BeyondTrust

Privileged Remote Access
Console d’accès iOS 2.2.4

TC:9/25/2020

Table des matières

Guide de la console d'accès pour iOS

Ce guide est destiné à vous aider à installer BeyondTrust sur votre appareil iOS et à comprendre les fonctionnalités de la console d'accès iOS. BeyondTrust vous permet d'accéder à des points de terminaison distants en vous y connectant par le biais du Secure Remote Access Appliance.

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

Installez la console d'accès sur iOS

La console d'accès BeyondTrust pour iOS est disponible en téléchargement gratuit depuis l'App Store d'Apple. Depuis votre appareil iOS, cherchez « BeyondTrust Console d'Accès » (ou en anglais, BeyondTrust Representative Console) dans l'App Store, puis installez l'appli.

Si votre société utilise une boutique d'applis d'entreprise pour distribuer les applis, contactez l'assistance technique de BeyondTrust pour rendre l'appli de console d'accès BeyondTrust disponible sur la boutique d'applis.

Pour exécuter la console d'accès BeyondTrust sur votre appareil, la version de votre logiciel BeyondTrust doit être 15.2 ou plus, et votre appareil doit être équipé d'iOS 7 au moins.

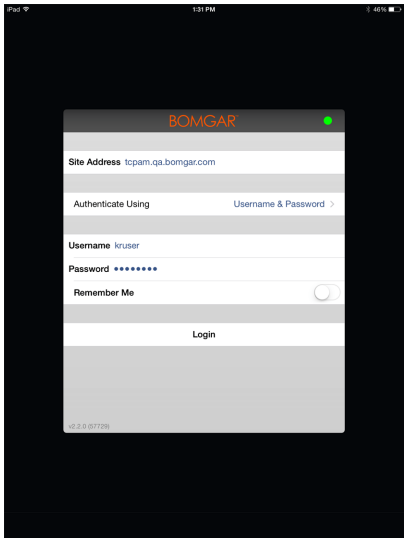
Remarque : *seule la console d'accès BeyondTrust peut être utilisée avec un site Privileged Remote Access (PRA). La console du technicien d'assistance BeyondTrust ne peut pas être utilisée pour se connecter à un site PRA, et la console d'accès BeyondTrust ne peut pas être utilisée pour se connecter à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

IMPORTANT !

Votre serveur Secure Remote Access Appliance doit être équipé d'un certificat SSL valide signé par une autorité de certificat. BeyondTrust ne prend pas en charge l'utilisation de certificats auto-signés pour la console d'accès iOS. Une fois que vous avez appliqué un certificat SSL signé par une AC à votre Secure Remote Access Appliance, contactez l'assistance technique de BeyondTrust. Votre technicien service client créera une nouvelle version logicielle s'intégrant à votre certificat SSL. Avec cette version mise à jour installée sur votre serveur, vous pouvez exécuter la console d'accès BeyondTrust sur votre appareil pour accéder à des points de terminaison depuis pratiquement n'importe où.

Connectez-vous à la console d'accès pour iOS

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



> ***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 uniquement ou de façon permanente. Cette restriction ne s'applique pas aux invites d'accès.*

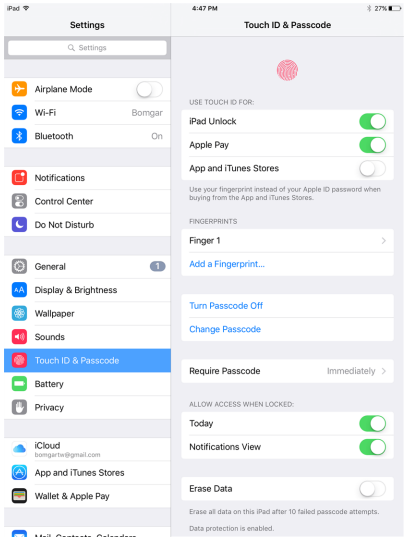
Autrement, si vous avez été invité par un autre utilisateur à rejoindre une session d'accès une fois seulement, appuyez sur **S'authentifier en utilisant** puis sélectionnez **Clé d'invitation d'accès**.

Saisissez la clé d'invitation d'accès avec votre invitation, puis appuyez sur **Connexion**.

Connectez-vous à la console Privileged Remote Access BeyondTrust pour iOS à l'aide de Touch ID

Touch ID est le capteur d'empreinte digitale disponible sur les appareils iOS suivants :

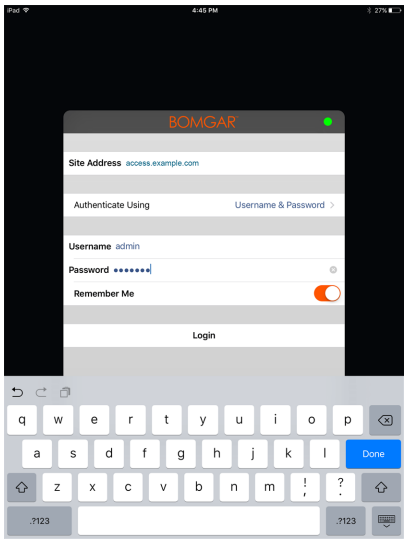
- **iPhone 5s ou ultérieur**
- **iPad Pro**
- **iPad Air 2**
- **iPad Mini 3 ou ultérieur**



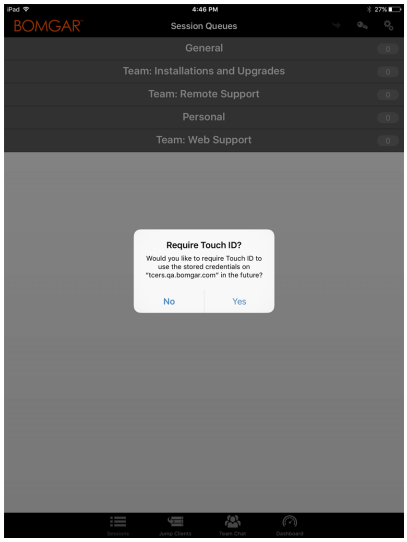
Grâce à cette fonction, vous pouvez déverrouiller votre appareil ou autoriser d'autres actions depuis votre iPhone ou votre iPad en utilisant votre empreinte digitale comme code. Pour en apprendre davantage sur Touch ID et savoir comment l'activer sur votre appareil, veuillez consulter À propos de la sécurité Touch ID pour iPhone et iPad à l'adresse https://support.apple.com/en-us/HT204587 et Utiliser Touch ID sur iPhone et iPad à l'adresse https://support.apple.com/en-us/HT201371.

À partir de la version 16.1 de l'Privileged Remote Access BeyondTrust, vous pouvez utiliser Touch ID pour vous connecter à la console d'accès mobile pour iOS. La même authentification par empreinte digitale utilisée pour déverrouiller votre appareil peut être utilisée pour obtenir l'accès à votre console d'accès. Suivez les étapes ci-dessous pour activer l'authentification Touch ID pour votre console d'accès mobile.

1. Ouvrez l'application de console d'accès mobile BeyondTrust.
2. Saisissez le nom d'hôte de votre site BeyondTrust, par exemple access.example.com, avec vos informations d'authentification.
3. Vérifiez que l'option **Se souvenir de moi** est activée. Cliquez sur **Connexion**.



4. Appuyez sur **Oui** sur la demande Touch ID qui apparaît à la connexion.
5. Déconnectez-vous de la console d'accès.



6. Appuyez sur l'option **Connexion avec Touch ID** qui apparaît sur l'écran de connexion.

7. Placez votre doigt sur le bouton **Accueil** de votre appareil pour finaliser la connexion à la console du technicien d'assistance.

> ***Remarque :*** *vous pouvez à tout moment vous connecter en utilisant votre nom d'utilisateur et votre mot de passe en appuyant sur l'option* ***Retour à la connexion****.*

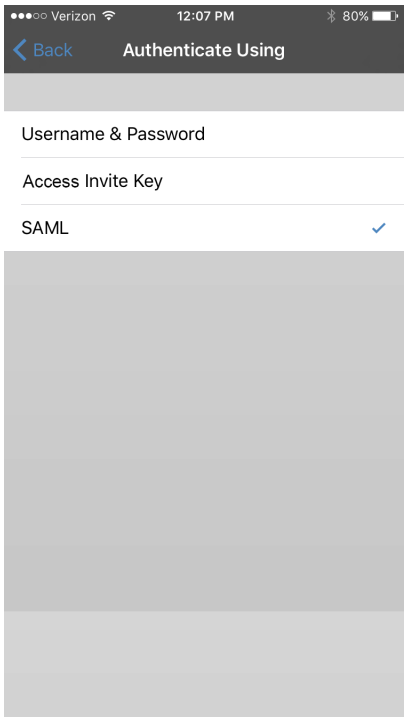
Connectez-vous à la console d'accès iOS à l'aide de SAML mobile

SAML mobile offre une méthode simple pour s'identifier en toute sécurité sur la console d'accès iOS. 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-après pour vous connecter à la console d'accès mobile à l'aide de SAML.

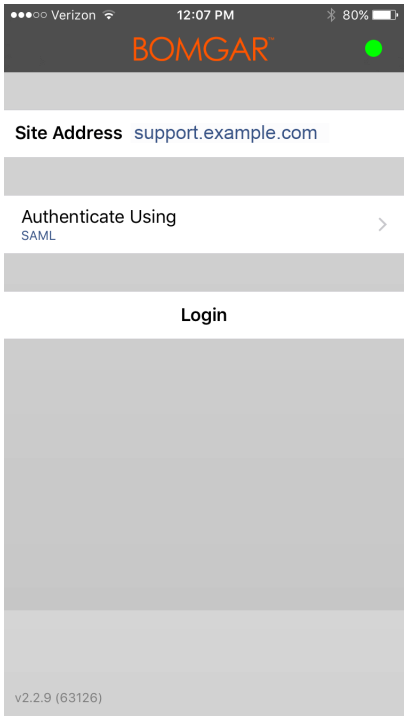
> ***Remarque :*** *Avant de vous connecter à la console d'accès iOS par le biais de SAML, consultez* ***Utilisateurs et sécurité > Fournisseurs de sécurité*** *pour vous assurer que le fournisseur SAML est bien configuré pour votre environnement administratif /login. Si SAML n'est pas configuré dans /login, SAML n'est pas disponible en tant que méthode d'authentification pour la console d'accès iOS. 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 console d'accès de votre appareil iOS.
2. Appuyez sur **S'authentifier avec** depuis l'écran de connexion.

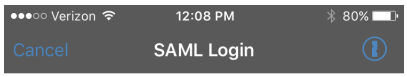
3. Sélectionnez le langage **SAML**.



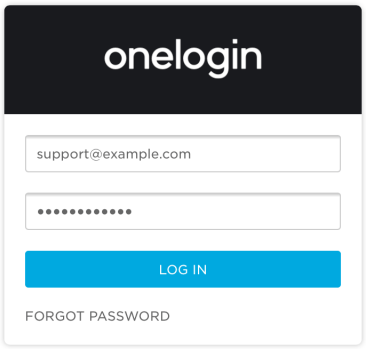
4. Appuyez sur **Connexion**. Votre page de fournisseur SAML apparaît.



5. Sur votre page de fournisseur, saisissez vos informations d'authentification.



> ***Remarque :*** *si une banque de mots de passe est configurée sur votre appareil, vous pouvez appuyer sur le symbole de verrouillage des touches en haut à droite pour accéder à votre banque de mots de passe et à vos informations d'authentification.*



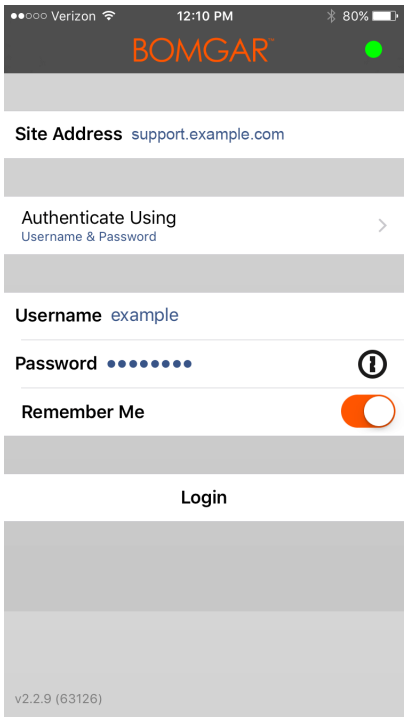
6. Appuyez sur **Connexion** pour accéder à la console.

Se connecter à la console d'accès iOS avec un gestionnaire de mots de passe

Les gestionnaires de mots de passe, comme 1Password et LastPass, vous permettent de conserver vos mots de passe en toute sécurité. Pour en savoir plus sur l'extension propriétaire 1Password, veuillez consulter Security is not just a feature. It's our foundation. (La sécurité n'est pas qu'une simple fonction. C'est notre cœur de métier.) sur https://1password.com/security/. Suivez les étapes ci-après pour utiliser 1Password, ou tout autre gestionnaire de mots de passe, et accéder à la console d'accès iOS de BeyondTrust.

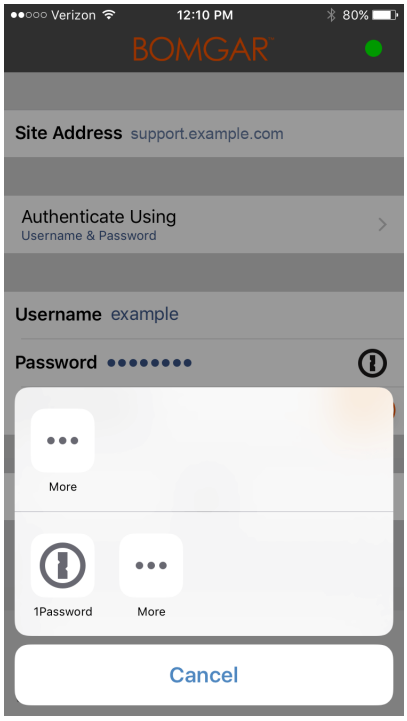
> ***Remarque :*** *Avant d'utiliser un gestionnaire de mots de passe à l'aide de la console d'accès iOS de BeyondTrust, vérifiez que vous avez bien configuré un compte avec le gestionnaire de mots de passe et que l'application est synchronisée avec votre appareil.*

1. Ouvrez l'appli de la console d'accès sur votre appareil iOS.
2. Appuyez sur le symbole de verrouillage de touches du champ **Mot de passe**.

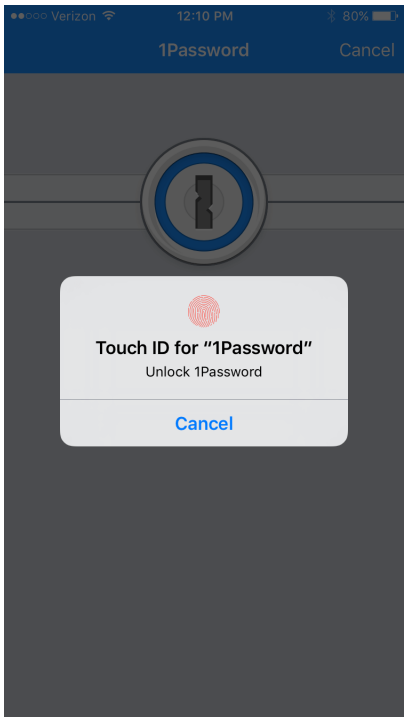


3. À partir de l'invite, appuyez sur le gestionnaire de mots de passe de votre choix pour être redirigé vers la page de connexion du gestionnaire de mots de passe.

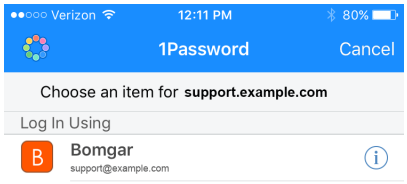
> ***Remarque :*** *si le gestionnaire de mots de passe n'est pas configuré sur l'appareil, le symbole de verrouillage des touches n'est pas visible.*



4. Si Touch ID est activé, vous aurez la possibilité d'utiliser votre empreinte digitale pour vous identifier et ouvrir l'application. Si Touch ID n'est pas activé sur votre appareil, il vous faudra saisir un mot de passe pour vous identifier.



5. Lorsque vous êtes connecté, le gestionnaire de mots de passe affiche les comptes pouvant accéder à la console. Appuyez sur le compte que vous souhaitez utiliser pour accéder à la console.



Définissez les préférences dans la console d'accès iOS

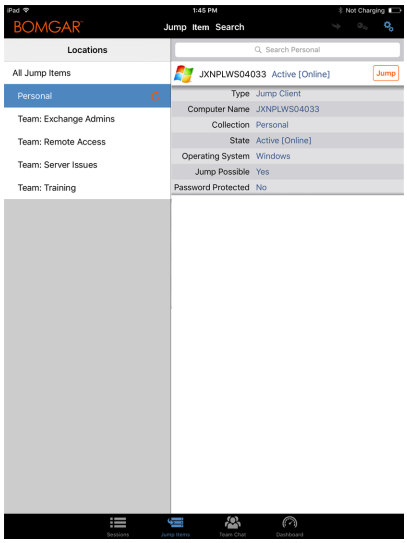
Pour changer vos préférences sur un iPad, appuyez sur l'icône **Engrenage** dans le coin supérieur droit de l'écran.

Pour changer vos préférences sur un iPhone, appuyez sur l'icône **Menu** dans le coin supérieur droit de l'écran.

Appuyez ensuite sur **Préférences**.

Alertes sonores	iPad et iPhone	Si cette option est activée, votre appareil jouera des alertes sonores pour certains évènements se produisant dans la console d'accès.
Pointeur de souris absolu	iPad et iPhone	Si cette option est désactivée, vous devez placer votre doigt sur le pointeur de la souris et faire glisser pour déplacer la souris. Maintenez appuyé pour trouver le pointeur de la souris lorsque la position réelle est désactivée. Si cette option est activée, vous pouvez placer le pointeur de la souris là où votre doigt touche l'écran. Lorsque le positionnement absolu est activé, maintenez appuyé pour ouvrir un menu volant à partir duquel vous pouvez choisir différentes méthodes de clic.
Secouez l'appareil pour obtenir de l'aide en vue session	iPad uniquement	Si cette option est activée, vous pouvez secouer l'appareil pour générer les gestes de partage d'écran pendant une session d'accès.

Utilisez les éléments de Jump pour accéder à des points de terminaison depuis la console d'accès iOS



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. Les types d'éléments de Jump suivants sont gérés par la console d'accès 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'onglet **Éléments de Jump** en haut de l'écran.

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.

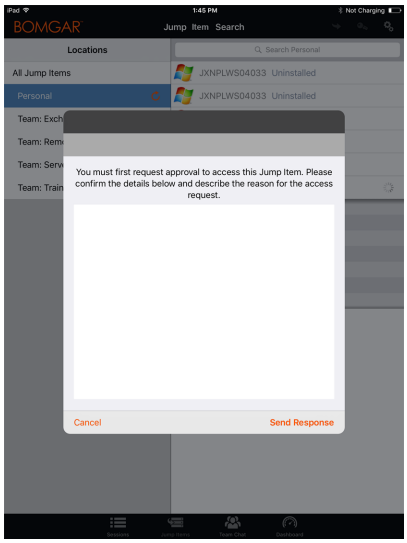
Selon les autorisations définies par l'administrateur pour votre compte, un utilisateur final ou une tierce partie peuvent être invités à accepter ou à refuser la session. En l'absence de réponse dans le délai imparti, la session démarre ou est annulée, ici encore en fonction des autorisations de votre compte.

Autorisation pour utilisateur final et tierce partie

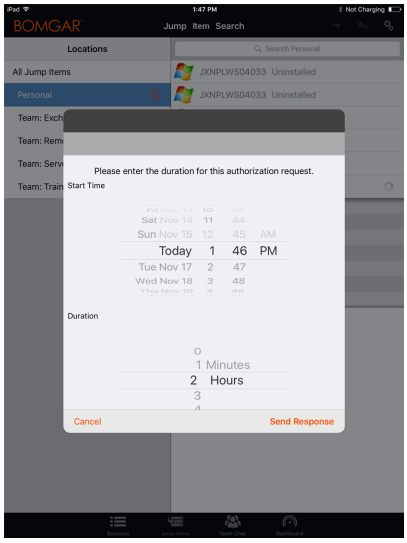
En fonction de la configuration des éléments de Jump dans l'interface d'administration /login, un élément de Jump peut être associé à une règle de Jump, et la règle peut définir une composante d'autorisation qui vous force à demander une autorisation auprès d'un tiers ou d'un administrateur avant de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

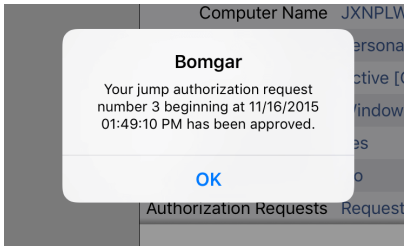
Après avoir appuyé sur le bouton Jump et sollicité l'accès, une invite vous demande de justifier votre demande d'accès au système.



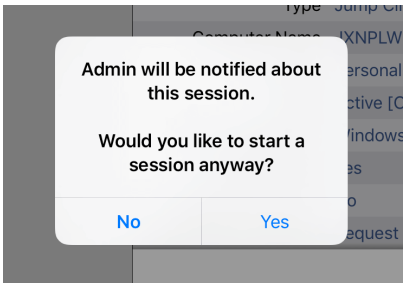
Vous devez ensuite indiquer à quel moment et pour combien de temps vous accéderez au système.



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. (missing or bad snippet)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.



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.



Informations d'authentification automatiques pour la console d'accès mobile

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.

Connectez-vous aux points de terminaison en utilisant l'injection d'informations d'authentification depuis la console d'accès iOS

Lorsque vous accédez à un Jump Client basé sur Windows à travers la console d'accès 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.

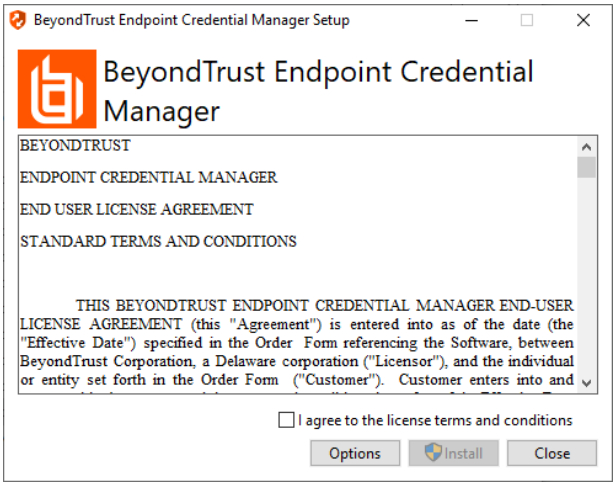
Installez et configurez le gestionnaire d'informations d'authentification de point de terminaison

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 (GIAPT) BeyondTrust.

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

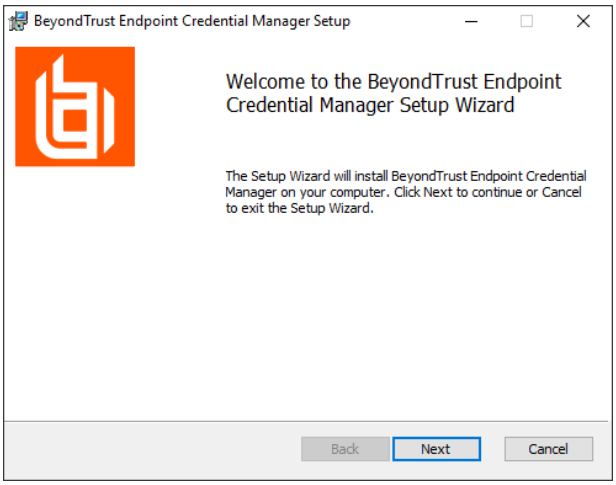
1. Pour commencer, téléchargez le gestionnaire d'informations d'authentification de point de terminaison (GIAPT) BeyondTrust auprès de BeyondTrustl'assistance technique à l'adresse beyondtrustcorp.service-now.com/csm
2. Lancez l'assistant de configuration du gestionnaire d'informations d'authentification 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 du GIAPT, cliquez sur le bouton **Options** pour choisir l'emplacement d'installation.

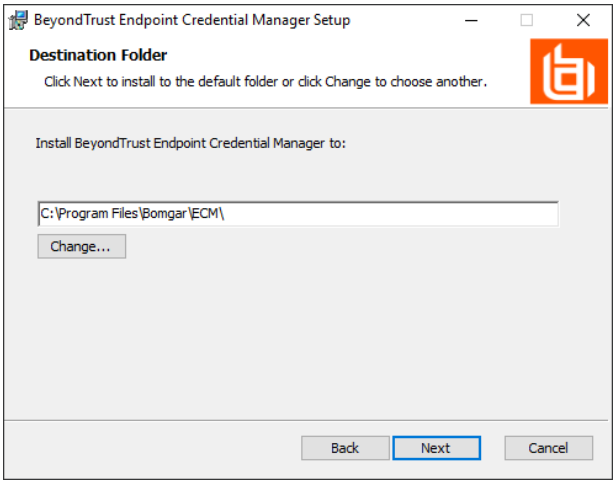


> ***Remarque :*** *vous ne pourrez pas poursuivre l'installation si vous n'acceptez pas le CLUF.*

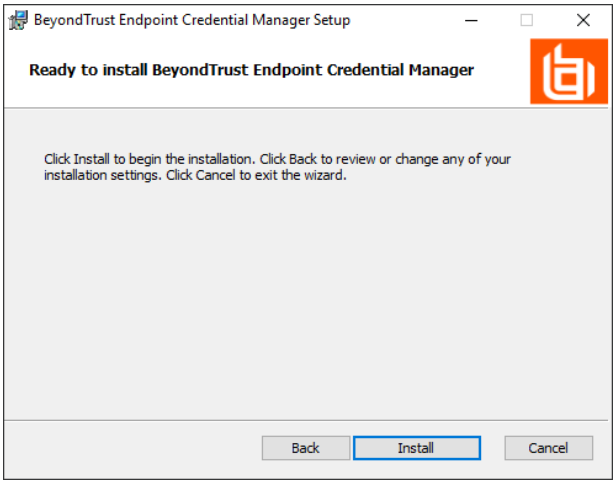
4. Cliquez sur **Suivant** dans l'écran de bienvenue.



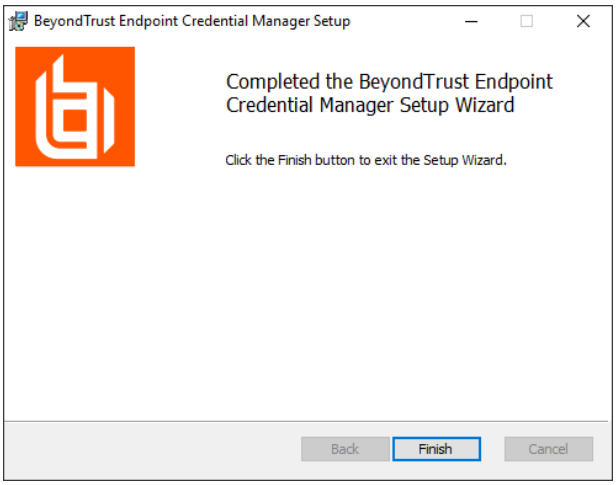
5. Choisissez un emplacement pour le gestionnaire d'informations d'authentification, puis cliquez sur **Suivant**.



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**.

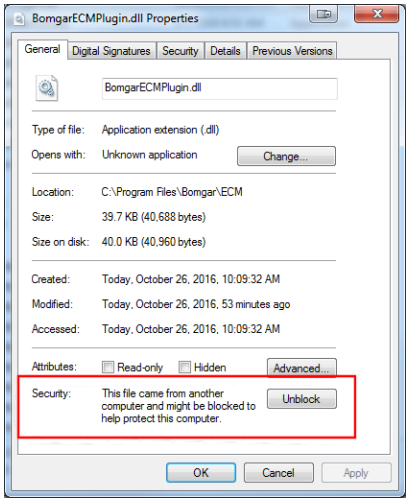


> ***Remarque :*** *pour optimiser le temps de disponibilité, les administrateurs peuvent installer jusqu'à 5 GIAPT sur plusieurs machines Windows pour communiquer avec le même site sur le Secure Remote Access Appliance. Une liste des GIAPT connectés au site du serveur est disponible sur* ***/login > État > Information > Clients GIAPT****.*

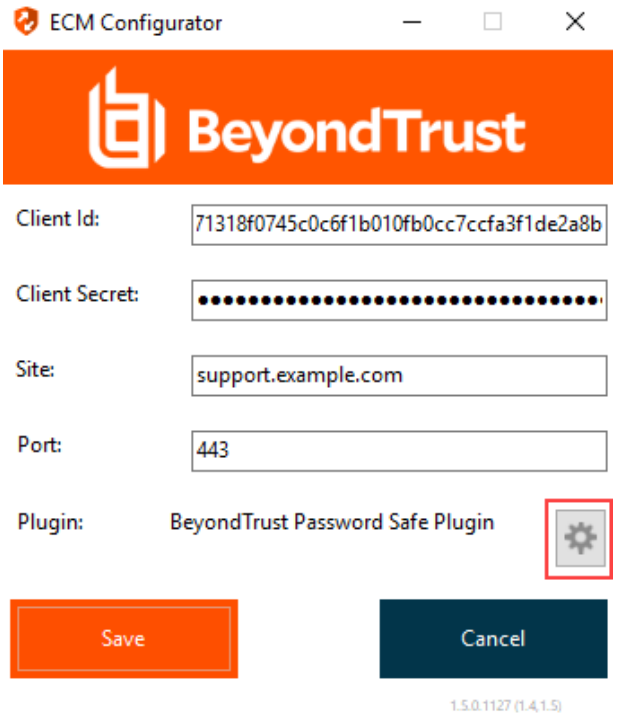
> ***Remarque :*** *lorsque plusieurs GIAPT sont connectés au site BeyondTrust, le Secure Remote Access Appliance achemine les demandes vers le GIAPT ayant été le plus longtemps connecté au serveur.*

Installer et configurer le plug-in

1. Une fois que le GIAPT 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 GIAPT** 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 :
    a. Tout d'abord, vérifiez que la DLL n'est pas bloquée. Faites un clic droit sur la DLL et sélectionnez **Propriétés**.
    b. 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.
    c. Répétez ces étapes pour toutes les autres DLL fournies avec le plug-in.
    d. Dans le configurateur, cliquez sur le bouton **Choisir plug-in...** et accédez à l'emplacement de la DLL du plug-in.



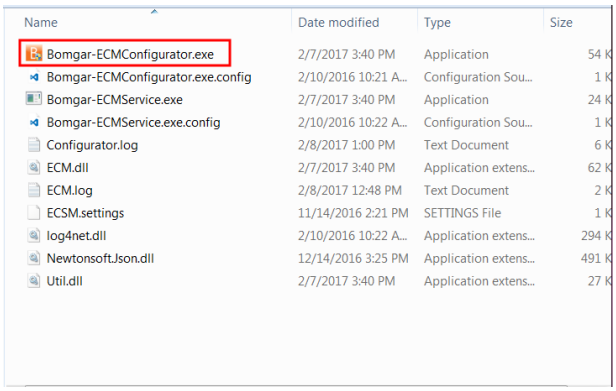
4. Cliquez sur l'icône en forme d'engrenage dans la fenêtre Configurateur pour configurer les paramètres du plug-in.



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

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

1. Trouvez le configurateur GIAPT 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.



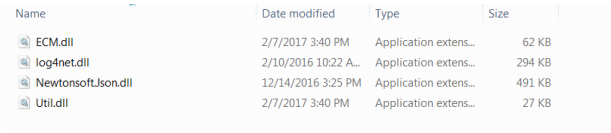
3. Lorsque le configurateur GIAPT s'ouvre, remplissez les champs. Tous les champs sont obligatoires.

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 le GIAPT 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 du GIAPT s'ouvre.
5. Collez vos fichiers de plug-in dans le dossier.
6. Ouvrez le fichier plug-in pour commencer le chargement.

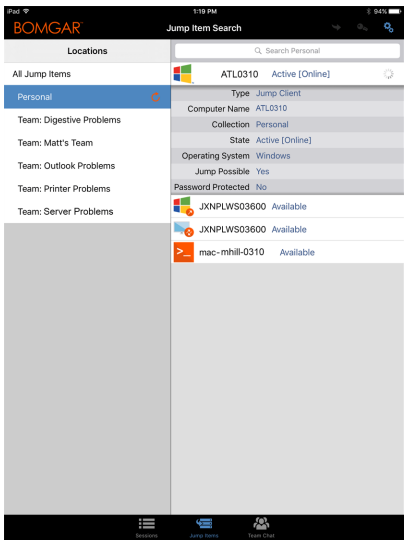


Remarque : *si vous vous connectez à la banque de mots de passe, une configuration supplémentaire au niveau plug-in peut être requise. Les besoins de plug-in varient en fonction du magasin d'informations d'authentification connecté.*

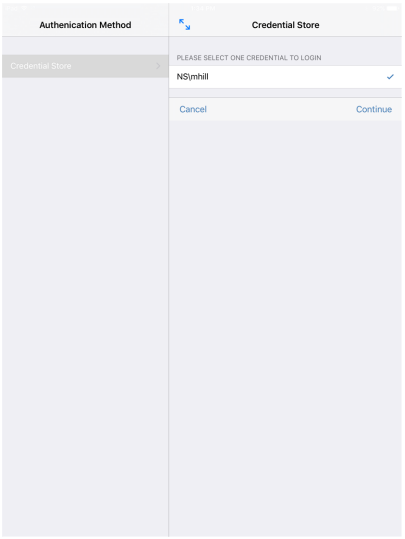
Utiliser l'injection d'informations d'authentification pour accéder à des points de terminaison

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.

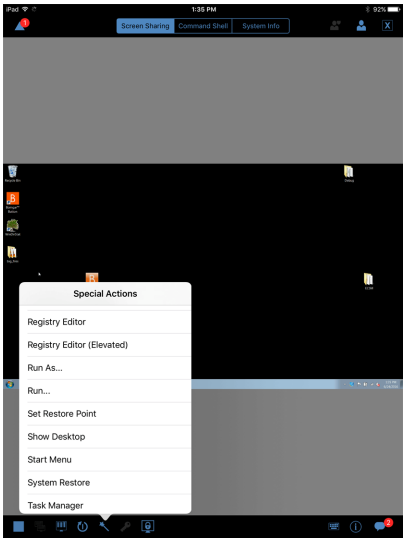
1. Allez à votre liste d'**éléments de Jump**.
2. Appuyez sur l'élément de Jump auquel vous souhaitez accéder.
3. Appuyez sur **Jump**.



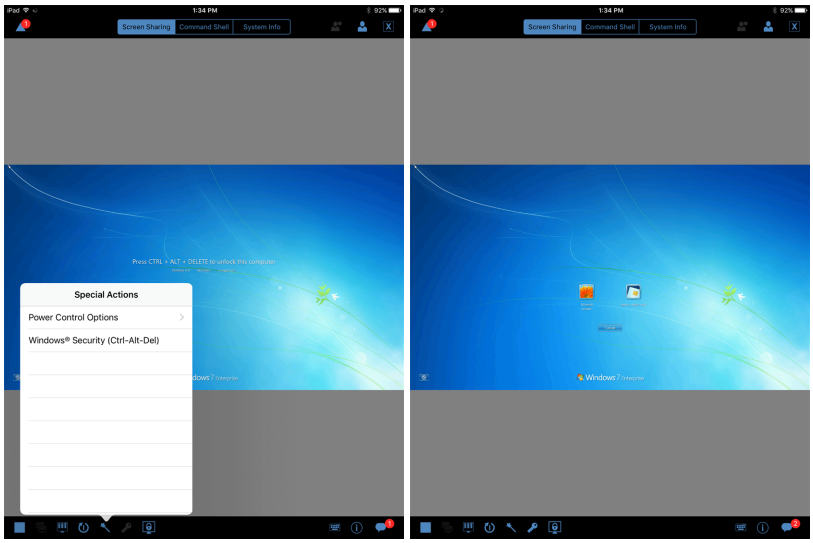
4. Appuyez sur **Magasin d'informations d'authentification**.
5. Appuyez sur les informations d'authentification que vous souhaitez utiliser pour accéder au système.
6. Appuyez sur **Continuer**.



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...**.



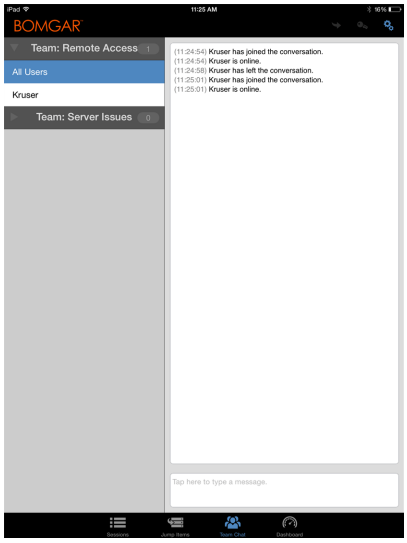
9. Appuyez sur **Sécurité Windows (Ctrl-Alt-Suppr)**.

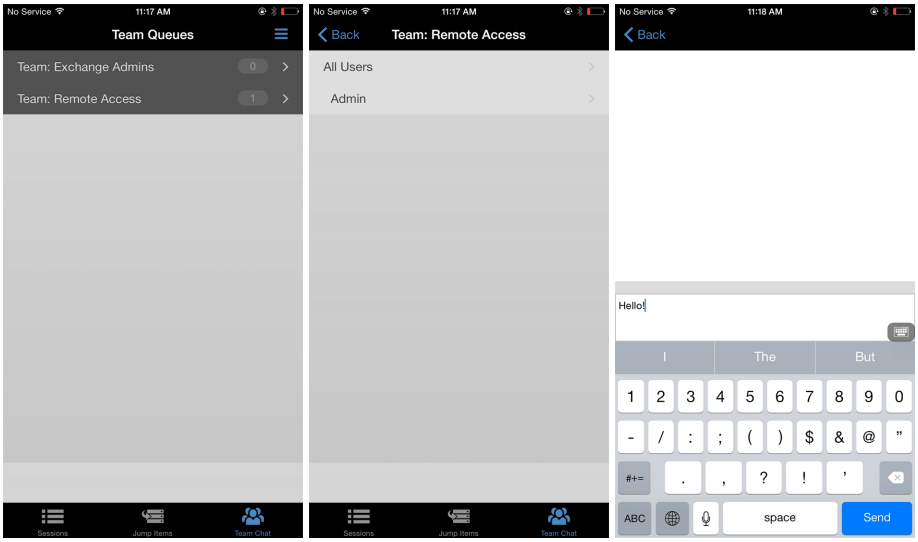


10. Appuyez sur l'icône de **clé**. L'icône de clé permet au système de voir vos informations d'authentification stockées pour accéder au point de terminaison.

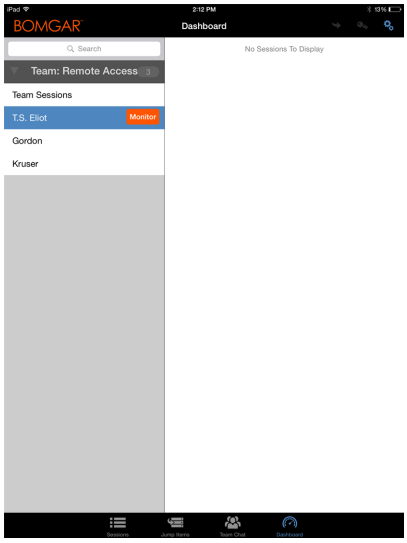
Discutez avec d'autres utilisateurs connectés dans la console d'accès iOS

En appuyant sur l'icône **Messagerie instantanée de l'équipe** en bas de l'écran, vous pouvez discuter avec d'autres membres d'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 un nom dans la liste des membres pour dialoguer avec lui en privé.





Gérez les membres d'équipe dans le tableau de bord (iPad uniquement)



Le tableau de bord permet aux utilisateurs privilégiés de voir et de surveiller les sessions en cours, permettant une supervision administrative pour aider à la gestion du personnel. D'après les rôles attribués sur la page **Équipes** de l'interface d'administration, les chefs d'équipe peuvent surveiller les membres d'une équipe donnée, et les responsables d'équipe peuvent surveiller les chefs et les membres de cette équipe.

Si un utilisateur est responsable ou chef d'une ou de plusieurs équipes, l'icône du tableau de bord s'affichera en bas de l'écran. Sur le tableau de bord, seuls les membres d'équipe connectés de rang inférieur pour l'équipe sélectionnée apparaîtront.

En outre, si cela a été configuré dans l'interface /login, un responsable ou chef d'équipe peut surveiller des membres d'équipe de rang inférieur même sans sessions en cours, tant que ces utilisateurs sont connectés à la console.

Sélectionnez l'utilisateur dont vous voulez voir l'écran, puis cliquez sur le bouton **Surveiller**. Ceci ouvrira une nouvelle page dans votre console d'accès, affichant soit l'intégralité de l'écran de l'ordinateur de l'utilisateur soit uniquement la console d'accès, en fonction des paramètres d'administration.

Au sein d'une équipe, un utilisateur ne peut gérer que ceux ayant un rang inférieur. Sachez toutefois que les rôles s'appliquent strictement par équipe. Ainsi, un utilisateur peut être en mesure d'administrer un autre utilisateur dans une équipe, sans pouvoir administrer ce même utilisateur dans une autre.

Utilisez 3D Touch pour l'accès mobile

3D Touch est une fonction sensible à la pression disponible sur iPhone 6s et les modèles plus récents.

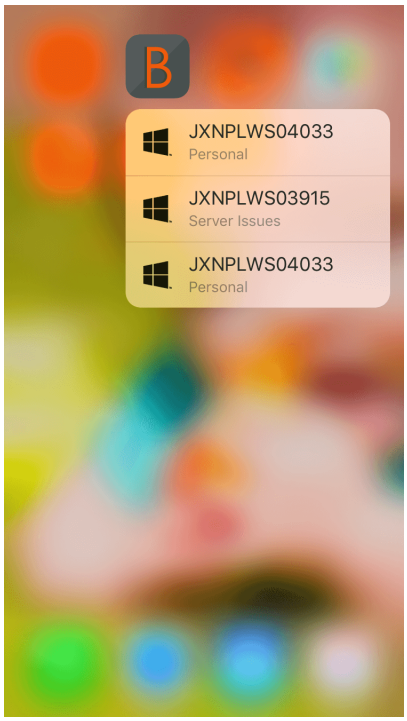
Cette fonction vous permet d'appuyer plus ou moins fort sur l'écran pour utiliser les actions Peek et Pop. Celles-ci vous permettent d'obtenir un aperçu de contenu et d'exécuter des commandes sur votre iPhone 6s/6s Plus sans avoir besoin d'ouvrir complètement une application. Pour en savoir plus sur 3D Touch, Peek et Pop, veuillez consulter Profiter des avantages de 3D Touch sur https://developer.apple.com/ios/3d-touch/.

À partir de la version 16.1 de Privileged Remote Access BeyondTrust, vous pouvez utiliser 3D Touch pour accéder facilement aux éléments de Jump. Veuillez consulter les sections ci-dessous pour en apprendre davantage sur les différentes façons dont 3D Touch vous permet d'accéder à vos systèmes essentiels.

Accédez aux éléments de Jump ayant reçu le plus souvent une assistance à l'aide de 3D Touch

En utilisant 3D Touch, vous pouvez accéder rapidement jusqu'à trois de vos éléments de Jump ayant reçu le plus souvent une assistance depuis l'écran d'accueil de l'iPhone. Suivez les étapes ci-dessous.

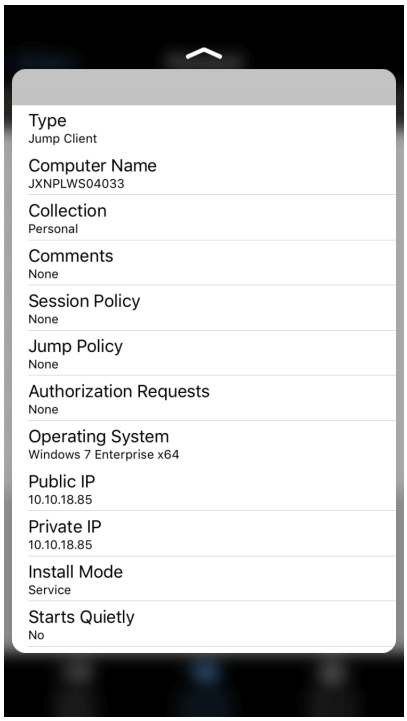
1. Maintenez appuyée l'icône de l'appli de la console d'accès mobile iOS, et une liste de vos éléments de Jump fréquemment utilisés apparaîtra. Notez que vous devrez appuyer plus fort sur l'écran pour voir les options d'élément de Jump.
2. Dans la liste, appuyez sur l'élément de Jump auquel vous souhaitez accéder.
3. Saisissez vos informations d'authentification de connexion.
4. Une session avec cet élément de Jump a démarré.



Prévisualisez les informations d'élément de Jump

Pour voir les détails d'élément de Jump avant de lancer une session, vous pouvez utiliser les actions Peek et Pop de 3D Touch. Suivez les étapes ci-dessous pour prévisualiser une session.

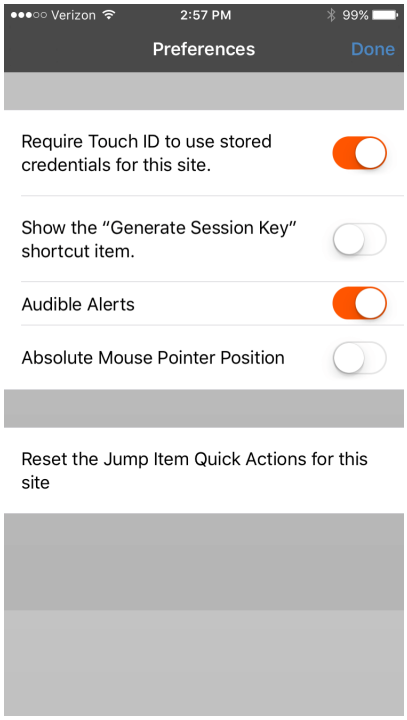
1. Depuis la page **Éléments de Jump**, sélectionnez la file d'attente où se trouve l'élément de Jump.
2. Une fois que vous avez appuyé sur la file d'attente, une liste d'éléments de Jump apparaît. Appuyez légèrement sur votre sélection jusqu'à ce que les informations de l'élément de Jump apparaissent.
3. Tout en continuant d'appuyer sur l'écran, balayez vers le haut pour voir l'action de **Jump**. Cliquez sur Jump pour démarrer une session.



> ***Remarque :*** *si vous n'appuyez pas assez fort ou pas assez longtemps, la prévisualisation n'apparaîtra pas, et à la place, la page des* ***Données de session*** *apparaîtra.*

Régler les préférences pour 3D Touch

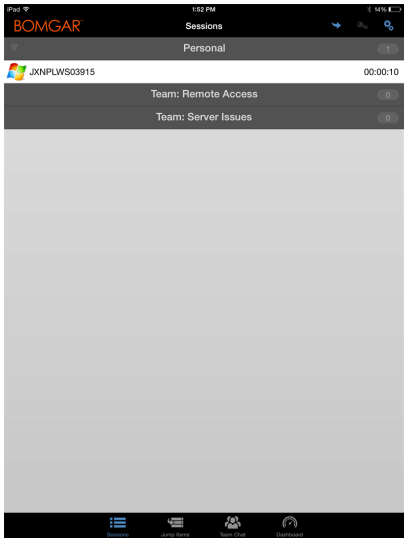
Dans la console d'accès mobile iOS, accédez au menu Préférences en appuyant sur l'icône menu située dans le coin supérieur droit de l'écran, puis sélectionnez **Préférences**. Dans les préférences, **Réinitialiser les actions rapides d'élément de Jump pour ce site** est propre à 3D Touch. Lorsque vous appuyez dessus, cette préférence vous permet de vider la liste des éléments de Jump fréquemment utilisés qui s'affiche lorsque vous maintenez appuyée l'icône de l'appli de la console d'accès mobile iOS.



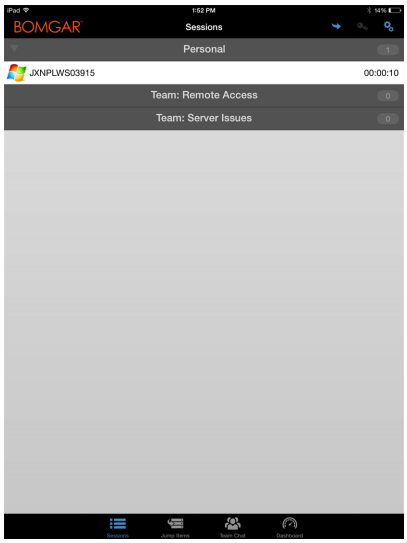
Consultez les sessions d'accès dans la console d'accès iOS

Dans la console d'accès, les sessions d'accès actives sont divisées dans des files d'attente d'équipe. Lorsque vous appuyez sur l'icône **Sessions** en bas de l'écran, une liste de toutes les files d'attente configurées apparaît. Ces files d'attente sont basées sur les équipes que vous avez définies dans l'interface d'administration /login. Une fois qu'une équipe est définie, une file d'attente devient disponible dans la section **Sessions** de la console d'accès. Cette file d'attente est toujours affichée tant qu'au moins un membre de l'équipe est connecté à la console d'accès.

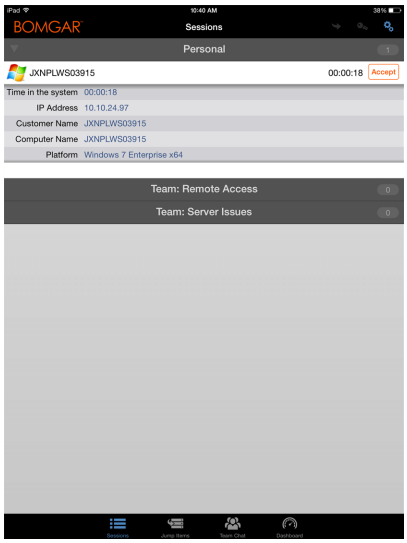
La file d'attente **Personnelle** contient les sessions actuellement en cours pour vous, ou des sessions qui ont été partagées avec vous spécifiquement par un autre membre. Les files d'attente restantes concernent des équipes spécifiques dont vous êtes membre.



Appuyez sur le nom de la file d'attente pour voir toute session en cours. Appuyez sur l'entrée d'une session pour voir des détails sur le système ou la session. Pour naviguer vers une session, appuyez sur l'option **Retour**.



> ***Remarque :*** *si une session a été partagée avec vous, appuyez simplement sur la file d'attente où se trouve la session. Appuyez ensuite sur la session. Sélectionnez* ***Accepter****. L'acceptation d'une session la fera apparaître sur votre écran.*



Effectuez un partage d'écran avec un point de terminaison depuis la console d'accès iOS

Sur la page **Partage d'écran**, appuyez sur le bouton **Lecture** pour demander à voir et contrôler le point de terminaison si le partage d'écran ne commence pas automatiquement. Une fois que vous avez accédé au point de terminaison, il apparaît sur votre écran. Vous aurez le contrôle total du clavier et de la souris du point de terminaison, ce qui vous permettra de travailler sur dessus 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 et faites glisser pour bouger la souris, **OU**, si la position réelle du pointeur de la souris est activée dans vos paramètres, placez le pointeur de la souris là où votre doigt touche l'écran.
- 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, **OU**, si la position absolue du pointeur de la souris est activée dans vos paramètres, maintenez appuyé pour ouvrir un menu volant à partir duquel vous pouvez choisir de faire un clic gauche, un clic droit ou un double clic.

> ***Remarque :*** *sur un iPad, et si cette fonction est activée dans vos paramètres, secouez l'appareil pour une aide rapide sur les gestes de partage d'écran.*

Sur un iPad, toutes les actions de partage d'écran sont disponibles en bas de l'écran. Pour accéder à davantage d'outils de partage d'écran sur un iPhone, appuyez sur l'icône **Menu** dans le coin supérieur droit de l'écran. Appuyez sur **Voir l'aide sur les gestes** pour une aide rapide sur les gestes de partage d'écran.

Actions de partage d'écran

	Commencer le partage d'écran.
	Arrêter le partage d'écran.
	Sélectionnez un autre écran distant à afficher. Le moniteur principal est désigné par la lettre **P**.
	Définissez 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.

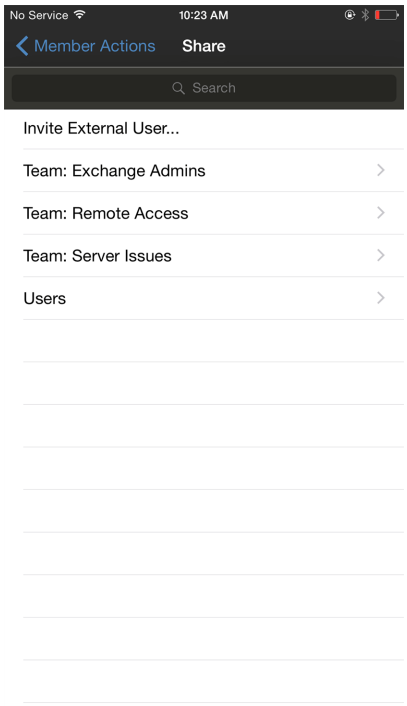
	Exécuter une action spéciale sur le système distant. Les tâches disponibles varient en fonction de la configuration et du système d'exploitation distants. Lors d'un fonctionnement avec des droits accrus, certaines actions peuvent être exécutées dans un contexte de système. Vous pouvez aussi fournir les informations d'authentification d'un utilisateur administrateur pour réaliser une action spéciale dans ce contexte utilisateur.
	Redémarrer le système distant sans perdre votre connexion à la session d'accès.
	Désactiver 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 client de point de terminaison doit être accru. Sur Windows 8, cette fonction est limitée à la désactivation du clavier et de la souris.
	Accéder au clavier afin d'écrire sur l'écran distant.

Partagez une session avec d'autres membres depuis la console d'accès iOS

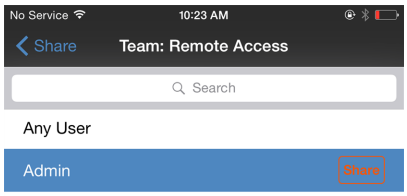
Pour partager une session avec un autre membre d'équipe sur un iPad, appuyez sur l'icône de personne dans l'angle supérieur droit de l'écran. Lorsque vous utilisez un iPhone, appuyez sur l'icône **Actions** en bas de l'écran. Appuyez sur **Actions de membre**.

Dans le menu, sélectionnez **Partager la session**.

Trouvez ensuite le membre avec lequel vous voulez partager la session en sélectionnant d'abord une équipe à laquelle le membre appartient. Sélectionnez un nom d'équipe pour en voir les membres.



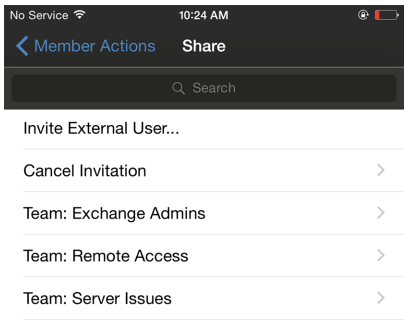
Vous pouvez sélectionner un utilisateur répertorié dans les équipes affichées pour l'inviter à rejoindre la session. Vous pouvez envoyer plusieurs invitations si vous souhaitez que plusieurs membres d'une équipe rejoignent votre session. Les utilisateurs sont répertoriés ici uniquement s'ils sont connectés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

Si vous avez envoyé une invitation et qu'elle est encore active, vous pouvez supprimer l'invitation en la sélectionnant dans le menu **Annuler l'invitation**. Appuyez ensuite sur le bouton **Annuler**. 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 disparaît 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.



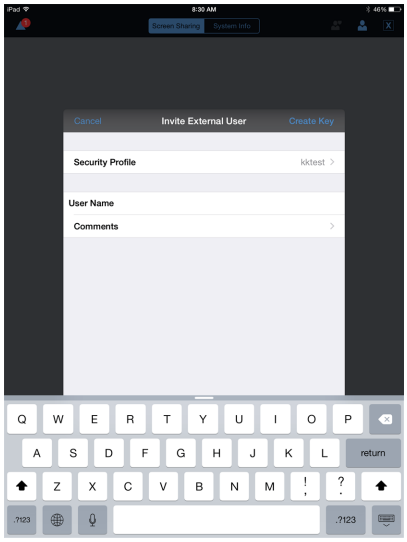
Invitez un utilisateur externe à rejoindre une session depuis la console d'accès iOS

Vous pouvez aussi partager une session avec un utilisateur qui n'a pas de compte sur votre Secure Remote Access Appliance. Pour inviter un utilisateur externe à rejoindre une session de manière ponctuelle, appuyez sur le bouton **Actions de membre**. Sur un iPhone, accédez à ce bouton en appuyant d'abord sur le bouton **Actions**.

Dans le menu, sélectionnez **Partager la session**.

Appuyez sur **Inviter un utilisateur externe**.

Un menu s'ouvrira, vous permettant de personnaliser l'invitation et de créer une clé de session d'accès.

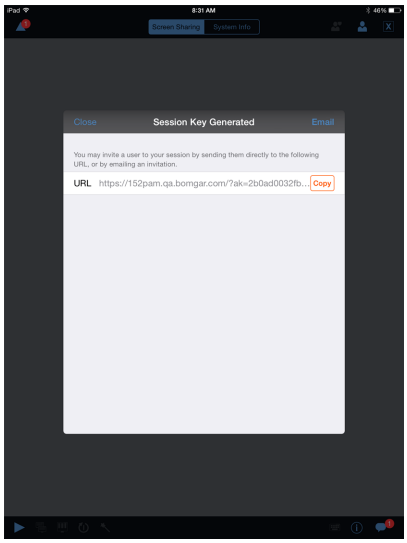


Appuyez sur **Profil de sécurité** pour accéder à une liste de profils d'utilisateurs disponibles. Ces profils sont créés dans l'interface d'administration et déterminent le niveau d'autorisation dont bénéficiera l'utilisateur externe. Lorsque vous sélectionnez un profil, la liste se fermera.

Appuyez ensuite sur l'option **Créer une clé**, située dans le coin supérieur droit de l'écran.

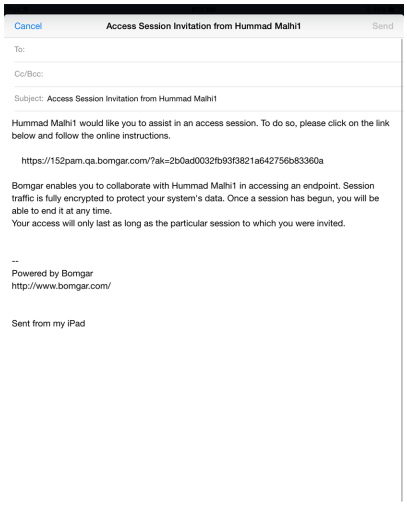
Une fois que vous avez appuyé dessus, la section **Clé de session générée** se remplira.

Appuyez sur l'option **E-mail** située dans le coin supérieur droit de l'écran.



Un e-mail a été créé. Apportez les modifications nécessaires à l'e-mail.

Lorsque vous avez terminé, appuyez sur **Envoyer**.



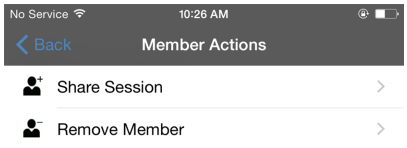
> ***Remarque :*** *vous avez aussi la possibilité de copier de l'URL présente dans la section* ***Clé de session générée****. Cliquez simplement sur l'option* ***Copier****, à côté de l'URL.*

Une fois que l'utilisateur externe a reçu l'e-mail, il doit toucher l'**URL** qui se trouve dedans. Il sera amené au **Portail d'accès**, où il lui sera demandé de télécharger la console d'accès.

Une fois la console téléchargée, la page de connexion à la console d'accès apparaîtra, avec le champ de clé de session d'accès déjà renseigné. L'utilisateur doit simplement appuyer sur **Connexion** pour accéder à la console.

Supprimez un membre de la session dans la console d'accès iOS

Vous pouvez supprimer un utilisateur d'une session partagée. Sur un iPhone, appuyez sur l'icône **Actions** en bas de l'écran. Sélectionnez **Actions de membre**. Appuyez sur **Supprimer membre**.



Su un iPad, appuyez sur le l'icône de la personne dans le coin supérieur droit de l'écran. Dans le menu, sélectionnez **Supprimer membre**.

Sélectionnez l'utilisateur que vous souhaitez supprimer. Appuyez ensuite sur l'option **Supprimer**.

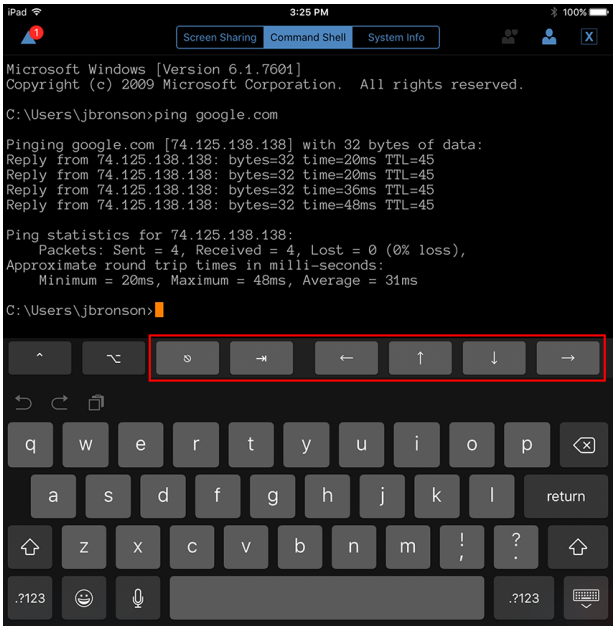
Ouvrez l'interpréteur de commandes sur le point de terminaison distant en utilisant la console d'accès (Apple iOS)

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.

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. Vous pouvez faire défiler les touches additionnelles en haut à droite (indiquées sur l'image) vers la droite ou la gauche pour révéler davantage 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.



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 ne sera pas interrompue.
	Fermer tous les interpréteurs de commandes ouverts.
	Afficher une liste des interpréteurs de commandes actuellement ouverts. Appuyez sur un élément de la liste pour accéder à l'interpréteur de commandes correspondant.

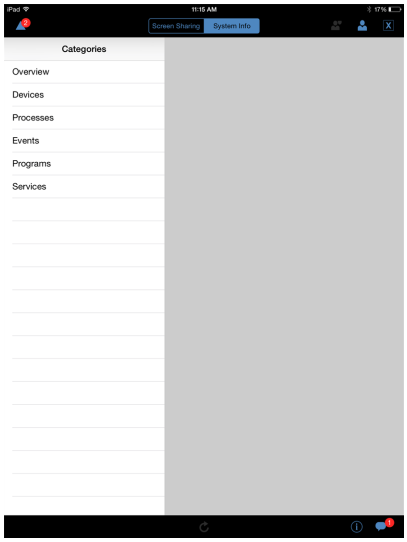
Consultez des informations sur le système distant dans la console d'accès iOS

Les utilisateurs privilégiés peuvent voir un instantané complet des informations système de l'appareil distant pour accélérer le diagnostic et la résolution des problèmes. Les informations système disponibles varient en fonction du système d'exploitation distant et de la configuration de l'ordinateur distant.

Pour demander les informations d'un système, allez dans **Informations système**. Appuyez sur **Demande**.

Sélectionnez des noms de catégories successives pour accéder aux données que vous voulez afficher. Pour revenir à la catégorie précédente, appuyez sur l'option **Retour**.

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



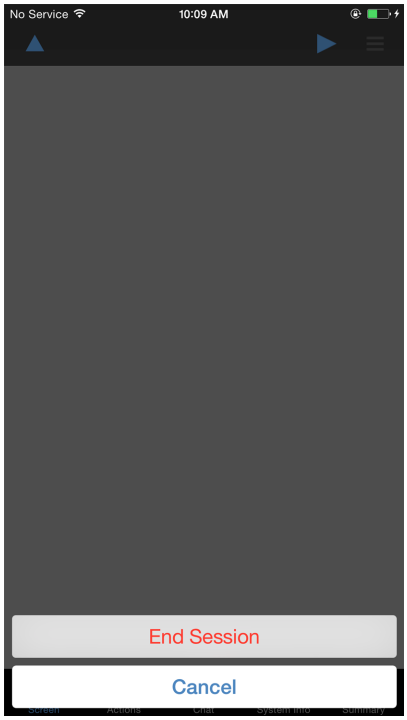
Consultez le résumé d'une session d'accès

La page **Résumé** fournit une vue d'ensemble du système distant auquel l'on accède. La page **Résumé** présente spécifiquement les informations suivantes concernant le système distant :

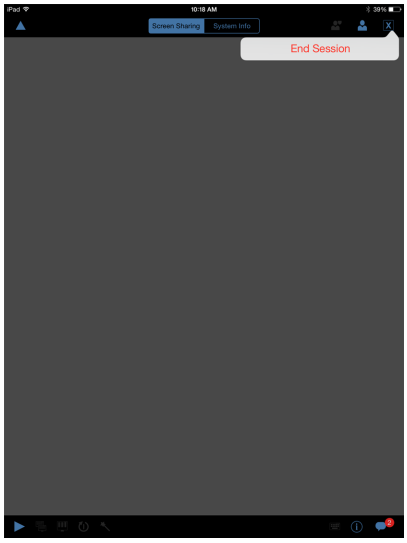
- **Adresse IP**
- **Nom d'utilisateur**
- **Nom d'ordinateur**
- **Plate-forme**

Fermez une session d'accès dans la console d'accès iOS

Pour quitter une session sur un iPhone, appuyez sur l'icône triangulaire dans le coin supérieur gauche de l'écran.



Pour quitter une session sur un iPad, appuyez sur le **X** dans l'angle supérieur droit de l'écran.



> ***Remarque :*** *une option* ***Mettre fin à la session*** *est aussi disponible en appuyant sur l'icône* ***Actions*** *en bas de l'écran.*

Si vous êtes le propriétaire, **Mettre fin à la session** ferme la page de session dans votre console d'accès et retire les utilisateurs additionnels qui partageaient la session. Cependant, cela ne supprimera pas un élément de Jump installé.

Si vous n'êtes pas le propriétaire de la session, appuyer sur l'icône **X** et sélectionner **Quitter la session** vous retirera simplement de la session. Cependant, le propriétaire de la session et les autres utilisateurs partageant la session continueront à accéder à la session.