voor gebruik van de Endpoint Credential Manager is een aparte onderhoudsovereenkomst met BeyondTrust vereist. Als een onderhoudsovereenkomst eenmaal is afgesloten, kunt u de benodigde middleware vanuit het BeyondTrust-ondersteuningsportaal downloaden.



Opmerking: In eerdere versies dan 15.2 is deze functie alleen beschikbaar in sessies die vanaf een opgevaardeerde Jump-client op Windows® zijn gestart. Vanaf versie 15.2 mag u ook een Endpoint Credential Manager gebruiken in sessies met externe Jump, sessies met Microsoft®-bureaublad op afstand, VNC-sessies en sessies met Shell Jump. U kunt deze functie ook gebruiken met de speciale actie 'Uitvoeren als' in een sessie met scherm delen op een Windows®-systeem.

Annotaties

Regels voor annotaties

Hierdoor kan de gebruiker hulpmiddelen voor annotaties gebruiken om op het externe scherm te tekenen. Als deze optie **Niet gedefinieerd** is, dan wordt deze ingesteld op het beleid met de naastlagere prioriteit. Deze instelling kan worden overschreven door een beleid met hogere prioriteit.

Bestandsoverdracht

Regels voor bestandsoverdracht

Hierdoor kan de gebruiker bestanden naar het externe systeem uploaden, van het externe systeem downloaden, of beide. Als deze optie **Niet gedefinieerd** is, dan wordt deze ingesteld op het beleid met de naastlagere prioriteit. Deze instelling kan worden overschreven door een beleid met hogere prioriteit.

Toegankelijke paden op het bestandssysteem van het eindpunt

Sta toe dat de gebruiker bestanden overdraagt naar of van alle mappen op het externe systeem of alleen naar of van gespecificeerde mappen.

Toegankelijke paden op het bestandssysteem van de gebruiker

Sta toe dat de gebruiker bestanden overdraagt naar of van alle mappen op zijn of haar lokale systeem of alleen naar of van gespecificeerde mappen.

Oprachtshell

Regels voor opdrachtshell

Hiermee kan de gebruiker via een virtuele interface opdrachten op de opdrachtregel van de externe computer geven. Als deze optie **Niet gedefinieerd** is, dan wordt deze ingesteld op het beleid met de naastlagere prioriteit. Deze instelling kan worden overschreven door een beleid met hogere prioriteit.



Opmerking: Toegang tot de opdrachtshell kan niet worden beperkt voor Shell Jump-sessies.

Oprachtfiltering configureren om het per ongeluk gebruiken van opdrachten die schadelijk kunnen zijn voor de eindpuntsystemen te voorkomen.



Raadpleeg [Shell-jump gebruiken om toegang tot een apparaat in een extern netwerk te krijgen](https://www.beyondtrust.com/docs/privileged-remote-access/getting-started/access-console/shell-jump.htm) op www.beyondtrust.com/docs/privileged-remote-access/getting-started/access-console/shell-jump.htm voor meer informatie over het filteren van opdrachten.

Systeeminformatie

Regels voor systeeminformatie

Hiermee kan de gebruiker systeeminformatie over de externe computer weergeven. Als deze optie **Niet gedefinieerd** is, dan wordt deze ingesteld op het beleid met de naastlagere prioriteit. Deze instelling kan worden overschreven door een beleid met hogere prioriteit.

Mag systeeminformatie-acties gebruiken

Hierdoor kan de gebruiker met processen en programma's op de externe computer communiceren zonder de noodzaak van scherm delen. Stop processen, start, stop, pauzeer, hervat services en start ze opnieuw; en maak de installatie van programma's ongedaan.

Register-toegang

Regels voor registertoegang

Hierdoor kan de gebruiker het register op een extern Windows-systeem benaderen zonder de noodzaak tot scherm delen. Bekijk sleutels, voeg ze toe en bewerk ze, zoek en importeer/exporteer sleutels.

Standaard scripts

Regels voor standaard scripts

Hierdoor kan de gebruiker standaardscripts uitvoeren die voor zijn of haar teams zijn aangemaakt. Als deze optie **Niet gedefinieerd** is, dan wordt deze ingesteld op het beleid met de naastlagere prioriteit. Deze instelling kan worden overschreven door een beleid met hogere prioriteit.

Beleid exporteren

U kunt een sessiebeleid van de ene site exporteren en die machtigingen naar een beleid op een andere site importeren. Bewerk het beleid dat u wilt exporteren en ga naar de onderkant van de pagina. Klik op **Beleid exporteren** en sla het bestand op.

Beleid importeren

U kunt deze beleidsinstellingen importeren op elke andere BeyondTrust-site die het importeren van sessiebeleid ondersteunt. Maak een nieuw sessiebeleid aan en ga naar de onderkant van de pagina. Blader naar het beleidsbestand en klik vervolgens op **Beleid importeren**. Nadat het beleidsbestand is geüpload wordt de pagina vernieuwd waarna u wijzigingen kunt aanbrengen. Klik op **Beleid opslaan** om het beleid beschikbaar te stellen.

Opslaan

Klik op **Opslaan** om dit beleid beschikbaar te stellen.

Sessiebeleid-simulator

Omdat het gebruik van gelaagd beleid ingewikkeld kan zijn, kunt u de **Sessiebeleid-simulator** gebruiken om te bepalen wat het resultaat is. Bovendien kunt u de simulator gebruiken om te onderzoeken waarom een machtiging niet beschikbaar is als u het tegendeel verwacht.

Gebruiker

Selecteer eerst de gebruiker die de sessie uitvoert. Deze vervolgkeuzelijst bevat zowel gebruikersaccounts als uitnodigingsbeleidslijnen.

Sessiestartmethode

Selecteer de sessiestartmethode.

Jump-client/jumpsnelkoppeling

Zoek een Jump-client of jumpsnelkoppeling aan de hand van de naam, opmerkingen, Jumpgroep of label.

Simuleer

Klik op **Simuleren**. In het gebied hieronder worden de machtigingen die door sessiebeleid kunnen worden geconfigureerd, in de modus alleen-lezen weergegeven. U kunt zien welke machtigingen wel en niet zijn toegestaan als resultaat van gestapelde beleidslijnen en door welke beleidslijn elk van de machtigingen is ingesteld.

Groepsbeleidslijnen: Gebruikersmachtigingen op groepen gebruikers toepassen



Gebruikers en beveiliging

Groepsbeleidslijnen

Groepsbeleidslijnen

Op de pagina **Groepsbeleidslijnen** kunt u groepen gebruikers instellen die dezelfde rechten delen.

Nieuw beleid toevoegen, bewerken, verwijderen

Maak een nieuw beleid aan, wijzig een bestaand beleid of verwijder een bestaand beleid.



Opmerking: Er verschijnt een waarschuwing als u het groepsbeleid bewerkt dat het standaard beleid is voor de lokale provider of als de groep beheerdergebruikers heeft en u beheerdersmachtigingen verwijdert. Zorg ervoor dat andere gebruikers beheerdersmachtigingen hebben voordat u verder gaat.

Volgorde veranderen

Klik op de knop **Volgorde wijzigen** om groepsbeleidslijnen te slepen en neer te zetten om de prioriteiten ervan in te stellen. Klik op **Volgorde opslaan** om de wijzigingen in de prioriteiten te effectueren. Als meerdere beleidslijnen van toepassing zijn voor een bepaalde gebruiker, gelden de machtigingen beginnend vanaf de bovenkant van de lijst **Groepsbeleidslijnen**, en vervolgens verderop in de lijst. Als een machtiging conflicteert met een machtiging uit een groepsbeleid dat hoger in de lijst staat, dan overschrijft de lagere machtiging de hogere machtiging, tenzij de hogere als **Definitief** stond ingesteld. Kort gezegd: groepsbeleidslijnen die lager in de lijst staan, hebben een hogere functionele prioriteit dan groepsbeleidslijnen die hoger in de lijst staan.

Kopiëren

Om het aanmaken van gelijksoortige beleidslijnen te versnellen, kunt u op **Kopiëren** klikken om een nieuwe beleidslijn aan te maken met identieke instellingen. U kunt deze nieuwe beleidslijn dan bewerken om aan uw wensen te voldoen.

Beleid toevoegen of bewerken

Naam beleid

Maak een unieke naam aan om dit beleid te identificeren.

Beschikbare leden en beleidsleden

Om leden toe te wijzen, selecteert u een lid uit de lijst met **Beschikbare leden** en klikt u op **Toevoegen** om het lid te verplaatsen naar het vak met **Beleidsleden**. Gebruik het zoekveld aan de rechterkant om bestaande leden te vinden.

U kunt gebruikers van uw lokale systeem of gebruikers of hele groepen van geconfigureerde beveiligingsproviders selecteren. Om gebruikers of groepen vanuit een extern adreslijstarchief toe te voegen zoals LDAP, RADIUS of Kerberos, moet u eerst op de pagina **/login > Gebruikers en beveiliging > Beveiligingsproviders** de verbinding configureren. Als een poging om een gebruiker van een

geconfigureerde beveiligingsprovider toe te voegen ongeldig is, dan verschijnt er hier en in de logboekregistratie een melding van een synchronisatiefout.

Accountinstellingen

Welke accountinstellingen moet dit Groepsbeleid beheren?

Selecteer voor elke instelling of die in dit beleid moet worden gedefinieerd of dat de instelling voor individuele gebruikers moet worden geconfigureerd. Als de instelling hier moet worden gedefinieerd, dan kunt u die machtiging niet voor een individuele gebruiker vanaf diens accountpagina wijzigen.

Als u een beleid hebt dat een machtiging definieert en u wilt dat geen enkel beleid die machtiging kan overschrijven, dan moet u selecteren dat dat beleid niet kan worden overschreven en moet het beleid een hogere prioriteit hebben dan andere beleidslijnen die ook die instelling definiëren.

Verificatie in twee stappen

Bij verificatie in twee stappen (two-factor authentication of 2FA) wordt gebruik gemaakt van een vericator-app waarmee een op tijd gebaseerde eenmalig code wordt gegenereerd. Met deze code kunt u vervolgens bij de beheerinterface en de toegangsconsole inloggen. Als **Vereist** is geselecteerd, worden gebruikers gevraagd te registreren en de volgende keer dat ze inloggen 2FA te gebruiken. Als **Optioneel** is geselecteerd, krijgen gebruikers de keuze om 2FA te gebruiken, maar zijn ze dat niet verplicht.



Opmerking: Gebruikers die al inlogcodes ontvangen, worden automatisch geüpgraded naar 2FA, hoewel ze e-mailcodes mogen blijven gebruiken tot ze hun app hebben geregistreerd. Op het moment dat ze 2FA gaan gebruiken, wordt de optie voor e-mailcodes permanent uitgeschakeld.

Verlopen van account

Account vervalt nooit als dit is aangevinkt. Er moet een vervaldatum voor het account zijn ingesteld als dit niet is aangevinkt.

Account uitgeschakeld

Hiermee kunt u het account uitschakelen, zodat de gebruiker niet kan inloggen. Als een account wordt uitgeschakeld, wordt deze NIET verwijderd.

Opmerkingen

Voeg commentaar toe om aan te geven wat het doel is van dit object.

Algemene machtigingen

Welke algemene instellingen moet dit Groepsbeleid beheren?

Selecteer voor elke instelling of die in dit beleid moet worden gedefinieerd of dat de instelling voor individuele gebruikers moet worden geconfigureerd. Als de instelling hier moet worden gedefinieerd, dan kunt u die machtiging niet voor een individuele gebruiker vanaf diens accountpagina wijzigen.

Als u een beleid hebt dat een machtiging definieert en u wilt dat geen enkel beleid die machtiging kan overschrijven, dan moet u selecteren dat dat beleid niet kan worden overschreven en moet het beleid een hogere prioriteit hebben dan andere beleidslijnen die ook die instelling definiëren.

Beheer

Beheerdersrechten

Hierdoor krijgt de gebruiker volledige beheerdersrechten.

Beheerdersrechten Vault

Stelt gebruikers in staat om toegang te krijgen tot de Vault.

Instelling voor wachtwoord

Hierdoor kan de gebruiker wachtwoorden instellen en accounts ontgrendelen voor lokale gebruikers die geen beheerder zijn.

Jumpoint bewerken

Hierdoor mogen gebruikers Jumpoints aanmaken of bewerken. Deze optie heeft geen invloed op de mogelijkheid voor de gebruikers om via Jumpoints toegang tot externe computers te krijgen. Dat wordt via beleid op Jumpoint- of groepsniveau geconfigureerd.

Bewerking van team

Hierdoor kunnen gebruikers teams aanmaken of bewerken.

Jumpgroep bewerken

Biedt gebruikers de mogelijkheid jumpgroepen aan te maken of te bewerken.

Standaard script bewerken

Hierdoor kan de gebruiker standaard scripts aanmaken of bewerken die worden gebruikt in sessies met scherm delen of met opdrachtshell.

Bewerking van aangepaste link

Hierdoor kan de gebruiker aangepaste koppelingen aanmaken of bewerken.

Rapportage

Toegang tot sessie- en teamrapporten

Stelt de gebruiker in staat om rapporten van toegangssessies te bekijken. Afhankelijk van de geselecteerde optie kunnen gebruikers hun eigen sessies, hun Jumpgroepsessies of alle sessies bekijken.

Mag rapporten van toegangssessies bekijken

Hierdoor kan de gebruiker rapporten maken over access session-activiteiten, alleen sessies weergeven waarvan hij of zij de primaire sessie-eigenaar is, alleen sessies weergeven voor eindpunten die tot een Jumpgroep behoren waarvan de gebruiker een lid is, of alle sessies weergeven.

Mag Access Session-opnamen bekijken

Hierdoor kan een gebruiker opnames bekijken van sessies met scherm delen en van sessies met opdrachtshell.

Toegang tot Vault-rapporten

Stelt de gebruiker in staat om Vault-rapporten te bekijken. Afhankelijk van de geselecteerde optie kunnen gebruikers hun eigen sessies of alle sessies bekijken.

Mag Vault-rapporten zien

Stelt de gebruiker in staat om zijn of haar eigen Vault-gebeurtenissen of alle Vault-gebeurtenissen te bekijken.

Toegangsmachtigingen

Mag eindpunten benaderen

Hierdoor mag de gebruiker de access console gebruiken om sessies uit te voeren. Als toegang tot een eindpunt is ingeschakeld, dan zijn er ook opties beschikbaar die betrekking hebben op toegang tot een eindpunt.

Sessiebeheer

Mag sessies delen met teams waarvan hij/zij geen deel uitmaakt

Hierdoor kan de gebruiker behalve zijn of haar teamleden ook een minder beperkte groep gebruikers uitnodigen om sessies te delen. Samen met de machtiging Uitgebreide beschikbaarheid vormt deze machtiging een uitbreiding van de mogelijkheden om sessies te delen.

Mag externe gebruikers uitnodigen

Hierdoor kan de gebruiker een gebruiker van een derde partij uitnodigen eenmalig aan een sessie deel te nemen.

Toegestaan om uitgebreide beschikbaarheid-modus in te schakelen

Hierdoor kan de gebruiker e-mailuitnodigingen van andere gebruikers ontvangen met het verzoek een sessie te delen, ook als hij of zij niet bij de access console is ingelogd.

Mag de externe code bewerken

Staat de gebruiker toe om de externe sleutel te wijzigen vanaf het informatievenster van een sessie binnen de access console.

Scherm delen van gebruiker tot gebruiker

Mag scherm tonen aan andere gebruikers

Hierdoor kan een gebruiker zijn of haar scherm delen met een andere gebruiker zonder dat de ontvanger aan een sessie hoeft aan te melden. Deze optie is zelfs beschikbaar als de gebruiker niet in een sessie is.

Mag besturing geven tijdens tonen van scherm aan andere gebruikers

Hierdoor kan de gebruiker tijdens scherm delen de besturing over muis en toetsenbord aan de gebruiker geven die zijn of haar scherm bekijkt.

Jump-technologie

Toegestane Jumpitem-methodes

Hiermee kan de gebruiker een Jump uitvoeren naar computers via **Jump-clients**, **Lokale Jump op het lokale netwerk**, **Externe Jump via een Jumpoint**, **Externe VNC via een Jumpoint**, **Extern RDP via een Jumpoint**, **Web Jump via een Jumpoint**, **Shell Jump via een Jumpoint** en **Jump via tunnelprotocol via een Jumpoint**.

Jumpitem-rollen

Een Jumpitem-rol is een van te voren gedefinieerde reeks machtigingen voor het beheer en gebruik van Jumpitems. Klik voor elke optie op **Tonen** om de Jumpitem-rol in een nieuw tabblad te openen.

De **Standaard** rol wordt alleen gebruikt als **Standaard van gebruiker toepassen** is ingesteld voor een bepaalde gebruiker in een Jumpgroep.

De **Persoonlijke** rol is alleen van toepassing op Jumpitems die zijn vastgespeld aan de persoonlijke lijst met Jumpitems van de gebruiker.

De **Teams**-rol is van toepassing op Jumpitems die zijn vastgespeld aan de persoonlijke lijst met Jumpitems van een teamlid met een lagere rol. Een teammanager kan bijvoorbeeld de persoonlijke Jumpitems van teamleiders en teamleden bekijken. En een teamleader kan de persoonlijke Jumpitems van teamleden bekijken.

De **Systeem** rol is van toepassing op alle andere Jumpitems in het systeem. Voor de meeste gebruikers moet dit worden ingesteld op **Geen toegang**. Als een andere optie is ingesteld, worden gebruikers toegevoegd aan Jumpgroepen waar ze normaal niet aan zouden worden toegewezen. Ook kunnen zij in de access console de lijst met persoonlijke Jumpitems van niet-leden zien.

Sessietoestemmingen

Stel de prompts en de machtigingsregels in die voor de sessies van deze gebruiker moeten gelden. Kies een bestaand sessiebeleid of definieer aangepaste machtigingen voor deze gebruiker. Als u **Niet gedefinieerd** specificeert, dan wordt het algemene standaard beleid gebruikt. Deze machtigingen kunnen door een beleid met hogere prioriteit worden overschreven.

Beschrijving

Bekijk de omschrijving van een vooraf gedefinieerd beleid voor sessietoestemming.

Scherm delen

Regels voor scherm delen

Stel de gebruiker in staat om het externe scherm weer te geven of te beheren. Als deze optie **Niet gedefinieerd** is, dan wordt deze ingesteld op het beleid met de naastlagere prioriteit. Deze instelling kan worden overschreven door een beleid met hogere prioriteit.

i Raadpleeg [Het externe eindpunt beheren met scherm delen](https://www.beyondtrust.com/docs/privileged-remote-access/getting-started/access-console/screen-sharing.htm) op <https://www.beyondtrust.com/docs/privileged-remote-access/getting-started/access-console/screen-sharing.htm> voor meer informatie.

Klembordsynchronisatierichting

Selecteer hoe uitwisseling van klembordinhoud tussen ondersteuningstechnici en eindgebruikers verloopt. De opties zijn:

- **Niet toegestaan:** De ondersteuningstechnicus mag het klembord niet gebruiken, er worden geen klembordpictogrammen weergegeven in de access console, en knippen en plakken werkt niet.
- **Van ondersteuningstechnicus naar klant toegestaan:** De ondersteuningstechnicus kan klembordinhoud naar de klant versturen, maar kan geen klembordinhoud van de eindgebruiker kopiëren en plakken. Alleen het klembordpictogram **Verzenden** wordt weergegeven in de access console.
- **In beide richtingen toegestaan:** Klembordinhoud kan in beide richtingen worden verzonden. De klembordpictogrammen **Verzenden** en **Ontvangen** worden weergegeven in de access console.

i Ga voor meer informatie over de Klembordsynchronisatiemodus naar "[Beveiliging: Beveiligingsinstellingen beheren](#)" op pagina 133.

Beperkingen voor het delen van een toepassing

Hierdoor wordt de toegang tot bepaalde toepassingen op het externe systeem beperkt met ofwel **Alleen de uitvoerbare bestanden uit een lijst toestaan** ofwel **Alleen de uitvoerbare bestanden uit een lijst weigeren**. U kunt ook kiezen of u toegang tot het bureaublad wilt toestaan of weigeren.



Opmerking: Deze functie is alleen van toepassing op Windows-besturingssystemen.

Nieuwe uitvoerbare bestanden toevoegen

Als beperkingen op toepassingen delen worden afgedwongen, dan verschijnt een knop **Nieuwe uitvoerbare bestanden toevoegen**. Als u op deze knop klikt, dan verschijnt een dialoog waarin u uitvoerbare bestanden kunt specificeren die moeten worden geweigerd of toegestaan, in overeenstemming met uw bedoelingen.

Nadat u uitvoerbare bestanden hebt toegevoegd, worden de bestandsnamen die u als beperking hebt geselecteerd in één of twee tabellen weergegeven. U kunt beheerdersopmerkingen in een bewerkbaar veld invoeren.

Voer bestandsnamen of SHA-256 hashes in, één per regel

Als u aan uitvoerbare bestanden beperkingen stelt, dan kunt u handmatig de namen of hashes van de uitvoerbare bestanden invoeren die u wilt toestaan of weigeren. Klik op **Uitvoerbare bestanden toevoegen** als u klaar bent met het toevoegen van de gekozen bestanden aan uw configuratie.

U mag per dialoog maximaal 25 bestanden invoeren. Als u er meer moet toevoegen, moet u op **Uitvoerbare bestanden toevoegen** klikken en vervolgens de dialoog opnieuw openen.

Naar een of meer bestanden bladeren

Bij het beperken van uitvoerbare bestanden kunt u deze optie selecteren om op uw systeem te bladeren en uitvoerbare bestanden te selecteren om de namen en hashes ervan automatisch af te leiden. Als u op deze wijze bestanden op uw lokale platform en systeem selecteert, wees dan voorzichtig en let erop dat de bestanden inderdaad uitvoerbare bestanden zijn. Er wordt geen verificatie op browserniveau uitgevoerd.

Kies **Bestandsnaam gebruiken** of **Bestandshash gebruiken** om ervoor te zorgen dat de browser de namen of hashes van de uitvoerbare bestanden automatisch kan afleiden. Klik op **Uitvoerbare bestanden toevoegen** als u klaar bent en de gekozen bestanden aan uw configuratie wilt toevoegen.

U mag per dialoog maximaal 25 bestanden invoeren. Als u er meer moet toevoegen, moet u op **Uitvoerbare bestanden toevoegen** klikken en vervolgens de dialoog opnieuw openen.



Opmerking: Deze optie is alleen beschikbaar in moderne browsers, niet in oudere browsers.

Toegestane eindpuntbeperkingen

Stel in of de gebruiker invoer van de muis en het toetsenbord van het externe systeem kan opschorten. De gebruiker kan er ook voor zorgen dat het bureaublad op afstand niet wordt weergegeven.



Raadpleeg [Het externe eindpunt beheren met scherm delen](https://www.beyondtrust.com/docs/privileged-remote-access/getting-started/access-console/screen-sharing.htm) op <https://www.beyondtrust.com/docs/privileged-remote-access/getting-started/access-console/screen-sharing.htm> voor meer informatie.

Annotaties

Regels voor annotaties

Hierdoor kan de gebruiker hulpmiddelen voor annotaties gebruiken om op het externe scherm te tekenen. Als deze optie **Niet gedefinieerd** is, dan wordt deze ingesteld op het beleid met de naastlagere prioriteit. Deze instelling kan worden overschreven door een beleid met hogere prioriteit.



Zie voor meer informatie [Annotaties gebruiken om op het externe scherm van het eindpunt te tekenen](https://www.beyondtrust.com/docs/privileged-remote-access/getting-started/access-console/annotations.htm) op <https://www.beyondtrust.com/docs/privileged-remote-access/getting-started/access-console/annotations.htm>.

Bestandsoverdracht

Regels voor bestandsoverdracht

Hierdoor kan de gebruiker bestanden naar het externe systeem uploaden, van het externe systeem downloaden, of beide. Als deze optie **Niet gedefinieerd** is, dan wordt deze ingesteld op het beleid met de naastlagere prioriteit. Deze instelling kan worden overschreven door een beleid met hogere prioriteit.

Toegankelijke paden op het bestandssysteem van het eindpunt

Sta toe dat de gebruiker bestanden overdraagt naar of van alle mappen op het externe systeem of alleen naar of van gespecificeerde mappen.

Toegankelijke paden op het bestandssysteem van de gebruiker

Sta toe dat de gebruiker bestanden overdraagt naar of van alle mappen op zijn of haar lokale systeem of alleen naar of van gespecificeerde mappen.



Zie voor meer informatie [Bestandsoverdracht naar en van het externe eindpunt](https://www.beyondtrust.com/docs/privileged-remote-access/getting-started/access-console/file-transfer.htm) op <https://www.beyondtrust.com/docs/privileged-remote-access/getting-started/access-console/file-transfer.htm>.

Opdrachtshell

Regels voor opdrachtshell

Hiermee kan de gebruiker via een virtuele interface opdrachten op de opdrachtregel van de externe computer geven. Als deze optie **Niet gedefinieerd** is, dan wordt deze ingesteld op het beleid met de naastlagere prioriteit. Deze instelling kan worden overschreven door een beleid met hogere prioriteit.



Opmerking: Toegang tot de opdrachtshell kan niet worden beperkt voor Shell Jump-sessies.

Opdrachtfiltering configureren om het per ongeluk gebruiken van opdrachten die schadelijk kunnen zijn voor de eindpuntssystemen te voorkomen.



Raadpleeg [Shell-jump gebruiken om toegang tot een apparaat in een extern netwerk te krijgen](https://www.beyondtrust.com/docs/privileged-remote-access/getting-started/access-console/shell-jump.htm) op www.beyondtrust.com/docs/privileged-remote-access/getting-started/access-console/shell-jump.htm voor meer informatie over het filteren van opdrachten.



Zie voor meer informatie [De opdrachtshell op het externe eindpunt openen met behulp van de toegangsconsole](https://www.beyondtrust.com/docs/privileged-remote-access/getting-started/access-console/command-shell.htm) op <https://www.beyondtrust.com/docs/privileged-remote-access/getting-started/access-console/command-shell.htm>.

Systeeminformatie

Regels voor systeeminformatie

Hiermee kan de gebruiker systeeminformatie over de externe computer weergeven. Als deze optie **Niet gedefinieerd** is, dan wordt deze ingesteld op het beleid met de naastlagere prioriteit. Deze instelling kan worden overschreven door een beleid met hogere prioriteit.

Mag systeeminformatie-acties gebruiken

Hierdoor kan de gebruiker met processen en programma's op de externe computer communiceren zonder de noodzaak van scherm delen. Stop processen, start, stop, pauzeer, hervat services en start ze opnieuw; en maak de installatie van programma's ongedaan.

i Raadpleeg [Systeeminformatie bekijken op het externe eindpunt op https://www.beyondtrust.com/docs/privileged-remote-access/getting-started/access-console/system-info.htm](https://www.beyondtrust.com/docs/privileged-remote-access/getting-started/access-console/system-info.htm) voor meer informatie.

Register-toegang

Regels voor registertoegang

Hierdoor kan de gebruiker het register op een extern Windows-systeem benaderen zonder de noodzaak tot scherm delen. Bekijk sleutels, voeg ze toe en bewerk ze, zoek en importeer/exporteer sleutels.

i Zie voor meer informatie [Toegang tot de register-editor op het externe eindpunt op https://www.beyondtrust.com/docs/privileged-remote-access/getting-started/access-console/registry-editor.htm](https://www.beyondtrust.com/docs/privileged-remote-access/getting-started/access-console/registry-editor.htm).

Standaard scripts

Regels voor standaard scripts

Hierdoor kan de gebruiker standaardscripts uitvoeren die voor zijn of haar teams zijn aangemaakt. Als deze optie **Niet gedefinieerd** is, dan wordt deze ingesteld op het beleid met de naastlagere prioriteit. Deze instelling kan worden overschreven door een beleid met hogere prioriteit.

i Raadpleeg [De opdrachtshell op het externe eindpunt openen met behulp van de Access Console op https://www.beyondtrust.com/docs/privileged-remote-access/getting-started/access-console/command-shell.htm](https://www.beyondtrust.com/docs/privileged-remote-access/getting-started/access-console/command-shell.htm) voor meer informatie.

Beschikbaarheidsinstellingen

Inlogschema

Beperk inloggen van gebruiker aan de hand van het volgende rooster

Stel een schema in om te bepalen wanneer gebruikers kunnen inloggen bij de access console. Stel de tijdzone in die u voor dit rooster wilt gebruiken en voeg vervolgens een of meer roostervermeldingen toe. Stel voor elke vermelding de startdatum en -tijd en de einddatum en -tijd in.

Als bijvoorbeeld de begintijd is ingesteld op 08:00 uur en de eindtijd op 17:00 uur, dan kan een gebruiker op elk tijdstip in deze periode inloggen en kan blijven doorwerken tot na de eindtijd. De gebruiker kan echter na 17:00 uur niet opnieuw inloggen.

Forceer uitloggen als het schema inloggen niet toestaat

Als strengere toegangscontrole is vereist, dan moet u deze optie aanvinken. Hierdoor wordt de gebruiker geforceerd op de geplande eindtijd uit te loggen. In dit geval ontvangt de gebruiker herhaalde berichten vanaf 15 minuten voordat de sessie wordt beëindigd.

Wanneer de gebruiker uitgelogd wordt, volgen eventuele eigen sessies de sessieterugval-regels.

Lidmaatschappen

Lidmaatschap van teams toevoegen

Zoek naar teams waartoe leden van dit groepsbeleid moeten behoren. U kunt de rol op **Teamlid**, **Teamleider** of **Teammanager** instellen. Deze rollen spelen een belangrijke rol in de **Dashboard**-functie van de access console. Klik op **Toevoegen**.

De toegevoegde leden worden in een tabel weergegeven. U kunt de rol van teamleden bewerken of het team van de lijst verwijderen.

Lidmaatschap van teams verwijderen

Zoek naar teams waarvan leden van dit groepsbeleid moeten worden verwijderd en klik vervolgens op **Toevoegen**. De verwijderde teams worden in een tabel weergegeven. U kunt een team van de lijst verwijderen.

Jumpoint-lidmaatschap toevoegen

Zoek naar Jumpoints waartoe leden van dit groepsbeleid toegang moeten hebben en klik vervolgens op **Toevoegen**. De toegevoegde Jumpoints worden in een tabel weergegeven. U kunt een Jumpoint van de lijst verwijderen.

Jumpoint-lidmaatschap verwijderen

Zoek naar Jumpoints waarvan leden van dit groepsbeleid niet mogen worden verwijderd en klik vervolgens op **Toevoegen**. De verwijderde Jumpoints worden in een tabel weergegeven. U kunt een Jumpoint van de lijst verwijderen.

Jumpgroep-lidmaatschappen toevoegen

Zoek naar Jumpgroepen waar leden van dit groepsbeleid bij moeten horen. U kunt voor elke gebruiker de [Jumpitemrol](#) instellen zodat hun machtigingen specifiek zijn ingesteld voor Jumpitems in deze Jumpgroep. Of u gebruikt de standaard Jumpitemrollen van de gebruiker die in dit groepsbeleid of op de pagina **Gebruikers en beveiliging > Gebruikers** zijn ingesteld. Een Jumpitem-rol is een van te voren gedefinieerde reeks machtigingen voor het beheer en gebruik van Jumpitems.



Raadpleeg [Jump-itemrollen gebruiken om machtigingssets te configureren voor Jump-items](https://www.beyondtrust.com/docs/privileged-remote-access/how-to/jumpoint/jump-item-roles.htm) op <https://www.beyondtrust.com/docs/privileged-remote-access/how-to/jumpoint/jump-item-roles.htm> voor meer informatie.

U kunt ook een [Jumpbeleid](#) toepassen om de toegang van gebruikers tot de Jumpitems in deze Jumpgroep te beheren. Als u in plaats hiervan **Op Jumpitem ingesteld** selecteert, wordt het Jumpbeleid toegepast op het Jumpitem zelf. Jump-beleidslijnen worden op de pagina **Jump > Jump-beleidslijnen** geconfigureerd en bepalen welke periodes een gebruiker toegang heeft tot dit Jumpitem. Er kan ook een kennisgeving worden verzonden als het Jumpbeleid wordt benaderd of er kan toestemming moeten worden gevraagd om het te benaderen. Als er op de gebruiker of het Jumpitem geen Jumpbeleid is toegepast, is de toegang tot dit Jumpitem onbeperkt.



Raadpleeg [Jump-beleidslijnen maken om toegang tot Jumpitems te beheren](https://www.beyondtrust.com/docs/privileged-remote-access/how-to/jumpoint/policies.htm) op <https://www.beyondtrust.com/docs/privileged-remote-access/how-to/jumpoint/policies.htm> voor meer informatie.

De toegevoegde Jumpgroepen worden in een tabel weergegeven. U kunt de instellingen van een Jumpgroep bewerken of de Jumpgroep van de lijst verwijderen.

Jumpgroep-lidmaatschappen verwijderen

Zoek naar Jumpgroepen waarvan leden van dit groepsbeleid moeten worden verwijderd en klik vervolgens op **Toevoegen**. De verwijderde Jumpgroepen worden in een tabel weergegeven. U kunt een Jumpgroep van de lijst verwijderen.

Accountlidmaatschappen voor Vault toevoegen

Zoek een account, selecteer de **Vault-accountrol** en klik vervolgens op **Toevoegen** om leden van het beleid toegang te verlenen tot het geselecteerde vault-account. Andere groepsbeleidslijnen kunnen lidmaatschappen van gebruikers toevoegen. Bekijk **Vault > Accounts** om alle leden binnen elk account te zien. Gebruikers kunnen een van deze twee rollen toegewezen krijgen voor het gebruik van het vault-account:

- **Injecteren** (standaardwaarde): Gebruikers met deze rol kunnen dit account gebruiken in Privileged Remote Access-sessies.
- **Injecteren en uitchecken**: Gebruikers met deze rol kunnen dit account gebruiken in Privileged Remote Access-sessies en het account uitchecken op **/login**. De machtiging **Uitchecken** heeft geen invloed op generieke SSH-accounts.



Opmerking: Activeer de machtiging **Vault-accountlidmaatschappen toevoegen** om een **Vault-accountrol** aan een vault-account in een groepsbeleid toe te wijzen. De **Vault-accountrol** is zichtbaar in de lijst met accounts die worden toegevoegd aan het groepsbeleid.

Accountgroepslidmaatschappen voor Vault toevoegen

Zoek een accountgroep, selecteer de **Vault-accountrol** en klik vervolgens op **Toevoegen** om leden van het beleid toegang te verlenen tot de groep met vault-accounts. Andere groepsbeleidslijnen kunnen lidmaatschappen van gebruikers toevoegen. Bekijk **Vault > Accountgroepen** om alle leden binnen elke groep te zien. Gebruikers kunnen een van deze twee rollen toegewezen krijgen voor het gebruik van de groep vault-accounts:

- **Injecteren** (standaardwaarde): Gebruikers met deze rol kunnen dit account gebruiken in Privileged Remote Access-sessies.
- **Injecteren en uitchecken**: Gebruikers met deze rol kunnen dit account gebruiken in Privileged Remote Access-sessies en het account uitchecken op **/login**. De machtiging **Uitchecken** heeft geen invloed op generieke SSH-accounts.



Opmerking: Activeer de machtiging **Vault-accountgroep toevoegen** om een **Vault-accountrol** aan een groep met vault-accounts in een groepsbeleid toe te wijzen. De **Vault-accountrol** is zichtbaar in de lijst met accountgroepen die worden toegevoegd aan het groepsbeleid.

Opslaan

Klik op **Opslaan** om het beleid te effectueren.

Beleid exporteren

U kunt een groepsbeleid vanuit een site exporteren en die machtigingen naar een beleid op een andere site importeren. Bewerk het beleid dat u wilt exporteren en ga naar de onderkant van de pagina. Klik op **Beleid exporteren** en sla het bestand op.



Opmerking: Als u een groepsbeleid exporteert worden alleen de beleidsnaam, accountinstellingen en machtigingen geëxporteerd. Beleidsleden, teamlidmaatschappen en Jumpoint-lidmaatschappen worden bij het exporteren niet meegenomen.

Beleid importeren

U kunt geëxporteerde beleidsinstellingen naar een andere BeyondTrust-site importeren die het importeren van groepsbeleid ondersteunt. Maak een nieuw groepsbeleid aan of bewerk een bestaand beleid waarvan u de machtigingen wilt overschrijven en ga naar het onderdeel **Beleid importeren** onderaan de pagina. Klik op **Beleidsbestand selecteren**, blader naar het beleidsbestand en klik vervolgens op **Openen**. Nadat het beleidsbestand is geüpload wordt de pagina vernieuwd waarna u wijzigingen kunt aanbrengen. Klik op **Opslaan** om het groepsbeleid te effectueren.



Opmerking: Als u een beleidsbestand in een bestaand groepsbeleid importeert, dan worden eventuele eerder gedefinieerde machtigingen overschreven, met uitzondering van beleidsleden, teamlidmaatschappen en Jumpoint-lidmaatschappen.

Kerberos Keytab: De Kerberos Keytab beheren



Gebruikers en beveiliging

Kerberos Keytab

Kerberos Keytab-beheer

BeyondTrust ondersteunt de eenmalige aanmelding door middel van het Kerberos-verificatieprotocol. Hiermee kunnen gebruikers op de B Series Appliance worden geverifieerd zonder hun inloggegevens in te hoeven voeren. Kerberos-verificatie geldt zowel voor de /login-webinterface als voor de access console.

Om Kerberos met uw B Series Appliance te integreren moet u al een Kerberos-systeem hebben geïmplementeerd of bezig zijn met de implementatie ervan. De vereisten zijn als volgt:

- U moet een werkend Key Distribution Center (KDC) hebben.
- De klokken moeten op alle apparaten, het KDC en de B Series Appliance gesynchroniseerd zijn. Met een Network Time Protocol-server (NTP) is dit eenvoudig te regelen.
- U moet op het KDC een Service Principal-naam (SPN) voor uw B Series Appliance hebben aangemaakt.

Geconfigureerde principals

De sectie **Geconfigureerde principals** bevat een overzicht van alle beschikbare SPN's voor elke keytab die u hebt geüpload.

Als u SPN's beschikbaar hebt, dan kunt u vanaf de pagina **Beveiligingsproviders** een Kerberos-beveiligingsprovider configureren en definiëren welke gebruikers-principals via Kerberos voor het B Series Appliance mogen worden geverifieerd.

Keytab importeren

Upload/Bestand kiezen

Exporteer de keytab voor de SPN vanaf uw KDC en upload deze via de sectie **Keytab importeren** op deze pagina naar het B Series Appliance.

Rapporten

Toegang: Rapport over sessie-activiteit



Rapporten

Toegang

Toegang tot rapporten

Beheerders en bevoorrechte gebruikers kunnen brede, volledige rapporten genereren en ook specifieke filters toepassen om de informatie in de rapporten aan de specifieke behoefte aan te passen.

Rapporttype

Genereer activiteitenrapporten volgens drie aparte rapporttypen: **Sessie**, **Samenvatting** en **Forensische gegevens van sessie** (indien ingeschakeld).

Sessierapport

Bekijk alle toegangssessies die voldoen aan de criteria die u in rapportfilters hebt opgegeven. Sessierapporten bevatten basisinformatie over de sessie plus koppelingen naar sessiedetails, transcripties van chats en video-opnames van scherm delen, Jumps via tunnelprotocol en opdrachtshells.

Sessierapporten bevatten een opname van de transcriptie van de volledige chat, het aantal overgedragen bestanden en bepaalde acties die tijdens de sessie zijn uitgevoerd. Gebeurtenissen in vensters die duidelijke visuele wijzigingen in een sessie voorstellen worden als gebeurtenissen in de sessiedetails opgenomen. Dit betreft hoofdzakelijk veranderingen in het voorgrondvenster, met de naam van het uitvoerbare programma en de schermtitel.

Andere sessie-informatie betreft de duur van de sessie, lokale en externe IP-adressen en informatie over het externe systeem (indien ingeschakeld). Rapporten kunnen online worden bekeken of naar uw lokale systeem worden gedownload.

Als sessie-opname is ingeschakeld, dan kunt u video-opnames van individuele sessies bekijken, inclusief bijschriften van wie op een bepaald punt in de sessie de besturing van de muis en het toetsenbord had. Als opname van Jump via tunnelprotocol is ingeschakeld, kunt u video-opnames van de volledige desktop van de gebruiker bekijken. Als het opnemen van de opdrachtregel is ingeschakeld, kunt u opnames en/of transcripties van de tekst zien voor alle opdrachtshells die tijdens de sessie zijn uitgevoerd. Alle opnamen worden in onbewerkte indeling op het B Series Appliance opgeslagen en naar een gecomprimeerde indeling omgezet tijdens het weergeven of downloaden.

Samenvattingsrapport

Samenvattingsrapporten bieden een overzicht van de sessieactiviteiten in de loop der tijd, gecategoriseerd per gebruiker. Er zijn statistieken voor het totaal aantal uitgevoerde sessies, het gemiddeld aantal sessies per weekdag en de gemiddelde duur van de sessies.

Rapport 'Forensische gegevens van sessies'

Met rapporten met forensische gegevens van toegangssessies kunt u zoeken naar sessiegebeurtenissen tijdens alle toegangssessies. Ook kunt u sessies vinden die de tekst of het trefwoordzin uit het filter bevatten. Er wordt gezocht in chatberichten, opdrachtshell-

opdrachten, bestandsoverdrachten, aanpassingen van bestandssystemen, aanpassingen in het register en titels van vensters op de voorgrond.

Filters

Pas indien nodig filters toe om uit de drie basistypen rapporten meer aangepaste rapporten af te leiden. Schakel naar wens een of meer filters in, maar alleen sessies die aan alle geselecteerde filters voldoen, worden weergegeven.

Sessie-ID of volgnummer

Voor deze unieke identificator is vereist dat u de ID (LSID) of het volgnummer specificeert voor die ene sessie die u zoekt. Dit is vaak handig als u een extern ticketsysteem of CRM-integratie hebt. U kunt dit filter niet met andere combineren.

Datumbereik

Selecteer een startdatum voor het ophalen van rapportagegegevens. Selecteer vervolgens ofwel het aantal dagen waarvoor rapportagegegevens moeten worden opgehaald ofwel een einddatum.

Eindpunt

Filter sessies op computernaam, publiek IP-adres of privé-IP-adres.

Jumpgroep

Filter sessies op Jumpitems die tot een bepaalde Jumpgroep behoren. Als deze optie is geselecteerd, zijn de volgende opties beschikbaar:

- Vind alle sessies die werden gestart via Jumpitems die tot een bepaalde Jumpgroep behoren.
- Vind alle sessies die werden gestart via persoonlijke Jumpitems voor een specifieke gebruiker.
- Vind alle sessies in uw persoonlijke Jumpgroep.

Gebruiker

Selecteer een gebruiker in het vak **Gebruiker zoeken** om sessies te filteren waaraan een specifieke gebruiker deelnam. Schakel **Alleen matchen als de geselecteerde gebruiker de primaire gebruiker van de sessie is** in om alleen sessies te vinden waarin de gebruiker de primaire gebruiker was.

Leveranciersgroep

Vind alle sessies waaraan gebruikers van een leveranciersgroep hebben deelgenomen. Via het zoekveld kunt u naar een specifieke leveranciersgroep zoeken.

Externe code

Filter om rapporten te genereren voor sessies die dezelfde externe code hebben gebruikt.

Alleen voltooide sessies bijvoegen

Filter om alleen sessies bij te voegen die voltooid zijn. Sessies die nog actief zijn, worden niet bijgevoegd.

Rapport teamactiviteit

Datumbereik

Selecteer een startdatum voor het ophalen van rapportagegegevens. Selecteer vervolgens ofwel het aantal dagen waarvoor rapportagegegevens moeten worden opgehaald ofwel een einddatum.

Team

Kies het team waarvoor u de activiteitenlogboeken wilt bekijken.

Bekijk alle teamactiviteit die aan de op de vorige pagina gespecificeerde criteria voldoet. Rapporten over teamactiviteiten bevatten informatie over gebruikers wanneer zij zich bij de access console aan- of afmelden, chatberichten die tussen teamleden werden uitgewisseld, acties waarbij het scherm werd gedeeld tussen gebruikers die in de chat zijn gelogd en gedeelde en gedownloade bestanden.

Vault: Rapport over Vault-account en gebruikersactiviteit



Rapporten

Vault

Resultaten rapporten accountactiviteit Vault

Datumbereik

Selecteer een startdatum voor het ophalen van rapportagegegevens. Selecteer vervolgens ofwel het aantal dagen waarvoor rapportagegegevens moeten worden opgehaald ofwel een einddatum.

Account

Typ een accountnaam of selecteer het account in de dynamische vervolgkeuzelijst om alle gebeurtenissen weer te geven waarbij een specifiek account was betrokken dat in de BeyondTrust Vault is opgeslagen.

Gebruiker

Om alle gebeurtenissen te zien waarbij een specifieke geprivilegieerde gebruiker betrokken is, typt u de naam van de gebruiker in of selecteert u de naam van de gebruiker in de dynamische pop-uplijst.

i Zie voor meer informatie [Technisch Whitepaper BeyondTrust Vault](https://www.beyondtrust.com/docs/privileged-remote-access/how-to/vault/index.htm) op <https://www.beyondtrust.com/docs/privileged-remote-access/how-to/vault/index.htm>.

Opmerking: Als een gebruiker geanonimiseerd is om te voldoen aan normen geeft de **Vault-account activiteit** mogelijk pseudoniemen weer voor gebruikersgegevens of wordt aangegeven dat de informatie is verwijderd. Zie voor meer informatie over het verwijderen en anonimiseren van gegevens omwille van naleving [Naleving: Gegevens anonimiseren om aan de nalegingsvereisten te voldoen](https://www.beyondtrust.com/docs/privileged-remote-access/getting-started/admin/compliance.htm) op <https://www.beyondtrust.com/docs/privileged-remote-access/getting-started/admin/compliance.htm>.

Resultaten rapporten met accountactiviteit Vault

Omdat gebruikers afzonderlijke toegang kunnen krijgen om accounts te gebruiken en uit te checken, maakt het **activiteitenrapport voor Vault-accounts** onderscheid tussen beide. Hierdoor kunnen beheerders het verschil zien tussen een gebruiker die het wachtwoord van het account kan weergeven en een gebruiker die alleen inloggegevens in een sessie kan injecteren.

De kolom **Gegevens** in het **activiteitenrapport voor Vault-accounts** geeft informatie weer met betrekking tot de gebeurtenis. De gebeurtenis **Inloggegevens uitgecheckt** bevat een koppeling **Details** in de nieuwe kolom **Gegevens** als inloggegevens tijdens een sessie werden uitgecheckt. De koppeling verwijst naar het **Detailrapport voor de technische ondersteuningssessie** waarin de inloggegevens werden gebruikt.

Opmerking: Als de inloggegevens via **/login** werden uitgecheckt, bevat de kolom **Gegevens** geen koppeling naar **Details**.

Leveranciers: Rapport over Leverancier-accounts en gebruikersactiviteit



Rapporten

Leveranciers

Resultaten rapporten accountactiviteit Vault

Datumbereik

Selecteer een startdatum voor het ophalen van rapportagegegevens. Selecteer vervolgens ofwel het aantal dagen waarvoor rapportagegegevens moeten worden opgehaald ofwel een einddatum.

Leveranciersgroep

Zoek alle gebeurtenissen met betrekking tot een specifieke leverancier. Rapporten bevatten onder meer: **Tijdstempel**, **Leveranciersgroep**, **Gebeurtenistype**, **Uitgevoerd door** en gekoppelde **Gegevens**. **Gebeurtenistypes** omvatten **Leveranciersgroep** of **Leveranciergebruiker aangevraagd/aangemaakt/verwijderd/afgewezen**.

Naleving: Gegevens uit Privileged Remote Access anonimiseren om aan compliance-normen te voldoen

 Rapporten**Naleving**

BELANGRIJK!

Het tabblad **Naleving** is standaard uitgeschakeld. Neem contact op met de afdeling ondersteuning van BeyondTrust via www.beyondtrust.com/docs/index.htm#support als uw organisatie deze functie wil gebruiken.

Anonimisering van gebruiker

Informatie over gebruikers en de acties die tijdens toegangssessies zijn uitgevoerd, kan worden geanonimiseerd zodat aan privacywetgeving en normen wordt voldaan.

Om deze gegevens anoniem te maken, typt u de gebruikersnaam, schermnaam of e-mailadres en selecteert vervolgens de gebruiker uit de lijst. Klik op **Activiteit ondersteuningstechnicus zoeken**. Als er gegevens worden gevonden, retourneert het systeem een lijst met de informatie die over de gebruiker is gevonden, met daarbij een voorgestelde, willekeurig gegenereerde term als vervanging voor de informatie. Er kan op de voorgestelde term worden geklikt, waarna de melding **Vervanging bewerken** wordt weergegeven. De gegevens kunnen in de melding worden geanonimiseerd door een vervangende term van uw voorkeur voor de gegevens in te voeren. Klik als u klaar bent op **Vervangende term bewerken in gehele geschiedenis** om de term in het gedeelte te vervangen.

De lijst wordt bijgewerkt met de nieuwe vervangende term en toont 'Alle toegangssessies en teamactiviteiten van deze gebruiker worden als geanonimiseerd gemarkeerd in: (datum en tijd)'. Klik nadat u de vervangende termen en tijdstempel hebt gecontroleerd op **Gebruiker verwijderen en anonimiseren** om het anonimiseringsproces voor de gehele software te starten. U bent verplicht om uw schermnaam in te voeren voordat u het anonimiseringsproces start.

BELANGRIJK!

Alle sessieopnames worden als gevolg van het anonimiseringsverzoek verwijderd.

Anonimisering van eindpunt

Informatie over eindpunten die tijdens toegangssessies zijn geopend, alsook over uitgevoerde acties, kan worden geanonimiseerd zodat aan privacywetgeving en normen wordt voldaan.

Voer de naam, de hostnaam en/of het IP-adres van het eindpunt in het veld in om de gegevens te anonimiseren. Schakel het selectievakje **Gedeeltelijke overeenkomst** in als gedeeltelijke overeenkomsten moeten worden vermeld. Klik daarna op **Klantactiviteit zoeken**. Als er gegevens worden gevonden, retourneert het systeem een lijst met de informatie die over het eindpunt is gevonden, waarbij de informatie wordt vervangen door een voorgestelde, willekeurig gegenereerde term. Er kan op de voorgestelde term worden geklikt, waarna de melding **Vervanging bewerken** wordt weergegeven. De gegevens kunnen in de melding worden geanonimiseerd door een vervangende term van uw voorkeur voor de gegevens in te voeren. Klik als u klaar bent op **Vervangende term bewerken in gehele geschiedenis** om de term in het gedeelte te vervangen.

De lijst wordt bijgewerkt met de nieuwe vervangende term en toont 'De geselecteerde toegangssessies worden als geanonimiseerd gemarkeerd in: (datum en tijd)'. Klik nadat u de vervangende termen en tijdstempel hebt gecontroleerd op **Geselecteerde sessies anonimiseren** om het anonimiseringsproces voor de gehele software te starten. U bent verplicht om uw schermnaam in te voeren voordat u het anonimiseringsproces start.

U kunt ook voor **Aangepaste informatie toevoegen** kiezen. U kunt dan aangepaste informatie, zoals bankrekeningnummers, invoeren en zoeken.

**BELANGRIJK!**

Alle sessieopnames worden als gevolg van het anonimiseringsverzoek verwijderd.

Status

Controleer informatie over anonimiseringstaken, inclusief de gevonden en vervangende termen, het soort gegevens dat wordt geanonimiseerd en de status van de taak.

De taakstatus wordt automatisch om de 15 seconden vernieuwd en de status van uitgevoerde verzoeken blijft 24 uur beschikbaar.



Opmerking: Deze statusinformatie is ook beschikbaar in de sessierapporten.



Opmerking: De anonimisering van gegevens zal in omgevingen waarin automatische omschakeling of Atlas is geconfigureerd pas klaar zijn als de synchronisatie heeft plaatsgevonden op alle nodes of back-up B Series Appliances.

Beheer

Software: Een back-up downloaden, software bijwerken



Beheer

Software

Back-upinstellingen

Het is een belangrijke beproefde methode voor herstel na noodgevallen om regelmatig een back-up van uw software-instellingen te maken. BeyondTrust adviseert u om steeds een back-up van uw B Series Appliance-configuratie te maken als u de instellingen wijzigt. Een back-up verkort de tijd tot herstel in geval van een hardwarestoring en stelt BeyondTrust zo nodig in staat om toegang te krijgen tot tijdelijke gehoste services waarop de instellingen van uw laatste back-up zijn behouden.

Back-up wachtwoord

Maak een wachtwoord aan om uw software-back-upbestand met een wachtwoord te beveiligen. Als u ervoor kiest een wachtwoord in te stellen, dan hebt u alleen toegang tot de back-up als u het wachtwoord invoert.

Inclusief logboekgeschiedenis rapportagedata

Als deze optie is aangevinkt, dan bevat uw back-up logboekregistraties van sessies. Als deze optie niet is aangevinkt, dan staan er in uw back-up geen rapportage-gegevens voor sessies.

Back-up downloaden

Bewaar een beveiligde kopie van uw softwareconfiguratie. Bewaar dit bestand op een veilige plaats.

Versleutelings sleutel back-up Vault

De versleutelings sleutel van Vault wordt gebruikt om alle Vault-inloggegevens die op het B Series Appliance zijn opgeslagen te versleutelen en te decoderen. Als u ooit wordt genoodzaakt om configuratiegegevens van een back-up naar een nieuw B Series Appliance te herstellen, moet u ook de versleutelings sleutel van Vault herstellen om de versleutelde Vault-inloggegevens in de back-up van de configuratie te kunnen gebruiken.

Instellingen herstellen

Back-upbestand van de configuratie en versleutelings sleutel voor Vault

Als u een back-up moet herstellen, ga dan naar het allerlaatste back-upbestand dat u hebt bewaard.

Back-upwachtwoord van de configuratie en versleutelings sleutel voor Vault

Als u een wachtwoord voor uw back-upbestand hebt aangemaakt, voer dat dan hier in.

Back-up uploaden

Upload het back-upbestand naar uw B Series Appliance en herstel de instellingen van uw site met de instellingen die in de back-up zijn opgeslagen.



Raadpleeg *Procedures voor back-up* op <https://www.beyondtrust.com/docs/privileged-remote-access/how-to/disaster-recovery/back-up-procedures.htm> voor meer informatie.

Update uploaden

Selecteer een software-updatebestand om handmatig nieuwe softwarepakketten van BeyondTrust te uploaden. U wordt gevraagd te bevestigen dat u het softwarepakket wilt uploaden. In de sectie **Update geüpload** wordt extra informatie weergegeven waarmee u uw geüploade pakket kunt verifiëren. Klik op **Installeren** als u de installatie wilt voltooien of op **Update verwijderen** als u de update van de tijdelijke locatie wilt verwijderen. Als uw updatepakket alleen extra licenties bevat, dan kunt u de update installeren zonder het B Series Appliance opnieuw te starten. Nadat u hebt bevestigd dat u wilt installeren verschijnt op de pagina een voortgangsbalk om u over het algehele installatieproces te informeren. Updates die hier worden gemaakt, werken automatisch alle sites en licenties op uw B Series Appliance bij.



Opmerking: De beheerder van het B Series Appliance kan ook de functie **Controleren op updates** in de B Series Appliance-interface gebruiken om automatisch naar nieuwe softwarepakketten te zoeken en deze te installeren.

Beveiliging: Beveiligingsinstellingen beheren



Beheer

Beveiliging

Wachtwoorden

Minimumlengte wachtwoord

Stel regels in voor lokale gebruikersaccounts voor de lengte van wachtwoorden.

Complexe wachtwoorden vereist

Stel regels in voor lokale gebruikersaccounts voor de complexiteit van wachtwoorden.

Standaard wachtwoordverloop

Stel regels in voor lokale gebruikersaccounts voor hoe vaak wachtwoorden verlopen.

Wachtwoord resetten inschakelen

Sta gebruikers met een geconfigureerd e-mailadres toe wachtwoorden te herstellen. De koppelingen in e-mails voor het opnieuw instellen van uw wachtwoord zijn geldig tot een van de volgende gebeurtenissen plaatsvindt:

- Er is 24 uur verstreken;
- Er wordt op de koppeling geklikt en het wachtwoord wordt met succes opnieuw ingesteld;
- Het systeem verzendt een andere koppeling naar het e-mailadres.

Accountvergrendeling na

Stel het aantal keren in dat een onjuist wachtwoord mag worden ingevoerd voordat de account wordt vergrendeld.

Duur accountvergrendeling

Bepaal hoelang een geblokkeerde gebruiker moet wachten voordat hij of zij opnieuw mag inloggen. U kunt ook vereisen dat een beheerder de gebruiker moet ontgrendelen.

Toegangsconsole

Sessie beëindigen als account wordt gebruikt

Als een gebruiker probeert op de access console in te loggen met een account die al in gebruik is, dan wordt, als het keuzevakje **Sessie beëindigen** is aangevinkt, de vorige verbinding verbroken zodat de gebruiker op de nieuwe verbinding kan inloggen.

Opgeslagen logins activeren

Sta al dan niet toe of de access console de inloggegevens van een gebruiker mag onthouden.

Inactieve gebruiker uitloggen na

Stel de periode in waarna een inactieve gebruiker van de access console wordt uitgelogd om de licentie voor een andere gebruiker vrij te geven.

Meldingen voor waarschuwingen en afmelding na verstrijken van wachttijd inschakelen

Stel deze optie in om een inactieve gebruiker 30 seconden voordat hij wordt uitgelogd een melding te geven. De gebruiker krijgt nog een andere melding nadat hij is uitgelogd.

Gebruiker van sessie verwijderen na inactiviteit

Met deze optie wordt een gebruiker uit een sessie verwijderd na een door u ingestelde periode zonder activiteit. Hiermee worden BeyondTrust-klienten geholpen om aan inactiviteits-eisen te voldoen. De gebruiker wordt gewaarschuwd 1 minuut voordat hij of zij wordt verwijderd en kan de time-out resetten.

Een gebruiker wordt geacht in een sessie actief te zijn als via het tabblad bestandsoverdracht of via de chat-interface bestanden worden overgedragen, of als hij of zij in het tabblad sessie op de muis klikt of een toets indrukt. Het bewegen van de muis alleen geldt niet als activiteit. Zodra de activiteit stopt, begint de timer voor inactiviteit te lopen.

Standaard verificatiemethode voor Access Console

Selecteer de standaard verificatiemethode. De hier geselecteerde verificatiemethode wordt automatisch geselecteerd op de inlogpagina wanneer de gebruiker de volgende keer inlogt bij de access console nadat de instelling is gewijzigd. Gebruikers kunnen desgewenst een andere methode selecteren.

U kunt deze instelling op elk moment wijzigen. U moet wel uitloggen bij de access console en opnieuw inloggen om de wijziging te kunnen zien.

Mobiele Access Console en Privileged Web Access Console toestaan om verbinding te maken

Sta toe dat gebruikers toegang krijgen tot externe systemen via de BeyondTrust access console-app voor iOS of Android, en ook via de privileged web access console, een browsergebaseerde access console.

Klembordsynchronisatiemodus

Met **Klembordsynchronisatiemodus** wordt bepaald hoe gebruikers binnen een sessie met scherm delen klemborden mogen synchroniseren. De beschikbare instellingen zijn als volgt:

- **Automatisch:** Het klembord van de klant en de ondersteuningstechnicus worden automatisch gesynchroniseerd wanneer er bij de ander veranderingen optreden.
- **Handmatig:** De ondersteuningstechnicus moet een van de klembordpictogrammen op de access console aanklikken om inhoud te versturen naar of op te halen van het klembord van het eindpunt

U MOET de software opnieuw starten op de statuspagina om deze instellingen door te voeren.

Beheerders kunnen verhinderen dat ondersteuningstechnici toegang hebben tot het klembord, ze kunnen ondersteuningstechnici toestaan om gegevens te verzenden naar het eindpunt of ze kunnen ondersteuningstechnici toegang in beide richtingen verlenen

(gegevens verzenden en ontvangen). Deze instellingen bepalen welke klembordpictogrammen de ondersteuningstechnicus ziet in de access console wanneer de modus **Handmatig** is geselecteerd en hoe de synchronisatie verloopt in de modus **Automatisch**.

Gedetailleerde controle van toegang tot het klembord kan worden ingesteld voor sessiebeleidslijnen en groepsbeleidslijnen; toegang kan ook worden verleend aan specifieke ondersteuningstechnici. Bekijk onderstaande koppelingen voor elk afzonderlijk geval:

- **Gebruikers: Gebruikersmachtigingen voor een ondersteuningstechnicus of beheerder toevoegen:** Gebruikers en beveiliging > Gebruikers > Toevoegen > Machtigingen voor bijgewoonde en niet-bijgewoonde sessies > Scherm delen
- **Sessiebeleidslijnen: Sessiemachtigingen en prompt-regels instellen:** Gebruikers en beveiliging > Gebruikers > Toevoegen > Machtiging > Scherm delen
- **Groepsbeleidslijnen: Gebruikersmachtigingen op groepen gebruikers toepassen:** Gebruikers en beveiliging > Groepsbeleidslijnen > Toevoegen > Machtigingen voor bijgewoonde sessie [gedefinieerd]



Opmerking: U **MOET** de software opnieuw starten op de statuspagina om deze instellingen door te voeren.

Overig

Dagen voor het behouden van loginformatie

In **Dagen voor het behouden van logboekinformatie** kunt u instellen hoe lang inlog-informatie op het B Series Appliance moet worden opgeslagen. Deze informatie bestaat uit de rapportagegegevens en opnames van sessies. De maximale tijd dat rapportage-gegevens en opnames voor een sessie op een B Series Appliance kan worden bewaard is 90 dagen. Dit is de standaard instelling bij een nieuwe installatie. Het is mogelijk dat voor sommige sessies binnen het retentietijdsframe de sessieopnames niet beschikbaar zijn. Dit komt wellicht door schijfruimtebeperkingen of door de instelling **Dagen voor het behouden van logboekinformatie**.

Het B Series Appliance voert elke dag een onderhoudsscript uit wat ervoor zorgt dat het schijfgebruik de 90% niet overschrijdt. Mocht dat toch gebeuren, dan verwijdert het script sessieopnames op basis van een formule tot het schijfgebruik onder de 90% is. Als de instelling **Dagen voor het behouden van logboekinformatie** recentelijk is gewijzigd, kan het tot 24 uur duren tot de nieuwe instelling in werking treedt.

i Als gegevens of opnames langer moeten worden bewaard dan de geconfigureerde limiet, raadt BeyondTrust gebruik van de **Rapportage-API** (www.beyondtrust.com/docs/privileged-remote-access/how-to/integrations/api/reporting) aan.

Vooraf gedeelde sleutel (code) voor communicatie tussen apparaten

Voer in het veld **Vooraf gedeelde sleutel voor communicatie tussen apparaten** een wachtwoord in om een vertrouwde relatie tussen twee B Series Appliances te maken. Als twee of meer B Series Appliances worden geconfigureerd voor functies als automatische omschakeling of clusteren, dan moeten de sleutels overeenstemmen. De sleutel moet uit ten minste 6 tekens bestaan en moet minstens één hoofdletter, één kleine letter, één cijfer en één speciaal teken bevatten.

Netwerkbeperkingen

Bepaal welke IP-netwerken toegang tot /login en /api en de BeyondTrust access console op uw B Series Appliance moeten kunnen krijgen. Als u netwerkbeperkingen inschakelt, dan kunt u ook afdwingen dat access consoles alleen op bepaalde netwerken mogen worden gebruikt.

Beheerinterface (/login) en API-interface (/api)

- **Netwerkbependingen altijd toepassen:** wanneer dit is geselecteerd hebt u de optie om een acceptatielijst met alleen de toegestane netwerken te maken of een lijst met netwerken die de toegang juist wordt geweigerd. Wanneer deze optie is geselecteerd, kunt u bepalen welke beperkingen, indien van toepassing, moeten worden toegepast op de toegangscodes voor desktop, mobiel en web.
- **Netwerkbependingen nooit toepassen:** wanneer dit is geselecteerd worden er geen beperkingen toegepast en zijn er geen andere opties beschikbaar om beperkingen toe toepassen op de console voor desktop, mobiel en web.

Toegangsconsole voor desktop en mobiel

- **Netwerkbependingen altijd toepassen:** wanneer dit is geselecteerd erft het de netwerkbependingen die zijn ingevoerd voor de beheerinterface.
- **Netwerkbependingen nooit toepassen:** wanneer dit is geselecteerd worden er geen beperkingen toegepast op de console voor desktop en mobiel, maar hebt u wel de optie om beperkingen toe te passen op de web-access console.
- **Netwerkbependingen alleen toepassen op de eerste verificatie van de gebruiker:** Hiermee worden de hierboven geselecteerde beperkingen toegepast, maar alleen wanneer de gebruiker eerst inlogt.

Webconsole (/console)

- **Netwerkbependingen altijd toepassen:** wanneer dit is geselecteerd erft de web-access console de netwerkbependingen die zijn ingevoerd voor de beheerinterface.
- **Netwerkbependingen nooit toepassen:** wanneer dit is geselecteerd worden er geen beperkingen toegepast op de web-access console, zelfs wanneer er beperkingen effectief zijn voor de andere toegangsconsole-methoden.

i Zie voor meer informatie de [Privileged Web Access Console-gids](https://www.beyondtrust.com/docs/privileged-remote-access/getting-started/access-console/web-access/index.htm) op <https://www.beyondtrust.com/docs/privileged-remote-access/getting-started/access-console/web-access/index.htm>.

Poortbeperkingen voor de beheerwebinterface

Stel de poorten in waarvandaan toegang tot uw /login-interface kan worden verkregen.

Proxyconfiguratie

Configureer een proxyserver om de gegevensstroom te controleren voor informatie die vanuit de B Series Appliance wordt verzonden. Dit is van toepassing op uitgaande gebeurtenissen en API-aanroepen.

Proxyprotocol

Configureer HTTP of HTTPS proxytypes voor uitgaande connectiviteit van het B Series Appliance.

Proxyconfiguratie inschakelen

Vink het vakje aan om de uitgaande proxy-instellingen in te inschakelen.

Proxyhost

Voer het IP-adres of de hostnaam van uw proxyserver in.

Proxypoort

Voer de poort in die uw proxyserver gebruikt. De standaardpoort is **1080**.

Gebruikersnaam en wachtwoord van proxy

Als uw proxyserver verificatie vereist, typt u een gebruikersnaam en wachtwoord.

Testen

Klik op **Testen** om te controleren of de configuratie-instellingen correct zijn ingevoerd. Het huidige testresultaat wordt weergegeven in het gedeelte **Laatste testresultaat**. Foutmeldingen geven aan op welke punten de configuratie-instellingen moeten worden aangepast.

Websiteconfiguratie: HTTP-poorten instellen, vereiste inlogovereenkomst inschakelen



Beheer

Websiteconfiguratie

HTTP

Websiteadressen

Stel een of meer DNS-adressen in die worden omgezet naar uw B Series Appliance.

HTTP-poort en HTTPS-poort

Ervaren netwerkspecialisten kunnen in niet-standaard netwerkomgevingen de poorten wijzigen waarlangs het BeyondTrust-verkeer verloopt. Deze poort-instellingen mogen alleen worden aangepast wanneer andere dan de standaard poorten 80 en 443 voor webtoegang worden gebruikt.

Vereiste inlogovereenkomst

Inlogovereenkomst activeren voor de beheerinterface/Access Console

U kunt een inlogovereenkomst activeren die gebruikers moeten accepteren voordat zij toegang krijgen tot de /login-beheerinterface, de access console, of beide. Met de overeenkomst, die u aan kunt passen, kunt u beperkingen en interne beleidsregels specificeren voordat gebruikers mogen inloggen.

Overeenkomst-titel

Pas de titel van de overeenkomst aan.

Overeenkomst-tekst

Geef de tekst voor de inlogovereenkomst.


E-mailconfiguratie: Software configureren om e-mails te verzenden



Beheer

E-mailconfiguratie

E-mailadres

 **Opmerking:** Als een B Series Appliance is aangewezen als een back-up B Series Appliance of een dataverkeer-node, dan wordt de e-mailconfiguratie voor dat B Series Appliance overschreven met de e-mailconfiguratie die op het primaire B Series Appliance is gedefinieerd.

Van adres

Stel het e-mailadres in dat automatisch berichten vanaf uw B Series Appliance verzendt.

SMTP-relayserver

Configureer uw B Series Appliance om met uw SMTP-relayserver samen te werken, zodat automatisch kennisgevingen per e-mail over bepaalde gebeurtenissen kunnen worden verzonden.

SMTP-relayserver

Voer de hostnaam of het IP-adres van uw SMTP-relayserver in.

SMTP-poort

Stel de SMTP-poort voor contact met deze server in.

SMTP-encryptie

Kies **TLS** of **STARTTLS** als uw SMTP-server TLS-versleuteling ondersteunt. Selecteer anders **Geen**.

SMTP-gebruikersnaam

Als uw SMTP-server verificatie vereist, voert u een gebruikersnaam in.

SMTP-wachtwoord

Als uw SMTP-server verificatie vereist, voert u een wachtwoord in.

Contactpersoon Admin

Standaard Contactpersoon Admin e-mailadressen

Voer een of meer e-mailadressen in waar e-mails naartoe moeten worden verzonden. De adressen moeten door een spatie worden gescheiden.

Verzenden dagelijkse communicatiekennisgeving

U kunt het B Series Appliance elke dag een kennisgeving laten verzenden om te controleren of de communicatie van waarschuwingen juist functioneert.

Naast de test-e-mail en de dagelijkse kennisgevingen die u hierboven kunt configureren, worden e-mails verzonden bij de volgende gebeurtenissen:

- Wanneer tijdens een automatische omschakeling de productversie op de primaire node niet overeenkomt met de productversie op de back-up-node.
- Wanneer tijdens een controle van de status van automatische omschakeling een van de volgende problemen wordt gedetecteerd.
 - Het huidige B Series Appliance is de primaire node en in /login is een gedeeld IP-adres geconfigureerd, maar de netwerk-interface ervan is niet ingeschakeld.
 - In /login is een gedeeld IP-adres geconfigureerd, maar dit is in /appliance niet als een IP-adres opgenomen.
 - De back-up-node kon geen contact met de primaire node krijgen en evenmin met de test-IP-adressen die op de pagina **Beheer > Automatische omschakeling** zijn geconfigureerd.
 - De back-up-node kon geen contact met de test-IP-adressen krijgen die op de pagina **Beheer > Automatische omschakeling** zijn geconfigureerd.
 - De back-up-verwerking van de back-up-node is op de pagina **Beheer > Automatische omschakeling** uitgeschakeld.
 - De zelftest van de back-up-node is onverwacht mislukt, wat aangeeft dat het apparaat niet goed functioneert.
 - De back-up-node kon via de hostnaam van de primaire node geen contact met de primaire node krijgen.
 - Automatische omschakeling is uitgeschakeld en de back-up-node kon de primaire node niet testen.
 - Automatische omschakeling is ingeschakeld en de back-up-node kon de primaire node niet testen. De back-up-node wordt automatisch de primaire node als de primaire node geen antwoord meer geeft.
 - Automatische omschakeling is ingeschakeld en de back-up-node wordt automatisch de primaire node omdat de primaire node te lang offline was.
 - Gegevenssynchronisatie van de primaire node naar de back-up-node is op enig moment in de afgelopen 24 uur mislukt.

Een test-e-mail verzenden als de instellingen zijn opgeslagen

Als u direct een test-e-mail wilt ontvangen om te verifiëren of uw SMTP-instellingen juist zijn geconfigureerd, kunt u deze optie inschakelen voordat u op de knop **Opslaan** klikt.

Uitgaande gebeurtenissen: Gebeurtenissen instellen om berichten uit te laten gaan



Beheer

Uitgaande gebeurtenissen

HTTP-geadresseerden

U kunt uw BeyondTrust Appliance B Series configureren om in geval van verschillende gebeurtenissen berichten naar een HTTP-server of naar een e-mailadres te verzenden.

De variabelen die door het B Series Appliance worden verzonden, komen aan als een HTTP POST-methode en kunnen worden benaderd door de methode aan te roepen die in uw coderingstaal wordt gebruikt om POST-gegevens op te halen. Als de server niet met HTTP 200 antwoordt om aan te geven dat de overdracht is geslaagd, zal het B Series Appliance de huidige gebeurtenis opnieuw in de wachtrij plaatsen en het later opnieuw proberen.

Nieuwe HTTP-geadresseerde toevoegen, bewerken, verwijderen

Maak een nieuwe geadresseerde aan, wijzig een bestaande geadresseerde of verwijder een bestaande geadresseerde.

HTTP-geadresseerde toevoegen of bewerken

Naam

Maak een unieke naam aan om deze uitgaande gebeurtenis te identificeren.

URL

Voer de bestemmings-URL in voor de uitgaande gebeurtenis-handler .



Opmerking: *BeyondTrust Cloud-klanten moeten URL's gebruiken die met HTTPS beginnen; alleen poort 443 wordt ondersteund.*

Ingeschakeld

Schakel **Ingeschakeld** in om de gebeurtenis-handler in te schakelen. Schakel het selectievakje **Uitgeschakeld** uit om snel berichten te stoppen voor de gebeurtenis-handler die u hebt ingesteld, zoals tijdens een geplande integratietest.

Een CA-certificaat gebruiken

Als u via een HTTPS-verbinding werkt, dan moet u het basiscertificaat van de certificaatautoriteit uploaden dat door de uitgaande eventserver wordt geadverteerd.

Aangepaste velden verzenden

Als deze optie is ingeschakeld, worden alle aangepaste velden die op de pagina **Aangepaste velden** zijn geconfigureerd in de uitgaande gebeurtenis opgenomen.

Te verzenden gebeurtenissen

Kies welke gebeurtenissen berichten genereren die verzonden moeten worden.

Interval voor opnieuw proberen

Stel in hoe vaak een poging herhaald moet worden als die niet slaagt.

Duur voor opnieuw proberen

Als een gebeurtenis blijft herhalen en steeds niet slaagt, dan kunt u instellen hoe lang moet worden herhaald voordat de poging wordt opgegeven.

E-mailcontact

Voer een of meer e-mailadressen in waar e-mails met kennisgeving naartoe moeten worden verzonden als er een fout optreedt.

E-mailwaarschuwing verzenden na

Stel in hoe lang na het optreden van de fout de e-mail moet worden verzonden. Als het probleem is opgelost voordat deze tijd is verstreken en de gebeurtenis slaagt, dan wordt geen foutkennisgeving verzonden.

E-mailwaarschuwingen opnieuw verzenden

Stel in hoe vaak e-mails over fouten moeten worden verzonden als de fout blijft bestaan.

E-mail-geadresseerden

Nieuwe e-mailontvanger toevoegen, bewerken, verwijderen

Maak een nieuwe geadresseerde aan, wijzig een bestaande geadresseerde of verwijder een bestaande geadresseerde.

Huidige status

Geeft een kort statusbericht van de SMTP-relayserver weer. Zolang het B Series Appliance berichten naar de relayserver kan verzenden, wordt de status als **OK** weergegeven. Anders moet u de instellingen van uw SMTP-relayserver controleren.

Duur voor opnieuw proberen

Als een gebeurtenis blijft herhalen en steeds niet slaagt, dan kunt u instellen hoe lang moet worden herhaald voordat de poging wordt opgegeven.

Geadresseerde voor e-mail toevoegen

Voordat u uw B Series Appliance instelt om berichten over gebeurtenissen naar een e-mailadres te verzenden, moet u controleren of uw B Series Appliance geconfigureerd is om met uw SMTP-relayserver te werken. Ga naar de pagina **Beheer > E-mailconfiguratie** om de instellingen te controleren.

Ingeschakeld

Schakel **Ingeschakeld** in om de gebeurtenis-handler in te schakelen. Schakel het selectievakje **Uitgeschakeld** uit om snel berichten te stoppen voor de gebeurtenis-handler die u hebt ingesteld, zoals tijdens een geplande integratietest.

Naam

Maak een unieke naam aan om deze uitgaande gebeurtenis te identificeren.

E-mailadres

Voer het e-mailadres in waarheen meldingen van geselecteerde gebeurtenissen moeten worden gezonden. U kunt maximaal tien e-mailadressen invoeren, gescheiden door komma's.

Externe code vereisen

Als deze optie is aangevinkt, dan worden e-mails alleen verzonden voor sessies die een externe code hebben op het moment waarop de gebeurtenis optreedt.

Te verzenden gebeurtenissen

Kies welke gebeurtenissen berichten genereren die verzonden moeten worden.

Onderwerp

Pas het onderwerp van deze e-mail aan. Klik op de koppeling onder het veld **Body** om de macro's weer te geven die kunnen worden gebruikt om de tekst in uw e-mails voor uw doeleinden aan te passen.

Bericht

Pas de inhoud van deze e-mail aan. Klik op de koppeling onder het veld **Body** om de macro's weer te geven die kunnen worden gebruikt om de tekst in uw e-mails voor uw doeleinden aan te passen.

Cluster: Atlas-clustertechnologie configureren voor loadbalancing



Beheer

Cluster

Status

Grootschalige geografische implementaties hebben voordeel van BeyondTrust Atlas-clustertechnologie, waarbij één enkele BeyondTrust-site wordt opgezet over meerdere B Series Appliances, die nodes in een cluster worden genoemd. Het hoofd B Series Appliance/primaire node is de plek waar de meeste beheertaken worden uitgevoerd. De dataverkeer-node is een B Series Appliance die een bijdrage levert aan het effectief routeren van uw ondersteunend gegevensverkeer.

Op de primaire node configureert u zowel de primaire node zelf als de dataverkeer-nodes.

i Meer informatie over Atlas vindt u in de [BeyondTrust Atlas-technologiegids](https://www.beyondtrust.com/docs/privileged-remote-access/how-to/atlas/index.htm) op <https://www.beyondtrust.com/docs/privileged-remote-access/how-to/atlas/index.htm>.

Huidige status

Bevestigt de rol van het site-exemplaar van waaruit u de pagina heeft bezocht.

Nu synchroniseren

Synchroniseert de geclusterde B Series Appliances.

Ontbind cluster

Het cluster ontbinden, waarbij effectief ieder B Series Appliance uit de rol in het cluster wordt verwijderd.

Statusgeschiedenis

Toon/verberg het logboek van geclusterde B Series Appliance-berichten.

Dataverkeer-nodes

De methode om dataverkeer-nodes te kiezen

De selector wordt gebruikt om te definiëren hoe een dataverkeer-node wordt gekozen voor een ondersteuningstechnicus of een klant-clientverbinding. De beschikbare methoden voor definitie van de verbinding zijn **Willekeurig**, **A-record opzoeken**, **SRV-record opzoeken**, **IP-Anycast**, en **Tijdzone-verschil**. De keuze van de verbindingmethode is in hoge mate afhankelijk van uw netwerkinfrastructuur, en andere complexe aspecten.

Nieuwe dataverkeer-node toevoegen, node bewerken, node verwijderen

Maak een nieuwe node aan, wijzig een bestaande node of verwijder een bestaande node.

Nieuwe client-verbindingen accepteren

Zorg dat dit is aangevinkt, anders kunnen clients de dataverkeer-node niet gebruiken.

Voeg dataverkeer-node toe

Nieuwe client-verbindingen accepteren

Zorg dat dit is aangevinkt, anders kunnen clients de dataverkeer-node niet gebruiken.

Naam

Maak een unieke naam aan om deze node te identificeren.

Tijdzone-verschil

Wordt alleen gebruikt als **Methode om dataverkeer-nodes te kiezen** is ingesteld op **Tijdzone-verschil**. Dit proces houdt in dat de tijdzone-instelling van de hostmachine wordt gedetecteerd en deze instelling wordt gebruikt om een passende dataverkeer-node te vinden met het kleinste tijdzone-verschil. Het tijdzone-verschil wordt bepaald aan de hand van de instelling van de tijdzone van de klant, relatief aan de gecoördineerde universele tijd (UTC).

Openbaar adres

Voer de poort in die in de DNS door u is ingesteld voor deze node, en vul de poort in die door clients wordt gebruikt om te communiceren met de node.

Intern adres

Dit kan hetzelfde zijn als het openbare adres. Via de uitgebreide configuratie kan optioneel een andere hostnaam worden ingesteld voor communicatie tussen apparaten.

Voorvoegsels van netwerkadres

U kunt dit leeg laten.

Voer voor geavanceerde configuraties voorvoegsels van netwerkadressen in, één per regel, in de vorm van **ip.add.re.ss[/netmask]**. Netmask is optioneel en kan in punt-decimaalindeling vorm worden gegeven of als een integer bitmask. Als netmask achterwege wordt gelaten, wordt uitgegaan van één IP-adres.

Als dit veld is ingevuld, probeert de primaire node een client toe te wijzen aan deze dataverkeer-node als het IP-adres van de client overeenkomt met een van de voorvoegsels van de netwerkadressen. Als het IP-adres van de client overeenkomt met meerdere voorvoegsels van de netwerkadressen, wordt de client toegewezen aan de dataverkeer-node met het langste overeenkomende voorvoegsel. Als de voorvoegsels even lang zijn, wordt een van de overeenkomende dataverkeer-nodes willekeurig gekozen. Als het IP-adres van de client niet overeenkomt met een van de voorvoegsels van de netwerkadressen, wordt de client toegewezen aan de hand van de deconfigurerde methode.

Configuratie primaire node

Primaire node

Naam

Maak een unieke naam aan om deze node te identificeren.

Openbaar adres

Voer de poort in die in de DNS door u is ingesteld voor deze node, en vul de poort in die door clients wordt gebruikt om te communiceren met de node.

Intern adres

Dit kan hetzelfde zijn als het openbare adres. Via de uitgebreide configuratie kan optioneel een andere hostnaam worden ingesteld voor communicatie tussen apparaten.

Maximale client-terugval naar primaire node

Het aantal door u ingestelde clients dat indien nodig kan teruggrijpen naar de primaire node voor dataverkeer.

Automatische omschakeling: Een back-up B Series Appliance instellen voor automatische omschakeling



Beheer

Automatische omschakeling



Opmerking: Deze functie is alleen beschikbaar voor klanten die een B Series Appliance op locatie bezitten. Klanten van BeyondTrust Cloud hebben geen toegang tot deze functie.



Zie voor meer informatie [Privileged Remote Access Configuratie automatische omschakeling](https://www.beyondtrust.com/docs/privileged-remote-access/configuring-automatic-failover) op <https://www.beyondtrust.com/docs/privileged-remote-access/how-to/failover/index.htm>.

Configuratie

Nieuwe verbindingdetails voor Backup-site

Hostnaam of IP-adres

Voer de hostnaam of het IP-adres in van het B Series Appliance die u als back-up wilt gebruiken in een relatie met automatische omschakeling.

Poort

Voer het TLS-poortnummer in waarmee dit primaire B Series Appliance een verbinding met het back-up B Series Appliance kan maken.

Omgekeerde verbindingdetails voor deze primaire site

Hostnaam of IP-adres

Voer de hostnaam of het IP-adres in van dit B Series Appliance die u als primair apparaat wilt gebruiken in een relatie met automatische omschakeling.

Poort

Voer het TLS-poortnummer in waarmee het back-up B Series Appliance een verbinding met dit primaire B Series Appliance kan maken.

Status

Status van deze host

Bekijk de hostnaam van deze site, alsook de status van het primaire exemplaar van de site of de back-up van de site.

Status van peer-host

Bekijk de hostnaam van deze site, alsook de status van het primaire exemplaar van de site of de back-up van de site. Bekijk ook de datum en het tijdstip van de laatste statuscontrole.

Statusgeschiedenis

Vouw een tabel met opgetreden statusgebeurtenissen uit of klap deze in.

Status van de primaire of back-up-site

De tekst geeft een bevestiging dat u zich ofwel op de primaire site of op de back-up-site van uw hostsite bevindt.

Nu synchroniseren

Forceer handmatig een gegevenssynchronisatie vanaf het primaire B Series Appliance naar het back-up B Series Appliance.

Back-up/primair worden

Verwissel met het andere B Series Appliance van rol, waardoor in feite een automatische omschakeling wordt uitgevoerd voor gepland onderhoud of voor een bekende gebeurtenis die voor automatische omschakeling zorgt.

Vink dit vakje aan om een gegevenssynchronisatie uit te voeren vanaf de site op example.com terwijl deze back-up/primair wordt.

Als u de gegevens tussen de twee B Series Appliances wilt synchroniseren voordat u de rollen verwisselt, dan moet u dit vakje aanvinken. Als deze optie wordt geselecteerd, dan wordt de verbinding met alle gebruikers op het bestaande primaire B Series Appliance tijdens de gegevenssynchronisatie verbroken en zijn er geen nieuwe bewerkingen mogelijk totdat het omwisselen is voltooid.

Vink dit vakje aan om een back-up te worden, zelfs als geen verbinding kan worden gemaakt met het andere apparaat op example.com.

U hebt op de primaire site de optie om back-up te worden, zelfs als geen contact met het andere B Series Appliance kan worden verkregen. Als deze optie niet is aangevinkt, dan wordt de automatische omschakeling geannuleerd als beide B Series Appliances voor wat hun rollen bij automatische omschakeling betreft (één primair en één back-up) niet kunnen worden gesynchroniseerd.

Als u bijvoorbeeld weet dat het huidige back-up B Series Appliance online is maar vanwege verbindingproblemen niet door het primaire apparaat kan worden bereikt, dan kunt u deze optie aanvinken om het primaire apparaat back-up te maken nog voordat de netwerkverbinding is hersteld. In dit voorbeeld hebt u ook toegang tot het back-up-apparaat nodig en moet u dat primair maken.

Relaties automatische omschakeling

Verbreuk de relatie voor automatische omschakeling en verwijder elke B Series Appliance van de rol als primair c.q. back-up.

Configuratie primaire of back-up-site

Gedeelde IP-adressen

Stel het gedeelde IP-adres in dat de site gebruikt in geval van een automatische omschakeling door het vakje voor het IP-adres voor automatische omschakeling aan te vinken. Als u de relatie tussen de sites wijzigt, dan worden de aangevinkte IP-adressen uitgeschakeld als een primaire site back-up wordt en ingeschakeld als een back-up-site primair wordt. U moet handmatig de instelling naar het andere apparaat kopiëren omdat de instelling niet wordt gedeeld.

Back-upinstellingen

De instellingen die u hier configureert worden alleen ingeschakeld als de site die u configureert als back-up functioneert.

Als u zich op de primaire site bevindt, selecteer dan **Instellingen voor back-up** > om de pagina met de te configureren velden uit of in te klappen.

Back-upsitebewerkingen activeren

Schakel back-ups van de site in of uit.

Interval voor automatische data-synchronisatie

U kunt de tijden van het interval voor automatische gegevenssynchronisatie handmatig instellen.

Bandbreedtelimiet gegevenssynchronisatie

Stel de parameters in voor de bandbreedte tijdens gegevenssynchronisatie.

Automatische omschakeling activeren

Schakel de automatische omschakeling snel in of uit.

Time-out voor primaire site

Stel in hoe lang de primaire site onbereikbaar moet zijn voordat automatische omschakeling optreedt.

IP-adressen voor netwerkverbindingstest

Voer het IP-adres voor de back-up-site in om te bepalen of het back-up-apparaat het primaire apparaat niet kan bereiken omdat het primaire apparaat offline is of omdat het back-up-apparaat geen netwerkverbinding meer heeft.

API-configuratie: De XML API inschakelen en aangepaste velden configureren



Beheer

API-configuratie

API-configuratie

XML API activeren

U kunt ervoor kiezen de BeyondTrust XML API in te schakelen, waardoor u rapporten kunt maken en opdrachten kunt geven zoals het starten of verplaatsen van sessies vanuit externe toepassingen of om automatisch een back-up van uw softwareconfiguratie te maken.

Toestemming voor HTTP-toegang tot XML API

Standaard is de toegang tot de API met SSL versleuteld. Maar u kunt ervoor kiezen niet-versleutelde HTTP-toegang toe te staan. Vanuit het oogpunt van beveiliging raden wij met klem aan om toegang via HTTP niet toe te staan.



Opmerking: Deze optie is vanaf versie 16.1 afgeschaft en verschijnt niet bij nieuwe gebruikers. De optie is nog wel beschikbaar voor gebruikers die upgraden van een versie voor 16.1 als u de afgeschafte verificatiemethode voor de API blijft gebruiken met een gebruikersaccount. Als u overstapt naar de aanbevolen verificatiemethode met een API-account, moet alle API-verkeer via HTTPS plaatsvinden.

API-accounts

In een API-account worden alle instellingen voor verificatie en autorisatie voor de API client opgeslagen. Om de API te gebruiken is ten minste één API-account vereist, ofwel in samenhang met de integratieclient, met een app van derden of met uw eigen intern ontwikkelde software.



Opmerking: Voorafgaand aan versie 16.1 werd een gebruikersaccount gebruikt voor verificatie met de API. Deze methode is afgeschaft, hoewel er voor klanten die deze methode al gebruiken nog wel ondersteuning is voor compatibiliteit met oudere versies.

API-account toevoegen, bewerken of verwijderen

Maak een nieuwe account aan, wijzig een bestaande account of verwijder een bestaande account.

API-account toevoegen of bewerken

Ingeschakeld

Als deze optie is ingeschakeld, mag dit account verifiëren met de API. Als een account is uitgeschakeld, worden alle OAuth-tokens die bij het account horen onmiddellijk uitgeschakeld.

Naam

Maak een unieke naam aan om dit account te identificeren.

Opmerkingen

Voeg commentaar toe om aan te geven wat het doel is van dit object.

OAuth-client-ID

De OAuth client-ID is een uniek ID dat door het B Series Appliance wordt gegenereerd. Het kan niet worden aangepast. De client-ID beschouwen we als openbare informatie en kan daarom worden gedeeld zonder de beveiliging van de integratie te compromitteren.

OAuth-clientgeheim

Het OAuth-clientgeheim wordt gegenereerd door het B Series Appliance met behulp van een veilig versleutelde pseudo-willekeurige nummergenerator.



Opmerking: Het clientgeheim kan niet worden aangepast, maar het kan wel opnieuw worden gegenereerd op de pagina **Bewerken**. Als een clientgeheim opnieuw wordt gegenereerd en als vervolgens de account wordt opgeslagen, worden alle OAuth-tokens die bij de account horen direct ongeldig. Alle API-oproepen met die tokens kunnen geen toegang tot de API verkrijgen.



Opmerking: De client-ID voor OAuth en het clientgeheim worden gebruikt om OAuth-tokens te maken. Deze zijn nodig voor het verifiëren bij de API.



Raadpleeg de [Handleiding voor API's](https://www.beyondtrust.com/docs/privileged-remote-access/how-to/integrations/api/index.htm) op www.beyondtrust.com/docs/privileged-remote-access/how-to/integrations/api/index.htm voor meer informatie.

Machtigingen

Selecteer de gebieden van de API die deze account mag gebruiken. U kunt voor de **Opdracht API** toegang weigeren, alleen lezen toestaan of volledige toegang geven. Stel ook in of dit account de **Rapportage-API**, de **Back-up-API** de **Configuratie-API** en/of de **API voor Endpoint Credential Manager** kan gebruiken.

Als ECM-groepen zijn ingeschakeld op de site, selecteer dan welke ECM-groep moet worden gebruikt. ECM's die niet aan een groep gekoppeld zijn, vallen onder **Standaard**.

Met de **Configuratie-API** kunt u veelvoorkomende taken voor het beheer en configuratie uitvoeren in **/login**, die geautomatiseerd kunnen worden en gekoppeld kunnen worden aan uw configuratieprocessen.

Met de **SCIM-API** is het mogelijk om gebruikers van een andere beveiligingsprovider te provisioneren. Als u toegang tot de SCIM-API toestaat, wordt de optie **Dragertokens met lange levensduur toestaan** beschikbaar. Het wordt niet aanbevolen om dragertokens met lange levensduur toe te staan tenzij dit vereist wordt door uw SCIM-cliënt, omdat deze dragertokens nooit verlopen. Omdat voor alle overige API-machtigingen tokens vereist zijn met een levensduur van één uur, worden door het toestaan van dragertokens met lange levensduur alle overige API-machtigingen uitgeschakeld.



Ga voor meer informatie naar [Vault Account Configuratie-API's](https://www.beyondtrust.com/docs/privileged-remote-access/how-to/integrations/api/configuration-api.htm) op www.beyondtrust.com/docs/privileged-remote-access/how-to/integrations/api/configuration-api.htm.

Netwerkbeperingen

Lijst met voorvoegsels van netwerkadressen waarvandaan deze account kan worden geverifieerd.



Opmerking: API-accounts zijn niet beperkt door de netwerkadresvoorvoegsels op de pagina **/login > Beheer > Beveiliging**. Ze worden alleen beperkt door de netwerkadresvoorvoegsels die zijn geconfigureerd voor de API-account.

ECM-groepen



Opmerking: Deze functie is alleen beschikbaar als de functie is ingeschakeld toen uw site werd gebouwd. Neem contact op met uw sitebeheerder als de functie niet beschikbaar is.

De functie ECM-groepen biedt ondersteuning voor meerdere referentieproviders die niet verbonden zijn. Met deze functie kan één PRA worden gebruikt om meerdere externe referentieproviders zoals Password Safe of Privileged Identity te integreren. Deze kunnen op verschillende externe locaties gevonden worden via meerdere ECM-exemplaren.

Nieuwe ECM-groepsnaam

Maak een unieke naam aan om deze ECM-groep te identificeren. U kunt maximaal vijftig ECM-groepen configureren.

Ondersteuning: Contact opnemen met BeyondTrust Technical Support



Beheer

Ondersteuning

Contactinformatie ondersteuning van BeyondTrust

De ondersteuningspagina bevat contactinformatie die u nodig hebt als u contact wilt opnemen met een ondersteuningstechnicus van BeyondTrust Technical Support.

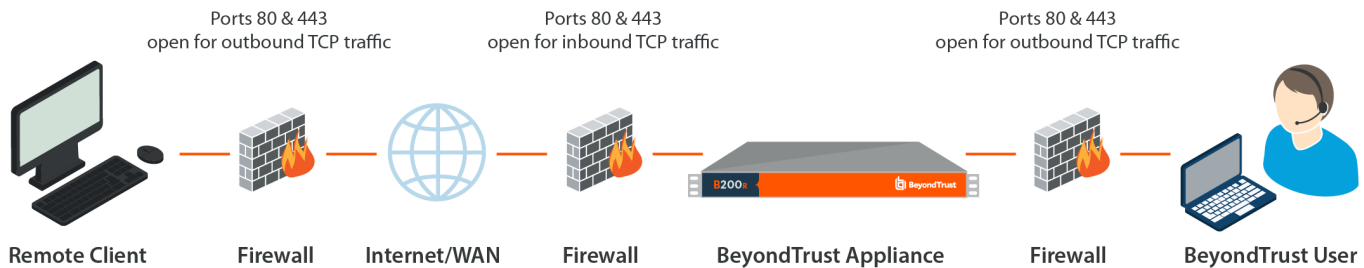
Uitgebreide technische ondersteuning van BeyondTrust

Mocht een ondersteuningstechnicus van BeyondTrust Technical Support toegang tot uw B Series Appliance nodig hebben, dan verstrekt hij of zij u codes voor ondersteuning, toegang en overschrijven die u op deze pagina kunt invoeren om een door het B Series Appliance opgezet en volledig versleuteld ondersteuningskanaal naar BeyondTrust aan te maken, zodat complexe problemen snel kunnen worden opgelost.

Poorten en firewalls

De oplossingen van BeyondTrust zijn ontworpen om firewalls op een transparante manier te gebruiken en een verbinding toe te staan met elke computer met internetverbinding, waar ook ter wereld. Maar bij bepaalde sterk beveiligde netwerken kan enige configuratie noodzakelijk zijn.

TYPICAL NETWORK SETUP



- De poorten 80 en 443 moeten openstaan voor uitgaand TCP-verkeer in zowel de firewall van het externe systeem als van de lokale gebruiker. Afhankelijk van het voor u samengestelde pakket moeten mogelijk meer poorten beschikbaar zijn. Het schema toont een normale netwerkinstelling. Meer informatie hierover vindt u in de [Hardware-installatiegids van het BeyondTrust Appliance B Series](#).
- Beveiligingssoftware voor internet, zoals softwarefirewalls, mogen het downloaden van uitvoerbare bestanden van BeyondTrust niet blokkeren. Voorbeelden van software firewalls zijn McAfee Security, Norton Security en Zone Alarm. Als u een software firewall hebt, dan krijgt u mogelijk verbindingproblemen. Om zulke problemen te voorkomen, moet u de instellingen van uw firewall zodanig configureren dat de volgende uitvoerbare bestanden worden toegestaan. Hierin is {uid} een unieke identicator bestaande uit een letter en cijfers:
 - bomgar-scc-{uid}.exe
 - bomgar-scc.exe
 - bomgar-pac-{uid}.exe
 - bomgar-pac.exe
 - bomgar-pec-{uid}.exe
 - bomgar-pec.exe

Neem contact op met de leverancier van uw firewallsoftware voor assistentie.

- Voorbeelden van regels voor firewalls op basis van de locatie van een B Series Appliance zijn te vinden op www.beyondtrust.com/docs/privileged-remote-access/getting-started/deployment/dmz/firewall-rules.htm.

Neem contact op met BeyondTrust Technical Support via www.beyondtrust.com/support als u nog steeds problemen ondervindt bij het maken van een verbinding.

Vrijwaringen, beperkingen voor licenties en technische ondersteuning

Vrijwaringen

Dit document is uitsluitend informatief. BeyondTrust Corporation behoudt zich het recht voor om de inhoud van dit document zonder kennisgeving te wijzigen. Dit document is niet gegarandeerd foutloos en het bevat geen andere garanties of voorwaarden, al dan niet mondeling of wettelijk impliciet, inclusief impliciete garanties en voorwaarden voor verkoopbaarheid of geschiktheid voor een bepaald doel. BeyondTrust Corporation sluit expliciet elke aansprakelijkheid uit met betrekking tot dit document. Het document vormt geen enkele contractuele verbintenis, direct noch indirect. De hierin beschreven technologieën, functionaliteit, services en processen kunnen zonder voorafgaande kennisgeving worden gewijzigd.

Alle rechten voorbehouden. Andere op deze pagina genoemde handelsmerken zijn eigendom van hun respectievelijke eigenaars. BeyondTrust is geen handelsbank, beleggingsmaatschappij of deposito-instelling. Het is niet gemachtigd om deposito's of trustrekeningen te aanvaarden en is niet erkend of gereguleerd door een staats- of federale bankautoriteit.

Licentiebeperkingen

Met één BeyondTrust Privileged Remote Access-licentie kan één ondersteuningstechnicus per keer problemen op een onbeperkt aantal externe computers (systemen met of zonder toezicht) oplossen. Hoewel er meerdere accounts kunnen bestaan in één licentie, zijn twee of meer licenties (één per gelijktijdige klantendiensttechnicus) vereist om het mogelijk te maken dat meerdere klantendiensttechnici gelijktijdig problemen oplossen.

Eén licentie voor BeyondTrust Privileged Remote Access biedt toegang tot één eindpuntstelsel. Hoewel deze licentie van het ene systeem naar een ander systeem mag worden overgezet als toegang tot het eerste systeem niet langer nodig is, zijn twee of meer licenties (één per eindpunt) nodig om gelijktijdige toegang tot meerdere eindpunten mogelijk te maken.

Technische ondersteuning

BeyondTrust zet zich in om service van de allerhoogste kwaliteit te bieden door te waarborgen dat onze klanten alles hebben wat zij nodig hebben om zo productief mogelijk te kunnen werken. Neem contact op met BeyondTrust Technical Support via www.beyondtrust.com/support als u ondersteuning nodig hebt.

Technische ondersteuning is beschikbaar wanneer de klant jaarlijks ons onderhoudscontract afneemt.