BeyondTrust

Bevoorrechte toegang op afstand 21.1

Privileged Web-toegangsconsole

TC:7/26/2021

Inhoudsopgave

Privileged Web-toegangsconsolegids

Met de BeyondTrust privileged web access console 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 access console. 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 access console en hoe deze access console 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 de 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 access console op uw systeem uit te kunnen voeren, moet uw B Series Appliance minimaal softwareversie 15.3 of hoger uitvoeren. De privileged web access console 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!

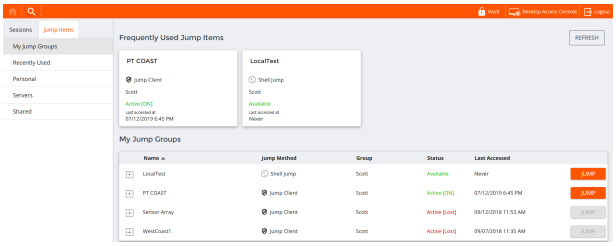
Uw B Series Appliance moet zijn voorzien van een geldig SSL-certificaat dat is ondertekend door een certificaatautoriteit. Neem contact op met BeyondTrust Technical Support nadat u een door een CA ondertekend SSL-certificaat op uw B Series Appliance hebt toegepast. Uw klantendiensttechnicus stelt dan 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 access console op uw apparaat uitvoeren om vanaf vrijwel elke willekeurige plaats toegang tot eindpunten te krijgen.

De Web-toegangsconsole openen

Met privileged web access console kunt u via een online access console op afstand veilig toegang tot uw eindpunten krijgen door verbinding te maken via de B Series Appliance. Volg de onderstaande stappen om toegang tot eindpunten te krijgen via de privileged web access console:

De Privileged Web-toegangsconsole openen met gebruik van /console

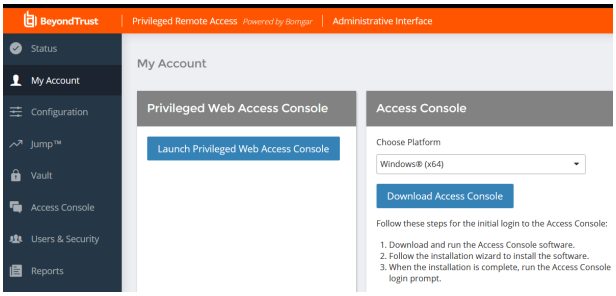
1. Voer in de adresbalk van uw browser de hostnaam van uw BeyondTrust-site in, gevolgd door **/console** (bijvoorbeeld toegang.voorbeeld.nl/console).
2. Voer de gebruikersnaam en wachtwoord van uw BeyondTrust-gebruikersaccount in.
3. Klik op **Inloggen** om uw onlinesessie in de access console te starten.



De Privileged Web-toegangsconsole openen met gebruik van /login

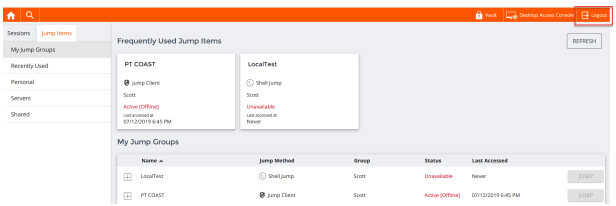
> ***Opmerking:*** *De knop* ***Privileged Web Access Console starten*** *is standaard niet beschikbaar in de /login-beheerinterface. Ga naar* ***Beheer > Beveiliging*** *en schakel* ***Mobiele Access Console en Privileged Web Access Console toestaan om verbinding te maken*** *in om de console te activeren.*

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.
3. Klik op **Inloggen**.
4. Selecteer **Mijn account**.
5. Klik op **Starten Privileged Web Access Console**.



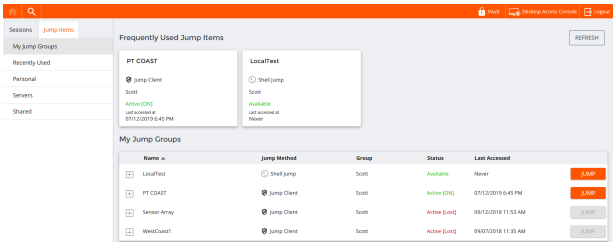
6. De privileged web access console wordt in een nieuw tabblad geopend, waarna u toegang tot eindpunten kunt krijgen.

   Klik op **Afmelden** in de rechterbovenhoek van het scherm om u af te melden bij de access console.



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

Om toegang tot een eindpunt te krijgen moet u vanaf de pagina **Jump-clients** van de /login-beheerinterface een Jumpitem op dat systeem installeren.



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:

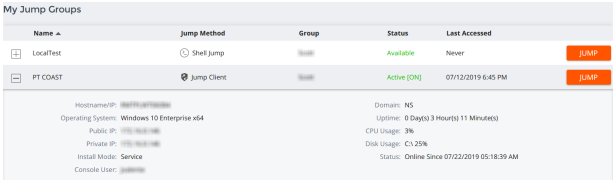
- Zoek en selecteer een eindpunt uit de lijst **Mijn Jumpgroepen**.
- Kies een Jumpgroep en selecteer vervolgens een eindpunt uit de lijst met eindpunten voor die groep.
- Selecteer een sessie uit de lijst **Veel gebruikte Jumpitems**.

> ***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**.



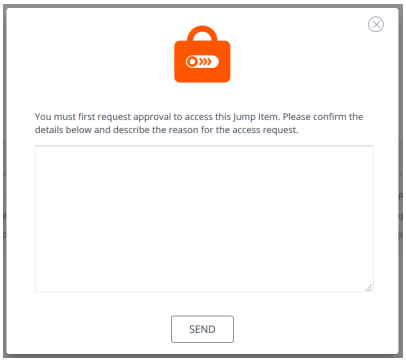
Autorisatie door eindgebruiker of derden

Afhankelijk van de configuratie van Jumpitems binnen de /login-beheerinterface kan er aan een Jumpitem een Jumpbeleid zijn geassocieerd en kan er in het beleid een autorisatiecomponent zijn gedefinieerd waarin wordt afgedwongen dat de gebruiker

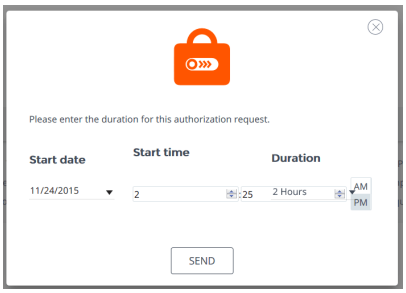
toestemming van een derde partij of een beheerder nodig heeft voordat hij of zij een toegangssessie met het Jumpitem kan starten.

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

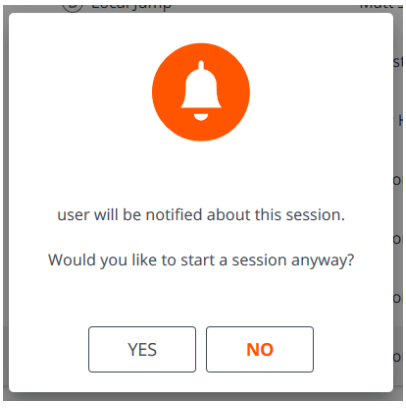
1. Nadat u op de knop **JUMP** hebt geklikt en toegang hebt aangevraagd, verschijnt er een prompt waarin u wordt gevraagd een reden in te voeren waarom u toegang tot het systeem wilt hebben.



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.



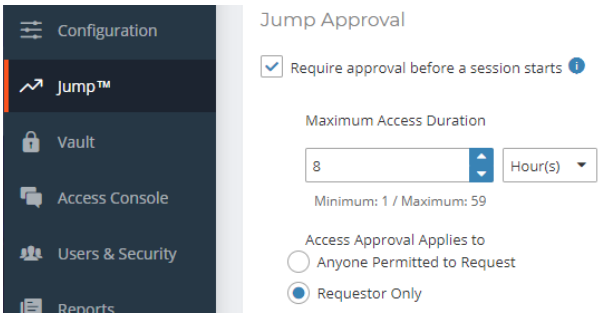
4. Nadat het verzoek is behandeld, wordt in de informatie van het Jumpitem een melding over de machtiging weergegeven met de tekst *goedgekeurd* of *geweigerd*. Als toegang wordt verleend, kan de gebruiker op de knop Jump tikken om toegang tot het systeem te krijgen.
5. U krijgt een bericht te zien met 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.



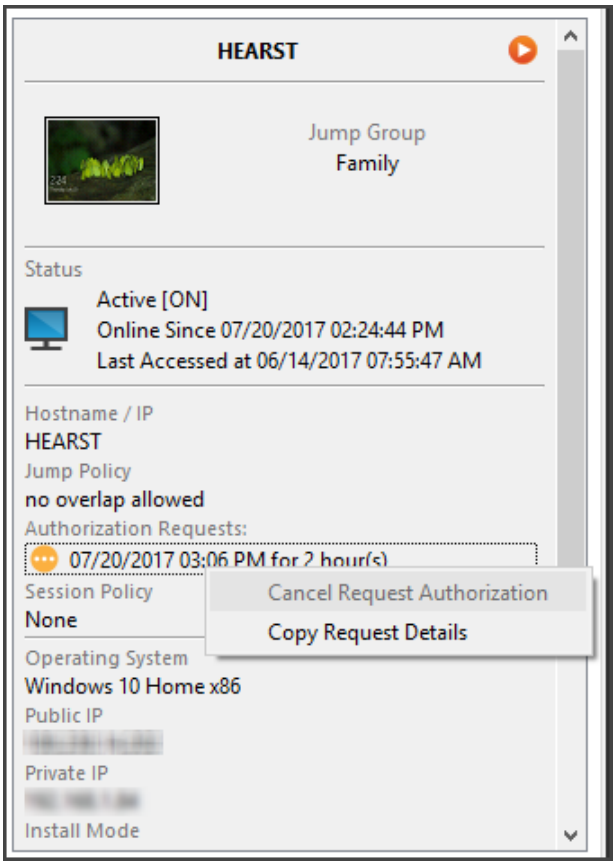
Intrekken van een goedkeuringsaanvraag voor toegang

De machtiging om goedgekeurde toegangsverzoeken in te trekken wordt bepaald door het Jump-beleid. In de **/login** webbeheerinterface gaat u naar **Jump > Jump-beleidslijnen**. Bij **Jump-goedkeuring** hebt u twee opties:

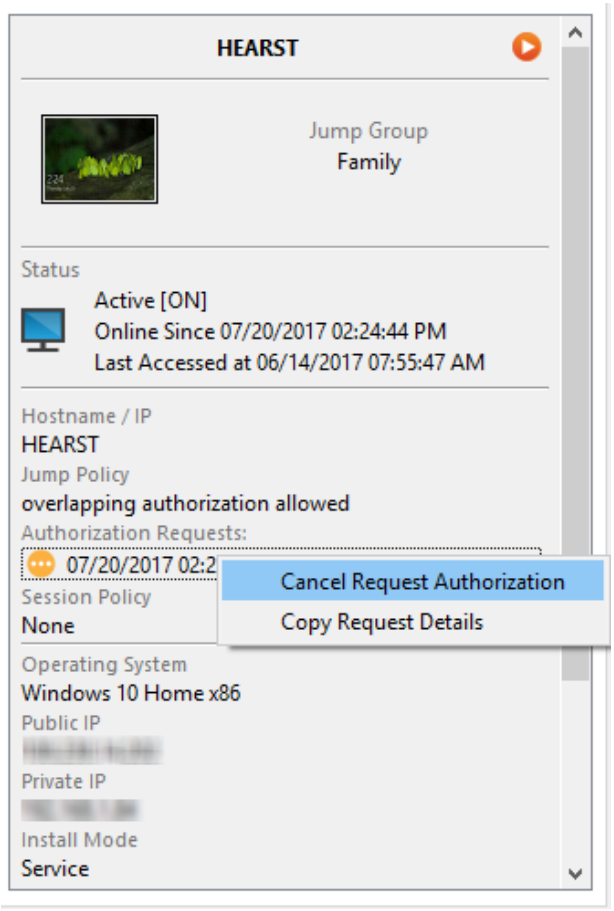
- **Iedereen mag een aanvraag indienen**
- **Alleen verzoeker**



Als het Jump-beleid is ingesteld op **Alleen verzoeker** en toegangsverzoek op dat moment is goedgekeurd voor gebruiker A, dan wordt gebruiker B gevraagd om een nieuw toegangsverzoek aan te maken als deze gebruiker probeert een Jump uit te voeren naar het Jumpitem, 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.

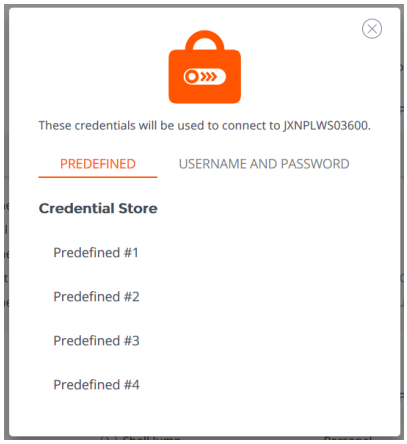


Als het Jump-beleid is ingesteld op **Iedereen mag een aanvraag indienen** en een toegangsverzoek op dat moment is goedgekeurd voor gebruiker A, dan mag gebruiker B een nieuwe sessie met het Jumpitem starten als B probeert een Jump naar dit item uit te voeren. Bovendien mag iedereen met toegangsrechten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

Inloggen bij eindpunten met gebruik van inloggegevensinjectie

Als u een op Windows gebaseerd Jumpitem via de privileged web access console 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.

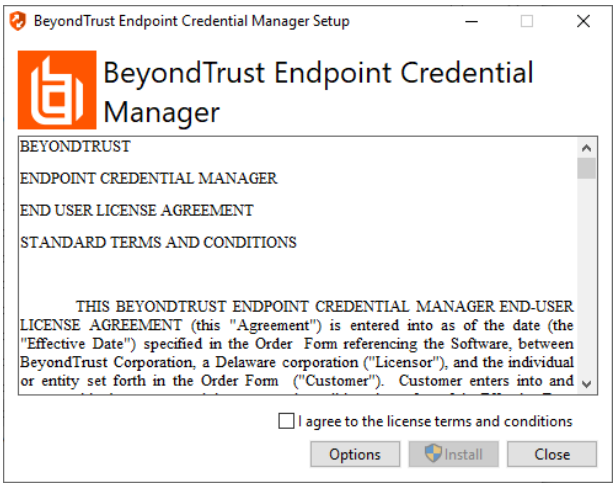
> ***Opmerking:*** *De ECM moet op uw systeem zijn geïnstalleerd om de BeyondTrust ECM Service in te schakelen en inloggegevensinjectie te gebruiken in BeyondTrust Privileged Remote Access.*

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

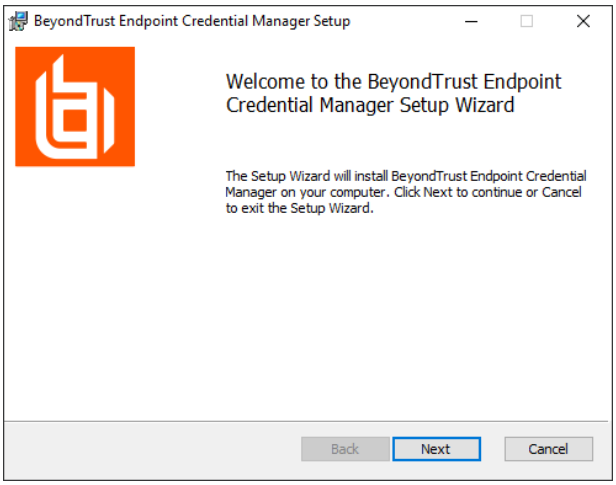
1. Download om te beginnen de BeyondTrust Endpoint Credential Manager (ECM) van BeyondTrust-ondersteuning op beyondtrustcorp.service-now.com/csm.
2. Start de installatiewizard voor BeyondTrust Endpoint Credential Manager.
3. Ga akkoord met de algemene voorwaarden uit de Gebruiksrechtovereenkomst. Schakel 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.

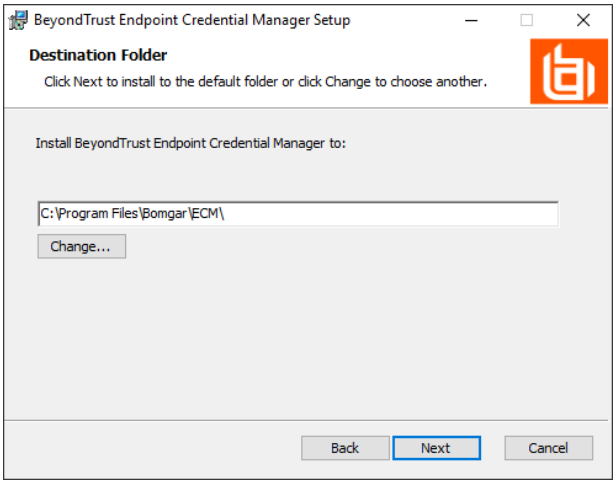


> ***Opmerking:*** *U kunt niet doorgaan met de installatie tenzij u akkoord gaat met de Gebruiksrechtovereenkomst.*

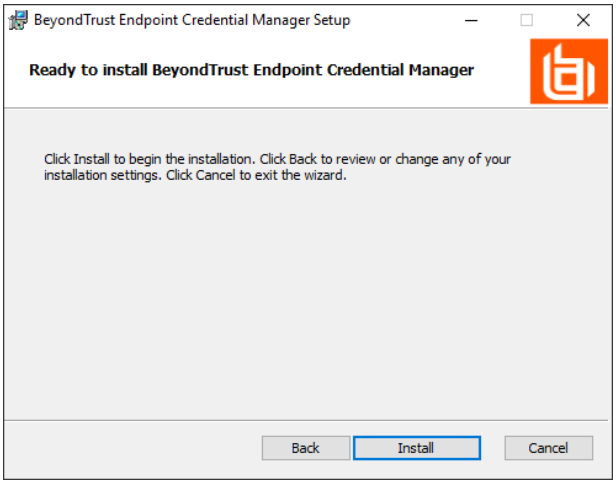
4. Klik op **Volgende** op het welkomstscherm.



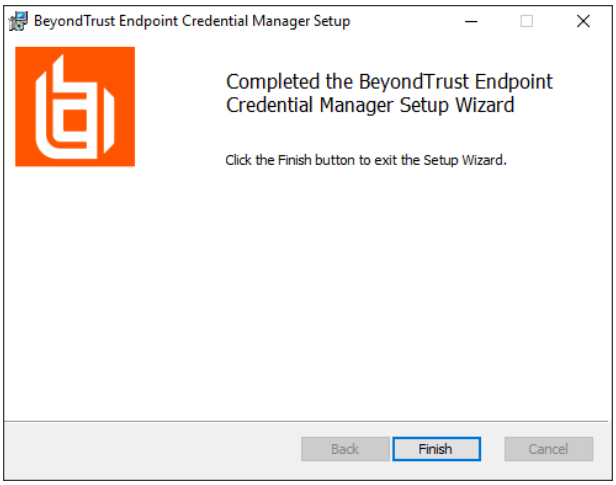
5. Kies een locatie voor de inloggegevensopslag en klik op **Volgende**.



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**.

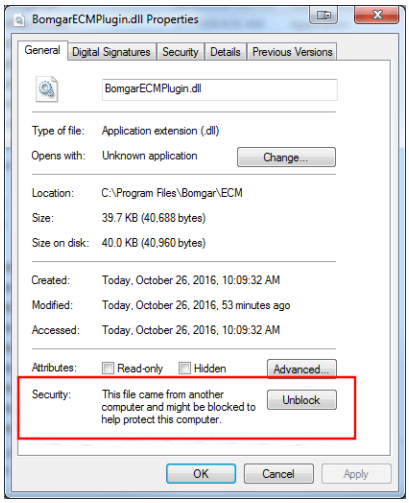


> ***Opmerking:*** *Om optimale up-time te waarborgen, kunnen beheerders maximaal drie ECM's op verschillende Windows-systemen installeren om met dezelfde inloggegevensopslag te communiceren. Een lijst met de ECM's die met het apparaat verbonden zijn, is te vinden op* ***/login > Status > Informatie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

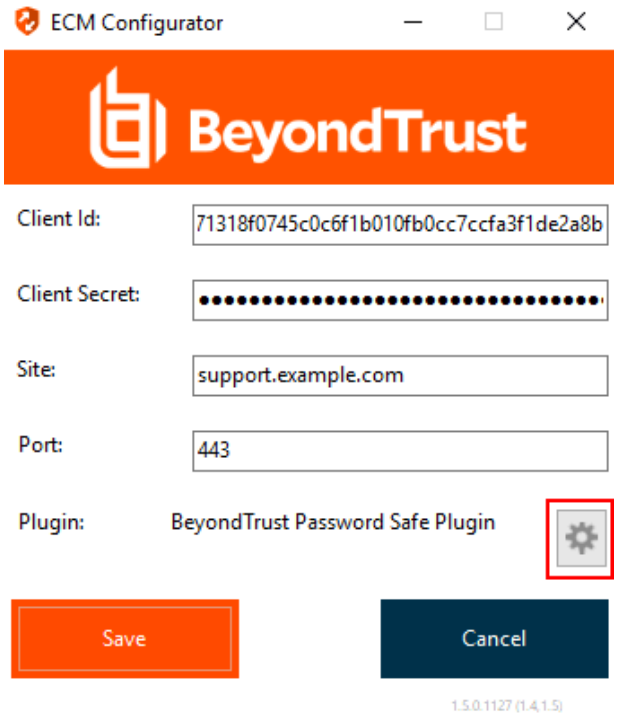
> ***Opmerking:*** *Als er meerdere ECM's in een configuratie met hoge beschikbaarheid zijn verbonden, stuurt het BeyondTrust Appliance B Series verzoeken naar de ECM in de ECM-groep die het langst met het apparaat is verbonden.*

De plugin installeren en configureren

1. Nadat de BeyondTrust ECM is geïnstalleerd, dient u de bestanden van de invoegtoepassing uit te pakken en naar de installatiemap (meestal **C:\Program Files\Bomgar \ECM**) te 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.



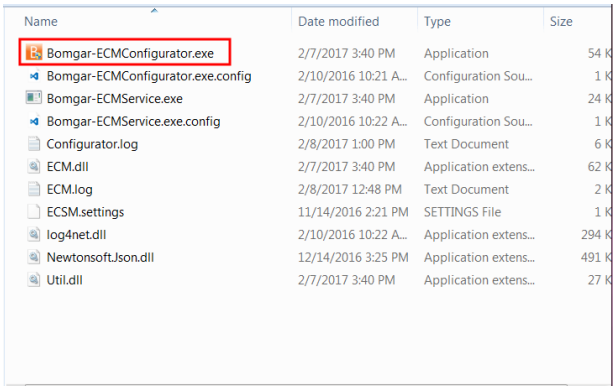
4. Klik op het pictogram met het tandwieltje in het venster van de **Configurator** om de instellingen voor de plug-in te configureren.



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.



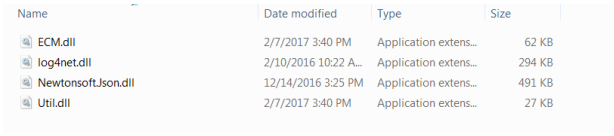
3. Vul de velden in wanneer de ECM Configurator opent. Alle velden zijn verplicht.

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 inloggevensopslag-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!

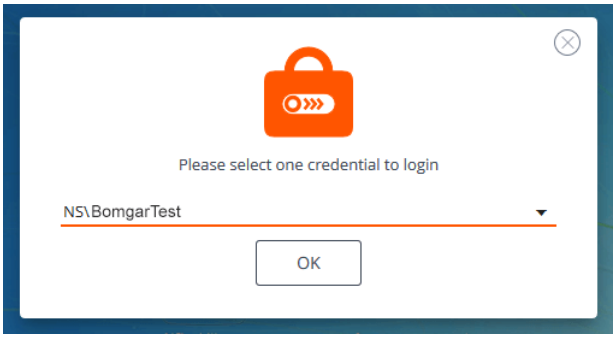
Om nieuwe instellingen in de configuratie toe te passen, moet u de ECM-service herstarten.

Inloggegevensinjectie gebruiken voor toegang tot eindpunten

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

1. Meld u aan bij de privileged web access console.
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.

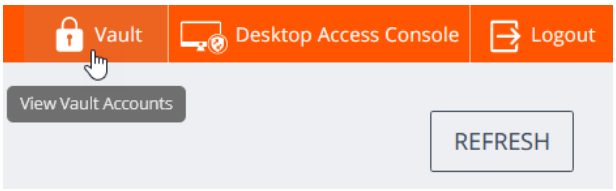
5. Selecteer uit de ECM de te gebruiken inloggegevens. Het systeem haalt de inloggegevens op bij de ECM en injecteert ze in het Windows-aanmeldscherm.
6. De gebruiker wordt aangemeld bij het eindpunt.



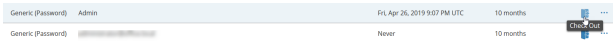
Inloggegevens in- en uitchecken

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 **Vault**-knop in de bovenste navigatiebalk. 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 access console 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 access console 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 access console en afgemeld bij de bureaubladtoepassing van de access console. 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 access console is ingelogd en de API **type=rep** aanroept, de gebruiker bij de bureaubladtoepassing van de access console wordt ingelogd en bij de privileged web access console 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 access console is ingelogd, voert de bovenstaande aanvraag de opdracht uit in het browsertabblad waarin privileged web access console wordt uitgevoerd. In dit geval start de opdracht een sessie met de Jump-client waarvan de hostnaam, opmerkingen of publiek of privé-IP-adres de tekenreeks 'ABCDEF02' bevat.

Als de gebruiker nog niet bij de privileged web access console 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 access console en de opdracht start een sessie met de Jump-client waarvan de hostnaam en opmerkingen en het openbare of particuliere 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 access console 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 access sessions hebt, kunt u op elk gewenst moment teruggaan naar een andere sessie. Om naar een eindpunt terug te gaan waar u al in een andere sessie toegang toe hebt, moet u de volgende stappen uitvoeren:

1. Klik op het vervolgkeuzemenu **Sessies**.

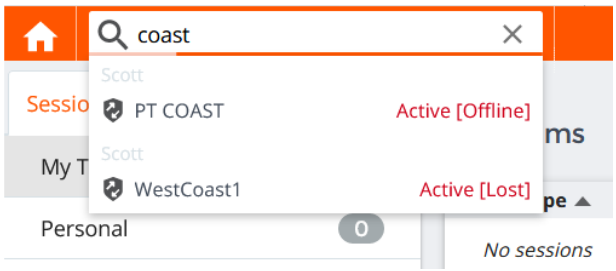
> ***Opmerking:*** *Het getal dat in de vervolgkeuzelijst* ***Sessies*** *is vermeld, geeft aan tot hoeveel actieve sessies u tegelijkertijd toegang hebt.*

2. Selecteer een eindpunt uit de lijst.
3. U gaat dan naar de sessie voor dat bepaalde eindpunt.

Naar eindpunten zoeken

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

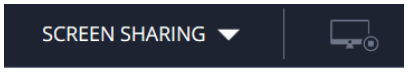
1. Klik op het pictogram **Zoeken** linksboven in het scherm.
2. Voer in de zoekbalk de naam van het eindpunt in.
3. Selecteer uit de zoekresultaten het eindpunt waarnaartoe u een sessie wilt starten en klik op de knop **Starten** om een sessie te starten.



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.

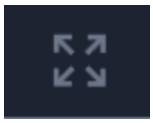
1. Klik in het sessievenster op de vervolgkeuzelijst **Scherm delen** en kies de optie **Scherm delen**. U kunt ook op het pictogram **Scherm delen starten** klikken om toegang te krijgen tot het eindpunt als het scherm niet automatisch wordt gedeeld.



2. U kunt in een sessie de volgende acties gebruiken om verschillende functies ut 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.
	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. 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 endpoint 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 virtuele toetsenbord om.
	Schakel het klembord om.
	Selecteer een alternatief beeldscherm op de externe computer om weer te geven. De primaire monitor wordt met een **P** aangegeven.

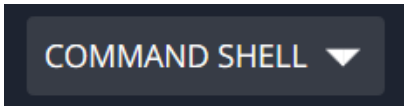
	Bekijk het externe scherm op ware grootte of op schaal.
	Selecteer de kleuroptimalisatiemodus waarmee u het externe systeem wilt bekijken. Als u vooral videobeelden gaat delen, kies dan **Geoptimaliseerd voor video**. Kies anders uit **Zwart-wit** (gebruikt minder bandbreedte), **Weinig kleuren**, **Meer 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**.

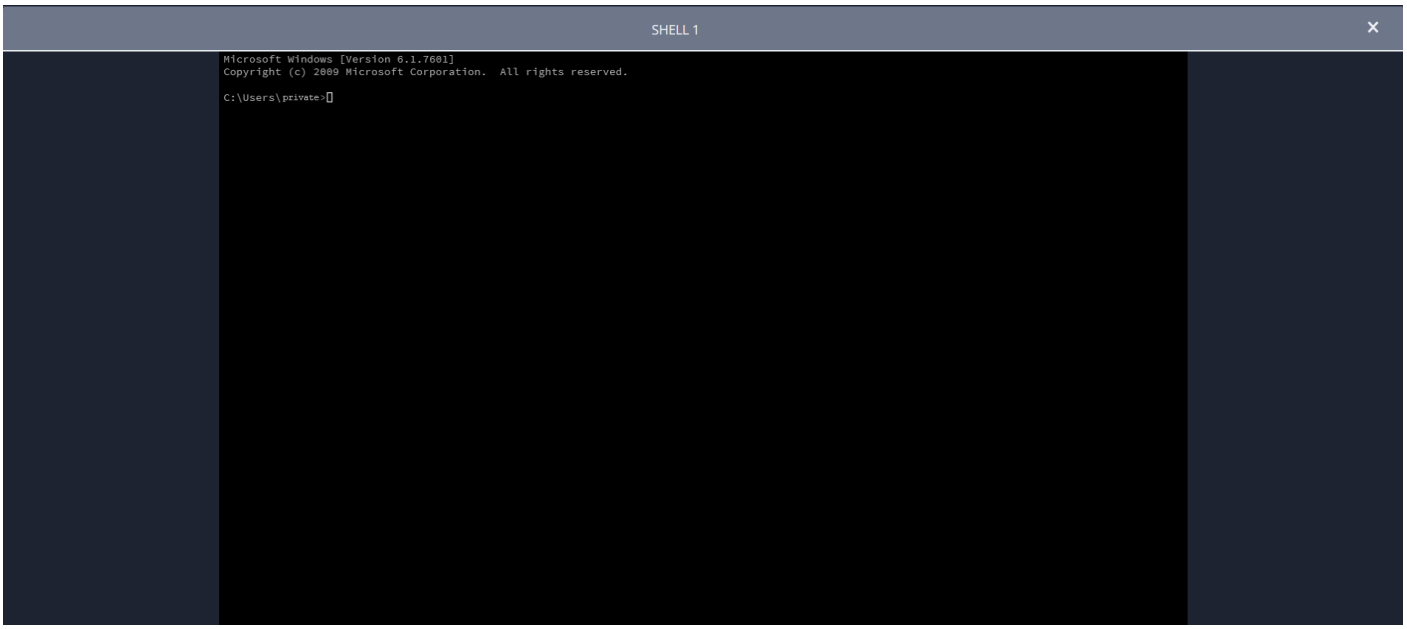
De opdrachtshell op het externe eindpunt openen via de Privileged Web-console

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.

1. Om in een toegangssessie toegang tot de **Opdrachtshell** te krijgen, moet u op de vervolgkeuzelijst **Scherm delen** in de bovenhoek van het scherm klikken.
2. Selecteer de optie **Opdrachtshell**.
3. Nadat u de optie **Opdrachtshell** hebt gekozen, verschijnen de opties voor opdrachten en verschijnt een prompt.





Ondersteuningsgereedschappen opdrachtshell

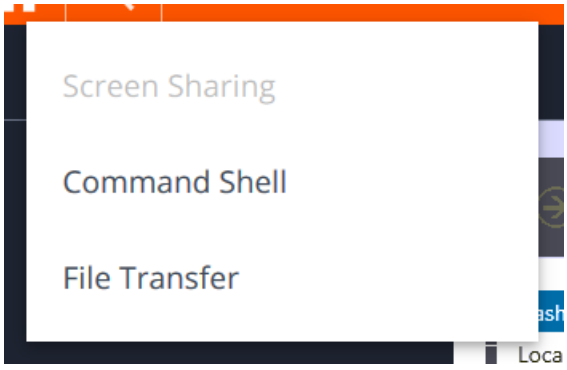
	Stop de toegang tot de opdrachtregel als u deze niet meer nodig hebt.
	Open een nieuwe shell om meerdere opdrachtregels uit te voeren of individuele shells te sluiten zonder toegang tot opdrachtregels te verlaten. Shells worden in tabbladen onderaan het scherm weergegeven.

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

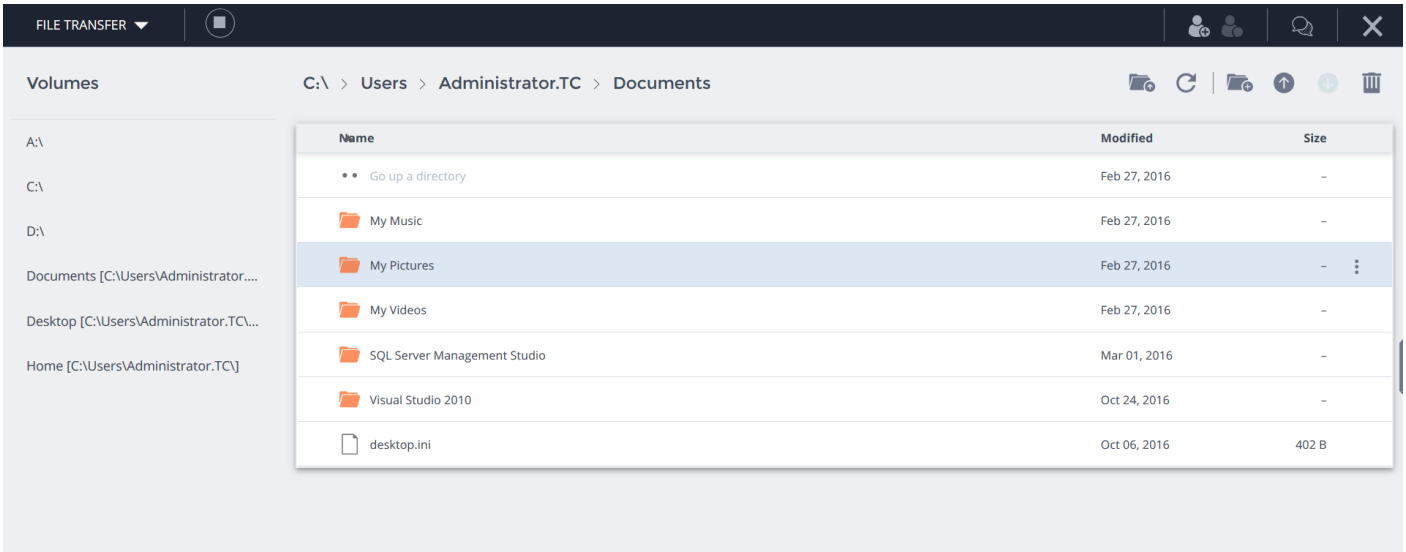
Bevoorrechte gebruikers kunnen tijdens een sessie bestanden en zelfs gehele mappen overdragen, verwijderen of de naam ervan wijzigen, van en naar de externe computer of van het externe apparaat en van of naar de SD-kaart van het apparaat. U hoeft geen volledige besturing over de externe computer te hebben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



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.



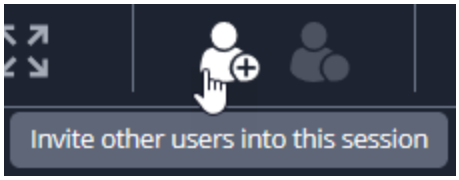
Hulpmiddelen voor bestandsoverdracht

 	Start of 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.
	Maak een nieuwe map aan.
	Upload een bestand naar een map.
	Download de geselecteerde bestanden vanuit een map.
	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.*

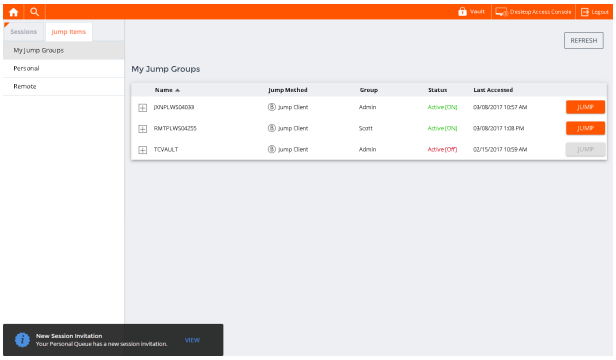
Een sessie delen met andere gebruikers via de Privileged Web-toegangsconsole

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

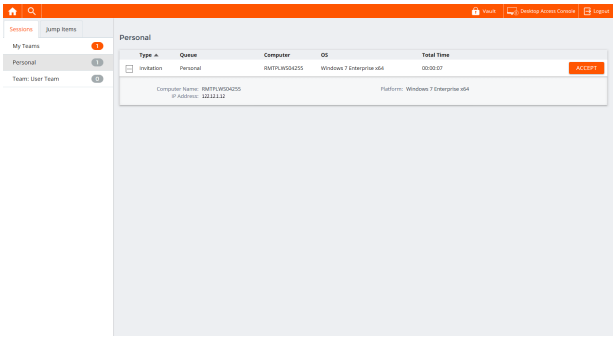
1. Klik op het pictogram **Andere gebruikers voor deze sessie uitnodigen**.
2. Selecteer uit het menu het team waar de gebruiker lid van is.
3. Kies uit de lijst met teamleden de gebruiker waar u de sessie mee wilt delen.



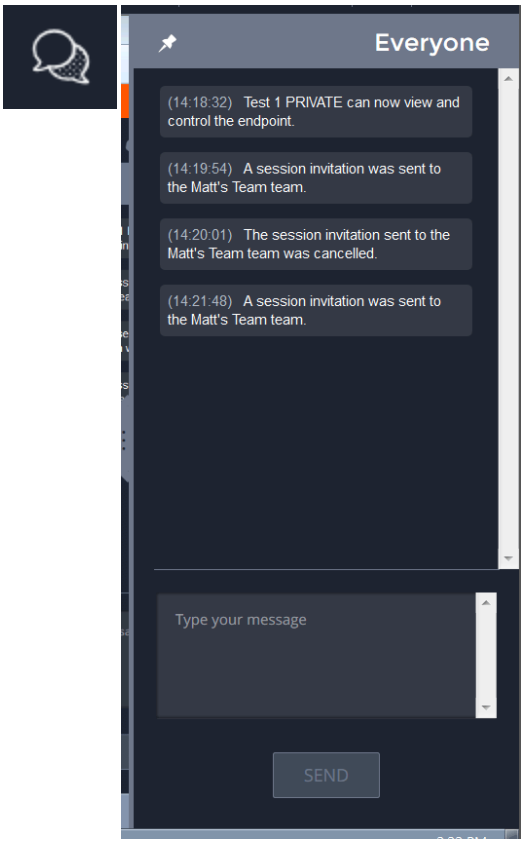
4. Uitgenodigde gebruikers zien in de linkeronderhoek van het scherm een uitnodiging verschijnen voor een nieuwe sessie.



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 **Chatten** 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 access console 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 access console 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.

Een lid van een Privileged Web-toegangsconsolesessie verwijderen

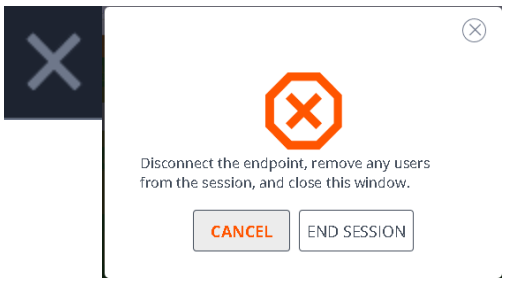
U kunt, indien nodig, een andere gebruiker uit een gedeelde toegangssessie verwijderen. Om een gebruiker te verwijderen, moet u op het pictogram **Lid verwijderen** klikken.

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

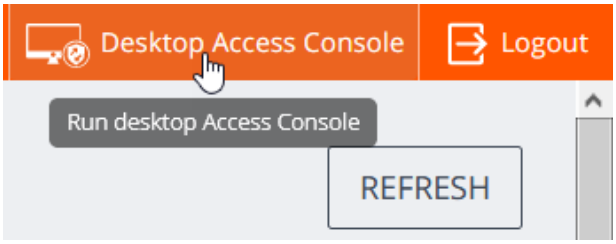
1. Klik op het pictogram **X** rechtsboven in het scherm om een toegangssessie te verlaten. Als u eigenaar van de sessie bent, moet u er rekening mee houden dat de actie **Sessie beëindigen** de sessiepagina in uw access console sluit en dat eventuele extra leden die de sessie delen, worden verwijderd.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



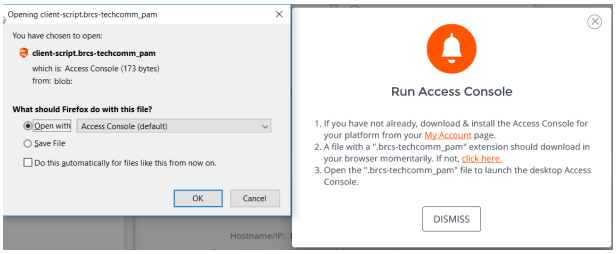
Het eigen bureaublad van de Privileged Web-toegangsconsole downloaden

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

1. U kunt de systeemeigen bureaubladtoepassing van access console via de privileged web access console downloaden door op de knop **Bureaublad Access Console** in de rechterbovenhoek van het scherm te klikken.



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.*