BeyondTrust

Privileged Remote Access 23.2 Gebruikershandleiding voor de toegangsconsole

TC:12/12/2023

Inhoudsopgave

BeyondTrust-toegangsconsole

Deze gids is bedoeld om u te helpen bij het installeren van de BeyondTrust-toegangsconsole op uw computer en om de functies van het systeem te begrijpen. BeyondTrust Privileged Remote Access stelt u in staat om toegang te krijgen tot externe eindpunten door een verbinding op te zetten via de BeyondTrust Appliance B Series.

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. Nadat BeyondTrust correct is geïnstalleerd, kunt u direct toegang krijgen tot uw eindpunten. Neem contact op met BeyondTrust Technical Support via www.beyondtrust.com/support als u ondersteuning nodig hebt.

De toegangsconsole installeren

Ga in uw webbrowser naar de URL van het B Series Appliance gevolgd door **/login** en voer de door uw beheerder ingestelde gebruikersnaam en het wachtwoord in. Als u de eerste keer inlogt, dan kan u worden gevraagd uw wachtwoord te wijzigen.

Download en installeer de BeyondTrust-toegangsconsole vanaf de pagina **Mijn account**. De optie heeft standaard het juiste installatieprogramma voor uw besturingssysteem.

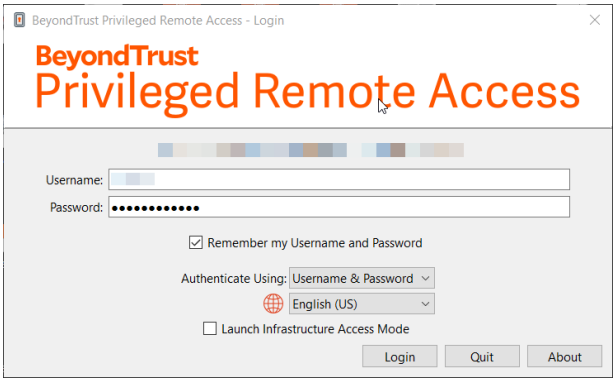
> ***Opmerking:*** *Op een Linux-systeem moet u het bestand op uw computer opslaan en het dan vanaf die locatie openen. Gebruik niet de koppeling* ***Openen*** *die na het downloaden bij sommige browsers verschijnt.*

Volg de instructies om de software te installeren als de installatiewizard verschijnt. Nadat u de toegangsconsole hebt geïnstalleerd, kunt u kiezen voor **BeyondTrust-Toegangsconsole nu uitvoeren** en/of **Uitvoeren bij opstarten**. Klik vervolgens op **Voltooien**.

> ***Opmerking:*** *Als u tijdens installeren kiest voor* ***BeyondTrust Toegangsconsole nu uitvoeren****, verschijnt er een loginprompt op uw scherm.*

Aanmelden bij de PRA-toegangsconsole

Nadat u de BeyondTrust-console hebt geïnstalleerd, kunt u de toegangsconsole openen vanuit de locatie die u tijdens de installatie hebt opgegeven.



> ***Opmerking:*** *Standaard kunt u in Windows toegang tot de toegangsconsole krijgen via* ***Start > Alle programma's > Bomgar > toegang.voorbeeld.nl****, waarbij* ***toegang.voorbeeld.nl*** *de hostnaam is van de site waar u de console hebt gedownload.*

Als de **Inlogovereenkomst** is ingeschakeld, moet u op **Accepteren** klikken om verder te gaan.

Voer op de prompt uw gebruikersnaam en wachtwoord in.

Aanmelden zonder wachtwoord

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**.

Modus infrastructuurtoegang

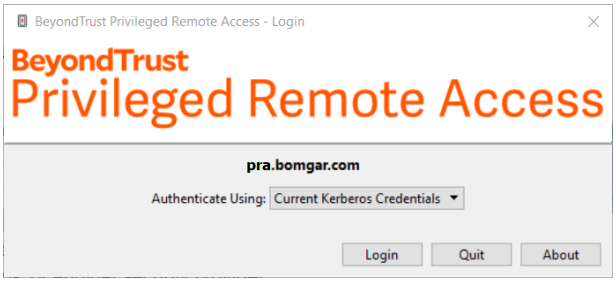
Geavanceerde gebruikers geven er mogelijk de voorkeur aan om de modus infrastructuurtoegang te gebruiken. Dit is voornamelijk om snel toegang te krijgen tot protocol- en databasetunneling en voor BYOT-sessies. Schakel desgewenst **Modus infrastructuurtoegang starten** in. De modus infrastructuurtoegang is niet beschikbaar op Linux-systemen.

> ***Opmerking:*** *Als meer dan één taal is ingeschakeld voor uw site, selecteer dan in het vervolgkeuzemenu de taal die u wilt gebruiken.*

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

Kerberos-server gebruiken

Maar als uw beheerder een Kerberos-server heeft geconfigureerd voor eenmalige aanmelding, dan kunt u op de console inloggen zonder uw inloggegevens in te voeren. De toegangsconsole onthoudt het laatst gebruikte aanmeldmechanisme –ongeacht of lokale inloggegevens, Kerberos of een andere beveiligingsprovider werd gebruikt.



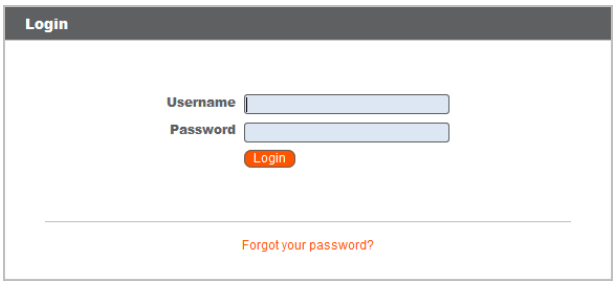
Uitgenodigde gebruikers kunnen ook een sessiecode invoeren om eenmalig een gedeelde sessie bij te wonen.

Klik op **Opgeslagen logins inschakelen** om te zorgen dat de console uw gebruikersnaam en wachtwoord opslaat. Deze optie kan vanaf **/login > Beheer > Beveiliging** worden in- of uitgeschakeld.

Nadat u bent ingelogd, wordt de console geopend en wordt er een BeyondTrust-pictogram in het systeemvak van uw computer weergegeven.

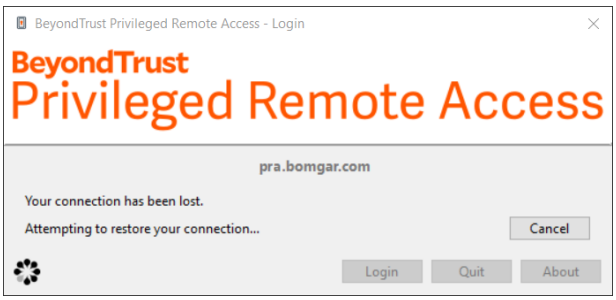
Opmerking: *Uw beheerder kan vereisen dat u een toegestaan netwerk gebruikt om bij de console aan te melden. Deze netwerkbeperking geldt mogelijk de eerste keer dat u zich aanmeldt of elke keer. Deze beperking is niet van toepassing op toegangsuitnodigingen.*

Opmerking: *Als u uw wachtwoord bent vergeten, gaat u naar* ***/login*** *en klikt u op de koppeling* ***Uw wachtwoord vergeten?*** *Deze optie is ingesteld door uw beheerder. Neem contact op met uw beheerder als u deze optie niet hebt.*



Als uw verbinding wordt verbroken, probeert de toegangsconsole de verbinding gedurende 60 seconden te herstellen. Als uw verbinding binnen deze tijd wordt hersteld, wordt uw toegangsconsole opnieuw geopend, waarbij al uw open sessies worden hersteld. Maar als uw verbinding niet binnen deze tijd kan worden hersteld, wordt u gevraagd opnieuw in te loggen of af te sluiten.

Als u op de ene locatie bij de toegangsconsole bent ingelogd en u daarna op een andere locatie aanmeldt, blijven uw open sessies behouden.



Opmerking: *U kunt alleen inloggen met een account dat al in gebruik is en de verbinding op een ander systeem verbreken als de instelling* ***Sessie beëindigen als account wordt gebruikt*** *op de pagina* ***/login > Beheer > Beveiliging*** *is aangevinkt.*

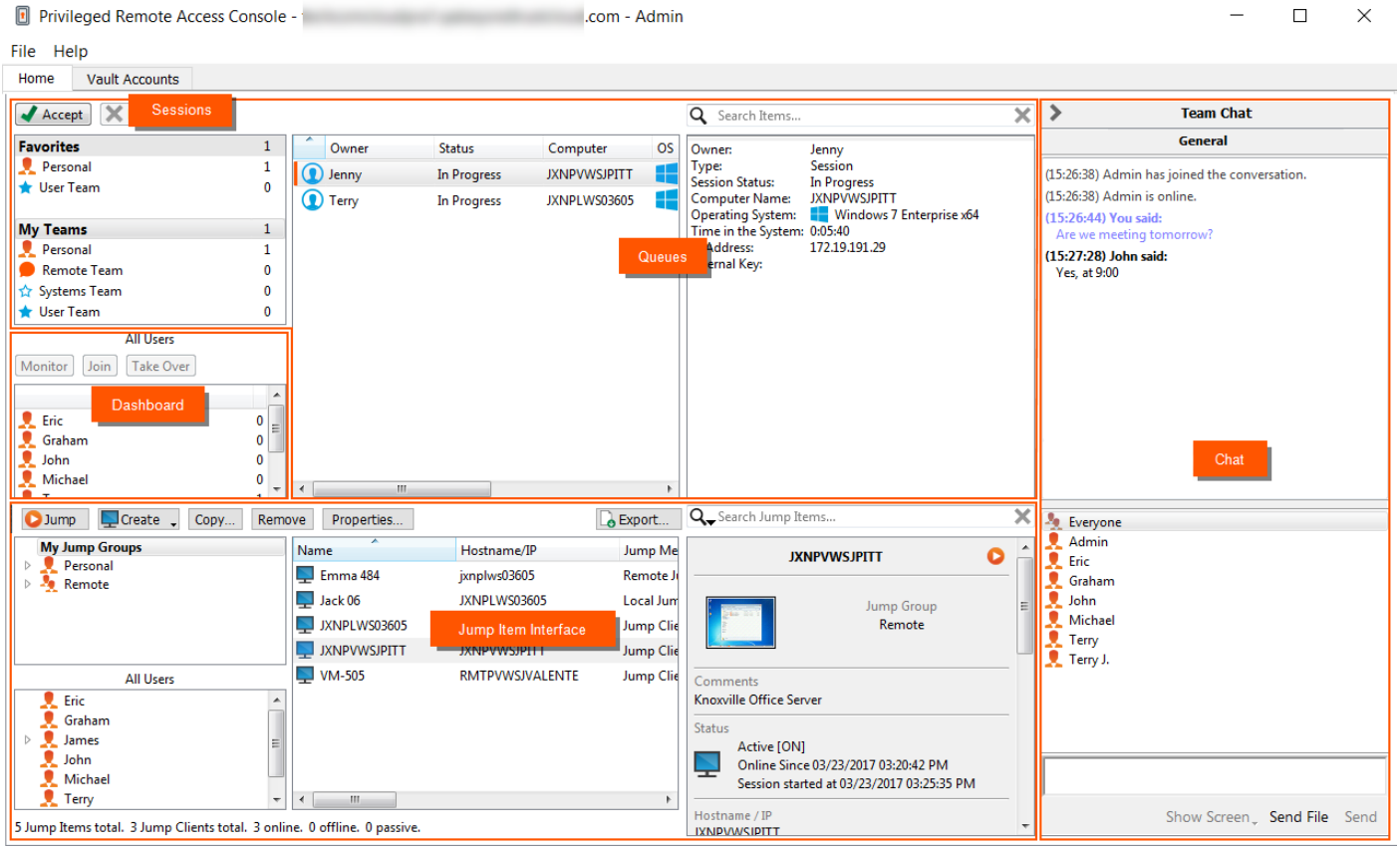
Na een upgrade of nadat de toegangsconsole voor het bureaublad voor de eerste keer is geopend, wordt het dialoogvenster **Wat is er nieuw** automatisch weergegeven als niet-uitgenodigde gebruikers inloggen. Dit dialoogvenster kan altijd worden weergegeven via het menu **Help** (**Help > Wat is er nieuw**) en toont informatie over de nieuwe release voor de huidige versie en oudere versies. Dit is een roaming-voorkeur per account. Het dialoogvenster wordt dus één keer weergegeven, ongeacht de locatie waar een gebruiker zich aanmeldt.

Voor meer informatie leest u het volgende:

- *Kijk bij het accepteren van de inlogovereenkomst naar de Websiteconfiguratie: HTTP-poorten instellen, vereiste inlogovereenkomst inschakelen op https://www.beyondtrust.com/docs/privileged-remote-access/getting-started/admin/site-configuration.htm*
- *Over uitgenodigde gebruikers: "Een externe gebruiker uitnodigen om een toegangssessie bij te wonen" op pagina 88*
- *Over het gebruik van de modus infrastructuurtoegang: "De modus infrastructuurtoegang gebruiken" op pagina 19*

Gebruikersinterface voor toegangsconsole

De toegangsconsole bevat meerdere panelen met hulpmiddelen en informatie over sessies.



Sessies: meerdere externe sessies tegelijkertijd beheren.

Wachtrijen: in wachtrijen staan sessies die momenteel worden uitgevoerd evenals verzoeken om sessies met een ander lid van een team te delen. De gegevens over het externe systeem waartoe de sessie toegang heeft, staan in deze sectie.

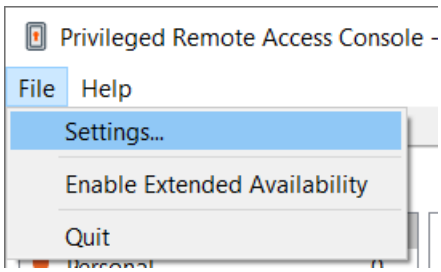
Dashboard: bevoorrechte gebruikers kunnen lopende sessies en teamleden met een lagere rol zien en meekijken, waardoor zij beheeroverzicht hebben om de medewerkers te managen.

Interface voor Jumpitem: geïnstalleerde Jump-clients en Jump-snelkoppelingen staan hier, gegroepeerd volgens wie er toegang toe kan krijgen.

Chat: chat met andere ingelogde gebruikers. U kunt uw scherm ook delen met een teamlid zonder dat u een sessie nodig hebt.

Instellingen en voorkeuren in de toegangsconsole wijzigen

Klik op **Bestand > Instellingen** in de linkerbovenhoek van de console om uw voorkeuren te configureren.



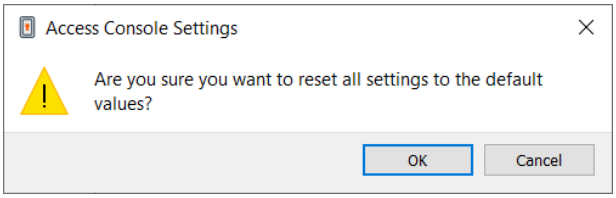
In het algemeen kunt u de console-instellingen naar uw eigen voorkeuren configureren. Uw BeyondTrust-beheerder kan er echter voor kiezen om uw instellingen te beheren en deze beheerde instellingen, desgewenst, afdwingen.

Als uw BeyondTrust-beheerder de standaardinstellingen heeft gewijzigd en toegepast, ziet u de waarschuwing **Instellingen gewijzigd** wanneer u zich de volgende keer bij uw console aanmeldt. Klik op **Instellingen weergeven** om uw instellingenvenster te openen om de wijzigingen te bekijken of klik op **OK** om de wijzigingen te bevestigen.

Instellingen wijzigen

Opmerking: *Bij deze instructies is ervan uitgegaan dat u de door uw console gebruikte instellingen vrij kunt kiezen. Instellingen die door uw beheerder zijn afgedwongen worden met een sterretje aangegeven en zijn grijs. Deze instellingen kunnen niet lokaal worden geconfigureerd. Raadpleeg uw beheerder of ga naar Instellingen voor de toegangsconsole beheren op https://www.beyondtrust.com/docs/privileged-remote-access/getting-started/admin/access-console-settings.htm voor meer informatie.*

Het venster met **Toegangsconsole-instellingen** bevat de knop **Standaardinstellingen opnieuw instellen** in de linkerbenedenhoek. Met deze knop kunt u de standaardinstellingen van BeyondTrust of eventueel door uw beheerder toegepaste standaardinstellingen opnieuw instellen. U wordt in een waarschuwingsdialoog gevraagd om te bevestigen dat u de instellingen naar de standaardinstellingen wilt wijzigen. Klik op **Annuleren** als u terug wilt keren naar de lokaal opgeslagen voorkeuren.



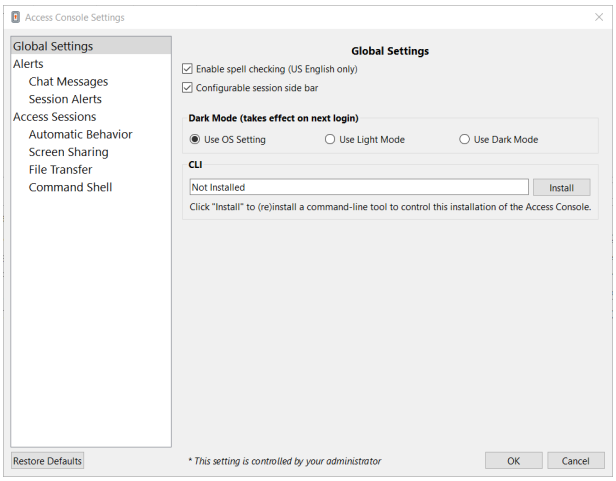
Opmerking: *Als een of meer van de standaardinstellingen door uw beheerder zijn afgedwongen, dan kunt u die niet configureren.*

U kunt onder het kopje **Algemene instellingen** kiezen om de spellingcontrole in of uit te schakelen voor de chat. Momenteel is spellingcontrole alleen beschikbaar voor Amerikaans Engels.

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

U kunt ervoor kiezen om uw weergavemodus te wijzigen. De opties zijn onder meer: **OS-instelling** (standaard), **Lichte modus** en **Donkere modus**.

> ***Opmerking:*** *De optie Donkere modus geldt alleen voor Windows en macOS.*
>
> *Naast schakelen tussen weergavemodi binnen de toegangsconsole kunnen gebruikers deze ook wijzigen in* ***OS-instellingen*** *door* ***Thema's en verwante instellingen > Kleur > Kies uw kleur*** *te selecteren.*



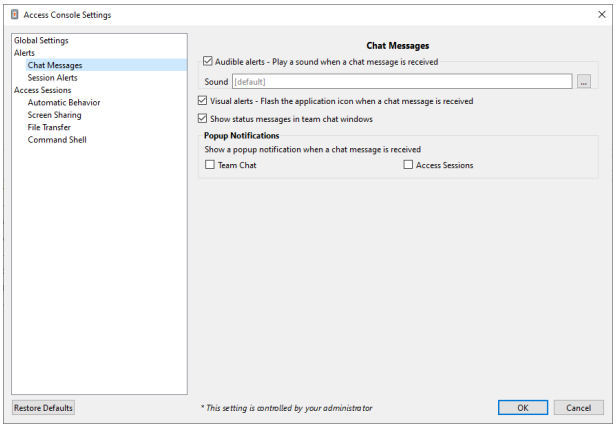
Het kopje **CLI** geeft aan of er een hulpprogramma voor de opdrachtregelinterface is geïnstalleerd voor deze installatie van de Toegangsconsole. Als dat niet het geval is, kunt u op **Installeren** klikken om het te installeren.

Kies uw instellingen voor waarschuwingen voor chatberichten. Als u een chatbericht ontvangt, dan kunt u kiezen of u een geluid hoort en het pictogram van de toepassing ziet knipperen.

Als u een aangepast geluid voor chatberichten wilt uploaden, klik dan op de knop **[...]** en selecteer een WAV-bestand op uw computer. Het bestand mag maximaal 1 MB groot zijn.

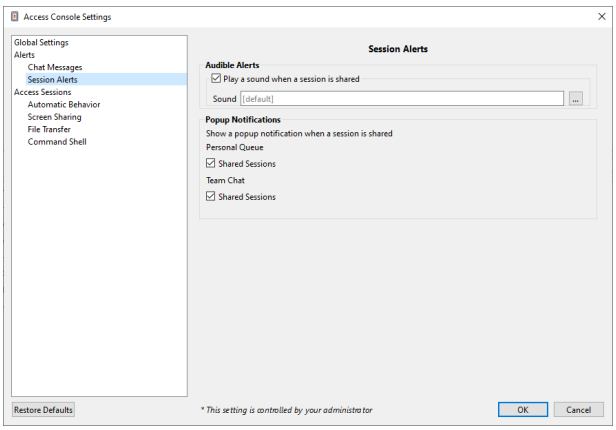
Kies of statusberichten in de teamchat worden meegenomen, zoals het in- of uitloggen van gebruikers, of alleen de tussen teamleden verzonden chats.

Kies of u popup-meldingen wilt ontvangen voor berichten die u in een teamchat en/of een sessiechat ontvangt.



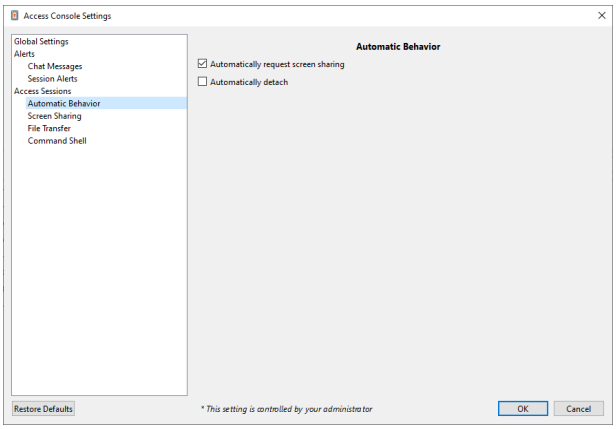
Kies of u een waarschuwingsgeluid wilt horen als een andere gebruiker vraagt om een sessie met u te delen. Als u een aangepast geluid voor gedeelde sessies wilt uploaden, klik dan op de knop **[...]** en selecteer een WAV-bestand op uw computer. Het bestand mag maximaal 1 MB groot zijn.

U kunt ook kiezen om pop-up-meldingen te ontvangen voor bepaalde gebeurtenissen. Deze meldingen verschijnen onafhankelijk van uw console en bovenop andere vensters. Stel in waar u popup-meldingen wilt ontvangen en hoe lang deze zichtbaar moeten zijn.



Kies of u bij het begin van een sessie automatisch scherm delen wilt opstarten.

U kunt ervoor kiezen sessies als tabbladen in de console te openen of om automatisch sessies los te koppelen en in nieuwe vensters weer te geven.

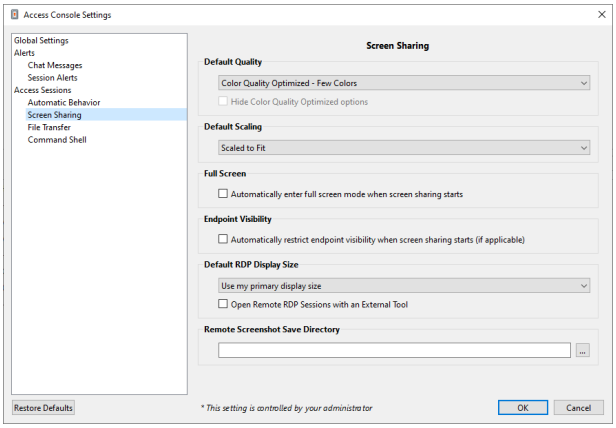


Stel de standaard kwaliteit en afmetingen in voor een sessie met scherm delen. Als scherm delen start, dan kunt u automatisch naar volledig scherm gaan, waarbij dan weer automatisch de chatbalk kan worden ingeklapt.

Daarnaast kan het externe systeem tijdens Scherm delen het scherm, de muis en de toetsenbordinvoer automatisch beperken en een privacyscherm weergeven.

Selecteer de standaard RDP-schermgrootte voor alle RDP-sessies.

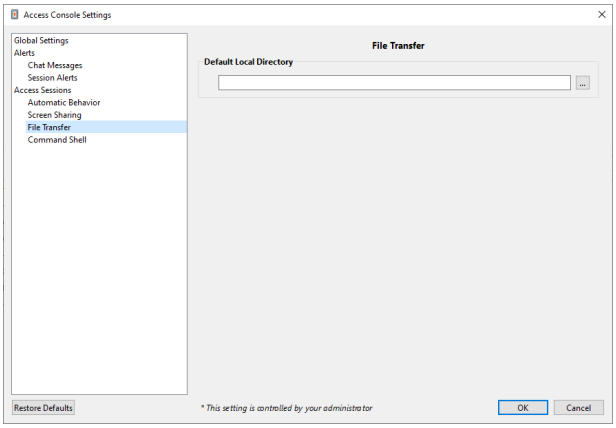
Een optie biedt u de mogelijkheid om een PRA-verbinding te openen die op alle beeldschermen wordt weergegeven op de clientcomputer, ongeacht de configuratie van het clientbeeldscherm. Met deze functie kun u alle beeldschermen die verbonden zijn met de clientcomputer volledig benutten. U kunt zo de schermgrootte en -schaal aanpassen tijdens een RDP-sessie op meerdere beeldschermen.



Als u uw eigen RDP-hulpprogramma wilt gebruiken, zet dan een vinkje bij **Externe RDP-sessies openen met een extern hulpprogramma**.

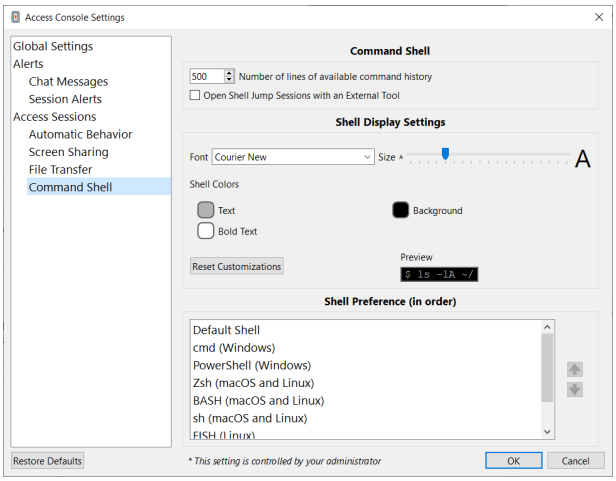
Om eenvoudiger toegang te krijgen tot schermopnames die u vanaf de console maakt, kunt u de standaardmap instellen waarin u de schermopnames van het externe systeem op wilt slaan die u via uw console hebt gemaakt.

Voor eenvoudiger bestandsoverdracht kunt u de standaard map instellen waarvandaan u op uw lokale systeem wilt gaan bladeren.



Stel het aantal regels in dat u in de historie van de opdrachtshell wilt opslaan.

Als u uw eigen SSH-hulpprogramma wilt gebruiken, zet dan een vinkje bij **Shell Jump-sessies openen met een extern hulpprogramma**. Deze instelling is van toepassing op zowel de opdrachtshell als Shell Jump.



> ***Opmerking:*** *De instelling* ***Open Shell Jump-sessies met een externe tool*** *kent beperkingen als deze wordt gebruikt met de opdrachtshell. De proxy is alleen voor de shell en vormt geen volledige SSH-tunnel. Voor bestandsoverdrachten zijn bijvoorbeeld nog steeds de bestaande hulpprogramma's op de Jump-client nodig.*

BELANGRIJK!

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

U kunt het scherm van de opdrachtshell wijzigen door het lettertype, de lettergrootte, de tekstkleur en de achtergrondkleur te selecteren.

Er zijn verschillende opties voor de standaardshell beschikbaar, waaronder Windows Opdrachtprompt, PowerShell, Zsh, Bash, sh, fish en tcsh. Selecteer elke shell en gebruik de pijltjesknoppen naast de lijst om de geselecteerde shell omhoog of omlaag te verplaatsen en daarmee de volgorde van de voorkeur voor shells in te stellen. Sessies starten met de eerst beschikbare shell voor de sessie.

> *Meer informatie over het gebruik van het hulpprogramma voor de opdrachtregelinterface voor de toegangsconsole vindt u in* *"De CLI gebruiken voor de Toegangsconsole" op pagina 16**.*

De CLI gebruiken voor de Toegangsconsole

Met het hulpprogramma voor de opdrachtregelinterface (CLI) kunt u sessies op afstand rechtstreeks starten en beheren via de opdrachtregel.

U moet zijn aangemeld bij de toegangsconsole en het CLI-hulpprogramma moet zijn geïnstalleerd om het te kunnen gebruiken. U kunt het hulpprogramma installeren vanuit **Algemene instellingen**. Tijdens de installatie ontvangt u mogelijk instructies om de installatielocatie toe te voegen aan het PATH, maar het is ook mogelijk dat het installatieproces de locatie zelf toevoegt aan het PATH.

Voer na de installatie opdrachten in een terminal of het dialoogvenster *uitvoeren* in om te communiceren met het exemplaar van de aangemelde ondersteuningstechnicus.

Opmerking: *De opdrachten werken alleen als u bent aangemeld bij de toegangsconsole.*

Opdrachten invoeren

Voer één CLI-opdracht in met subopdrachten.

Voorbeeld:

```
1bt ssh <user>@<host>
```

Subopdrachten zien er als volgt uit:

```
bt <command>
```

Een sessie starten

Zoek een Vault-account op naam (voor typen die injecties kunnen uitvoeren) en een Jumpitem op naam. Zoekopdrachten naar Jumpitems zijn beperkt tot het type dat in de opdracht is gespecificeerd. **bt ssh** zoekt bijvoorbeeld alleen naar Shell Jumpitems.

Als er slechts één exemplaar van een gezochte naam wordt gevonden, start de sessie met dat specifieke Jumpitem en de bijbehorende referentie. Als er meer dan één resultaat wordt gevonden, ziet u een melding om het juiste account en/of Jumpitem te kiezen.

Er kan een markering worden ingesteld om de tunnelinformatie uit te voeren in een indeling die door een ander proces of script kan worden gebruikt, zodat sessie-aanroepen kunnen worden doorgegeven aan andere functies of kunnen worden opgenomen in geautomatiseerde taken, zoals VS-codetaken. Als deze markering is ingesteld, wordt de tunnelinformatie getoond. De verbinding en het externe hulpprogramma worden echter niet geopend.

onExternalToolClicked() Callback uitvoeren

De ondersteuningstechnicus kan voor alle typen, behalve voor SSH, proberen de **onExternalToolClicked()**-callback uit te voeren voor het specifieke type voordat controle wordt geretourneerd aan het CLI-hulpprogramma in plaats van dat de logica aan het CLI-hulpprogramma zelf wordt overgedragen.

Bij SSH vervangt de SSH-sessie het proces van het CLI-hulpprogramma.

Specifieke subopdrachten voor sessies gebruiken

SSH

SSH-subopdrachten zien er als volgt uit:

```
ssh <account>@<host>
```

Nadat de sessie tot stand is gebracht, start deze direct het SSH-proces om verbinding te maken met de lokale tunnel. Daarna wordt het afgesloten.

Voorbeeld: *Een SSH-sessie maken:*

```
bt ssh <user>@<host>
```

RDP

RDP-subopdrachten zien er als volgt uit:

```
rdp <account>@<host>
```

Nadat de sessie tot stand is gebracht,

- start hij de standaard RDP-client.
- toont hij de tunnelinformatie ter informatie voor de CLI.
- sluit hij af.

Voorbeeld: *Voer de volgende opdracht in om het RDP-hulpprogramma te openen:*

```
bt rdp <user>@<host>
```

DB

DB-subopdrachten zien er als volgt uit:

```
db <account>@<host>
```

Nadat de sessie tot stand is gebracht:

- start hij, indien mogelijk, de DB-client voor het geselecteerde DB-type. Een deel van de retourwaarde moet een DB-type en/of uit te voeren opdracht zijn.

- toont de informatie over de DB-verbinding.
- sluit hij af.

Protocoltunnel

Subopdrachten voor protocoltunnels zien er als volgt uit:

```
pt <host>
```

Er is geen inloggegevensinjectie voor protocoltunnels.

Nadat de sessie tot stand is gebracht, worden de tunneldefinities getoond en wordt de sessie afgesloten.

Omdat de tunnel generiek is, kan hij geen specifiek hulpprogramma starten.

Andere subopdrachten gebruiken

Lijst

Lijst-subopdrachten zien er als volgt uit:

```
list
```

De lijst-subopdracht geeft verbonden sessies weer op naam van het Jumpitem.

Sluiten

Subopdrachten om te sluiten zien er als volgt uit:

```
close <session>
```

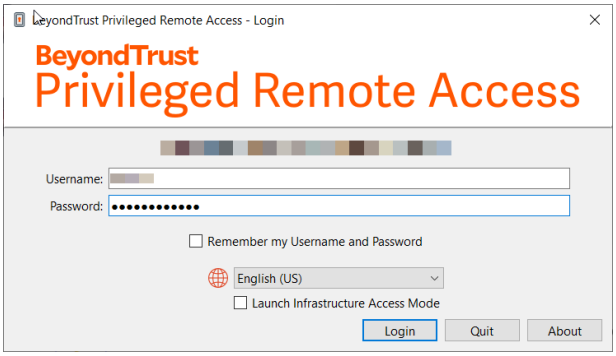
De subopdracht om te sluiten, sluit de tunnel voor de specifieke sessie.

De modus infrastructuurtoegang gebruiken

Geavanceerde gebruikers, zoals ontwikkelaars, kunnen de modus infrastructuurtoegang gebruiken wanneer ze zich aanmelden bij de console. Dat resulteert in een eenvoudiger console, die beschikbaar is in het systeemvak of de menubalk. Dit is handig voor protocol- en databasetunneling en BYOT-sessies, maar er worden ook andere sessietypes ondersteund.

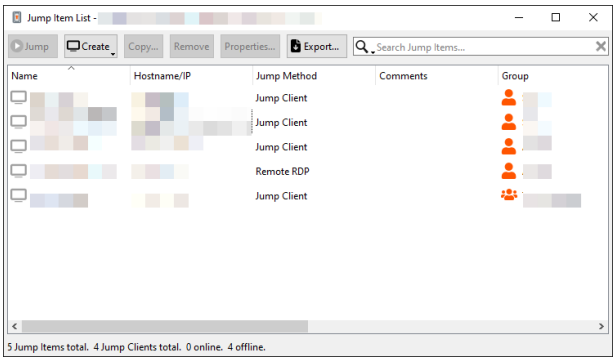
> ***Opmerking:*** *De modus infrastructuurtoegang is niet beschikbaar op Linux-systemen.*

Schakel **Modus infrastructuurtoegang starten** in op het verificatiescherm van de console om de modus infrastructuurtoegang te starten. De optie is standaard ingeschakeld als u de modus infrastructuurtoegang eerder hebt ingeschakeld.



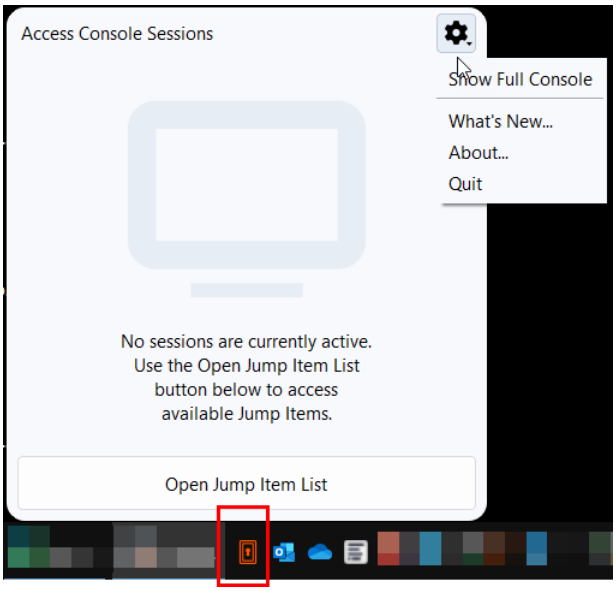
Na het aanmelden wordt het venster **Jumpitem-lijst** weergegeven. Ook wordt er een pictogram in het systeemvak (Windows) of in de menubalk (macOS) weergegeven. U kunt in deze lijst op de gebruikelijke manier een sessie selecteren en openen. Als u het sessievenster sluit, kunt u het opnieuw openen door op het pictogram Modus infrastructuurtoegang op de taakbalk te klikken, zodat het menu wordt geopend. Klik vervolgens op **Sessie weergeven**.

De eerste keer dat u alle vensters sluit, wordt er een melding weergegeven om u eraan te herinneren dat de modus infrastructuurtoegang nog actief is en dat u deze kunt openen via het pictogram in het systeemvak of op de menubalk.



Via het pictogram kunt u het venster Jumpitem-lijst openen. U kunt onder het menu met pictograminstellingen overschakelen naar de volledige toegangsconsole. U hebt de volledige console nodig om een chatsessie te starten of sessie-uitnodiging te accepteren en om bepaalde sessietypes te kunnen uitvoeren. U kunt de volwaardige toegangsconsole sluiten wanneer u die niet meer nodig hebt, waarna u de console kunt blijven gebruiken in de modus infrastructuurtoegang.

U kunt actieve sessies weergeven en sluiten via de opties bij het pictogram. Ook kunt u de modus infrastructuurtoegang beëindigen via het menu met pictograminstellingen.

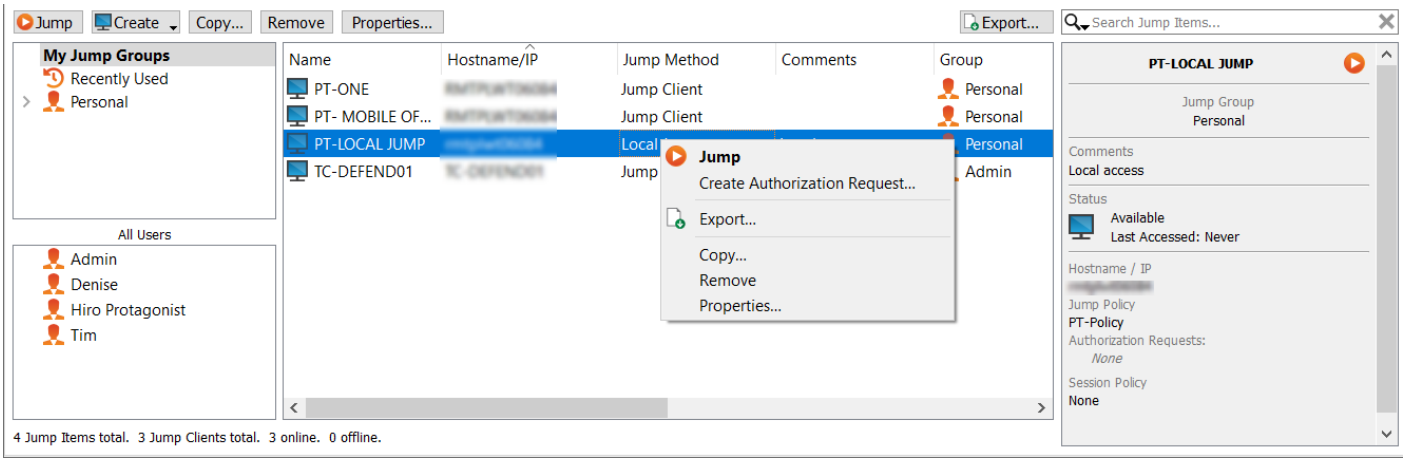


Jump-interface: Jumpitems gebruiken voor toegang tot externe systemen

De Jump-interface wordt in de onderste helft van de toegangsconsole weergegeven en bevat de Jumpitems die beschikbaar zijn. De lijst kan zowel actieve als passieve Jump-clients bevatten, evenals snelkoppelingen naar Jumps voor externe Jumps, lokale Jumps, sessies met extern bureaublad (RDP), VNC-sessies, Jumps via tunnelprotocol, Shell Jumps en Web Jumps.

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. Als u een Jumpgroep selecteert en vervolgens op **Maken** klikt, wordt de bewuste Jumpgroep automatisch geselecteerd in het configuratievenster voor het Jumpitem.

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.

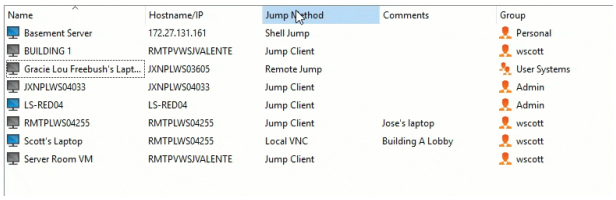


Jumpitems kopiëren

Jumpitems kunnen gekopieerd worden en kunnen bij meerdere Jumpgroepen horen. Hieronder vallen ook Jumpitems waarmee beheerders aparte beleidslijnen en groepsmachtigingen kunnen instellen zonder dat ze een extra Jump-client moeten installeren op het doeleindpunt. Gebruikers met de juiste machtigingen kunnen de optie om Jumpitems te **kopiëren** in de Toegangsconsole zien door met de rechter muisknop op het item te klikken. Gebruikers kunnen deze functie ook op meerdere Jumpitems uitvoeren.

Met behulp van deze functie kunnen beheerders en gebruikers op een doeltreffende manier verschillende beleidslijnen voor Jumpitems en Jump-clients beheren, zonder dat er een nieuw Jumpitem moet worden aangemaakt. Met deze functie kunnen gebruikers het aantal clients beperken dat nodig is om Jump-clientsessies mogelijk te maken. Ook wordt hiermee het aantal handmatige beheertaken teruggedrongen wanneer er toegangspaden voor gebruikers worden gedefinieerd.

Jump naar een Jumpitem



Blader door de groepen op zoek naar de computer waartoe u toegang wilt hebben. Om het bladeren door een lijst met Jumpitems te ondersteunen, kunt u de kolommen verslepen naar elke gewenste volgorde. Vervolgens kunt u een kolom sorteren door op de kolomkop te klikken. De toegangsconsole onthoudt de volgorde van de kolommen en de sorteervolgorde als de toegangsconsole de volgende keer wordt geopend.

Behalve naar Jumpitems bladeren, kunt u ook een zoekopdracht uitvoeren op basis van verschillende velden. Voer een tekenreeks in het zoekveld in en druk op **Enter**. Om de velden die u wilt zoeken te wijzigen, klikt u op het vergrootglas en vinkt u de beschikbare al dan niet aan. Voorbeelden van doorzoekbare velden zijn: **Opmerkingen**, **Consolegebruiker**, **Domein**, **FQDN**, **Groep**, **Hostnaam/IP-adres**, **Jump-methode**, **Laatste toegang**, **Naam**, **Privé-IP-adres**, **Openbaar IP-adres**, **Status**, **Label** en **Werkgroep**.

Als u de computer hebt gevonden waar u toegang toe wilt krijgen, dan moet u op de vermelding ervan dubbelklikken of deze selecteren en op de knop **Jump** klikken. Dan wordt een poging gedaan een sessie met de externe computer op te starten.

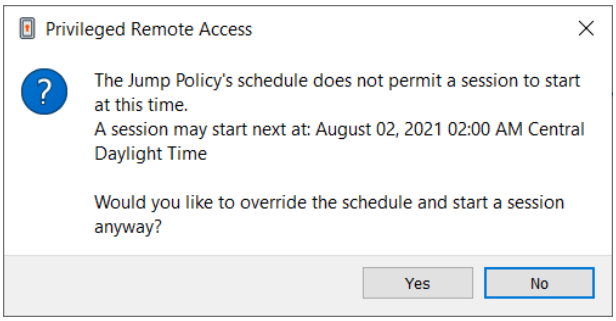
U kunt met een programma direct vanaf uw hulpprogramma voor systeembeheer of ticketsysteem verbinding maken met een Jumpitem. Als uw zoekopdracht maar één Jumpitem oplevert, dan start de sessie meteen. Als er meerdere Jumpitems worden gevonden, dan moet u een van de in het selectievenster vermelde Jumpitems selecteren en op **OK** klikken.

> ***Opmerking:*** *Zie voor meer informatie over scripts Toegangsconsole-scripting en API voor clientscripts op www.beyondtrust.com/docs/privileged-remote-access/how-to/integrations/api/client-script.*

Als er op het Jumpitem een jump-beleid van toepassing is, dan bepaalt dat beleid hoe en/of wanneer toegang tot een Jumpitem mag worden verkregen.

Rooster

Als een Jump-beleid een rooster aan dit Jumpitem oplegt, dan voorkomt een poging om buiten dit rooster om toegang tot het Jumpitem te verkrijgen, dat de Jump plaatsvindt. U krijgt een prompt te zien met informatie over de restricties als gevolg van het beleid en met de datum en tijd waarop het Jumpitem weer toegankelijk is.



Kennisgeving

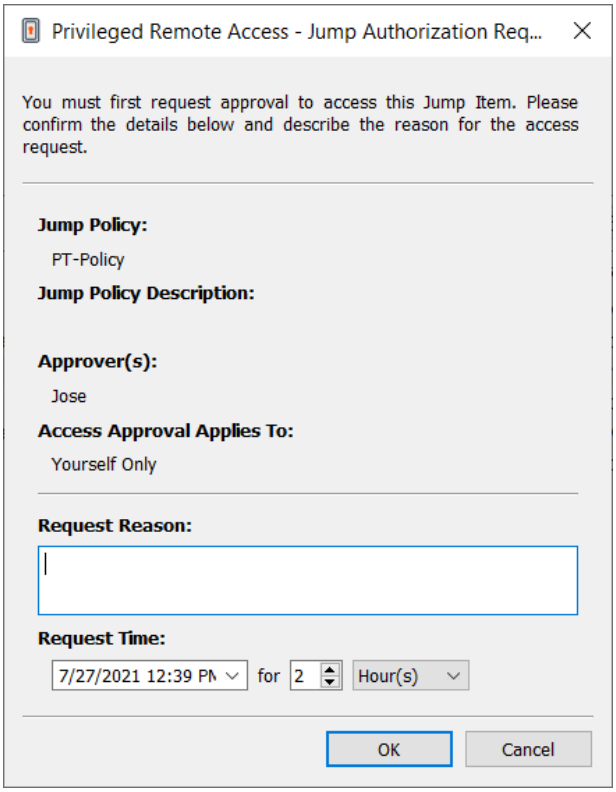
Als een Jump-beleid is geconfigureerd om bij het starten of beëindigen van sessies een melding te verzenden, ziet u een melding dat er een e-mail zal worden verzonden als u een Jumpitem probeert te openen. U kunt kiezen verder te gaan met de Jump en de kennisgeving te verzenden, of u kunt de Jump annuleren.

Ticket-ID

Als voor een Jump-beleid een ticket-ID van uw externe ITSM of ticket-ID-systeem moet worden ingevoerd voordat de Jump kan worden uitgevoerd, dan wordt een dialoog geopend. Voer in de dialoog de gevraagde ticket-ID in waarmee u toestemming krijgt om dit Jumpitem te gebruiken.

Autorisatie

Als voor een Jump-beleid autorisatie is vereist voordat de Jump kan worden uitgevoerd, dan wordt een dialoog geopend. Voer in de dialoog de reden in waarom u dit Jumpitem moet gebruiken. Voer vervolgens de datum en het tijdstip in waarop u wilt dat de autorisatie ingaat, evenals hoe lang u toegang tot het Jumpitem nodig hebt. Zowel de reden voor de aanvraag als het tijdstip zijn zichtbaar voor de fiatteur en helpen hem of haar om te beslissen of de toegang kan worden goedgekeurd of moet worden geweigerd.



Als u op **OK** klikt, dan wordt een e-mail verzonden naar de adressen die als fiatteurs voor dit beleid zijn gedefinieerd. Deze e-mail bevat een URL waar een fiatteur het verzoek kan zien, opmerkingen kan toevoegen en het verzoek kan goedkeuren of weigeren.

Als het verzoek door één persoon is goedgekeurd, kan een tweede persoon naar de URL gaan om de goedkeuring te overschrijven en te weigeren. Als een verzoek was geweigerd, dan kan elke andere fiatteur die naar de site gaat de gegevens zien maar kan de status geweigerd niet overschrijven. Als een gebruiker al een goedgekeurde sessie uitvoert, dan kan die toegang niet meer worden geweigerd. Hoewel andere fiatteurs het e-mailadres kunnen zien van de persoon die het verzoek heeft goedgekeurd of geweigerd, kan de aanvrager dit niet. Afhankelijk van de instellingen van het Jump-beleid kan een goedgekeurd verzoek toegang verlenen aan elke gebruiker die de betreffende Jump-client kan zien en er toegang toe kan vragen, of alleen aan de gebruiker die toegang heeft gevraagd.

In de Jump-interface wordt in het deelvenster met informatie over het Jumpitem de status van eventuele autorisatieverzoeken weergegeven als in behandeling, goedgekeurd, alleen goedgekeurd voor een andere gebruiker of geweigerd. Als een fiatteur een verzoek beantwoordt, dan verschijnt een popup-melding op het scherm van de aanvrager om hem of haar te waarschuwen dat de toegang is toegestaan of geweigerd. Als de aanvrager een e-mailadres heeft geconfigureerd, wordt er een kennisgeving per e-mail aan de aanvrager verzonden.

Als een gebruiker een Jump naar een Jumpitem uitvoert waarvoor toestemming is gegeven, dan krijgt hij of zij een kennisgeving met eventuele opmerkingen van de fiatteur.

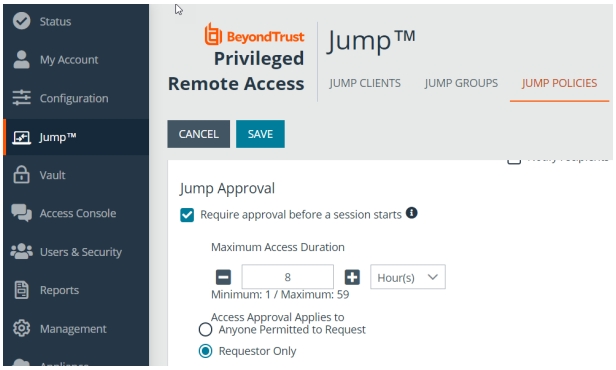
Wanneer goedkeuring voor een Jumpitem is verleend, komt dat Jumpitem beschikbaar ofwel voor elke gebruiker die het betreffende Jumpitem kan zien en er toegang toe kan aanvragen of alleen voor de gebruiker die toestemming heeft aangevraagd. Dit wordt bepaald door het Jump-beleid.

> ***Opmerking:*** *Er kunnen meerdere verzoeken worden verzonden voor verschillende tijden. De aangevraagde toegangstijden kunnen elkaar overlappen als de Jump-goedkeuringsaanvraag het kenmerk* ***Alleen verzoeker*** *heeft. De toegangstijden kunnen elkaar niet overlappen als de goedkeuring* ***Iedereen mag een aanvraag indienen*** *betreft. Als een verzoek is geweigerd, dan mag voor hetzelfde tijdstip een tweede verzoek worden verzonden.*

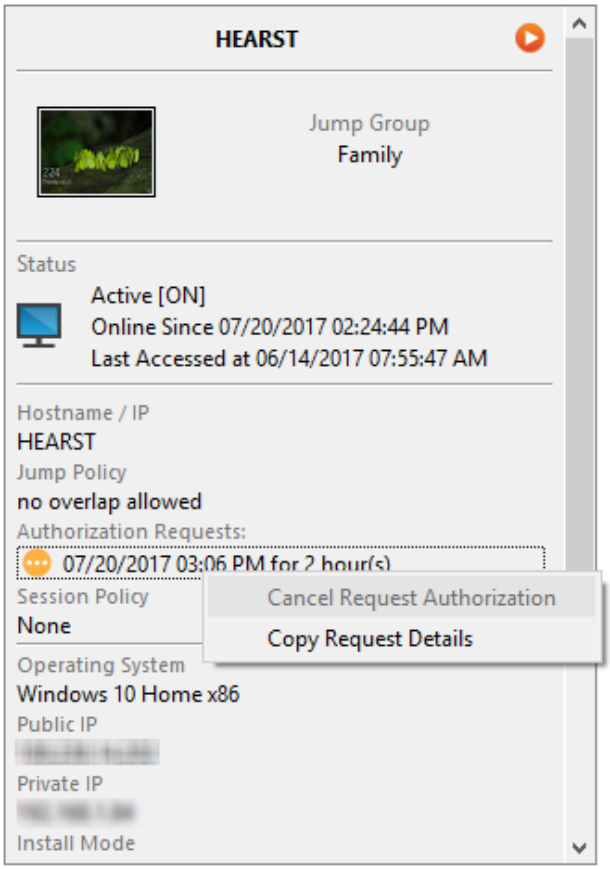
Een goedkeuringsaanvraag voor toegang intrekken

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:

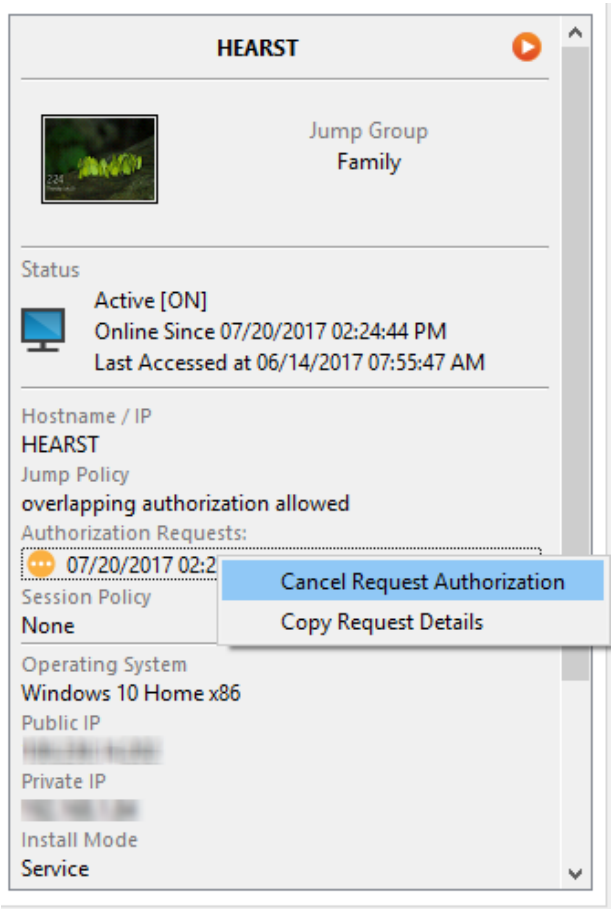
- **Iedereen mag een aanvraag indienen**
- **Alleen verzoeker**



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.



Jump-clients gebruiken om toegang tot externe eindpunten te krijgen

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 verschijnen in de Jump-interface naast andere typen Jumpitems.

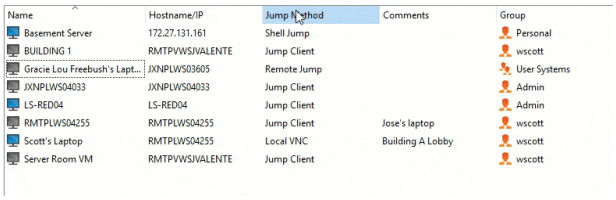
Een Jump-client gebruiken

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

> ***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.*

Jump-clients sorteren

Blader door de groepen op zoek naar de computer waartoe u toegang wilt hebben. Om het bladeren door een lijst met Jumpitems te ondersteunen, kunt u de kolommen verslepen naar elke gewenste volgorde. Vervolgens kunt u een kolom sorteren door op de kolomkop te klikken. De toegangsconsole onthoudt de volgorde van de kolommen en de sorteervolgorde als de toegangsconsole de volgende keer wordt geopend.



Naar een Jump-client zoeken

Behalve naar Jumpitems bladeren, kunt u ook een zoekopdracht uitvoeren op basis van verschillende velden. Voer een tekenreeks in het zoekveld in en druk op **Enter**. Om de velden die u wilt zoeken te wijzigen, klikt u op het vergrootglas en vinkt u de beschikbare al dan niet aan. Voorbeelden van doorzoekbare velden zijn: **Opmerkingen**, **Consolegebruiker**, **Domein**, **FQDN**, **Groep**, **Hostnaam/IP-adres**, **Jump-methode**, **Laatste toegang**, **Naam**, **Privé-IP-adres**, **Openbaar IP-adres**, **Status**, **Label** en **Werkgroep**.

Detailvenster Jump-clients

Als u een Jump-client selecteert, wordt er een deelvenster met details rechts naast de Jump-interface weergegeven. Welke details daar worden weergegeven, wordt bepaald door de instelling **Statistieken voor Jump-Clients** in het /login-scherm en door het externe besturingssysteem.

Als een Jump-client offline gaat en gedurende het aantal dagen dat voor **Instellingen voor Jump-Clients** in het /login-interface is ingesteld niet opnieuw verbinding met het B Series Appliance maakt, wordt de client aangemerkt als verloren. Er wordt geen specifieke actie op de Jump-client uitgevoerd. Deze wordt alleen als 'Verloren' aangemerkt ter identificatie, zodat een beheerder de reden voor de verbroken verbinding kan diagnosticeren en actie kan ondernemen om de situatie te corrigeren. In het detailvenster wordt de geplande verwijderingsdatum weergegeven voor het geval de Jump-client geen verbinding meer maakt.

Jump-clients worden automatisch bijgewerkt na een software-update. Het aantal gelijktijdige upgrades van Jump-clients wordt bepaald door instellingen op de pagina **/login > Jump > Jump-clients**. Als een Jump-client nog niet is bijgewerkt, wordt deze gemarkeerd als

Upgrade in behandeling. De versie en het revisienummer worden in het detailvenster weergegeven. U kunt een verouderde Jump-client wijzigen, maar er niet naar jumpen. Als u een jump probeert uit te voeren, wordt de Jump-client echter vooraan in de upgradewachtrij geplaatst.

Wake-On-Lan (WOL)

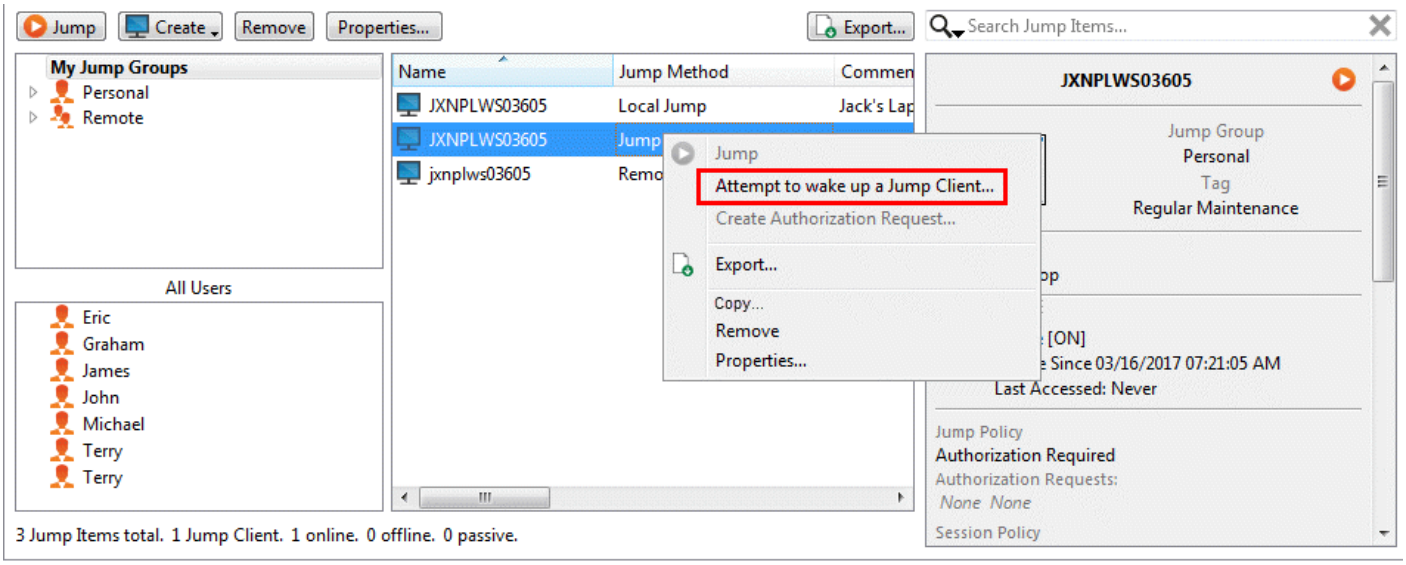
Met Wake-On-Lan (WOL) kunt u systemen waarvoor in BeyondTrust WOL is geconfigureerd op afstand inschakelen of uit de slaapstand halen. Klanten kunnen in een geconfigureerde omgeving hun systeem uitschakelen, maar ontvangen zo nodig nog steeds ondersteuning van BeyondTrust.

> ***Opmerking:*** *WOL is geen technologie van BeyondTrust. De BeyondTrust-software kan worden geïntegreerd met bestaande WOL-systemen. Om WOL via BeyondTrust te gebruiken, moet WOL op het systeem zijn ingeschakeld en moet het netwerk het verzenden van WOL-pakketten toestaan.*

U kunt ondersteuning voor WOL in BeyondTrust inschakelen door de WOL-instelling in te schakelen in de /login-beheerinterface **Jump > Jump-clients**. Wanneer u WOL inschakelt, moet u met het volgende rekening houden:

- WOL werkt niet voor draadloze clients. U moet een vaste netwerkverbinding hebben.
- WOL wordt ondersteund door de onderliggende systeemhardware en is afhankelijk van het geïnstalleerde besturingssysteem.
- WOL wordt ondersteund door actieve Jump-clients. Passieve Jump-clients, Jumpoints en lokale Jumps van consoles van ondersteuningstechnici bieden geen ondersteuning voor WOL.

Om een actieve Jump-client met WOL uit slaapmodus te halen, klikt u vanuit de console van de ondersteuningstechnicus met uw rechtermuisknop op een bestaande Jump-client. U kunt een systeem uit slaapmodus proberen te halen door op de optie **Poging om de Jump-client uit de slaapmodus te halen** te klikken.



Deze optie is alleen beschikbaar als u een enkele Jump-client selecteert. De optie is niet beschikbaar wanneer meerdere Jump-clients zijn geselecteerd.

WOL-pakketten worden verzonden vanuit andere Jump-clients die zich op hetzelfde netwerk bevinden als de doelmachine. Wanneer een actieve Jump-client wordt geïnstalleerd of incheckt, worden de netwerkgegevens van deze Jump-client op het B Series Appliance geregistreerd. Met deze gegevens bepaalt het B Series Appliance welke Jump-clients op hetzelfde netwerk zijn.

Nadat een poging is gedaan om een geselecteerde Jump-client uit de slaapmodus te halen, wordt de WOL-optie gedurende 30 seconden uitgeschakeld voordat er een nieuwe poging kan worden gedaan. Als er geen andere Jump-clients op datzelfde netwerk beschikbaar zijn om WOL-pakketten naar de doelmachine te verzenden, ontvangt de ondersteuningstechnicus een bericht dat er geen andere Jump-clients op het netwerk beschikbaar zijn. Bij het verzenden van een WOL-pakket beschikt de ondersteuningstechnicus over de geavanceerde optie om een wachtwoord mee te sturen voor WOL-omgevingen waar zo'n WOL-wachtwoord vereist is. Een WOL-pakket werkt maar in één richting en de ondersteuningstechnicus ontvangt geen bevestiging, behalve dat de console van de ondersteuningstechnicus aangeeft als de client online komt.

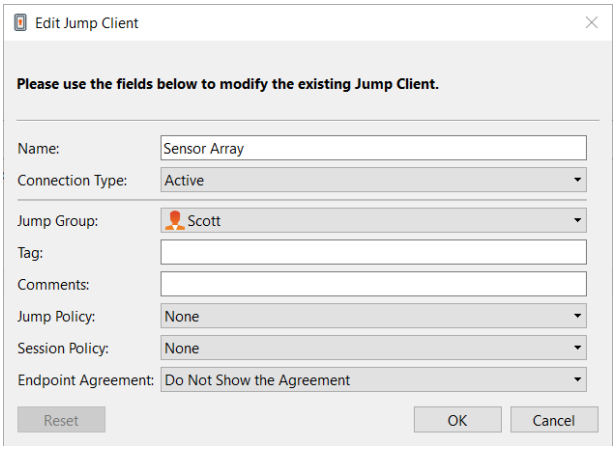
Jumpitems kopiëren

Jumpitems kunnen gekopieerd worden en kunnen bij meerdere Jumpgroepen horen. Hieronder vallen ook Jumpitems waarmee beheerders aparte beleidslijnen en groepsmachtigingen kunnen instellen zonder dat ze een extra Jump-client moeten installeren op het doeleindpunt. Gebruikers met de juiste machtigingen kunnen de optie om Jumpitems te **kopiëren** in de Toegangsconsole zien door met de rechter muisknop op het item te klikken. Gebruikers kunnen deze functie ook op meerdere Jumpitems uitvoeren.

Met behulp van deze functie kunnen beheerders en gebruikers op een doeltreffende manier verschillende beleidslijnen voor Jumpitems en Jump-clients beheren, zonder dat er een nieuw Jumpitem moet worden aangemaakt. Met deze functie kunnen gebruikers het aantal clients beperken dat nodig is om Jump-clientsessies mogelijk te maken. Ook wordt hiermee het aantal handmatige beheertaken teruggedrongen wanneer er toegangspaden voor gebruikers worden gedefinieerd.

Eigenschappen Jump-client

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.).*

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.

Wijzig de modus van een Jump-client vanuit de vervolgkeuzelijst **Type verbinding**. Actieve Jump-clients verzenden met vastgestelde intervallen statistieken naar het B Series Appliance. Passieve Jump-clients verzenden eens per dag of na een handmatige controle statistieken naar het B Series Appliance.

> ***Opmerking:*** *Deze functie is alleen beschikbaar voor klanten die een B Series Appliance op locatie bezitten. Klanten van BeyondTrust Cloud hebben geen toegang tot deze functie.*

Op basis van de door uw beheerder ingestelde opties kunnen deze statistieken de volgende gegevens bevatten: de op de externe computer ingelogde consolegebruiker, het besturingssysteem, de bedrijfstijd, CPU- en schijfgebruik en een schermopname van de laatste update.

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.

Als u geen toegang meer nodig hebt tot een extern systeem, selecteert u het Jumpitem en klikt u op **Verwijderen**. Ook kunt u met de rechtermuisknop op het Jumpitem klikken en in het menu **Verwijderen** selecteren. U kunt meerdere Jumpitems selecteren om die allemaal tegelijkertijd te verwijderen.

> ***Opmerking:*** *Als een externe gebruiker handmatig een Jump-client verwijdert, wordt het verwijderde item als gedeïnstalleerd gemarkeerd of uit de lijst met Jumpitems gehaald in de toegangsconsole. Als de Jump-client op het moment van verwijderen geen contact met het B Series Appliance kan maken, blijft het item offline. Deze instelling is beschikbaar op* ***/login > Jump > Jump-clients****. Als een Jump-client offline gaat en gedurende 180 dagen geen verbinding meer met het B Series Appliance maakt, wordt hij automatisch van de doelcomputer en de Jump-interface verwijderd.*

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.

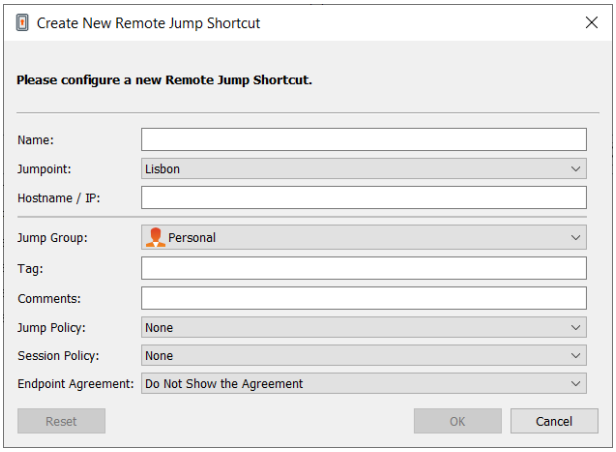
> ***Opmerking:*** *Jumpoint is beschikbaar voor Windows- en Linux-systemen. Jump-clients zijn nodig voor toegang op afstand tot Mac-computers. Om een Jump uit te voeren naar een Windows-computer zonder Jump-client, moet op die computer Remote Registry-service zijn ingeschakeld (op Vista is deze standaard 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.*

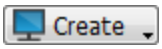
Lokale Jump gebruiken voor toegang tot computers zonder toezicht in uw lokale netwerk

Met Lokale jump kan een bevoorrechte gebruiker verbinding maken met een onbeheerde computer op het lokale netwerk. De computer van de BeyondTrust-gebruiker kan binnen het lokale netwerk een sessie naar een Windows-systeem direct starten zonder een Jumpoint te gebruiken, als de juiste gebruikersmachtigingen zijn ingeschakeld. Een Jumpoint is alleen nodig als de computer van de BeyondTrust-gebruiker niet rechtstreeks toegang tot de doelcomputer kan krijgen.

> ***Opmerking:*** *Lokale Jump is alleen beschikbaar voor Windows-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.*

Een snelkoppeling naar een lokale Jump aanmaken

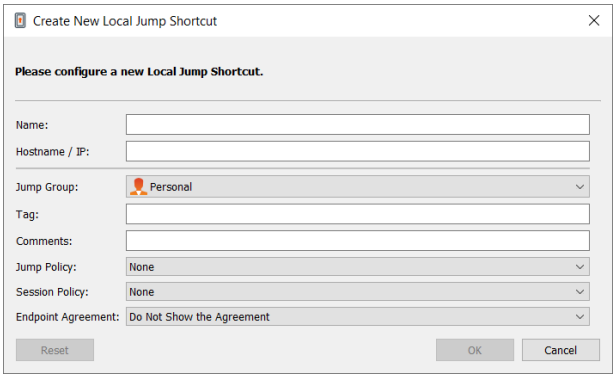
Om een snelkoppeling naar een lokale Jump te maken, moet u in de Jump-interface op de knop **Aanmaken** klikken. Selecteer uit het vervolgkeuzemenu **Lokale Jump**. Snelkoppelingen naar lokale Jumps verschijnen in de Jump-interface naast Jump-clients en andere typen Jumpitems.



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.



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 lokale 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:*** *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 pagina 12.*

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.*

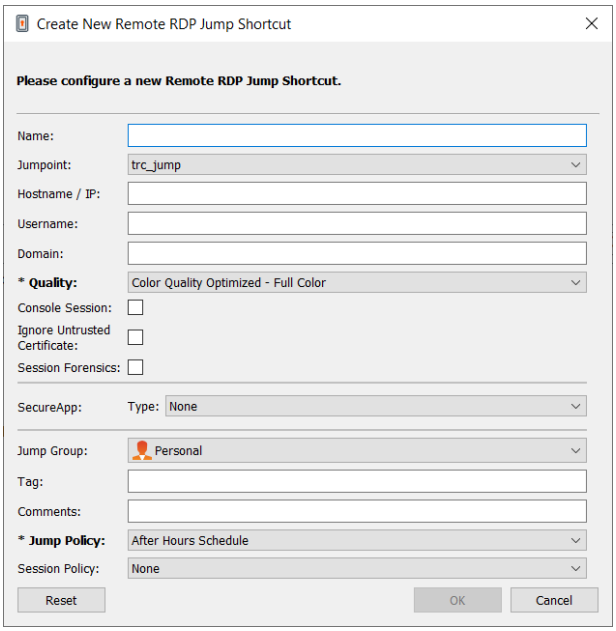
Voer een **Naam** in voor het Jumpitem. Het item is onder deze naam te vinden in de sessietabbladen. Deze tekenreeks mag maximaal 128 tekens lang zijn.

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)

Macronaam	Resultaat
%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.

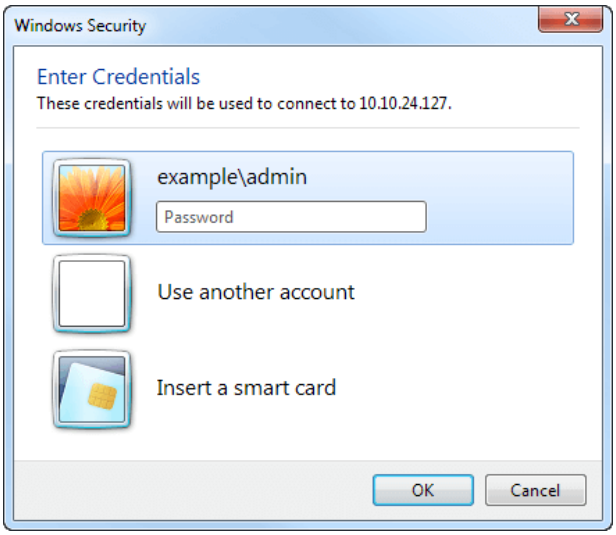
U moet een **Jump-beleid** kiezen om in te stellen welke gebruikers toegang tot dit Jumpitem hebben, of een kennisgeving van toegang moet worden verzonden en/of een machtiging of een ticket-ID van uw externe ticketsysteem is vereist om dit Jumpitem te gebruiken. Deze beleidslijnen worden door uw beheerder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

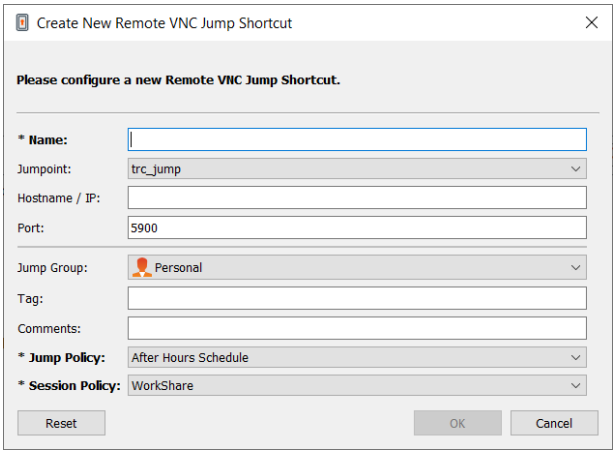
Klik in de Jump-interface op de knop **Aanmaken** om een VNC-snelkoppeling te maken. Selecteer **Externe VNC** in het vervolgkeuzemenu. Snelkoppelingen naar VNC verschijnen in de Jump-interface naast Jump-clients en andere typen Jumpitems.

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.

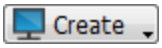
> ***Opmerking:*** *Jumpitems kunnen zo worden ingesteld dat zij meerdere gebruikers toestaan tegelijkertijd dezelfde Jumpitems te openen. Als **Bij bestaande sessie voegen** is ingeschakeld, kunnen andere gebruikers een sessie bijwonen die al gaande is. De oorspronkelijke eigenaar van de sessie ontvangt 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.*

Een Jump via tunnelprotocol gebruiken om een TCP-verbinding te maken met een extern systeem

Maak via een Jump via tunnelprotocol een TCP-verbinding vanaf uw systeem naar een eindpunt op het externe netwerk. Omdat de verbinding tot stand komt via een Jumpoint, kan de beheerder bepalen welke gebruikers toegang hebben, wanneer ze toegang hebben en of sessies worden opgenomen.

Snelkoppeling maken naar Jump via tunnelprotocol

Om een snelkoppeling naar een Jump via tunnelprotocol aan te maken, moet u in de Jump-interface op de knop **Aanmaken** klikken. Selecteer in het vervolgkeuzemenu **Jump via tunnelprotocol**. Snelkoppelingen naar Jumps via tunnelprotocol verschijnen in de Jump-interface naast Jump-clients en andere typen Jumpitems.



> ***Opmerking:*** *Snelkoppelingen naar Jumps via tunnelprotocol zijn alleen ingeschakeld als het betreffende Jumpoint geconfigureerd is voor de methode Jump via tunnelprotocol op de pagina* ***/login > Jump > Jumpoint****.*

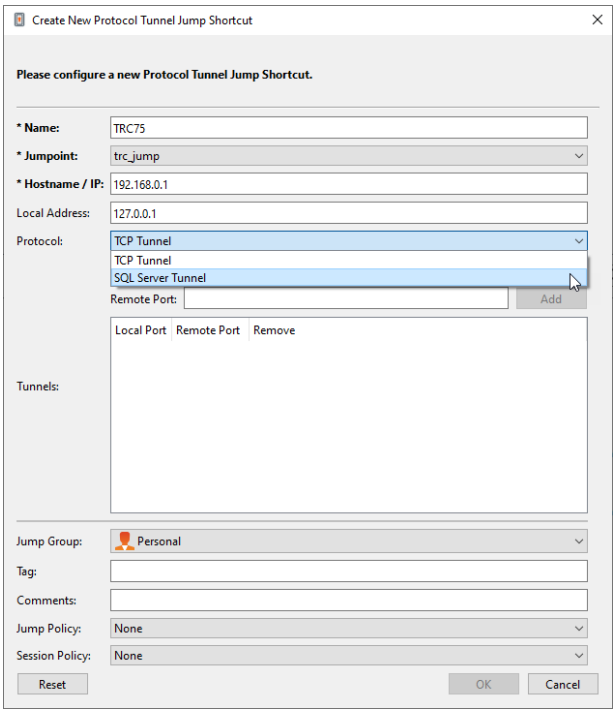
Voer een **Naam** in voor het Jumpitem. Het item is onder deze naam te vinden in de sessietabbladen. Deze tekenreeks mag maximaal 128 tekens lang zijn.

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.

Specificeer een **Lokaal adres**. Het standaard adres is 127.0.0.1. Als u tegelijkertijd verbinding moet maken naar meerdere systemen op dezelfde externe poort, kunt u die verbinding maken door de adressen van alle snelkoppelingen naar Jump via tunnelprotocol te veranderen naar een ander adres met het sub-bereik 127.x.x.x.

Selecteer voor **Protocol** de optie **TCP-tunnel** of **SQL-servertunnel**. **SQL-servertunnel** gebruikt het Microsoft SQL Server-protocol als databaseproxy, waardoor inloggegevensinjectie voor gebruikers en verbeterde audits mogelijk zijn. Verificatie is mogelijk door middel van Windows-verificatie en aanmelden via SQL.

Specificeer in **Lokale poort** de poort voor luisteren op het lokale systeem van de gebruiker. Als u deze instelling laat staan op automatisch, wordt door de toegangsconsole een vrije poort toegewezen.



Specificeer in **Externe poort** de poort op het externe systeem waarmee verbinding gemaakt moet worden. Dit wordt bepaald door het type server waar u verbinding mee maakt.

U kunt meerdere paren van **TCP-tunnels** definiëren wanneer dit nodig is in uw configuratie.

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.

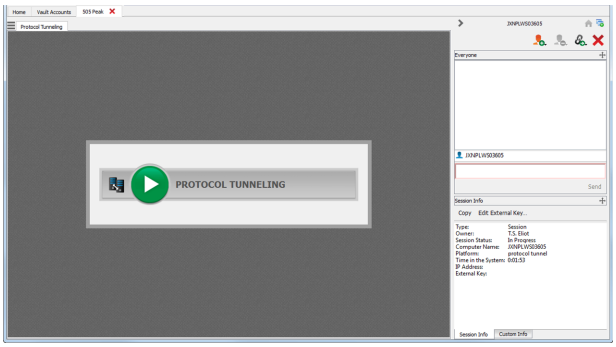
Organiseer en beheer bestaande Jumpitems door een of meer Jumpitems te selecteren en op **Eigenschappen** te klikken.

> ***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.*

Een snelkoppeling naar Jump via tunnelprotocol gebruiken

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

Er wordt een sessie weergegeven in uw toegangsconsole. Klik op de knop **Protocol tunnelen** om de verbinding tot stand te brengen.

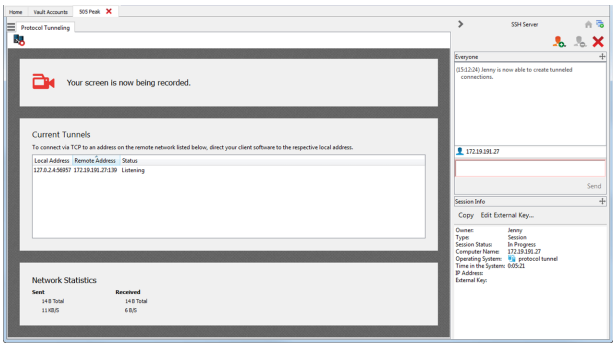


Als opnemen van scherm is ingeschakeld, verschijnt er een prompt waarin u wordt geïnformeerd dat uw desktop wordt opgenomen. Klik op **OK** om verder te gaan. Als u op **Annuleren** klikt, wordt het tunnelprotocol niet gemaakt.

Als opnemen van scherm is ingeschakeld, verschijnt er bovenin uw sessiescherm een controlelampje.

De sectie **Huidige tunnels** toont de huidige verbindingen en de bijbehorende statussen. U kunt ook korte **Netwerkstatistieken** bekijken.

U kunt nu een externe client openen om taken op het externe systeem uit te voeren. Gebruik de aangegeven poorten om een verbinding te maken met de Jumpoint.



Voorschriften voor correct functioneren

Met de functie Protocol tunnelen wordt netwerkverkeer via een tunnel geleid op een manier die enkele beperkingen oplevert voor de manier waarop communicatie tussen het systeem van de gebruiker en het eindpunt moet plaatsvinden.

- Alle verkeer moet via TCP gaan.
- Er kunnen niet meer dan 256 gelijktijdige verbindingen behandeld worden.
- Alle TCP-verbindingen moeten vanuit het eindpunt komen en moeten door het systeem van de luisterende gebruiker geaccepteerd worden. Het protocol van de applicatie mag niet vereisen dat het systeem van de gebruiker een aparte verbinding terug naar het eindpunt maakt.
- Alle TCP-verbindingen die het eindpunt terug naar het systeem van de gebruiker maakt, moeten via tunnels worden geleid die al zijn bepaald binnen de eigenschappen van het Jumpitem via tunnelprotocol.
- Besturingssystemen staan meestal niet toe dat processen zonder verhoogde bevoegdheid luisteren op poorten lager dan 1024. Daarom moet de lokale poort over het algemeen groter zijn dan 1024. De eindpuntsoftware maakt verbinding met de server door verbinding te maken met de lokale poort waar de toegangsconsole (een proces zonder verhoogde bevoegdheid) luistert.
- De eindpuntsoftware kan geen verbindingen maken naar andere systemen dan het systeem dat is aangegeven in de eigenschappen van het Jumpitem via tunnelprotocol.
- Het protocol mag geen beperking hebben voor de hostnaam die het eindpunt heeft gebruikt om te verbinden met de server. Anders moeten andere manieren worden ingesteld om te voldoen aan de eisen van het protocol, zoals een hostnaam toewijzen aan 127.0.0.1 in het hosts-bestand of een speciale configuratie toepassen op de eindpuntclient.
- Als de tunneldefinitie een lokale poort heeft die anders is dan de externe poort (dit is het geval als de lokale poort groter moet zijn dan 1024 omdat de poort van de server kleiner is dan 1024), mag het protocol geen beperking hebben voor de poort die de eindpuntclient heeft gebruikt om te verbinden met de server.
- Voor elk protocol dat verder gaat dan een enkele TCP-verbinding vanaf de eindpuntclient naar het systeem van de gebruiker, is vereist dat de beheerder het specifieke protocol en de bovenstaande voorschriften begrijpt.

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 12*.

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.

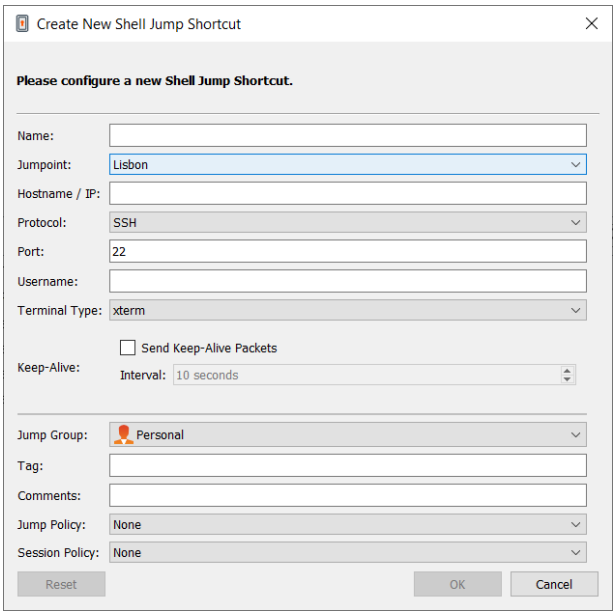
Kies het te gebruiken **Protocol**: **SSH** of **Telnet**.

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**.*

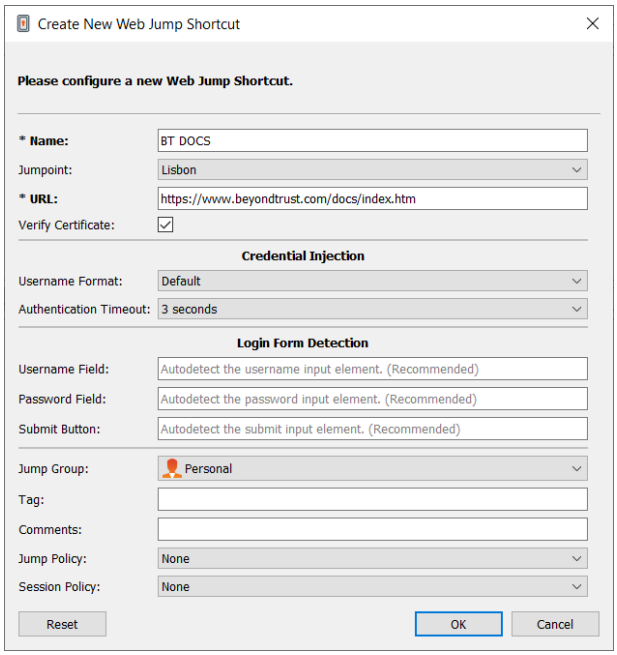
Om een snelkoppeling naar een Web Jump aan te maken, klikt u in de Jump-interface op de knop **Aanmaken**. Selecteer in het vervolgkeuzemenu **Web Jump**. Snelkoppelingen naar Web Jumps worden in de Jump-interface weergegeven naast Jump-clients en andere soorten snelkoppelingen naar Jumpitems.

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.

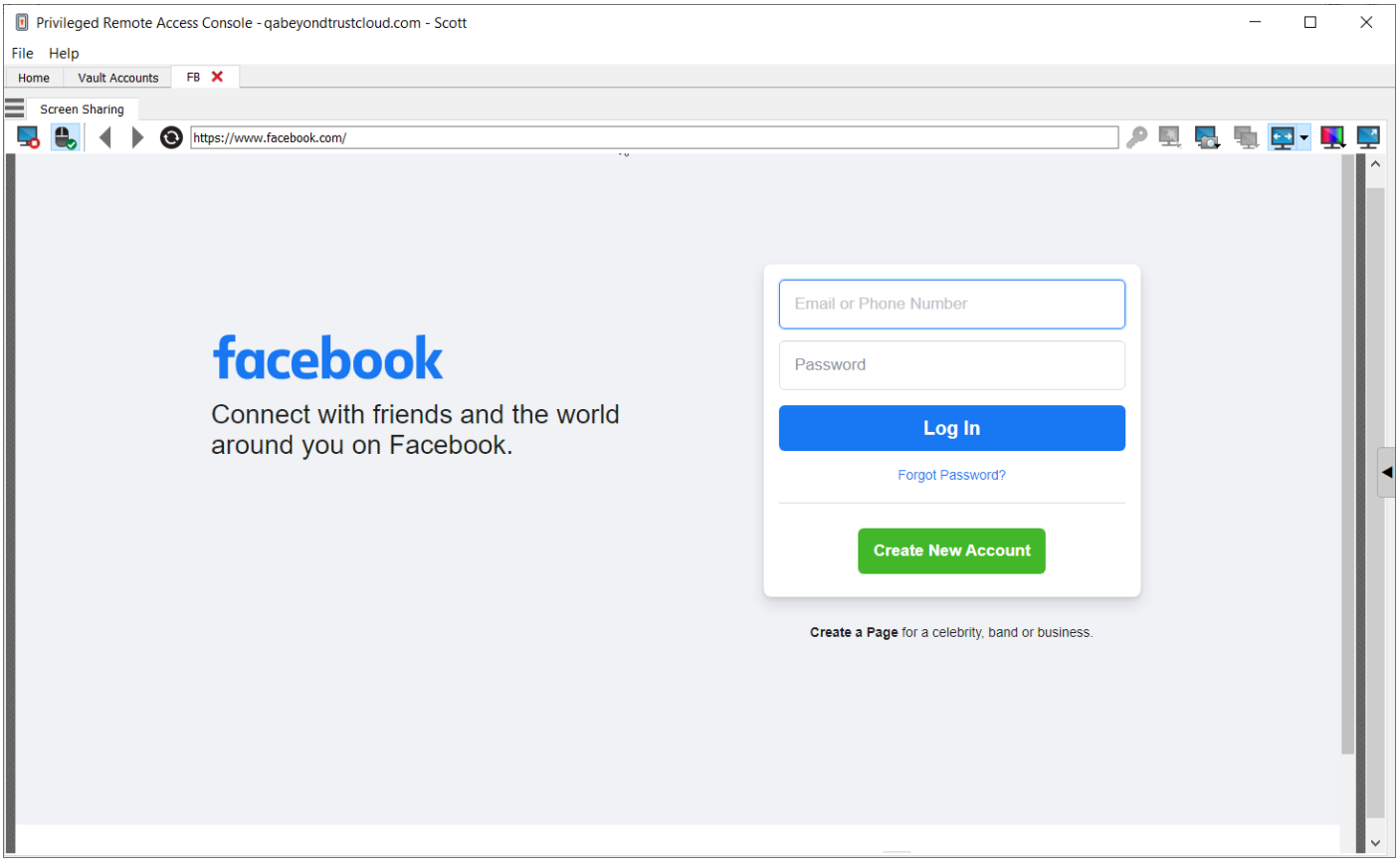
Kies een **Sessiebeleid** om aan dit Jumpitem toe te kennen. Het aan dit Jumpitem toegekende sessiebeleid heeft de hoogste prioriteit bij het instellen van sessiemachtigingen. Of u een sessiebeleid kunt instellen hangt van uw accountmachtigingen af.

> *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.*

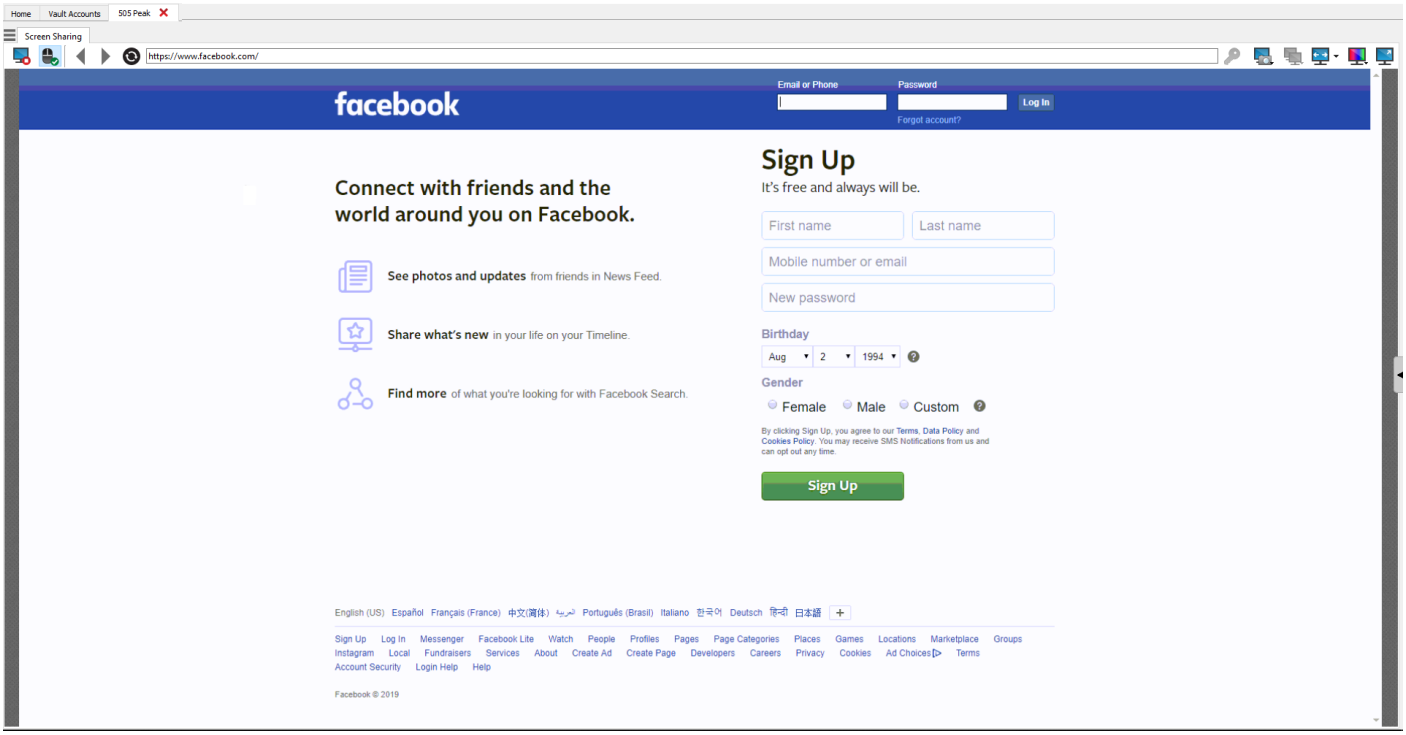
Opmerking: *Voor naadloze inloggegevensinjectie op een VMware-console moeten enkele configuraties worden uitgevoerd.*

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.

Set hulpmiddelen voor toegang

Overzicht van toegangssessies en hulpmiddelen



Sessiegereedschappen

	Klik op het pictogram Menu linksboven in het sessievenster om sessiebesturingselementen voor uw sessie te openen. U kunt ook met de rechtermuisknop op het sessietabblad klikken om de sessiebesturingselementen te zien. Selecteer **Sessietabblad loskoppelen** uit het menu om de sessie van de console los te koppelen of klik op het sessietabblad en sleep het weg van het hoofdvenster. Het pictogram Menu blijft bij uw sessie zelfs als u het sessietabblad loskoppelt, zodat u het sessietabblad overal kunt plaatsen, bijvoorbeeld op een apart beeldscherm, en toegang tot de sessiehulpmiddelen houdt. Maak de sessie weer vast door in het menu **Sessietabblad vastmaken** te selecteren of door op de X te klikken om het losgekoppelde venster te sluiten. Bovendien kunt u in het menu **Kantlijnartikel vinden** selecteren om het kantlijnartikel voor de sessie te vinden. Dit kan handig zijn als u her en der kantlijnartikelen voor verschillende losgekoppelde sessies op uw scherm hebt staan. U kunt vanuit het menu de naam van de sessie ook wijzigen of de naam terugzetten naar de standaard naam.
	Vouw het kantlijnartikel in om de werkruimte voor uw sessie zo groot mogelijk te maken. Om het kantlijnartikel weer vast te spelden moet u de muis boven het pijltje van het ingevouwen kantlijnartikel plaatsen en op het pictogram **Kantlijnartikel vastspelden** klikken.
	Klik op dit pictogram om het kantlijnartikel los te koppelen. Als het kantlijnartikel is losgekoppeld, dan kunt u het overal op uw bureaublad plaatsen, zelfs op een apart beeldscherm. U kunt de grootte van het kantlijnartikel ook aan uw wensen aanpassen of de grootte van de deelvensters in het kantlijnartikel aanpassen om meer ruimte te hebben om de sessie te bekijken. Klik op het pictogram **Kantlijnartikel vastmaken** om het kantlijnartikel weer vast te maken. Als het kantlijnartikel is losgekoppeld, dan is het pictogram **Start** ingeschakeld (zie hieronder).
	Het pictogram **Start** is altijd ingeschakeld als het kantlijnartikel is losgekoppeld. Mocht u verschillende sessies tegelijkertijd actief hebben en mochten er verschillende losgekoppelde kantlijnartikelen op uw scherm staan, dan kunt u op het pictogram **Start** van een kantlijnartikel klikken om de bijbehorende sessie naar voren te brengen. U bespaart zo tijd en u voorkomt verwarring als u probeert te zien welk kantlijnartikel bij welke sessie hoort.
	Het is mogelijk de positie van de in het kantlijnartikel weergegeven widget-secties te wijzigen, zoals het chat-venster of het deelvenster met sessie-informatie. Als u met uw muis boven de titelbalk van een sectie zweeft, dan verandert de cursor in een gesloten hand, zodat u die sectie kunt wegslepen en in het kantlijnartikel kunt plaatsen.
	Nodig een andere gebruiker uit in een gedeelde sessie. U blijft eigenaar van de sessie maar u kunt invoer van een of meerdere teamleden of van een externe gebruiker krijgen.
	De sessie-eigenaar kan een andere gebruiker van een gedeelde sessie verwijderen.
	Open in een webbrowser op uw computer een van de sites die door uw beheerder zijn gedefinieerd. Deze knop kan worden geconfigureerd om gedetailleerde informatie op te nemen over de sessie, het eindpunt en/of de BeyondTrust-gebruiker die de aangepaste koppeling opent. Als de externe code bijvoorbeeld met de unieke identificator van een case in uw CRM-systeem overeenkomt, dan kunt u op deze knop klikken om de bijbehorende case in het externe systeem op te halen.
	Sluit uw sessieblad volledig. U kunt de sessie vanaf het kantlijnartikel, het sessiemenu of het sessietabblad sluiten.

Rechts onderin het sessievenster staat informatie over het externe systeem. Als uw beheerder de XML API heeft ingeschakeld, kunt u bovendien een externe code aanwijzen voor gebruik in sessierapporten. Eventuele door uw beheerder ingeschakelde aangepaste attributen verschijnen in het tabblad **Aangepaste informatie**. Klik op **Kopiëren** om alle informatie naar uw klembord te kopiëren.

Uw beheerder kan er bovendien voor kiezen de optie in te schakelen om de Windows-gebruiker automatisch uit te loggen of de externe computer te vergrendelen als de sessie wordt afgesloten. Als u bijvoorbeeld op een systeem zonder toezicht hebt gewerkt, dan wordt aanbevolen de computer te vergrendelen om te voorkomen dat niet-geautoriseerde gebruikers privé-informatie te zien krijgen. Stel in het vervolgkeuzemenu onderin het deelvenster de te nemen actie in.

Inloggen bij externe systemen met behulp van inloggegevensinjectie via de Toegangsconsole

Als u een op Windows gebaseerd Jumpitem via de 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.

> ***Opmerking:*** *Inloggegevensinjectie is niet beschikbaar voor Mac of Linux Jump-clients.*

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.

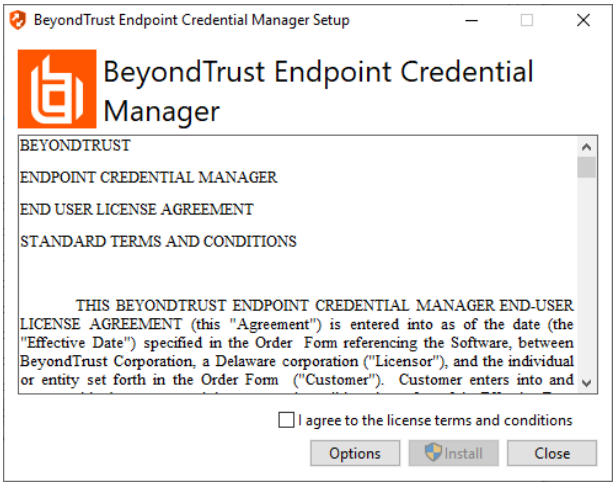
> ***Opmerking:*** *De ECM moet op uw systeem zijn geïnstalleerd om de BeyondTrust ECM Service in te schakelen en inloggegevensinjectie te gebruiken in BeyondTrust Privileged Remote Access.*

Systeemvereisten

- **Windows Vista of nieuwer, alleen 64-bit**
- **.NET 4.5 of nieuwer**

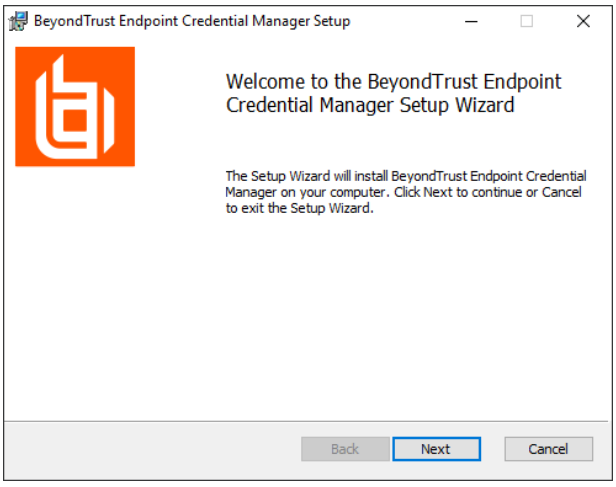
1. Download om te beginnen de BeyondTrust Endpoint Credential Manager (ECM) van BeyondTrust Support op beyondtrustcorp.service-now.com/csm.
2. Start de installatiewizard voor BeyondTrust Endpoint Credential Manager.
3. Ga akkoord met de algemene voorwaarden uit de Gebruiksrechtovereenkomst. Schakel het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

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

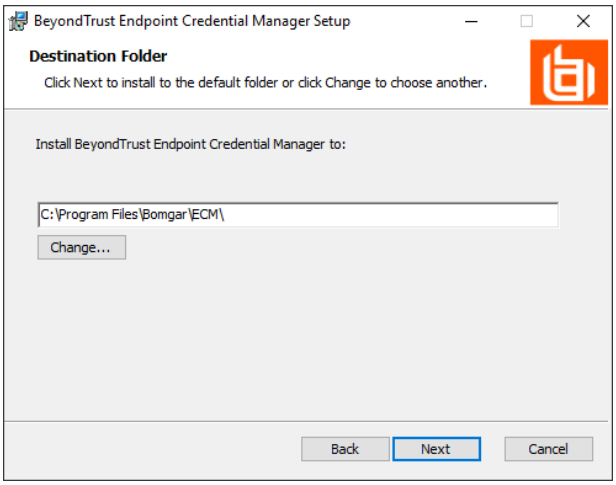


> ***Opmerking:*** *U kunt niet doorgaan met de installatie tenzij u akkoord gaat met de Gebruiksrechtovereenkomst.*

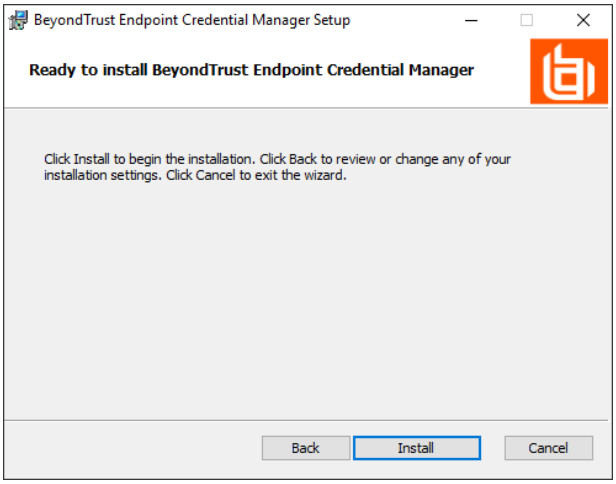
4. Klik op **Volgende** op het welkomstscherm.



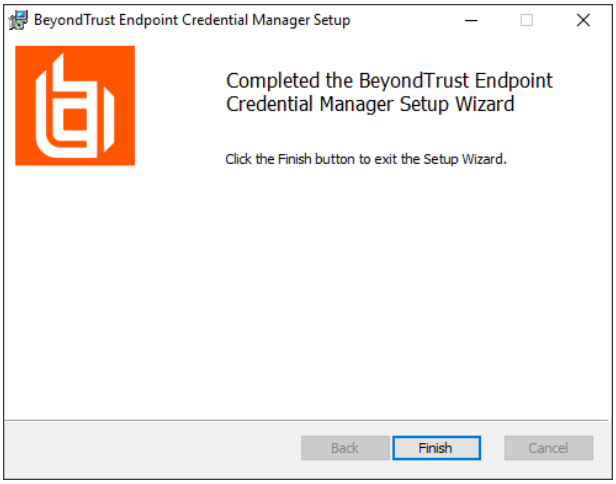
5. Kies een locatie voor de inloggegevensopslag en klik op **Volgende**.
6. In het volgende scherm kunt u de installatie beginnen of een voorgaande stap nog eens bekijken.



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



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

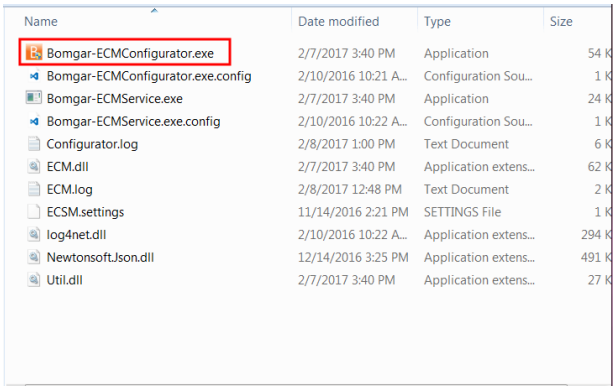
> ***Opmerking:*** *Als er meerdere ECM's in een configuratie met hoge beschikbaarheid zijn verbonden, stuurt de BeyondTrust Appliance B Series verzoeken naar de ECM in de ECM-groep die het langst met het apparaat is verbonden.*

> ***Opmerking:*** *Zoek en deblokkeer BeyondTrustVaultRestPlugin.dll als u tijdens de installatie een fout voor de invoegtoepassing ziet in Windows.*

Een verbinding met uw inloggegevensopslag configureren

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

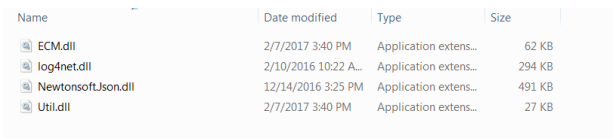
1. Zoek de BeyondTrust ECM Configurator die u zojuist hebt geïnstalleerd via Windows zoeken of via het invoerveld in de programmalijst in het menu **Start**.
2. Voer het programma uit om een verbinding te maken.
3. Vul de velden in wanneer de ECM Configurator opent. Alle velden zijn verplicht.



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.*

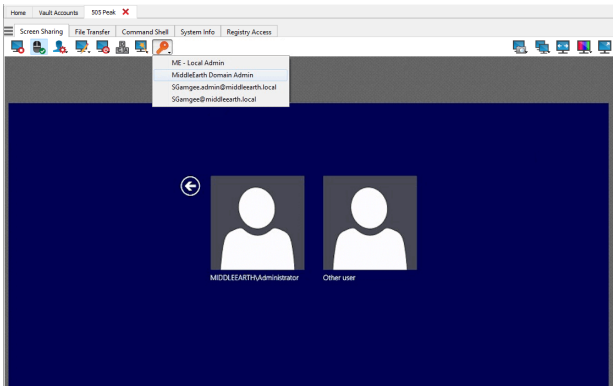
BELANGRIJK!

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

Inloggegevensinjectie gebruiken voor toegang tot externe systemen

Nadat de inloggegevensopslag is geconfigureerd en er verbinding is gemaakt, kan de toegangsconsole de inloggegevens uit de inloggegevensopslag gebruiken om aan te melden bij externe systemen.

1. Meld u aan bij de toegangsconsole.
2. Jump naar een extern systeem 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 externe systeem. Als het externe systeem 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 ondersteuningstechnicus wordt ingelogd bij het externe systeem.



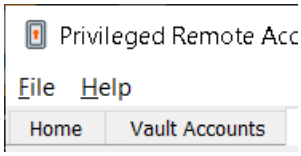
Kies uit favoriete inloggegevens voor injectie

Nadat u een set inloggegevens hebt gebruikt om in te loggen op een eindpunt, bewaart het systeem uw voorkeursinloggegevens voor het eindpunt en de context waarin deze gebruikt zijn (om in te loggen, om een speciale actie uit te voeren, om op te waarderen of te pushen) in de B Series Appliance-database. De volgende keer dat u inloggegevens gebruikt om toegang tot hetzelfde eindpunt te krijgen, doet het inloggegevens-injectiemenu een aanbeveling voor de te gebruiken inloggegevens. De inloggegevens worden weergegeven bovenaan de lijst met inloggegevens, onder **Aanbevolen accounts**, gevolgd door alle overige inloggegevens. Als er geen geschiedenis van inloggegevens is voor een eindpunt, geeft het B Series Appliance alle mogelijke inloggegevens weer, gegroepeerd op accounts die gekoppeld zijn met het Jumpitem en niet gekoppeld zijn met het Jumpitem. Jumpitem-koppelingen voor accounts en accountgroepen worden geconfigureerd in /login.

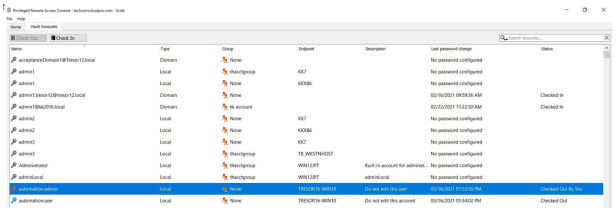
De lijst met inloggegevens geeft niet meer dan 5 inloggegevens weer.

Vault-inloggegevens in- en uitchecken

U hebt gemakkelijk toegang tot de Privileged Remote Access Vault, rechtstreeks vanuit de toegangsconsole. Zo kunt u inloggegevens in- of uitchecken wanneer u dat wenst; dit kan tijdens een sessie of op uw lokale computer.

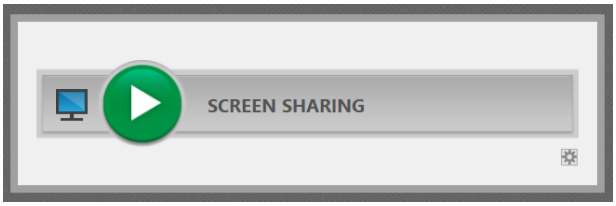


Selecteer het tabblad **Vault-accounts** om een lijst met beschikbare inloggegevens en bijbehorende informatie te bekijken.



Extern eindpunt beheren met scherm delen

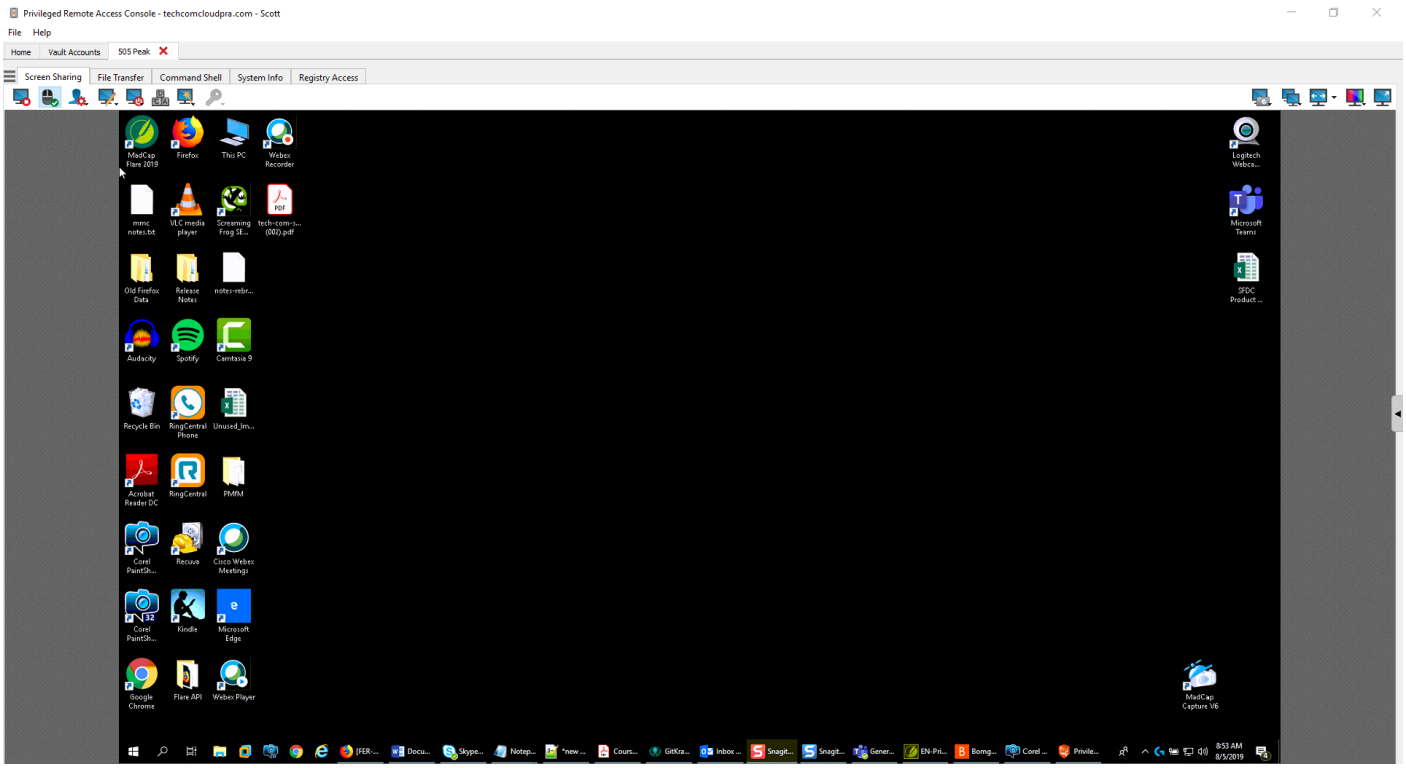
Klik in het sessievenster op de knop **Scherm delen** om de besturing over de externe computer te vragen als het scherm niet automatisch wordt gedeeld. Er zijn afhankelijk van de instellingen voor uw account onder de knop mogelijk opties beschikbaar. Klik op de knop met het tandwiel om opties te zien.



Nadat u een sessie hebt gestart, deelt de toegangsconsole direct het scherm met het eindpunt. Afhankelijk van het systeem hebt u mogelijk volledige controle of alleen-lezenrechten wanneer het scherm met het systeem wordt gedeeld.

Opties voor scherm delen

- Als u geen enkele optie aanvinkt, dan verzoekt u om het meest uitgebreide scherm delen, waarbij u het gehele bureaublad en alle toepassingen op het externe systeem kunt zien en beheren.
- Als u **Alleen weergeven** aanvinkt, dan kunt u het externe scherm wel zien maar niet beheren.
- Met de optie **Privacyscherm** aangevinkt wordt de sessie gestart waarbij de weergave en de besturing van het eindpunt zijn uitgeschakeld. Privacyscherm is niet beschikbaar bij ondersteuning van Windows 8.



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.
	Met Hulpmiddelen voor annotaties kunt u tijdens gedeelde sessies gemakkelijker samenwerken. Er is een aantal hulpmiddelen beschikbaar, waaronder vormen en vrij tekenen.
	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.
	Bekijk een vervolgkeuzelijst met alle op uw systeem beschikbare smartcardlezers. Gebruik de virtuele smartcard om beheeracties uit te voeren, programma's in een andere gebruikerscontext uit te voeren of zelfs als een andere gebruiker in te loggen. De juiste stuurprogramma's voor virtuele smartcards moeten zowel op uw lokale systeem als op het externe systeem zijn geïnstalleerd en de services ervoor moeten actief zijn.
	Scherm delen op een iOS-apparaat opnieuw starten. Raadpleeg Ondersteuning voor Apple iOS-apparaten op www.beyondtrust.com/docs/privileged-remote-access/getting-started/access-console/apple-ios/index.htm voor meer informatie. Als u een Apple OS X 10.10+ systeem ondersteunt dat met een Apple iOS 8.0.1+ mobiel apparaat verbonden is, dan kunt u op deze knop klikken om een sessie met scherm delen in de modus alleen weergeven op het aangesloten iOS-apparaat te starten of te beëindigen. NB: Deze knop is niet zichtbaar tenzij u in een standaard toegangssessie met de functie 'Scherm delen' actief bent op een Apple OS X Yosemite-systeem en de knop niet is ingeschakeld, tenzij er een apparaat met Apple iOS 8.0.1+ is verbonden met het ondersteunde OS X Yosemite-systeem.

	Meld u met de inloggegevens uit de externe inloggegevensopslag aan bij het eindpunt. 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. In eerdere versies dan 15.2 is deze functie alleen beschikbaar in sessies die vanaf een opgewaardeerde Jump-client op Windows® zijn gestart. Vanaf versie 15.2 mag u ook een Endpoint Credential Manager gebruiken in sessies met externe Jump, sessies met Microsoft® Extern bureaublad, VNC-sessies en sessies met Shell Jump.
	Tijdens het delen van het scherm kunt u een schermopname van het externe scherm of van de externe schermen in de volledige resolutie maken; deze schermopname wordt opgeslagen als PNG-bestand. Sla het bestand op uw lokale systeem of op uw klembord op. De opname wordt in het chatlogboek opgenomen met een koppeling naar de lokaal opgeslagen afbeelding. De koppeling blijft zelfs actief nadat de klant de sessie heeft verlaten, maar blijft niet in het BeyondTrust-sessierapport staan. U kunt de map waarin de schermopnamen worden opgeslagen aanpassen via het menu **Bestand > Instellingen > Hulpmiddelen** in de toegangsconsole. Deze functie werkt op Mac, Windows en Linux.
	Verzend de inhoud van het klembord handmatig naar de externe computer. Dit pictogram is niet zichtbaar als u niet gemachtigd bent om de inhoud van uw klembord automatisch te verzenden of als u geen toestemming hebt om de informatie van het klembord naar het externe systeem te verzenden.
	Haal de inhoud van het klembord handmatig van de externe computer op. Dit pictogram is niet zichtbaar als u niet gemachtigd bent om de inhoud van uw klembord automatisch op te halen of als u geen toestemming hebt om de informatie van het klembord van het externe systeem op te halen.
	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**.

Annotaties gebruiken om op het externe scherm van het eindpunt te tekenen

Gebruik hulpmiddelen voor annotaties om tijdens een gedeelde sessie met anderen te communiceren. Annotaties vormen een interactieve manier om visueel te communiceren, waardoor minder frustrerende situaties voorkomen en de processen sneller verlopen.

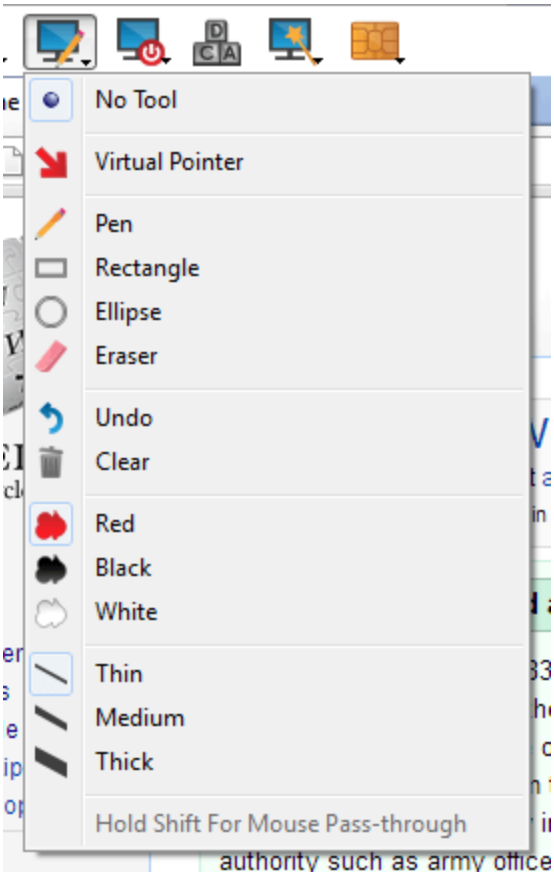
U kunt in annotatie-modus nog steeds uw muis gebruiken om items op het externe bureaublad te bewegen of te besturen. Als u de **Shift**-toets ingedrukt houdt, dan wordt de annotatie-modus tijdelijk opgeschort.

Annotaties inschakelen

Klik op het pictogram Annotaties om **Annotaties** te gaan gebruiken.

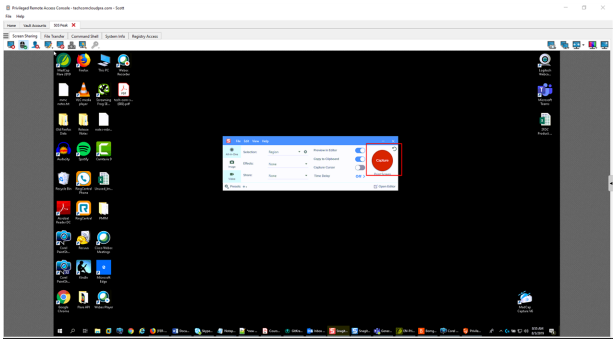
Klik op een van de opties in het vervolgkeuzemenu om de **Annotatie**-modus in te schakelen. De volgende hulpmiddelen en functies zijn beschikbaar:

- Virtuele aanwijzer
- Pen
- Tekenhulpmiddel rechthoek
- Tekenhulpmiddel ellips
- Gum
- Ongedaan maken
- Wissen
- Kleuren rood, zwart of wit
- Lijndikte dun, gemiddeld of dik



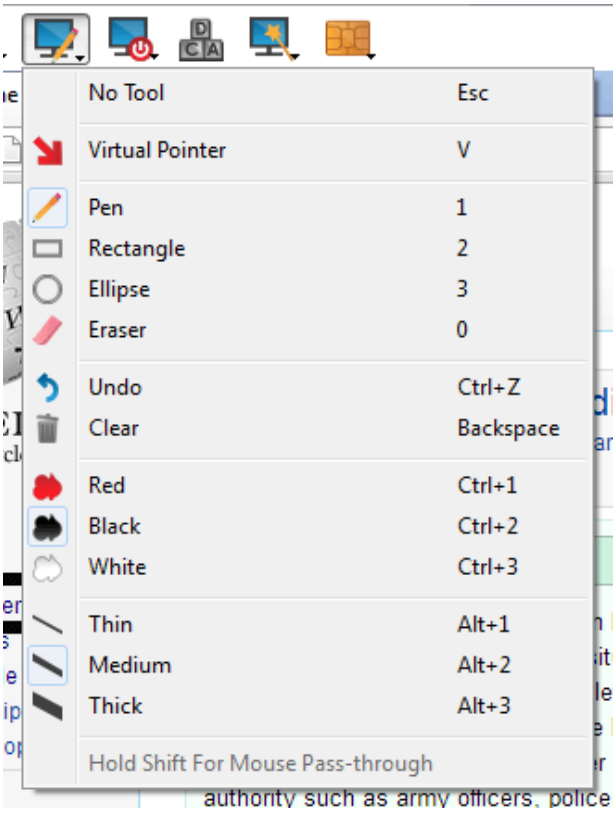
U kunt uw hulpmiddel selecteren in het vervolgkeuzemenu **Annotaties** of door met de rechtermuisknop op het gebied van het externe scherm te klikken. Als u op de gebieden buiten het externe scherm klikt, dan verschijnt het vervolgkeuzemenu niet.

Annotaties verschijnen op het externe scherm om, indien nodig, de aandacht op bepaalde interessante punten te vestigen of om gebieden te markeren.



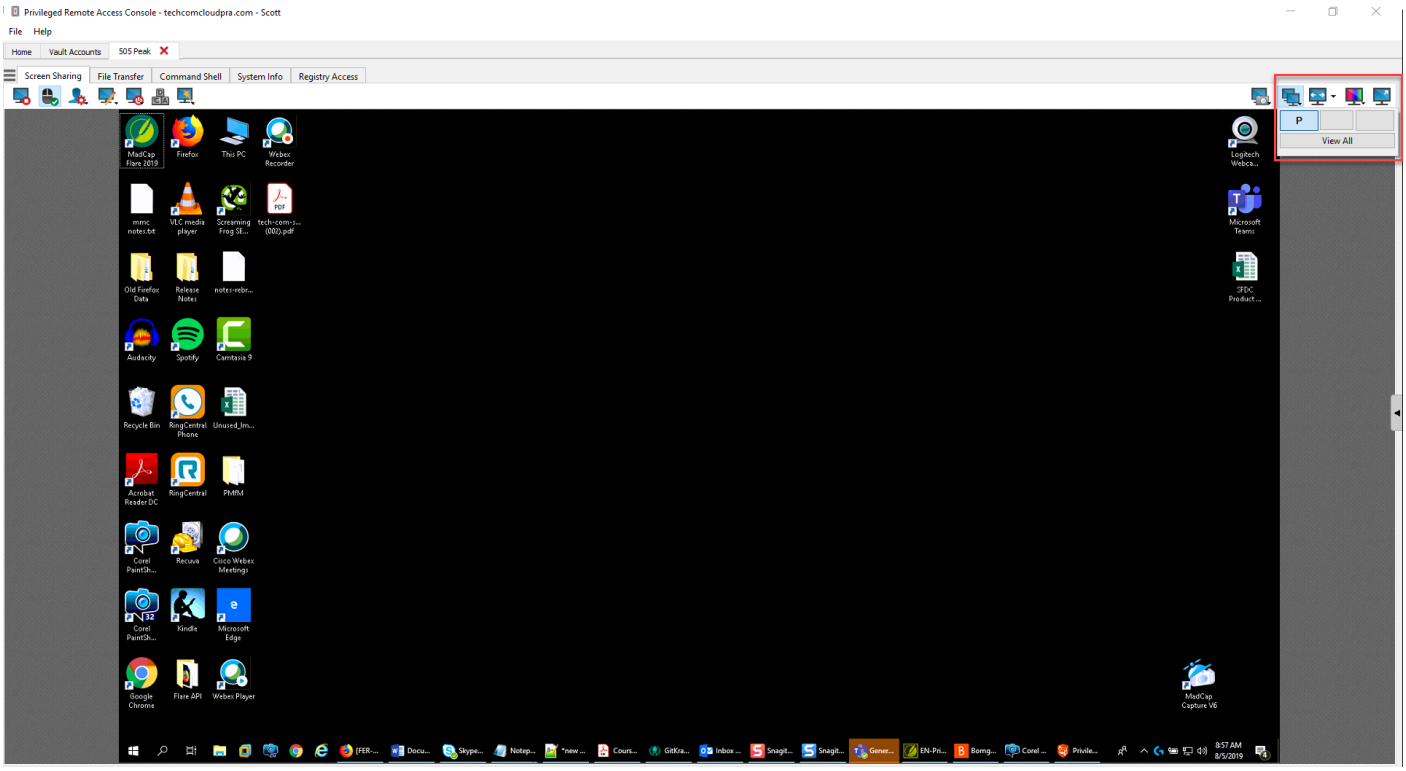
Om **Annotaties** uit te schakelen, kunt u **Geen hulpmiddel** uit het vervolgkeuzemenu selecteren of op **Esc** drukken.

Alle annotaties worden van het scherm van de klant verwijderd als de sessie eindigt.



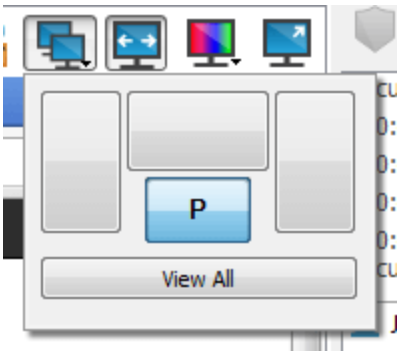
Meerdere beeldschermen op het externe eindpunt bekijken

BeyondTrust ondersteunt externe bureaubladen met configuraties voor meerdere beeldschermen. Als u de eerste keer met een extern bureaublad verbinding maakt, dan ziet u in het tabblad **Scherm delen** het primaire beeldscherm. Als er extra beeldschermen zijn geconfigureerd, dan wordt een pictogram **Beeldscherm** actief in de werkbalk **Scherm delen** en verschijnt een tabblad **Beeldschermen** in de rechteronderhoek van de console.



Het pictogram Beeldscherm gebruiken

Selecteer het pictogram **Beeldscherm** om alle beeldschermen te zien die aan de externe computer zijn verbonden. In deze weergave worden de externe beeldschermen als rechthoeken weergegeven en niet als miniatuurweergave. De positie van elk van de rechthoeken komt overeen met de positie zoals die op de externe computer voor de beeldschermen is geconfigureerd.

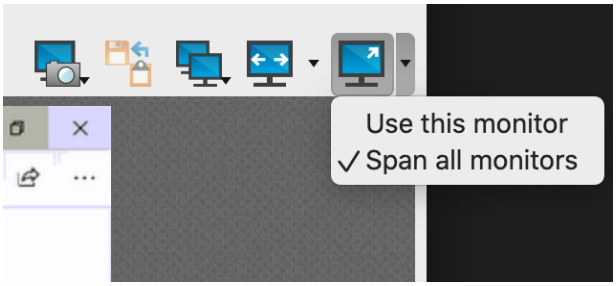


Het primaire beeldscherm verschijnt standaard in het venster **Scherm delen**. Om uw weergave te wijzigen, moet u op de rechthoek klikken die met het beeldscherm overeenkomt dat u wilt zien. U kunt ook **Alles bekijken** selecteren om alle beeldschermen te zien die in het venster **Scherm delen** aan de externe computer zijn verbonden.

Als er aan de externe computer geen extra beeldschermen zijn verbonden, dan is het pictogram **Beeldscherm** niet actief.

RDP-sessieondersteuning voor meerdere beeldschermen

Een optie biedt u de mogelijkheid om een PRA-verbinding te openen die op alle beeldschermen wordt weergegeven op de clientcomputer, ongeacht de configuratie van het clientbeeldscherm. Met deze functie kun u alle beeldschermen die verbonden zijn met de clientcomputer volledig benutten. U kunt zo de schermgrootte en -schaal aanpassen tijdens een RDP-sessie op meerdere beeldschermen.

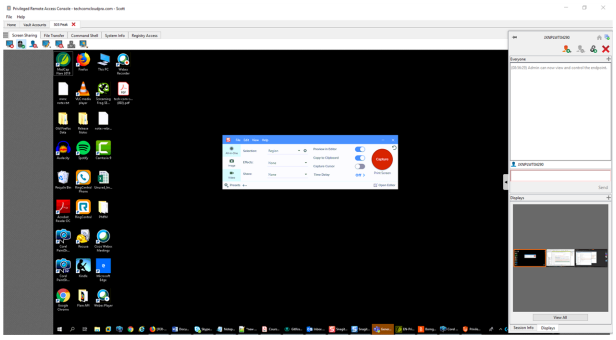


> ***Opmerking:*** *Als u deze functie gebruikt in volledige schermweergave, wordt het externe systeem weergegeven op al uw beeldschermen.*

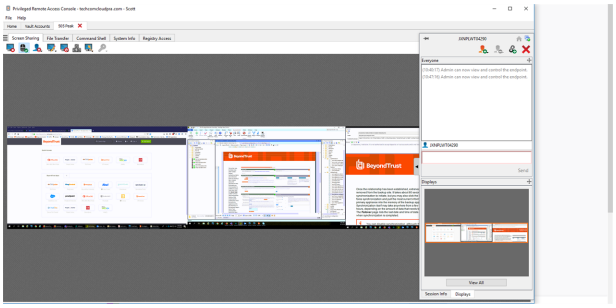
Het tabblad Beeldschermen gebruiken

Selecteer het tabblad **Beeldscherm** om miniatuurweergaves van alle beeldschermen te zien die aan de externe computer zijn verbonden. De positie van elk van de miniatuurweergaves komt overeen met de positie zoals die op de externe computer voor de beeldschermen is geconfigureerd.

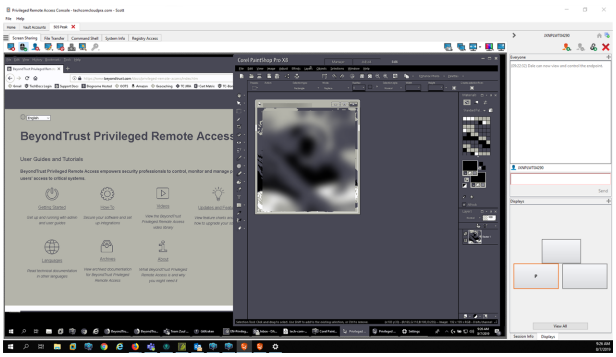
Het beeldscherm dat op dat moment in het tabblad **Scherm delen** wordt weergegeven, is gemarkeerd.



Het primaire beeldscherm verschijnt standaard in het venster **Scherm delen**. Om uw weergave te wijzigen, moet u op de miniatuurweergave klikken die met het beeldscherm overeenkomt dat u wilt zien. U kunt ook **Alles bekijken** selecteren om alle beeldschermen te zien die in het venster **Scherm delen** aan de externe computer zijn verbonden.



Als de sessie in zwart-wit wordt weergegeven, dan worden de externe beeldschermen als rechthoeken weergegeven en niet als miniatuurweergave. De positie van elk van de rechthoeken komt overeen met de positie zoals die op de externe computer voor de beeldschermen is geconfigureerd.



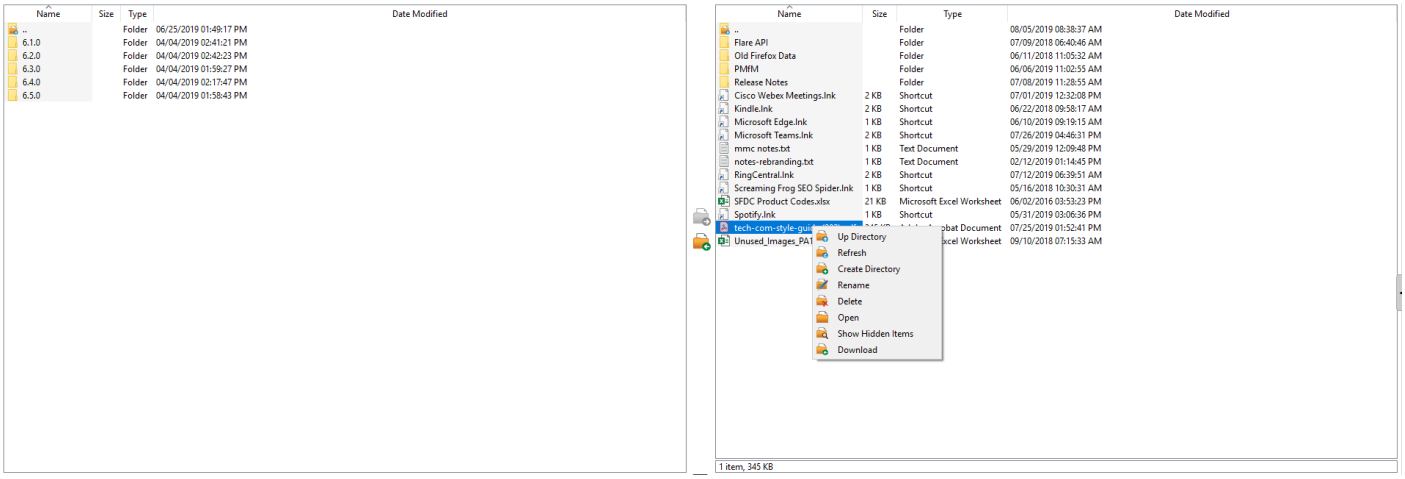
> ***Opmerking:*** *De miniatuurweergaves worden onder ideale omstandigheden ongeveer om de drie seconden vernieuwd, maar deze periode kan langer zijn, afhankelijk van de verbindingssnelheid en de hoeveelheid te verzenden gegevens.*

Bestandsoverdracht naar en van het externe eindpunt

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, mag u alleen bestanden naar het externe systeem uploaden of bestanden naar uw lokale computer downloaden. De toegang tot het bestandssysteem kan ook worden beperkt voor bepaalde paden op het externe of lokale systeem, waarmee wordt afgedwongen dat uploaden of downloaden alleen voor bepaalde mappen is toegestaan.

Zet bestanden over met de knoppen Uploaden of Downloaden of door bestanden te slepen en neer te zetten. Als u met de rechter muisknop op een bestand klikt, dan verschijnt een contextafhankelijk menu waarmee u onder andere een nieuwe map kunt aanmaken, het bestand kunt openen of verwijderen of de naam ervan kunt veranderen, of het direct naar uw machine kunt downloaden.



Als er een ICAP-server is ingeschakeld, wordt er "Bezig met scannen" voor het bestand weergegeven totdat de overdracht is beëindigd. De resultaten van de scan worden tijdens of na een bestandsoverdracht weergegeven in het ***Bestandsoverdrachtslogboek****. Het bestand wordt niet overgedragen als er malware in wordt gedetecteerd. 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

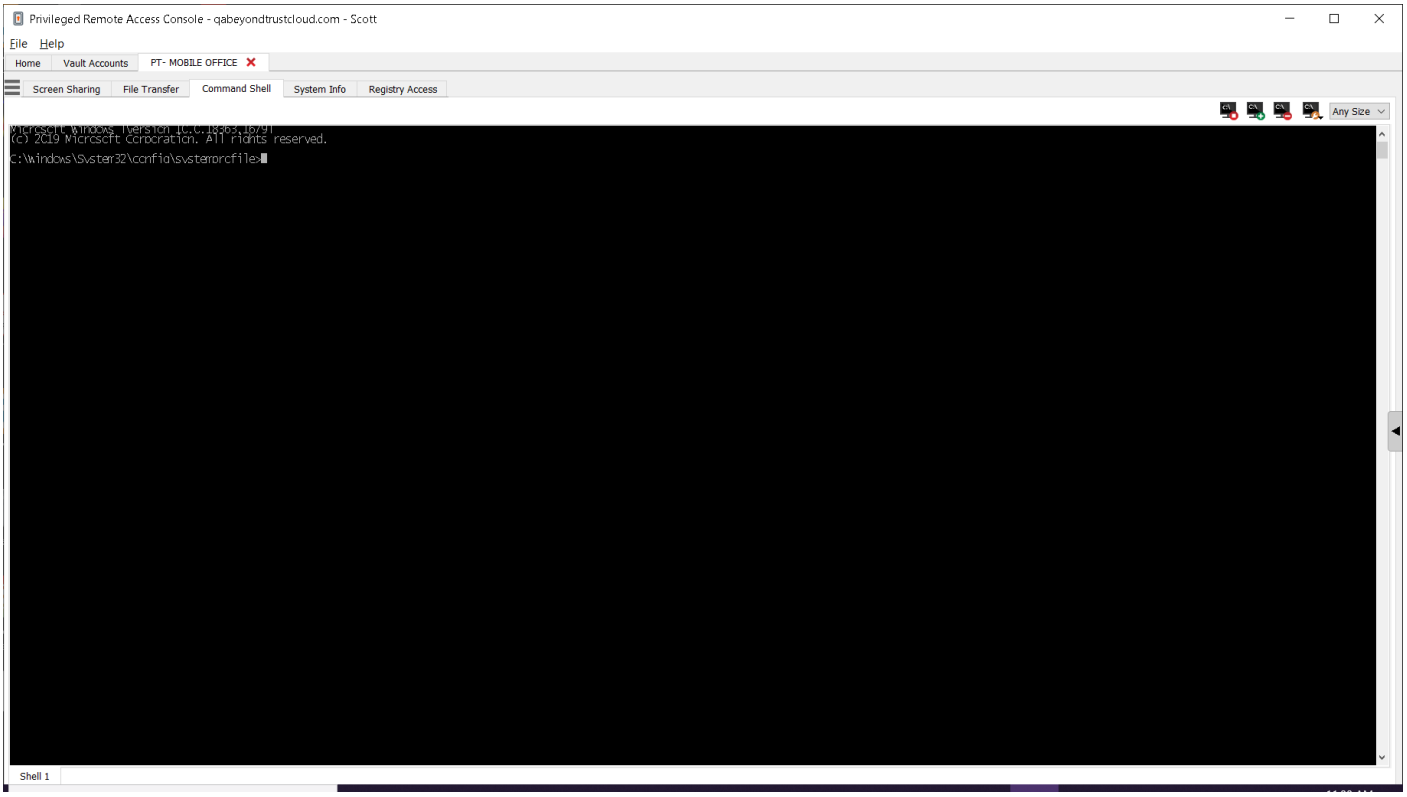
	Stop de toegang tot het bestandssysteem op de externe computer als u deze niet meer nodig hebt.
	Ga naar een map op één niveau hoger in het geselecteerde bestandssysteem.
	Vernieuw de weergave van het geselecteerde bestandssysteem.
	Maak een nieuwe map aan.

	Wijzig de naam van een map of bestand.
	Verwijder een map of bestand. NB: Als u een bestand of map verwijdert, dan is de verwijdering permanent. De map of het bestand gaat niet naar de prullenbak.
	Geef verborgen bestanden weer.
 	Selecteer een of meer bestanden of mappen en klik vervolgens op de betreffende knop om de bestanden naar het externe systeem te uploaden of naar uw lokale systeem te downloaden. U kunt bestanden ook slepen en neerzetten om ze over te dragen.
	Als een bestand met dezelfde naam al bestaat op de locatie waar u een bestand naartoe wilt overdragen, dan moet u kiezen of het bestaande bestand automatisch moet worden overschreven of dat bij elk bestand met gelijke naam een prompt moet verschijnen. NB: Als de inhoud van de bestanden identiek is, dan wordt de upload overgeslagen en krijgt u een waarschuwingsbericht.
	Door de bestandsinformatie te bewaren wordt het oorspronkelijke tijdstempel van het bestand bewaard. Als deze optie is uitgezet, dan komt het tijdstempel van het bestand overeen met de datum en tijd waarop het bestand is overgedragen.
	Als automatische bestandsoverdracht is ingeschakeld, dan begint de overdracht zodra u op de knop Uploaden of Downloaden klikt of u een bestand van het ene bestandssysteem naar het andere sleept.
	Als automatische bestandsoverdracht niet is ingeschakeld, dan moet u in de overdrachtsmanager de bestanden selecteren die u wilt overdragen en vervolgens op de knop **Start** klikken om met de overdacht te beginnen.
	Selecteer in de overdrachtsmanager een bestand en klik op de knop **Details** om informatie te zien zoals datum en tijd van de overdracht, de oorsprong en bestemming van de bestanden en het aantal overgedragen bytes.
	Selecteer in de overdrachtsmanager een of meer bestanden en klik vervolgens op **Annuleren** om de overdracht af te breken.
	Wis alle informatie in de bestandsmanager.

Open de opdrachtshell op het externe eindpunt met behulp van de toegangsconsole

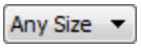
Met externe opdrachtshell kunnen bevoorrechte gebruikers een interface naar een virtuele opdrachtregel op externe computers openen. Gebruikers kunnen dan op hun lokale systeem opdrachten invoeren die op het externe systeem worden uitgevoerd. U kunt vanuit meerdere shells werken. NB: Scripts die de gebruiker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

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



Ondersteuningsgereedschappen opdrachtshell

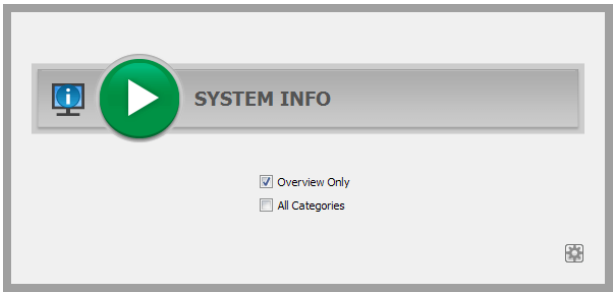
	Stop de toegang tot de opdrachtregel als u deze niet meer nodig hebt.
 	Open een nieuwe shell om meerdere opdrachtregels uit te voeren of individuele shells te sluiten zonder toegang tot opdrachtregels te verlaten. Shells worden in tabbladen onderaan het scherm weergegeven.
	Indien u daartoe gemachtigd bent, hebt u toegang tot een vervolgkeuzelijst van reeds geschreven scripts. Als u een script selecteert om uit te voeren, dan krijgt u een prompt met een korte beschrijving van dat script. Als u op **Ja** klikt, dan wordt het script in de actieve opdrachtshell uitgevoerd.

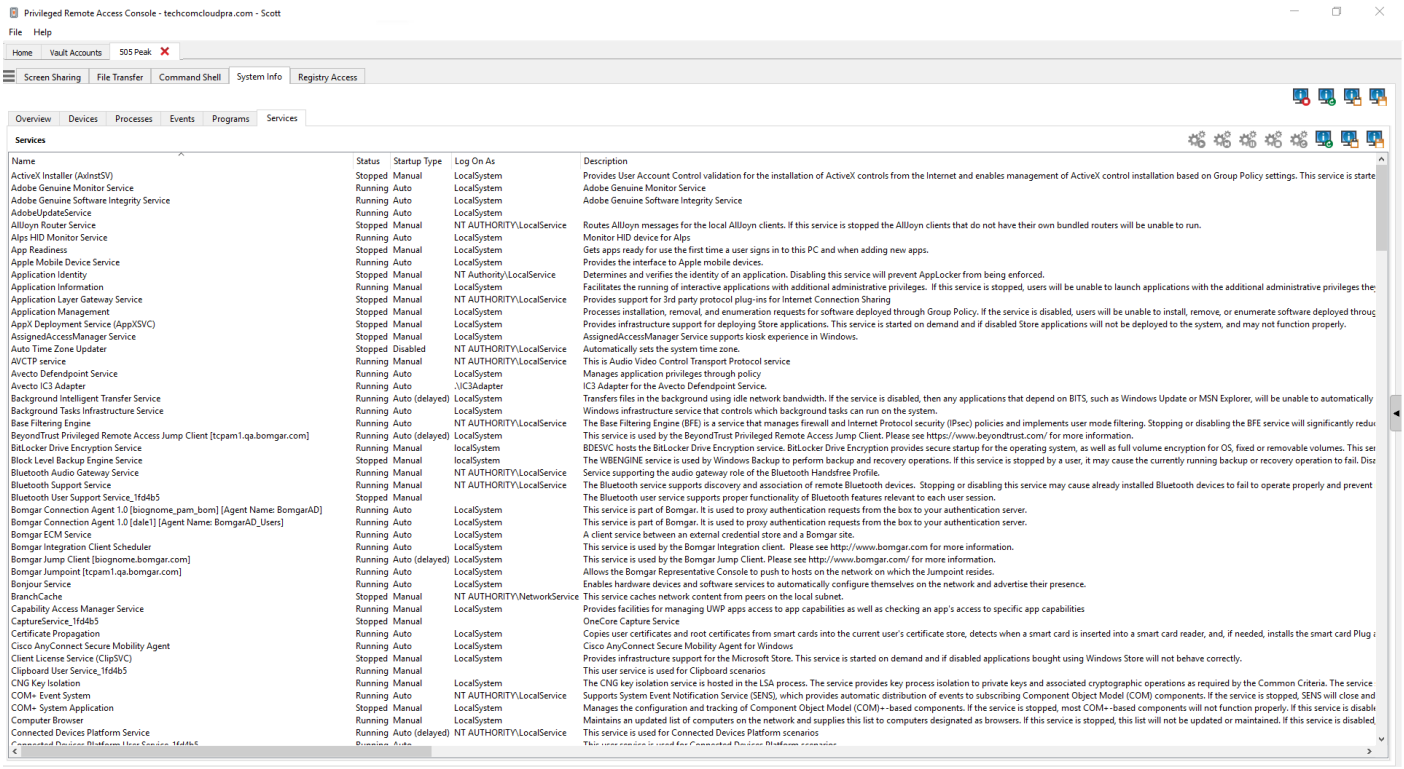
	Open hulpmiddelen om te gebruiken binnen de opdrachtprompt. Plak de inhoud van uw klembord door deze in het menu te selecteren of door met de rechtermuisknop in het terminalvenster te klikken. Kopieer een logboek van de huidige shell naar uw klembord of sla dit op uw computer op. Selecteer een gedeelte van de tekst als u een bepaald deel wilt kopiëren. Wis alle regels die op dit moment niet zichtbaar zijn of wis alle inhoud van de terminal. Hulpmiddelen kunnen ook worden geopend door in het terminalvenster op Ctrl te drukken en met de rechtermuisknop te klikken.
	Selecteer de afmetingen waarmee u het beeldscherm wilt bekijken. Kies uit 80x50, 80x25 of voer willekeurige afmetingen in.

Systeeminformatie bekijken op het externe eindpunt

Bevoorrechte gebruikers mogen 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. Gebruikers met de juiste machtigingen kunnen ook processen afsluiten, services starten, stoppen, pauzeren, hervatten en opnieuw starten en de installatie van programma's verwijderen.

Omdat de grote hoeveelheid gegevens die kan worden opgehaald lange overdrachtstijden tot gevolg kan hebben, kunt u ervoor kiezen uw weergave alleen met het tabblad **Overzicht** te beginnen of om de gegevens voor alle tabbladen op te halen. Als u ervoor kiest om met **Alleen overzicht** te beginnen, dan kunt u de gegevens voor de andere tabbladen ophalen door naar de sectie te gaan die u wilt bekijken en op de knop **Vernieuwen** bovenaan die sectie te klikken.



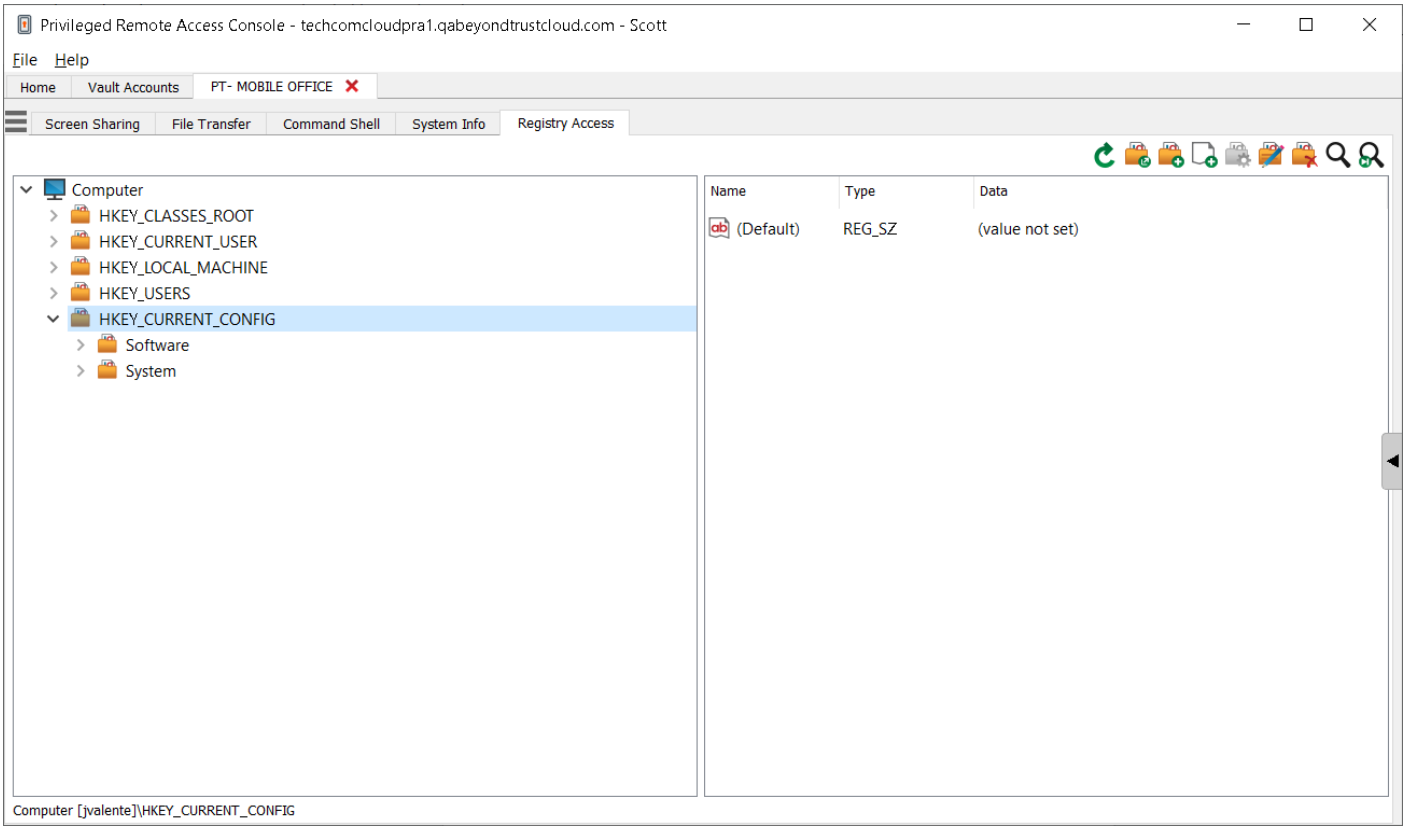


Hulpmiddelen voor systeeminformatie

	Stop met het ophalen van informatie over het externe systeem. Na het stoppen blijft de laatst bijgewerkte informatie beschikbaar om te bekijken, maar er wordt dan geen nieuwe informatie meer opgehaald.
	Vernieuw uw weergave van de systeeminformatie of haal de informatie op voor tabbladen waarnaar u in eerste instantie geen toegang had gevraagd. Het vernieuwen kan plaatsvinden voor individuele secties of voor alle secties van het geselecteerde tabblad.
	Vernieuw een categorie systeeminformatie automatisch.
	Kopieer de informatie naar uw klembord. Kopieer individuele secties of alle secties van het geselecteerde tabblad.
	Sla een tekstbestand met systeeminformatie op uw lokale computer op. U kunt individuele secties opslaan of alle secties van het geselecteerde tabblad.
	Beëindig een lopend proces op het externe systeem.
	Verwijder de installatie van een app op het externe systeem.
	Start een gestopte service op het externe systeem.
	Hervat een gepauzeerde service op het externe systeem.
	Pauzeer een lopende service op het externe systeem.
	Stop een lopende service op het externe systeem.
	Herstart een lopende service op het externe systeem.

Toegang tot de register-editor op het externe eindpunt

Krijg toegang tot een extern Windows-register zonder de noodzaak van scherm delen. Terwijl u de virtuele register-editor uitvoert, kunt u nieuwe sleutels toevoegen, sleutels verwijderen, sleutels bewerken, sleutels opzoeken of sleutels importeren of exporteren.



Hulpmiddelen voor de Register-editor

	Het register vernieuwen
	Registerinvoer vanuit een bestand importeren
	Registerinvoer naar een bestand exporteren
	Nieuwe registersleutel aanmaken
	Nieuwe registerwaarde aanmaken

	Geselecteerde registerwaarde wijzigen
	Naam van de geselecteerde registerinvoer wijzigen
	Geselecteerde registerinvoer verwijderen
	Register doorzoeken
	Volgend item zoeken

Sessiebeheer en teamsamenwerking

Actieve toegangssessies bekijken

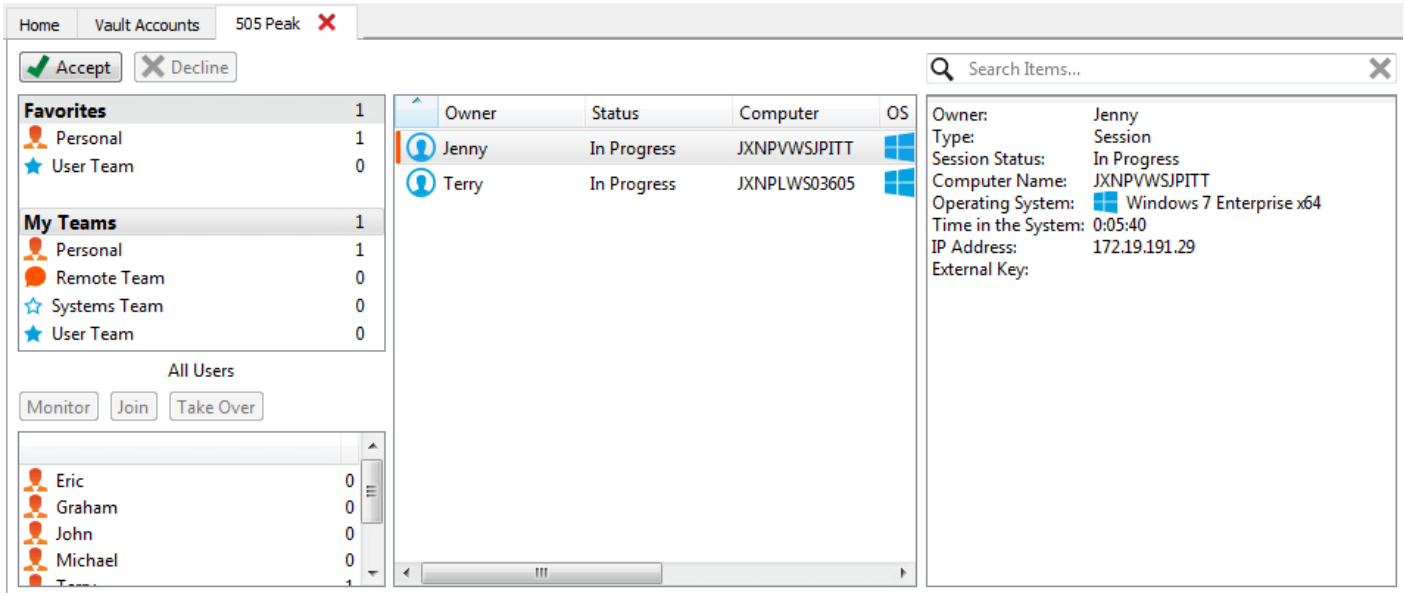
Sessiewachtrijen bieden informatie over en toegang tot actieve sessies. De **Persoonlijke wachtrij** bevat sessies die u op dit moment uitvoert, evenals uitnodigingen om een gedeelde sessie bij te wonen.

U hebt ook wachtrijen voor alle teams waar u lid van bent. Als een andere gebruiker een ander teamlid verzoekt een sessie bij te wonen, verschijnt die uitnodiging in de wachtrij van het team. Wanneer er geen specifiek team is geselecteerd, kunnen teammanagers en teamleiders ook zien welke teamleden op dat moment sessies hebben.

Klik op de ster links van de teamnaam om die wachtrij als favoriet te markeren. Als een teamchatbericht is verzonden, verandert de ster in een oranje chatballon.

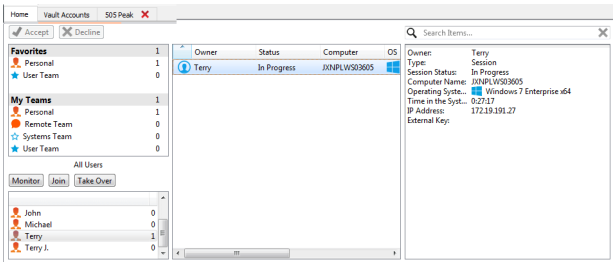
Sorteer uw wachtrijen op verschillende criteria, zoals de duur van de sessie, de naam van de computer of de externe code. U kunt ook naar een actieve sessie zoeken. Klik op een item in de wachtrij om informatie over dat item te bekijken. Klik er nogmaals op om het informatievenster te sluiten. De toegangsconsole onthoudt de volgorde van de kolommen en de sorteervolgorde van de sessiewachtrij bij de volgende keer dat de toegangsconsole wordt gestart.

U kunt meerdere sessies gelijktijdig uitvoeren. Bovenaan de toegangsconsole is een tabblad aanwezig voor elk van uw open sessies.



Het dashboard gebruiken om teamleden te beheren

Via het dashboard kunnen bevoorrechte gebruikers lopende sessies zien en erop meekijken, zodat zij als manager toezicht op hun medewerkers hebben. Op basis van de rollen die op de pagina **Teams** van de beheerinterface zijn toegewezen, kunnen teamleiders van een bepaald team met teamleden meekijken en kunnen teambeheerders zowel met teamleiders als met teamleden van dat team meekijken.



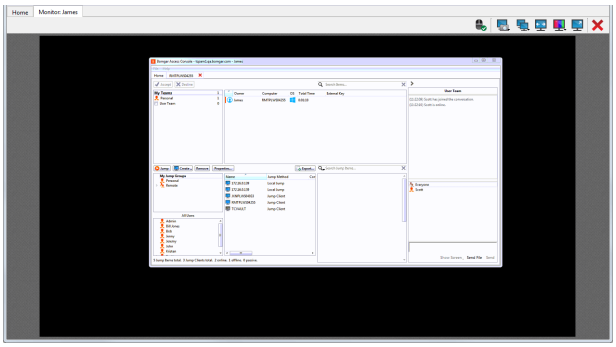
Als een gebruiker teambeheerder of teamleider van een of meer teams is en een van die wachtrijen selecteert, dan verschijnt het dashboard-deelvenster onder het wachtrijselectie-deelvenster op het tabblad **Start** van de console. In dit deelvenster verschijnen alleen ingelogde teamleden met een lagere rol voor het geselecteerde team.

Selecteer een gebruiker vanuit het dashboard-deelvenster om sessies te bekijken die deze uitvoert. Een teambeheerder of teamleider kan een sessie van een andere gebruiker van dat team overnemen door de betreffende sessie uit de wachtrij te selecteren en op de knop **Overnemen** te klikken. Hiermee wordt het eigendom van de sessie naar die teambeheerder of teamleider overgedragen, terwijl de oorspronkelijke eigenaar als deelnemer in de sessie blijft.

Een teammanager kan ook aan een sessie deelnemen die al aan de gang is door op de knop **Bij sessie voegen** te klikken. Dit is bijna hetzelfde als wanneer iemand aan een sessie deelneemt via een sessie-uitnodiging, alleen is er geen uitnodiging vereist.

> ***Opmerking:*** *De teamleider kan alleen dan deelnemen of de sessie van een teamlid overnemen als de teamleider startsessie-toegang heeft tot het Jumpitem dat is gebruikt om de sessie aan te maken of als het hokje is aangevinkt bij de dashboardinstelling zodat deelnemen of overnemen zonder startsessie-toegang is toegestaan.*

Als dit in de /login-interface is geconfigureerd, kan een teambeheerder of teamleider met teamleden van een lagere rol meekijken - ook als er geen lopende sessies zijn - zolang die gebruikers in de console zijn ingelogd.



In de hoek van het bureaublad van de gebruiker verschijnt een pictogram dat aangeeft dat er wordt meegekeken. Als de gebruiker met de cursor naar dit pictogram gaat, dan gaat het pictogram naar een andere hoek om te voorkomen dat de gebruiker dat deel van het scherm niet kan gebruiken. Selecteer de gebruiker van wie u het scherm wilt bekijken en klik dan op de knop **Meekijken**. Hierdoor wordt een nieuw tabblad op uw console geopend, waarin de console van de gebruiker wordt weergegeven.

Om de besturing van de computer van de gebruiker over te nemen, moet u op de knop **Muis/toetsenbordbediening inschakelen** klikken.

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

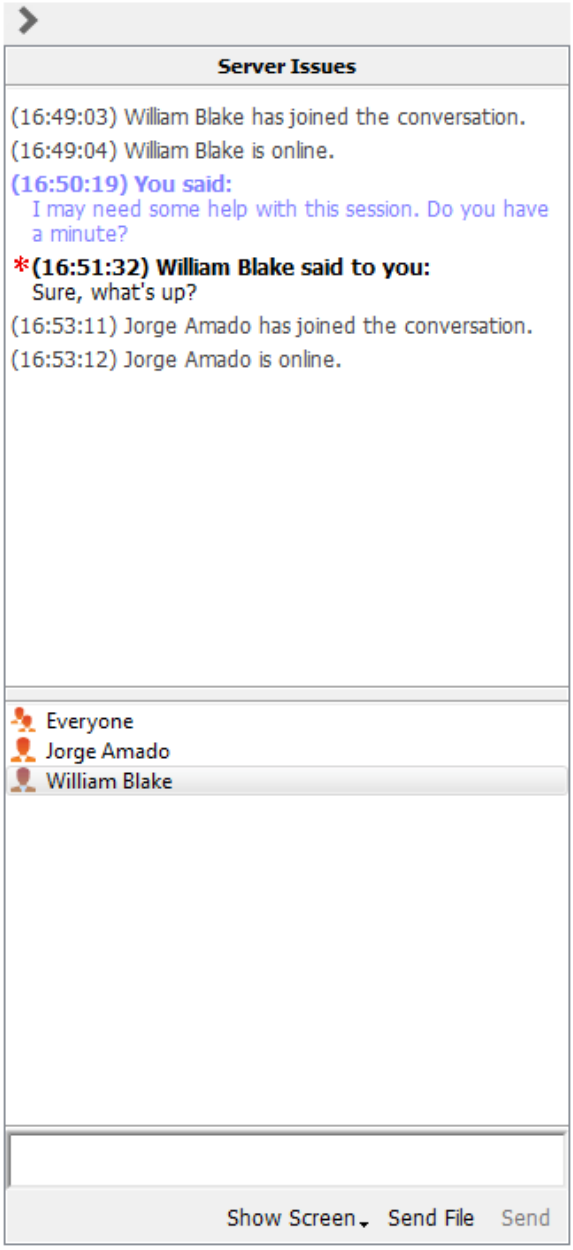
Met andere gebruikers chatten

U kunt vanaf het tabblad **Start** van de console met andere ingelogde gebruikers chatten. Als u lid bent in een of meer teams, dan kunt u uit de lijst wachtrijen links op het tabblad **Start** een willekeurig team selecteren om mee te chatten. U kunt met alle leden van dat team chatten of alleen met één lid.

Klik op het pijltje linksboven in het kantlijnartikel om het schuivende kantlijnartikel in te klappen. Als het kantlijnartikel ingeklapt is, kunt u de muis boven het verborgen venster laten zweven om het zichtbaar te maken. Klik op de speld die linksboven in het kantlijnartikel voor het pijltje in de plaats is gekomen om het schuivende kantlijnartikel weer vast te spelden.

Woorden die tijdens het typen verkeerd worden gespeld, worden rood onderstreept. Klik met de rechtermuisknop voor spellingssuggesties of om die spelling voor de huidige sessie op de console te negeren.

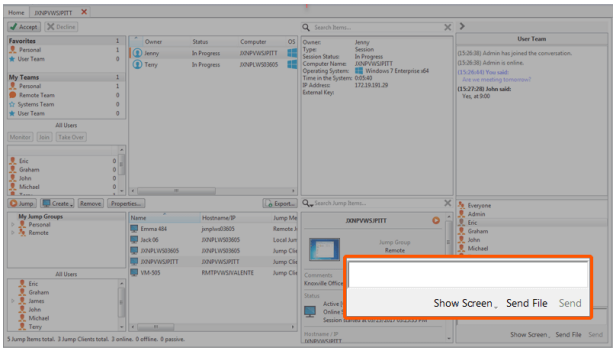
U kunt in de instellingen kiezen of in de teamchat statusberichten worden meegenomen, zoals het in- of uitloggen van gebruikers, of alleen de tussen leden verzonden chats.



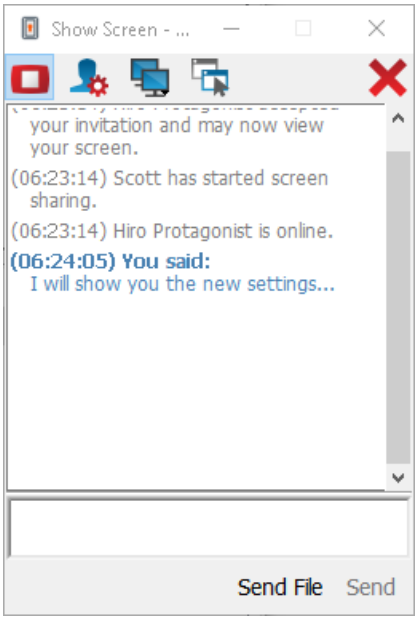
Uw scherm met een andere gebruiker delen

Als uw beheerder deze machtiging heeft ingeschakeld, dan kunt u uw scherm met een andere gebruiker delen zonder dat de ontvangende gebruiker een sessie hoeft bij te wonen. Deze optie is beschikbaar zelfs als u geen sessie bijwoont.

Selecteer een gebruiker uit een teamwachtrij en klik op **Scherm tonen**. Als u met meer dan één beeldscherm werkt, dan kunt u selecteren welk scherm u wilt delen of welke apps zichtbaar zijn voor de andere gebruiker. Nadat u uw selectie hebt gemaakt, krijgt de ontvangende gebruiker een kennisgeving met de optie de uitnodiging te accepteren of af te wijzen.



Er verschijnt een venster **Scherm tonen** met de naam van de gebruiker die uw scherm nu bekijkt. Dit venster bevat een chatvak en de opties om te stoppen met scherm delen, de ontvangende gebruiker de besturing te geven en te selecteren welk beeldscherm en welke apps u wilt delen. U kunt het delen van uw scherm beëindigen of u kunt de gedeelde sessie helemaal afsluiten. Als u het venster **Scherm tonen** open laat, dan kunt u het delen van uw scherm opnieuw starten.



Gereedschappen voor Mijn scherm tonen

Gebruiker die deelt

	Stop tijdelijk met het delen van uw scherm met een andere gebruiker. Hierdoor wordt scherm delen gepauzeerd maar wordt het venster **Scherm tonen** niet gesloten, zodat u het delen van het scherm opnieuw kunt starten.
	Start (opnieuw) het delen van uw scherm.
	Geef de besturing van uw muis en toetsenbord aan de gebruiker die uw scherm bekijkt.

	Selecteer welk beeldscherm u met een andere gebruiker wilt delen. Het primaire beeldscherm wordt met een **P** aangegeven.
	Selecteer welke apps u wilt delen met de gebruiker die uw scherm bekijkt.
	Beëindig de sessie met scherm delen. Hierdoor wordt de interface voor scherm delen gesloten.

Gebruiker die kijkt

	De gebruiker die zijn of haar scherm met u deelt heeft de besturing over muis en toetsenbord aan u gegeven.
	Zet een virtuele muisaanwijzer aan die zichtbaar is op het scherm van de gebruiker die zijn of haar scherm deelt.
	Maak een schermopname van het scherm van de gebruiker die zijn of haar scherm deelt met de volledige resolutie.
	Bekijk het externe scherm op ware grootte of op schaal.
	Bekijk het externe bureaublad als volledig scherm of keer terug naar de weergave van de interface.
	Beëindig de sessie met scherm delen. Hierdoor wordt de interface voor scherm delen gesloten.

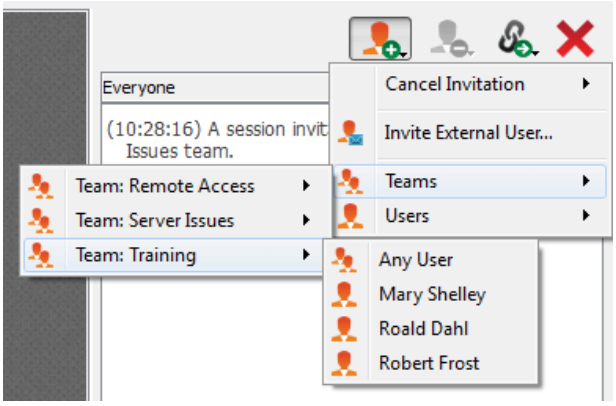
Een sessie met andere gebruikers delen

Nodig een andere gebruiker uit om een sessie bij te wonen door in de sessiehulpmiddelen op de knop **Delen** te klikken. Standaard worden hier alleen de teams vermeld waar u toe behoort.

U kunt een gebruiker selecteren uit de lijst met teams om uit te nodigen om de sessie bij te wonen.

Als u **Elke gebruiker** selecteert, dan wordt de uitnodiging naar de teamwachtrij verstuurd zodat een willekeurige individuele gebruiker in het geselecteerde team de sessie kan bijwonen. U kunt meerdere uitnodigingen verzenden als u wilt dat meerdere gebruikers uit het team de sessie bijwonen.

Gebruikers worden hier alleen vermeld als zij op de console zijn ingelogd of als voor hen uitgebreide beschikbaarheid is ingeschakeld.



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

Als u een gebruiker waarvoor uitgebreide beschikbaarheid is ingeschakeld uitnodigt, dan wordt per e-mail een kennisgeving naar hem of haar verzonden.

Als u een uitnodiging hebt verzonden en deze nog steeds actief is, dan kunt u de uitnodiging intrekken door deze in het menu **Uitnodiging annuleren** te selecteren. 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.

Een uitnodiging wordt inactief als een van de volgende gebeurtenissen optreedt:

- De uitnodigende gebruiker annuleert de uitnodiging
- De sessie stopt
- De uitgenodigde gebruiker aanvaardt de uitnodiging
- De uitgenodigde gebruiker wijst de uitnodiging af

Als een extra gebruiker zich bij een gedeelde sessie voegt, kan hij of zij de gehele chat-geschiedenis zien.

Met andere gebruikers chatten tijdens een gedeelde sessie

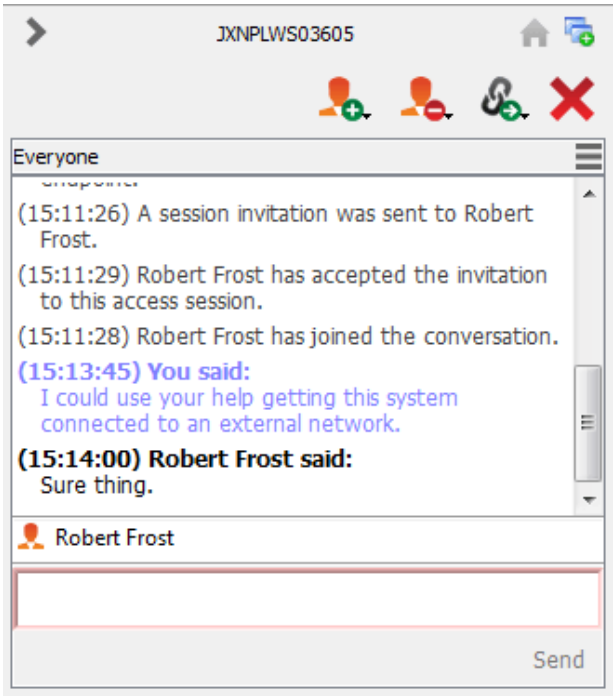
Het venster met de sessiechat dient als een continue logboekregistratie van alles wat er tijdens de sessie gebeurt, inclusief bestandsoverdracht en gebruikte hulpmiddelen.

Als een of meer gebruikers de sessie delen, kunt u met de andere gebruikers chatten. Als een extra gebruiker zich bij een gedeelde sessie voegt, kan hij of zij de gehele chat-geschiedenis zien.

Klik op het pijltje linksboven in het kantlijnartikel om het schuivende kantlijnartikel in te klappen. Als het kantlijnartikel ingeklapt is, kunt u de muis boven het verborgen venster laten zweven om het zichtbaar te maken. Klik op de speld die linksboven in het kantlijnartikel voor het pijltje in de plaats is gekomen om het schuivende kantlijnartikel weer vast te spelden.

Woorden die tijdens het typen verkeerd worden gespeld, worden rood onderstreept. Klik met de rechtermuisknop voor spellingssuggesties of om die spelling voor de huidige sessie op de console te negeren.

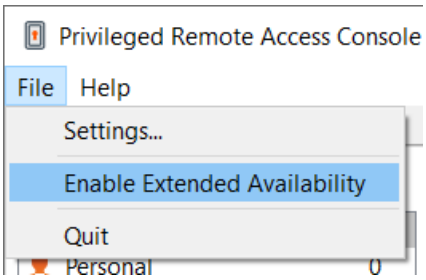
Berichten verschijnen als tekst zonder opmaak in het chat-invoergebied. U kunt in een bericht BBCode-tags toevoegen of bewerken om te helpen bij de tekstopmaak. Tekstopmaak wordt toegepast nadat het bericht verzonden is.



Opmerking: *Het is mogelijk de positie van de in het kantlijnartikel weergegeven widget-secties te wijzigen, zoals het chat-venster of het deelvenster met sessie-informatie. Als u met uw muis boven de titelbalk van een sectie zweeft, dan verandert de cursor in een gesloten hand, zodat u die sectie kunt wegslepen en in het kantlijnartikel kunt plaatsen.*

Uitgebreide beschikbaarheid gebruiken om beschikbaar te blijven als u niet bent ingelogd

Gebruikers kunnen met uitgebreide beschikbaarheid e-mailuitnodigingen ontvangen om sessies te delen, zelfs al zijn ze niet op de console ingelogd. Als u een uitnodiging verzendt, dan kunt u leden uit uw team uitnodigen. Indien u daartoe gemachtigd bent, kunt u gebruikers uitnodigen uit teams waar u niet toe behoort.



Als uw account voor uitgebreide beschikbaarheid is geconfigureerd, dan kunt u de functionaliteit vanaf het menu **Bestand** op de toegangsconsole in- of uitschakelen.

Als uitgebreide beschikbaarheid voor u is ingeschakeld, dan ziet u een melding als u op de console inlogt. Vanuit deze dialoog kunt u eenvoudig uitgebreide beschikbaarheid uitschakelen, bijvoorbeeld om te voorkomen dat u tijdens een sessie wordt gestoord.

E-mailmelding en -uitnodiging

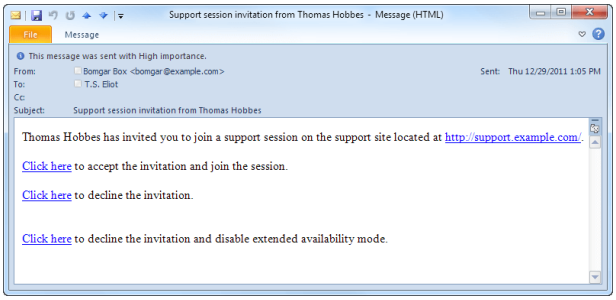
Telkens als u de uitgebreide beschikbaarheid-modus inschakelt, wordt door het B Series Appliance een melding verzonden naar het voor uw gebruikersaccount geconfigureerde e-mailadres.

Opmerking: *BeyondTrust haalt geen e-mailadressen van externe LDAP-adreslijstarchieven. Het e-mailadres moet op een van de volgende twee manieren in BeyondTrust zijn geconfigureerd:*

1. *Een beheerder kan een e-mailadres aan een gebruikersaccount toevoegen door naar **/login > Gebruikers en beveiliging > Gebruikers** te gaan en de account te bewerken.*
2. *De gebruiker kan zijn of haar eigen e-mailadres instellen door naar de pagina **/login > Mijn account** te gaan.*

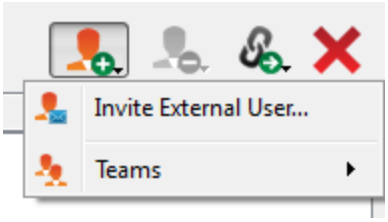
De melding bevat de URL van de site evenals een koppeling om de modus uitgebreide beschikbaarheid snel uit te schakelen.

Het B Series Appliance verzendt ook e-mailmeldingen als u voor een sessie wordt uitgenodigd. Zo kunt u een sessie bijwonen zelfs als u op dat moment niet op de console bent ingelogd. De e-mailmelding bevat koppelingen om de uitnodiging te accepteren of af te wijzen, en om de uitnodiging af te wijzen en tegelijkertijd de modus uitgebreide beschikbaarheid uit te schakelen.



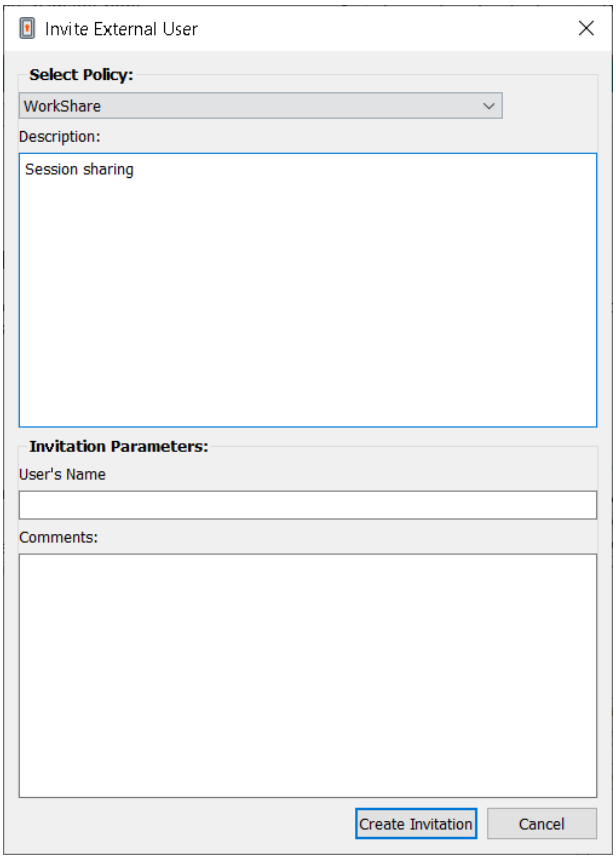
Een externe gebruiker uitnodigen om een toegangssessie bij te wonen

Een gebruiker kan in een sessie een externe gebruiker uitnodigen eenmalig aan een sessie deel te nemen. De uitnodigende gebruiker moet op de knop **Sessie delen** klikken en vervolgens **Externe gebruiker uitnodigen** selecteren.

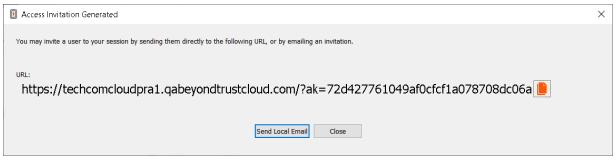


Er verschijnt een dialoogvenster waarin de gebruiker wordt gevraagd een sessiebeleid te selecteren. Deze beleidslijnen worden in de beheerinterface aangemaakt en hiermee wordt het machtigingsniveau bepaald dat voor de externe gebruiker geldt. Als u een beleid selecteert, wordt de volledige omschrijving van het beleid eronder weergegeven.

Voer de naam van de uitgenodigde gebruiker in. Deze naam verschijnt in het chatvenster en in rapporten. Voer vervolgens opmerkingen in om aan te geven waarom u deze gebruiker uitnodigt. Klik op **Uitnodiging aanmaken**, waarna een nieuw dialoogvenster verschijnt met de URL voor de uitnodiging.



Klik op de knop **Verzenden** om te selecteren hoe u de sessiecode naar de externe gebruiker wilt verzenden. Afhankelijk van de door uw beheerder geselecteerde opties kunt u de uitnodiging van uw lokale e-mailadres verzenden of van een e-mailadres op de server. U kunt de URL ook rechtstreeks naar de externe gebruiker kopiëren en plakken. De externe gebruiker moet het installatieprogramma voor de toegangsconsole downloaden en uitvoeren. Dit is een verkort proces vergeleken met de installatie van de volledige toegangsconsole.

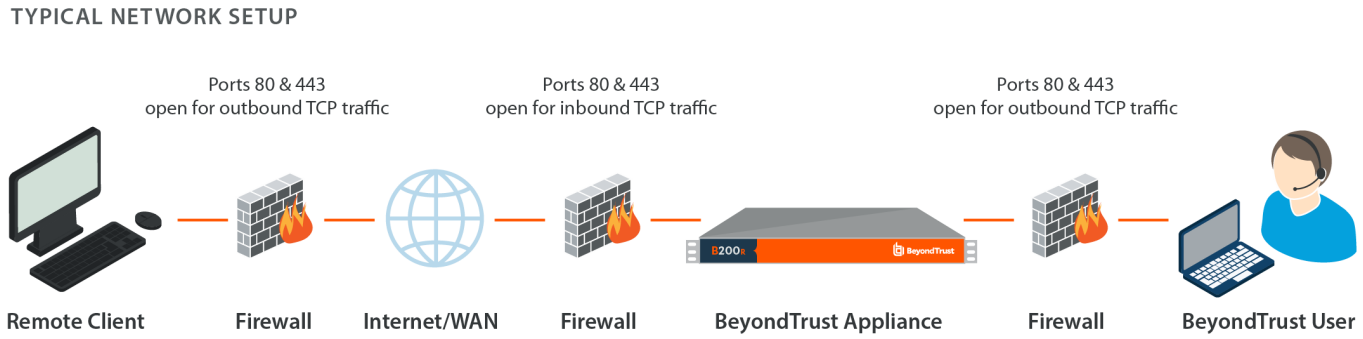


De externe gebruiker heeft alleen toegang tot het sessietabblad en heeft beperkte machtigingen. De externe gebruiker kan nooit de eigenaar van de sessie zijn. Als de uitnodigende gebruiker de sessie verlaat, dan wordt de externe gebruiker uitgelogd.

U kunt meerdere externe gebruikers voor een sessie uitnodigen.

Poorten en firewalls

De oplossingen van BeyondTrust zijn ontworpen om firewalls op een transparante manier te gebruiken en een verbinding toe te staan met elke computer met internetverbinding, waar ook ter wereld. Maar bij bepaalde sterk beveiligde netwerken kan enige configuratie noodzakelijk zijn.



- De poorten 80 en 443 moeten openstaan voor uitgaand TCP-verkeer in zowel de firewall van het externe systeem als van de lokale gebruiker. Afhankelijk van het voor u samengestelde pakket moeten mogelijk meer poorten beschikbaar zijn. Het schema toont een normale netwerkinstelling. Meer informatie hierover vindt u in de Hardware-installatiegids van het BeyondTrust Appliance B Series op https://www.beyondtrust.com/docs/privileged-remote-access/getting-started/deployment/hardware-sra/index.htm.
- Beveiligingssoftware voor internet, zoals softwarefirewalls, mogen het downloaden van uitvoerbare bestanden van BeyondTrust niet blokkeren. Voorbeelden van softwarefirewalls zijn McAfee Security, Norton Security en Zone Alarm. Als u een softwarefirewall hebt, dan krijgt u mogelijk verbindingsproblemen. Om zulke problemen te voorkomen, moet u de instellingen van uw firewall zodanig configureren dat de volgende uitvoerbare bestanden worden toegestaan. Hierin is {uid} een unieke identificator bestaande uit een letter en cijfers:
    - bomgar-scc-{uid}.exe
    - bomgar-scc.exe
    - bomgar-pac-{uid}.exe
    - bomgar-pac.exe
    - bomgar-pec-{uid}.exe
    - bomgar-pec.exe

    Neem contact op met de leverancier van uw firewallsoftware voor assistentie.
- Voorbeelden van regels voor firewalls op basis van de locatie van een B Series Appliance zijn te vinden op www.beyondtrust.com/docs/privileged-remote-access/getting-started/deployment/dmz/firewall-rules.htm.

Neem contact op met BeyondTrust Technical Support via www.beyondtrust.com/support als u nog steeds problemen ondervindt bij het maken van een verbinding.