BeyondTrust

Privileged Remote Access
iOS-toegangsconsole 2.2.4

TC:7/26/2021

Inhoudsopgave

Gids voor de toegangsconsole voor iOS

Deze gids is bedoeld om u te helpen bij het installeren van de BeyondTrust op uw iOS-apparaat en om de functies van de BeyondTrust voor iOS te begrijpen. B Series Appliance stelt u in staat om toegang te krijgen tot externe eindpunten door een verbinding op te zetten via de access console.

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

Toegangsconsole op iOS installeren

De BeyondTrust access console voor iOS kan gratis worden gedownload in de Apple App Store. Zoek in de App Store op uw iOS-apparaat naar 'BeyondTrust Access Console' en installeer de app vervolgens.

Als uw bedrijf een Enterprise App Store gebruikt om apps te distribueren, moet u contact met opnemen met BeyondTrust Technical Support om de BeyondTrust access console-app via uw Enterprise App Store beschikbaar te maken.

Om de BeyondTrust access console op uw apparaat te kunnen uitvoeren, moet uw BeyondTrust minimaal softwareversie 15.2 bevatten. Het iOS-apparaat moet minimaal iOS 7 bevatten.

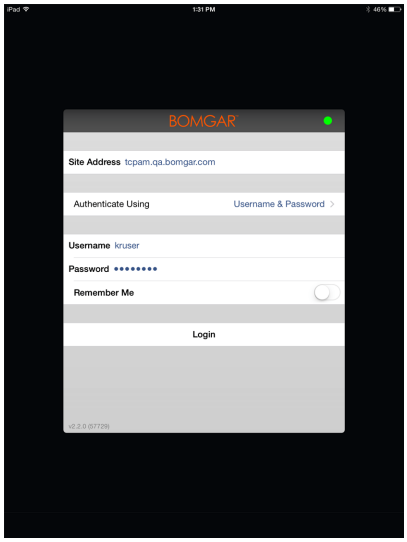
Opmerking: *Alleen de BeyondTrust access console kan worden gebruikt met een Privileged Remote Access-site met (PRA). De BeyondTrust-console voor ondersteuningstechnici kan niet worden gebruikt om verbinding met een PRA-site te maken en de BeyondTrust-access console kan niet worden gebruikt om verbinding 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 iOS-access console. Neem contact op met B Series Appliance Technical Support nadat u een door een CA ondertekend SSL-certificaat op uw BeyondTrust hebt toegepast. Uw klantendiensttechnicus stelt dan een nieuw softwarepakket samen waarin uw SSL-certificaat is geïntegreerd. U kunt met de bijgewerkte build nadat deze geïnstalleerd is op uw B Series Appliance de BeyondTrust access console op uw apparaat uitvoeren om vanaf vrijwel elke willekeurige plaats toegang tot eindpunten te krijgen.

Inloggen op de toegangsconsole voor iOS

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



> ***Opmerking:*** *Uw beheerder kan vereisen dat u op een toegestaan netwerk bent om op de console in te kunnen loggen. Deze netwerkbeperking geldt mogelijk alleen de eerste keer dat u inlogt of elke keer. Deze beperking is niet van toepassing op toegangsuitnodigingen.*

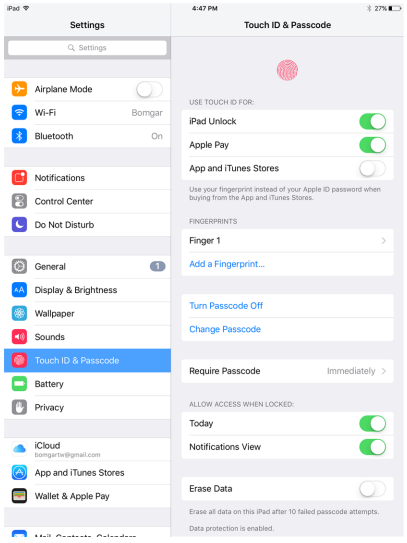
Als u door een andere gebruiker bent uitgenodigd om eenmalig een toegangssessie bij te wonen, moet u op **Verificatie met behulp van** en **Code voor toegangsuitnodiging** tikken.

Voer de code in van de toegangsuitnodiging die u hebt ontvangen en tik vervolgens op **Inloggen**.

Inloggen bij de BeyondTrust Privileged Remote Access-console voor iOS met gebruik van Touch ID

Touch ID is een vingerafdrukidentiteitssensor die in de volgende iOS apparaten aanwezig is:

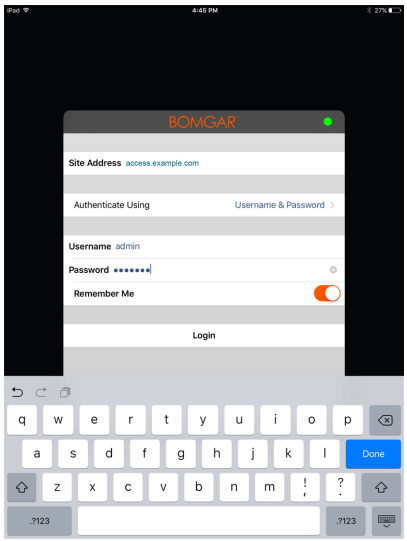
- **iPhone 5s of nieuwer**
- **iPad Pro**
- **iPad Air 2**
- **iPad Mini 3 of nieuwer**



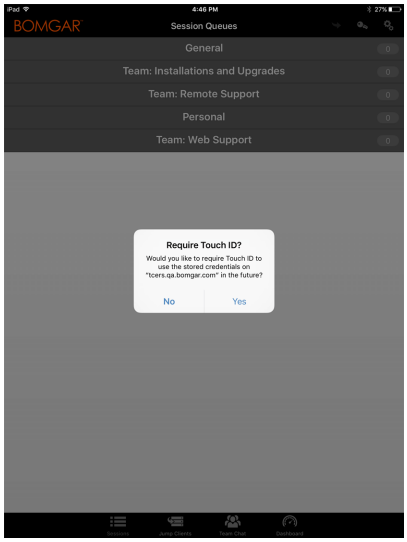
Met deze functie kunt u uw apparaat ontgrendelen of andere acties verifiëren vanaf uw iPhone of iPad met gebruik van uw vingerafdruk als toegangscode. Voor meer informatie over Touch ID en hoe u dit voor uw apparaat kunt inschakelen, gaat u naar Over Touch ID-beveiliging op iPhone en iPad op https://support.apple.com/en-us/HT204587 en Touch ID gebruiken op iPhone en iPad op https://support.apple.com/en-us/HT201371.

Vanaf BeyondTrust Privileged Remote Access 16.1 kunt u Touch ID gebruiken om in te loggen op de mobiele access console voor iOS. Dezelfde vingerafdrukverificatie die u gebruikt om uw apparaat te ontgrendelen kunt u ook gebruiken om toegang te krijgen tot uw access console. Volg de onderstaande stappen om Touch ID-verificatie voor uw mobiele access console in te schakelen.

1. Open de BeyondTrust mobiele access console-app.
2. Voer uw inloggegevens en de hostnaam van uw BeyondTrust-site in, bijvoorbeeld access.example.com.
3. Controleer of de optie **Mij herinneren** is ingeschakeld. Klik op **Inloggen**.



4. Tik op **Ja** op de Touch ID-prompt die bij het inloggen verschijnt.
5. Uitloggen bij de access console.



6. Tik op de optie **Inloggen met Touch ID** die verschijnt op het inlogscherm.
7. Plaats uw vinger op de knop **Home** op uw apparaat om het aanmelden bij de console van ondersteuningstechnicus te voltooien.

> ***Opmerking:*** *U kunt zich op elk gewenst moment aanmelden met uw gebruikersnaam en wachtwoord door te tikken op de optie* ***Terug naar inloggen****.*

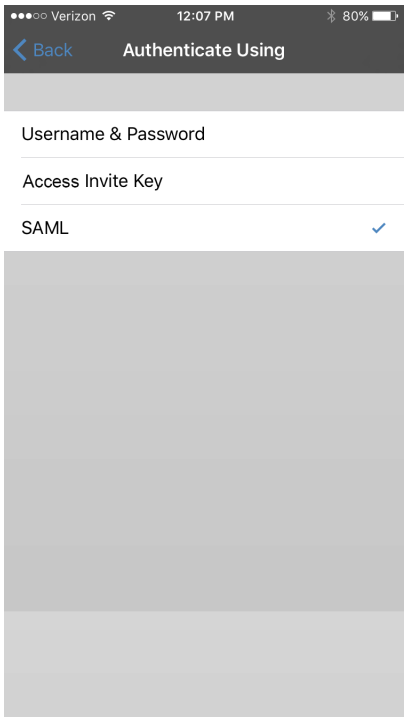
Inloggen bij de iOS-toegangsconsole met SAML voor mobiel

SAML voor mobiel is een eenvoudige en veilige verificatiemethode voor de iOS-access console. 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 met SAML bij de mobiele access console in te loggen.

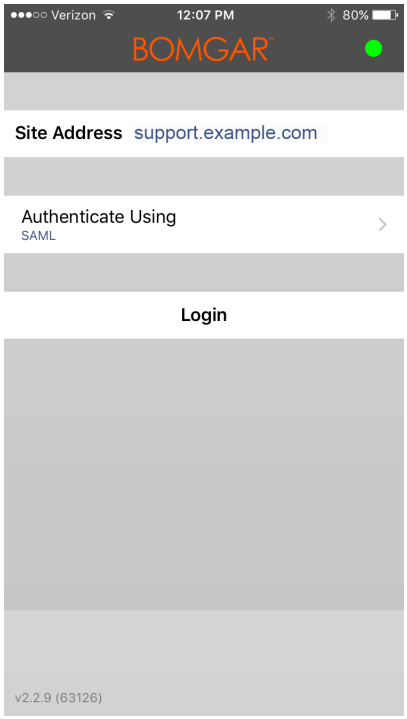
> ***Opmerking:*** *Voordat u met SAML bij de iOS-access console probeert in te loggen, moet u eerst controleren of een SAML-provider is geconfigureerd voor uw /login administratieve omgeving door naar* ***Gebruikers en beveiliging > Beveiligingsproviders*** *te gaan. Als SAML niet in /login is geconfigureerd, is SAML niet beschikbaar als verificatiemethode voor de iOS-access console. 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 access console-app op uw iOS-apparaat.
2. Op het inlogscherm tikt u op **Verificatie met behulp van**.

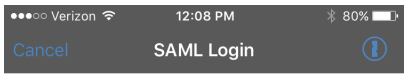
3. Selecteer **SAML**.



4. Tik op **Inloggen**. De pagina van uw SAML-provider verschijnt nu.

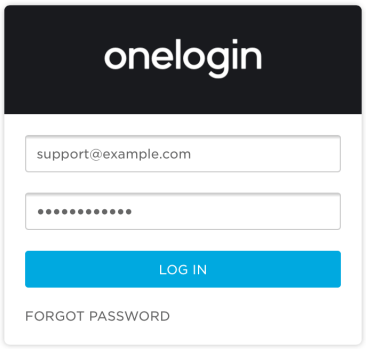


5. Voer op de pagina van de provider uw inloggegevens in.



> ***Opmerking:*** *Als u op uw apparaat een wachtwoordkluis hebt geconfigureerd, kunt u op het hangslotsymbool in de rechterbovenhoek tikken voor toegang tot uw wachtwoordkluis en uw inloggegevens.*

6. Tik op **Inloggen** om toegang tot de console te krijgen.

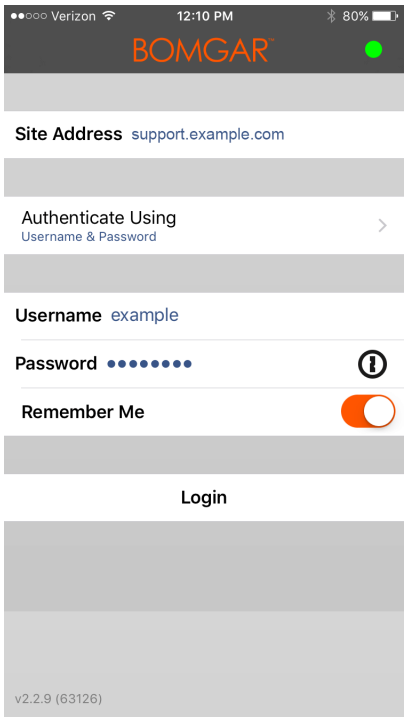


Inloggen bij de iOS-toegangsconsole met een wachtwoordmanager

Wachtwoordmanagers zoals 1Password en LastPass zijn een eenvoudige manier om uw wachtwoorden veilig en vertrouwelijk te bewaren. Lees voor meer informatie over de bedrijfseigen extensie 1Password Security is not just a feature. It's our foundation. op https://1password.com/security/. Volg de onderstaande stappen om 1Password of een andere wachtwoordmanager te gebruiken voor de iOS-toegangsconsole van BeyondTrust.

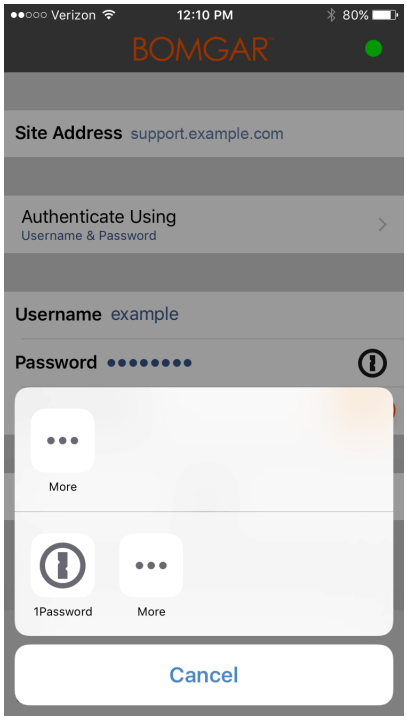
> ***Opmerking:*** *Voordat u een wachtwoordmanager met de BeyondTrust iOS-toegangsconsole gebruikt, moet u controleren of u een account hebt geconfigureerd met de wachtwoordmanager en of de app met uw apparaat is gesynchroniseerd.*

1. Open de toegangsconsole-app op uw iOS-apparaat.
2. Tik op het hangslotsymbool in het veld **Wachtwoord**.

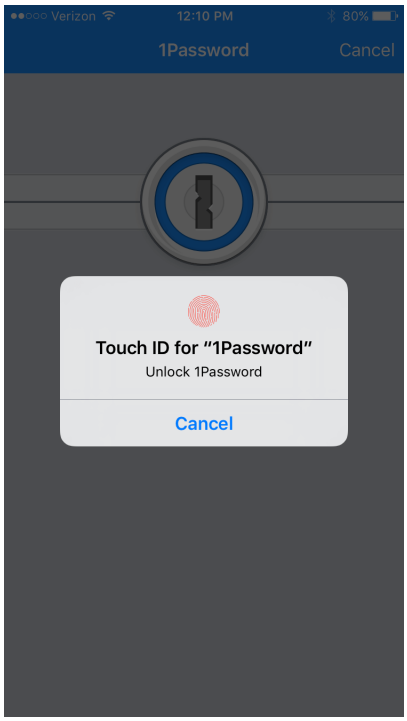


3. Kies de wachtwoordmanager die u wilt gebruiken. U wordt doorverwezen naar de inlogpagina van de wachtwoordmanager.

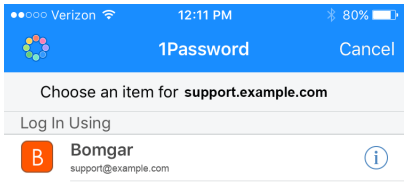
> ***Opmerking:*** *Als de wachtwoordmanager niet op het apparaat is geconfigureerd, ziet u geen hangslotsymbool.*



4. Als TouchID is ingeschakeld, kunt u uw vingerafdruk gebruiken als verificatie om de toepassing op uw computer te openen. Als TouchID niet is ingeschakeld, moet u uw wachtwoord invoeren.



5. Nadat u hebt ingelogd, geeft de wachtwoordmanager een lijst van accounts weer met toegang tot de console. Tik op het account dat u wilt gebruiken voor toegang tot de console.

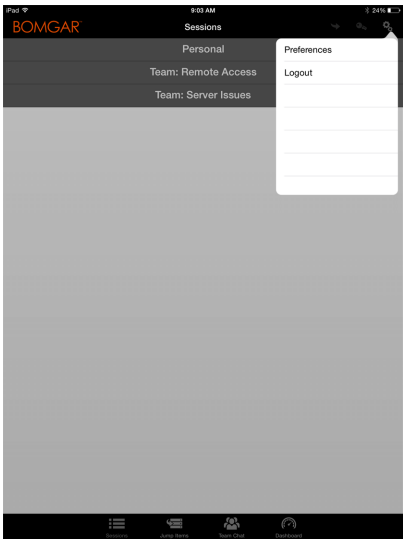


Voorkeuren in het iOS-toegangsconsole instellen

Om uw voorkeuren op een iPad te wijzigen, moet u op het symbool **Tandwiel** rechtsboven in het scherm tikken.

Om uw voorkeuren op een iPhone te wijzigen, moet u op het symbool **Menu** rechtsboven in het scherm tikken.

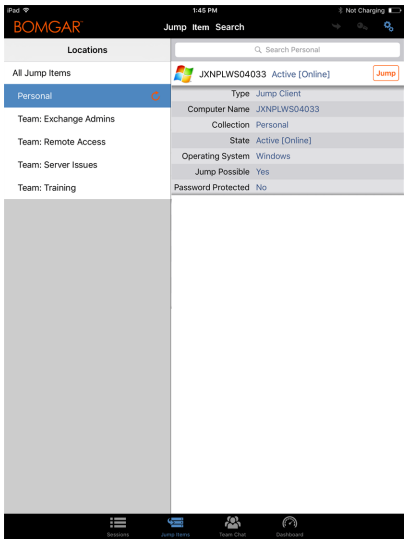
Tik vervolgens op **Voorkeuren**.



Hoorbare waarschuwingen	iPad en iPhone	Als deze optie is ingeschakeld, krijgt u audio-waarschuwingen voor bepaalde gebeurtenissen binnen de access console.
Absolute muisaanwijzer	iPad en iPhone	Als deze optie is uitgeschakeld, dan moet u uw vinger op de muisaanwijzer zetten en hiermee slepen om de muis te verplaatsen. Tik met uw vinger en houd die op dezelfde plaats om de muisaanwijzer te vinden als absolute positie is uitgeschakeld. Als deze optie is ingeschakeld, dan kunt u de muisaanwijzer plaatsen waar u maar met uw vinger het scherm aanraakt. Als absolute positie is ingeschakeld, dan kunt u met uw vinger tikken en die op dezelfde plaats houden om een uitklapmenu te openen waar u uit verschillende methodes om te klikken kunt kiezen.
Het apparaat schudden voor help bij het bekijken van een sessie	Alleen iPad	Als deze optie is ingeschakeld, dan kunt u het apparaat schudden om de gids Gebaren voor scherm delen te openen terwijl u in een toegangssessie bent.

Jumpitems gebruiken voor toegang tot eindpunten vanaf de iOS-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. De volgende typen Jumpitems worden door de mobiele access console ondersteund:



- **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 het tabblad **Jumpitems** bovenaan het scherm.

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.

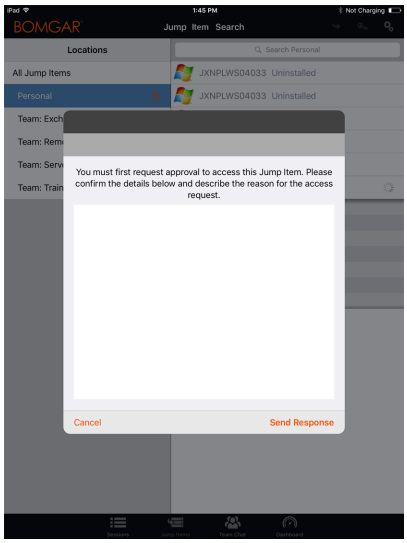
Afhankelijk van de machtigingen die uw beheerder voor uw account heeft ingesteld, kan een eindgebruiker of derde worden gevraagd om de sessie toe te staan of te weigeren. Als er binnen een bepaald interval geen antwoord is ontvangen, dan start de sessie of wordt deze geannuleerd, afhankelijk van de instellingen in uw account.

Autorisatie door eindgebruiker of derden

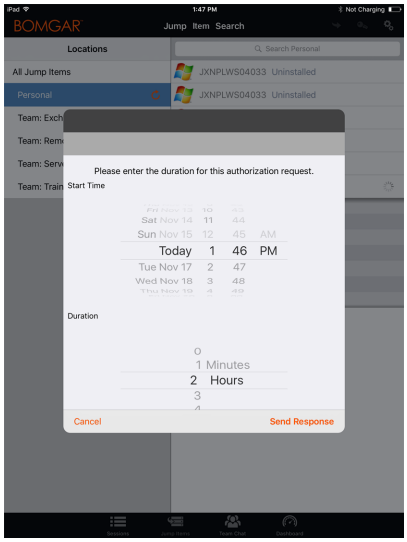
Afhankelijk van de configuratie van Jumpitems binnen de /login-beheerinterface kan er aan een Jumpitem een Jumpbeleid zijn geassocieerd en kan er in het beleid een autorisatiecomponent zijn gedefinieerd waarin wordt afgedwongen dat de gebruiker toestemming van een derde partij of een beheerder nodig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

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

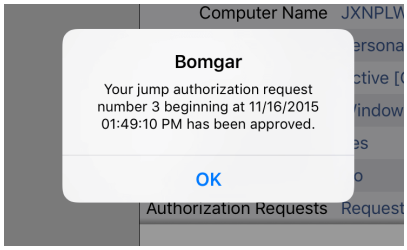
Nadat u op de knop Jump hebt getikt en toegang hebt aangevraagd, verschijnt er een prompt waarin u wordt gevraagd een reden in te voeren waarom u toegang tot het systeem wilt hebben.



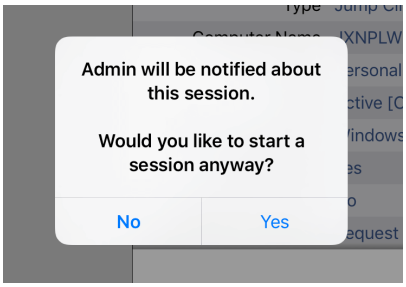
Vervolgens moet u aangeven wanneer en hoe lang u toegang tot het systeem wilt hebben.



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.



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.



Automatische inloggegevens voor de mobiele toegangsconsole

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

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

Inloggen bij eindpunten met gebruik van inloggegevensinjectie vanuit de iOS-toegangsconsole

Bij toegang tot een Windows-gebaseerde Jump-client via de mobiele access console kunt u inloggegevens gebruiken uit een inloggegevensopslagplaats door u 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

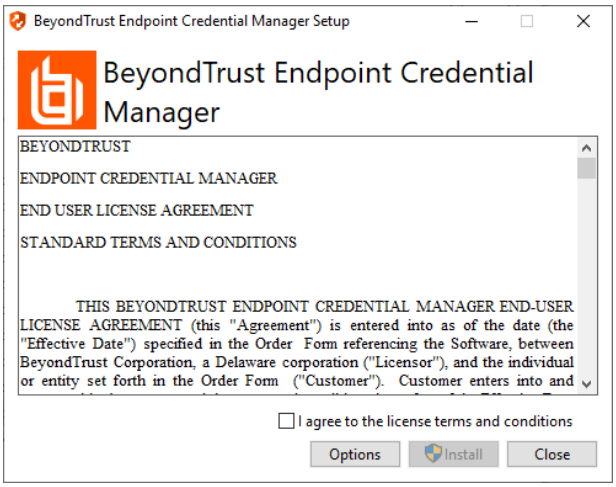
Voordat u kunt beginnen met Jumpitems openen met behulp van inloggegevensinjectie, moet u de BeyondTrust Endpoint Credential Manager (ECM) downloaden, installeren en configureren.

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

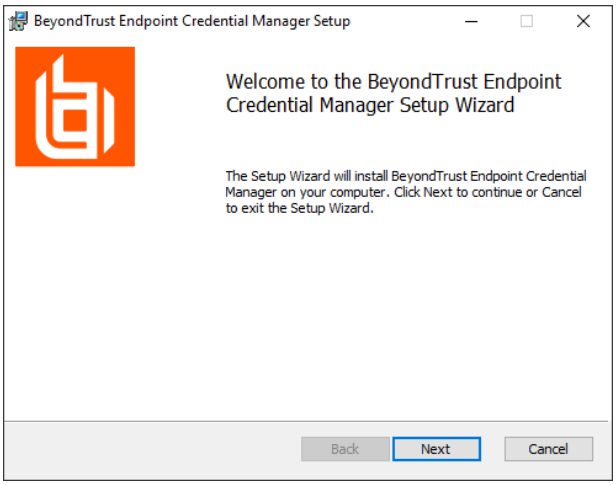
1. Download om te beginnen de BeyondTrust Endpoint Credential Manager (ECM) van BeyondTrust-ondersteuning op beyondtrustcorp.service-now.com/csm.
2. Start de installatiewizard voor BeyondTrust Endpoint Credential Manager.
3. Ga akkoord met de algemene voorwaarden uit de Gebruiksrechtovereenkomst. Schakel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

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

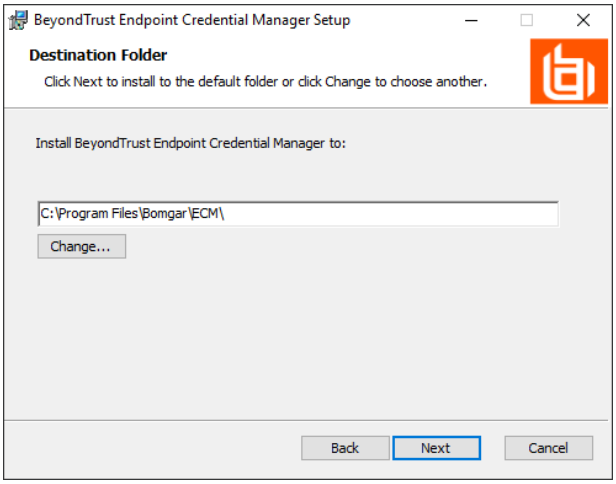
> ***Opmerking:*** *U kunt niet doorgaan met de installatie tenzij u akkoord gaat met de Gebruiksrechtovereenkomst.*



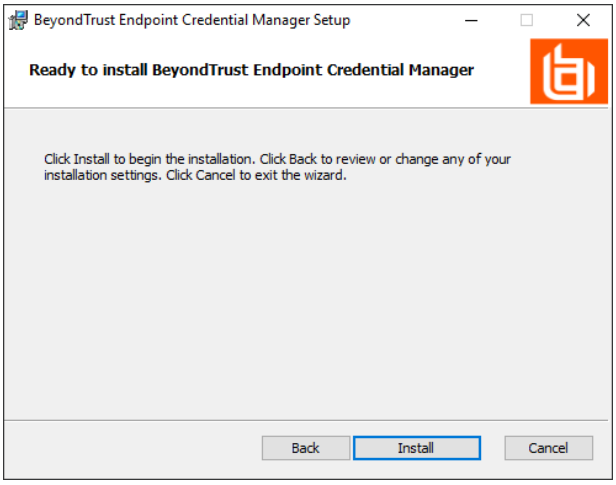
4. Klik op **Volgende** op het welkomstscherm.



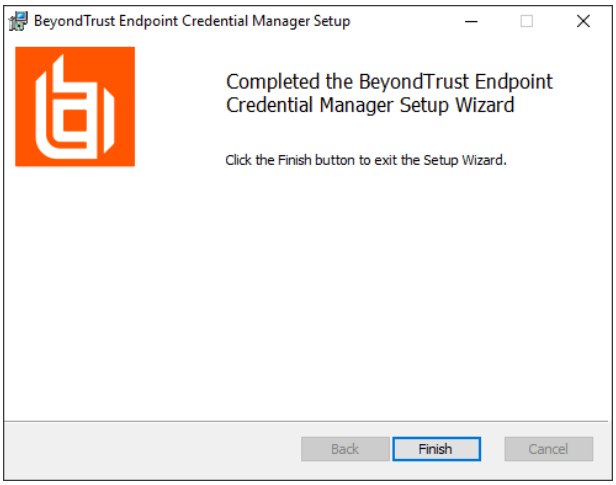
5. Kies een locatie voor de inloggegevensopslag en klik op **Volgende**.



6. In het volgende scherm kunt u de installatie beginnen of een voorgaande stap nog eens bekijken.
7. Klik op **Installeren** als u klaar bent om te beginnen.



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

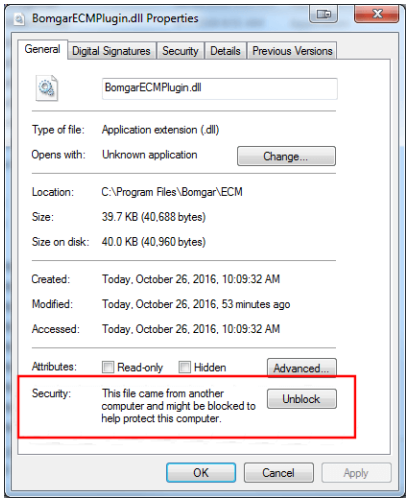


> ***Opmerking:*** *Om optimale up-time te waarborgen, kunnen beheerders maximaal drie ECM's op verschillende Windows-systemen installeren om met dezelfde inloggegevensopslag te communiceren. Een lijst met de ECM's die met het apparaat verbonden zijn, is te vinden op* ***/login > Status > Informatie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

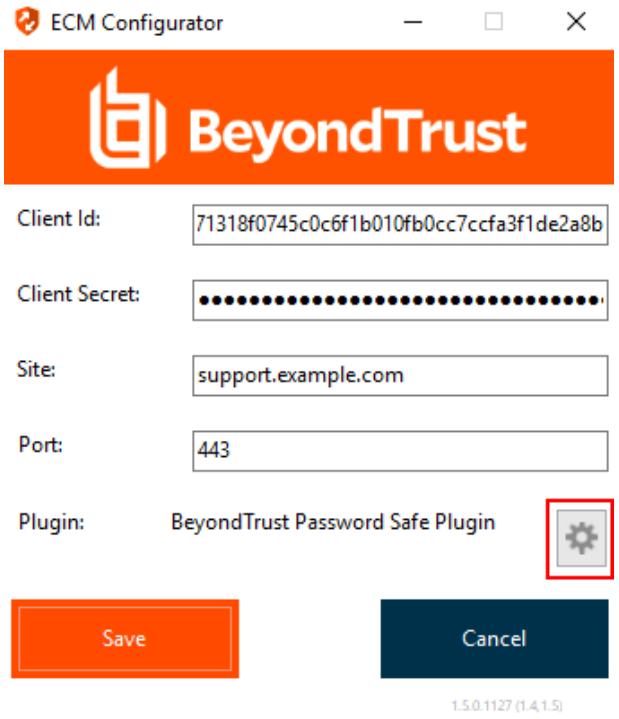
> ***Opmerking:*** *Als er meerdere ECM's in een configuratie met hoge beschikbaarheid zijn verbonden, stuurt het BeyondTrust Appliance B Series verzoeken naar de ECM in de ECM-groep die het langst met het apparaat is verbonden.*

De plugin installeren en configureren

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



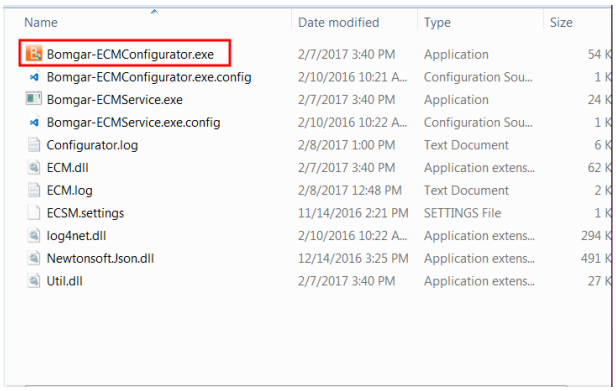
4. Klik op het pictogram met het tandwieltje in het venster van de **Configurator** om de instellingen voor de plug-in te configureren.



Een verbinding met uw inloggegevensopslag configureren

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

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



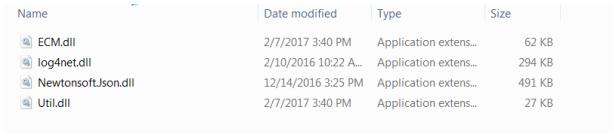
3. Vul de velden in wanneer de ECM Configurator opent. Alle velden zijn verplicht.

Vul de volgende waarden in:

Veldlabel	Waarde
Client-ID	De ID van uw inloggegevensopslag.
Clientgeheim	De geheime sleutel voor uw inloggegevensopslag.
Site	De URL van uw inloggevensopslag-instantie.

Poort	De serverpoort waardoor de ECM verbinding maakt met uw site.
Plugin	Klik op de knop **Plugin kiezen...** om de plugin te vinden.

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

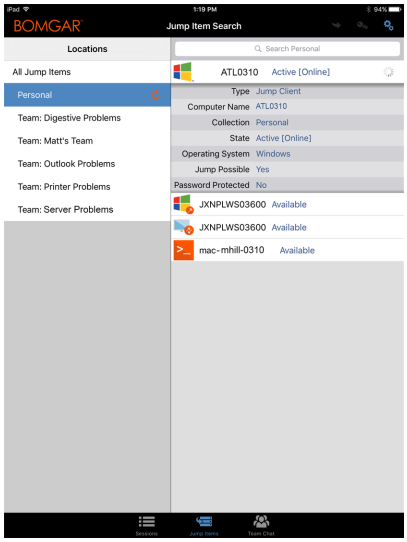


Opmerking: *Als u verbinding maakt met een wachtwoordkluis, zijn wellicht meer configuraties op plugin-niveau nodig. De pluginvereisten kunnen verschillen per inloggegevensopslag waarmee verbinding wordt gemaakt.*

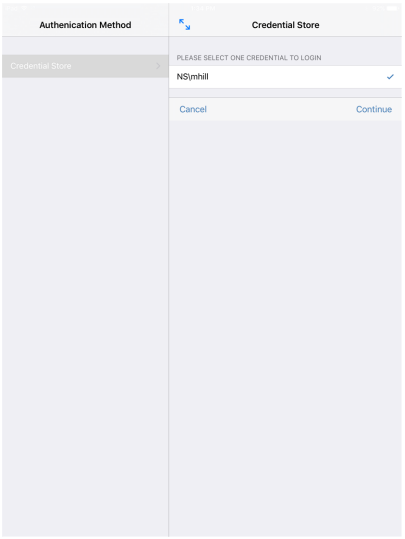
Inloggegevensinjectie gebruiken voor toegang tot eindpunten

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.

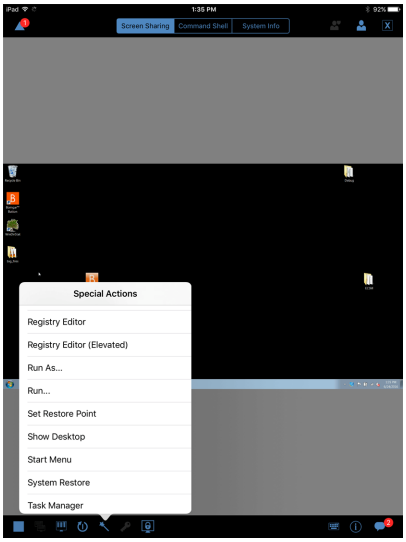
1. Ga naar uw lijst met **Jumpitems**.
2. Tik op het Jumpitem waar u toegang toe wilt hebben.
3. Tik op **Jump**.



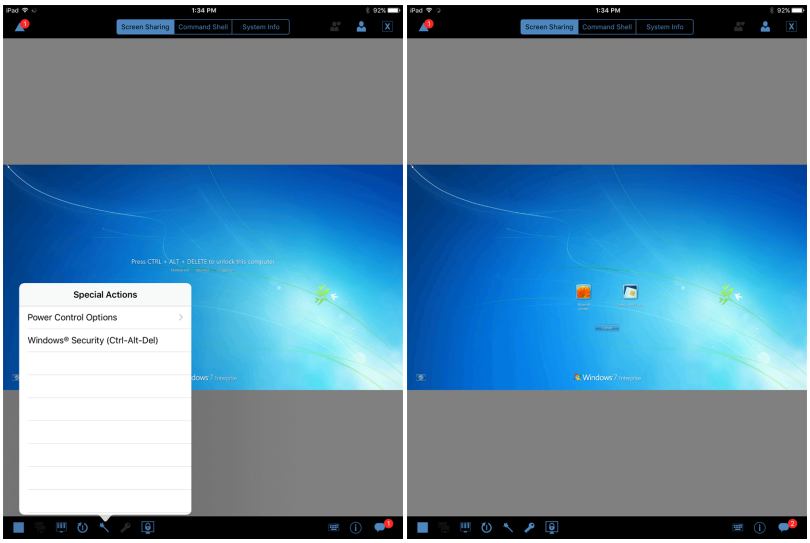
4. Tik op **Opslagplaats voor inloggegevens**.
5. Tik op de inloggegevens die u wilt gebruiken voor toegang tot het systeem.
6. Tik op **Doorgaan**.



7. Tik vanuit de sessie op **Start** om te beginnen met scherm delen.
8. Tik op de optie **Speciale acties**. Tik op **Uitvoeren als...**.



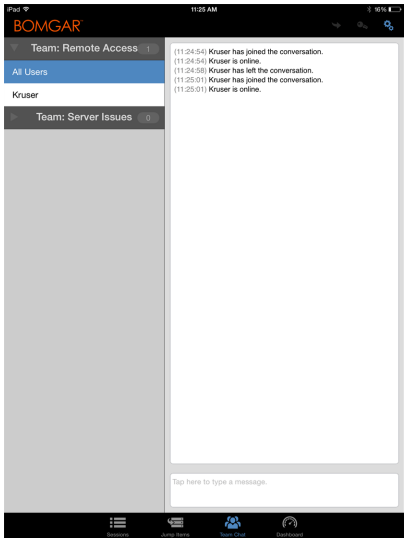
9. Tik op **Windows-beveiliging (Ctrl-Alt-Del)**.

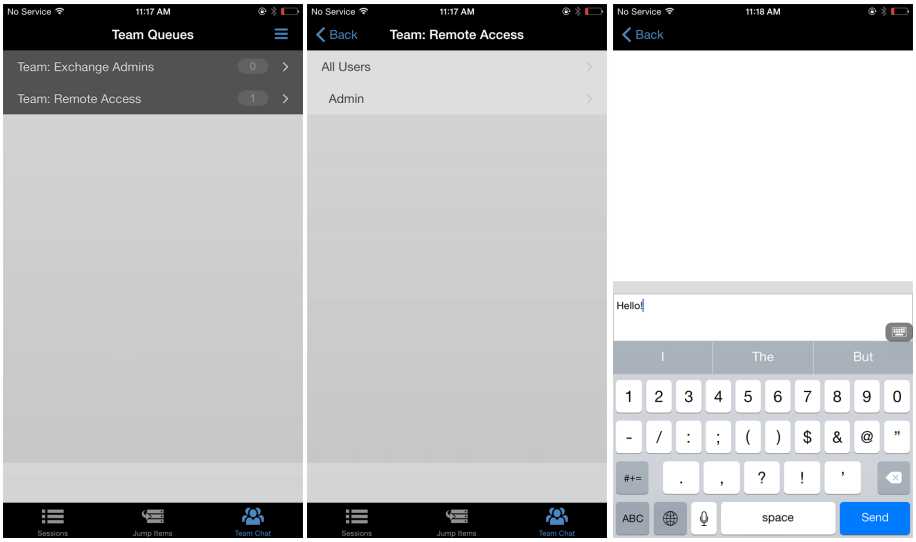


10. Tik op het symbool met de **Sleutel**. Met het sleutelsymbool kan het systeem uw opgeslagen inloggegevens weergeven om toegang te verkrijgen tot het eindpunt.

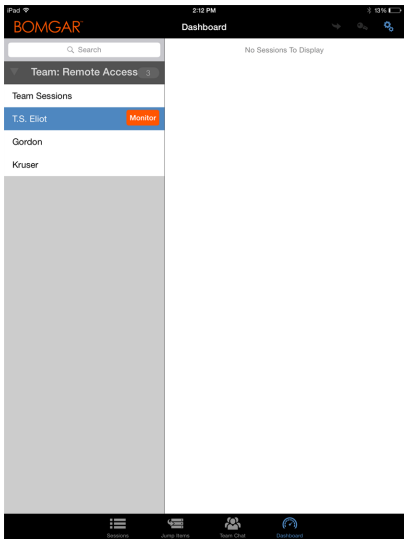
In de iOS-toegangsconsole met andere ingelogde gebruikers chatten

U kunt met andere ingelogde teamleden chatten door op het symbool **Teamchat** onderaan het scherm 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 ledenlijst selecteren om alleen met dat ene lid te chatten.





Teamleden in het dashboard beheren (alleen iPad)



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, dan verschijnt het symbool dashboard onderop het scherm. Op het dashboard verschijnen alleen ingelogde teamleden met een lagere rol voor het geselecteerde team.

Bovendien, 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.

Selecteer de gebruiker van wie u het scherm wilt bekijken en tik dan op de knop **Meekijken**. Hierdoor wordt een nieuwe pagina in uw access console geopend waarop ofwel het volledige beeldscherm ofwel alleen de access console wordt weergegeven, afhankelijk van de beheerinstellingen.

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

Gebruik 3D Touch voor mobiele toegang

3D Touch is een drukgevoelige functie die in de iPhone 6s en nieuwere versies te vinden is.

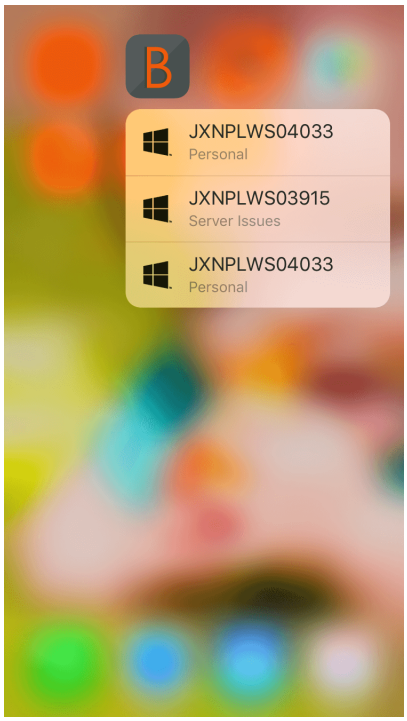
Met deze functie kunt u geen, weinig of veel druk uitoefenen op het scherm om Peek en Pop-acties te gebruiken. Met deze acties kunt u content bekijken en opdrachten uitvoeren met uw iPhone 6s-/6s Plus-apparaat zonder dat u de app volledig hoeft te openen. Voor meer informatie over 3D Touch, Peek en Pop, zie Maak gebruik van 3D Touch op https://developer.apple.com/ios/3d-touch/.

Vanaf BeyondTrust Privileged Remote Access 16.1 kunt u 3D Touch gebruiken voor eenvoudige toegang tot Jumpitems. Bekijk de onderstaande secties voor meer informatie om over de verschillende manieren waarop u met 3D Touch snel toegang krijgt tot kritieke systemen.

Toegang tot vaak ondersteunde Jumpitems met gebruik van 3D Touch

Met 3D Touch kunt u snel toegang krijgen tot maximaal drie van uw meest ondersteunde Jumpitems vanaf het beginscherm van de iPhone. Volg de onderstaande stappen.

1. Houd het pictogram van de mobiele access console-app voor iOS ingedrukt; er verschijnt dan een lijst met uw vaak geopende Jumpitems. Let op dat u extra druk moet uitoefenen op het scherm om de Jumpitem-opties te zien.
2. Tik in de lijst op het Jumpitem waar u toegang toe wilt hebben.
3. Vul uw inloggegevens in.
4. Er wordt een sessie met dat Jumpitem gestart.

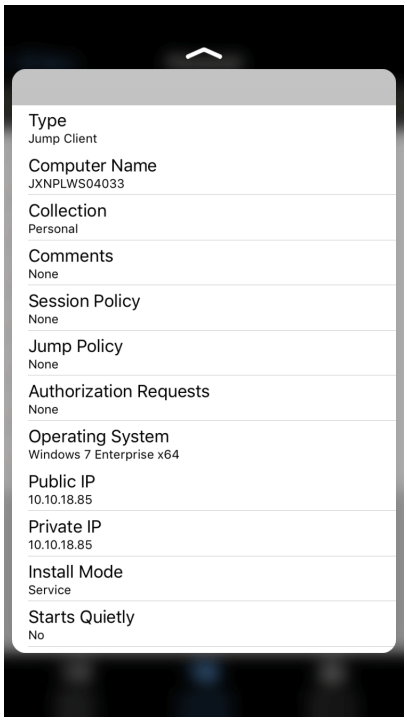


Voorbeeld van Jumpitem-informatie bekijken

Om informatie over een Jumpitem te bekijken voordat u een sessie start, kunt u de acties Peek en Pop van 3D Touch gebruiken. Volg de onderstaande stappen om een voorbeeld van een sessie te zien.

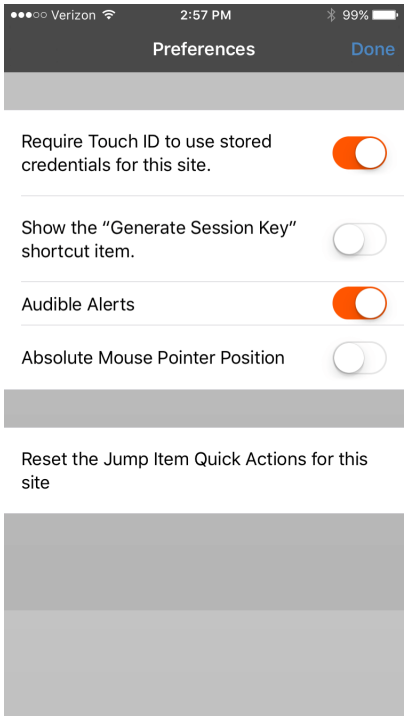
1. Selecteer op de pagina **Jumpitems** de wachtrij waar het Jumpitem zich bevindt.
2. Nadat u op de wachtrij hebt getikt, verschijnt een lijst met Jumpitems. Tik en oefen lichte druk uit op uw selectie tot de informatie van het Jumpitem in beeld verschijnt.
3. Blijf drukken op het scherm en veeg naar boven om de **Jump**-actie te zien. Klik op Jump om een sessie te starten.

> ***Opmerking:*** *Als u niet genoeg druk uitoefent of niet lang genoeg, verschijnt het voorbeeld niet en verschijnt in plaats daarvan de pagina* ***Sessie-informatie****.*



Voorkeuren voor 3D Touch instellen

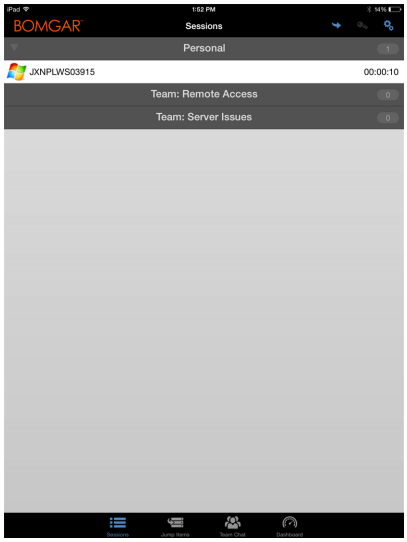
Ga vanuit de mobiele toegangsconsole voor iOS naar Voorkeuren door te tikken op het hamburgersymbool rechtsboven in het scherm en selecteer daar **Voorkeuren**. **De snelle acties van een Jumpitem voor deze site resetten** in de voorkeuren is specifiek voor 3D Touch. Als u op deze voorkeur tikt, kunt u de lijst met veelgebruikte Jumpitems wissen die u ziet wanneer u lang op het pictogram van de mobiele access console-app voor iOS tikt.



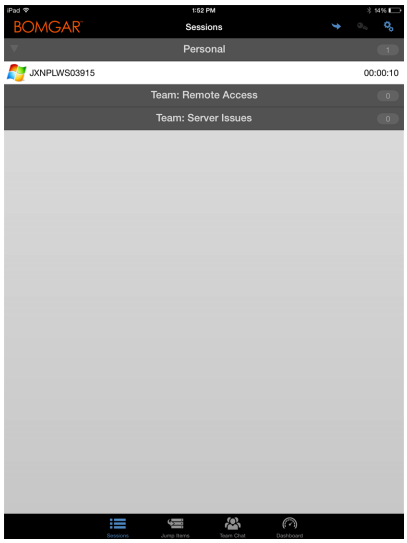
Toegangssessies op de iOS-toegangsconsole bekijken

Actieve toegangssessies zijn binnen de access console onderverdeeld in teamwachtrijen. Als u op het symbool **Sessies** onderop het scherm tikt, dan verschijnt een overzicht met alle geconfigureerde wachtrijen. Deze wachtrijen zijn gebaseerd op de teams die u in de /login-beheerinterface hebt ingesteld. Nadat een team is gedefinieerd, komt een wachtrij beschikbaar in de sectie **Sessies** van de access console. Deze wachtrij wordt altijd weergegeven zolang ten minste één teamlid in de access console is ingelogd.

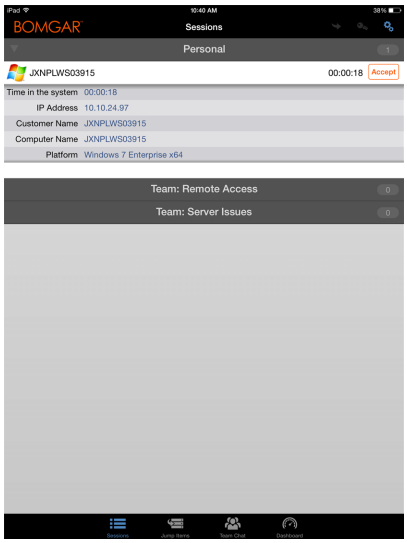
De **Persoonlijke** wachtrij bevat sessies die u momenteel in uitvoering hebt of sessies die door een ander lid specifiek met u zijn gedeeld. De overige wachtrijen zijn voor specifieke teams waar u lid van bent.



Tik op de naam van de wachtrij om sessies te zien die in uitvoering zijn. Tik op een sessie om informatie over het systeem of de sessie te zien. Tik op de optie **Terug** om naar een sessie te gaan.



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, dan verschijnt deze op uw scherm.*



Scherm delen met een eindpunt vanaf de iOS-toegangsconsole

Tik op de pagina **Scherm delen** op de knop **Afspelen** om weergave en beheer van het eindpunt aan te vragen als het scherm niet automatisch wordt gedeeld. Nadat u toegang tot het eindpunt hebt gekregen, verschijnt dit op uw scherm. U kunt de muis en het toetsenbord van het eindpunt volledig gebruiken, zodat u erop kunt werken alsof u erachter zit.

- Tik eenmaal om links te klikken.
- Dubbeltik om te dubbelklikken.
- Plaats uw vinger op de cursor en sleep deze om de muisaanwijzer te bewegen, **OF** als de absolute muisaanwijzer is ingeschakeld, dan kunt u de muisaanwijzer plaatsen waar u maar met uw vinger het scherm aanraakt.
- 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 en houdt vast om de cursor te vinden, **OF** als in uw instellingen de absolute muisaanwijzer is ingeschakeld, tik met uw vinger en houd die op dezelfde plaats om een uitklapmenu te openen waarin u kunt kiezen uit links klikken, rechts klikken of dubbelklikken.

> ***Opmerking:*** *Als dit in uw instellingen is ingeschakeld, kunt u op een iPad met het apparaat schudden voor een kort overzicht van de gebaren voor scherm delen.*

Op een iPad zijn alle acties voor scherm delen onderaan het scherm beschikbaar. Om op een iPhone toegang tot meer gereedschappen voor scherm delen te krijgen, moet u op het symbool **Menu** rechtsboven in het scherm tikken. Tik op **Bekijk hulp voor gebaren** voor een kort overzicht van de gebaren voor scherm delen.

Acties voor scherm delen

	Start met scherm delen.
	Stop met scherm delen.
	Selecteer een alternatief beeldscherm op de externe computer om weer te geven. Het primaire beeldscherm wordt met een **P** aangegeven.
	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.
	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. In de modus met hogere rechten kunnen sommige acties in de systeemcontext worden uitgevoerd. Ook kunt u de inloggegevens van een beheerder invoeren om een speciale actie in die gebruikerscontext uit te voeren.
	Start het externe systeem opnieuw op zonder de verbinding met de toegangssessie te verliezen.

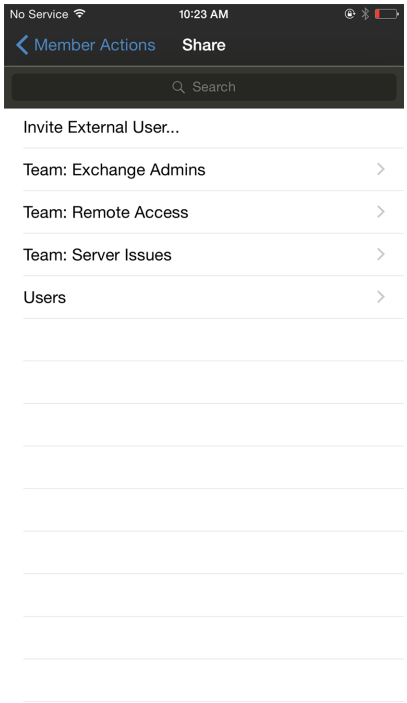
	Schakel de schermweergave, de muis en de toetsenbordinvoer uit voor de externe gebruiker. Beperkte interactie met het eindpunt is alleen beschikbaar bij toegang tot macOS- of Windows-computers. Beperkte interactie met klanten is alleen beschikbaar wanneer Windows-computers worden ondersteund. In Windows Vista en nieuwere versies moet de endpoint client worden opgewaardeerd. In Windows 8 is deze functie beperkt tot uitschakelen van de muis en het toetsenbord.
	Krijg toegang tot het toetsenbord om op het externe scherm te typen.

Een sessie met een andere gebruikers delen in de iOS-toegangsconsole

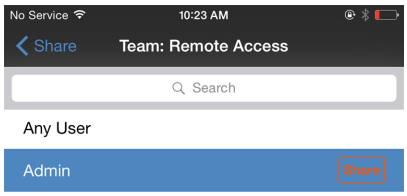
Tik op een iPad op het persoon-symbool rechtsboven in het scherm om een sessie met een ander teamlid te delen. Tik op een iPhone op het symbool **Actie** onderop het scherm. Tik op **Ledenacties**.

Selecteer uit het menu **Sessie delen**.

Zoek vervolgens het teamlid waarmee u de sessie wilt delen door eerst een team te zoeken waar die gebruiker lid van is. Selecteer een teamnaam om de leden van dat team te bekijken.



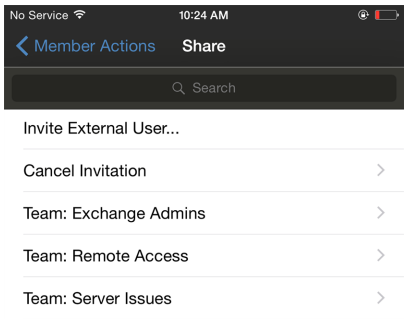
U kunt een gebruiker selecteren uit de lijst met teams om uit te nodigen om de sessie bij te wonen. U kunt meerdere uitnodigingen verzenden als u wilt dat meerdere teamleden de sessie bijwonen. Gebruikers worden hier alleen vermeld als zij bij de access console zijn ingelogd of als voor hen uitgebreide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



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

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. Tik vervolgens op de knop **Annuleren**. 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.



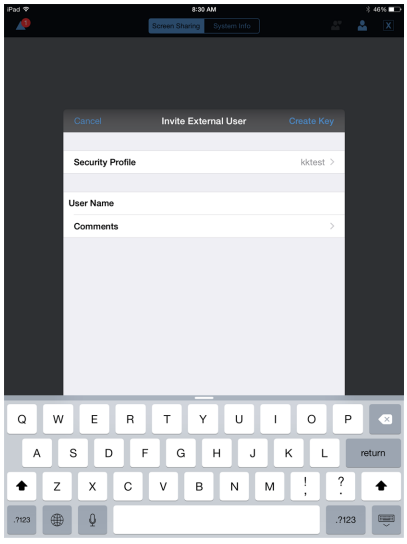
Een externe gebruiker vanuit de iOS-toegangsconsole uitnodigen om een sessie bij te wonen

Eventueel kunt u een sessie delen met een gebruiker die geen account op uw B Series Appliance heeft. Om een externe gebruiker uit te nodigen eenmalig een sessie bij te wonen, moet u op de knop **Ledenacties** tikken. Op een iPhone moet u eerst op de optie **Acties** tikken om bij deze knop te komen.

Selecteer uit het menu **Sessie delen**.

Tik op **Externe gebruiker uitnodigen**.

Een menu wordt geopend waarin u de uitnodiging kunt aanpassen en een toegangssessiecode kunt aanmaken.

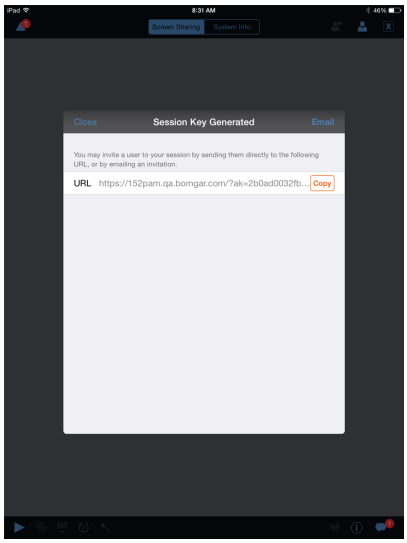


Tik op **Beveiligingsprofiel** voor een lijst met alle beschikbare gebruikersprofielen. Deze profielen worden in de beheerinterface aangemaakt en hiermee wordt het machtigingsniveau bepaald dat voor de externe gebruiker geldt. Als u een profiel selecteert, verdwijnt de lijst.

Tik vervolgens op de optie **Code creëren** rechtsboven in het scherm.

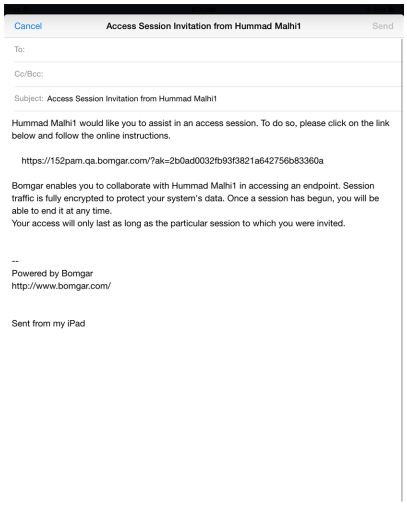
Hierna wordt de sectie **Sessiecode gegenereerd** gevuld.

Tik op de optie **E-mail** rechtsboven in het scherm.



Er wordt een e-mail gegenereerd. Wijzig de e-mail indien nodig.

Tik op **Verzenden** als u klaar bent.



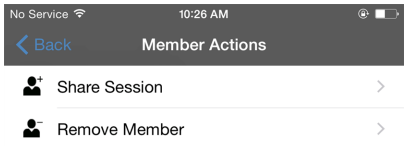
> ***Opmerking:*** *U kunt ook de URL kopiëren vanuit de sectie* ***Sessiecode gegenereerd****. Klik op de optie* ***Kopiëer*** *naast de URL.*

Als de externe gebruiker de e-mail heeft ontvangen, dan moet hij of zij op de **URL** klikken die in de e-mail staat. De gebruiker wordt dan naar de **Toegangsportaal** omgeleid, waar wordt gevraagd om de access console te downloaden.

Nadat de console is gedownload, wordt de aanmeldpagina voor de access console weergegeven; de toegangssessiesleutel is al ingevuld. De gebruiker moet op **Inloggen** tikken om toegang tot de console te krijgen.

In de iOS-toegangsconsole een lid van de sessie verwijderen

U kunt een gebruiker van een gedeelde sessie verwijderen. Tik op een iPhone op het symbool **Acties** onderop het scherm. Selecteer **Ledenacties**. Tik op **Lid verwijderen**.



Tik op een iPad op het persoon-symbool rechtsboven in het scherm. Selecteer uit het menu **Lid verwijderen**.

Selecteer de gebruiker die u wilt verwijderen. Tik vervolgens op de optie **Verwijderen**.

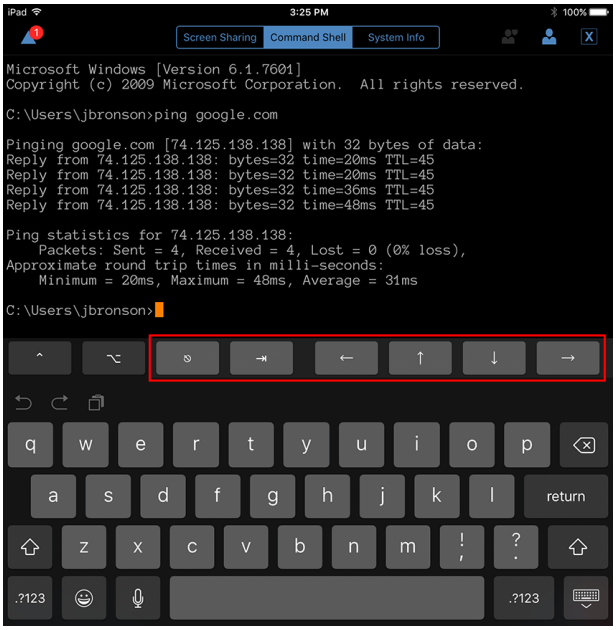
Open de opdrachtshell op het externe eindpunt met behulp van de toegangsconsole (Apple iOS)

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.

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. De serie met extra toetsen rechtsboven (gemarkeerd in de afbeelding) kan naar links en rechts worden geveegd om meer opties te tonen.

Indien er meerdere opdrachtshells geopend zijn, kunt u de opdrachtshell naar links en rechts vegen om te wisselen tussen de open shells.



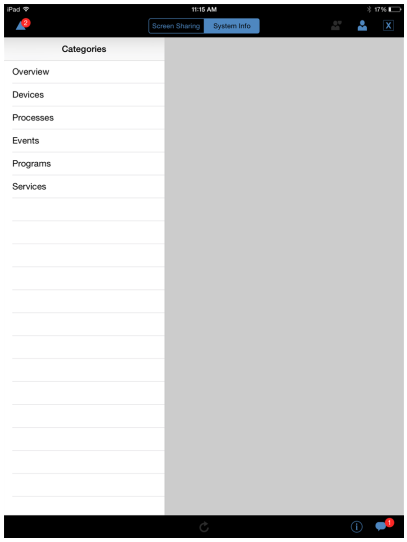
Ondersteuningsgereedschappen opdrachtshell

	Open een nieuwe shell om meerdere opdrachtregels uit te voeren.
	Sluit de huidige opdrachtshell. Overige geopende opdrachtshells blijven actief.
	Alle open opdrachtshells sluiten.
	Een lijst met momenteel geopende opdrachtshells weergeven. Tik op een item in de lijst voor toegang tot de bijbehorende opdrachtshell.

Systeeminformatie van extern systeem op de iOS-toegangsconsole bekijken

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

Om de systeeminformatie van een systeem te bekijken, gaat u naar **Systeeminformatie**. Tik op **Aanvragen**.



Selecteer de verschillende categorienamen waarvan u de gegevens wilt bekijken. Om naar de vorige categorie te gaan, tikt u op de optie **Terug**.

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

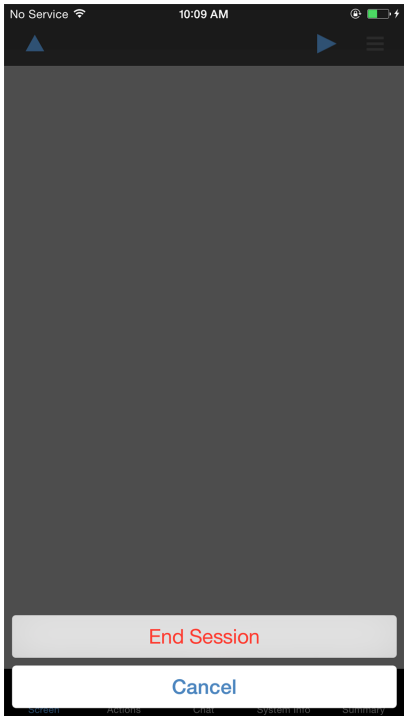
Een samenvatting van een toegangssessie bekijken

Op de pagina **Samenvatting** staat een overzicht van het externe systeem waar u op dat moment toegang toe hebt. Meer specifiek bevat de pagina **Samenvatting** de volgende informatie over het externe systeem:

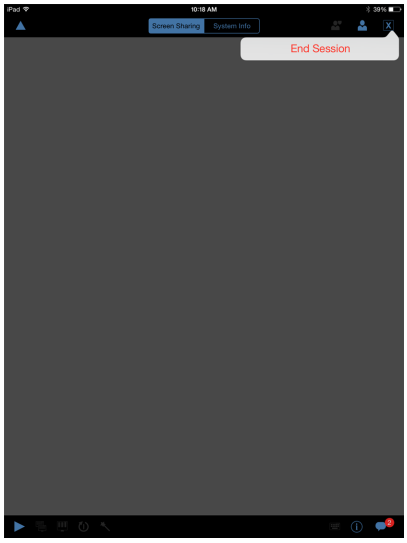
- **IP-adres**
- **Naam klant**
- **Naam computer**
- **Platform**

Een toegangssessie in de iOS-toegangsconsole sluiten

Om op een iPhone een sessie af te sluiten, moet u op het driehoekige symbool linksboven in het scherm tikken.



Om op een iPad een sessie af te sluiten, moet u op de **X** rechtsboven in het scherm tikken.



> ***Opmerking:*** *Er is ook een optie* ***Sessie beëindigen*** *beschikbaar door op het sybool* ***Acties*** *onderaan het scherm te tikken.*

Als u de eigenaar bent en op **Sessie beëindigen** tikt, dan wordt de sessiepagina in uw access console gesloten en worden eventuele extra gebruikers die de sessie delen verwijderd. Maar een geïnstalleerd Jumpitem wordt niet verwijderd.

Als u niet de eigenaar van de sessie bent en u op het symbool **X** tikt en **Verlaat sessie** selecteert, dan wordt u uit de sessie verwijderd. Maar de eigenaar van de sessie heeft nog steeds toegang tot de sessie evenals andere gebruikers die de sessie delen.