BeyondTrust

Privileged Remote Access 23.2
Privileged Web-toegangsconsole

TC:12/12/2023

Inhoudsopgave

Privileged Web-toegangsconsolegids

Met de BeyondTrust-privileged web-toegangsconsole kunnen informatie- en cyber security-teams bevoorrechte gebruikers beveiligde toegang op afstand tot kritieke systemen geven –zelfs als die gebruikers geen software in hun eigen computeromgeving mogen installeren. In plaats daarvan kunnen zij toegang tot eindpunten krijgen via de webversie van toegangsconsole. Zo wordt verzekerd dat de noodzakelijke toegang altijd kan worden verleend en kunnen systeembeheerders ervoor zorgen dat vereisten zoals beschikbaarheid en alle interne en externe voorschriften kunnen worden nageleefd zonder de verdedigingslinies van de organisatie tegen cybercriminaliteit te compromitteren.

In deze gids bespreken we specifiek de privileged web-toegangsconsole en hoe deze toegangsconsole in een webbrowser toegang tot eindpunten kan krijgen en andere noodzakelijke functies kan uitvoeren terwijl toch het hoogste beveiligingsniveau wordt gehandhaafd.

> ***Opmerking:*** *Gebruik deze gids pas nadat een beheerder de eerste instelling en configuratie van het B Series Appliance heeft uitgevoerd volgens de beschrijving in de BeyondTrust Appliance B Series Hardware-installatiegids. Neem contact op met BeyondTrust Technical Support via www.beyondtrust.com/support als u ondersteuning nodig hebt.*

Vereisten voor Privileged Web-toegangsconsole

Om de privileged web-toegangsconsole op uw systeem uit te kunnen voeren, moet uw B Series Appliance minimaal softwareversie 15.3 of hoger uitvoeren. De privileged web-toegangsconsole wordt ondersteund op de volgende platformen en browsers:

Platformen

- Windows
- Macintosh
- Linux

Browsers

- Chrome 46+
- Firefox 42+
- Internet Explorer 11+
- Safari 8+
- Windows Edge

BELANGRIJK!

Uw B Series Appliance moet over een geldig SSL-certificaat beschikken dat is ondertekend door een certificaatautoriteit. Neem contact op met BeyondTrust Technical Support nadat u een door een CA ondertekend SSL-certificaat op uw B Series Appliance hebt toegepast. Uw klantendiensttechnicus stelt dan een nieuw softwarepakket samen waarin uw SSL-certificaat is geïntegreerd. U kunt met de bijgewerkte build nadat deze geïnstalleerd is op uw B Series Appliance de BeyondTrust-toegangsconsole op uw apparaat uitvoeren om vanaf vrijwel elke willekeurige plaats toegang tot eindpunten te krijgen.

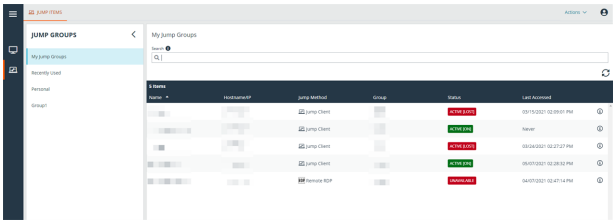
De online Toegangsconsole starten

Met de privileged web-toegangsconsole kunt u veilig eindpunten toevoegen, openen, bewerken en verwijderen door op afstand verbinding te maken via het B Series Appliance. Volg de onderstaande stappen om de console te starten en toegang tot de eindpunten te krijgen via de privileged web-toegangsconsole.

De online Toegangsconsole starten via /console

Dit is de snelste manier om toegang te krijgen tot de webconsole.

1. Voer in de adresbalk van uw browser de hostnaam van uw BeyondTrust-site in, gevolgd door **/console**, bijvoorbeeld **toegang.voorbeeld.nl/console**.
2. Voer de gebruikersnaam en het wachtwoord van uw BeyondTrust-gebruikersaccount in.
3. Klik op **Inloggen** om uw onlinesessie in de toegangsconsole te starten.



Door FIDO2 gecertificeerde verificatoren kunnen worden gebruikt om u veilig zonder wachtwoord aan te melden bij de bureaubladversie van toegangsconsole (alleen Windows), privileged web-toegangsconsole en de /login-beheerinterface. U kunt maximaal 10 verificatoren registreren.

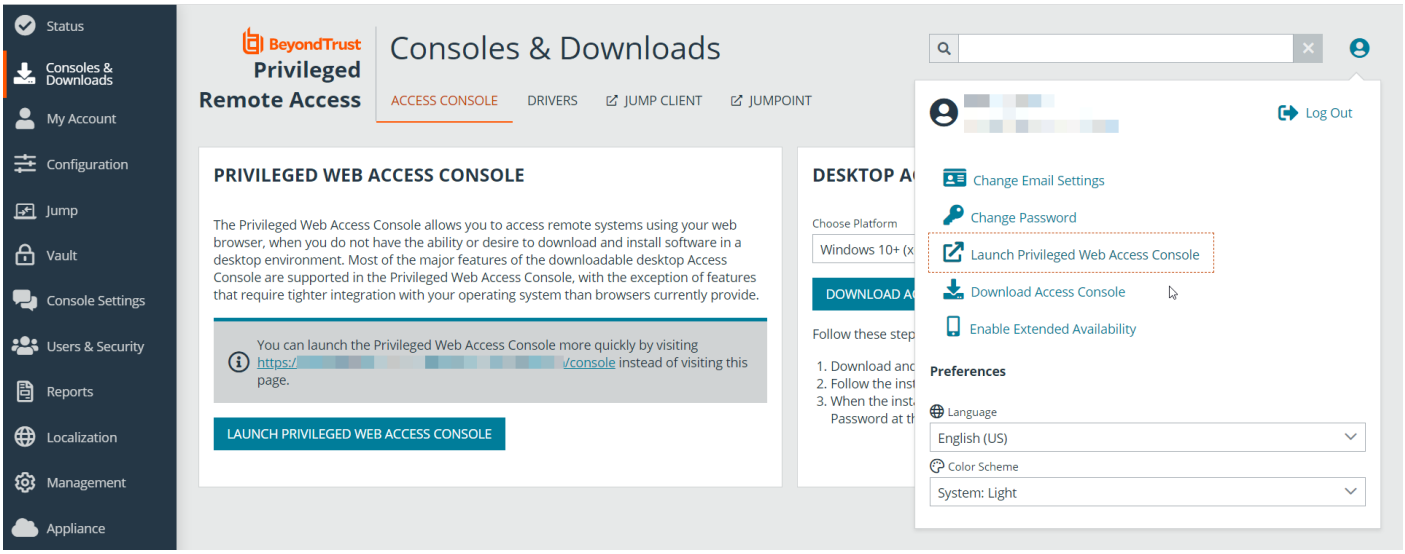
Als aanmelden zonder wachtwoord is ingeschakeld, is **Verifiëren met behulp van** mogelijk standaard ingesteld op **FIDO2 zonder wachtwoord**. Anders kan deze optie worden geselecteerd. Het exacte proces voor aanmelden zonder wachtwoord is afhankelijk van het type apparaat en de fabrikant.

U kunt aanmelden zonder wachtwoord inschakelen en de standaard verificatiemethode instellen nadat u zich hebt aangemeld bij de /login-beheerinterface. Ga vervolgens naar **Beheer > Beveiliging** en registreer wachtwoordloze verificatoren onder **Mijn account > Beveiliging**.

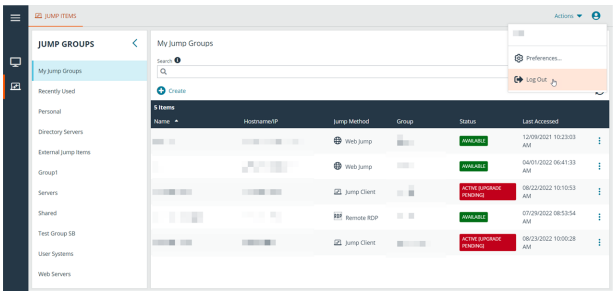
De online Toegangsconsole starten via /login

> ***Opmerking:*** *Deze optie is standaard niet beschikbaar. Ga naar* ***Beheer > Beveiliging*** *en schakel* ***Mobiele Toegangsconsole en Privileged Web-toegangsconsole toestaan om verbinding te maken*** *in om de webconsole te starten vanuit de /login-beheerinterface.*

1. Voer in de adresbalk van uw browser de hostnaam van uw BeyondTrust-site in, gevolgd door **/login**, bijvoorbeeld **toegang.voorbeeld.nl/login**.
2. Voer de gebruikersnaam en wachtwoord van uw BeyondTrust-gebruikersaccount in en klik op **Inloggen** of meld u aan met behulp van verificatie zonder wachtwoord.
3. Klik in het menu aan de linkerkant op **Consoles en downloads** of klik op het gebruikerspictogram in de rechterbovenhoek van het scherm. In de onderstaande afbeelding zijn beide opties geselecteerd.



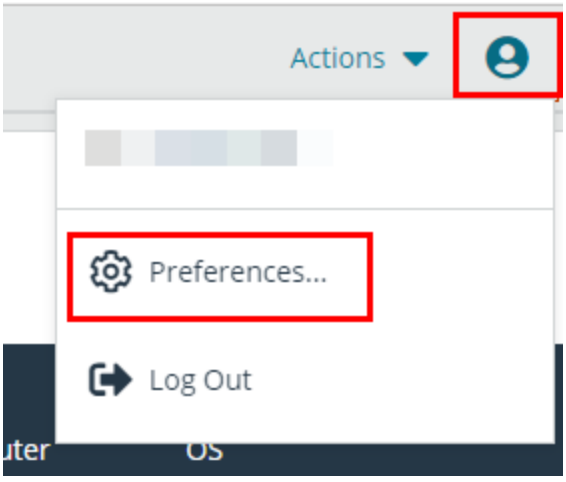
4. Klik op **Privileged Web-toegangsconsole starten** in het scherm **Consoles en downloads** of in het venster met gebruikersopties.
5. De privileged web-toegangsconsole wordt in een nieuw tabblad geopend, waarna u kunt gaan werken met eindpunten.



Klik op het gebruikerspictogram in de rechterbovenhoek van het scherm en klik op **Afmelden** om u af te melden bij de toegangsconsole. U wordt hierdoor niet afgemeld bij de /login-beheerinterface. Klik op het gebruikerspictogram in de rechterbovenhoek van het scherm en klik op **Afmelden** om u af te melden bij de /login-beheerinterface.

Voorkeuren voor Privileged Web-toegangsconsole

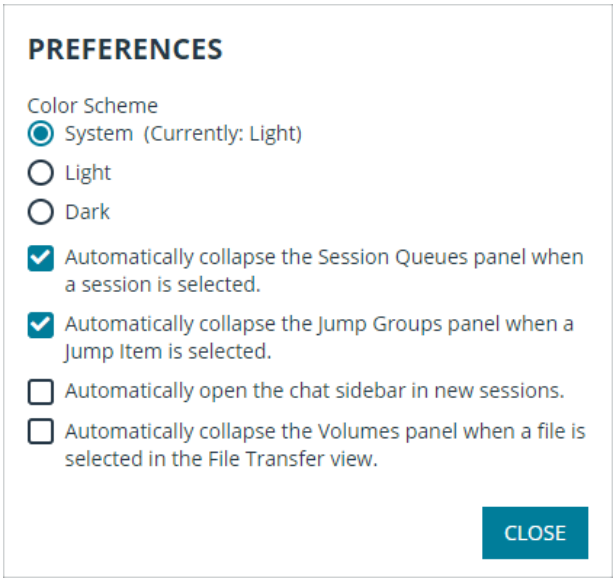
De opties voor taal en kleurenschema die zichtbaar zijn wanneer in de /login-beheerinterface op het gebruikerspictogram wordt geklikt, hebben alleen gevolgen voor die interface. U kunt voorkeuren in de online toegangsconsole instellen door op het gebruikerspictogram in de rechterbovenhoek van de Web toegangsconsole te klikken en vervolgens op **Voorkeuren** te klikken. Selecteer uw voorkeuren in het pop-upvenster.



Selecteer uw favoriete kleurenschema. U kunt schakelen tussen de modi **Licht** en **Donker** en kiezen uit **Systeem**. Deze laatste optie gebruikt de modus die voor uw systeem is geselecteerd.

Selecteer een van de automatische opties die u wilt gebruiken:

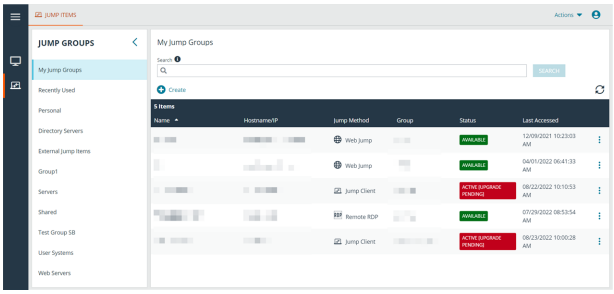
- Het deelvenster **Sessiewachtrijen** automatisch samenvouwen wanneer een sessie is geselecteerd.
- Het deelvenster **Jumpgroepen** automatisch samenvouwen wanneer een Jumpitem is geselecteerd.
- De chat-zijbalk automatisch openen in nieuwe sessies.
- Het deelvenster **Volumes** automatisch samenvouwen wanneer een bestand is geselecteerd in de weergave **Bestandsoverdracht**.



Jumpitems gebruiken voor toegang tot eindpunten in de Privileged Web-toegangsconsole

Installeer een Jumpitem om toegang te krijgen tot een eindpunt. U kunt een Jumpitem installeren door op **Maken** aan de bovenkant van de Jump-interface te klikken. Verderop in deze handleiding staan alle details voor het maken van Jumpitems. Om toegang te krijgen tot een individuele Windows-, Mac- of Linux-computer die niet op een toegankelijk netwerk is aangesloten, moet u vanaf de pagina **/login > Jump > Jump-clients** een Jump-client op dat systeem installeren. Jump-clients worden in de Jump-interface weergegeven, evenals snelkoppelingen naar Jumpitems.

Jumpitems worden weergegeven in Jumpgroepen. Als u aan een of meer Jumpgroepen bent toegewezen, hebt u toegang tot de Jumpitems in die groepen met de machtigingen die uw beheerder u heeft toegekend.



Uw persoonlijke lijst met Jumpitems is voornamelijk bedoeld voor eigen gebruik, hoewel uw teamleiders, teammanagers en gebruikers die alle Jumpitems mogen zien, toegang kunnen hebben tot uw persoonlijke lijst met Jumpitems. Evenzo kunt u, als u een teammanager of teamleider bent met de juiste machtigingen, de persoonlijke lijsten met Jumpitems van uw teamleden zien. Daarnaast kunt u toegangsrechten hebben tot Jumpitems in Jumpgroepen waartoe u niet behoort en de persoonlijke Jumpitems van niet-teamleden.

U kunt op drie manieren toegang krijgen tot eindpunten:

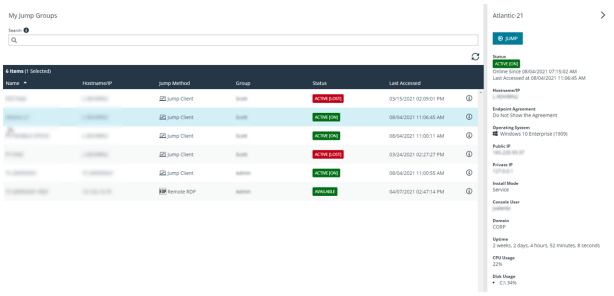
- Zoek en selecteer een eindpunt uit de lijst **Mijn Jumpgroepen**.
- Kies een Jumpgroep en selecteer vervolgens een eindpunt uit de lijst met eindpunten voor die groep.
- Selecteer een sessie uit de lijst **Veel gebruikte Jumpitems**.

> ***Opmerking:*** *In de lijst **Veel gebruikte Jumpitems** worden alle Jumpitems weergegeven waar u regelmatig toegang toe hebt. Om een sessie te starten met een veel gebruikt item, plaatst u de muis boven de sessie en klikt u op **Sessie starten**.*

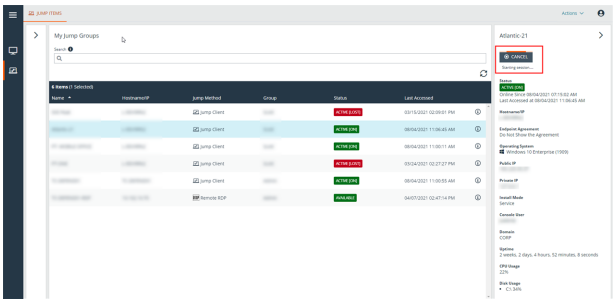
> ***Opmerking:*** *De lijst met Jumpitems kan maximaal 50 Jumpitems weergeven.*

Volg onderstaande stappen om toegang tot een Jumpitem te krijgen:

1. Selecteer een Jumpgroep en klik op de knop **Vernieuwen**.
2. Er wordt een lijst met Jumpitems gevuld, waarin u informatie over het Jumpitem kunt bekijken, zoals: **Naam**, **Methode**, **Groep**, **Status** en **Laatste toegang**. Om meer informatie over het Jumpitem te zien, kunt u op het plus-teken naast de naam van het Jumpitem klikken.
3. Klik op de knop **JUMP** om een sessie met het eindpunt te starten.



4. Om een Jump-toegangsverzoek te annuleren, klikt u op **Annuleren**.

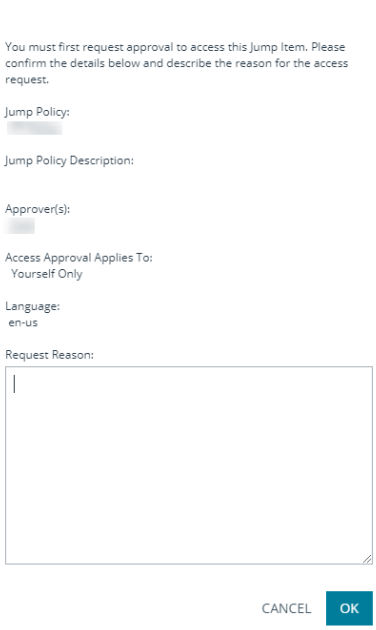


Autorisatie door eindgebruiker of derden

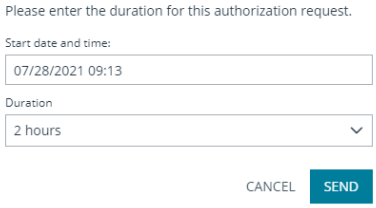
Afhankelijk van de configuratie van Jumpitems binnen de /login-beheerinterface kan er aan een Jumpitem een Jump-beleid zijn geassocieerd en kan er in het beleid een autorisatiecomponent zijn gedefinieerd waarin wordt afgedwongen dat de gebruiker toestemming van een derde partij of een beheerder nodig heeft voordat hij of zij een toegangssessie met het Jumpitem kan starten.

> *Meer informatie over het configureren van kennisgevingen van externe partijen en eindgebruikers en over goedkeuring vindt u in Jump-beleid: Roosters, kennisgevingen en toestemming voor Jumpitems instellen op https://www.beyondtrust.com/docs/privileged-remote-access/getting-started/admin/jump-policies.htm.*

1. Nadat u op de knop **JUMP** hebt geklikt en toegang hebt aangevraagd, verschijnt er een prompt waarin u wordt gevraagd een reden in te voeren waarom u toegang tot het systeem wilt hebben.



2. Vervolgens moet u aangeven wanneer en hoe lang u toegang tot het systeem wilt hebben.
3. Nadat het verzoek is ingediend, krijgt de externe partij of persoon die verantwoordelijk is voor goedkeuring van toegangsverzoeken een waarschuwing via een e-mailmelding, zodat hij of zij het verzoek kan goedkeuren of weigeren. Hoewel andere fiatteurs het e-mailadres kunnen zien van de persoon die het verzoek heeft goedgekeurd of geweigerd, kan de aanvrager dit niet.

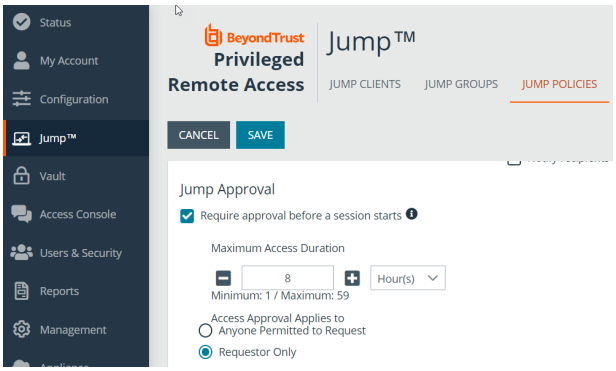


4. Nadat het verzoek is behandeld, wordt in de informatie van het Jumpitem een melding over de machtiging weergegeven met de tekst *goedgekeurd* of *geweigerd*. Als toegang wordt verleend, kan de gebruiker op de knop Jump tikken om toegang tot het systeem te krijgen.
5. U krijgt een bericht te zien met de vraag of u een toegangssessie wilt opstarten.
6. Als u besluit de sessie op te starten, verschijnen de opmerkingen van de goedkeurende partij en kunt u het systeem openen.

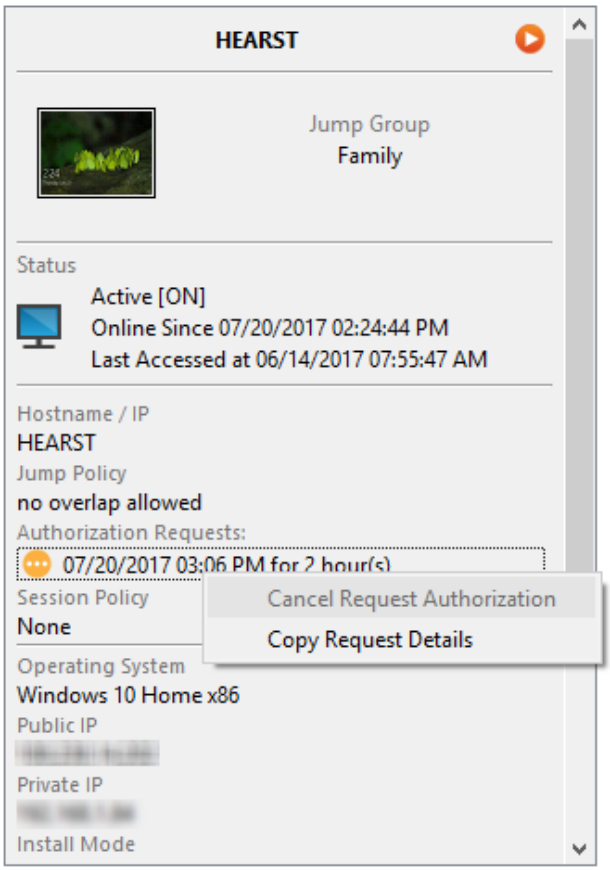
Een goedkeuringsaanvraag voor toegang intrekken

De machtiging om goedgekeurde toegangsverzoeken in te trekken wordt bepaald door het Jump-beleid. Elke gebruiker die aanvragen voor het Jump-beleid kan goedkeuren, kan aanvragen annuleren (afhankelijk van het type goedkeuring). In de **/login** webbeheerinterface gaat u naar **Jump > Jump-beleidslijnen**. Bij **Jump-goedkeuring** hebt u twee opties:

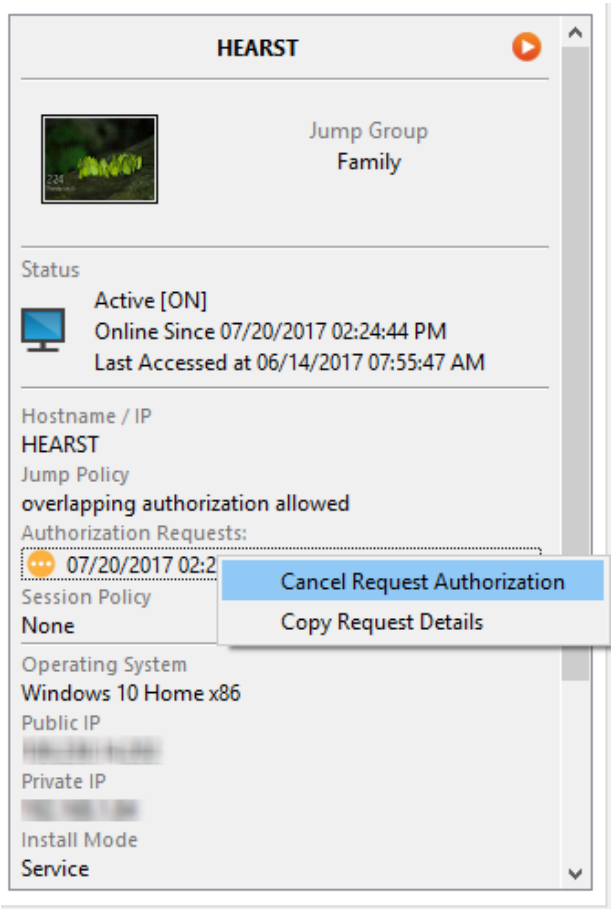
- **Iedereen mag een aanvraag indienen**
- **Alleen verzoeker**



Als het Jump-beleid op **Alleen verzoeker** is ingesteld en er op dat moment een toegangsverzoek voor gebruiker A is goedgekeurd, wordt gebruiker B gevraagd om een nieuw toegangsverzoek aan te maken als deze gebruiker probeert een Jump naar het Jumpitem uit te voeren, aangezien het verzoek niet op B van toepassing is. Bovendien wordt de optie grijs gemaakt (en dus niet beschikbaar) als gebruiker B probeert om het goedkeuringsverzoek voor toegang te annuleren. De enige gebruiker die het goedkeuringsverzoek kan annuleren is gebruiker A, omdat A de goedgekeurde gebruiker voor het verzoek is.



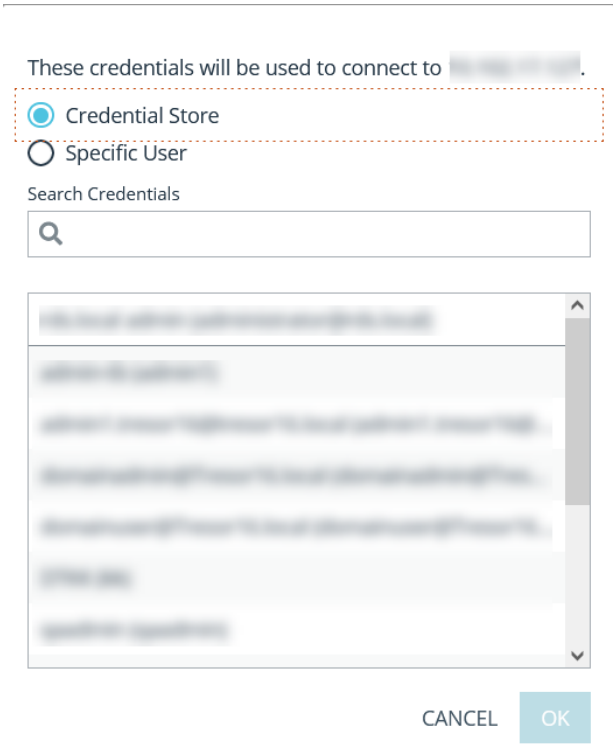
Als het Jump-beleid is ingesteld op **Iedereen mag een aanvraag indienen** en een toegangsverzoek op dat moment is goedgekeurd voor gebruiker A, dan mag gebruiker B een nieuwe sessie met het Jumpitem starten als B probeert een Jump naar dit item uit te voeren. Bovendien mag iedereen met toegangsrechten tot het Jumpitem het verzoek annuleren of intrekken.



Inloggegevens voor automatisch inloggen

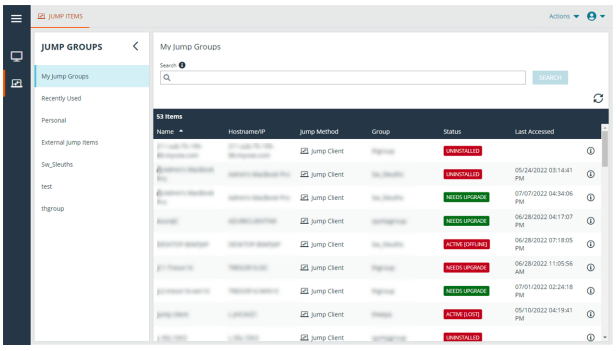
Inloggegevens afkomstig van de **Endpoint Credential Manager** kunnen worden gebruikt voor RDP en voor het uitvoeren van een externe Jump. Als een gebruiker besluit een externe Jump of een externe RDP uit te voeren en er geen automatische inloggegevens beschikbaar zijn, dan moeten er bij de prompt een gebruikersnaam en wachtwoord worden ingevoerd voordat de toegangssessie met het eindpunt kan starten. Als de /login-beheerinterface is geconfigureerd met automatische inloggegevens en antwoordt dat er voor een bepaalde gebruiker en Jumpitem maar één set inloggegevens beschikbaar is, dan wordt het verzoek om inloggegevens overgeslagen en wordt die enkele set inloggegevens gebruikt om de sessie te starten. Als er in de /login-beheerinterface meerdere inloggegevens zijn geconfigureerd, dan kan de gebruiker kiezen om de inloggegevens uit de inloggegevensopslag te gebruiken of om handmatig inloggegevens in te voeren.

Zie voor meer informatie over beheer en configuratie van inloggegevens Beveiliging: Beheer beveiligingsinstellingen op www.beyondtrust.com/docs/privileged-remote-access/getting-started/admin/security.htm.

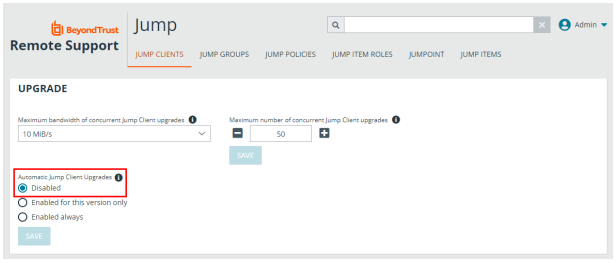


Upgrade van Jump-client

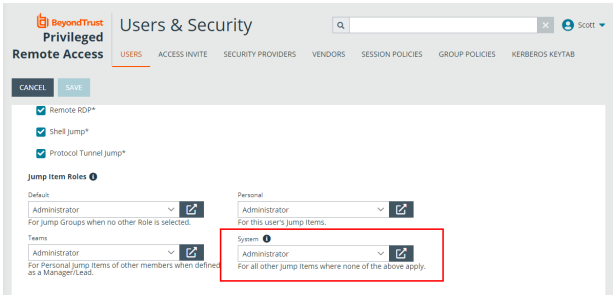
U kunt Jump-clients upgraden vanuit de privileged web-toegangsconsole. Er wordt een banner **Moet worden bijgewerkt** weergegeven onder **Status**. Deze banner is groen als de Jump-client online is en rood als deze offline is. U kunt alleen Jump-clients upgraden die online zijn. Klik op de groene banner om een specifieke Jump-client te upgraden.



Zorg ervoor dat **Automatische upgrades voor Jump-clients** in /login is uitgeschakeld om een Jump-client te kunnen upgraden vanuit de privileged web-toegangsconsole. Ga daarvoor naar **/login > Jump > Jump-clients > Upgrades** en schakel **Automatische upgrades voor Jump-clients** uit. Als automatische upgrades niet zijn uitgeschakeld, wordt er een banner met **Upgrade in behandeling** weergegeven voor Jump-clients die moeten worden geüpgraded.



De ondersteuningstechnicus moet ook het recht hebben om de update uit te voeren. Dit kan worden ingesteld in **/login > Gebruikers en beveiliging > Gebruikers > Toegangsmachtigingen > Jumpitem-rollen**. Zorg dat **Systeem** bovendien is ingesteld op **Beheerder**.



Externe Jump gebruiken voor toegang tot computers zonder toezicht op een ander netwerk

Met Externe Jump kan een bevoorrechte gebruiker verbinding maken met een externe computer zonder toezicht buiten zijn of haar eigen netwerk. Voor Externe Jump is een Jumpoint nodig.

Een Jumpoint werkt als een doorvoerkanaal voor toegang zonder toezicht tot computers die op Windows of Linux draaien op een bekend extern netwerk. Eén enkel Jumpoint geïnstalleerd op een computer binnen een lokaal netwerk kan worden gebruikt om toegang tot meerdere systemen te krijgen, zodat de noodzaak vervalt om vooraf software te installeren op elke computer waartoe u mogelijk toegang zou willen krijgen.

> ***Opmerking:*** *Jumpoint is beschikbaar voor Windows- en Linux-systemen. Jump-clients zijn nodig voor toegang op afstand tot Mac-computers. Om een Jump uit te voeren naar een Windows-computer zonder Jump-client, moet op die computer Remote Registry-service zijn ingeschakeld (op Vista is deze standaard uitgeschakeld) en moet u op een domein zijn aangesloten. U kunt geen Jump uitvoeren naar een mobiel apparaat, ook al is de Jump-technologie beschikbaar vanaf mobiele BeyondTrust-consoles.*

Een snelkoppeling naar een externe Jump aanmaken

Om een snelkoppeling naar een externe Jump te maken, moet u in de Jump-interface op de knop **Aanmaken** klikken. Selecteer uit het vervolgkeuzemenu **Externe Jump**. Snelkoppelingen naar externe Jumps worden in de Jump-interface weergegeven, evenals Jump-clients en andere soorten snelkoppelingen naar Jumpitems.

Organiseer en beheer bestaande Jumpitems door een of meer Jumpitems te selecteren en op **Eigenschappen** te klikken.

> ***Opmerking:*** *Om de eigenschappen van meerdere Jumpitems te bekijken, moeten de geselecteerde items van hetzelfde type zijn (allemaal Jump-clients, allemaal externe Jumps, enz.). Zie de betreffende sectie van deze gids om de eigenschappen van andere typen Jumpitems te bekijken.*

Voer een **Naam** in voor het Jumpitem. Het item is onder deze naam te vinden in de sessietabbladen. Deze tekenreeks mag maximaal 128 tekens lang zijn.

Selecteer vanuit de vervolgkeuzelijst **Jumpoint** het netwerk waarop de computer is aangesloten waar u toegang toe wilt krijgen. De toegangsconsole onthoudt uw gekozen Jumpoint wanneer u de volgende keer dit type Jumpitem maakt. Voer de **Hostnaam/IP** in van het systeem waar u toegang toe wilt krijgen.

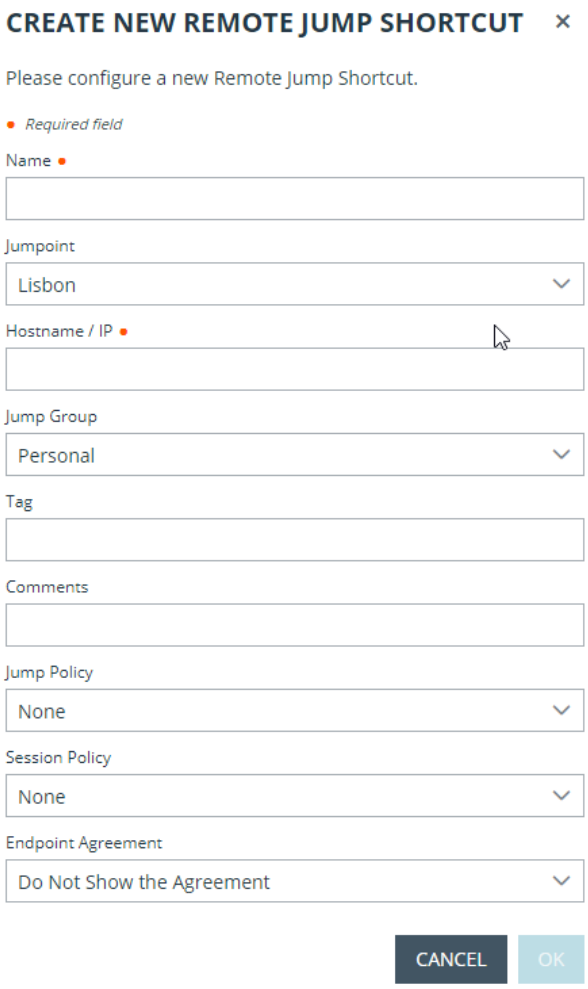
Verplaats Jumpitems van de ene Jumpgroep naar een andere met gebruik van de afrolkeuzelijst **Jumpgroep**. Of u Jumpitems naar of van verschillende Jumpgroepen kunt verplaatsen, hangt van de machtigingen van uw account af.

Organiseer Jumpitems verder door de naam van een nieuwe of bestaande **Tag** in te voeren. Hoewel de geselecteerde Jumpitems samen onder de tag worden gegroepeerd, staan ze nog steeds in een lijst onder de Jumpgroep waarin elk Jumpitem is vastgemaakt. Om een Jumpitem naar het hoogste niveau Jumpgroep terug te zetten, moet dit veld leeg worden gelaten.

Jumpitems bevatten een veld **Opmerkingen** voor een naam of omschrijving, waardoor Jumpitems sneller en eenvoudiger kunnen worden gesorteerd, opgezocht en geïdentificeerd.

U moet een **Jump-beleid** kiezen om in te stellen welke gebruikers toegang tot dit Jumpitem hebben, of een kennisgeving van toegang moet worden verzonden en/of een machtiging of een ticket-ID van uw externe ticketsysteem is vereist om dit Jumpitem te gebruiken. Deze beleidslijnen worden door uw beheerder in de /login-interface ingesteld.

Kies een **Sessiebeleid** om aan dit Jumpitem toe te kennen. Het aan dit Jumpitem toegekende sessiebeleid heeft de hoogste prioriteit bij het instellen van sessiemachtigingen. Of u een sessiebeleid kunt instellen hangt van uw accountmachtigingen af.



Kies een **Eindpuntovereenkomst** om die aan dit Jumpitem toe te wijzen. Afhankelijk van de selectie wordt er een eindpuntovereenkomst weergegeven. Als er geen reactie is, wordt de overeenkomst automatisch geaccepteerd of geweigerd.

Een snelkoppeling naar een externe Jump gebruiken

Om een Jumpsnelkoppeling te gebruiken om een sessie te starten, moet u de snelkoppeling in de Jump-interface selecteren en op de knop **Jump** klikken.

Er wordt een dialoogvenster geopend waar u inloggegevens van een beheerder aan de externe computer kunt verstrekken om de Jump te voltooien. De beheerdersrechten moeten ofwel voor een lokale beheerder op het externe systeem ofwel voor een domeinbeheerder zijn.

De bestanden van de client worden naar het externe systeem gepusht en er wordt geprobeerd een sessie te starten.

Opmerking: *Omdat een externe Jump probeert rechtstreeks verbinding te maken via het apparaat moet het eindsysteem ook kunnen communiceren met het apparaat. Als dat niet het geval is, kunt u de proxyfunctie Jump Zone gebruiken om het verkeer via een proxy naar de Jumpoint door te verwijzen.*

Opmerking: *Jumpitems kunnen zo worden ingesteld dat zij meerdere gebruikers toestaan tegelijkertijd dezelfde Jumpitems te openen. Als* ***Bij bestaande sessie voegen*** *is ingeschakeld, kunnen andere gebruikers een sessie bijwonen die al gaande is. De oorspronkelijke eigenaar van de sessie ontvangt een bericht dat een gebruiker aan de sessie is toegevoegd, maar kan deze gebruiker de toegang niet weigeren. Ga voor meer informatie over gelijktijdige Jumps naar Instellingen voor Jumpitems op www.beyondtrust.com/docs/privileged-remote-access/getting-started/admin/jump-items.htm.*

RDP gebruiken om toegang tot een extern Windows-eindpunt te krijgen

Gebruik BeyondTrust om een RDP-sessie met een extern bureaublad te starten met een extern Windows- of Linux-systeem. Omdat RDP-sessies werken via een Jumpoint dat als proxy fungeert en naar BeyondTrust-sessies worden omgezet, kunnen gebruikers sessies delen of overdragen. Ook kunnen sessies automatisch worden gecontroleerd en opgenomen overeenkomstig de instellingen die uw beheerder voor uw site heeft opgegeven. Om RDP via BeyondTrust te gebruiken, moet u toegang tot een Jumpoint hebben en moet de gebruikersaccount de toestemming hebben **Toegestane Jump-methodes: RDP via een Jumpoint**.

Opmerking: *U kunt uw eigen RDP-hulpprogramma gebruiken voor externe RDP-sessies. Meer informatie vindt u onder Instellingen en voorkeuren in de toegangsconsole wijzigen op https://www.beyondtrust.com/docs/privileged-remote-access/getting-started/access-console/settings.htm.*

BELANGRIJK!

*Om uw eigen hulpmiddel te gebruiken, moet u **Jump via tunnelprotocol** inschakelen in **/login > Gebruikers en beveiliging > Gebruikers > Jump-technologie > Jump via tunnelprotocol**.*

Een RDP-snelkoppeling aanmaken

Om een snelkoppeling naar Microsoft Extern bureaublad (RDP) aan te maken, moet u in de Jump-interface op de knop **Aanmaken** klikken. Selecteer uit het vervolgkeuzemenu **Externe RDP**. RDP-snelkoppelingen worden in de Jump-interface weergegeven naast Jump-clients en andere soorten snelkoppelingen naar Jumpitems.

Organiseer en beheer bestaande Jumpitems door een of meer Jumpitems te selecteren en op **Eigenschappen** te klikken.

Opmerking: *Om de eigenschappen van meerdere Jumpitems te bekijken, moeten de geselecteerde items van hetzelfde type zijn (allemaal Jump-clients, allemaal externe Jumps, enz.). Zie de betreffende sectie van deze gids om de eigenschappen van andere typen Jumpitems te bekijken.*

Voer een **Naam** in voor het Jumpitem. Het item is onder deze naam te vinden in de sessietabbladen. Deze tekenreeks mag maximaal 128 tekens lang zijn.

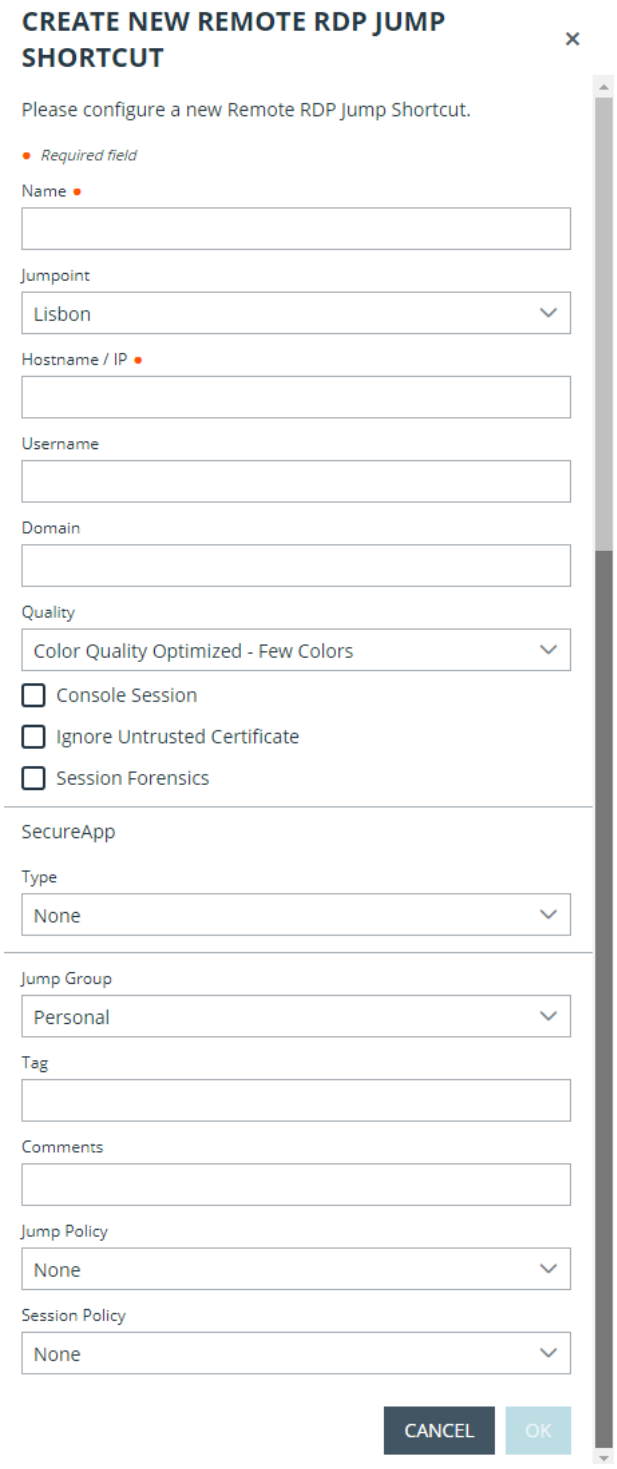
Selecteer vanuit de vervolgkeuzelijst **Jumpoint** het netwerk waarop de computer is aangesloten waar u toegang toe wilt krijgen. De toegangsconsole onthoudt uw gekozen Jumpoint wanneer u de volgende keer dit type Jumpitem maakt. Voer de **Hostnaam/IP** in van het systeem waar u toegang toe wilt krijgen.

Geef de **Gebruikersnaam** om in te loggen evenals het **Domein**.

Selecteer de **Kwaliteit** waarmee u het externe systeem wilt bekijken. Dit kan tijdens de sessie met extern bureaublad (RDP) niet worden gewijzigd. Selecteer de kleuroptimalisatiemodus waarmee u het externe systeem wilt bekijken. Als u vooral videobeelden gaat delen, kies dan **Geoptimaliseerd voor video**. Kies anders uit **Zwart-wit** (gebruikt minder bandbreedte), **Weinig kleuren**, **Meer kleuren** of **Alle kleuren** (gebruikt meer bandbreedte). U kunt met zowel de modus **Geoptimaliseerd voor video** als met de modus **Alle kleuren** de echte bureaubladachtergrond weergeven.

Om een consolesessie te starten in plaats van een nieuwe sessie, kunt u het keuzevakje **Consolesessie** aanvinken.

Als het certificaat van een server niet kan worden geverifieerd, ontvangt u een certificaatwaarschuwing. Als u **Onbetrouwbaar certificaat negeren** aanvinkt, dan kunt u een verbinding met het externe systeem maken zonder dat u dit bericht te zien krijgt.



> ***Opmerking:*** *Wanneer onder het kopje SecureApp de optie* ***Externe app*** *of* ***BeyondTrust Extern bureaublad-agent*** *is geselecteerd, is het selectievakje* ***Consolesessie*** *uitgeschakeld. Externe toepassingen kunnen niet in een consolesessie op een RDP-server worden uitgevoerd.*

Raadpleeg **Forensische gegevens van sessies** voor uitgebreidere informatie over de RDP-sessie. Om deze functie te kunnen gebruiken, moet u een **RDP-serviceaccount** selecteren voor het Jumpoint dat wordt gebruikt. Als u deze instelling controleert, wordt de volgende herinnering weergegeven:

Om deze functie in te schakelen, moet de RDP-server zo worden geconfigureerd dat de controleagent wordt ontvangen, en moet er een RDP-serviceaccount worden geconfigureerd voor dit Jumpoint. Als er niet aan deze voorwaarden is voldaan, zullen alle pogingen om een sessie te starten mislukken.

> ***Opmerking:*** *Bij gebruikelijke installaties vereist het RDP-serviceaccount machtigingen, waaronder toegang voor het maken en beheren van externe services en schrijftoegang op externe bestandssystemen. We adviseren om een AD-account te maken en AD-groepsbeleidsinstellingen te gebruiken om de machtigingen te configureren. De exacte machtigingen zijn echter afhankelijk van uw AD-configuratie.*

Als **Forensische gegevens van sessies** is ingeschakeld, worden de volgende aanvullende gegevens geregistreerd:

- Gewijzigd voorgrondvenster-gebeurtenis
- Muis geklikt-gebeurtenis
- Menu geopend-gebeurtenis
- Nieuw venster geopend-gebeurtenis

Om een sessie met een externe toepassing te starten, moet u het gedeelte **SecureApp** configureren. De volgende vervolgkeuzemenu-opties zijn beschikbaar:

- **Geen:** Wanneer u toegang verkrijgt tot een extern RDP-Jumpitem, wordt er geen toepassing gestart.
- **RemoteApp:** De gebruiker kan een toepassingsprofiel of opdrachtargument configureren, dat wordt uitgevoerd en een toepassing op een externe server opent. Selecteer de optie **RemoteApp** en voer de volgende informatie in om de configuratie uit te voeren:
  - **Naam externe app:** Voer de naam van de toepassing in waarmee u verbinding wilt maken.
  - **Parameters externe app:** Voer de profieldetails of opdrachtregelargumenten in die nodig zijn om de toepassing te openen.
- **BeyondTrust-agent voor extern bureaublad:** Met deze optie is het mogelijk om parameters door te geven via een agent om zo applicaties te starten op een externe host. Selecteer de optie **BeyondTrust-agent voor extern bureaublad** om deze te configureren en voer de volgende informatie in:
  - **Pad met uitvoerbare bestanden:** Voer het pad in van de toepassing waarmee de agent verbinding maakt.
  - **Parameters:** Voer parameters in die u normaal gesproken op een opdrachtregel zou typen wanneer u de app op het externe systeem start.

> *Meer informatie over forensische gegevens voor sessies en het RDP-serviceaccount is te vinden in Jumpoint: Toegang zonder toezicht naar een netwerk instellen > RDP-serviceaccount op https://www.beyondtrust.com/docs/privileged-remote-access/getting-started/admin/jumpoint.htm.*

Inloggegevens injecteren

De optie **Inloggegevens injecteren** is beschikbaar als het type **BeyondTrust-agent voor extern bureaublad** is geselecteerd. Met deze optie is het mogelijk om parameters en ook inloggegevens door te geven via een agent om zo applicaties te starten op een externe host. De eerste set referenties staat in de Jump-definitie. Dit zijn de referenties voor het gebruikersaccount dat u gebruikt om u aan te melden bij het externe systeem. Er is een secundaire prompt voor aanvullende inloggegevens, handmatig geleverd of uit een wachtwoordkluis. Deze secundaire referenties worden beschikbaar gesteld in de opdrachtregel die u definieert via de macro's **%USERNAME%** en **%PASSWORD%** (aanvullende macro's worden hieronder getoond). Hiermee kunt u aanvullende inloggegevens doorgeven aan de toepassing die u opstart (bijv. SQL Server Management Studio). Selecteer de optie **BeyondTrust-agent voor extern bureaublad** om deze te configureren en voer de volgende informatie in:

- Voer het **Pad naar uitvoerbaar bestand** en de **Parameters** in zoals hierboven beschreven.
- **Doelsysteem:** Voer de naam van het systeem in dat de toepassing uitvoert.
- **Type inloggegevens:** Voer het referentietype in zoals gedefinieerd door het referentiebeheersysteem (bijv. SQL).

Macronaam	Resultaat
%USERNAME%	gebruikersnaam
%USERPRINCIPLENAME%	gebruikersnaam@domein
%DOWNLEVELLOGONNAME%	domein\gebruikersnaam
%DOMAIN%	domein
%PASSWORD%	wachtwoord
%PASSWORDRAW%	wachtwoord (zonder poging om speciale tekens te negeren)
%TARGETSYSTEM%	opgegeven waarde voor doelsysteem, in het geval van een SQL-server is dit de naam van de SQL-server.
%APPLICATIONNAME%	optionele toepassingsnaam, in het geval van SQL-server, dit kan worden vastgelegd als 'SQL-server' of iets vergelijkbaars.

Opmerking: *De optie* ***BeyondTrust-agent voor extern bureaublad*** *vereist dat een* ***BeyondTrust-agent voor extern bureaublad*** *op het doelsysteem is geconfigureerd. Deze agent kan worden gedownload van de pagina* ***Mijn account*** *in de interface* ***/login****. Dit is niet versie- of sitespecifiek, waardoor dezelfde agent kan worden gebruikt voor zoveel toepassingen als de beheerder wil ondersteunen. Nadat de agent is geïnstalleerd, kunt u BeyondTrust gebruiken om RDP-Jumpitems te maken die zijn geconfigureerd om de optionele BeyondTrust-agent voor extern bureaublad te gebruiken om geïnstalleerde toepassingen op het externe systeem te starten.*

Opmerking: *SecureApp is afhankelijk van publicatietoepassingen die Microsoft RDS RemoteApps gebruiken. Raadpleeg de documentatie van Microsoft voor publicatietoepassingen.*

Verplaats Jumpitems van de ene Jumpgroep naar een andere met gebruik van de afrolkeuzelijst **Jumpgroep**. Of u Jumpitems naar of van verschillende Jumpgroepen kunt verplaatsen, hangt van de machtigingen van uw account af.

Organiseer Jumpitems verder door de naam van een nieuwe of bestaande **Tag** in te voeren. Hoewel de geselecteerde Jumpitems samen onder de tag worden gegroepeerd, staan ze nog steeds in een lijst onder de Jumpgroep waarin elk Jumpitem is vastgemaakt. Om een Jumpitem naar het hoogste niveau Jumpgroep terug te zetten, moet dit veld leeg worden gelaten.

Jumpitems bevatten een veld **Opmerkingen** voor een naam of omschrijving, waardoor Jumpitems sneller en eenvoudiger kunnen worden gesorteerd, opgezocht en geïdentificeerd.

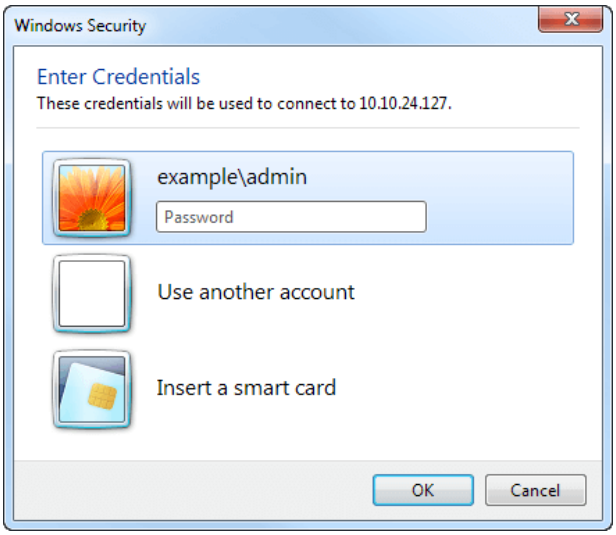
U moet een **Jump-beleid** kiezen om in te stellen welke gebruikers toegang tot dit Jumpitem hebben, of een kennisgeving van toegang moet worden verzonden en/of een machtiging of een ticket-ID van uw externe ticketsysteem is vereist om dit Jumpitem te gebruiken. Deze beleidslijnen worden door uw beheerder in de /login-interface ingesteld.

Raadpleeg Gebruikers van een ingesloten database - uw database mobiel maken op docs.microsoft.com/en-us/sql/relational-databases/security/contained-database-users-making-your-database-portable voor meer informatie over gebruikers van een ingesloten database.

Een RDP-snelkoppeling gebruiken

Om een Jumpsnelkoppeling te gebruiken om een sessie te starten, moet u de snelkoppeling in de Jump-interface selecteren en op de knop **Jump** klikken.

U wordt gevraagd het wachtwoord in te voeren voor de eerder door u opgegeven gebruikersnaam.



Uw RDP-sessie begint nu.

***Opmerking:** Als u een RDP-sessie start, zal het RDP-toetsenbord automatisch de taalinstellingen overnemen die u in de toegangsconsole hebt ingesteld. Deze functionaliteit is alleen beschikbaar op toegangsconsoles op basis van Windows.*

Begin met scherm delen om het externe bureaublad te bekijken. U kunt de opdracht **Ctrl-Alt-Del** verzenden, een schermopname van het externe bureaublad maken, de inhoud van het klembord delen, **Alt-** en **Shift**-opdrachten gebruiken en een sleutelinjectie uitvoeren. U kunt de RDP-sessie ook delen met andere ingelogde BeyondTrust-gebruikers overeenkomstig de gebruikelijke instellingen van uw gebruikersaccount.

***Opmerking:** Jumpitems kunnen zo worden ingesteld dat zij meerdere gebruikers toestaan tegelijkertijd dezelfde Jumpitems te openen. Als deze is ingesteld op **Nieuwe sessie starten**, begint er voor elke gebruiker die een Jump uitvoert naar een specifiek RDP-Jumpitem een nieuwe onafhankelijke sessie. De RDP-configuratie op het eindpunt bepaalt verder gedrag met betrekking tot gelijktijdige RDP-verbindingen. Ga voor meer informatie over gelijktijdige Jumps naar Instellingen voor Jumpitems op www.beyondtrust.com/docs/privileged-remote-access/getting-started/admin/jump-items.htm.*

VNC gebruiken om toegang tot een extern Windows-eindpunt te krijgen

Gebruik BeyondTrust om een VNC-sessie te starten met een extern Windows- of Linux-systeem. Omdat VNC-sessies werken via een Jumpoint dat als proxy fungeert en naar BeyondTrust-sessies worden omgezet, kunnen gebruikers sessies delen of overdragen. Ook kunnen sessies automatisch worden gecontroleerd en opgenomen overeenkomstig de instellingen die uw beheerder voor uw site heeft opgegeven. Om BeyondTrust via VNC te gebruiken, moet u toegang tot een Jumpoint hebben en moet de gebruiker beschikken over de toegangsmachtiging **Toegestane Jump-methoden: Externe VNC via een Jumpoint**.

Een VNC-snelkoppeling aanmaken

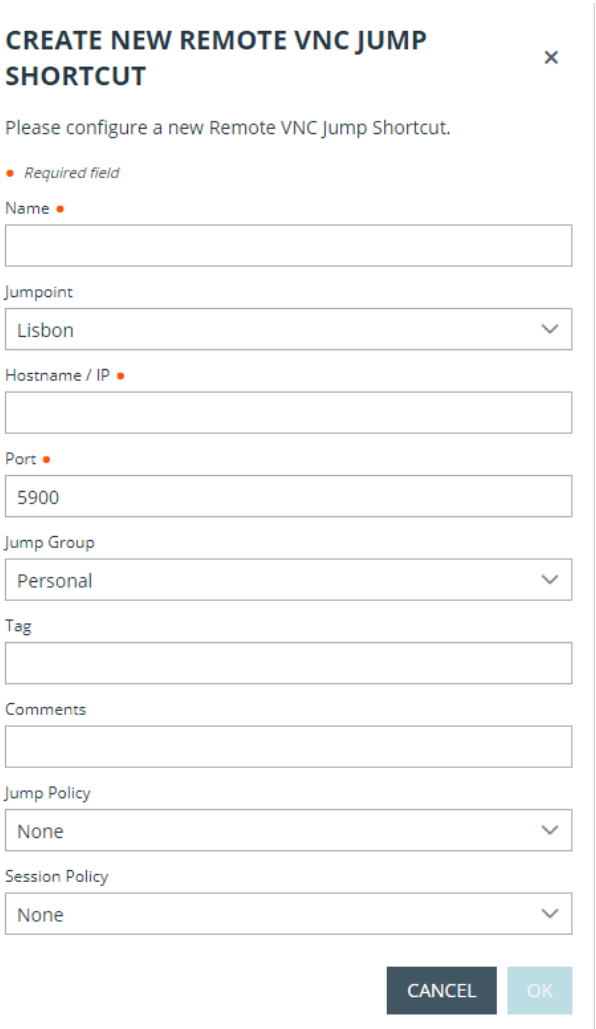
Klik in de Jump-interface op de knop **Aanmaken** om een VNC-snelkoppeling te maken. Selecteer **Externe VNC** in het vervolgkeuzemenu. Snelkoppelingen naar VNC verschijnen in de Jump-interface naast Jump-clients en andere typen Jumpitems.

Organiseer en beheer bestaande Jumpitems door een of meer Jumpitems te selecteren en op **Eigenschappen** te klikken.

> ***Opmerking:*** *Om de eigenschappen van meerdere Jumpitems te bekijken, moeten de geselecteerde items van hetzelfde type zijn (allemaal Jump-clients, allemaal externe Jumps, enz.). Zie de betreffende sectie van deze gids om de eigenschappen van andere typen Jumpitems te bekijken.*

Voer een **Naam** in voor het Jumpitem. Het item is onder deze naam te vinden in de sessietabbladen. Deze tekenreeks mag maximaal 128 tekens lang zijn.

Selecteer vanuit de vervolgkeuzelijst **Jumpoint** het netwerk waarop de computer is aangesloten waar u toegang toe wilt krijgen. De toegangsconsole onthoudt uw gekozen Jumpoint wanneer u de volgende keer dit type Jumpitem maakt. Voer de **Hostnaam/IP** in van het systeem waar u toegang toe wilt krijgen.



> ***Opmerking:*** *Standaard luistert de VNC-server naar poort 5900. Dit is dan ook de standaardpoort voor BeyondTrust. Als de externe VNC-server geconfigureerd is om een andere poort te gebruiken, dan moet u dit poortnummer na de hostnaam of het IP-adres toevoegen in de vorm* ***<hostname>:<port>*** *of* ***<ipaddress>:<port>*** *(bijv. 10.10.24.127:40000).*

Verplaats Jumpitems van de ene Jumpgroep naar een andere met gebruik van de afrolkeuzelijst **Jumpgroep**. Of u Jumpitems naar of van verschillende Jumpgroepen kunt verplaatsen, hangt van de machtigingen van uw account af.

Organiseer Jumpitems verder door de naam van een nieuwe of bestaande **Tag** in te voeren. Hoewel de geselecteerde Jumpitems samen onder de tag worden gegroepeerd, staan ze nog steeds in een lijst onder de Jumpgroep waarin elk Jumpitem is vastgemaakt. Om een Jumpitem naar het hoogste niveau Jumpgroep terug te zetten, moet dit veld leeg worden gelaten.

Jumpitems bevatten een veld **Opmerkingen** voor een naam of omschrijving, waardoor Jumpitems sneller en eenvoudiger kunnen worden gesorteerd, opgezocht en geïdentificeerd.

U moet een **Jump-beleid** kiezen om in te stellen welke gebruikers toegang tot dit Jumpitem hebben, of een kennisgeving van toegang moet worden verzonden en/of een machtiging of een ticket-ID van uw externe ticketsysteem is vereist om dit Jumpitem te gebruiken. Deze beleidslijnen worden door uw beheerder in de /login-interface ingesteld.

Een VNC-snelkoppeling gebruiken

Om een Jumpsnelkoppeling te gebruiken om een sessie te starten, moet u de snelkoppeling in de Jump-interface selecteren en op de knop **Jump** klikken.

Wanneer u verbinding met de VNC-server maakt, probeert het systeem te bepalen of er bijbehorende referenties zijn. Als die inderdaad bestaan, wordt u gevraagd ze in te voeren.

Uw VNC-sessie begint nu. Begin met scherm delen om het externe bureaublad te bekijken. U kunt de opdracht **Ctrl-Alt-Del** verzenden, een schermopname van het externe bureaublad maken en de tekstinhoud van het klembord delen. U kunt de VNC-sessie ook delen, overbrengen of opnemen volgens de gebruikelijke regels voor de instellingen van uw gebruikersaccount.

> ***Opmerking:*** *Jumpitems kunnen zo worden ingesteld dat zij meerdere gebruikers toestaan tegelijkertijd dezelfde Jumpitems te openen. Als* ***Bij bestaande sessie voegen*** *is ingeschakeld, kunnen andere gebruikers een sessie bijwonen die al gaande is. De oorspronkelijke eigenaar van de sessie ontvangt een bericht dat een gebruiker aan de sessie is toegevoegd, maar kan deze gebruiker de toegang niet weigeren. Ga voor meer informatie over gelijktijdige Jumps naar Instellingen voor Jumpitems op www.beyondtrust.com/docs/privileged-remote-access/getting-started/admin/jump-items.htm.*

Shell Jump gebruiken om toegang te krijgen tot een netwerkapparaat op afstand

Met Shell Jump kunt u snel verbinding maken met een netwerkapparaat met SSH of Telnet om de opdrachtregel op dat externe systeem te gebruiken. U kunt bijvoorbeeld een standaardscript in meerdere systemen uitvoeren om een patch te installeren of een netwerkprobleem op te lossen. Beheerders kunnen opdrachtfilters inschakelen om gebruikers te helpen voorkomen dat ze onbedoeld schadelijke opdrachten gebruiken op eindpunten met een SSH-verbinding.

Opmerking: *U kunt uw eigen SSH-hulpprogramma gebruiken voor het SSH-protocol. Meer informatie vindt u onder* *"Instellingen en voorkeuren in de toegangsconsole wijzigen" op pagina 1*.

BELANGRIJK!

Om uw eigen hulpmiddel te gebruiken, moet u ***Jump via tunnelprotocol*** *inschakelen in* ***/login > Gebruikers en beveiliging > Gebruikers > Jump-technologie > Jump via tunnelprotocol***.

Een snelkoppeling naar een Shell Jump aanmaken

Om een snelkoppeling naar een Shell Jump aan te maken, moet u in de Jump-interface op de knop **Aanmaken** klikken. Selecteer in het vervolgkeuzemenu **Shell Jump**. Snelkoppelingen naar Shell Jumps worden in de Jump-interface weergegeven, evenals Jump-clients en andere typen Jumpitem-snelkoppelingen.

Opmerking: *Snelkoppelingen naar Shell Jumps zijn alleen ingeschakeld als het betreffende Jumpoint geconfigureerd is voor open of beperkte toegang via Shell Jump.*

Organiseer en beheer bestaande Jumpitems door een of meer Jumpitems te selecteren en op **Eigenschappen** te klikken.

Opmerking: *Om de eigenschappen van meerdere Jumpitems te bekijken, moeten de geselecteerde items van hetzelfde type zijn (allemaal Jump-clients, allemaal externe Jumps, enz.). Zie de betreffende sectie van deze gids om de eigenschappen van andere typen Jumpitems te bekijken.*

Voer een **Naam** in voor het Jumpitem. Het item is onder deze naam te vinden in de sessietabbladen. Deze tekenreeks mag maximaal 128 tekens lang zijn.

Selecteer vanuit de vervolgkeuzelijst **Jumpoint** het netwerk waarop de computer is aangesloten waar u toegang toe wilt krijgen. De toegangsconsole onthoudt uw gekozen Jumpoint wanneer u de volgende keer dit type Jumpitem maakt. Voer de **Hostnaam/IP** in van het systeem waar u toegang toe wilt krijgen.

Kies het te gebruiken **Protocol**: **SSH** of **Telnet**.

Poort wordt automatisch op de standaardpoort voor het geselecteerde protocol ingesteld, maar kan worden gewijzigd als de instellingen van uw netwerk dit vereisen.

Voer de **Gebruikersnaam** in om u mee aan te melden.

Selecteer het **Type terminal**: **xterm** of **VT100**.

U kunt ook **Keepalive-pakketten verzenden** selecteren om te voorkomen dat niet-actieve sessies stoppen. Voer het aantal seconden in tussen de te verzenden pakketten.

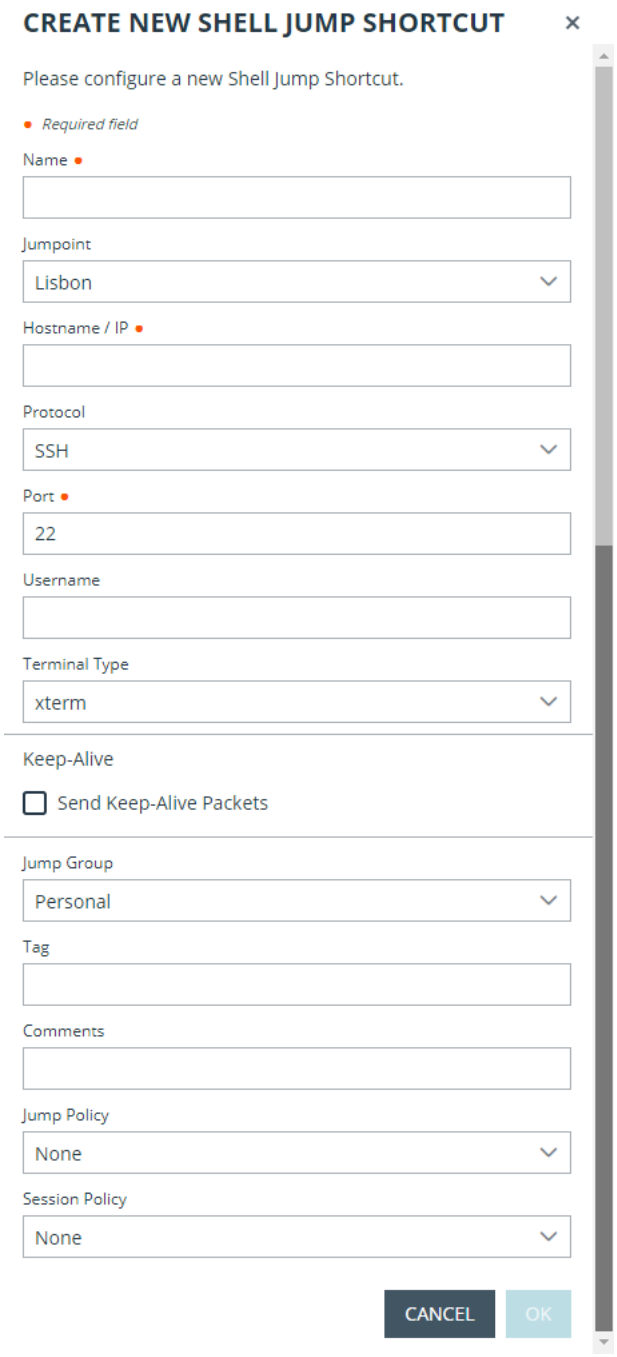
Verplaats Jumpitems van de ene Jumpgroep naar een andere met gebruik van de afrolkeuzelijst **Jumpgroep**. Of u Jumpitems naar of van verschillende Jumpgroepen kunt verplaatsen, hangt van de machtigingen van uw account af.

Organiseer Jumpitems verder door de naam van een nieuwe of bestaande **Tag** in te voeren. Hoewel de geselecteerde Jumpitems samen onder de tag worden gegroepeerd, staan ze nog steeds in een lijst onder de Jumpgroep waarin elk Jumpitem is vastgemaakt. Om een Jumpitem naar het hoogste niveau Jumpgroep terug te zetten, moet dit veld leeg worden gelaten.

Jumpitems bevatten een veld **Opmerkingen** voor een naam of omschrijving, waardoor Jumpitems sneller en eenvoudiger kunnen worden gesorteerd, opgezocht en geïdentificeerd.

U moet een **Jump-beleid** kiezen om in te stellen welke gebruikers toegang tot dit Jumpitem hebben, of een kennisgeving van toegang moet worden verzonden en/of een machtiging of een ticket-ID van uw externe ticketsysteem is vereist om dit Jumpitem te gebruiken. Deze beleidslijnen worden door uw beheerder in de /login-interface ingesteld.

Kies een **Sessiebeleid** om aan dit Jumpitem toe te kennen. Het aan dit Jumpitem toegekende sessiebeleid heeft de hoogste prioriteit bij het instellen van sessiemachtigingen. Of u een sessiebeleid kunt instellen hangt van uw accountmachtigingen af.



Een snelkoppeling naar een Shell Jump gebruiken

Om een snelkoppeling naar een Shell Jump te gebruiken om een sessie op te starten, moet u de snelkoppeling in de Jump-interface selecteren en op de knop **Jump** klikken.

Als er wordt geprobeerd om een Shell Jump uit te voeren naar een SSH-apparaat zonder een in het cachegeheugen opgeslagen hostsleutel, krijgt u een waarschuwing dat de hostsleutel van de server niet in het cachegeheugen is opgeslagen en dat niet kan worden gegarandeerd dat de server de computer is die u denkt dat hij is.

Als u voor **Sleutel opslaan en verbinden** kiest, wordt de sleutel in het cachegeheugen op het hostsysteem van de Jumpoint opgeslagen, zodat deze waarschuwing niet wordt weergegeven bij toekomstige pogingen om een Shell Jump naar dit systeem te gebruiken. **Alleen verbinden** start de sessie zonder de sleutel in het cachegeheugen op te slaan. **Afbreken** beëindigt de Shell Jump-sessie.

Als u een Shell Jump naar een extern apparaat uitvoert, start er direct een sessie met opdrachtshell voor dat apparaat. Er wordt niet om een wachtwoord gevraagd als u een Shell Jump uitvoert naar een geïmplementeerd SSH-apparaat met een onversleutelde sleutel of een versleutelde sleutel waarvan het wachtwoord in het cachegeheugen is opgeslagen. Anders moet u een wachtwoord invoeren. U kunt vervolgens opdrachten naar het externe systeem verzenden.

Als u een Shell Jump uitvoert naar een SSH-apparaat waarop interactieve MFA met behulp van een toetsenbord is ingeschakeld, wordt er een secundaire inputprompt weergegeven.

Beheerders kunnen opdrachtfiltering configureren op Shell Jumpitems om bepaalde opdrachten te blokkeren en andere toe te staan, om te proberen te voorkomen dat de gebruiker onbedoeld een opdracht gebruikt die ongewenst resultaat tot gevolg kan hebben. Wanneer een gebruiker probeert een opdracht te gebruiken die overeenkomt met een expressie die niet is toegestaan, ontvangt hij of zij een melding en mag de opdracht niet worden uitgevoerd.

> ***Opmerking:*** *Het opdrachtfilter van BeyondTrust gebruikt uitgebreide reguliere expressies –niet te verwarren met* ***egrep****. Kijk voor meer informatie in Reguliere expressies (C++) op docs.microsoft.com/en-us/cpp/standard-library/regular-expressions-cpp.*

Shell Prompt-filtering configureren:

1. Meld u aan bij de interface /login als gebruiker met machtigingen om Jumpitems en sessiebeleidslijnen te configureren.
2. Blader naar **Jump > Jumpitems** en scroll omlaag naar de sectie **Shell Jump-filtering**.
3. Voer in het tekstvak **Herkende shell-prompts** regexes in om te matchen met de opdrachtshells-prompts op uw eindpunt-systemen, één per regel.

> ***Opmerking:*** *Regeleinden, of nieuwe regels, zijn niet toegestaan binnen de ingevoerde patronen voor opdracht-prompts. Voer, als een eindpunt-systeem een prompt met meerdere regels gebruikt, een expressie in die overeenkomt met alleen de laatste regel van de prompt in het tekstvak.*

4. Klik op **Opslaan**.

> ***Opmerking:*** *Als u de regexes die u wilt gebruiken hebt ingevoerd, kunt u een shell-prompt testen om te bepalen of het overeenkomt met een van de regexes in de lijst. Hiermee kunt u uw regexes testen zonder een sessie te starten. Voer de expressie in het tekstvak* ***Shell-prompt*** *in en klik op de knop* ***Controleren****. Er wordt een kennisgeving weergegeven, ongeacht of de shell-prompt die u hebt ingevoerd overeenkomt met één van de regexes in de lijst.*

Opdrachtfiltering configureren:

1. Blader naar **Gebruikers en beveiliging > Sessiebeleidslijnen** en maak of een nieuw beleid of bewerk een bestaand.

> ***Opmerking:*** *U kunt die ook configureren voor gebruikers- en/of groepsbeleidslijnen.*

2. Zoek de **Opdrachtshell**-instellingen onder het kopje **Machtigingen**.
3. Selecteer, omdat u opdrachtfiltering gaat gebruiken bij Shell Jumpitems, het keuzerondje **Toestaan** om het gebruik van de opdrachtshell toe te staan.
4. Kies uit **Alle opdrachten toestaan**, **Onderstaande opdrachtpatronen toestaan** of **Onderstaande opdrachtpatronen weigeren** en geef in het tekstvak op welke regex-patronen u wilt toestaan of blokkeren.

> ***Opmerking:*** *Nadat u de opdrachtpatronen die u wilt toestaan of blokkeren hebt ingevoerd kunt u de opdrachten testen in het tekstvak **Opdrachtentester**. Er wordt een kennisgeving weergegeven, ongeacht of de opdrachtprompt die u hebt ingevoerd wel of niet mag worden uitgevoerd op het externe systeem op basis van de regexes die gespecificeerd zijn in de lijst.*
>
> *De twee mogelijke berichten zijn:*
>
> - *"De ingevoerde shell-opdracht wordt op basis van uw keuzes toegestaan."*
> - *"De ingevoerde shell-opdracht wordt op basis van uw keuzes niet toegestaan."*

Inloggegevensinjectie gebruiken met SUDO op een Linux-eindpunt

Om inloggegevensinjectie met SUDO te gebruiken, moet een beheerder een of meer functionele accounts op elk Linux-eindpunt configureren voor toegang via Shell Jump. Omdat het configureren van een sudoers-bestand een complex proces is dat verschilt per platform, verwijzen we u naar de documentatie van uw platform voor informatie over het voltooien van dit proces. Iedere functionele account moet:

- Verificatie via SSH toestaan (wachtwoord of SSH-sleutel).
- De referenties voor het account laten opslaan in de Endpoint Credential Manager (ECM).
- Een of meer vermeldingen hebben in **/etc/sudoers** met toestemming voor functionele account-toegang tot een of meer opdrachten om uit te voeren als root zonder een wachtwoord te vereisen (**NOPASSWD**).

Een beheerder moet een Jumpitem voor een Shell Jump voor het eindpunt aanmaken.

Vervolgens moet een beheerder de ECM en/of de wachtwoordkluis configureren om gebruikers toegang te verlenen tot de juiste functionele accounts voor dat Jumpitem.

Als een gebruiker een Jump naar het Jumpitem voor een Shell Jump uitvoert, dan kan hij of zij kiezen uit een lijst met functionele accounts die beschikbaar zijn voor dat eindpunt. Elk functioneel account heeft een eigen set opdrachten die kunnen worden uitgevoerd met SUDO, zoals ingesteld door de beheerder bij het eindpunt. De referenties voor het account worden vanuit de ECM doorgegeven naar het eindpunt.

Opmerking: *Jumpitems kunnen zo worden ingesteld dat zij meerdere gebruikers toestaan tegelijkertijd dezelfde Jumpitems te openen. Als* ***Bij bestaande sessie voegen*** *is ingeschakeld, kunnen andere gebruikers een sessie bijwonen die al gaande is. De oorspronkelijke eigenaar van de sessie ontvangt een bericht dat een gebruiker aan de sessie is toegevoegd, maar kan deze gebruiker de toegang niet weigeren. Ga voor meer informatie over gelijktijdige Jumps naar Instellingen voor Jumpitems op www.beyondtrust.com/docs/privileged-remote-access/getting-started/admin/jump-items.htm.*

Een Web Jump gebruiken voor toegang tot webservices

Met de verspreiding van infrastructuurcomponenten die zijn overgegaan op webgebaseerde interfaces voor configuratie, krijgen IT-beheerders te maken met een steeds complexere beveiligingsbeheersituatie. Met bevoorrechte toegang tot webgebaseerde bronnen is het een uitdaging om goede verificatie te beheren, controleren en handhaven zonder dat de productiviteit van het bedrijf negatief beïnvloed wordt. IT-beheerders hebben een manier nodig om bronnen die worden beheerd via web-interfaces effectief te beheren en controleren, waaronder:

- Extern gehoste IaaS-servers (Infrastructure as a Service) zoals Amazon AWS, Microsoft Azure, IBM Softlayer en Rackspace
- Intern gehoste servers die beheerd worden met hypervisor-software zoals VMware vSphere, Citrix XenServer en Microsoft Hyper-V
- Moderne kern-netwerkinfrastructuur die web-based configuratie-interfaces gebruikt

De mogelijkheden voor beheer van identiteiten en toegang verschillen enorm tussen IaaS, hypervisor-leveranciers en kerninfrastructuursystemen, en veel daarvan hebben geen eigen ondersteuning voor multifactorverificatie en ze missen dus een extra beveiligingslaag. Door deze verschillen tussen systemen ontstaan mogelijke kwetsbaarheden voor het bedrijf, zoals misbruik van accounts en toegang, waardoor gevoelige informatie kan uitlekken. BeyondTrust Web Jump is de extra beveiligingslaag voor verificatie voor deze systemen.

BELANGRIJK!

Web Jump ondersteunt geen Flash. Zorg ervoor dat u de hypervisor-documentatie raadpleegt en het bijwerkt naar een versie die HTML5 ondersteunt.

***Opmerking:** Het Web Jumpitem is een toevoeging voor Privileged Remote Access en moet apart worden aangeschaft.*

Een snelkoppeling naar een Web Jump aanmaken

***Opmerking:** Controleer voordat u snelkoppelingen naar Web Jumps aanmaakt dat uw gebruikersaccount de mogelijkheid heeft voor toegang tot Web Jumps. Deze machtiging is ingesteld op uw gebruikersaccount in de /login-interface onder **Toegangsmachtigingen > Jump-technologie**.*

Om een snelkoppeling naar een Web Jump aan te maken, klikt u in de Jump-interface op de knop **Aanmaken**. Selecteer in het vervolgkeuzemenu **Web Jump**. Snelkoppelingen naar Web Jumps worden in de Jump-interface weergegeven naast Jump-clients en andere soorten snelkoppelingen naar Jumpitems.

Organiseer en beheer bestaande Jumpitems door een of meer Jumpitems te selecteren en op **Eigenschappen** te klikken.

***Opmerking:** Om de eigenschappen van meerdere Jumpitems te bekijken, moeten de geselecteerde items van hetzelfde type zijn (allemaal Jump-clients, allemaal externe Jumps, enz.). Zie de betreffende sectie van deze gids om de eigenschappen van andere typen Jumpitems te bekijken.*

Voer een **Naam** in voor het Jumpitem. Het item is onder deze naam te vinden in de sessietabbladen. Deze tekenreeks mag maximaal 128 tekens lang zijn.

Selecteer vanuit de vervolgkeuzelijst **Jumpoint** het Windows- of Linux-Jumpoint dat als host fungeert voor de computer waar u toegang toe wilt krijgen.

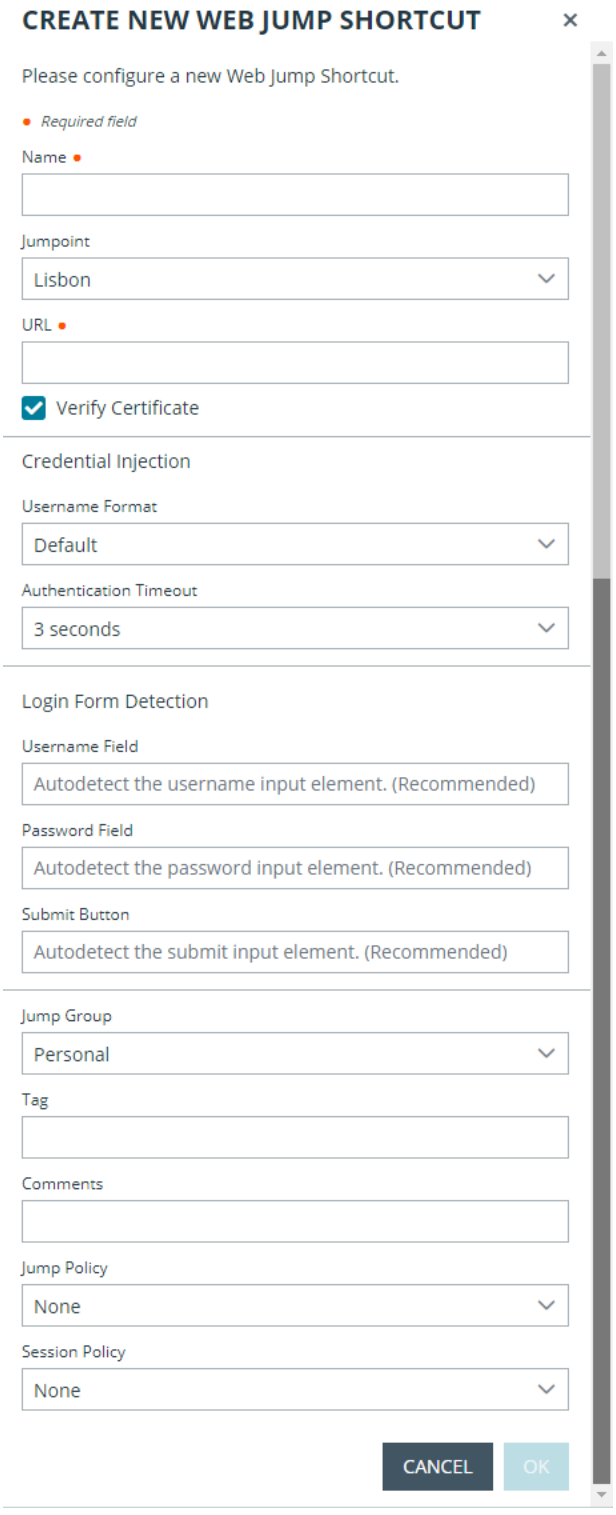
> ***Opmerking:*** *Kopiëren/plakken wordt niet ondersteund voor Linux-Jumpoints.*

Typ de **URL** van de website waar u toegang toe wilt.

Vink de optie **Certificaat verifiëren** aan als u het websitecertificaat wilt valideren voordat de verbinding wordt gemaakt. Als het vakje is aangevinkt en er worden problemen met het certificaat geconstateerd, begint de sessie niet.

BELANGRIJK!

*U moet het vinkje alleen uit het vakje **Certificaat verifiëren** verwijderen als u een Jump uitvoert naar een website die u vertrouwt, maar die een zelf-ondertekend certificaat gebruikt.*



Als u gebruik wilt maken van inloggegevensinjectie, moet u eerst **Opmaak gebruikersnaam:** selecteren.

- **Standaard:** Dit is de standaard waarde voor nieuwe en bestaande Web-jumpitems. De gebruikersnaam wordt niet aangepast voorafgaand aan het invoeren op de webpagina en wordt gebruikt in de opgeslagen indeling. Voor de Endpoint Credential Manager (ECM) mogen de inloggegevens UPN- of DLLN-indeling hebben. Voor Vault moet de gebruikersnaam altijd in UPN-indeling zijn.
- **Alleen gebruikersnaam:** Ongeacht de opgeslagen opmaak in Vault of ECM **(gebruikersnaam@domein** of **domein\gebruikersnaam**), wordt het domein verwijderd en wordt alleen de gebruikersnaam gebruikt.

Het is aan te bevelen om de drie velden onder **Detectie inlogformulier** leeg te laten, en het systeem de opgeslagen inloggegevens automatisch te laten detecteren en gebruiken. Als de automatische detectie mislukt, mislukt ook de injectie en wordt er een bericht weergegeven dat het **veld Gebruikersnaam**, het **veld Wachtwoord** en/of de **knop Verzenden** niet kon worden gevonden.

Voer bij het invoeren van de namen van de invoerelementen de HTML-ID, de HTML-naam of CSS-selector in voor elk element van de aanmeldpagina.

Voorbeeld: *Er worden dan HTML-ID's met invoervelden en een verzendknop weergegeven, zoals deze kunnen worden weergegeven in de codeweergave van een aanmeldpagina. De HTML-ID's hier zijn* ***user****,* ***pwd*** *en* ***button****.*

```
<form action="/action_page.php">
Gebruikersnaam: <input type="text" id="user"><br>
Wachtwoord: <input type="password" id="pwd"><br>
<input type="submit" value=”Verzenden" id="button">
</form>
```

Verplaats Jumpitems van de ene Jumpgroep naar een andere met gebruik van de afrolkeuzelijst **Jumpgroep**. Of u Jumpitems naar of van verschillende Jumpgroepen kunt verplaatsen, hangt van de machtigingen van uw account af.

Organiseer Jumpitems verder door de naam van een nieuwe of bestaande **Tag** in te voeren. Hoewel de geselecteerde Jumpitems samen onder de tag worden gegroepeerd, staan ze nog steeds in een lijst onder de Jumpgroep waarin elk Jumpitem is vastgemaakt. Om een Jumpitem naar het hoogste niveau Jumpgroep terug te zetten, moet dit veld leeg worden gelaten.

Jumpitems bevatten een veld **Opmerkingen** voor een naam of omschrijving, waardoor Jumpitems sneller en eenvoudiger kunnen worden gesorteerd, opgezocht en geïdentificeerd.

U moet een **Jump-beleid** kiezen om in te stellen welke gebruikers toegang tot dit Jumpitem hebben, of een kennisgeving van toegang moet worden verzonden en/of een machtiging of een ticket-ID van uw externe ticketsysteem is vereist om dit Jumpitem te gebruiken. Deze beleidslijnen worden door uw beheerder in de /login-interface ingesteld.

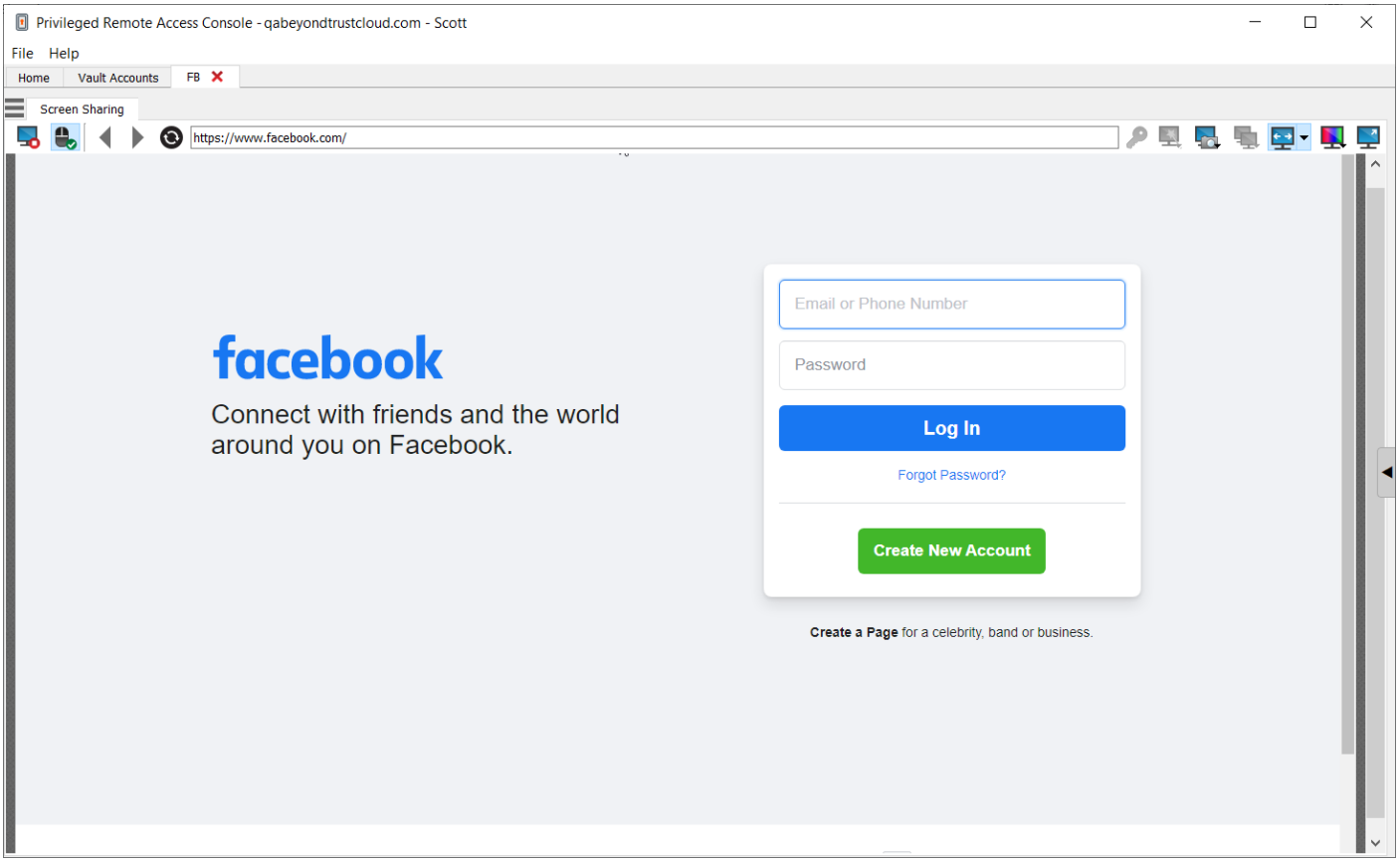
Kies een **Sessiebeleid** om aan dit Jumpitem toe te kennen. Het aan dit Jumpitem toegekende sessiebeleid heeft de hoogste prioriteit bij het instellen van sessiemachtigingen. Of u een sessiebeleid kunt instellen hangt van uw accountmachtigingen af.

Raadpleeg de online hulpbronnen, zoals deze pagina met daarop uitleg over het gebruik van CSS-selectors op https://developer.mozilla.org/en-US/docs/Web/CSS/CSS_Selectors voor meer informatie over het identificeren van HTML-formuliervelden.

Een snelkoppeling naar een Web Jump gebruiken

Om een Jumpsnelkoppeling te gebruiken om een sessie te starten, moet u de snelkoppeling in de Jump-interface selecteren en op de knop **Jump** klikken.

Nadat de verbinding met de website tot stand is gekomen, klikt u op de knop om het scherm te delen. Daarna is de login-interface van de website beschikbaar.



Opmerking: *U kunt een nieuw tabblad in Windows of Linux openen door de **CTRL**-toets ingedrukt te houden en op de muisknop te klikken. In iOS houdt u de **Command**-toets ingedrukt en klikt u op de muisknop.*

Tip: *U kunt tekst kopiëren en plakken van en naar de website door gebruik te maken van de mogelijkheden van kopiëren/plakken van uw besturingssysteem.*

Bestanden uploaden en downloaden met behulp van een snelkoppeling naar Web Jump

Als u op een koppeling klikt om een bestand van de website te downloaden, verschijnt er een prompt in uw chatvenster en wordt u gevraagd of u de download accepteert of weigert. Als u accepteert, verschijnt er een venster op uw computer om een locatie te selecteren voor uw download.

Uploaden van bestanden naar de website werkt nagenoeg hetzelfde. Er verschijnt een venster om te kiezen welk bestand u wilt uploaden.

Opmerking: *De privileged web-toegangsconsole ondersteunt niet het uploaden van bestanden naar een webpagina via een Web Jump. Het uploaden van bestanden naar een webpagina via een Web Jump wordt alleen ondersteund door de bureaubladtoepassing van de toegangsconsole.*

Inloggegevensinjectie gebruiken

BELANGRIJK!

Inloggegevensinjectie wordt niet ondersteund voor niet-beveiligde sites (niet-HTTPS).

Als BeyondTrust PRA met een wachtwoordkluis wordt geïntegreerd, kunt u door middel van inloggegevensinjectie naadloos uw websiteaccounts gebruiken zonder het aanmeldscherm te bekijken of inloggegevens in te voeren.

Opmerking: *Web Jump ondersteunt meerstaps-verificatie, waarbij niet op dezelfde browserpagina om de gebruikersnaam en het wachtwoord wordt gevraagd. Web Jump ondersteunt ook scenario's waarbij een gebruiker verbinding maakt met een niet-geverifieerd deel van een website, maar vervolgens probeert toegang te krijgen tot een gebied met gebruik van basis-verificatie. Daarnaast ondersteunt Web Jump websites die CAPTCHA's bevatten, door de gebruikers in staat te stellen de CAPTCHA af te ronden zonder het proces van inloggegevensinjectie te beëindigen. Nadat de interactie met een CAPTCHA is afgerond, klikt de gebruiker op het sleutelpictogram in de toegangsconsole om de inloggegevensinjectie te voltooien.*

Opmerking: *Voor naadloze inloggegevensinjectie op een VMware-console moeten enkele configuraties worden uitgevoerd.*

1. *Ga naar de hostcomputer van het Jumpoint.*
2. *Download en installeer de clientintegratieplugin voor VMware.*
3. *Open met behulp van beheerdermachtigingen Windows-services (**services.msc**) op de Jumpoint-host.*
4. *Klik met de rechtermuisknop op het BeyondTrust-Jumpoint en selecteer **Eigenschappen**.*
5. *Vink op het tabblad **Inloggen** onder **Lokaal systeemaccount** het vakje **Service toestaan op desktop te reageren** aan.*
6. *Klik op **OK**.*
7. *Start op het lokale systeem van de gebruiker, waarop de toegangsconsole is geïnstalleerd, een Web Jump met de hierboven weergegeven VMware-URL.*
8. *Selecteer **Inloggegevens voor Windows gebruiken**.*
9. *Een prompt verschijnt op het Jumpoint-hostsysteem voor toestemming om services te laten reageren op een extern programma. Geef de service toestemming.*
10. *Er verschijnt een prompt voor VMware-inloggegevensinjectie. Verwijder het vinkje uit het vakje of deze prompt elke keer wanneer het programma wordt geopend, moet worden weergegeven. Selecteer **Accepteren**.*
11. *U kunt nu zonder prompt Web Jumps naar de VMware-console starten met behulp van Windows-inloggegevens.*

Raadpleeg Upgrading VMware Client Integration Plug-in to the latest version (De integratieplug-in voor de VMware-client upgraden naar de meest recente versie) op https://kb.vmware.com/s/article/2145066 voor meer informatie over het downloaden van de juiste integratieplug-in voor de VMware-client.

Inloggen bij eindpunten met gebruik van inloggegevensinjectie

Als u een op Windows gebaseerd Jumpitem via de privileged web-toegangsconsole opent, kunt u inloggegevens uit een inloggegevensopslag gebruiken om u bij het eindpunt aan te melden of om toepassingen uit te voeren als beheerder.

Controleer voordat u inloggegevensinjectie gebruikt of er een inloggegevensopslag of een wachtwoordkluis beschikbaar is die aan BeyondTrust Privileged Remote Access kan worden gekoppeld.

De Endpoint Credential Manager installeren en configureren

Voordat u kunt beginnen met Jumpitems openen met behulp van inloggegevensinjectie, moet u de BeyondTrust Endpoint Credential Manager (ECM) downloaden, installeren en configureren. Met BeyondTrust ECM kunt u uw verbinding met een inloggegevensopslag, zoals een wachtwoordkluis, snel configureren.

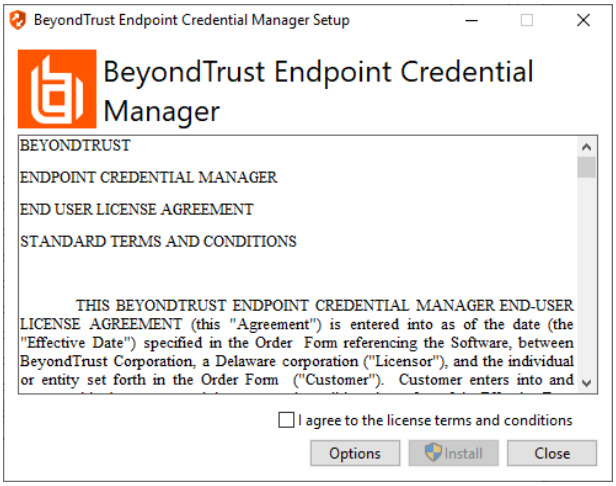
> ***Opmerking:*** *De ECM moet op uw systeem zijn geïnstalleerd om de BeyondTrust ECM Service in te schakelen en inloggegevensinjectie te gebruiken in BeyondTrust Privileged Remote Access.*

Systeemvereisten

- Windows Vista of nieuwer, alleen 64-bit
- .NET 4.5 of nieuwer
- Processor: 2 GHz of sneller
- Geheugen: 2 GB of meer
- Beschikbare schijfruimte: 80 GB of meer

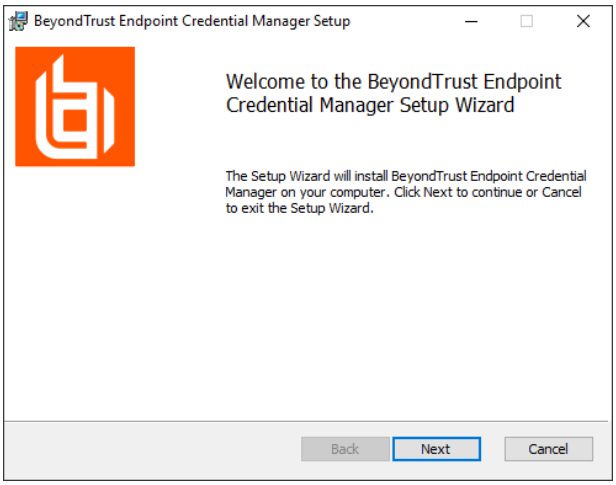
1. Download om te beginnen de BeyondTrust Endpoint Credential Manager (ECM) van BeyondTrust-ondersteuning op beyondtrustcorp.service-now.com/csm.
2. Start de installatiewizard voor BeyondTrust Endpoint Credential Manager.
3. Ga akkoord met de algemene voorwaarden uit de Gebruiksrechtovereenkomst. Schakel het selectievakje in als u akkoord bent en klik op **Installeren**.

   Als u het ECM-installatiepad wilt wijzigen, klikt u op de knop **Opties** om de installatielocatie aan te passen.

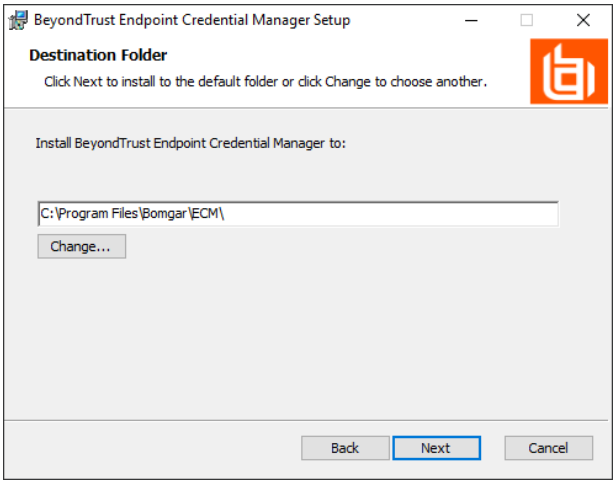


> ***Opmerking:*** *U kunt niet doorgaan met de installatie tenzij u akkoord gaat met de Gebruiksrechtovereenkomst.*

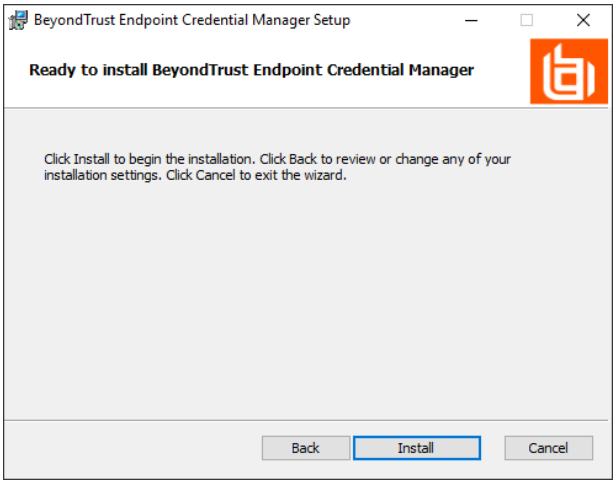
4. Klik op **Volgende** op het welkomstscherm.



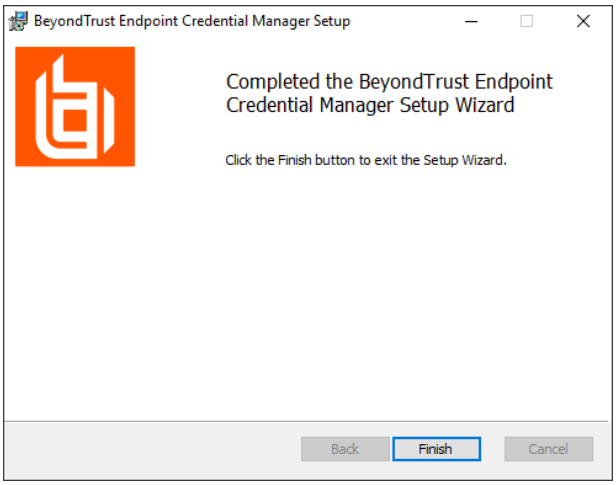
5. Kies een locatie voor de inloggegevensopslag en klik op **Volgende**.
6. In het volgende scherm kunt u de installatie beginnen of een voorgaande stap nog eens bekijken.



7. Klik op **Installeren** als u klaar bent om te beginnen.



8. De installatie duurt enkele ogenblikken. Klik op het scherm **Voltooid** op **Voltooien**.

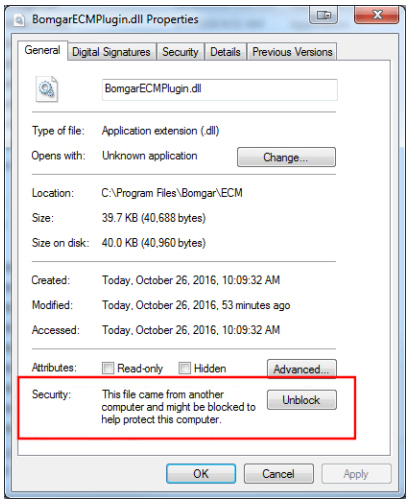


Opmerking: *Om optimale up-time te waarborgen, kunnen beheerders maximaal drie ECM's op verschillende Windows-systemen installeren om met dezelfde inloggegevensopslag te communiceren. Een lijst met de ECM's die met het apparaat verbonden zijn, is te vinden op* ***/login > Status > Informatie > ECM-clients****.*

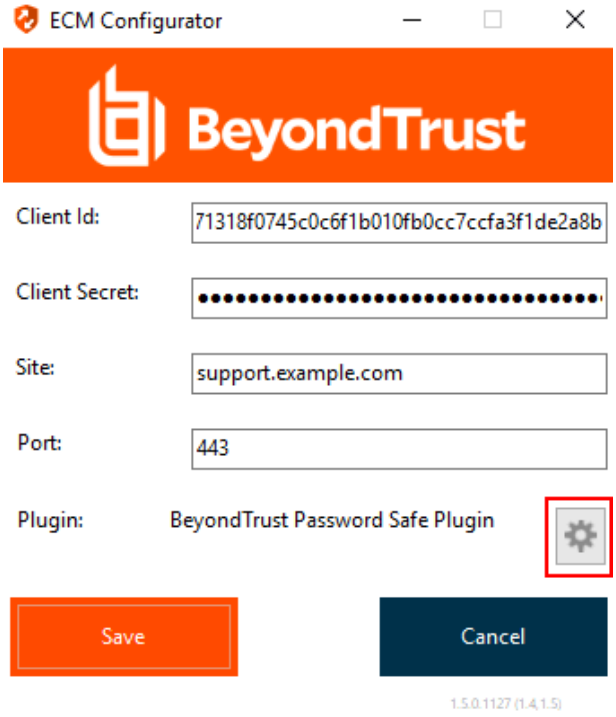
Opmerking: *Als er meerdere ECM's in een configuratie met hoge beschikbaarheid zijn verbonden, stuurt de BeyondTrust Appliance B Series verzoeken naar de ECM in de ECM-groep die het langst met het apparaat is verbonden.*

De plugin installeren en configureren

1. Nadat de BeyondTrust ECM is geïnstalleerd, moet u de bestanden van de invoegtoepassing uitpakken en naar de installatiemap (meestal **C:\Program Files\Bomgar\ECM**) kopiëren.
2. Voer **ECM Configurator** uit om de invoegtoepassing te installeren.
3. Het configuratieprogramma moet de invoegtoepassing automatisch detecteren en laden. Ga naar stap 4 als dat het geval is. Volg anders deze stappen:
    - Controleer eerst of de DLL niet is geblokkeerd. Klik met de rechtermuisknop op de DLL en selecteer **Eigenschappen**.
    - Ga naar de onderkant van het deelvenster op het tabblad **Algemeen**. Als er een kopje **Beveiliging** met een knop **Blokkering opheffen** is, moet u op de knop klikken.
    - Herhaal deze stappen voor alle andere DLL-bestanden die in de invoegtoepassing zijn verpakt.
    - Klik op de knop **Invoegtoepassing kiezen** in het configuratieprogramma en zoek de locatie van het DLL-bestand van de invoegtoepassing.



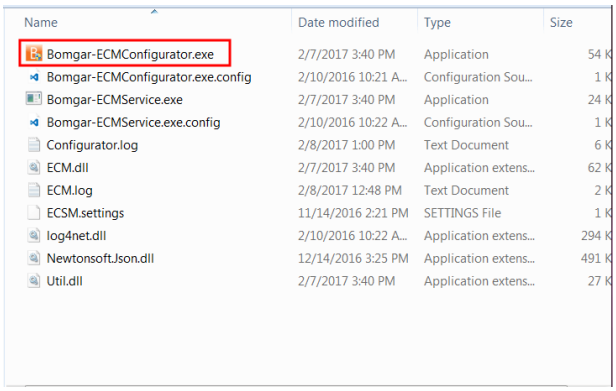
4. Klik op het pictogram met het tandwieltje in het venster van de **Configurator** om de instellingen voor de plug-in te configureren.



Een verbinding met uw inloggegevensopslag configureren

Maak een verbinding met uw inloggegevensopslag met behulp van de ECM Configurator.

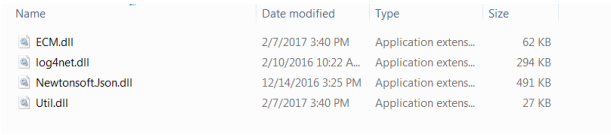
1. Zoek de BeyondTrust ECM Configurator die u zojuist hebt geïnstalleerd via Windows zoeken of via het invoerveld in de programmalijst in het menu **Start**.
2. Voer het programma uit om een verbinding te maken.
3. Vul de velden in wanneer de ECM Configurator opent. Alle velden zijn verplicht.



Vul de volgende waarden in:

Veldlabel	Waarde
Client-ID	De ID van uw inloggegevensopslag.
Clientgeheim	De geheime sleutel voor uw inloggegevensopslag.
Site	De URL van uw inloggegevensopslag-instantie.
Poort	De serverpoort waardoor de ECM verbinding maakt met uw site.
Plugin	Klik op de knop **Plugin kiezen...** om de plugin te vinden.

4. Als u klikt op de knop **Plugin kiezen...** opent de locatiemap van de ECM.
5. Plak uw pluginbestanden in de map.
6. Open het pluginbestand om te beginnen met laden.



Opmerking: *Als u verbinding maakt met een wachtwoordkluis, zijn wellicht meer configuraties op plugin-niveau nodig. De pluginvereisten kunnen verschillen per inloggegevensopslag waarmee verbinding wordt gemaakt.*

BELANGRIJK!

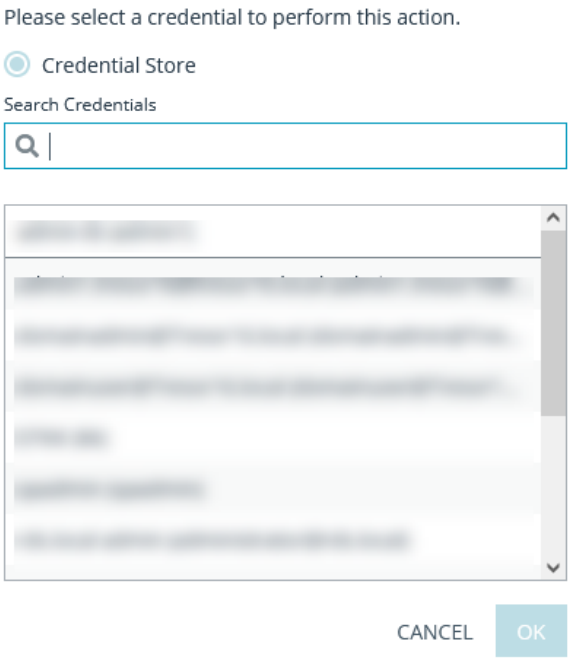
Om nieuwe instellingen in de configuratie toe te passen, moet u de ECM-service herstarten.

Inloggegevensinjectie gebruiken voor toegang tot eindpunten

Nadat de inloggegevensopslag is geconfigureerd en er een verbinding is gemaakt, kan privileged web-toegangsconsole de inloggegevens uit de opslagplaats gebruiken om aan te melden bij eindpunten.

1. Meld u aan bij de privileged web-toegangsconsole.
2. Jump naar een eindpunt met een Jumpitem dat is geïnstalleerd als een verhoogde service op een Windows-machine.
3. Tik op de knop **Afspelen** om te beginnen met scherm delen met het eindpunt. Als het eindpunt zich bij het aanmeldscherm van Windows bevindt, wordt de knop **Inloggegevens injecteren** gemarkeerd.
4. Klik op de knop **Inloggegevens injecteren**. Er verschijnt een popup met een dialoogvenster om inloggegevens te selecteren met een overzicht van de inloggegevens die in de ECM beschikbaar zijn.

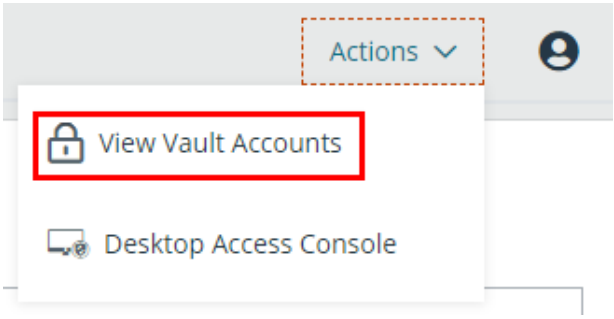
5. Selecteer uit de ECM de te gebruiken inloggegevens. Het systeem haalt de inloggegevens op bij de ECM en injecteert ze in het Windows-aanmeldscherm.
6. De gebruiker wordt aangemeld bij het eindpunt.



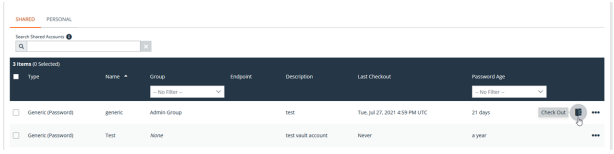
Inloggegevens in- en uitchecken

Via de web-toegangsconsole krijgt u gemakkelijk toegang tot de Privileged Remote Access Vault in de /login interface om inloggegevens in- en uit te checken als dit nodig is; dit kan tijdens een sessie of op uw lokale computer.

Om naar de Vault te gaan, klikt u op de **Acties**-knop in de bovenste navigatiebalk en selecteert u **Vault-accounts weergeven**. Als u bent ingelogd, komt u dan meteen op de pagina **Vault > Accounts** in de **/login** interface.



U kunt vervolgens een Vault-account zoeken en hierop in- of uitchecken.



Verifiëren vanuit de API voor client-scripts

Met deze functie kunnen gebruikers inloggen bij de privileged web-toegangsconsole en naar een eindpunt jumpen met gebruik van de PRA Clientscripting-API (https://www.beyondtrust.com/docs/privileged-remote-access/how-to/integrations/api/client-script/index.htm#client-scripting-api).

De URL van de API voor client-scripting volgt de indeling **https://toegang.voorbeeld.nl/api/client_script**, waarbij toegang.voorbeeld.nl de hostnaam van uw B Series Appliance is.

Deze API ondersteunt een client-type (**web_console**), een uit te voeren bewerking (**uitvoeren**) en een opdracht (**start_jump_item_session**). Er worden geen andere opdrachten ondersteund voor het clienttype **web_console**.

Als de gebruiker bij de bureaubladtoepassing van de toegangsconsole is ingelogd wanneer de URL van de API voor client-scripting wordt geopend met **type=web_console**, wordt de gebruiker ingelogd bij de privileged web-toegangsconsole en afgemeld bij de bureaubladtoepassing van de toegangsconsole. Als dit niet het gewenste gedrag is, moet de gebruiker een Client Scripting API URL gebruiken met **type=rep** in plaats van **type=web_console**.

Andersom geldt dat als de gebruiker bij de privileged web-toegangsconsole is ingelogd en de API **type=rep** aanroept, de gebruiker bij de bureaubladtoepassing van de toegangsconsole wordt ingelogd en bij de privileged web-toegangsconsole wordt afgemeld.

Hier volgt een voorbeeld van een geldig API-verzoek voor een client-script:

```
https://toegang.voorbeeld.nl/api/client_script?type=web_console&operation=execute&action=start_jump_item_session&search_string=ABCDEF02
```

Als de gebruiker al bij de privileged web-toegangsconsole is ingelogd, voert de bovenstaande aanvraag de opdracht uit in het browsertabblad waarin privileged web-toegangsconsole wordt uitgevoerd. In dit geval start de opdracht een sessie met de Jump-client waarvan de hostnaam, opmerkingen of het publiek of privé-IP-adres de tekenreeks 'ABCDEF02' bevat.

Als de gebruiker nog niet bij de privileged web-toegangsconsole is ingelogd, opent de bovenstaande opdracht een nieuw browsertabblad en wordt de gebruiker omgeleid naar /login voor verificatie (deze stap wordt overgeslagen als de gebruiker al is ingelogd bij /login). De gebruiker wordt vervolgens omgeleid naar de privileged web-toegangsconsole en de opdracht start een sessie met de Jump-client waarvan de hostnaam en opmerkingen en het openbare of privé IP-adres overeenkomen met de tekenreeks 'ABCDEF02'.

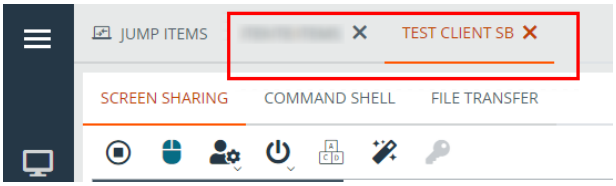
In beide gevallen moet de gebruiker, in het geval dat meer dan één Jumpitem overeenkomt met de zoekcriteria, het juiste Jumpitem in een lijst selecteren. Als er geen Jumpitems met de zoekcriteria overeenkomen, toont de privileged web-toegangsconsole een foutmelding aan de gebruiker.

Alle zoekcriteria voor de opdracht **start_jump_item_session** worden ondersteund met **type=web_console**, waaronder:

- jump.method
- search_string
- client.hostname
- client.comments
- client.tag
- client.public_ip
- client.private_ip
- session.custom.<naam attribuutcode>

Terug naar een actieve sessie in de Privileged Web-toegangsconsole

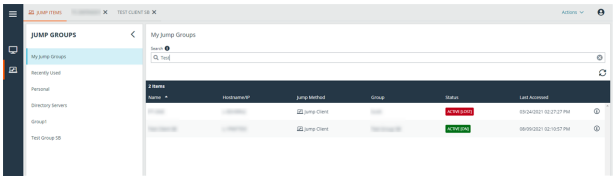
Als u meerdere toegangssessies hebt lopen, kunt u op elk gewenst moment teruggaan naar een andere sessie. Om terug te keren naar een eindpunt waartoe u al in een andere sessie toegang had, klikt u op de sessie bovenaan het scherm.



Naar eindpunten zoeken

Als u de privileged web-toegangsconsole gebruikt, kunt u zoeken naar specifieke eindpunten terwijl u in een toegangssessie bent. U kunt in de zoekresultaten ook op de knop **Starten** klikken om een sessie naar dat eindpunt te starten.

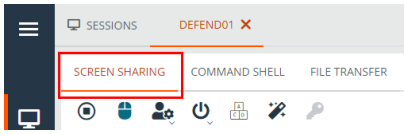
1. Klik op het pictogram **Zoeken** linksboven in het scherm.
2. Voer in de zoekbalk de naam van het eindpunt in.
3. Selecteer uit de zoekresultaten het eindpunt waarnaartoe u een sessie wilt starten en klik op de knop **Jump** om een sessie te starten.



Het externe eindpunt met gedeeld scherm beheren via Privileged Web

Om externe systemen te bekijken en te beheren, kunt u in een toegangssessie de actie Scherm delen gebruiken.

1. Klik in het sessievenster op het tabblad **Scherm delen** bovenaan het scherm. U kunt ook op het pictogram **Scherm delen starten** klikken om toegang te krijgen tot het eindpunt als het scherm niet automatisch wordt gedeeld.
2. U kunt in een sessie de volgende acties gebruiken om verschillende functies uit te voeren.



Hulpmiddelen voor scherm delen

	Stop met scherm delen.
	Start of stop de besturing van het externe toetsenbord en de externe muis terwijl u de externe computer bekijkt. Ondersteuningstechnici met een macOS-systeem kunnen **CTRL+klikken met de linkermuisknop** in de verbonden Scherm delen-sessie op het externe systeem gebruiken door **CTRL+CMD+klikken met de linkermuisknop** te gebruiken.
	Als uw machtigingen dat toestaan, kunt u voor de externe gebruiker de schermweergave en de invoer vanuit de muis en het toetsenbord uitschakelen. In de weergave van de eindgebruiker van het privacyscherm wordt duidelijk uitgelegd dat de BeyondTrust-gebruiker de weergave van de eindgebruiker heeft uitgeschakeld. De eindgebruiker kan op elk gewenst moment de controle terugkrijgen door **Ctrl+Alt+Del** in te drukken. Als alternatief kunt u voor de externe gebruiker de invoer vanuit de muis en het toetsenbord uitschakelen terwijl hij of zij het scherm nog wel kan zien. Wanneer de invoer beperkt is, wordt rond de beeldschermen van de eindgebruiker een oranje kader weergegeven en een bericht getoond dat de BeyondTrust-gebruiker de muis en toetsenbord beheert. De eindgebruiker kan op elk gewenst moment de controle terugkrijgen door **Ctrl+Alt+Del** in te drukken. Beperkte interactie met het eindpunt is alleen beschikbaar bij toegang tot macOS- of Windows-computers. Beperkte interactie met klanten is alleen beschikbaar wanneer Windows-computers worden ondersteund. In Windows Vista en nieuwere versies moet de eindpunt-client worden opgewaardeerd. In Windows 8 is deze functie beperkt tot uitschakelen van de muis en het toetsenbord.
	Start het externe systeem opnieuw op in normale of veilige modus met netwerkmogelijkheden of sluit het externe systeem af.
	Zend een opdracht **Ctrl-Alt-Del** naar de externe computer.

	Voer een speciale actie op het externe systeem uit. De beschikbare mogelijkheden zijn afhankelijk van het besturingssysteem op het externe systeem en van de configuratie ervan. Standaard scripts zijn voor de gebruiker beschikbaar in een uitklapmenu. Met de speciale actie 'Uitvoeren als' kunt u op een Windows®-systeem inloggegevens selecteren uit een Endpoint Credential Manager. 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.
	Schakel het klembord om.
	Schakel het virtuele toetsenbord om.
	Maak een schermopname. U kunt deze opslaan naar een bestand of naar het klembord.
	Selecteer een alternatief beeldscherm op de externe computer om weer te geven. De primaire monitor wordt met een **P** aangegeven.
	Bekijk het externe scherm op ware grootte of op schaal.
	Selecteer de kleuroptimalisatiemodus waarmee u het externe systeem wilt bekijken. Als u vooral videobeelden gaat delen, kies dan **Geoptimaliseerd voor video**. Kies anders uit **Zwart-wit** (gebruikt minder bandbreedte), **Weinig kleuren**, **Meer kleuren** of **Alle kleuren** (gebruikt meer bandbreedte). U kunt met zowel de modus Geoptimaliseerd voor video als met de modus Alle kleuren de echte bureaubladachtergrond weergeven.
	Bekijk het externe bureaublad als volledig scherm of keer terug naar de weergave van de interface. In de modus voor weergave in volledig scherm worden speciale toetsen doorgegeven aan het externe systeem. Dit zijn onder meer wijzigingstoetsen, functietoetsen en de Windows-starttoets. NB: dit is niet van toepassing op de opdracht **Ctrl-Alt-Del**.

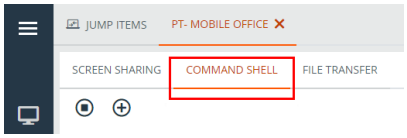
De opdrachtshell op het externe eindpunt openen via de Privileged Web-console

Met externe opdrachtshell kan een bevoorrechte gebruiker een interface met virtuele opdrachtregel op het externe systeem openen. De gebruiker kan dan lokaal opdrachten invoeren die op het externe systeem worden uitgevoerd. U kunt vanuit meerdere shells werken. NB: Scripts die de gebruiker tot zijn of haar beschikking heeft kunnen ook via de interface met scherm delen op het externe systeem worden uitgevoerd.

Uw beheerder kan ook opnames van een externe shell inschakelen zodat u van elke shell een video kunt maken die later vanuit het sessierapport kan worden bekeken. Als opname van opdrachtshell is ingeschakeld, dan is ook een transcript van de opdrachtshell beschikbaar.

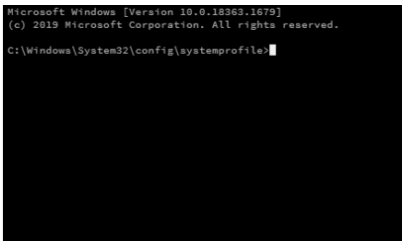
> ***Opmerking:*** *Afhankelijk van het sessiebeleid en het type jump kan het zijn dat* ***Opdrachtshell*** *niet beschikbaar is.*

1. Om in een toegangssessie toegang tot de **Opdrachtshell** te krijgen, moet u op het tabblad **Opdrachtshell** bovenaan het scherm klikken.



2. Als u niet automatisch wordt doorverwezen naar de opdrachtshell, klikt u op de knop **Opdrachtshell starten**.

3. De opdrachtopties en prompt worden weergegeven.



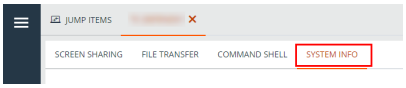
Ondersteuningsgereedschappen opdrachtshell

	Stop de toegang tot de opdrachtregel als u deze niet meer nodig hebt.
	Open een nieuwe shell om meerdere opdrachtregels uit te voeren of individuele shells te sluiten zonder toegang tot opdrachtregels te verlaten. Shells worden in tabbladen onderaan het scherm weergegeven.

Systeeminformatie bekijken op het externe eindpunt

Bevoorrechte gebruikers kunnen een complete momentopname van de systeeminformatie van het externe apparaat of van de externe computer bekijken om de tijd te verkorten die nodig is om een probleem te onderzoeken en op te lossen. De beschikbare systeeminformatie hangt van het externe besturingssysteem en de configuratie af.

1. Klik in het sessievenster op het tabblad **Systeeminformatie** bovenaan het scherm. U kunt klikken op de knop **Systeeminformatie starten**, als de systeeminformatie niet automatisch wordt geopend.
2. U kunt in een sessie de volgende acties gebruiken om verschillende functies uit te voeren.



Hulpmiddelen voor systeeminformatie

	Systeeminformatie vernieuwen.
	Kopiëren naar klembord.
	Opslaan naar bestand.

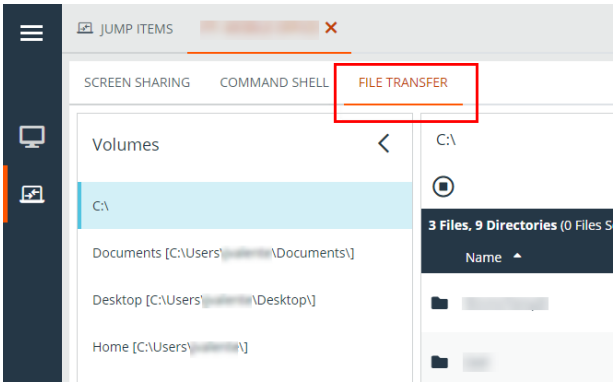
De Privileged Web-console gebruiken om bestanden van en naar externe systemen te verplaatsen

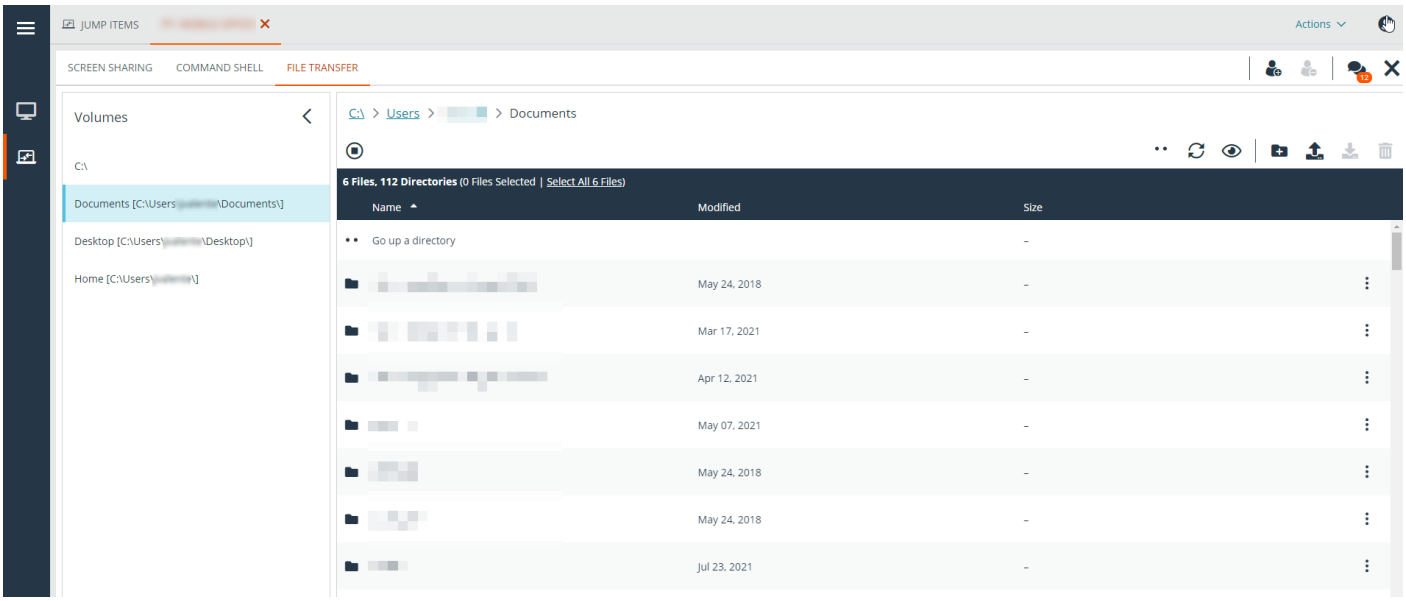
Bevoorrechte gebruikers kunnen tijdens een sessie bestanden en zelfs gehele mappen overdragen, verwijderen of de naam ervan wijzigen, van en naar de externe computer of van het externe apparaat en van of naar de SD-kaart van het apparaat. U hoeft geen volledige besturing over de externe computer te hebben om bestanden te kunnen overdragen.

Afhankelijk van de machtigingen die uw beheerder voor uw account heeft ingesteld, hebt u mogelijk alleen toestemming om bestanden naar het externe systeem te uploaden of bestanden naar uw lokale computer te downloaden. De toegang tot het bestandssysteem kan ook worden beperkt voor bepaalde paden op het externe of lokale systeem, waarmee het uploaden en downloaden naar bepaalde mappen wordt beperkt. Zet bestanden over met de knoppen Uploaden of Downloaden. Bekijk de voortgang van verplaatsen en verwijderen door te klikken op het plusteken onderaan het scherm. Download, hernoem of verwijder bestanden door te klikken op het pictogram **Meer opties**.

Klik op het tabblad **Bestandsoverdracht** bovenaan het scherm om te beginnen met het verplaatsen van bestanden naar een systeem.

Selecteer in de kolom **Volumes** een plek om te beginnen met bladeren. De breadcrumbs bovenaan tonen uw huidige locatie. Dubbelklik op een map om deze te openen.





Als een ICAP-server is ingeschakeld, worden alle bestandsoverdrachten via FTP gescand op malware. Het bestand wordt niet overgedragen als er malware in wordt gedetecteerd. Details over mislukte bestandsoverdrachten kunnen worden

weergegeven op het scherm voor de bestandsoverdracht en zijn beschikbaar in sessie- of teamrapporten. Raadpleeg Beveiliging op https://www.beyondtrust.com/docs/privileged-remote-access/getting-started/admin/security.htm als u een ICAP-server wilt inschakelen.

Hulpmiddelen voor bestandsoverdracht

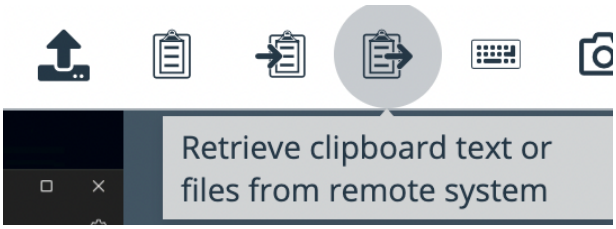
	Stop de toegang tot het bestandssysteem op het externe apparaat.
	Ga naar een map op één niveau hoger in het geselecteerde bestandssysteem.
	Vernieuw de weergave van het geselecteerde bestandssysteem.
	Geef verborgen bestanden weer.
	Maak een nieuwe map aan.
	Upload een bestand naar een map / deel bestanden via het RDP-klembord.
	Download de geselecteerde bestanden vanuit een map.
	Wissel wijzigingstoetsen.
	Verzend klembordtekst naar extern systeem.
	Haal klembordtekst op van extern systeem / haal klembordtekst of -bestanden op vanaf een extern systeem (RDP).

	Verwijder de geselecteerde bestanden uit een map.
	Download of verwijder een map of bestand of wijzig de naam ervan.  ***Opmerking:*** *Als u een bestand of map verwijdert, dan is de verwijdering permanent. Het gaat niet naar de prullenbak.*

RDP-bestandsoverdracht

Bestanden downloaden

U kunt bestanden overdragen tijdens RDP-sessies door **Ctrl+C** te gebruiken om ze naar het klembord te kopiëren, met de rechtermuisknop te klikken en Kopiëren te selecteren in een contextmenu of op de knop Kopiëren in de werkbalk in Verkenner te klikken. *Deze bestanden worden naar het klembord van het eindpunt gekopieerd*.

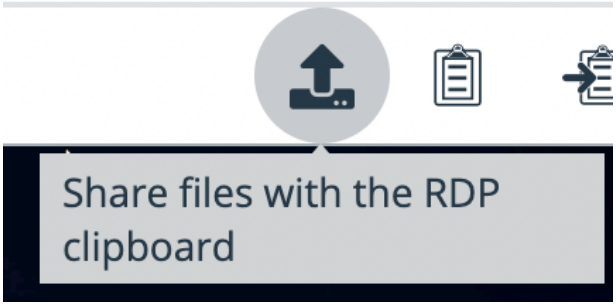


Wanneer u bestanden of mappen naar het externe eindpunt kopieert, wordt er een downloadbewerking geactiveerd in uw browser. Het geselecteerde bestand wordt gedownload in de map die u op uw systeem hebt opgegeven. Afhankelijk van uw browserinstellingen ziet u mogelijk de vraag om een downloadlocatie op te geven.

Bestanden uploaden

Het proces voor het uploaden van bestanden in de privileged web-toegangsconsole bestaat uit twee stappen:

1. U geeft in de browser aan welke bestanden u wilt delen met het externe klembord.
2. U voert een plakbewerking uit op het externe eindpunt.



U kunt in de browser op twee manieren aangeven welke bestanden moeten worden gedeeld:

1. Klik in de werkbalk op een knop met een standaard bestandskiezer, vergelijkbaar met het uploaden van bestanden via het tabblad voor bestandsoverdrachten.
2. Sleep bestanden naar de weergave met het gedeelde scherm.

Nadat u een van deze methoden hebt geselecteerd, herinnert een melding aan de onderkant van de pagina u eraan dat u nog moet plakken op het externe eindpunt.

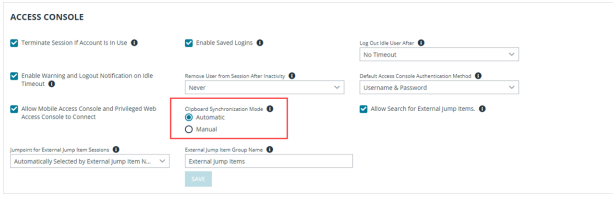
Zodra u op het eindpunt hebt geplakt, geeft Windows de voortgang van de overdracht weer in een dialoogvenster op het eindpunt. Ook ziet u de knop Annuleren.

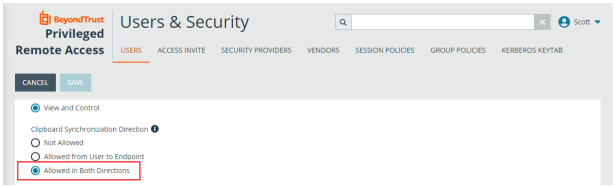
> ***Opmerking:*** *Als u meer dan één bestand in de bestandskiezer selecteert of sleept voordat u de eerder geselecteerde bestanden op het eindpunt plakt, wordt het eerst geselecteerde bestand overschreven.*

Instellingen

U moet ervoor zorgen dat de volgende instellingen als volgt zijn, zodat de bestandsoverdracht naar behoren werkt:

- **Klembordsynchronisatiemodus** is ingesteld op **Automatisch** (zie **/login > Beheer > Beveiliging > Toegangsconsole**)
- De **synchronisatierichting van het klembord** van de gebruiker is ingesteld op **Toegestaan in beide richtingen** (zie **/login > Gebruikers en beveiliging > Gebruikers > Sessietoestemmingen > Klembordsynchronisatierichting**).





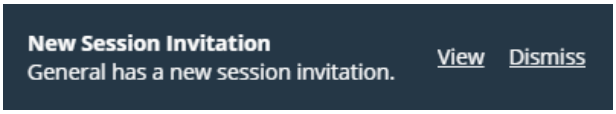
Een sessie delen met teamleden of externe gebruikers via de Privileged Web-toegangsconsole

Teamleden uitnodigen

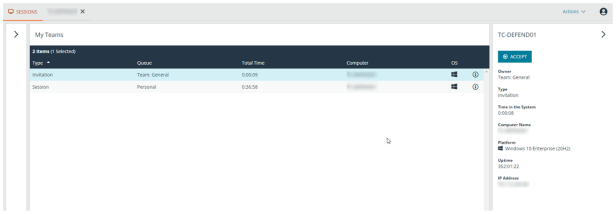
In een sessie kunt u een ander teamlid verzoeken aan een toegangssessie mee te doen. Volg onderstaande stappen om een sessie te delen.

1. Klik op het pictogram **Andere gebruikers voor deze sessie uitnodigen**.
2. Selecteer uit het menu het team waar de gebruiker lid van is.
3. Kies uit de lijst met teamleden de gebruiker waar u de sessie mee wilt delen.

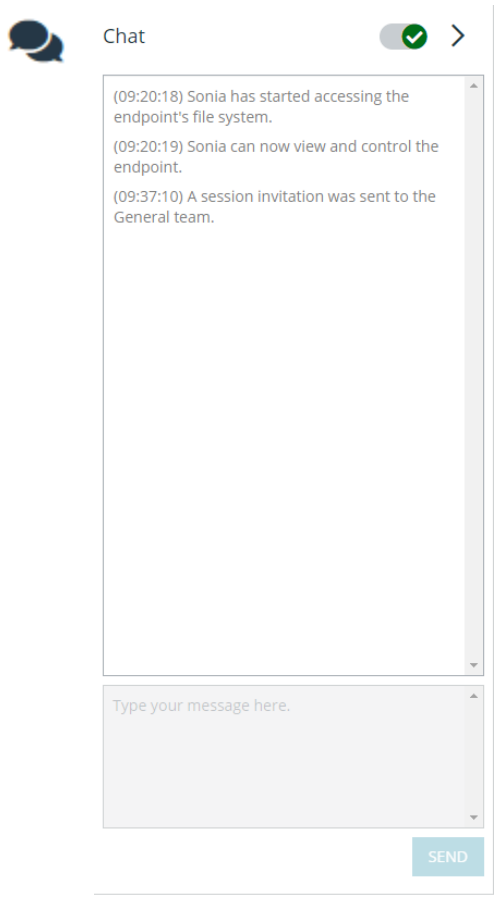
4. Uitgenodigde gebruikers zien in de linkeronderhoek van het scherm een uitnodiging verschijnen voor een nieuwe sessie.



5. Door op **BEKIJKEN** op de meldingsbanner te klikken, kan informatie over de sessie worden weergegeven. De gebruiker kan dan op **ACCEPTEREN** klikken om de sessie bij te wonen.



6. Als de gebruiker in de sessie is gekomen, kunt u met hem of haar chatten door op het pictogram **Chat** bovenaan het scherm te klikken.



U kunt meerdere uitnodigingen verzenden als u wilt dat meerdere teamleden de sessie bijwonen. Gebruikers worden hier alleen vermeld als zij bij de toegangsconsole zijn ingelogd of als voor hen uitgebreide beschikbaarheid is ingeschakeld.

Als u bent gemachtigd om sessies te delen met gebruikers die geen lid van uw teams zijn, worden er extra teams weergegeven, mits deze ten minste één lid bevatten dat bij de toegangsconsole is ingelogd of waarvoor uitgebreide beschikbaarheid is ingeschakeld.

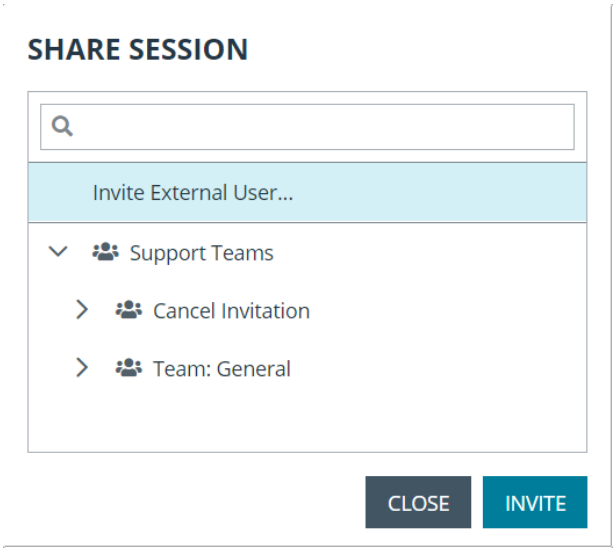
Alleen de eigenaar van de sessie kan uitnodigingen verzenden. Uitnodigingen verlopen niet zolang u de eigenaar van de sessie blijft. Eén gebruiker kan voor een bepaalde sessie maar één keer worden uitgenodigd. De uitnodiging verdwijnt als:

- De uitnodigende gebruiker de uitnodiging annuleert.
- De uitnodigende gebruiker de sessie verlaat.
- De sessie stopt.
- De uitgenodigde gebruiker de uitnodiging aanvaardt.

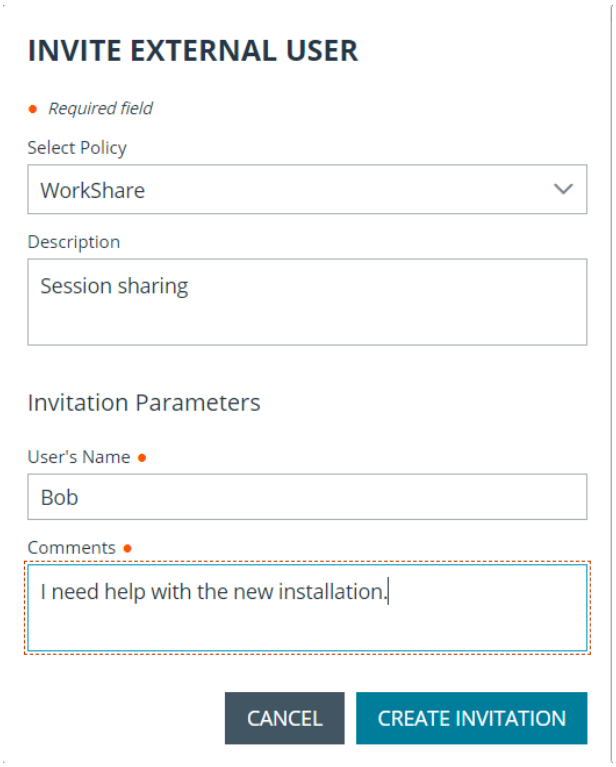
Externe gebruikers uitnodigen

U kunt een externe gebruiker of leverancier uitnodigen om een toegangssessie bij te wonen. Volg onderstaande stappen om een sessie te delen:

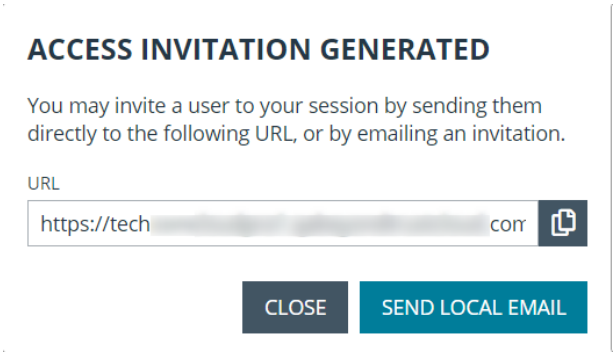
1. Klik op het pictogram **Andere gebruikers voor deze sessie uitnodigen**.
2. Selecteer **Externe gebruiker uitnodigen**.



1. Selecteer een beleid, voor zover van toepassing, en voer een korte beschrijving voor het type uitnodiging in.
2. In het gedeelte **Uitnodigingsparameters** kunt u de naam invoeren van de persoon die wordt uitgenodigd, plus enkele opmerkingen die u bij de uitnodiging wilt plaatsen.
3. Klik op **Uitnodiging aanmaken**.



U kunt nu een externe gebruiker uitnodigen door te klikken op het pictogram **Kopiëren naar klembord** en de gebruiker de koppeling naar de sessie-URL te geven, of door een e-mailuitnodiging te sturen.



Een lid van een Privileged Web-toegangsconsolesessie verwijderen

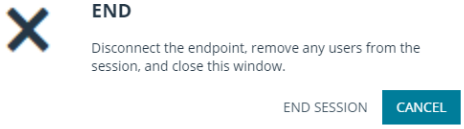
U kunt, indien nodig, een andere gebruiker uit een gedeelde toegangssessie verwijderen. Om een gebruiker te verwijderen, moet u op het pictogram **Lid verwijderen** klikken.

Kies uit het menu welke deelnemer u wilt verwijderen. Klik op **Lid verwijderen**.

Opmerking: *U moet de eigenaar van de sessie zijn om een ander lid te mogen verwijderen.*

De Privileged Web-toegangsconsolesessie afsluiten

1. Klik op het pictogram **X** rechtsboven in het scherm om een toegangssessie te verlaten. Als u eigenaar van de sessie bent, moet u er rekening mee houden dat de actie **Sessie beëindigen** de sessiepagina in uw toegangsconsole sluit en dat eventuele extra leden die de sessie delen, worden verwijderd.

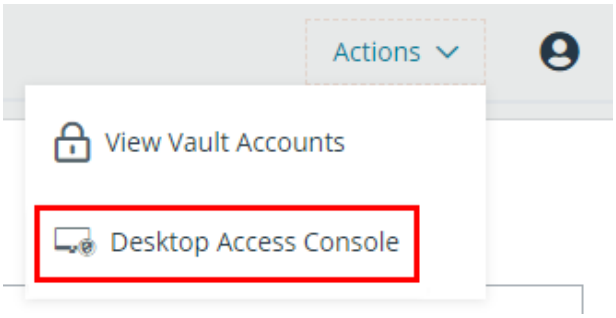


2. Vervolgens wordt u gevraagd of u de sessie wilt beëindigen.
3. Als u op **OK** klikt, dan wordt de sessie beëindigd en gaat u terug naar de lijst **Alle Jumpitems**.

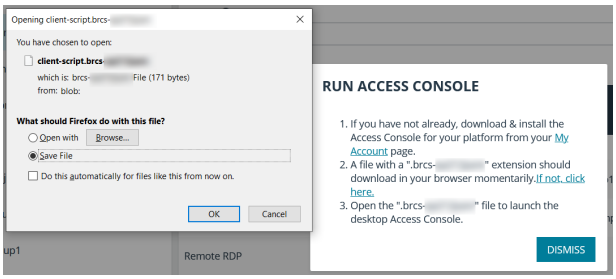
Het eigen bureaublad van de Privileged Web-toegangsconsole downloaden

Als u in de privileged web-toegangsconsole werkt, kunt u er op elk gewenst moment voor kiezen om de systeemeigen toegangsconsole-bureaubladversie op uw computer te downloaden.

1. U kunt de systeemeigen bureaubladtoepassing van toegangsconsole via de privileged web-toegangsconsole downloaden door op de knop **Bureaublad Toegangsconsole** te klikken, die zich onder het **Actief**-menu in de rechterbovenhoek van het scherm bevindt.



2. Volg de instructies om de software te installeren als het installatieprogramma verschijnt.



> ***Opmerking:*** *Op een Linux-systeem moet u het bestand op uw computer opslaan en het dan vanaf die locatie openen. Gebruik niet de koppeling* ***Openen*** *die na het downloaden bij sommige browsers verschijnt.*