BeyondTrust

Privileged Remote Access
Console d’accès Android 2.2.7

TC:7/19/2021

Table des matières

Guide de la console d'accès BeyondTrust pour Android **3**

Installer la console d'accès sur Android **4**

Connexion à la console d'accès pour Android **5**

Modifier les paramètres dans la console d'accès Android **8**

Utiliser des éléments de Jump pour accéder à des points de terminaison depuis la console d'accès Android **9**

Autorisation pour utilisateur final et tierce partie 9

Informations d'authentification pour connexion automatique 11

Connexion à des points de terminaison en utilisant l'injection d'informations d'authentification dans la console d'accès Android **12**

Installer et configurer le gestionnaire d'informations d'authentification de point de terminaison 12

Installer et configurer le plug-in 14

Configurer une connexion à votre magasin d'informations d'authentification 15

Utiliser l'injection d'informations d'authentification pour accéder à des points de terminaison 16

Utiliser la messagerie instantanée d'équipe pour discuter avec d'autres utilisateurs dans la console d'accès Android **19**

Consulter les sessions d'accès dans la console d'accès Android **20**

Partage d'écran avec le point de terminaison depuis la console d'accès Android 21

Partage d'une session avec d'autres utilisateurs dans la console d'accès Android 23

Inviter un utilisateur externe à rejoindre une session dans la console d'accès Android 24

Supprimer un membre de la session dans la console d'accès Android 26

Ouvrir l'interpréteur de commandes sur un point de terminaison distant en utilisant la console d'accès Android 27

Consulter les informations système du point de terminaison distant dans la console d'accès Android 29

Consulter un résumé de la session d'accès et ajoutez des remarques dans la console d'accès Android 30

Fermer la session dans la console d'accès Android 31

Guide de la console d'accès BeyondTrust pour Android

Ce guide est destiné à vous aider à installer BeyondTrust sur votre appareil Android et à comprendre les fonctionnalités de la access console Android. BeyondTrust vous permet d'accéder à distance et en toute sécurité à vos points de terminaison en vous connectant à eux à travers le support_button.

Bien que des captures d'écran d'un smartphone Android sont utilisées dans ce guide, notez que les fonctions sont les mêmes avec une tablette Android.

Utilisez ce guide uniquement après que l'administrateur a procédé à l'installation et à la configuration initiales du B Series Appliance, qui sont expliquées dans le Guide d'installation matérielle du BeyondTrust Appliance B Series. Si vous avez besoin d'aide, contactez l'BeyondTrust Technical Support à l'adresse www.beyondtrust.com/support.

Installer la console d'accès sur Android

La access console BeyondTrust pour Android est disponible en téléchargement gratuit sur Google Play. Depuis votre appareil Android, cherchez « Access Console BeyondTrust » (BeyondTrust Representative Console en anglais) sur Google Play, puis installez l'appli.

Pour exécuter la access console BeyondTrust sur votre appareil, votre B Series Appliance doit utiliser la version 15.2 du logiciel ou plus. La access console BeyondTrust est compatible avec les téléphones Android 2.3 et supérieur, et les tablettes Android 3.0 et supérieur.

Remarque : *seule la access console BeyondTrust peut être utilisée avec un site Privileged Remote Access (PRA). La console du technicien d'assistance BeyondTrust ne peut pas être utilisée pour se connecter à un site Privileged Remote Access, et la access console BeyondTrust ne peut pas être utilisée pour se connecter à un site d'Remote Support BeyondTrust.*

IMPORTANT !

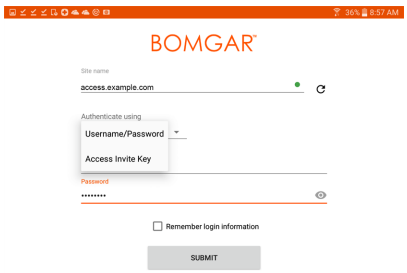
Votre B Series Appliance doit être équipé d'un certificat SSL valide signé par une autorité de certificat. BeyondTrust ne prend pas en charge pas l'utilisation de certificats auto-signés pour la access console Android.[1] Une fois que vous avez appliqué un certificat SSL signé par une AC à votre B Series Appliance, contactez l'BeyondTrust Technical Support. Votre technicien service client créera une nouvelle version logicielle s'intégrant à votre certificat SSL. Avec cette version mise à jour installée sur votre B Series Appliance, vous pouvez exécuter la access console BeyondTrust sur votre appareil pour accéder à vos points de terminaison depuis pratiquement n'importe où.

[1]Les appareils Android disposant d'un système d'exploitation inférieur à 4.0 peuvent rencontrer une erreur lorsqu'ils tentent de joindre votre site BeyondTrust. Ce problème vient d'un certificat racine SSL manquant dans le magasin de certificats de l'appareil Android. Le problème est uniquement lié au système d'exploitation Android, et pas au logiciel BeyondTrust. Pour le résoudre, mettez à niveau l'appareil Android ou contactez l'autorité de certificat pour demander un autre certificat racine SSL compatible avec l'appareil Android.

Connexion à la console d'accès pour Android

Sur l'écran de connexion, saisissez le nom d'hôte de votre site BeyondTrust, par ex. access.example.com. Indiquez ensuite le nom d'utilisateur et le mot de passe associés à votre compte utilisateur BeyondTrust. Vous pouvez faire en sorte que la access console BeyondTrust se souvienne de vos informations d'authentification. Appuyez ensuite sur **Connexion**.

Pour les utilisateurs privilégiés et les fournisseurs utilisant la access console, vous pouvez choisir de changer la méthode d'authentification en appuyant sur l'emplacement du **nom d'utilisateur/mot de passe**. Sélectionnez **Clé d'invitation d'accès** dans le menu déroulant pour saisir la clé qui vous a été fournie.



> ***Remarque :*** *votre administrateur peut exiger que vous soyez sur un réseau autorisé pour pouvoir vous connecter à la console. Cette restriction réseau peut s'appliquer à votre première connexion ou de façon permanente. Cette restriction ne s'applique pas aux invites d'accès.*

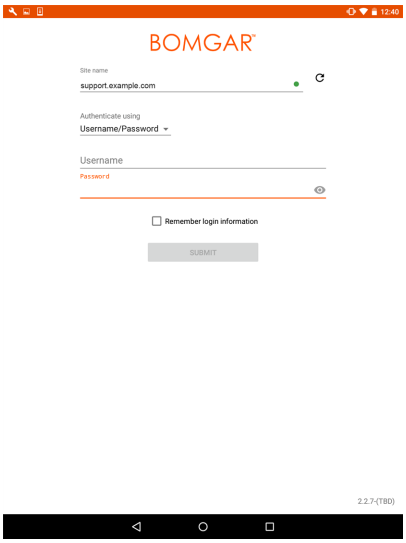
Connectez-vous à la console d'accès Android à l'aide de SAML mobile

SAML mobile offre une méthode simple pour s'identifier en toute sécurité sur la access console Android. Pour en savoir plus sur l'authentification unique SAML, veuillez consulter Security Assertion Markup Language à l'adresse https://en.wikipedia.org/wiki/Security_Assertion_Markup_Language. Suivez les étapes ci-dessous pour vous connecter à la access console Android à l'aide de SAML.

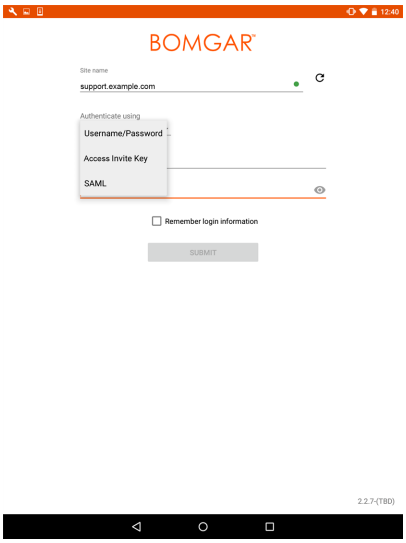
> ***Remarque :*** *avant de vous connecter à la access console Android avec SAML, consultez* ***Utilisateurs et sécurité > Fournisseurs de sécurité*** *pour vous assurer que le fournisseur SAML est bien configuré pour votre environnement administratif /login. Si SAML n'est pas configuré dans /login, SAML ne sera pas disponible en tant que méthode d'identification pour la access console Android. Pour en savoir plus sur l'intégration de l'authentification unique SAML dans votre environnement Privileged Remote Access BeyondTrust, veuillez consulter Créer et configurer le fournisseur de sécurité SAML à l'adresse www.beyondtrust.com/docs/privileged-remote-access/how-to/integrations/security-providers/saml/configure-settings.htm.*

1. Appuyez sur l'appli de access console de votre appareil Android.

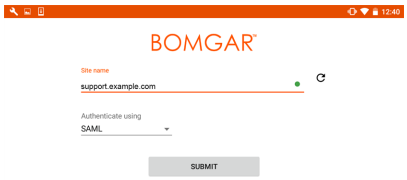
2. Appuyez sur **Nom d'utilisateur et mot de passe** à partir de l'écran de connexion.



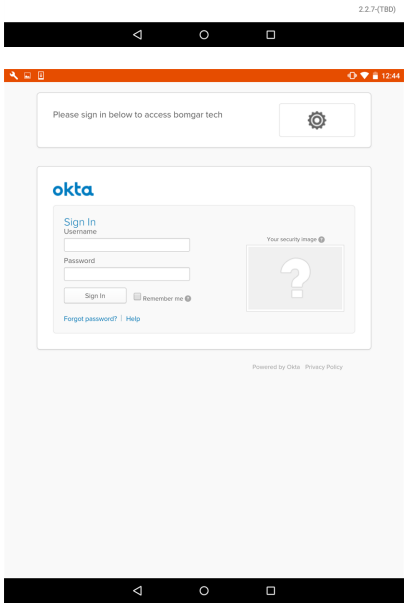
3. Sélectionnez le langage **SAML**.



4. Appuyez sur **Envoyer**.



5. Une fois sur votre page de fournisseur SAML, saisissez vos informations d'authentification.
6. Appuyez sur **Connexion** pour accéder à la console.



Modifier les paramètres dans la console d'accès Android

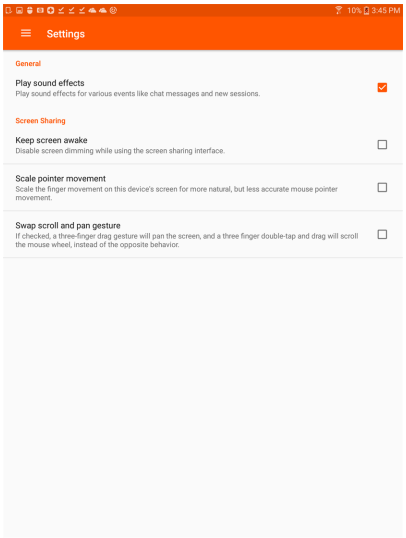
Pour modifier vos paramètres, sélectionnez **Paramètres** dans le menu.

Lire les alertes sonores lit les alertes sonores pour certains événements se produisant dans la access console.

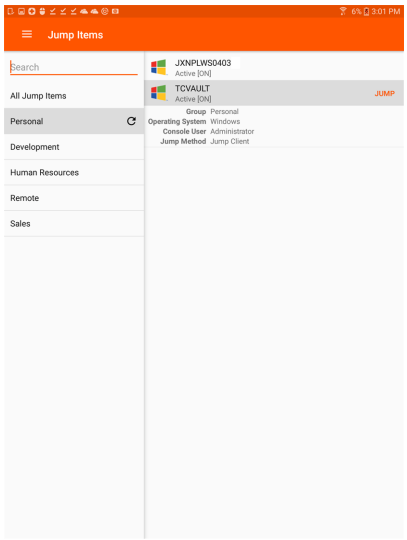
Pour empêcher la baisse de luminosité de votre écran pendant le partage d'écran, cochez **Garder l'écran actif**.

Si l'option **Mettre le mouvement du pointeur à l'échelle** est cochée, le pointeur distant suit les mouvements de votre doigt sur l'écran. Si elle n'est pas cochée, le pointeur peut subir un décalage dans les mouvements, mais sa position est plus précise.

Avec **Échanger gestes défiler et panoramique**, définissez lequel des deux gestes doit faire défiler la roue de la souris distante, et lequel doit faire un panoramique sur l'écran.



Utiliser des éléments de Jump pour accéder à des points de terminaison depuis la console d'accès Android



Pour accéder à un point de terminaison individuel sans l'aide de l'utilisateur final, installez un élément de Jump sur ce système depuis la page **Jump Clients** de l'interface d'administration /login. De plus, les types d'éléments de Jump suivants sont gérés par la access console mobile :

- **Jump distant**
- **VNC distant**
- **RDP**
- **Shell Jump**

Les éléments de Jump sont répertoriés dans les groupes de Jump. Si vous êtes associé à un ou plusieurs groupes de Jump, vous pouvez accéder aux éléments de Jump de ces groupes, selon les autorisations accordées par votre administrateur.

Votre liste personnelle d'éléments de Jump a avant tout un usage personnel, bien que les chefs d'équipe, les responsables d'équipe et les utilisateurs autorisés à consulter l'ensemble des éléments de Jump sont susceptibles d'accéder à votre liste personnelle. De même, si vous êtes un responsable ou un chef d'équipe doté des autorisations adéquates, vous êtes susceptible de consulter les listes personnelles d'éléments de Jump des membres de votre équipe. En outre, vous pouvez être autorisé à accéder aux éléments de Jump de groupes de Jump dont vous ne faites pas partie et aux éléments de Jump de membres n'appartenant pas à votre équipe.

Pour trouver un élément de Jump, appuyez sur l'option **Éléments de Jump** du menu.

Sélectionnez un emplacement et appuyez sur le bouton **Actualiser**. Une fois que vous avez trouvé le point de terminaison auquel vous voulez accéder, sélectionnez l'entrée pour afficher les détails.

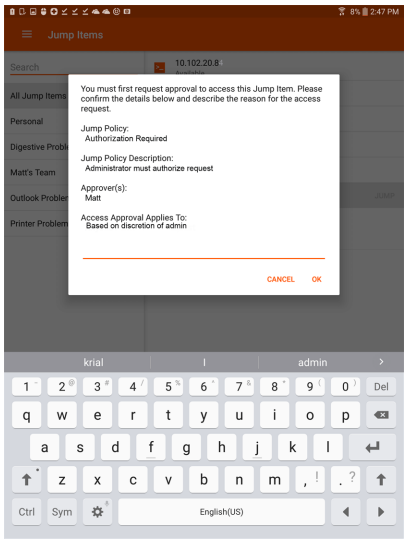
Appuyez sur le bouton **Jump** pour démarrer une session.

Autorisation pour utilisateur final et tierce partie

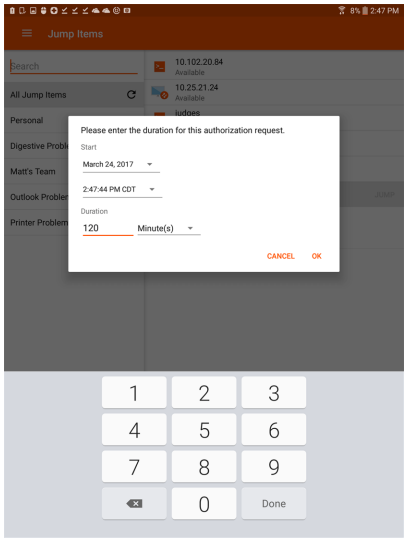
En fonction de la configuration des éléments de Jump dans l'interface d'administration /login, un élément de Jump peut être associé à une règle de Jump, et la règle peut définir une composante d'autorisation qui vous force à demander une autorisation auprès d'un tiers ou d'un administrateur avant de pouvoir lancer une session d'accès avec cet élément de Jump.

> *Pour en apprendre davantage sur la configuration des notifications et l'approbation de l'utilisateur final et d'une tierce partie, veuillez consulter Règles de Jump : Définir les plannings, les notifications et les approbations pour les éléments de Jump à l'adresse https://www.beyondtrust.com/docs/privileged-remote-access/getting-started/admin/jump-policies.htm.*

Après avoir appuyé sur le bouton Jump et sollicité l'accès, une invite vous demande de justifier votre demande d'accès au système.



Vous devez ensuite indiquer à quel moment et pour combien de temps vous accéderez au système.



Une fois la requête soumise, la tierce partie ou la personne responsable de l'approbation des demandes d'accès est prévenue par e-mail et peut accepter ou refuser la demande. Bien que d'autres approbateurs sont susceptibles de consulter l'adresse e-mail de la personne ayant autorisé ou refusé la demande, le demandeur n'est pas en mesure de le faire. Après qu'une autorisation a été établie, une notification d'autorisation apparaît dans les informations de l'élément de Jump, affichant *approuvée* ou *refusée*. Si l'accès est autorisé, vous pouvez appuyer sur le bouton Jump pour accéder au système.

Bomgar

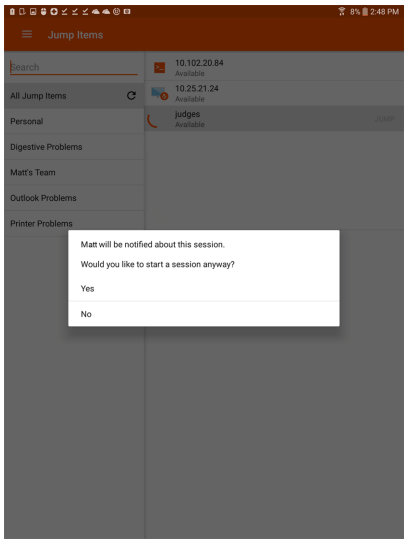
Your jump authorization request number 1 beginning at 05/31/49198 10:19:53 PM has been approved.

OK

Après avoir appuyé sur le bouton de Jump, un message vous demande si vous souhaitez lancer une session d'accès. Si vous choisissez de commencer une session, les commentaires de l'approbateur apparaîtront, et vous pourrez accéder au système.

Si l'utilisateur choisit de continuer, les commentaires de l'approbateur apparaîtront, et l'utilisateur pourra commencer à travailler sur le système.

Pour savoir comment les éléments de Jump fonctionnent avec les planning de Jump, les ID de ticket, les flux de travail, etc., veuillez consulter Interface de Jump : Utilisez les éléments de Jump pour accéder à des systèmes distants.



Informations d'authentification pour connexion automatique

Les informations d'authentification venant du **gestionnaire d'informations d'authentification de point de terminaison** peuvent être utilisées pour le RDP et pour effectuer un Jump distant. Si un utilisateur choisit de faire un Jump vers un Jump distant ou un RDP distant et qu'aucune information de connexion n'est automatiquement disponible, un nom d'utilisateur et un mot de passe doivent être saisis dans l'invite avant que la session d'accès au point de terminaison ne puisse commencer. Si l'interface d'administration /login a été configurée avec des informations de connexion automatique et qu'elle ne renvoie qu'un groupe d'informations d'authentification disponibles pour un utilisateur et un élément de Jump spécifiques, la demande d'informations d'authentification est ignorée et un seul set d'informations d'authentification est utilisé pour commencer la session. Si plus d'un groupe d'informations d'authentification est configuré dans l'interface d'administration /login, l'utilisateur aura le choix entre choisir des informations d'authentification dans le magasin d'informations d'authentification ou saisir ses propres informations d'authentification manuellement.

> *Pour plus d'informations sur la configuration et la gestion des informations d'authentification, veuillez consulter Sécurité : Gestion des paramètres de sécurité à l'adresse www.beyondtrust.com/docs/privileged-remote-access/getting-started/admin/security.htm.*

Connexion à des points de terminaison en utilisant l'injection d'informations d'authentification dans la console d'accès Android

Lorsque vous accédez à un Jump Client basé sur Windows à travers la access console mobile, vous pouvez utiliser les informations d'authentification d'un magasin d'informations d'authentification pour vous connecter au point de terminaison ou pour lancer des applications en tant qu'admin.

Avant d'utiliser l'injection d'informations d'authentification, vérifiez que vous disposez d'un magasin d'informations d'authentification disponible pour vous connecter au PRA BeyondTrust, tel qu'une banque de mots de passe.

Installer et configurer le gestionnaire d'informations d'authentification de point de terminaison

Exigences requises :

- Windows Vista® ou supérieur, 64 bits seulement
- .NET 4.5 ou supérieur
- Processeur : 2 GHz ou plus
- Mémoire : 2 Go ou plus
- Espace disponible sur le disque : 80 Go ou plus

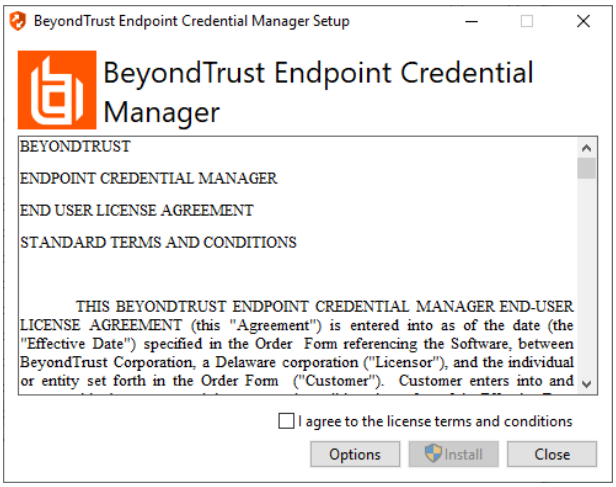
Avant de pouvoir commencer à accéder à des éléments de Jump en utilisant l'injection d'informations d'authentification, vous devez télécharger, installer et configurer le gestionnaire d'informations d'authentification de point de terminaison (ECM) BeyondTrust. L'ECM BeyondTrust vous permet de configurer rapidement votre connexion à un magasin d'informations d'authentification, comme une banque de mots de passe.

> ***Remarque :*** *L'ECM doit être installé sur votre réseau pour activer le service ECM BeyondTrust et utiliser l'injection d'informations d'authentification dans le PRA BeyondTrust.*

1. Pour commencer, téléchargez le gestionnaire d'informations d'authentification de point de terminaison (ECM) BeyondTrust auprès de l'assistance technique BeyondTrust à l'adresse beyondtrustcorp.service-now.com/csm.

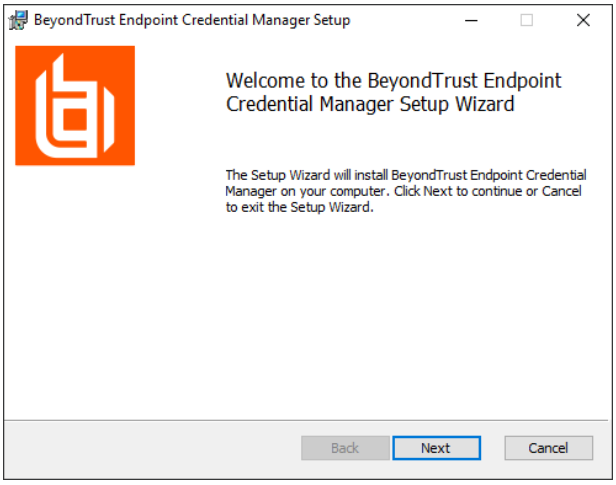
2. Lancez l'assistant de configuration du gestionnaire d'informations d'authentification de point de terminaison BeyondTrust.
3. Acceptez les conditions générales du CLUF. Cochez la case si vous acceptez, puis cliquez sur **Installer**.

   Pour modifier le chemin d'installation de l'ECM, cliquez sur le bouton **Options** pour choisir l'emplacement d'installation.

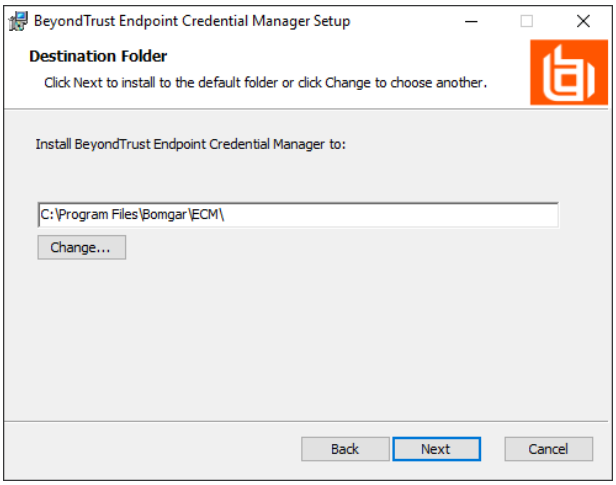


> ***Remarque :*** *vous ne pourrez pas poursuivre l'installation si vous n'acceptez pas le CLUF.*

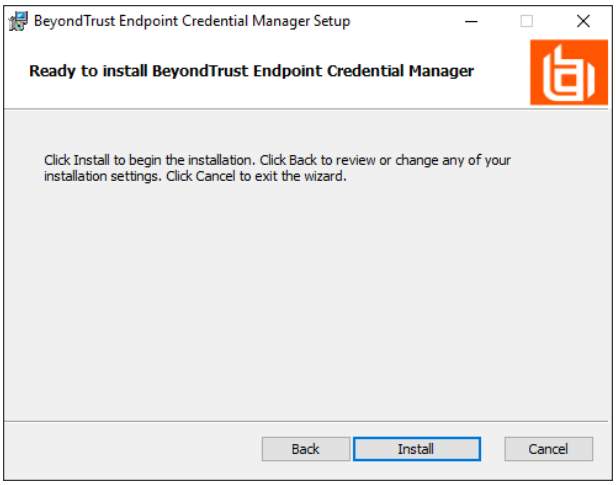
4. Cliquez sur **Suivant** dans l'écran de bienvenue.



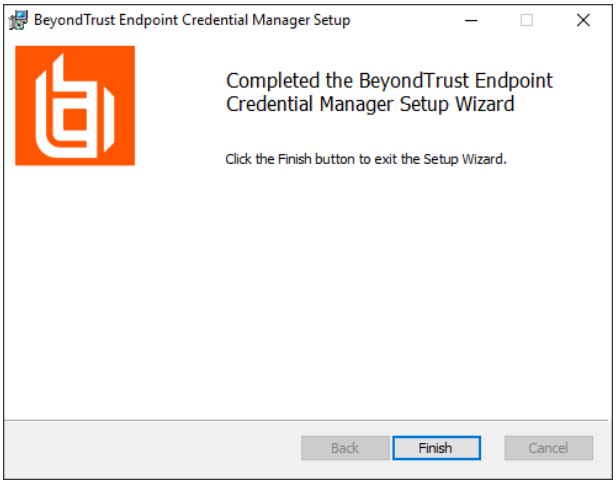
5. Choisissez un emplacement pour le gestionnaire d'informations d'authentification, puis cliquez sur **Suivant**.



6. Sur l'écran suivant, vous pouvez lancer l'installation ou vérifier les étapes précédentes.
7. Cliquez sur **Installer** lorsque vous êtes prêt à commencer.



8. L'installation prend quelques instants. Dans l'écran indiquant la finalisation de l'opération, cliquez sur **Terminé**.



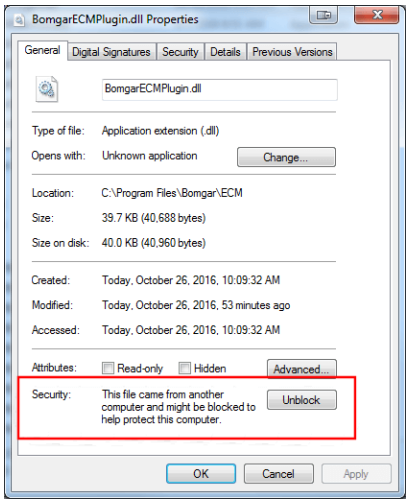
> ***Remarque :*** *pour optimiser le temps de disponibilité, les administrateurs peuvent installer jusqu'à trois ECM sur plusieurs machines Windows pour communiquer avec le même magasin d'informations d'authentification. Une liste des ECM connectés au site du serveur est disponible sur* ***/login > État > Information > Clients ECM****.*

> ***Remarque :*** *lorsque des ECM sont connectés dans une configuration de haute disponibilité, le BeyondTrust Appliance B Series achemine les demandes vers le groupe d'ECM ayant été le plus longtemps connecté au serveur.*

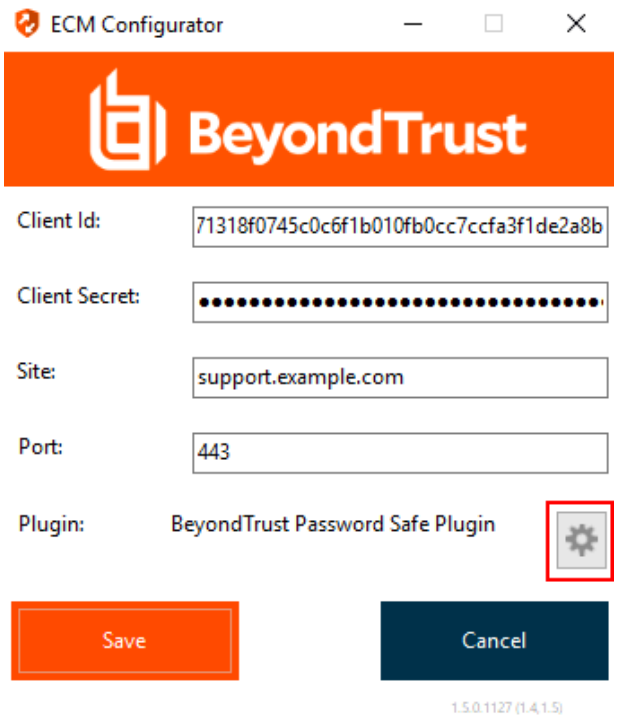
Installer et configurer le plug-in

1. Une fois que l'ECM BeyondTrust est installé, procédez à l'extraction et à la copie des fichiers du plug-in dans le répertoire d'installation (généralement **C:\Program Files\Bomgar \ECM**).
2. Exécutez le **configurateur ECM** pour installer le plug-in.
3. Le configurateur devrait automatiquement détecter le plug-in et le charger. Si c'est le cas, passez à l'étape 4 ci-dessous. Autrement, suivez ces étapes :

- Tout d'abord, vérifiez que la DLL n'est pas bloquée. Faites un clic droit sur la DLL et sélectionnez **Propriétés**.
- Dans l'onglet **Général** regardez au bas de l'écran. S'il y a une section **Sécurité** avec un bouton **Débloquer**, cliquez sur ce dernier.
- Répétez ces étapes pour toutes les autres DLL fournies avec le plug-in.
- Dans le configurateur, cliquez sur le bouton **Choisir plug-in...** et accédez à l'emplacement de la DLL du plug-in.



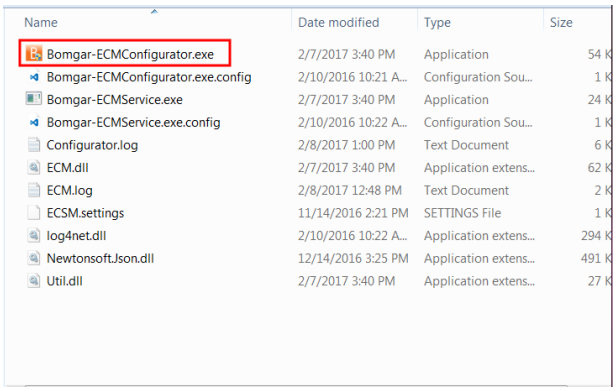
4. Cliquez sur l'icône en forme d'engrenage dans la fenêtre **Configurateur** pour configurer les paramètres du plug-in.



Configurer une connexion à votre magasin d'informations d'authentification

En utilisant le configurateur ECM, établissez une connexion à votre magasin d'informations d'authentification.

1. Trouvez le configurateur ECM BeyondTrust que vous venez d'installer en utilisant le champ de recherche de Windows, ou en consultant la liste des programmes du menu **Démarrer**.
2. Lancez le programme pour commencer l'établissement d'une connexion.

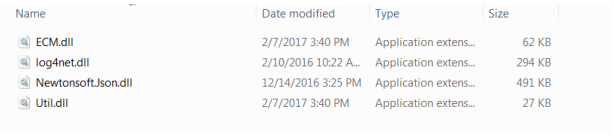


3. Lorsque le configurateur ECM s'ouvre, remplissez les champs. Tous les champs sont obligatoires.

Saisissez les valeurs suivantes :

Nom de champ	Valeur
ID client	L'ID pour votre magasin d'informations d'authentification.
Secret de client	La clé secrète pour votre magasin d'informations d'authentification.
Site	L'URL pour votre instance de magasin d'informations d'authentification.
Port	Le port de serveur à travers lequel l'ECM se connecte à votre site.
Plug-in	Cliquez sur le bouton **Choisir plug-in...** pour trouver le plug-in.

4. Lorsque vous cliquez sur le bouton **Choisir plug-in...**, le dossier de l'ECM s'ouvre.
5. Collez vos fichiers de plug-in dans le dossier.
6. Ouvrez le fichier plug-in pour commencer le chargement.

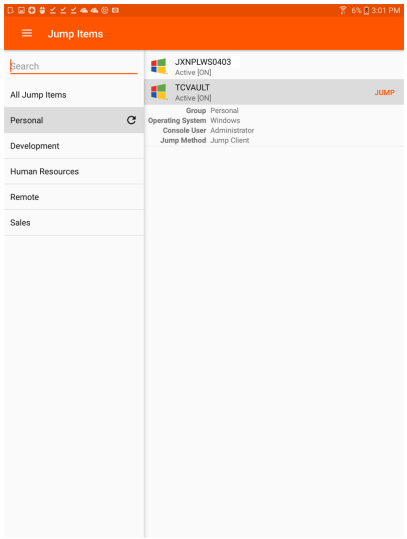


Remarque : *Si vous vous connectez à la banque de mots de passe, une configuration supplémentaire au niveau plug-in peut être requise. Les besoins de plug-in varient en fonction du magasin d'informations d'authentification connecté.*

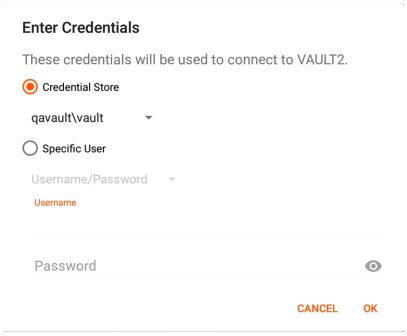
Utiliser l'injection d'informations d'authentification pour accéder à des points de terminaison

Une fois que le magasin d'informations d'authentification a été configuré et qu'une connexion a été établie, le PRA BeyondTrust peut utiliser des informations d'authentification dans le magasin d'informations d'authentification pour se connecter à des points de terminaison.

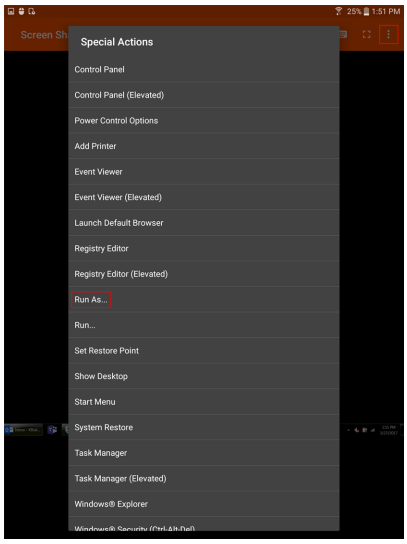
1. Allez à votre liste d'**éléments de Jump**.
2. Appuyez sur l'élément de Jump auquel vous souhaitez accéder.
3. Appuyez sur **Jump**.



4. Le dialogue **Saisir des informations d'authentification** s'affiche. Appuyez sur **Magasin d'informations d'authentification**.
5. Appuyez sur les informations d'authentification que vous souhaitez utiliser pour accéder au système.
6. Appuyez sur **OK**.

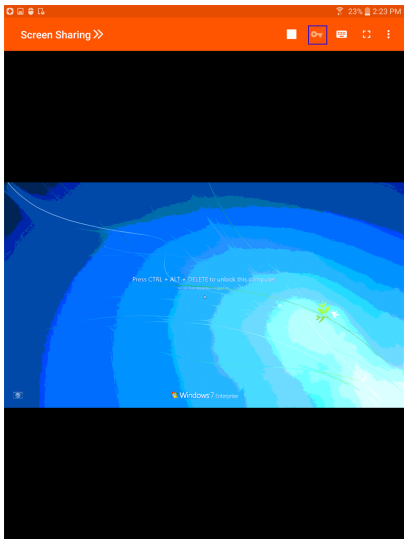


7. Depuis la session, appuyez sur le bouton **Démarrer** pour lancer le partage d'écran.
8. Appuyez sur l'option **Actions spéciales**. Appuyez sur **Exécuter en tant que...**.
9. Appuyez sur **Sécurité Windows (Ctrl-Alt-Suppr)**.



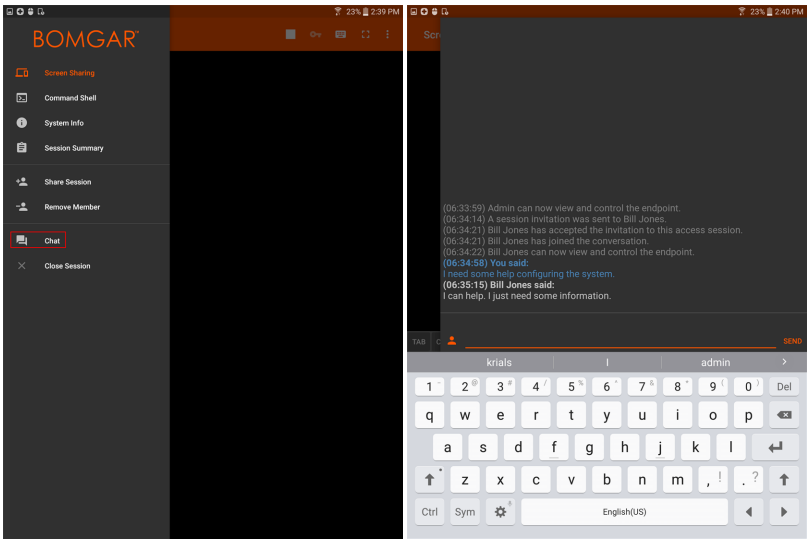
10. Appuyez sur l'icône de **clé**. L'icône de clé permet au système de voir vos informations d'authentification stockées pour accéder au point de terminaison

.



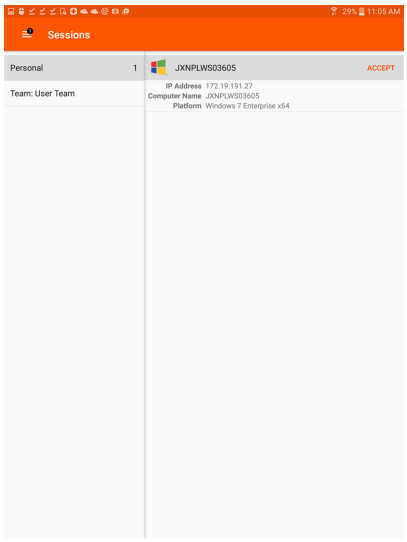
Utiliser la messagerie instantanée d'équipe pour discuter avec d'autres utilisateurs dans la console d'accès Android

En appuyant sur l'option **Messagerie**, vous pouvez discuter avec d'autres membres de l'équipe connectés. Si vous appartenez à une ou plusieurs équipes, sélectionnez l'équipe avec laquelle vous souhaitez discuter dans la liste. Vous pouvez discuter avec tous les membres de cette équipe ou sélectionner dans la liste le nom d'un membre pour discuter avec lui en privé.



Consulter les sessions d'accès dans la console d'accès Android

Dans la access console, les sessions d'accès actives sont divisées dans des files d'attente d'équipe. Appuyez sur l'option **Sessions** du menu pour afficher la liste des files d'attente configurées. Ces files d'attente reflètent les équipes qui ont été définies dans l'interface d'administration /login. Après avoir défini une équipe, il est possible d'accéder à une file d'attente dans la section **Sessions** de la access console.



La file d'attente **Personnelle** contient les sessions qu'un autre membre de l'équipe a partagées avec vous. Les files d'attente restantes représentent les équipes spécifiques dont vous êtes membre.

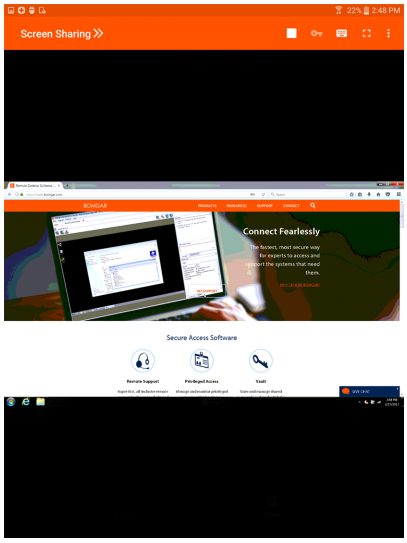
Appuyez sur le nom d'une file d'attente d'équipe pour afficher les sessions en cours. Le nombre à côté de l'option Session indique le nombre de sessions en cours dans cette file d'attente.

Remarque : *si une session a été partagée avec vous, appuyez sur la file d'attente où se trouve la session. Appuyez ensuite sur la session. Sélectionnez* ***Accepter****. Si vous acceptez une session, cette dernière s'ouvrira sur votre appareil.*

Partage d'écran avec le point de terminaison depuis la console d'accès Android

Si le partage d'écran ne se lance pas automatiquement, appuyez sur le bouton **Lecture** en haut de la page de **Partage d'écran** pour demander à voir et contrôler le système distant. Vous avez le contrôle total du clavier et de la souris du système distant, ce qui vous permet de travailler sur l'ordinateur distant comme si vous y étiez.

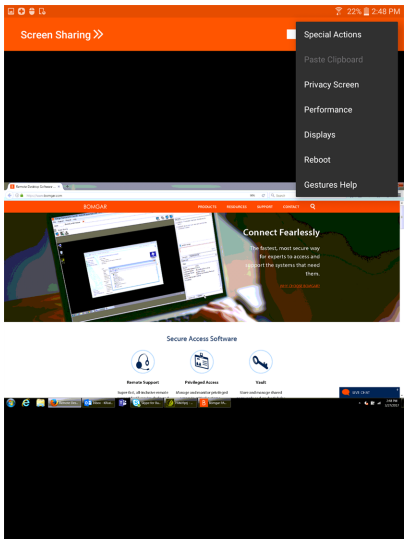
- Appuyez une fois pour faire un clic gauche.
- Appuyez deux fois pour faire un double clic.
- Placez votre doigt sur le curseur ou faites glisser pour bouger la souris.
- Appuyez deux fois sur un élément, puis faites-le glisser pour le déplacer.
- Pincez pour voir l'écran distant à sa taille réelle ou mis à l'échelle. Le zoom se produit où les doigts sont placés, où que se trouve le pointeur.
- Appuyez avec deux doigts pour faire un clic droit.
- Utilisez la molette de la souris en faisant glisser trois doigts.
- Appuyez avec trois doigts pour activer/désactiver le clavier.
- Maintenez appuyé pour trouver le curseur.



Outils de partage d'écran

Partage d'écran	Demandez ou arrêtez le partage d'écran.
Aide	Consultez les actions additionnelles disponibles lors du partage d'écran.
Clavier	Accédez au clavier afin d'écrire sur l'écran distant.
Options	Sélectionnez parmi les actions et outils additionnels du partage d'écran.
Plein écran	Affichez le bureau distant en mode plein écran.

Actions et outils additionnels du partage d'écran



Actions Spéciales - Exécutez une action spéciale sur le système distant. Les tâches disponibles varient en fonction de la configuration et du système d'exploitation distants.

Coller dans le presse-papiers - Collez les éléments dans le presse-papiers de votre appareil.

Écran de confidentialité - Désactivez l'affichage et l'entrée souris et clavier de l'utilisateur distant. L'interaction restreinte avec le point de terminaison n'est disponible que lors d'un accès à un ordinateur Windows ou MacOS. L'interaction restreinte avec le client n'est disponible que lors d'une assistance technique à un ordinateur Windows. Dans Windows Vista et les versions supérieures, le endpoint client doit être accru. Sur Windows 8, cette fonction est limitée à la désactivation du clavier et de la souris.

Performance - Définir le mode d'optimisation de la couleur d'affichage de l'écran distant. Si vous comptez principalement partager de la vidéo, sélectionnez **Vidéo optimisée** ; sinon, choisissez entre **Noir et blanc** (utilise moins de bande passante), **Quelques couleurs**, **Davantage de couleurs** ou **Toutes les couleurs** (utilise plus de bande passante). Les modes Vidéo optimisée et Toutes les couleurs vous permettent de voir votre fond d'écran.

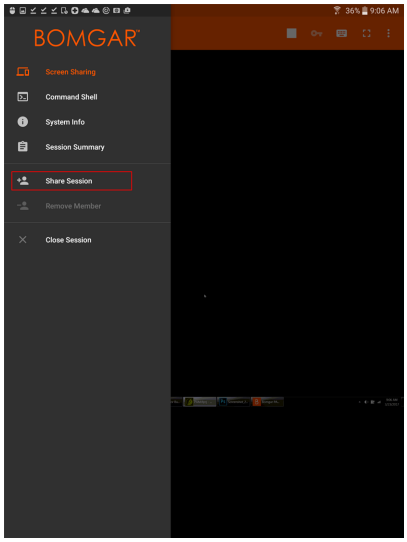
Affichages - Sélectionnez un autre écran distant à afficher. Le moniteur principal apparaît en surbrillance.

Redémarrer - Sélectionnez cette option pour redémarrer le système distant.

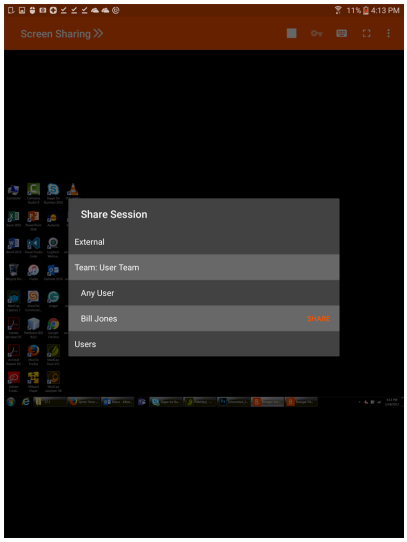
Aide à la navigation - Sélectionnez cette option pour obtenir des conseils de navigation liés à la console d'accès mobile.

Partage d'une session avec d'autres utilisateurs dans la console d'accès Android

Pour partager une session avec un autre membre d'équipe, appuyez sur l'option **Partager la session** dans le menu.



Vous pouvez sélectionner un utilisateur répertorié dans les équipes affichées pour l'inviter à rejoindre la session. Vous pouvez envoyer plusieurs invitations si vous souhaitez que plusieurs membres d'une équipe rejoignent votre session. Les utilisateurs sont répertoriés ici uniquement s'ils sont connectés à la access console, ou si leur mode Disponibilité étendue est activé.



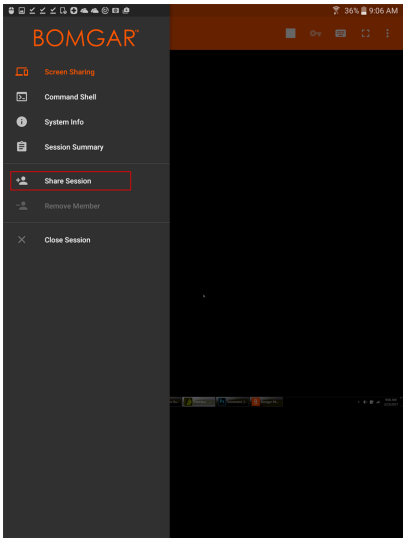
Si vous êtes autorisé à partager des sessions avec des utilisateurs qui ne sont pas membres de vos équipes, des équipes supplémentaires seront affichées, à condition qu'elles comprennent au moins un membre connecté à la access console ou disposant du mode Disponibilité étendue activé.

Seul le propriétaire de la session peut envoyer des invitations. Les invitations n'expirent pas tant que vous restez propriétaire de la session. Un utilisateur ne peut pas disposer de plusieurs invitations actives pour rejoindre une même session. L'invitation disparaîtra si :

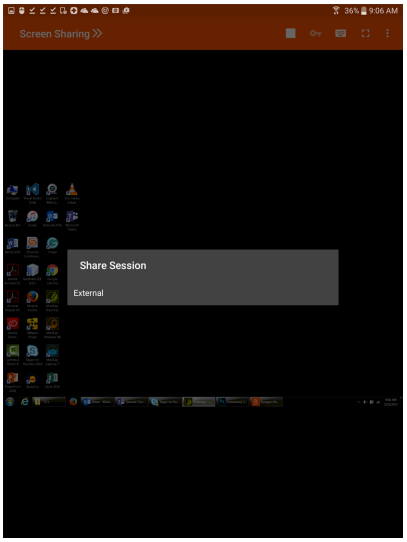
- L'utilisateur qui invite annule l'invitation.
- L'utilisateur qui invite quitte la session.
- La session se termine.
- L'utilisateur invité accepte l'invitation.

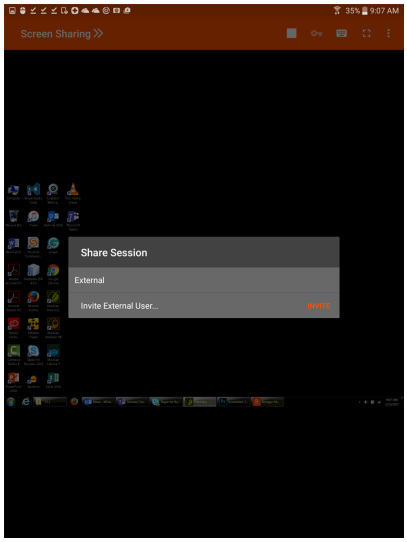
Inviter un utilisateur externe à rejoindre une session dans la console d'accès Android

Dans une session, un utilisateur peut demander à un utilisateur externe de participer à une session de manière ponctuelle. L'utilisateur qui invite doit appuyer sur le menu déroulant et sélectionner le menu **Partager la session**.



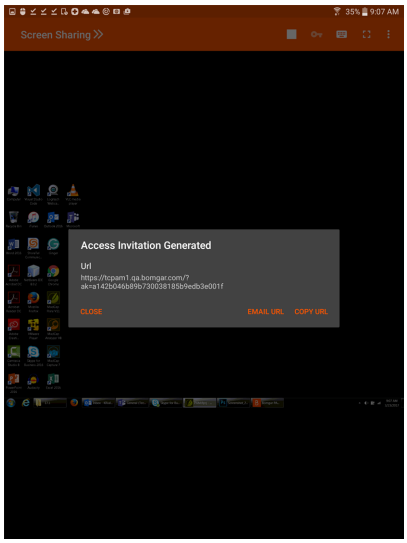
Sélectionnez **Externe**, puis **Inviter un utilisateur externe**. Appuyez sur le bouton **Inviter** pour continuer.





Sélectionnez ensuite une règle de sécurité. Ces règles sont créées dans l'interface d'administration et définissent le niveau d'autorisation dont dispose l'utilisateur externe. Lorsque vous sélectionnez une règle, la description complète s'affiche en dessous.

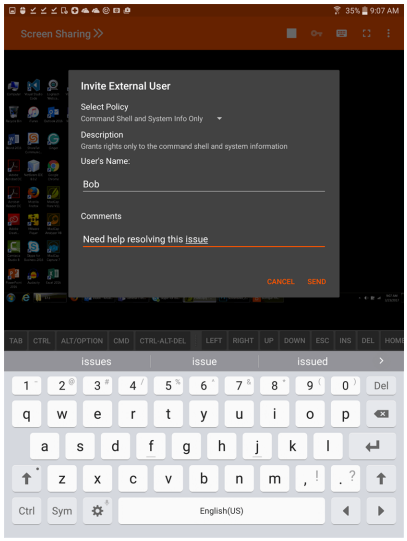
Saisissez le nom de l'utilisateur externe. Ce nom apparaît dans la fenêtre de messagerie instantanée et dans les rapports. Saisissez ensuite des commentaires sur le motif de l'invitation de cet utilisateur. Cliquez sur **Envoyer**. Une nouvelle boîte de dialogue contenant l'URL d'invitation s'affiche.



En fonction des options sélectionnées par votre administrateur, il se peut que vous puissiez envoyer des invitations depuis votre adresse e-mail locale ou depuis une adresse e-mail du serveur. Vous pouvez aussi copier l'URL directe pour la donner à l'utilisateur externe. L'utilisateur externe doit télécharger et exécuter l'installeur de la access console, qui correspond à une procédure raccourcie de l'installation complète de la access console.

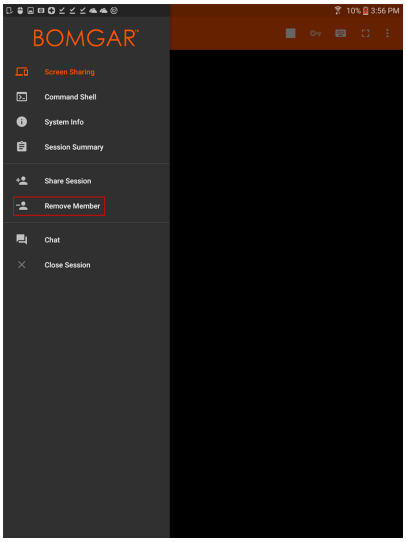
L'utilisateur externe peut accéder uniquement à l'onglet de **session** et dispose de privilèges restreints. L'utilisateur externe ne peut jamais être le propriétaire de la session. Lorsque l'utilisateur qui invite quitte la session, l'utilisateur externe est déconnecté.

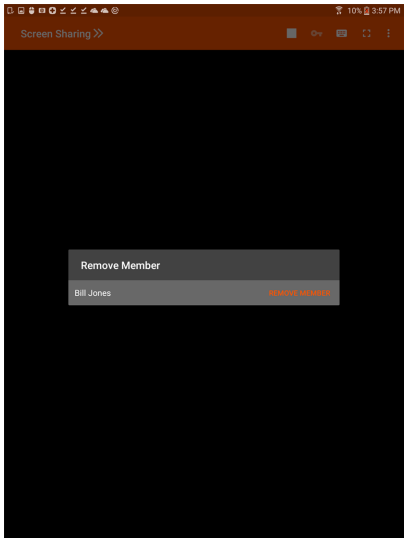
Vous pouvez inviter plus d'un utilisateur externe à une session.



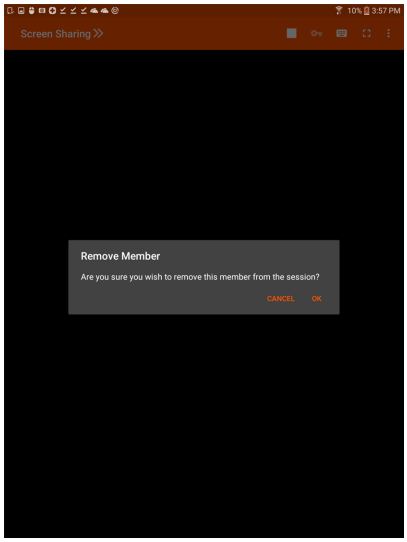
Supprimer un membre de la session dans la console d'accès Android

Il est possible de supprimer un autre utilisateur d'une session partagée. Dans le menu, sélectionnez l'option **Supprimer membre** dans le menu.





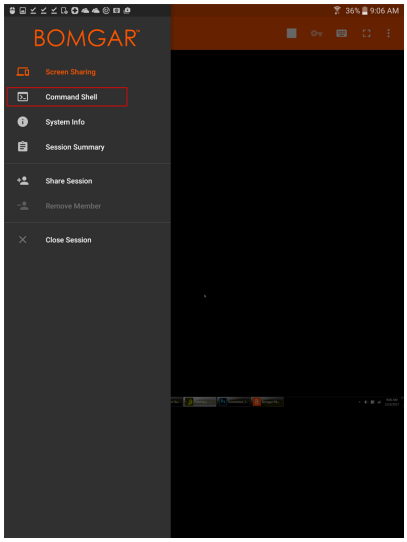
Sélectionnez les participants que vous souhaitez supprimer. Appuyez ensuite sur **Supprimer**. Appuyez sur **OK** dans l'invite suivante. vous devez être le propriétaire de la session pour supprimer un autre membre.



Ouvrir l'interpréteur de commandes sur un point de terminaison distant en utilisant la console d'accès Android

L'interpréteur de commandes distant permet aux utilisateurs privilégiés d'ouvrir une interface de ligne de commande virtuelle sur des ordinateurs distants. Les utilisateurs peuvent ensuite saisir localement pour exécuter les commandes sur le système distant. Vous pouvez travailler depuis plusieurs interpréteurs.

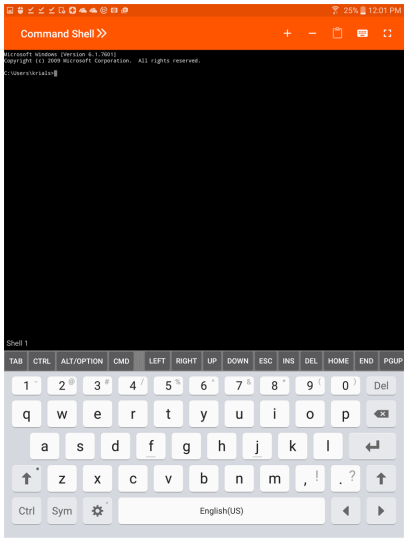
Pour accéder à un interpréteur de commandes, sélectionnez **Interpréteur de commandes** dans le menu. Appuyez sur le symbole **+** pour ouvrir un nouvel interpréteur.



Votre administrateur peut aussi activer l'enregistrement d'interpréteur distant afin de permettre la lecture ultérieure d'une vidéo de chaque instance d'interpréteur à partir du rapport de session. Si l'enregistrement d'interpréteur est activé, une transcription de l'interpréteur de commandes est également disponible.

Des commandes et des caractères de clavier supplémentaires sont disponibles au-dessus du clavier standard. Il est possible de faire défiler d'autres touches vers la gauche ou vers la droite pour afficher plus d'options.

Si plusieurs interpréteurs de commandes sont ouverts, vous pouvez faire défiler l'écran à droite et à gauche pour passer d'un interpréteur à l'autre. Le nom de l'interpréteur actuel est affiché dans le coin inférieur gauche de la fenêtre.



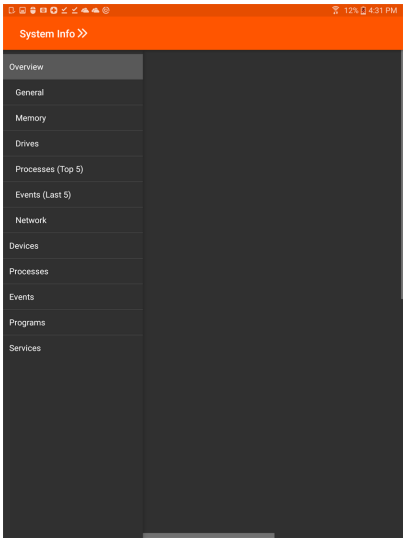
Outils d'interpréteur de commandes

+	Ouvrir un nouvel interpréteur pour exécuter plusieurs instances d'invite de commande.
—	Fermer l'interpréteur de commandes actuel. L'exécution des autres interpréteurs de commandes n'est pas interrompue.

	Accéder au clavier pour écrire des commandes dans l'interpréteur de commandes.
	Accéder au menu de l'interpréteur de commandes pour effectuer des actions supplémentaires (voir d'autres sessions d'interpréteur ou passer en affichage plein écran, par exemple).

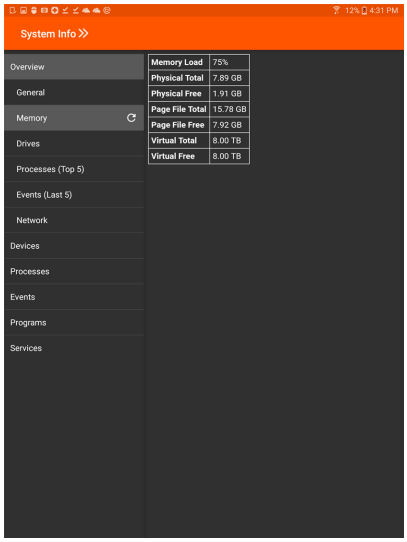
Consulter les informations système du point de terminaison distant dans la console d'accès Android

Les utilisateurs peuvent afficher un instantané complet des informations système du point de terminaison pour accélérer le diagnostic et la résolution du problème. Les informations système disponibles varient en fonction du système d'exploitation distant et de la configuration de l'ordinateur distant.



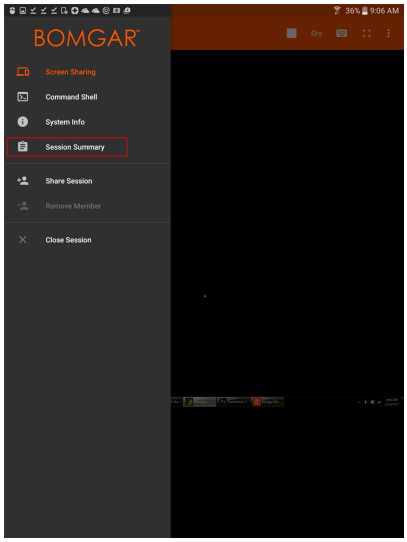
Sélectionnez des noms de catégories successives pour accéder aux données que vous voulez afficher.

Une fois que les données se sont propagées, vous pouvez appuyer sur le bouton **Actualiser** pour récupérer les données les plus récentes.



Consulter un résumé de la session d'accès et ajoutez des remarques dans la console d'accès Android

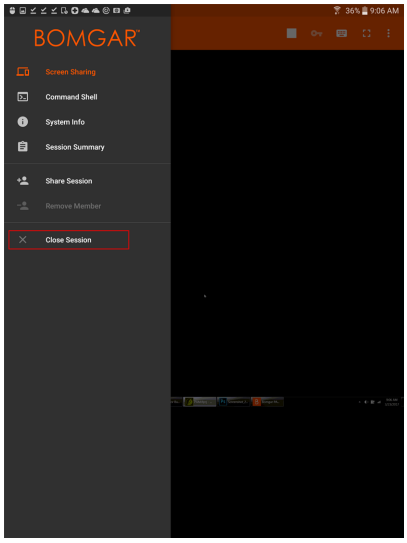
La page **Résumé** fournit une vue d'ensemble du système distant auquel l'on accède.



Vous pouvez aussi ajouter des notes sur la session en faisant défiler l'écran sur la gauche. Les notes peuvent être envoyées par un utilisateur et rappelées par un autre pour consultation. Ces notes sont également disponibles dans le rapport de session.

Fermer la session dans la console d'accès Android

Pour quitter une session, appuyez sur **Fermer la session** dans le Menu.



Si vous êtes le propriétaire de la session, **Mettre fin à la session** ferme la page de session dans votre access console et retire tous les membres additionnels qui partageaient la session.

Si vous n'êtes pas le propriétaire de la session et que vous appuyez sur **Quitter la session**, vous serez exclu de la session. La session continuera avec le propriétaire de la session. Si d'autres membres partagent la session, ils resteront dans la session.