BeyondTrust

Privileged Remote Access
Android-toegangsconsole 2.2.10

TC:12/12/2023

Inhoudsopgave

Handleiding voor de BeyondTrust-toegangsconsole voor Android

Deze gids is bedoeld om u te helpen bij het installeren van de BeyondTrust op uw Android-apparaat en om de functies van de BeyondTrust voor Android te begrijpen. U kunt met de support_button toegang krijgen tot externe eindpunten door een verbinding op te zetten via de toegangsconsole.

Let op: hoewel in deze gids schermopnames van een Android-smartphone worden gebruikt, is de functionaliteit gelijk als u een Android-tablet gebruikt.

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

De toegangsconsole op Android installeren

De BeyondTrust toegangsconsole voor Android kan gratis worden gedownload in Google Play. Zoek in Google Play op uw Android-apparaat naar 'BeyondTrust Toegangsconsole' en installeer de app vervolgens.

Om de BeyondTrust-toegangsconsole op uw apparaat te kunnen uitvoeren, moet uw B Series Appliance minimaal softwareversie 15.2 bevatten. De BeyondTrust toegangsconsole wordt ondersteund op Android-telefoons met minimaal versie 2.3 en op Android-tablets met minimaal versie 3.0.

Opmerking: *Alleen de BeyondTrust-toegangsconsole kan worden gebruikt met een Privileged Remote Access-site (PRA). De BeyondTrust-console voor ondersteuningstechnici kan niet worden gebruikt om verbinding met een Privileged Remote Access-site te maken en de BeyondTrust-toegangsconsole kan niet worden gebruikt om verbinding met een BeyondTrust Remote Support-site te maken.*

BELANGRIJK!

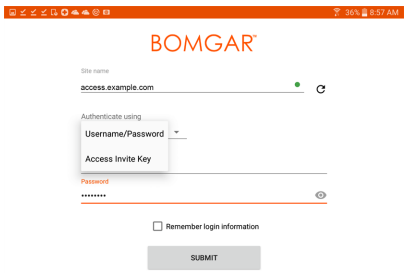
Uw B Series Appliance moet zijn voorzien van een geldig SSL-certificaat dat is ondertekend door een certificaatautoriteit. BeyondTrust ondersteunt geen zelf-ondertekende certificaten voor de Android-toegangsconsole.[1] Neem contact op met BeyondTrust Technical Support nadat u een door een CA ondertekend SSL-certificaat op uw B Series Appliance hebt toegepast. Uw klantendiensttechnicus stelt dan een nieuw softwarepakket samen waarin uw SSL-certificaat is geïntegreerd. U kunt met de bijgewerkte build nadat deze geïnstalleerd is op uw B Series Appliance de BeyondTrust-toegangsconsole op uw apparaat uitvoeren om vanaf vrijwel elke willekeurige plaats toegang tot eindpunten te krijgen.

[1]Android-apparaten met een oudere versie van het besturingssystemen dan versie 4.0 zien mogelijk een certificaatfout als wordt geprobeerd om toegang tot uw BeyondTrust-site te krijgen. Dit probleem komt door een ontbrekend SSL-basiscertificaat in het certificaatarchief van het Android-apparaat. Dit probleem betreft alleen het Android-besturingssysteem en niet de BeyondTrust-software. Om dit probleem op te lossen moet u ofwel het Android-apparaat bijwerken of contact opnemen met de certificaatautoriteit om een ander SSL-basiscertificaat aan te vragen dat compatibel is met het Android-apparaat.

Inloggen op de toegangsconsole voor Android

Voer op het inlogscherm de hostnaam van uw BeyondTrust-site in, bijvoorbeeld toegang.voorbeeld.nl. Voer vervolgens de gebruikersnaam en het wachtwoord van uw BeyondTrust-gebruikersaccount in. U kunt ervoor kiezen dat de BeyondTrust-toegangsconsole uw inloggegevens onthoudt. Tik vervolgens op **Inloggen**.

Voor bevoorrechte gebruikers of leveranciers die de toegangsconsole gebruiken, kunt u de verificatiemethode wijzigen door op het label **Gebruikersnaam/wachtwoord** te tikken. Selecteer uit het vervolgkeuzemenu **Sleutel toegangsuitnodiging** en voer de aan u verstrekte sleutel in.



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.*

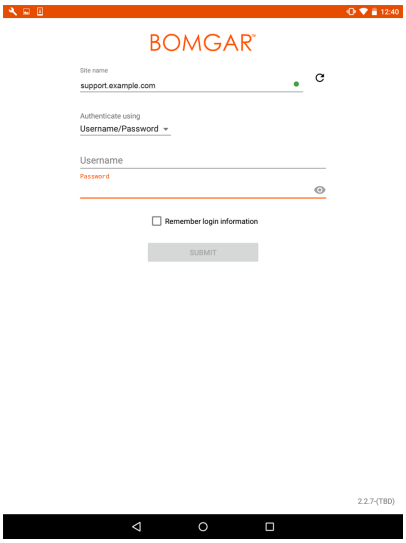
Inloggen bij de Android-toegangsconsole met SAML voor mobiel

SAML voor mobiel is een eenvoudige en veilige verificatiemethode voor de Android-toegangsconsole. Voor meer informatie over eenmalige aanmelding met SAML gaat u naar Security Assertion Markup Language op https://en.wikipedia.org/wiki/Security_Assertion_Markup_Language. Volg de onderstaande stappen om bij de Android-toegangsconsole in te loggen met SAML.

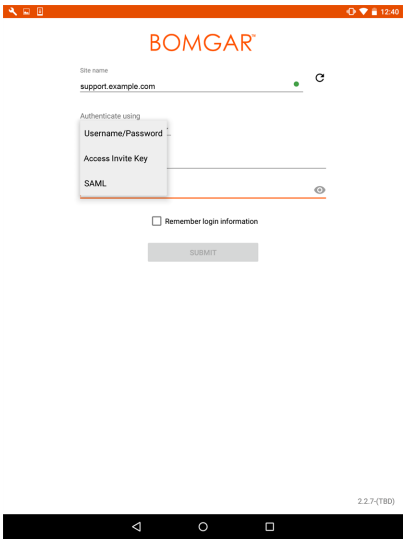
Opmerking: *Voordat u met SAML bij de Android-toegangsconsole probeert in te loggen, moet u eerst controleren of er een SAML-provider is geconfigureerd voor uw /login-beheeromgeving door naar* ***Gebruikers en beveiliging > Beveiligingsproviders*** *te gaan. Als SAML niet in /login is geconfigureerd, is SAML niet beschikbaar als verificatiemethode voor de Android-toegangsconsole. Voor meer informatie over het integreren van SAML eenmalige aanmelding in uw BeyondTrust Privileged Remote Access-omgeving, zie De SAML-beveiligingsprovider aanmaken en configureren op www.beyondtrust.com/docs/privileged-remote-access/how-to/integrations/security-providers/saml/configure-settings.htm.*

1. Tik op de toegangsconsole-app op uw Android-apparaat.

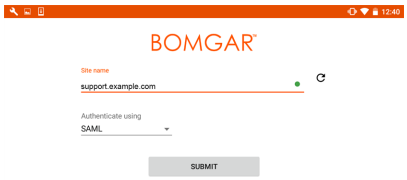
2. Op het inlogscherm tikt u op **Gebruikersnaam en wachtwoord**.



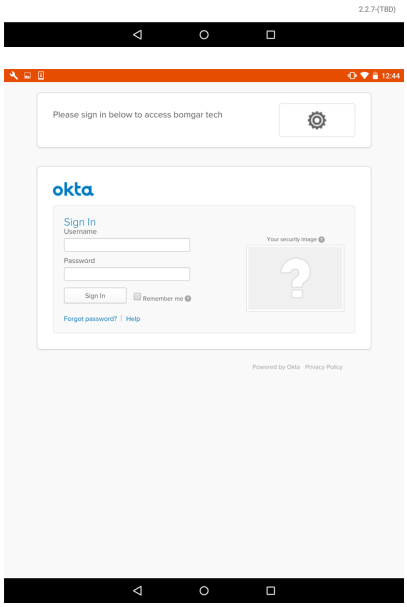
3. Selecteer **SAML**.



4. Tik op **Verzenden**.



5. Wanneer u wordt doorverwezen naar de webpagina van uw SAML-provider voert u uw inloggegevens in.
6. Tik op **Inloggen** voor toegang tot de console.



Instellingen wijzigen in de Android-toegangsconsole

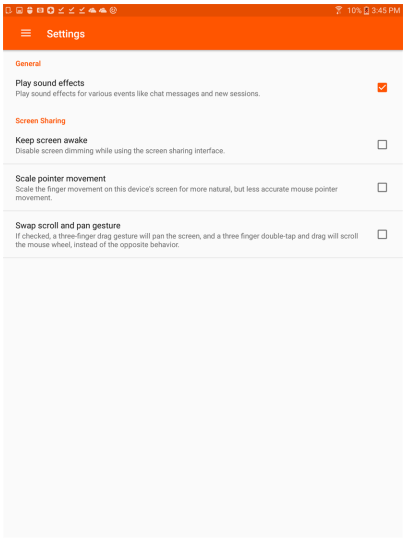
Om uw instellingen te wijzigen, selecteert u **Instellingen** uit het menu.

Met **Geluidseffecten afspelen** hoort u waarschuwingen voor bepaalde gebeurtenissen binnen de toegangsconsole.

Om ervoor te zorgen dat tijdens scherm delen uw scherm niet wordt gedimd, moet u **Scherm actief houden** aanvinken.

Als **Cursorbeweging schalen** is aangevinkt, volgt de cursor op de externe computer de beweging van uw vinger op het scherm. Als deze optie niet is aangevinkt, volgt de cursor mogelijk vertraagd, maar is de positie ervan nauwkeuriger.

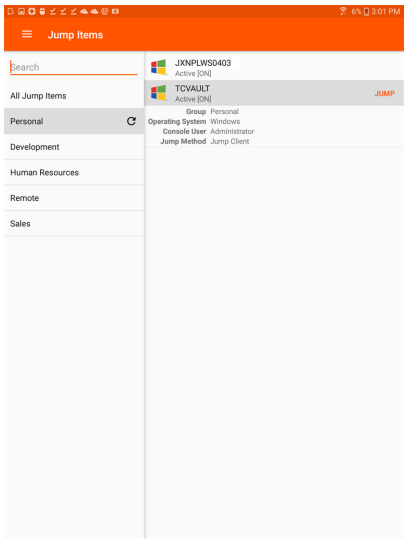
Met **Scrollen en pannen omwisselen** kunt u instellen met welke beweging u het muiswiel op de externe computer bedient en met welke beweging u op het scherm pant.



Jumpitems gebruiken voor toegang tot eindpunten vanaf de Android-toegangsconsole

Om toegang tot een individueel eindpunt te krijgen zonder assistentie van de eindgebruiker, moet u vanaf de pagina **Jump-clients** van de /login-beheerinterface een Jumpitem op dat systeem installeren. Daarnaast worden de volgende typen Jumpitems ondersteund door de mobiele toegangsconsole:

- **Externe Jump**
- **Externe VNC**
- **RDP**
- **Shell Jump**



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

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

Om een Jumpitem te vinden, tikt u op **Jumpitems** in het menu.

Selecteer een locatie en tik op de knop **Vernieuwen**. Als u het eindpunt hebt gevonden waar u toegang toe wilt krijgen, dan moet u de vermelding ervan selecteren om de details ervan te bekijken.

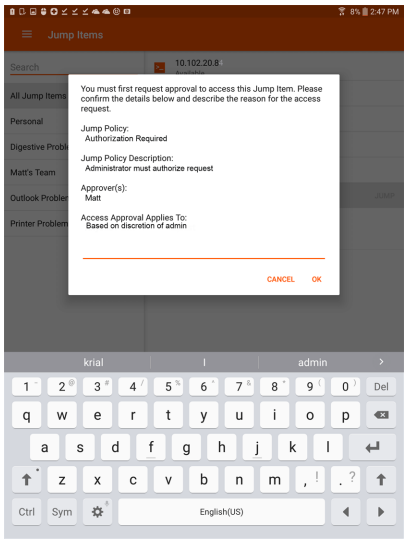
Tik op de knop **Jump** om een sessie te starten.

Autorisatie door eindgebruiker of derden

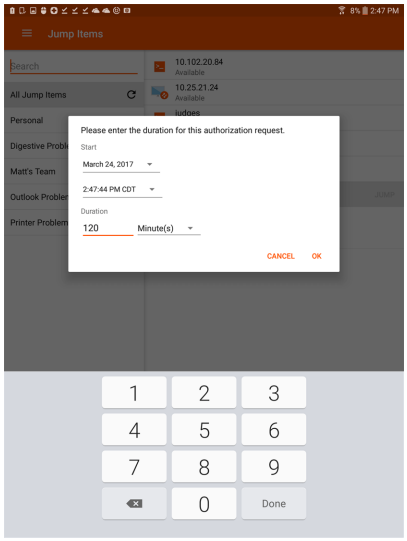
Afhankelijk van de configuratie van Jumpitems binnen de /login-beheerinterface kan er aan een Jumpitem een Jump-beleid zijn geassocieerd en kan er in het beleid een autorisatiecomponent zijn gedefinieerd waarin wordt afgedwongen dat de gebruiker toestemming van een derde partij of een beheerder nodig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

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

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



Vervolgens moet u aangeven wanneer en hoe lang u toegang tot het systeem wilt hebben.



Nadat het verzoek is ingediend, krijgt de externe partij of persoon die verantwoordelijk is voor goedkeuring van toegangsverzoeken een waarschuwing via een e-mailmelding, zodat hij of zij het verzoek kan goedkeuren of weigeren. Hoewel andere fiatteurs het e-mailadres kunnen zien van de persoon die het verzoek heeft goedgekeurd of geweigerd, kan de aanvrager dit niet. Nadat het verzoek is behandeld, wordt in de informatie van het Jumpitem een melding over de machtiging weergegeven met de tekst *goedgekeurd* of *geweigerd*. Als toegang wordt verleend, kan de gebruiker op de knop Jump tikken om toegang tot het systeem te krijgen.

Bomgar

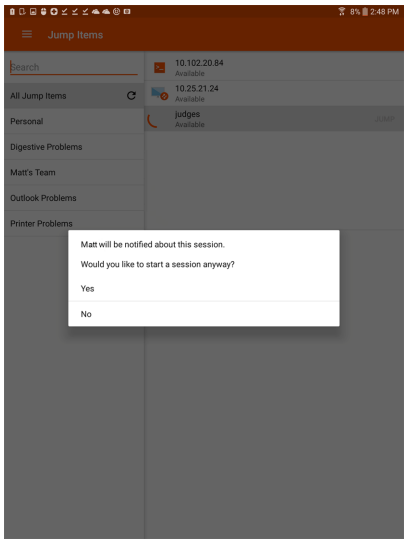
Your jump authorization request number 1 beginning at 05/31/49198 10:19:53 PM has been approved.

OK

Nadat u op de knop Jump hebt getikt, krijgt u een bericht te zien met de vraag of u een toegangssessie wilt opstarten. Als u besluit de sessie op te starten, dan verschijnen de opmerkingen van de goedkeurende partij en kunt u verdergaan om toegang tot het systeem te krijgen.

Als de gebruiker besluit verder te gaan, dan verdwijnen de opmerkingen van de goedkeurende partij en kan de gebruiker met het systeem gaan werken.

Voor meer informatie over hoe Jumpitems werken met Jump-roosters, Ticket-ID workflow etc. gaat u naar Jump-interface: Jumpitems gebruiken voor toegang tot externe systemen op https://www.beyondtrust.com/docs/privileged-remote-access/getting-started/access-console/jump-interface.htm.



Inloggegevens voor automatisch inloggen

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

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

Inloggen bij eindpunten met behulp van inloggegevensinjectie in de Android-toegangsconsole

Bij toegang tot een Windows-gebaseerde Jump-client via de mobiele toegangsconsole kunt u inloggegevens gebruiken uit een inloggegevensopslagplaats door bij het eindpunt in te loggen of door toepassingen uit te voeren als beheerder.

Voordat u inloggegevensinjectie gebruikt, moet u controleren of u een beschikbare inloggegevensopslag hebt om verbinding met BeyondTrust PRA te maken, zoals een wachtwoordkluis.

De Endpoint Credential Manager installeren en configureren

Vereisten:

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

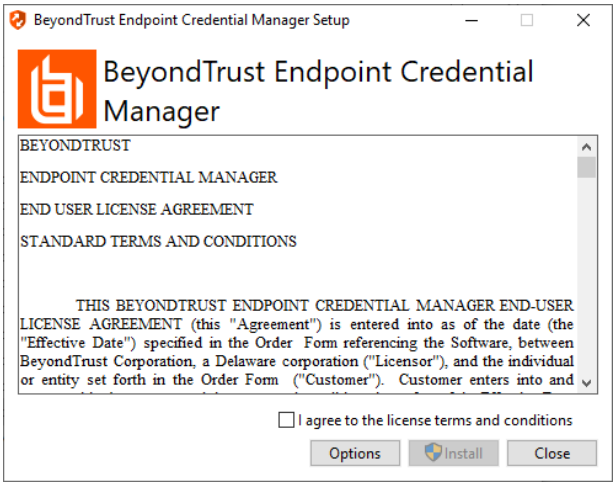
Voordat u kunt beginnen met Jumpitems openen met behulp van inloggegevensinjectie, moet u de BeyondTrust Endpoint Credential Manager (ECM) downloaden, installeren en configureren. Met BeyondTrust ECM kunt u uw verbinding met een inloggegevensopslag, zoals een wachtwoordkluis, snel configureren.

> ***Opmerking:*** *De ECM moet op uw netwerk zijn geïnstalleerd om de BeyondTrust ECM Service in te schakelen en inloggegevensinjectie in BeyondTrust PRA te gebruiken.*

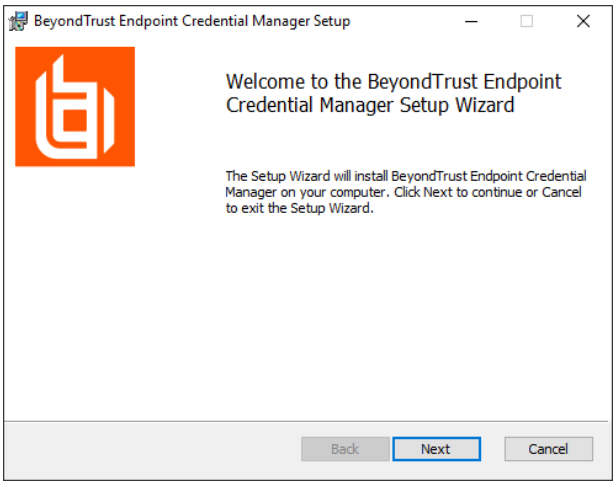
1. Download om te beginnen de BeyondTrust Endpoint Credential Manager (ECM) van BeyondTrust-ondersteuning op beyondtrustcorp.service-now.com/csm.
2. Start de installatiewizard voor BeyondTrust Endpoint Credential Manager.
3. Ga akkoord met de algemene voorwaarden uit de Gebruiksrechtovereenkomst. Schakel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

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

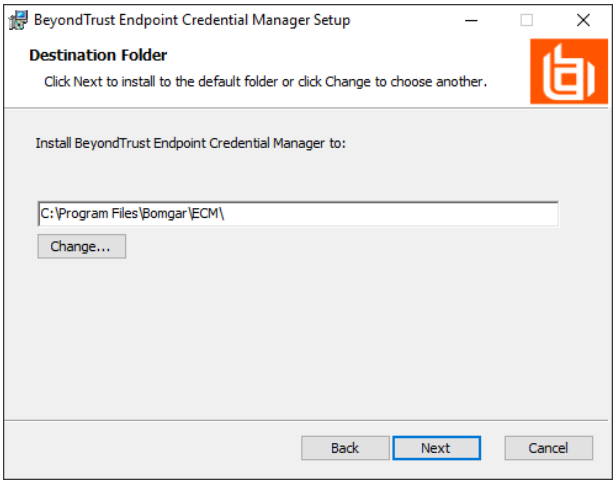
> ***Opmerking:*** *U kunt niet doorgaan met de installatie tenzij u akkoord gaat met de Gebruiksrechtovereenkomst.*



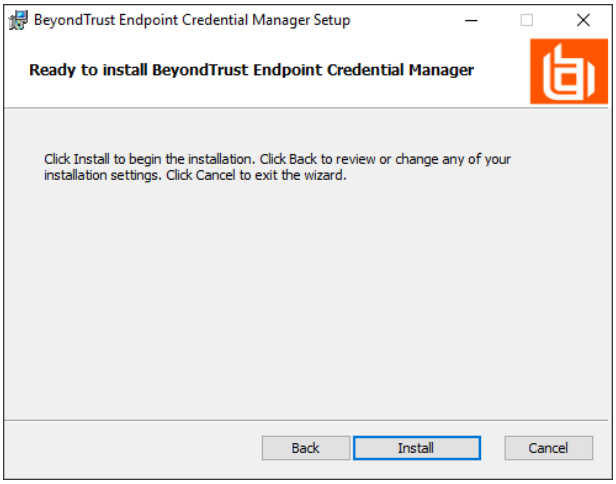
4. Klik op **Volgende** op het welkomstscherm.



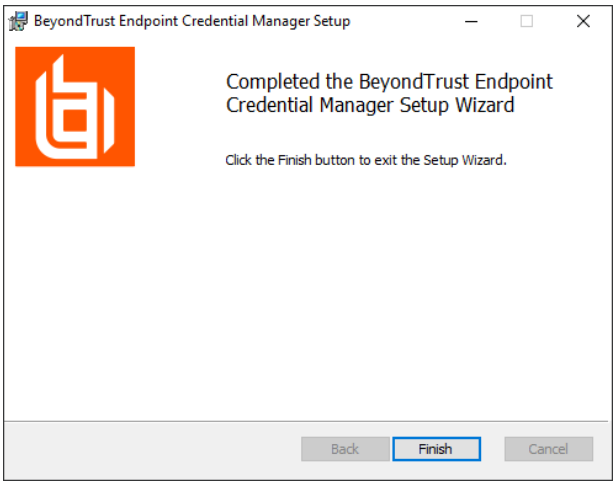
5. Kies een locatie voor de inloggegevensopslag en klik op **Volgende**.
6. In het volgende scherm kunt u de installatie beginnen of een voorgaande stap nog eens bekijken.



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



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

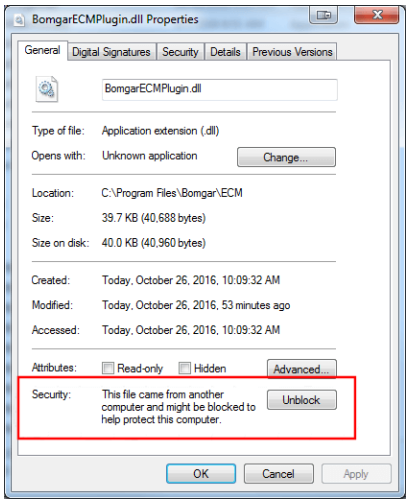


Opmerking: *Om optimale up-time te waarborgen, kunnen beheerders maximaal drie ECM's op verschillende Windows-systemen installeren om met dezelfde inloggegevensopslag te communiceren. Een lijst met de ECM's die met het apparaat verbonden zijn, is te vinden op* ***/login > Status > Informatie > ECM-clients****.*

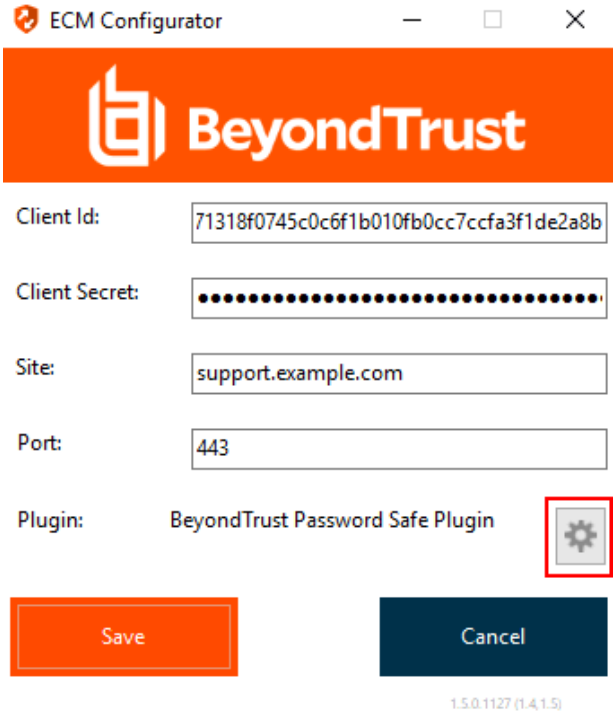
Opmerking: *Als er meerdere ECM's in een configuratie met hoge beschikbaarheid zijn verbonden, stuurt de BeyondTrust Appliance B Series verzoeken naar de ECM in de ECM-groep die het langst met het apparaat is verbonden.*

De plugin installeren en configureren

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



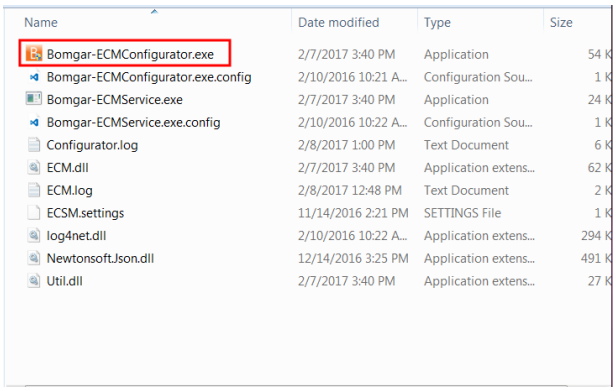
4. Klik op het pictogram met het tandwieltje in het venster van de **Configurator** om de instellingen voor de plug-in te configureren.



Een verbinding met uw inloggegevensopslag configureren

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

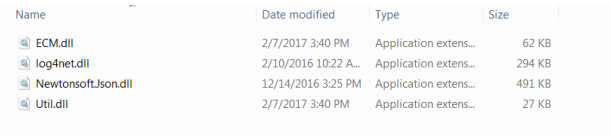
1. Zoek de BeyondTrust ECM Configurator die u zojuist hebt geïnstalleerd via Windows zoeken of via het invoerveld in de programmalijst in het menu **Start**.
2. Voer het programma uit om een verbinding te maken.
3. Vul de velden in wanneer de ECM Configurator opent. Alle velden zijn verplicht.



Vul de volgende waarden in:

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

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

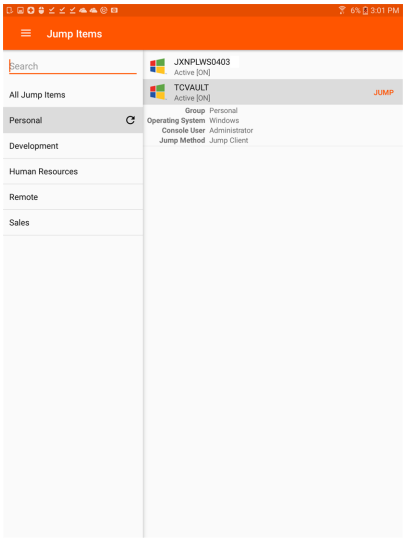


Opmerking: *Als u verbinding maakt met een wachtwoordkluis, zijn wellicht meer configuraties op plugin-niveau nodig. De pluginvereisten kunnen verschillen per inloggegevensopslag waarmee verbinding wordt gemaakt.*

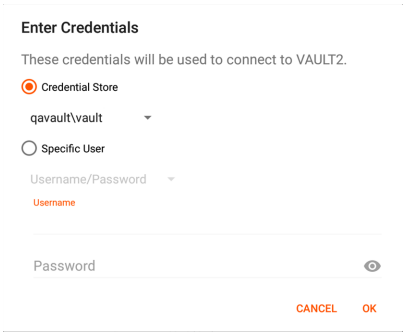
Inloggegevensinjectie gebruiken voor toegang tot eindpunten

Nadat de inloggegevensopslag is geconfigureerd en er een verbinding is gemaakt, kan BeyondTrust PRA de inloggegevens in de opslagplaats gaan gebruiken om bij eindpunten in te loggen.

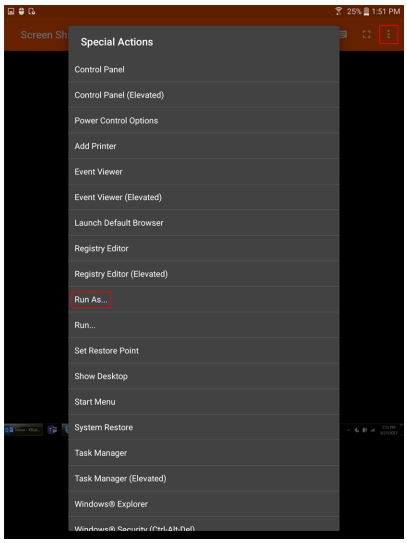
1. Ga naar uw lijst met **Jumpitems**.
2. Tik op het Jumpitem waar u toegang toe wilt hebben.
3. Tik op **Jump**.



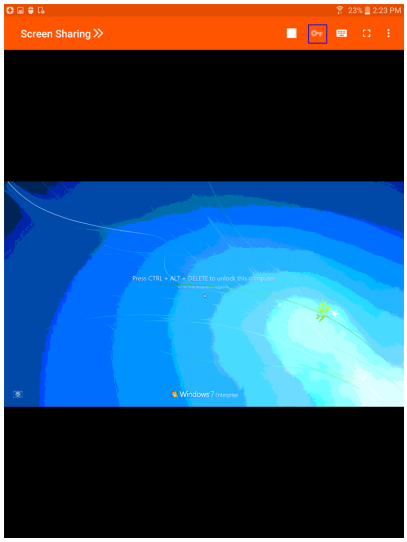
4. De melding **Voer inloggegevens in** verschijnt. Tik op **Opslagplaats voor inloggegevens**.
5. Tik op de inloggegevens die u wilt gebruiken voor toegang tot het systeem.
6. Tik op **OK**.



7. Tik vanuit de sessie op **Start** om te beginnen met scherm delen.
8. Tik op de optie **Speciale acties**. Tik op **Uitvoeren als...**.
9. Tik op **Windows-beveiliging (Ctrl-Alt-Del)**.

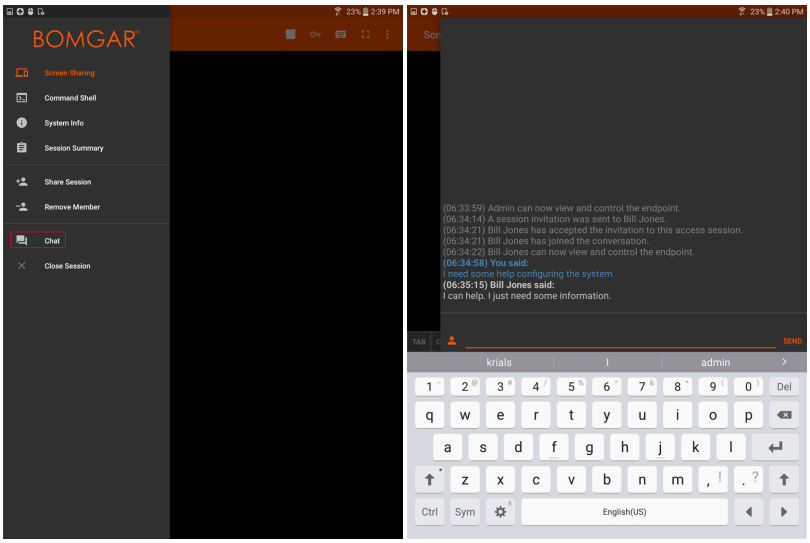


10. Tik op het symbool met de **Sleutel**. Via het sleutelpictogram kan het systeem uw opgeslagen inloggegevens weergeven om toegang te verkrijgen tot het eindpunt.



Teamchat gebruiken om in de Android-toegangsconsole met andere gebruikers te chatten

U kunt met andere ingelogde teamleden chatten door op de optie **Chat** te tikken. Als u lid bent van een of meer teams, dan kunt u uit de lijst een willekeurig team selecteren om mee te chatten. U kunt met alle leden van dat team chatten of een naam uit de lijst selecteren om alleen met dat ene lid te chatten.

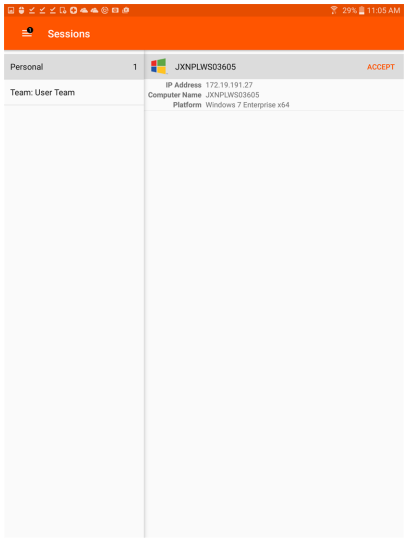


Toegangssessies in de Android-toegangsconsole bekijken

Actieve toegangssessies zijn binnen de toegangsconsole onderverdeeld in teamwachtrijen. Als u in het menu op de optie **Sessies** tikt, verschijnt er een overzicht met alle geconfigureerde wachtrijen. Deze wachtrijen tonen de teams die in de /login-beheerinterface zijn ingesteld. Nadat een team is gedefinieerd, komt een wachtrij beschikbaar in de sectie **Sessies** van de toegangsconsole.

De **Persoonlijke** wachtrij bevat sessies die door een ander teamlid specifiek met u zijn gedeeld. De overige wachtrijen zijn voor specifieke teams waar u lid van bent.

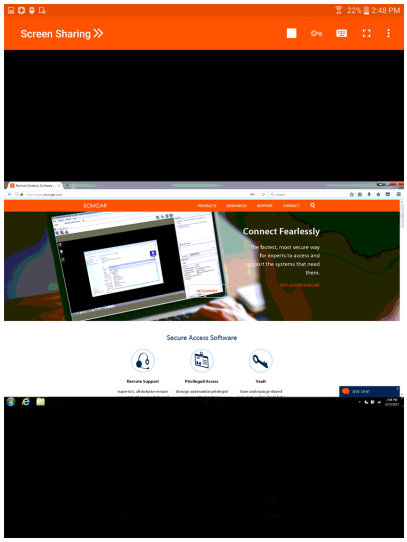
Tik op de naam van de wachtrij om sessies te zien die in uitvoering zijn. Het getal naast de Sessie-optie geeft aan hoeveel sessies er in die wachtrij in uitvoering zijn.



Opmerking: *Als er een sessie met u wordt gedeeld, dan kunt u op de wachtrij tikken waar de sessie binnen valt. Tik vervolgens op de sessie. Selecteer* ***Accepteren****. Als u een sessie accepteert, wordt deze op uw apparaat geopend.*

Scherm delen met het eindpunt vanaf de Android-toegangsconsole

Tik op de knop **Afspelen** boven aan de pagina **Scherm delen** om toegang te vragen om het externe systeem weer te geven en te beheren als het scherm niet automatisch wordt gedeeld. U kunt de muis en het toetsenbord van het externe systeem gebruiken, zodat u op de externe computer kunt werken alsof u erachter zit.

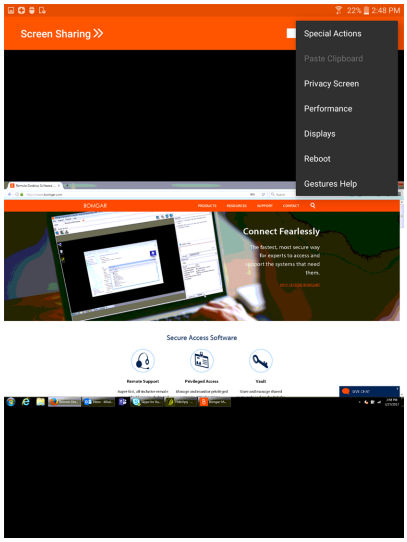


- Tik eenmaal om links te klikken.
- Dubbeltik om te dubbelklikken.
- Zet uw vinger op de cursor of sleep deze om met de muis te navigeren.
- Dubbeltik op een object, sleep het en zet het neer.
- Knijp om het externe scherm op schaal of op volle resolutie te bekijken. U zoomt door uw vingers ergens te plaatsen, onafhankelijk van de huidige locatie van de muisaanwijzer.
- Tik met twee vingers om rechts te klikken.
- Draai aan het muiswiel door met drie vingers te slepen.
- Tik met drie vingers om het toetsenbord om te schakelen.
- Tik met uw vinger en houd die op dezelfde plaats om de cursor te vinden.

Hulpmiddelen voor scherm delen

Scherm delen	Verzoek tot of stop met scherm delen.
Help	Bekijk de extra acties die beschikbaar zijn als het scherm is gedeeld.
Toetsenbord	Krijg toegang tot het toetsenbord om op het externe scherm te typen.
Opties	Selecteer uit de extra acties en hulpmiddelen voor scherm delen.
Volledig scherm	Bekijk het externe bureaublad als volledig scherm.

Extra acties en hulpmiddelen voor scherm delen



Speciale acties: Voer een speciale actie op het externe systeem uit. De beschikbare mogelijkheden zijn afhankelijk van het externe besturingssysteem en de configuratie.

Kopiëren naar klembord: Kopieer items naar het klembord van uw apparaat.

Privacyscherm: Schakel de schermweergave, de muis en de toetsenbordinvoer uit voor de externe gebruiker. 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.

Prestaties: 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.

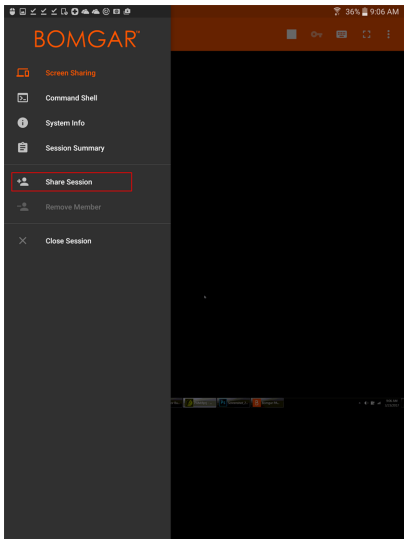
Beeldschermen: Selecteer een alternatief beeldscherm op de externe computer om weer te geven. Het primaire beeldscherm is geaccentueerd.

Opnieuw opstarten: Tik om het externe systeem opnieuw op te starten.

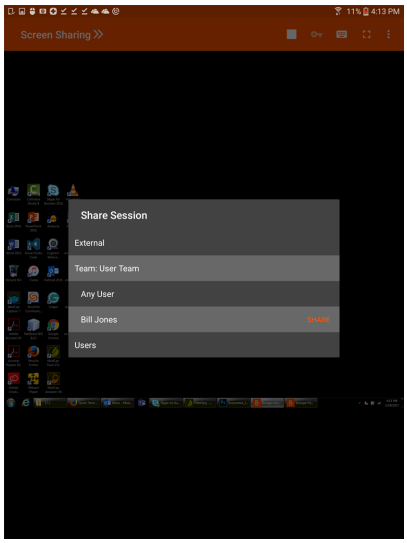
Hulp voor gebaren: Tik om navigatietips te ontvangen voor de mobiele toegangsconsole.

Een sessie met andere gebruikers delen vanaf de Android-toegangsconsole

Om een sessie met een ander teamlid te delen, tikt u op de optie **Sessie delen** in het menu.



U kunt een gebruiker selecteren uit de lijst met teams om uit te nodigen om de sessie bij te wonen. U kunt meerdere uitnodigingen verzenden als u wilt dat meerdere teamleden de sessie bijwonen. Gebruikers worden hier alleen vermeld als zij bij de toegangsconsole zijn ingelogd of als voor hen uitgebreide beschikbaarheid is ingeschakeld.



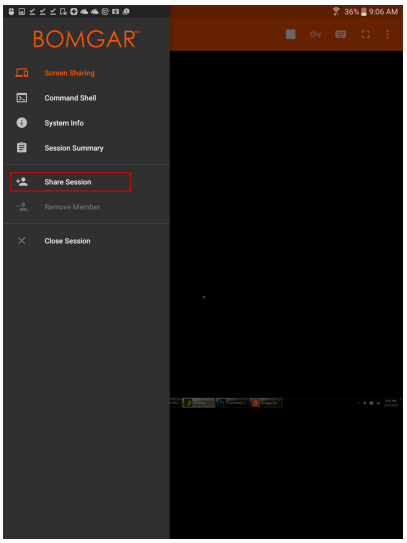
Als u bent gemachtigd om sessies te delen met gebruikers die geen lid van uw teams zijn, worden er extra teams weergegeven, mits deze ten minste één lid bevatten dat bij de toegangsconsole is ingelogd of waarvoor uitgebreide beschikbaarheid is ingeschakeld.

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

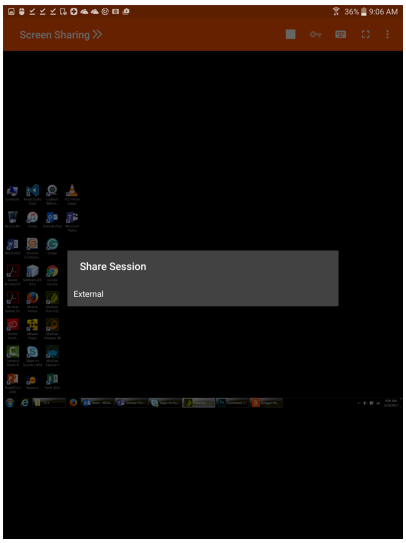
- De uitnodigende gebruiker de uitnodiging annuleert.
- De uitnodigende gebruiker de sessie verlaat.
- De sessie stopt.
- De uitgenodigde gebruiker de uitnodiging aanvaardt.

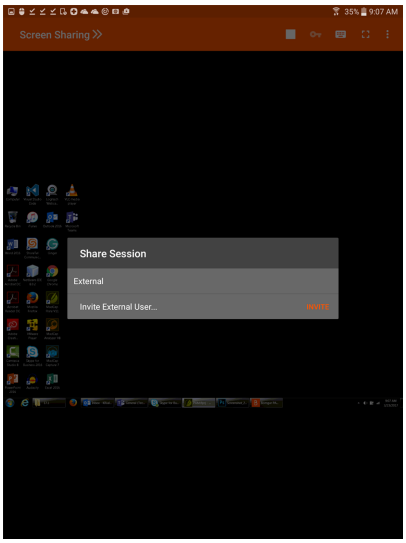
Een externe gebruiker vanuit de Android-toegangsconsole uitnodigen om een sessie bij te wonen

Een gebruiker kan in een sessie een externe gebruiker uitnodigen eenmalig aan een sessie deel te nemen. De uitnodigende gebruiker moet op het uitklapmenu tikken en het menu **Sessie delen** selecteren.



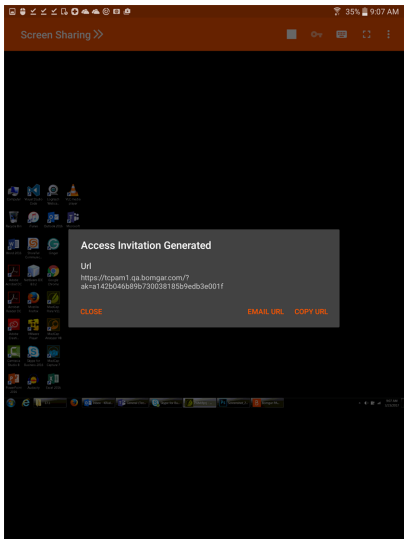
Selecteer **Extern** en vervolgens **Externe gebruiker uitnodigen**. Tik op de knop **Uitnodigen** om verder te gaan.





Selecteer vervolgens een beveiligingsbeleid. Deze beleidslijnen worden in de beheerinterface aangemaakt en bepalen het machtigingsniveau voor de externe gebruiker. Als u een beleid selecteert, wordt de volledige omschrijving van het beleid eronder weergegeven.

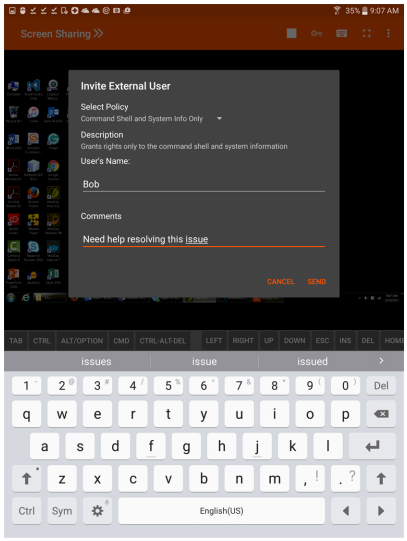
Voer de naam van de externe gebruiker in. Deze naam verschijnt in het chatvenster en in rapporten. Voer vervolgens opmerkingen in om aan te geven waarom u deze gebruiker uitnodigt. Klik op **Verzenden**, waarna een nieuw dialoogvenster verschijnt met de URL voor de uitnodiging.



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.

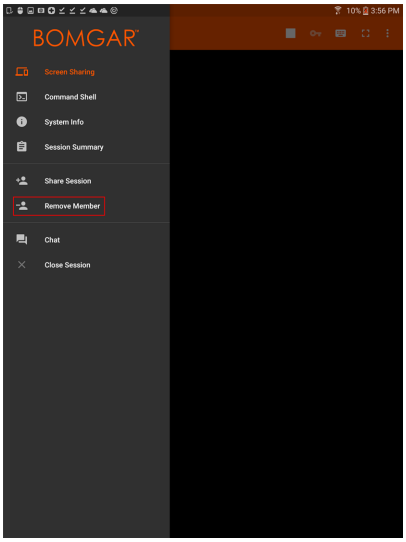
De externe gebruiker heeft alleen toegang tot het tabblad **Sessie** en heeft beperkte machtigingen. De externe gebruiker kan nooit de eigenaar van de sessie zijn. Als de uitnodigende gebruiker de sessie verlaat, dan wordt de externe gebruiker uitgelogd.

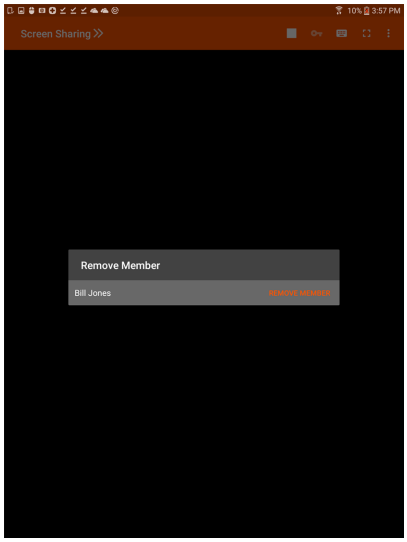
U kunt meerdere externe gebruikers voor een sessie uitnodigen.



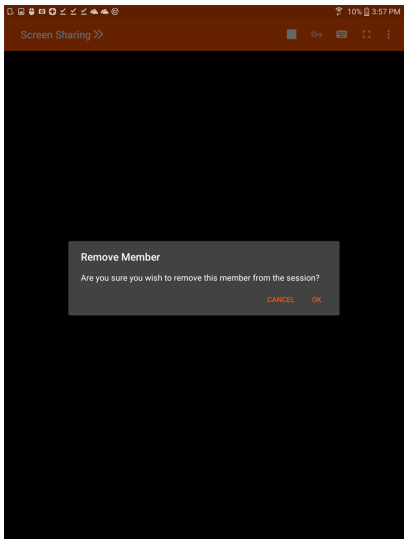
In de Android-toegangsconsole een lid van de sessie verwijderen

U kunt een andere gebruiker van een gedeelde sessie verwijderen. Tik op de optie **Lid verwijderen** in het menu.





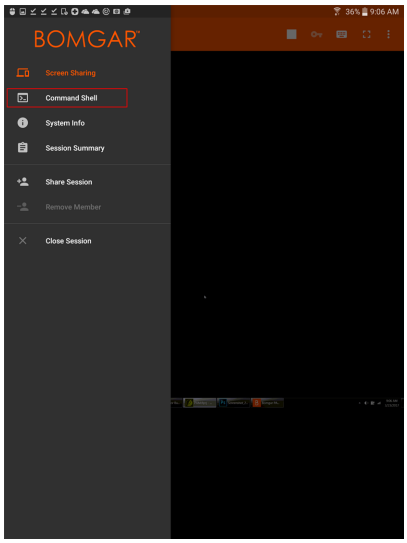
Selecteer de deelnemer die u wilt verwijderen. Tik vervolgens op **Verwijderen**. Tik in de volgende melding op **OK**. U moet de eigenaar van de sessie zijn om een ander lid te mogen verwijderen.



Open de opdrachtshell op een extern eindpunt met behulp van de Android-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.

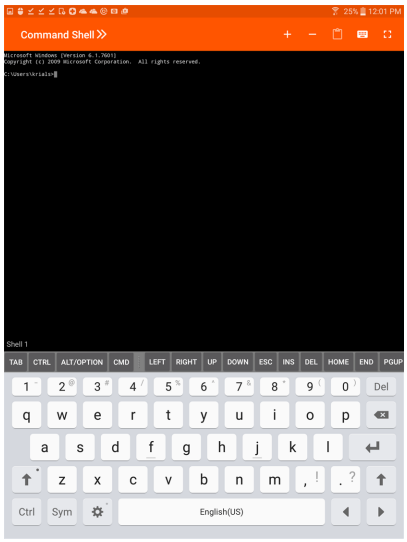
Selecteer **Opdrachtshell** in het menu om de opdrachtshell te openen. Tik op het pictogram **+** om een nieuwe shell te openen.



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.

Er zijn extra keyboardopdrachten en -tekens beschikbaar boven het standaardkeyboard. Er zijn verschillende extra toetsen die u naar links en rechts kunt vegen voor meer opties.

Indien er meerdere opdrachtshells geopend zijn, kunt u de opdrachtshell naar links en rechts vegen om te wisselen tussen de open shells. De naam van de huidige shell wordt getoond in de hoek linksonder in het shellscherm.

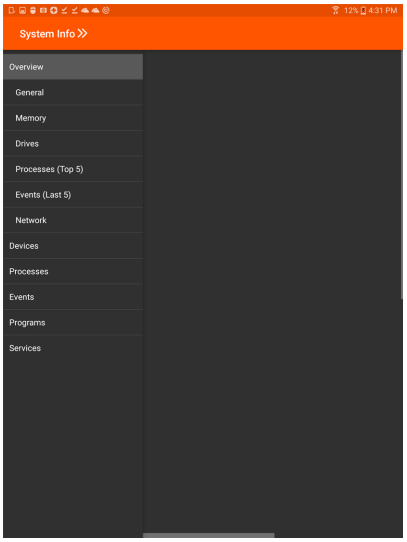


Ondersteuningsgereedschappen opdrachtshell

	Open een nieuwe shell om meerdere opdrachtregels uit te voeren.
	Sluit de huidige opdrachtshell. Overige geopende opdrachtshells blijven actief.
	Krijg toegang tot het toetsenbord om opdrachten in de opdrachtshell te typen.
	Ga naar het opdrachtshellmenu om extra acties uit te voeren, zoals andere shellsessies bekijken of naar volledig scherm overschakelen.

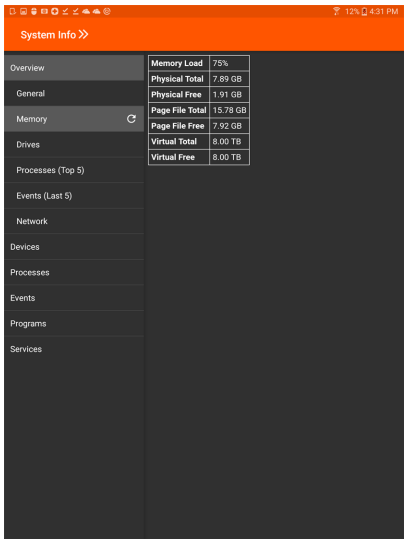
Systeeminformatie over een eindpunt bekijken vanaf de Android-toegangsconsole

Gebruikers kunnen een complete momentopname van de systeeminformatie van het eindpunt bekijken om de voor het onderzoeken en oplossen van het probleem benodigde tijd te beperken. De beschikbare systeeminformatie hangt van het externe besturingssysteem en de configuratie af.



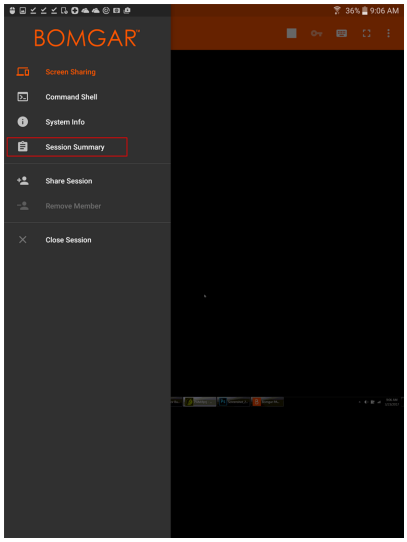
Selecteer de verschillende categorienamen waarvan u de gegevens wilt bekijken.

Als de gegevens eenmaal zijn ingevuld, kunt u op de knop **Vernieuwen** tikken om de allerlaatste gegevens op te halen.



Op de Android-toegangsconsole een overzicht van de gegevens over de technische ondersteuningssessie bekijken en opmerkingen toevoegen

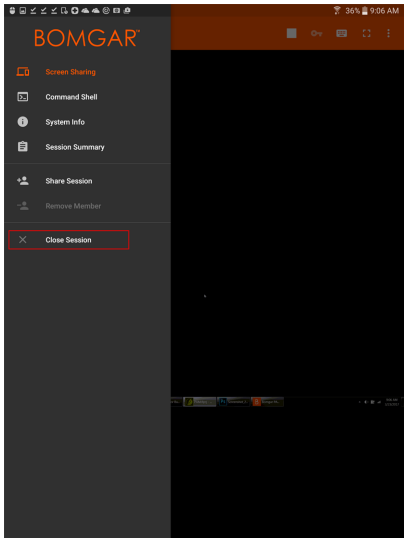
Op de pagina **Samenvatting** staat een overzicht van het externe systeem waar u op dat moment toegang toe hebt.



U kunt ook opmerkingen over de sessie toevoegen door naar links over het scherm te vegen. Opmerkingen kunnen door de ene gebruiker worden toegevoegd en door een andere gebruiker worden opgevraagd om te bekijken. Deze opmerkingen zijn ook beschikbaar in het sessierapport.

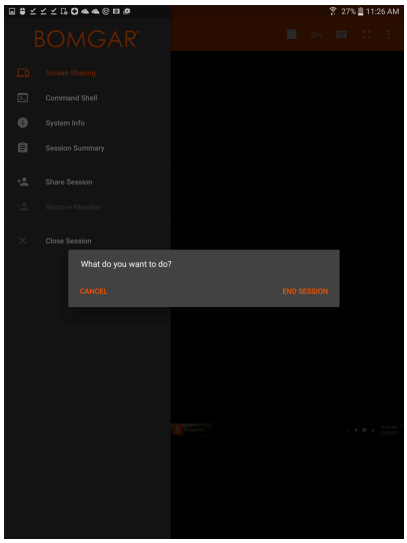
In de Android-toegangsconsole de sessie sluiten

U kunt een sessie afsluiten door in het menu op **Sessie sluiten** te tikken.



Als u de eigenaar van de sessie bent, dan wordt door de actie **Sessie beëindigen** de sessiepagina in uw toegangsconsole afgesloten en worden eventuele extra leden die de sessie delen, verwijderd.

Als u niet de eigenaar van de sessie bent, wordt u wanneer u op **Sessie verlaten** tikt van de sessie verwijderd. De sessie wordt verder door de eigenaar van de sessie ondersteund. Eventuele extra leden die de sessie deelden, blijven in de sessie.



De Toegangsconsole-app beheren en implementeren met behulp van Intune

Deze instructies zijn gebaseerd op de documentatie van Microsoft voor het gebruiken van Intune om Android-apparaten te beheren.

Volg de onderstaande stappen om een configuratiebeleid voor de app te maken.

1. Meld u aan bij het Microsoft Intune-beheercentrum op https://intune.microsoft.com/.
2. Ga naar **Apps > App-configuratiebeleid > Toevoegen > Beheerde apparaten**.
3. Stel op de pagina **Basisinstellingen** de volgende gegevens in:
    - **Naam**: De naam van het profiel dat in het portaal wordt weergegeven.
    - **Beschrijving**: De beschrijving van het profiel dat in het portaal wordt weergegeven.
    - **Type apparaatinschrijving**: Het type apparaat. Laat op de standaardinstelling, Beheerde apparaten.
4. Selecteer **Android Enterprise** als het **Platform**.
5. Klik op **App selecteren** naast **Doel-app**. Het deelvenster **Gekoppelde app** wordt weergegeven.
6. Kies in het deelvenster **Gekoppelde app** de BeyondTrust-app Support of Support+ om deze aan het configuratiebeleid te koppelen en klik op **OK**.
7. Klik op **Volgende** om de pagina **Instellingen** weer te geven.
8. Klik op **Toevoegen** om het deelvenster **Machtigingen toevoegen** weer te geven.
9. Klik op de machtigingen die u wilt overschrijven. De app vraagt om de volgende machtigingen. We adviseren om Automatisch verlenen in te schakelen:
    - READ_PHONE_STATE
    - READ_CONTACTS
    - GET_ACCOUNTS
    - CAMERA
    - WRITE_EXTERNAL_STORAGE
    - READ_EXTERNAL_STORAGE
10. Desgewenst kan ook het standaardgedrag voor het ondersteuningsportaal worden geconfigureerd in de vervolgkeuzelijst **Indeling van configuratie-instellingen**. Selecteer **Configuratie-ontwerper gebruiken**.
11. Klik op **Toevoegen**. Voeg waarden toe voor elke configuratie-instelling en wijs deze toe overeenkomstig de beschrijvingen.
12. Klik op **Volgende** om de pagina **Toewijzingen** weer te geven.
13. Selecteer in het vervolgkeuzevenster naast **Toewijzen aan** de optie **Groepen toevoegen**, **Alle gebruikers toevoegen** of **Alle apparaten toevoegen** om het configuratiebeleid voor de app toe te wijzen. Nadat u een toewijzingsgroep hebt geselecteerd, kunt u een filter selecteren om de omvang van de toewijzing te verfijnen tijdens het implementeren van app-configuratiebeleid voor beheerde apparaten.
14. Klik op **Volgende** om de pagina **Controleren en maken** weer te geven.
15. Klik op **Maken** om het app-configuratiebeleid toe te voegen aan Intune.

Raadpleeg App-configuratiebeleid toevoegen voor beheerde Android Enterprise-apparaten op https://learn.microsoft.com/nl-nl/mem/intune/apps/app-configuration-policies-use-android voor meer informatie.