BeyondTrust

Privileged Remote Access 22.1 Guide d'utilisateur de la console d'accès

TC:11/17/2022

Table of Contents

Console d'accès BeyondTrust

Ce guide est destiné à vous aider à installer la access console BeyondTrust sur votre ordinateur et à en comprendre les différentes fonctions. Privileged Remote Access BeyondTrust vous permet d'accéder à des points de terminaison distants en vous y connectant par le biais de la BeyondTrust Appliance B Series.

Utilisez ce guide uniquement après que l'administrateur a procédé à l'installation et à la configuration initiales de la B Series Appliance, qui sont expliquées dans le Guide d'installation matérielle de la BeyondTrust Appliance B Series. Une fois BeyondTrust correctement installé, vous pouvez commencer immédiatement à accéder à vos points de terminaison. Si vous avez besoin d'aide, contactez l'BeyondTrust Technical Support à l'adresse www.beyondtrust.com/support.

Installation de la console d'accès

Dans votre navigateur Web, accédez à l'URL de la B Series Appliance suivie de **/login** et entrez le nom d'utilisateur et le mot de passe définis par votre administrateur. Lors de votre première connexion, vous pouvez être invité à changer de mot de passe.

Sur la page **Mon compte**, téléchargez et installez la access console BeyondTrust. L'option sélectionne par défaut l'installeur adapté à votre système d'exploitation.

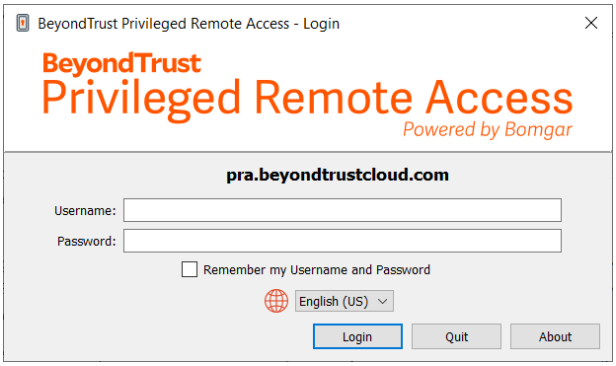
> ***Remarque :*** *sur un système Linux, vous devez enregistrer le fichier sur votre ordinateur, puis l'ouvrir depuis le répertoire d'enregistrement. N'utilisez pas le lien* ***Ouvrir*** *qui s'affiche après le téléchargement d'un fichier sur certains navigateurs.*

Lorsque l'assistant d'installation apparaît, suivez les instructions pour installer le logiciel. Une fois la access console installée, vous pouvez choisir **Exécuter la Access Console BeyondTrust maintenant** et/ou **Exécuter au démarrage**. Cliquez ensuite sur **Terminé**.

> ***Remarque :*** *si vous choisissez* ***Exécuter la Access Console BeyondTrust maintenant*** *durant l'installation, une invite de connexion s'affichera sur votre écran.*

Se connecter à la console d'accès PRA

Une fois la console BeyondTrust installée, démarrez la access console à partir de son répertoire, tel que défini au cours de l'installation.



> ***Remarque :*** *dans Windows, vous pouvez par défaut accéder à la console d'accès depuis* ***Menu Démarrer > Tous les programmes > Bomgar > access.example.com****,* ***access.example.com*** *étant le nom d'hôte du site depuis lequel vous avez téléchargé la console.*

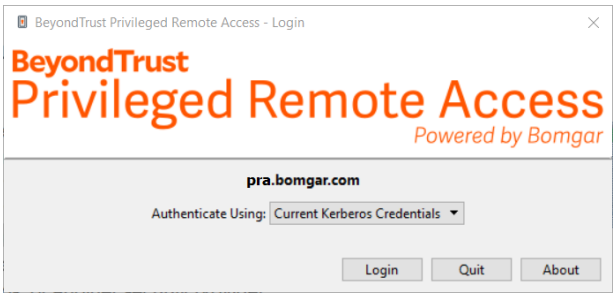
Si l'**Accord de connexion** a été activé, vous devez cliquer sur **Accepter** pour poursuivre.

À l'invite, entrez vos nom d'utilisateur et mot de passe.

Si l'authentification à deux facteurs est activée sur votre compte, saisissez le code de l'application d'authentification.

> ***Remarque :*** *Si plusieurs langues sont activées pour votre site, sélectionnez celle que vous souhaitez utiliser dans la liste déroulante.*

> ***Remarque :*** *les utilisateurs qui se connectent à l'aide de codes obtenus par e-mail passent automatiquement à l'authentification à deux facteurs (2FA). Ils ont toutefois la possibilité d'utiliser des codes reçus par e-mail jusqu'à ce qu'ils soient inscrits sur une application. Après une première utilisation de 2FA, l'option du code e-mail n'est plus disponible.*



Autrement, si votre administrateur a configuré un serveur Kerberos pour autoriser l'authentification unique, vous pouvez vous connecter à la console sans saisir vos informations d'authentification. La access console se souvient du dernier mécanisme de connexion utilisé, que cela ait été au moyen d'informations d'authentification locales, de Kerberos, ou d'un autre fournisseur de sécurité.

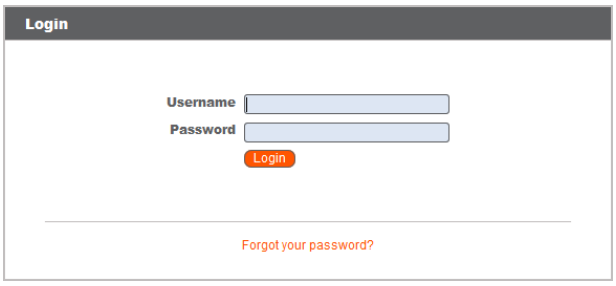
Les utilisateurs invités peuvent également saisir une clé de session pour rejoindre une session partagée de manière ponctuelle.

Cochez la case **Autoriser l'enregistrement des informations de connexion** pour enregistrer votre nom d'utilisateur et votre mot de passe dans la console. Cette option peut être activée ou désactivée sous **/login > Gestion > Sécurité**.

Lorsque vous êtes connecté, la console s'ouvre, et une icône BeyondTrust apparaît dans la barre d'état système de votre ordinateur.

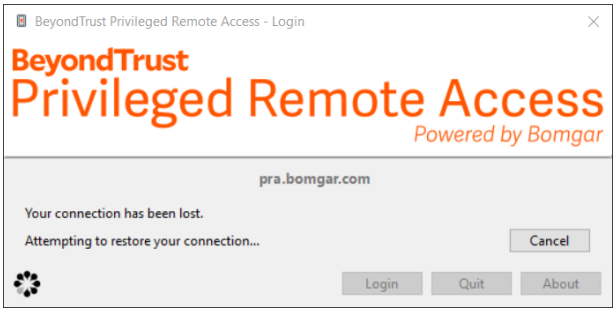
> ***Remarque :*** *votre administrateur peut exiger que vous soyez sur un réseau autorisé pour pouvoir vous connecter à la console. Cette restriction réseau peut s'appliquer à votre première connexion ou de façon permanente. Cette restriction ne s'applique pas aux invites d'accès.*

Remarque : *si vous avez oublié votre mot de passe, allez dans* ***/login*** *et cliquez sur le lien* ***Vous avez oublié votre mot de passe ?****. Cette option est définie par votre administrateur. Si vous n'avez pas cette option, veuillez contacter votre administrateur.*



Si vous perdez votre connexion, la access console tente de se reconnecter pendant 60 secondes. Si votre connexion est rétablie pendant ce laps de temps, votre access console rouvre, et toutes vos sessions ouvertes sont récupérées. Dans le cas contraire, vous êtes invité à réessayer de vous connecter ou de vous déconnecter.

Si vous êtes connecté à une access console à un emplacement et que vous vous connectez ailleurs, vos sessions ouvertes sont maintenues.



Remarque : *pour se connecter avec un compte en cours d'utilisation et forcer la connexion d'un autre système à se fermer, il est nécessaire de cocher l'option* ***Mettre fin à la session si le compte est en cours d'utilisation*** *sur la page* ***/login > Gestion > Sécurité****.*

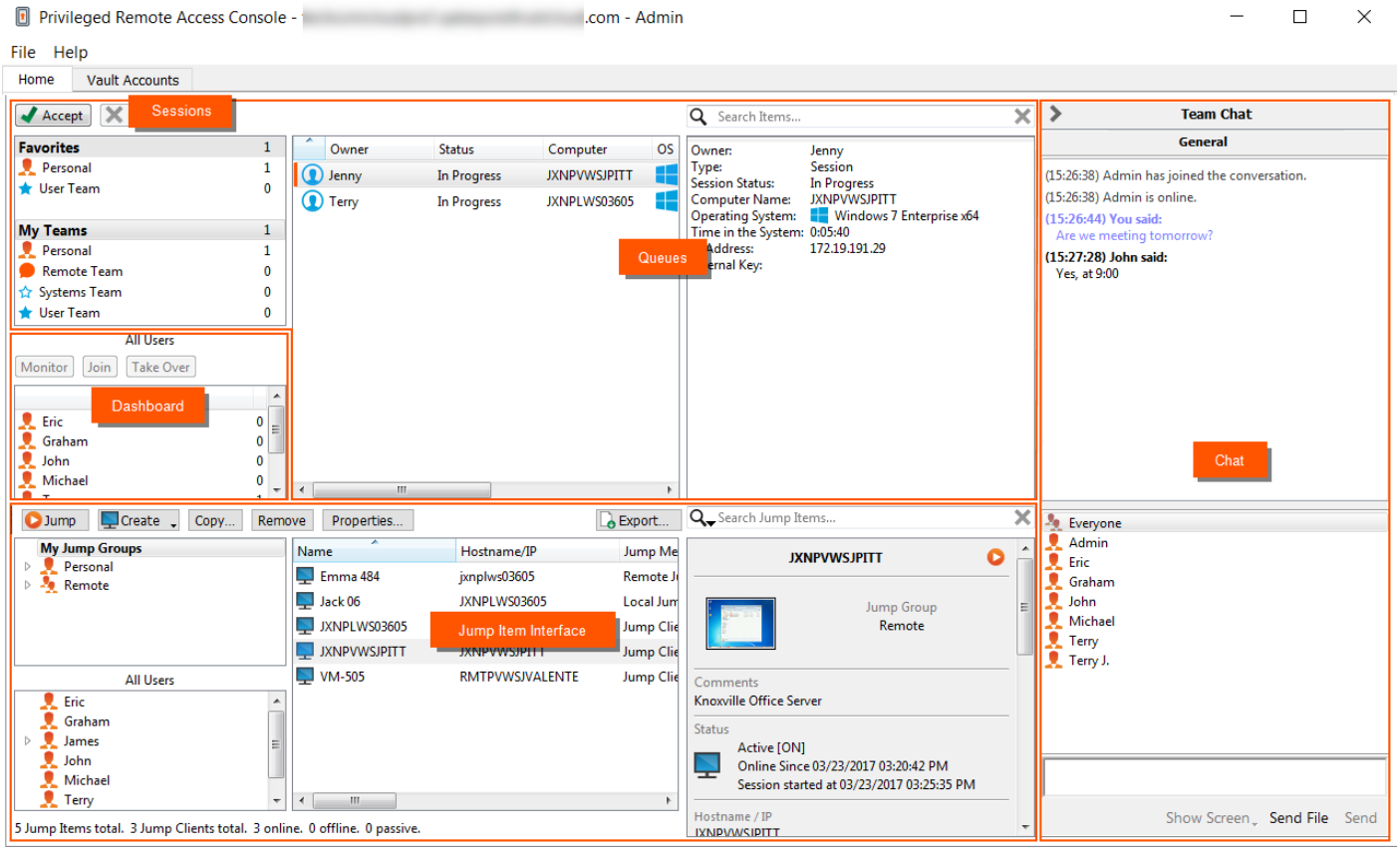
Après une mise à niveau, ou au premier lancement de la access console de bureau, le dialogue **Nouveautés** s'affiche automatiquement à la connexion pour tous les utilisateurs non invités. Ce dialogue peut être consulté à tout moment par le biais du menu **Aide** (**Aide > Nouveautés**) et montre des informations sur les versions actuelles et passées. Ceci est une préférence itinérante par compte, et le dialogue n'apparaîtra donc qu'une fois là où un utilisateur se connecte.

Pour plus d'informations, veuillez consulter :

- *Pour plus d'informations sur l'accord de connexion, veuillez consulter Configuration du site : Configuration des ports HTTP et activation de l'accord de connexion à l'adresse https://www.beyondtrust.com/fr/docs/privileged-remote-access/getting-started/admin/site-configuration.htm*
- *Sur les utilisateurs invités, veuillez consulter la section « Inviter un utilisateur externe à rejoindre une session d'accès », page 76.*

Interface utilisateur de la console d'accès

La access console contient différents panneaux fournissant des outils et des informations concernant les sessions.



Sessions : gérez plusieurs sessions distantes à la fois.

Files d'attente : les files d'attente listent les sessions actuellement en cours, et les demandes de partage de sessions avec tout membre d'une équipe. Les détails sur le système distant auquel l'on accède apparaissent dans cette section.

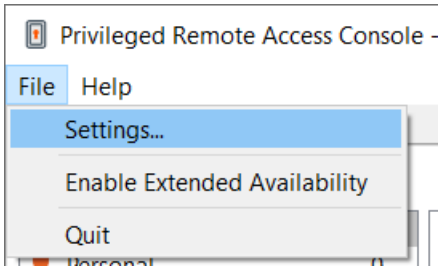
Tableau de bord : les utilisateurs privilégiés peuvent voir et surveiller les sessions en cours et les membres de leur équipe de rang inférieur, permettant une supervision administrative pour aider à gérer le personnel.

Interface d'élément de Jump : les Jump Clients installés et les raccourcis de Jump apparaissent ici, regroupés en fonction des personnes qui peuvent y accéder.

Messagerie instantanée : discutez avec d'autres utilisateurs connectés. Vous pouvez également partager votre écran avec un membre de votre équipe, sans besoin d'être en session.

Changer les paramètres et préférences dans la console d'accès

Cliquez sur **Fichier > Paramètres** dans le coin supérieur gauche de la console pour configurer vos préférences.



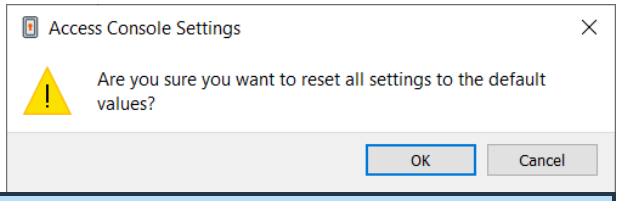
En général, vous pouvez configurer les paramètres de la console selon vos préférences. Cependant, votre administrateur BeyondTrust peut choisir de gérer lui-même ces paramètres et d'en forcer l'application.

Si votre administrateur BeyondTrust a modifié et appliqué les paramètres par défaut, l'alerte **Paramètres modifiés** s'affichera lors de votre prochaine connexion à la console. Cliquez sur **Afficher les paramètres** pour accéder à la fenêtre des paramètres afin de consulter les modifications, ou cliquez sur **OK** pour accuser réception des changements.

Modification des paramètres

> ***Remarque :*** *ces instructions supposent que vous êtes autorisé à choisir les paramètres utilisés dans votre console. Les paramètres définis par votre administrateur sont signalés par un astérisque et grisés, et ils ne peuvent pas être modifiés localement. Pour plus d'informations, contactez votre administrateur ou consultez la section Paramètres de la access console dans le guide d'administration.*

La fenêtre **Access ConsoleParamètres** contient un bouton **Valeurs par défaut** dans le coin inférieur gauche, qui permet de rétablir les paramètres BeyondTrust par défaut ou les paramètres par défaut définis par l'administrateur, le cas échéant. Un message d'alerte vous demande alors de confirmer la sélection du paramétrage par défaut. Cliquez sur **Annuler** si vous souhaitez conserver vos préférences locales.

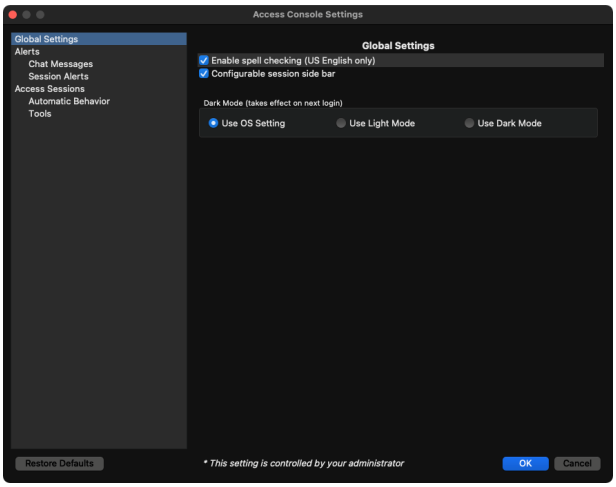


> ***Remarque :*** *si les paramètres par défaut sont imposés par l'administrateur, vous ne pourrez toutefois pas les configurer.*

Dans la section **Paramètres globaux**, vous pouvez choisir d'activer ou de désactiver le correcteur orthographique pour la messagerie instantanée. Le correcteur est actuellement disponible en anglais US uniquement.

Choisissez si vous souhaitez que l'icône de menu de session soit affichée, si la barre latérale peut être détachée, et si les widgets de la barre latérale de session peuvent être réorganisés et redimensionnés.

Vous pouvez choisir de changer votre mode d'affichage. Les options incluent **Paramètres du SE** (par défaut), **Mode lumineux** et **Mode sombre**.



Remarque : *l'option Mode sombre s'applique uniquement à Windows et macOS.*

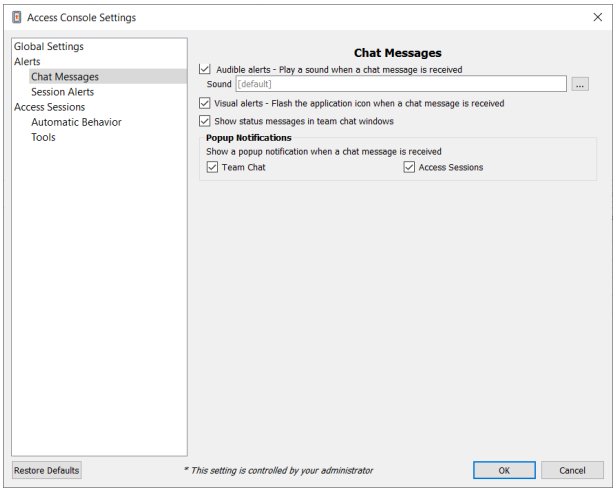
En plus de changer le mode d'affichage dans la access console, les utilisateurs peuvent le changer dans ***Paramètres du SE*** *en sélectionnant* ***Paramètres des thèmes et paramètres associés > Couleur > Choisissez votre couleur****.*

Configurez les paramètres d'alerte pour les messages instantanés. Vous pouvez ainsi choisir d'entendre une alerte sonore et de voir l'icône de l'application clignoter pour vous signaler la réception d'un message instantané.

Pour transférer un signal sonore personnalisé pour les messages instantanés, cliquez sur le bouton **[…]**, puis sélectionnez un fichier WAV sur votre ordinateur. Notez que le fichier doit être inférieur à 1 Mo.

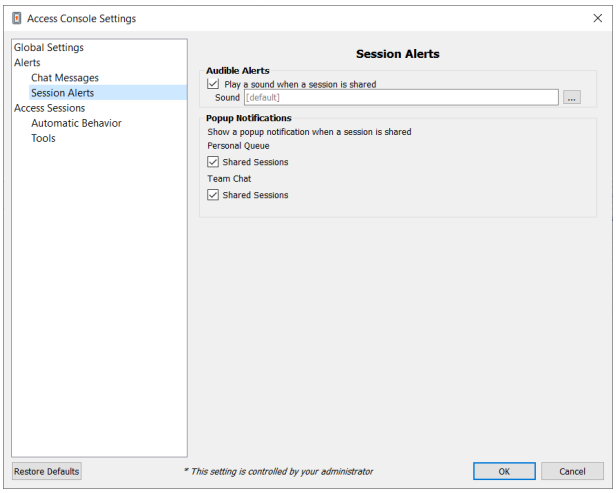
Choisissez si la messagerie instantanée de l'équipe doit inclure les messages de statut, comme la connexion et déconnexion des utilisateurs, ou seulement les messages instantanés entre les membres de l'équipe.

Choisissez si vous souhaitez recevoir des avertissements contextuels pour les messages reçus dans la messagerie instantanée de l'équipe et/ou de session.



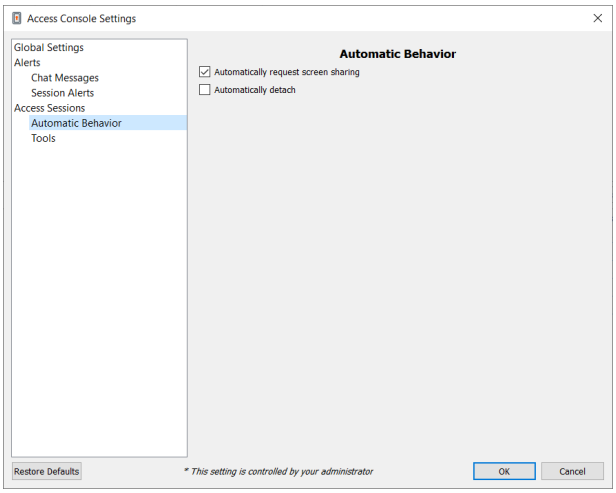
Choisissez si vous souhaitez entendre une alerte sonore lorsqu'un autre utilisateur demande à partager une session avec vous. Pour transférer un signal sonore personnalisé pour les sessions partagées, cliquez sur le bouton **[…]**, puis sélectionnez un fichier WAV sur votre ordinateur. Notez que le fichier doit être inférieur à 1 Mo.

Vous pouvez également choisir de recevoir des notifications contextuelles pour certains événements. Ces notifications s'afficheront indépendamment de votre console et par-dessus les autres fenêtres. Définissez l'emplacement où vous souhaitez voir apparaître ces notifications contextuelles ainsi que leur durée d'affichage.



Choisissez si vous souhaitez lancer automatiquement le partage d'écran au début d'une session.

Vous pouvez choisir d'ouvrir les sessions sous forme d'onglets dans la console ou de les détacher automatiquement dans de nouvelles fenêtres.

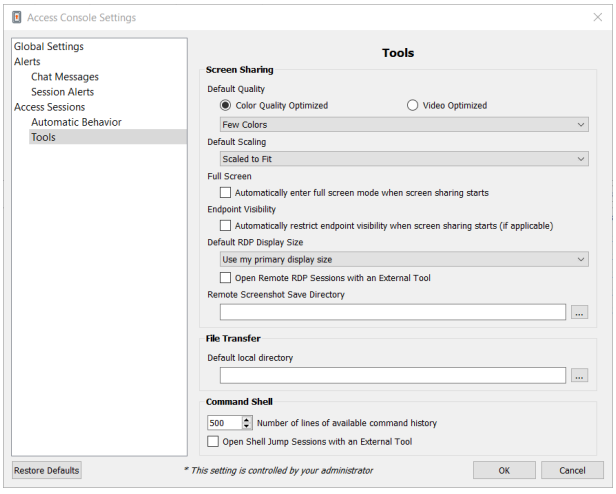


Définissez la qualité et la taille d'écran par défaut d'une session de partage d'écran. Lorsque le partage d'écran démarre, vous pouvez automatiquement basculer en mode plein écran, qui à son tour peut automatiquement faire disparaître la barre de discussion.

De plus, lorsque le partage d'écran commence, le système distant peut automatiquement voir son affichage et son entrée au clavier et à la souris restreints, fournissant un écran de confidentialité.

Sélectionne la taille d'affichage RDP par défaut pour toutes les sessions RDP.

Une option vous permet d'ouvrir une connexion PRA étendue à tous les moniteurs de l'ordinateur client, quelle que soit la configuration des moniteurs client. Avec cette fonctionnalité, vous pouvez utiliser pleinement tous les moniteurs connectés à l'ordinateur client, ce qui vous permet d'ajuster le dimensionnement et la mise à l'échelle de l'écran pendant une session RDP sur plusieurs moniteurs.



Si vous souhaitez utiliser votre propre outil RDP, cochez **Ouvrir des sessions RDP distantes avec un outil externe**.

Pour accéder plus facilement aux captures d'écran de la console, définissez le répertoire par défaut dans lequel vous enregistrerez vos captures d'écrans distantes prises dans la console.

Afin de faciliter le transfert de fichiers, définissez le répertoire par défaut depuis lequel vous voulez démarrer la navigation de votre système de fichiers local.

Définissez le nombre de lignes à enregistrer dans l'historique de l'interpréteur de commandes.

Si vous souhaitez utiliser votre propre outil SSH, cochez **Ouvrir des sessions Shell Jump avec un outil externe**.

IMPORTANT !

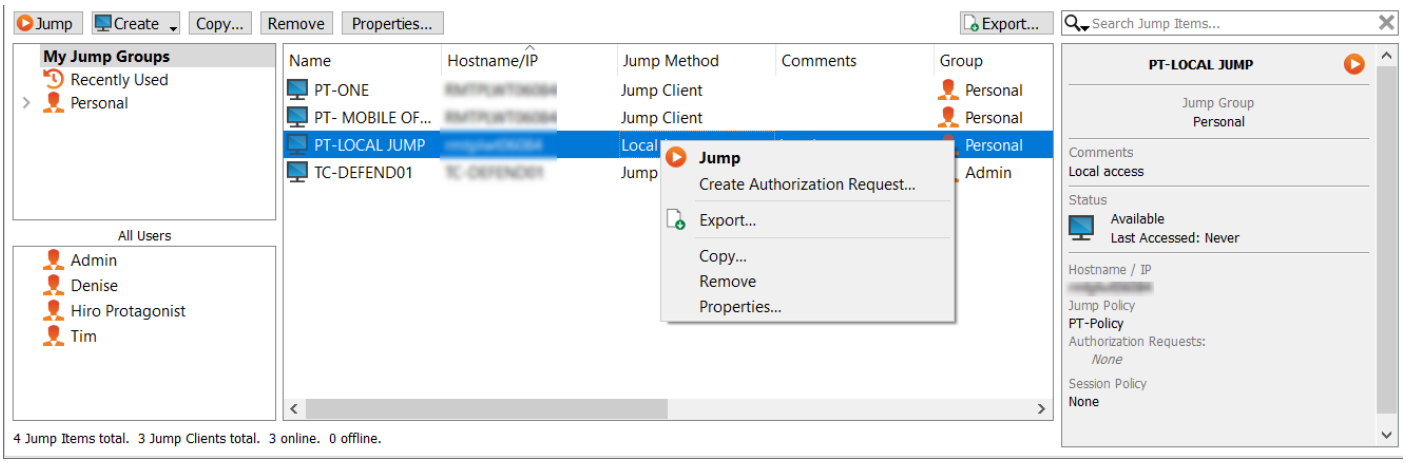
*Afin d'utiliser votre propre outil, vous devez activer **Jump en tunnel par protocole** dans **/login > Utilisateurs et sécurité > Utilisateurs > Technologie Jump > Jump en tunnel par protocole**.*

Interface de Jump : utiliser les éléments de Jump pour accéder à des systèmes distants

L'interface de Jump apparaît dans la partie basse de la access console, et affiche la liste des éléments de Jump auxquels vous avez accès. Cette liste peut contenir des Jump Clients actifs et passifs, ainsi que des raccourcis de Jump pour des Jumps distants, des Jumps locaux, des sessions RDP, des sessions VNC, des Jumps en tunnel par protocole, des Shell Jumps et des Jumps Web.

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. Sélectionner un groupe de Jump et cliquer sur **Créer** sélectionne automatiquement ce groupe de Jump dans la fenêtre de configuration d'élément de Jump.

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.



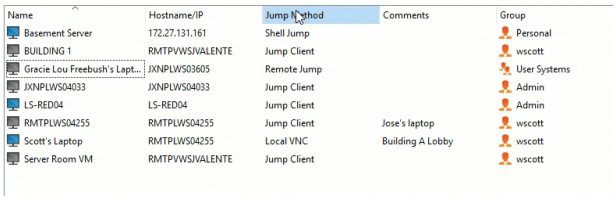
Copier des éléments de Jump

Les éléments de Jump peuvent être copiés et peuvent appartenir à plusieurs groupes de Jump. Cela comprend des éléments de Jump Client, fournissant aux administrateurs la capacité de définir des règles et des autorisations de groupe distinctes sans devoir installer un Jump Client additionnel sur le point de terminaison cible. Les utilisateurs dotés des autorisations appropriées voient l'option de **Copier** des éléments de Jump dans la Access Console en faisant un clic droit sur l'élément. Les utilisateurs peuvent aussi utiliser cette fonction sur plusieurs éléments de Jump.

Cette fonctionnalité permet aux administrateurs et aux utilisateurs de gérer efficacement différentes stratégies pour les éléments de Jump et les Jump Clients sans avoir besoin de créer un nouvel élément de Jump. Cette fonctionnalité permet aux utilisateurs de limiter le nombre de clients nécessaires pour activer les sessions Jump Client et de limiter les tâches administratives manuelles lors de la définition des chemins d'accès pour les utilisateurs.

Jump vers un élément de Jump

Parcourez les groupes pour accéder à l'ordinateur de votre choix. Pour faciliter la navigation dans la liste des éléments de Jump, vous pouvez glisser/déposer les colonnes pour les faire apparaître dans l'ordre de votre choix, puis organiser une colonne en cliquant sur son en-tête. La access console se souviendra de l'ordre des colonnes ainsi que de leur organisation la prochaine fois que la access console sera lancée.



Vous avez la possibilité de naviguer pour trouver des éléments de Jump, mais aussi de lancer une recherche en fonction de plusieurs champs. Saisissez une chaîne dans le champ de recherche, puis appuyez sur **Entrée**. Pour modifier les champs de recherche, cliquez sur la loupe, et cochez ou décochez un champ disponible. Les champs de recherche comprennent **les commentaires**, **l'utilisateur de la console**, **le domaine**, **le FQDN**, **le groupe**, **le nom d'hôte/l'IP**, **la méthode de Jump**, **le dernier accès**, **le nom**, **l'IP privée**, **l'IP publique**, **l'état**, **la balise et le groupe de travail**.

Une fois que vous avez trouvé l'ordinateur auquel vous voulez accéder, double-cliquez sur l'entrée ou sélectionnez l'entrée et cliquez sur le bouton **Effectuer un Jump**. Une session tente alors de démarrer avec l'ordinateur distant.

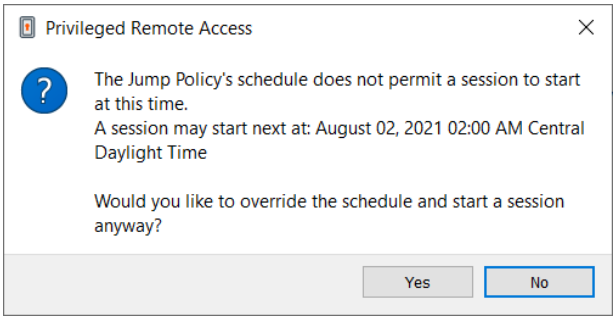
Vous pouvez vous connecter par programme à un élément de Jump directement depuis votre outil de création de ticket ou de gestion des systèmes. Si vos résultats de recherche aboutissent à un seul élément de Jump, la session démarre immédiatement. Si plusieurs éléments de Jump sont renvoyés, sélectionnez l'un des éléments de Jump répertoriés dans la fenêtre de sélection et cliquez sur **OK**.

> ***Remarque :*** *pour en savoir plus sur les scripts, consultez API de script pour Access Console et de scripts client à l'adresse www.beyondtrust.com/docs/privileged-remote-access/how-to/integrations/api/client-script.*

Si une règle de Jump est appliquée à cet élément de Jump, cette règle affecte la façon et/où le moment auquel cet élément de Jump est accessible.

Planifier

Si une règle de Jump impose un planning pour cet élément de Jump, une tentative d'accès à cet élément de Jump en dehors de son planning autorisé empêche le Jump. Une invite vous informe des restrictions de la règle et vous donne la date et l'heure à laquelle cet élément de Jump sera disponible pour un accès.



Notification

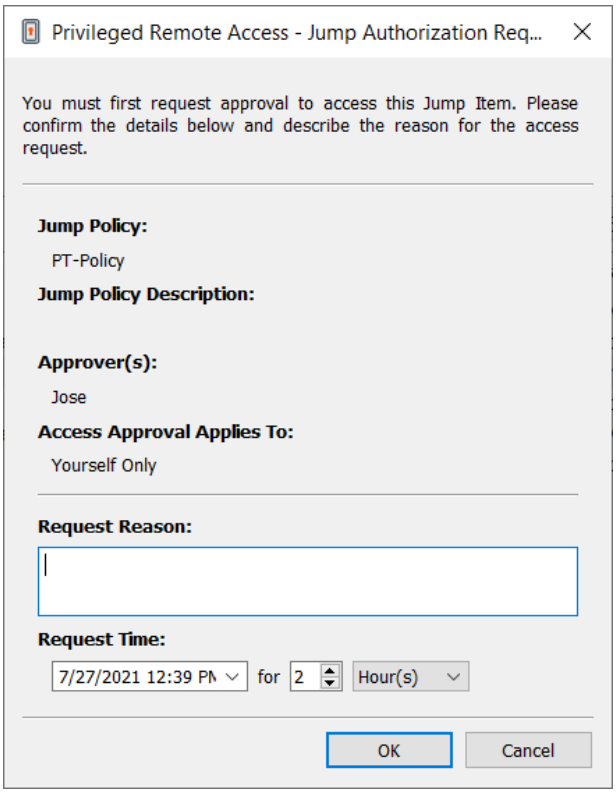
Si une règle de Jump est configurée pour envoyer une notification au démarrage ou à l'arrêt d'une session, une tentative d'accès à un élément de Jump vous alertera qu'un e-mail sera envoyé. Vous pouvez choisir de continuer le Jump et d'envoyer une notification, ou d'annuler ce Jump.

ID de ticket

Si une règle de Jump requiert l'entrée d'un ID de ticket provenant de votre ITSM externe ou du système d'ID de ticket avant que le Jump soit exécuté, un dialogue s'ouvrira. Dans ce dialogue, saisissez l'ID de ticket dont vous avez besoin, autorisant l'accès à cet élément de Jump.

Autorisation

Si une règle de Jump requiert une autorisation avant que le Jump soit exécuté, un dialogue s'ouvrira. Dans ce dialogue, saisissez la raison pour laquelle vous voulez accéder à cet élément de Jump. Saisissez ensuite la date et l'heure à laquelle vous souhaitez que l'autorisation débute, ainsi que la durée pendant laquelle vous voulez accéder à l'élément de Jump. La raison d'accès et le moment de la demande sont visibles pour l'approbateur et l'aident à décider d'approuver ou de rejeter l'accès.



Lorsque vous cliquez sur **OK**, un e-mail est envoyé aux adresses définies comme approbatrices pour cette règle. Cet e-mail contient une URL où l'approbateur peut voir la demande, ajouter des commentaires et approuver ou rejeter la demande.

Si une demande a été approuvée pour quelqu'un, quelqu'un d'autre peut accéder à l'URL pour outrepasser l'approbation et rejeter la demande. Si une demande a été rejetée, n'importe quel autre approbateur accédant au site peut voir les détails, mais ne peut pas outrepasser le rejet. Si un utilisateur a déjà rejoint une session approuvée, l'accès ne peut pas être rejeté. 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. En fonction des paramètres de règle de Jump, une demande accordée donne l'accès à tout utilisateur qui peut voir et demander l'accès à ce Jump Client, ou seulement à l'utilisateur qui a demandé l'accès.

Dans l'interface de Jump, le volet de détails de l'élément de Jump affiche l'état de toutes les demandes d'autorisation comme étant en attente, approuvées, approuvées seulement pour un autre utilisateur, ou rejetées. Lorsqu'un approbateur répond à une demande, une notification contextuelle apparaît sur l'écran du demandeur, le prévenant que l'accès a été approuvé ou rejeté. Si le demandeur a configuré une adresse e-mail, une notification lui sera également envoyée par e-mail.

Lorsqu'un utilisateur effectue un Jump vers un élément de Jump pour lequel l'accès a été approuvé, une notification transmet à l'utilisateur tout commentaire laissé par l'approbateur.

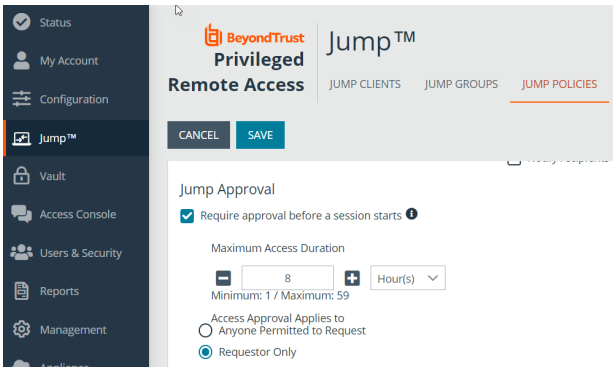
Lorsque l'approbation a été accordée à un élément de Jump, celui-ci devient disponible pour tout utilisateur pouvant le voir et en demander l'accès, ou seulement à l'utilisateur qui a demandé l'accès. Ceci est déterminé par la règle de Jump.

> ***Remarque :*** *bien que plusieurs demandes peuvent être envoyées pour des moments différents, les temps d'accès demandés ne peuvent pas se chevaucher. Si une demande est rejetée, une deuxième demande peut être envoyée pour la même date/heure.*

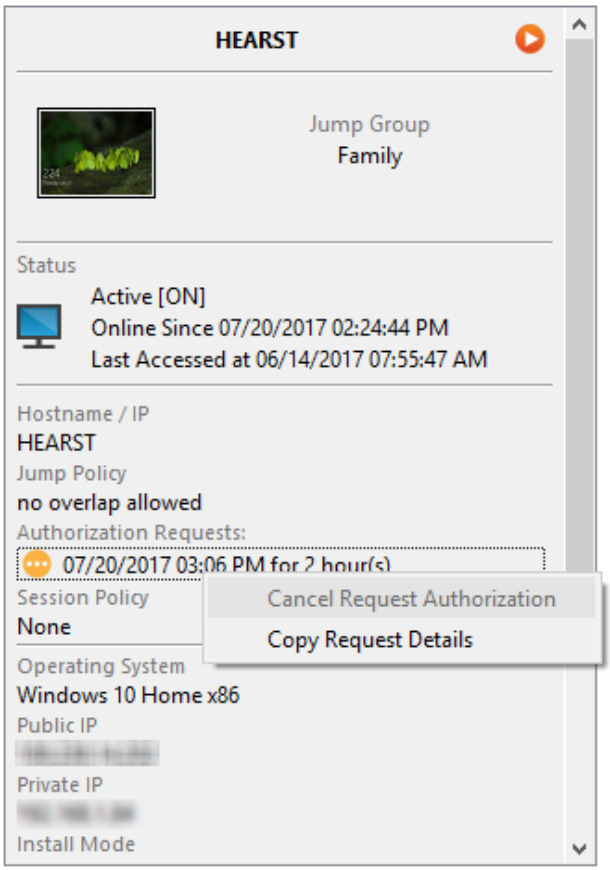
Révocation de la requête d'approbation d'accès

L'autorisation de révoquer une demande d'accès approuvée est contrôlée par une règle de Jump. Dans l'interface de gestion Web **/login**, accédez à **Jump > Règles de Jump**. Sous **Approbation de Jump** figurent deux options :

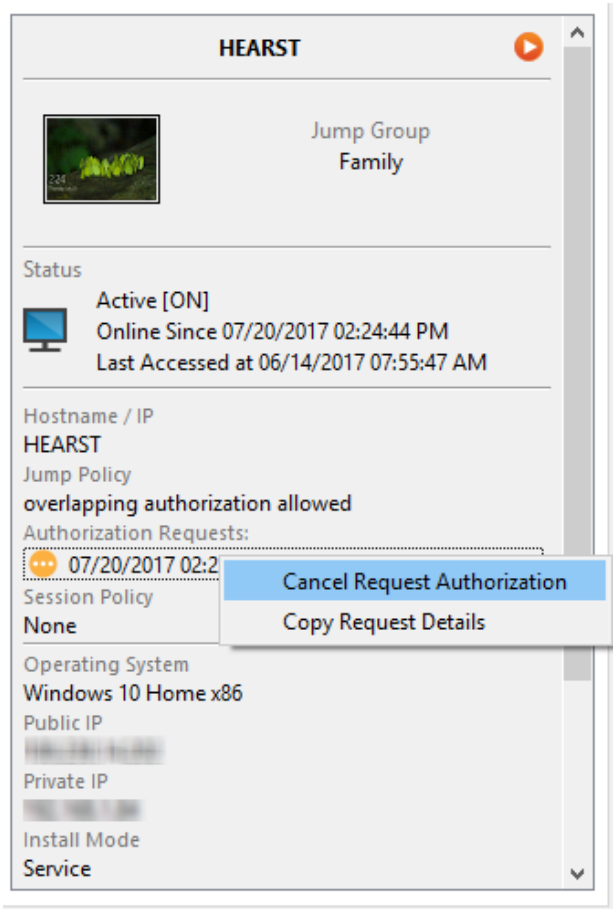
- **Toute personne autorisée à faire une requête**
- **Demandeur seulement**



Si la règle de Jump est définie sur **Demandeur seulement** et qu'une demande d'accès est actuellement approuvée pour l'utilisateur A, l'utilisateur B est invité à créer une nouvelle demande d'accès s'il tente d'effectuer un Jump vers l'élément de Jump, car cette demande ne s'applique pas à lui. De plus, si l'utilisateur B tente d'annuler la demande d'approbation d'accès, l'option est grisée. Le seul utilisateur qui peut annuler la demande approuvée est l'utilisateur A, car il est l'utilisateur approuvé pour la demande.



Cependant, si la règle de Jump est définie sur **Toute personne autorisée à faire une requête** et qu'une demande d'accès est actuellement approuvée pour l'utilisateur A, l'utilisateur B est autorisé à démarrer une nouvelle session avec l'élément de Jump s'il tente d'effectuer un Jump vers lui. De plus, toute personne autorisée à accéder à l'élément de Jump est autorisée à annuler/révoquer la demande.



Utiliser les Jump Clients pour accéder à des points de terminaison distants

Pour accéder à un ordinateur individuel Windows, Mac ou Linux qui n'est pas sur un réseau accessible, installez un Jump Client sur ce système depuis la page **/login > Jump > Jump Clients**. Les Jump Clients apparaissent dans l'interface de Jump avec les raccourcis d'élément de Jump.

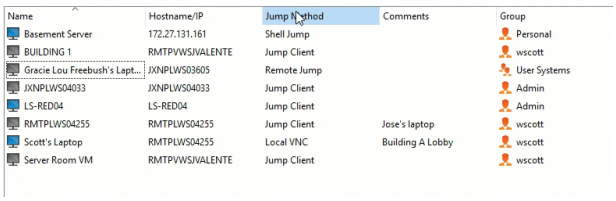
Utiliser un Jump Client

Pour utiliser un Jump Client pour lancer une session, sélectionnez le Jump Client dans l'interface de Jump et cliquez sur le bouton **Jump**.

> ***Remarque :*** *il est possible de configurer les éléments de Jump pour permettre à plusieurs utilisateurs d'accéder au même élément de Jump en simultané. Si l'option* ***Rejoindre une session existante*** *est activée, d'autres utilisateurs sont susceptibles de rejoindre une session déjà en cours. Le propriétaire initial de la session reçoit une notification lui indiquant qu'un autre utilisateur a rejoint la session, mais il n'est pas autorisé à lui refuser l'accès. Pour en savoir plus sur les Jumps simultanés, veuillez consulter Paramètres d'élément de Jump à l'adresse www.beyondtrust.com/docs/privileged-remote-access/getting-started/admin/jump-items.htm.*

Organiser les Jump Clients

Parcourez les groupes pour accéder à l'ordinateur de votre choix. Pour faciliter la navigation dans la liste des éléments de Jump, vous pouvez glisser/déposer les colonnes pour les faire apparaître dans l'ordre de votre choix, puis organiser une colonne en cliquant sur son en-tête. La access console se souviendra de l'ordre des colonnes ainsi que de leur organisation la prochaine fois que la access console sera lancée.



Name	Hostname/IP	Jump Method	Comments	Group
Basement Server	172.27.131.161	Shell Jump		Personal
BUILDING 1	RMTPVWSJVALENTE	Jump Client		wscott
Gracie Lou Freebush's Lapt...	JXNPLWS03605	Remote Jump		User Systems
JXNPLWS04033	JXNPLWS04033	Jump Client		Admin
LS-RED04	LS-RED04	Jump Client		Admin
RMTPLWS04255	RMTPLWS04255	Jump Client	Jose's laptop	wscott
Scott's Laptop	RMTPLWS04255	Local VNC	Building A Lobby	wscott
Server Room VM	RMTPVWSJVALENTE	Jump Client		wscott

Trouver un Jump Client

Vous avez la possibilité de naviguer pour trouver des éléments de Jump, mais aussi de lancer une recherche en fonction de plusieurs champs. Saisissez une chaîne dans le champ de recherche, puis appuyez sur **Entrée**. Pour modifier les champs de recherche, cliquez sur la loupe, et cochez ou décochez un champ disponible. Les champs de recherche comprennent **les commentaires**, **l'utilisateur de la console**, **le domaine**, **le FQDN**, **le groupe**, **le nom d'hôte/l'IP**, **la méthode de Jump**, **le dernier accès**, **le nom**, **l'IP privée**, **l'IP publique**, **l'état**, **la balise et le groupe de travail**.

Panneau de détails sur le Jump Client

Lorsque vous sélectionnez un Jump Client, un panneau de détails s'affiche à droite de l'interface de Jump. Les détails affichés ici sont déterminés par le paramètre de **Statistiques des Jump Clients** dans l'interface /login, ainsi que par le système d'exploitation distant.

Si un Jump Client est déconnecté et ne se reconnecte pas à la B Series Appliance pendant le nombre de jours défini par les **Paramètres du Jump Client** de l'interface /login, il sera identifié comme étant perdu. Aucune action spécifique n'est effectuée sur le Jump Client. Il n'est défini comme étant perdu qu'à des fins d'identification, afin qu'un administrateur puisse diagnostiquer la raison de la perte de connexion et faire le nécessaire pour remédier à la situation. Dans le panneau de détails, la date de suppression planifiée s'affiche au cas où le Jump Client ne se reconnecte pas.

Après une mise à jour logicielle, les Jump Clients se mettent à jour automatiquement. Le nombre de mises à jour de Jump Client simultanées est déterminé par les paramètres sur la page **/login > Jump > Jump Clients**. Si un Jump Client n'a pas encore été mis à jour, il reçoit l'étiquette **Mise à niveau en attente**, et son numéro de version et de révision s'affiche dans le panneau de détails. Vous pouvez modifier un Jump Client obsolète, mais vous ne pouvez pas effectuer de Jump vers lui. Si vous tentez d'effectuer un Jump, ce Jump Client sera déplacé au début de la file d'attente de mise à niveau.

Wake-On-Lan (WOL)

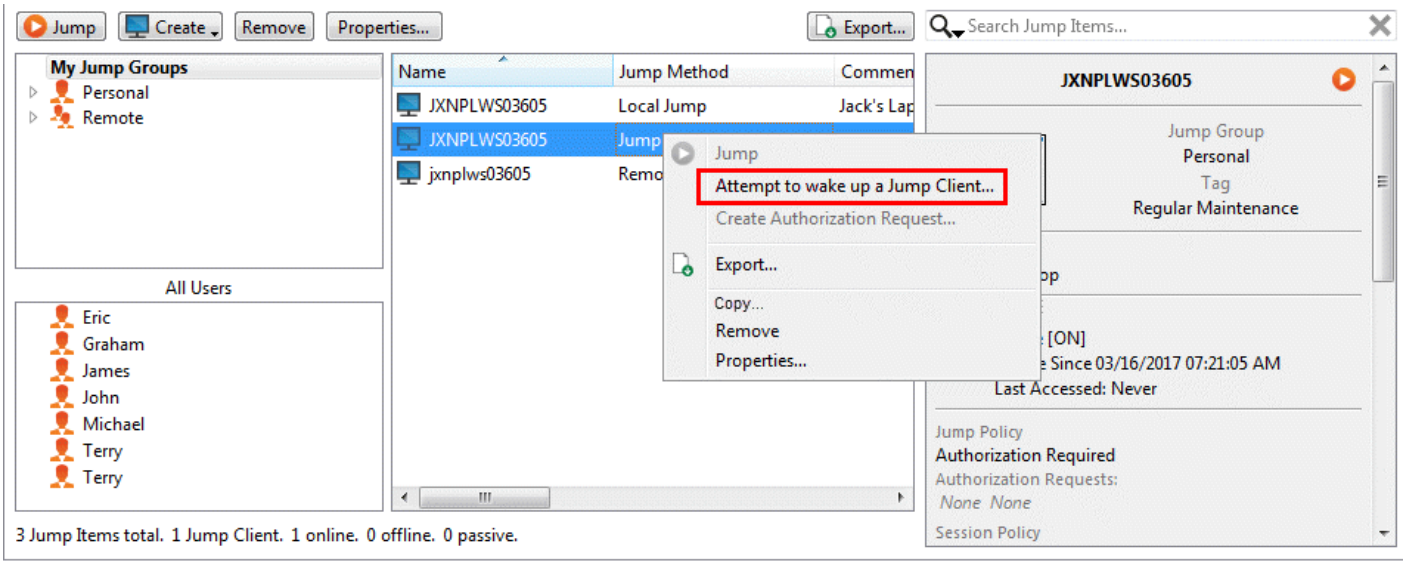
Le Wake-On-Lan (WOL) sert à mettre en route ou à réveiller à distance les machines configurées pour le WOL de BeyondTrust. Dans un environnement configuré, le client peut éteindre sa machine et bénéficier quand même de l'assistance technique BeyondTrust, si nécessaire.

> ***Remarque :*** *WOL n'est pas une technologie BeyondTrust. Le logiciel BeyondTrust s'intègre aux systèmes WOL existants. Pour utiliser WOL avec BeyondTrust, la fonction WOL du système doit être activée, et le réseau doit autoriser l'envoi de paquets de WOL.*

Pour autoriser la fonctionnalité WOL pour BeyondTrust, activez le paramètre WOL dans l'interface d'administration /login dans **Jump > Jump Clients**. Lors de l'activation de l'option WOL, veuillez prendre en compte ce qui suit :

- Le WOL n'est pas compatible avec les clients sans fil. Il est nécessaire de disposer d'une connexion câblée.
- Le WOL est pris en charge par le matériel du système sous-jacent, qui est indépendant du système d'exploitation installé.
- Le WOL n'est pris en charge que par les Jump Clients actifs. Les Jump Clients passifs, les Jumpoints et les Jump locaux des console du technicien d'assistance ne prennent pas en charge le WOL.

Pour réveiller un Jump Client actif à l'aide d'un WOL, faites un clic droit sur un Jump Client existant depuis la console du technicien d'assistance. Essayez de réveiller le système en cliquant sur l'option **Tentative de réveil d'un Jump Client**.



L'option de réveil n'est disponible que lors de la sélection d'un seul Jump Client. Elle n'est pas disponible lorsque plusieurs Jump Clients sont sélectionnés.

Les paquets WOL sont envoyés depuis des Jump Clients situés sur le même réseau que la machine cible. Lorsqu'on installe ou qu'on lance un Jump Client actif, ce dernier enregistre ses informations de réseau dans la B Series Appliance, et la B Series Appliance les utilise pour savoir quels Jump Clients se trouvent sur le même réseau.

Après avoir essayé de réveiller un Jump Client sélectionné, l'option WOL est grisée pendant 30 secondes avant de pouvoir envoyer une nouvelle demande de réveil. Si aucun autre Jump Client n'est disponible sur ce même réseau pour envoyer des paquets WOL à la machine cible, le technicien d'assistance reçoit un message lui indiquant qu'aucun autre Jump Client n'est disponible sur le réseau. Lors de l'envoi d'un paquet WOL, le technicien d'assistance dispose d'une option avancée pour fournir un mot de passe pour les environnements WOL nécessitant un mot de passe WOL sécurisé. Un paquet WOL est un paquet unidirectionnel, et le technicien d'assistance ne reçoit aucune confirmation, à part le fait d'observer le client en ligne sur sa console.

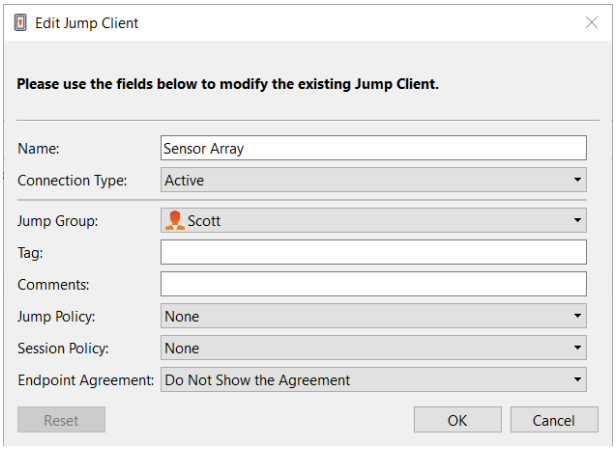
Copier des éléments de Jump

Les éléments de Jump peuvent être copiés et peuvent appartenir à plusieurs groupes de Jump. Cela comprend des éléments de Jump Client, fournissant aux administrateurs la capacité de définir des règles et des autorisations de groupe distinctes sans devoir installer un Jump Client additionnel sur le point de terminaison cible. Les utilisateurs dotés des autorisations appropriées voient l'option de **Copier** des éléments de Jump dans la Access Console en faisant un clic droit sur l'élément. Les utilisateurs peuvent aussi utiliser cette fonction sur plusieurs éléments de Jump.

Cette fonctionnalité permet aux administrateurs et aux utilisateurs de gérer efficacement différentes stratégies pour les éléments de Jump et les Jump Clients sans avoir besoin de créer un nouvel élément de Jump. Cette fonctionnalité permet aux utilisateurs de limiter le nombre de clients nécessaires pour activer les sessions Jump Client et de limiter les tâches administratives manuelles lors de la définition des chemins d'accès pour les utilisateurs.

Propriétés des Jump Clients

Organisez et gérez les éléments de Jump existants en en sélectionnant un ou plusieurs et en cliquant sur **Propriétés**.



> ***Remarque :*** *pour voir les propriétés de plusieurs éléments de Jump, les éléments sélectionnés doivent tous être du même type (que des Jump Clients, que des Jumps distants, etc.).*

Saisissez un **Nom** pour l'élément de Jump. Ce nom identifie l'élément dans les onglets de la session. Cette chaîne contient 128 caractères au maximum.

Changez le mode d'un Jump Client depuis le menu déroulant **Type de connexion**. Les Jump Clients actifs envoient des statistiques vers la B Series Appliance à intervalles définis. Les Jump Clients passifs envoient des statistiques vers la B Series Appliance une fois par jour, ou lors de l'« archivage » manuel.

> ***Remarque :*** *cette fonction n'est disponible que pour les clients possédant une B Series Appliance dans leurs locaux. Les clients du Cloud BeyondTrust n'ont pas accès à cette fonction.*

Selon les options définies par votre administrateur, ces statistiques peuvent inclure l'utilisateur de la console connecté, le système d'exploitation, le temps de fonctionnement du système, le processeur, le taux d'utilisation du disque et une capture d'écran de la dernière mise à jour de l'ordinateur distant.

Déplacez des éléments de Jump d'un groupe de Jumps à l'autre en utilisant le menu déroulant **Groupe de Jumps**. La possibilité de déplacer des éléments de Jump vers et depuis différents groupes de Jumps dépend des autorisations pour votre compte.

Organisez encore mieux vos éléments de Jump en saisissant le nom d'une **Balise** nouvelle ou existante. Bien que les éléments de Jump sélectionnés soient rassemblés sous cette balise, ils seront toujours listés dans le groupe de Jump auquel chacun d'eux est attaché. Pour ramener un élément de Jump vers son groupe de Jump de plus haut niveau, laissez ce champ vide.

Les éléments de Jump comprennent un champ **Commentaires** pour un nom ou une description, ce qui facilite et accélère le tri, la recherche et l'identification des éléments de Jump.

Pour régler le moment pendant lequel les utilisateurs sont autorisés à accéder à cet élément de Jump, si une notification d'accès doit être envoyée, ou si une autorisation ou un ID de ticket provenant de votre système de ticket externe est requis pour l'utilisation de cet élément de Jump, choisissez une **Règle de Jump**. Ces règles doivent être configurées par l'administrateur dans l'interface /login.

Choisissez une **règle de session** à attribuer à cet élément de Jump. La règle de session attribuée à cet élément de Jump a la priorité la plus élevée lors de la configuration des autorisations de session. Le fait de pouvoir définir ou non une règle de session dépend là encore des autorisations définies pour votre compte.

Choisissez un **Accord de point de terminaison** à attribuer à cet élément de Jump. En fonction de ce qui est sélectionné, un accord de point de terminaison s'affiche. S'il n'y a pas de réponse, l'accord est automatiquement accepté ou rejeté.

Si vous n'avez plus besoin d'accéder à un système distant, sélectionnez l'élément de Jump et cliquez sur **Supprimer** ou faites un clic droit sur l'élément de Jump et sélectionnez **Supprimer** dans le menu. Vous pouvez sélectionner plusieurs éléments de Jump afin de les supprimer simultanément.

> ***Remarque :*** *si l'utilisateur distant désinstalle manuellement un Jump Client, l'élément supprimé peut être signalé comme désinstallé ou être retiré de la liste d'éléments de Jump dans la access console. Si le Jump Client n'est pas en mesure de contacter la B Series Appliance lors de l'installation, l'élément affecté se maintient hors ligne. Cette option est disponible dans* ***/login > Jump > Jump Clients****. Si un Jump Client est déconnecté et ne se reconnecte pas à la B Series Appliance pendant 180 jours, il sera automatiquement désinstallé de l'ordinateur cible et supprimé de l'interface de Jump.*

Utiliser un Jump distant pour un accès autonome aux ordinateurs d'un réseau séparé

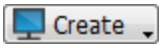
Un Jump distant permet à un utilisateur privilégié de se connecter à un ordinateur distant non autonome sur un réseau se trouvant en dehors de son réseau. Un Jump distant repose sur un Jumpoint.

Un Jumpoint sert de conduit pour un accès autonome aux ordinateurs Windows et Linux sur un réseau distant connu. Un Jumpoint unique installé sur un ordinateur dans un réseau local est utilisé pour accéder à plusieurs systèmes, ce qui élimine le besoin de préinstaller un logiciel sur chaque ordinateur auquel l'accès pourrait être nécessaire.

> ***Remarque :*** *Jumpoint est disponible uniquement pour les systèmes Windows et Linux. Des Jump Clients sont nécessaires pour l'accès à distance aux ordinateurs Mac. Pour effectuer un Jump vers un ordinateur Windows sans Jump Client, celui-ci doit être dans un domaine et le Service d'accès à distance au registre (désactivé par défaut sur Vista) doit être activé. Vous ne pouvez pas effectuer de Jump vers un appareil portable, mais la technologie Jump est disponible dans les consoles mobiles BeyondTrust.*

Créer un raccourci de Jump distant

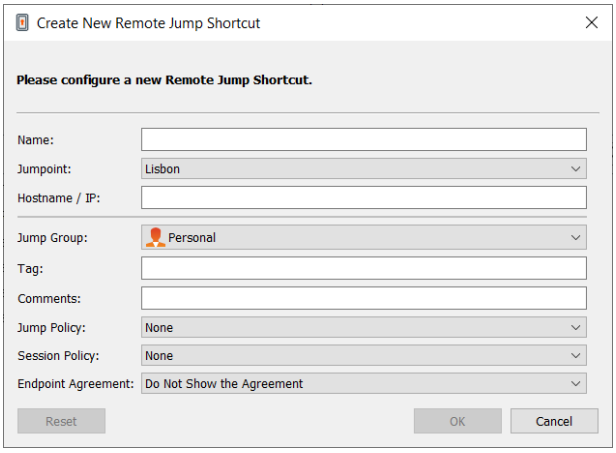
Pour créer un raccourci de Jump distant, cliquez sur le bouton **Créer** dans l'interface de Jump. Dans le menu déroulant, sélectionnez **Jump distant**. Les raccourcis de Jump distant apparaissent dans l'interface de Jump avec les Jump Clients et d'autres types de raccourcis d'élément de Jump.



Organisez et gérez les éléments de Jump existants en en sélectionnant un ou plusieurs et en cliquant sur **Propriétés**.

> ***Remarque :*** *pour voir les propriétés de plusieurs éléments de Jump, les éléments sélectionnés doivent tous être du même type (que des Jump Clients, que des Jumps distants, etc.).Pour examiner les propriétés d'autres types d'éléments de Jump, veuillez consulter la section correspondante de ce guide.*

Saisissez un **Nom** pour l'élément de Jump. Ce nom identifie l'élément dans les onglets de la session. Cette chaîne contient 128 caractères au maximum.



Dans la liste déroulante **Jumpoint**, sélectionnez le réseau qui héberge l'ordinateur auquel vous voulez accéder. La access console se souviendra de votre choix de Jumpoint la prochaine fois que vous créerez ce type d'élément de Jump.Saisissez le **nom d'hôte / IP** du système auquel vous souhaitez accéder.

Déplacez des éléments de Jump d'un groupe de Jumps à l'autre en utilisant le menu déroulant **Groupe de Jumps**. La possibilité de déplacer des éléments de Jump vers et depuis différents groupes de Jumps dépend des autorisations pour votre compte.

Organisez encore mieux vos éléments de Jump en saisissant le nom d'une **Balise** nouvelle ou existante. Bien que les éléments de Jump sélectionnés soient rassemblés sous cette balise, ils seront toujours listés dans le groupe de Jump auquel chacun d'eux est attaché. Pour ramener un élément de Jump vers son groupe de Jump de plus haut niveau, laissez ce champ vide.

Les éléments de Jump comprennent un champ **Commentaires** pour un nom ou une description, ce qui facilite et accélère le tri, la recherche et l'identification des éléments de Jump.

Pour régler le moment pendant lequel les utilisateurs sont autorisés à accéder à cet élément de Jump, si une notification d'accès doit être envoyée, ou si une autorisation ou un ID de ticket provenant de votre système de ticket externe est requis pour l'utilisation de cet élément de Jump, choisissez une **Règle de Jump**. Ces règles doivent être configurées par l'administrateur dans l'interface /login.

Choisissez une **règle de session** à attribuer à cet élément de Jump. La règle de session attribuée à cet élément de Jump a la priorité la plus élevée lors de la configuration des autorisations de session. Le fait de pouvoir définir ou non une règle de session dépend là encore des autorisations définies pour votre compte.

Choisissez un **Accord de point de terminaison** à attribuer à cet élément de Jump. En fonction de ce qui est sélectionné, un accord de point de terminaison s'affiche. S'il n'y a pas de réponse, l'accord est automatiquement accepté ou rejeté.

Utiliser un raccourci de Jump distant

Pour utiliser un raccourci de Jump pour démarrer une session, sélectionnez simplement le raccourci dans l'interface de Jump et cliquez sur le bouton **Jump**.

Une boîte de dialogue s'ouvre pour que vous fournissiez les informations d'authentification d'administration de l'ordinateur distant afin de pouvoir effectuer le Jump. Les droits d'administration utilisés doivent correspondre à un administrateur local du système distant ou à un administrateur de domaine.

Les fichiers clients seront envoyés sur le système distant, et une session essaiera de se lancer.

Remarque : *il est possible de configurer les éléments de Jump pour permettre à plusieurs utilisateurs d'accéder au même élément de Jump en simultané. Si l'option* ***Rejoindre une session existante*** *est activée, d'autres utilisateurs sont susceptibles de rejoindre une session déjà en cours. Le propriétaire initial de la session reçoit une notification lui indiquant qu'un autre utilisateur a rejoint la session, mais il n'est pas autorisé à lui refuser l'accès. Pour en savoir plus sur les Jumps simultanés, veuillez consulter Paramètres d'élément de Jump à l'adresse www.beyondtrust.com/docs/privileged-remote-access/getting-started/admin/jump-items.htm.*

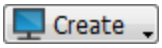
Utiliser un Jump local pour un accès autonome à des ordinateurs sur votre réseau local

Un Jump local permet à un utilisateur privilégié de se connecter à un ordinateur distant sans surveillance de son réseau local. Au sein du réseau local, l'ordinateur de l'utilisateur BeyondTrust peut initier une session vers un système Windows directement sans utiliser de Jumpoint, si les autorisations d'utilisateur appropriées sont activées. Un Jumpoint n'est nécessaire que lorsque l'ordinateur de l'utilisateur BeyondTrust ne peut pas accéder directement à l'ordinateur cible.

> ***Remarque :*** *le Jump local est disponible uniquement pour les systèmes Windows. Des Jump Clients sont nécessaires pour l'accès à distance aux ordinateurs Mac. Pour effectuer un Jump vers un ordinateur Windows sans Jump Client, celui-ci doit être dans un domaine et le Service d'accès à distance au registre (désactivé par défaut sur Vista) doit être activé.*

Créer un raccourci de Jump local

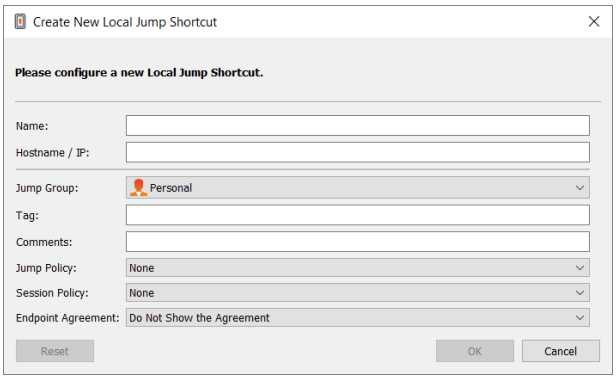
Pour créer un raccourci de Jump local, cliquez sur le bouton **Créer** dans l'interface de Jump. Dans le menu déroulant, sélectionnez **Jump local**. Les raccourcis de Jump local apparaissent dans l'interface de Jump avec les Jump Clients et d'autres types de raccourcis d'élément de Jump.



Organisez et gérez les éléments de Jump existants en en sélectionnant un ou plusieurs et en cliquant sur **Propriétés**.

> ***Remarque :*** *pour voir les propriétés de plusieurs éléments de Jump, les éléments sélectionnés doivent tous être du même type (que des Jump Clients, que des Jumps distants, etc.).Pour examiner les propriétés d'autres types d'éléments de Jump, veuillez consulter la section correspondante de ce guide.*

Saisissez un **Nom** pour l'élément de Jump. Ce nom identifie l'élément dans les onglets de la session. Cette chaîne contient 128 caractères au maximum.



Saisissez le **nom d'hôte / IP** du système auquel vous souhaitez accéder.

Déplacez des éléments de Jump d'un groupe de Jumps à l'autre en utilisant le menu déroulant **Groupe de Jumps**. La possibilité de déplacer des éléments de Jump vers et depuis différents groupes de Jumps dépend des autorisations pour votre compte.

Organisez encore mieux vos éléments de Jump en saisissant le nom d'une **Balise** nouvelle ou existante. Bien que les éléments de Jump sélectionnés soient rassemblés sous cette balise, ils seront toujours listés dans le groupe de Jump auquel chacun d'eux est attaché. Pour ramener un élément de Jump vers son groupe de Jump de plus haut niveau, laissez ce champ vide.

Les éléments de Jump comprennent un champ **Commentaires** pour un nom ou une description, ce qui facilite et accélère le tri, la recherche et l'identification des éléments de Jump.

Pour régler le moment pendant lequel les utilisateurs sont autorisés à accéder à cet élément de Jump, si une notification d'accès doit être envoyée, ou si une autorisation ou un ID de ticket provenant de votre système de ticket externe est requis pour l'utilisation de cet élément de Jump, choisissez une **Règle de Jump**. Ces règles doivent être configurées par l'administrateur dans l'interface /login.

Choisissez une **règle de session** à attribuer à cet élément de Jump. La règle de session attribuée à cet élément de Jump a la priorité la plus élevée lors de la configuration des autorisations de session. Le fait de pouvoir définir ou non une règle de session dépend là encore des autorisations définies pour votre compte.

Choisissez un **Accord de point de terminaison** à attribuer à cet élément de Jump. En fonction de ce qui est sélectionné, un accord de point de terminaison s'affiche. S'il n'y a pas de réponse, l'accord est automatiquement accepté ou rejeté.

Utiliser un raccourci de Jump local

Pour utiliser un raccourci de Jump pour démarrer une session, sélectionnez simplement le raccourci dans l'interface de Jump et cliquez sur le bouton **Jump**.

Une boîte de dialogue s'ouvre pour que vous fournissiez les informations d'authentification d'administration de l'ordinateur distant afin de pouvoir effectuer le Jump. Les droits d'administration utilisés doivent correspondre à un administrateur local du système distant ou à un administrateur de domaine.

Les fichiers clients seront envoyés sur le système distant, et une session essaiera de se lancer.

Remarque : *il est possible de configurer les éléments de Jump pour permettre à plusieurs utilisateurs d'accéder au même élément de Jump en simultané. Si l'option* ***Rejoindre une session existante*** *est activée, d'autres utilisateurs sont susceptibles de rejoindre une session déjà en cours. Le propriétaire initial de la session reçoit une notification lui indiquant qu'un autre utilisateur a rejoint la session, mais il n'est pas autorisé à lui refuser l'accès. Pour en savoir plus sur les Jumps simultanés, veuillez consulter Paramètres d'élément de Jump à l'adresse www.beyondtrust.com/docs/privileged-remote-access/getting-started/admin/jump-items.htm.*

Utiliser RDP pour accéder à un point de terminaison Windows distant

Utilisez BeyondTrust pour démarrer une session de protocole de bureau à distance (RDP) avec des systèmes Windows et Linux distants. Comme les sessions de protocole de bureau à distance passent à travers un Jumpoint et sont converties en sessions BeyondTrust, les utilisateurs peuvent partager ou transférer des sessions, et celles-ci peuvent être automatiquement contrôlées et enregistrées, selon la configuration définie par l'administrateur pour votre site. Pour utiliser RDP à travers BeyondTrust, vous devez avoir accès à un Jumpoint et avoir l'autorisation du compte utilisateur **Méthodes de Jump autorisées : RDP à travers un Jumpoint**.

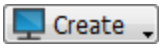
Remarque : *Vous pouvez utiliser votre propre outil RDP pour des sessions RDP distantes. Pour plus d'informations, consultez* *« Changer les paramètres et préférences dans la console d'accès », page 10*.

IMPORTANT !

Afin d'utiliser votre propre outil, vous devez activer ***Jump en tunnel par protocole*** *dans* ***/login > Utilisateurs et sécurité > Utilisateurs > Technologie Jump > Jump en tunnel par protocole***.

Créer un raccourci de RDP

Pour créer un raccourci de protocole de bureau à distance Microsoft, cliquez sur le bouton **Créer** dans l'interface de Jump. Dans le menu déroulant, sélectionnez **RDP distant**. Les raccourcis RDP apparaissent dans l'interface de Jump avec les Jump Clients et d'autres types de raccourcis d'élément de Jump.



Organisez et gérez les éléments de Jump existants en en sélectionnant un ou plusieurs et en cliquant sur **Propriétés**.

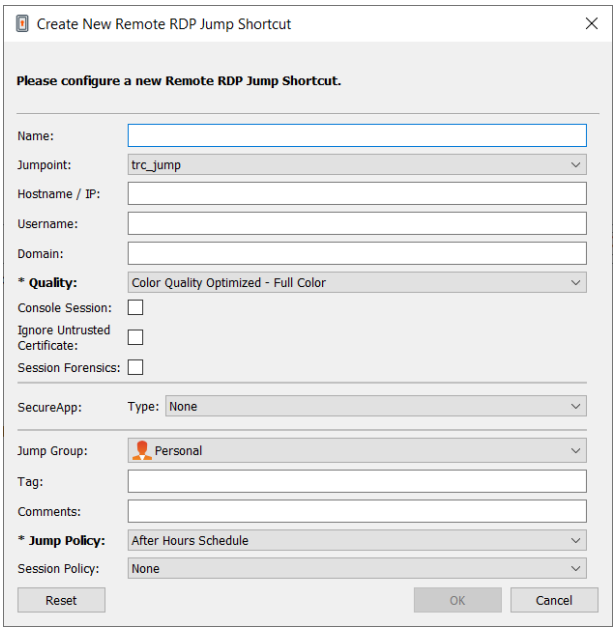
Remarque : *pour voir les propriétés de plusieurs éléments de Jump, les éléments sélectionnés doivent tous être du même type (que des Jump Clients, que des Jumps distants, etc.).Pour examiner les propriétés d'autres types d'éléments de Jump, veuillez consulter la section correspondante de ce guide.*

Saisissez un **Nom** pour l'élément de Jump. Ce nom identifie l'élément dans les onglets de la session. Cette chaîne contient 128 caractères au maximum.

Dans la liste déroulante **Jumpoint**, sélectionnez le réseau qui héberge l'ordinateur auquel vous voulez accéder. La access console se souviendra de votre choix de Jumpoint la prochaine fois que vous créerez ce type d'élément de Jump.Saisissez le **nom d'hôte / IP** du système auquel vous souhaitez accéder.

Indiquez le **nom d'utilisateur** à utiliser pour la connexion, ainsi que le **domaine**.

Définissez la **qualité** d'affichage de l'écran distant. Notez que ce réglage ne peut plus être modifié une fois la session de protocole de bureau à distance démarrée. 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.



Pour démarrer une session de console plutôt qu'une nouvelle session, cochez la case **Session de console**.

Si le certificat du serveur ne peut pas être vérifié, vous recevrez un avertissement. Cocher l'option **Ignorer ce certificat non approuvé** vous permet de vous connecter au système distant sans voir ce message.

> ***Remarque :*** *lorsque RemoteApp ou l'agent d'accès au bureau à distance BeyondTrust est sélectionné dans la section SecureApp, la case* ***Session de console*** *est décochée. Les applications distantes ne peuvent s'exécuter sur une session de console d'un serveur RDP.*

Pour obtenir des informations plus détaillées sur la session RDP, cochez **Preuves de session**. Pour que cette fonction soit utilisable, vous devez sélectionner un **Compte de service RDP** pour le Jumpoint en cours d'utilisation. Lors de la coche de ce paramètre, le rappel suivant s'affiche :

L'activation de cette fonction exige que le serveur RDP soit configuré pour recevoir l'agent de contrôle et qu'un compte de service RDP soit configuré avec ce Jumpoint. Si ces exigences ne sont pas satisfaites, toutes les tentatives de démarrer une session échoueront.

> ***Remarque :*** *le paramètre de compte de service RDP ne doit pas utiliser un compte d'administrateur local et doit utiliser un compte d'administrateur de domaine avec des privilèges minimaux, y compris l'accès pour créer des services distants et accéder à des systèmes de fichiers distants.*

Lorsque **Preuves de session** est coché, les détails supplémentaires qui suivent sont enregistrés :

- Événement modifié de fenêtre ciblée
- Événement de clic de souris
- Événement de menu ouvert
- Événement de nouvelle fenêtre ouverte

Pour lancer une session avec une application distante, configurez la section **SecureApp**. Les paramètres du menu déroulant suivants sont disponibles :

- **Aucun :** lorsqu'on accède à un élément de Jump RDP distant, aucune application n'est lancée.
- **RemoteApp :** l'utilisateur peut configurer un profil d'application ou un argument de commande qui exécute et ouvre une application sur un serveur distant. Pour la configuration, sélectionnez l'option **RemoteApp** et indiquez les informations suivantes.
    - **Nom de l'appli distante :** saisissez le nom de l'application à laquelle vous souhaitez vous connecter.
    - **Paramètres de l'appli distante :** saisissez les informations de profil ou les arguments de la ligne de commande nécessaires pour ouvrir l'application.
- **Agent de bureau à distance de BeyondTrust :** cette option facilite le transfert de paramètres à travers un agent afin de lancer des applications sur un hôte distant. Pour la configuration, sélectionnez l'option **Agent de bureau à distance de BeyondTrust** et indiquez les informations suivantes :
    - **Emplacement d'exécutable :** saisissez le chemin de l'application à laquelle l'agent se connectera.
    - **Paramètres :** saisissez tout paramètre que vous saisiriez normalement dans une ligne de commande lors du lancement d'une application sur le système distant.

> *Pour plus d'informations sur les preuves de session et le compte de service RDP, veuillez consulter Jumpoint : Configuration d'un accès sans surveillance à un réseau > Compte de service RDP à l'adresse https://www.beyondtrust.com/fr/docs/privileged-remote-access/getting-started/admin/jumpoint.htm.*

Injecter des informations d'authentification

L'option **Injecter des informations d'authentification** sera disponible lorsque le type **Agent de bureau à distance de BeyondTrust** est sélectionné. Cette option facilite le transfert de paramètres et d'informations d'authentification à travers un agent afin de lancer des applications sur un hôte distant. Le premier ensemble d'informations d'authentification se trouve dans la définition du Jump et comporte les informations d'authentification du compte utilisateur que vous utiliserez pour vous connecter au système distant. Il existe une invite secondaire pour des informations d'authentification supplémentaires, qu'elles soient fournies manuellement ou à partir d'une banque de mots de passe. Ces informations d'authentification secondaires sont rendues disponibles pour la ligne de commande que vous avez définie à travers les macros %USERNAME% et %PASSWORD% (macros supplémentaires montrées ci-dessous). Cela vous permet de transmettre des informations d'authentification supplémentaires à l'application que vous lancez (exemple : SQL Server Management Studio). Pour la configuration, sélectionnez l'option **Agent de bureau à distance de BeyondTrust** et indiquez les informations suivantes :

- Saisissez l'**emplacement d'exécutable** et les **paramètres** tel que décrit ci-dessus.
- **Système cible :** saisissez le nom du système exécutant l'application.
- **Type d'informations d'authentification :** saisissez le type d'informations d'authentification tel que défini par le système de gestion d'informations d'authentification (exemple : SQL)

Nom de la macro	Résultat
%USERNAME%	nom d'utilisateur
%USERPRINCIPLENAME%	utilisateur@domaine
%DOWNLEVELLOGONNAME%	domain\username
%DOMAIN%	domaine
%PASSWORD%	mot de passe
%PASSWORDRAW%	mot de passe (sans tentative d'échappement des caractères spéciaux)
%TARGETSYSTEM%	valeur système de la cible fournie ; dans le cas d'un serveur SQL, cela serait le nom du serveur SQL.
%APPLICATIONNAME%	nom d'application facultatif ; dans le cas d'un serveur SQL, cela pourrait être incorporé en programme sous « SQL Server » ou similaire.

> ***Remarque :*** *l'option* ***Agent de bureau à distance de BeyondTrust*** *nécessite la préconfiguration de l'****Agent de bureau à distance de BeyondTrust*** *sur le système cible. Cet agent peut être téléchargé sur la page* ***Mon compte*** *dans l'interface* ***/login****. Cela n'est spécifique à aucune version ou aucun site ; ainsi, le même agent peut être utilisé pour autant d'applications que l'administrateur souhaite prendre en charge. Une fois l'agent installé, vous pourrez alors utiliser BeyondTrust pour créer des éléments de Jump RDP configurés pour utiliser l'option Agent d'accès au bureau à distance de BeyondTrust afin de lancer toute application installée sur le système distant.*

> ***Remarque :*** *SecureApp s'appuie sur des applications de publication utilisant RemoteApps de Microsoft RDS. Veuillez consulter la documentation de Microsoft pour les applications de publication.*

Déplacez des éléments de Jump d'un groupe de Jumps à l'autre en utilisant le menu déroulant **Groupe de Jumps**. La possibilité de déplacer des éléments de Jump vers et depuis différents groupes de Jumps dépend des autorisations pour votre compte.

Organisez encore mieux vos éléments de Jump en saisissant le nom d'une **Balise** nouvelle ou existante. Bien que les éléments de Jump sélectionnés soient rassemblés sous cette balise, ils seront toujours listés dans le groupe de Jump auquel chacun d'eux est attaché. Pour ramener un élément de Jump vers son groupe de Jump de plus haut niveau, laissez ce champ vide.

Les éléments de Jump comprennent un champ **Commentaires** pour un nom ou une description, ce qui facilite et accélère le tri, la recherche et l'identification des éléments de Jump.

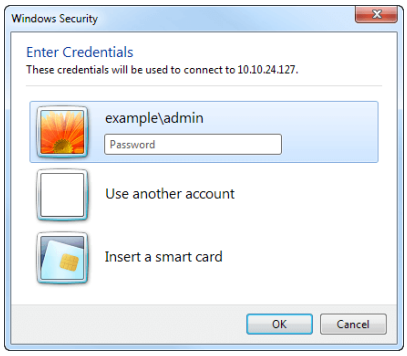
Pour régler le moment pendant lequel les utilisateurs sont autorisés à accéder à cet élément de Jump, si une notification d'accès doit être envoyée, ou si une autorisation ou un ID de ticket provenant de votre système de ticket externe est requis pour l'utilisation de cet élément de Jump, choisissez une **Règle de Jump**. Ces règles doivent être configurées par l'administrateur dans l'interface /login.

> *Pour en savoir plus sur les utilisateurs de base de données autonome, consultez Utilisateurs de base de données autonome - Rendre votre base de données portable à l'adresse docs.microsoft.com/en-us/sql/relational-databases/security/contained-database-users-making-your-database-portable.*

Utiliser un raccourci de RDP

Pour utiliser un raccourci de Jump pour démarrer une session, sélectionnez simplement le raccourci dans l'interface de Jump et cliquez sur le bouton **Jump**.

Vous êtes invité à saisir le mot de passe associé au nom d'utilisateur indiqué au préalable.



La session de protocole de bureau à distance (RDP) démarre.

Remarque : *lorsque vous lancez une session RDP, la langue du clavier RDP correspondra automatiquement à celle de la console d'accès. Cette fonction n'est disponible que pour les consoles d'accès sur Windows.*

Vous pouvez alors initier le partage d'écran afin de visualiser le bureau distant. Vous pouvez envoyer la commande Ctrl-Alt-Suppr, effectuer une capture d'écran du bureau distant, partager le contenu du presse-papiers, utiliser les commandes Alt et Maj et envoyer des pressions de touche. Vous pouvez aussi partager la session RDP avec d'autres utilisateurs BeyondTrust connectés, selon les règles habituelles définies par les paramètres de votre compte d'utilisateur.

Remarque : *il est possible de configurer les éléments de Jump pour permettre à plusieurs utilisateurs d'accéder au même élément de Jump en simultané. Si ce paramètre est réglé sur* ***Démarrer une nouvelle session****, une nouvelle session indépendante commence pour chaque utilisateur effectuant un jump vers un élément de Jump RDP spécifique. La configuration RDP sur le point de terminaison définit le comportement relatif aux connexions RDP simultanées. Pour en savoir plus sur les Jumps simultanés, veuillez consulter Paramètres d'élément de Jump à l'adresse www.beyondtrust.com/docs/privileged-remote-access/getting-started/admin/jump-items.htm.*

Utiliser le VNC pour accéder à un point de terminaison Windows distant

Utilisez BeyondTrust pour démarrer une session VNC avec un système Windows distant. Étant donné que les sessions VNC passent à travers un Jumpoint et sont converties en sessions BeyondTrust, les utilisateurs peuvent partager ou transférer des sessions, et celles-ci peuvent être automatiquement contrôlées et enregistrées, selon la configuration définie par l'administrateur pour votre site. Pour utiliser le VNC à travers BeyondTrust, vous devez avoir accès à un Jumpoint et avoir l'autorisation du compte utilisateur **Méthodes de Jump autorisées : VNC distant à travers un Jumpoint**.

Créer un raccourci VNC

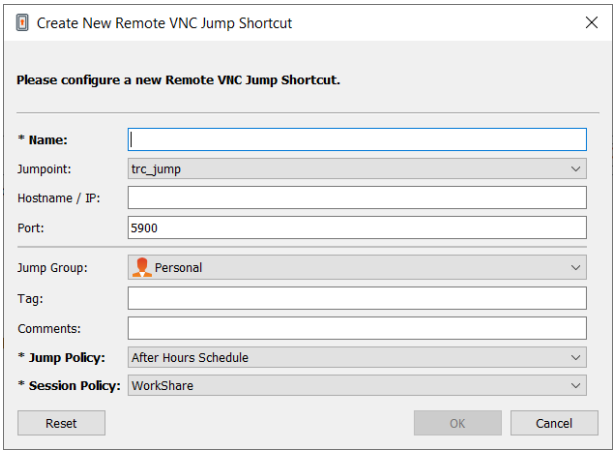
Pour créer un raccourci VNC, cliquez sur le bouton **Créer** dans l'interface de Jump. Dans le menu déroulant, sélectionnez **VNC distant**. Les raccourcis VNC apparaissent dans l'interface de Jump avec les Jump Clients et d'autres types de raccourcis d'élément de Jump.

Organisez et gérez les éléments de Jump existants en en sélectionnant un ou plusieurs et en cliquant sur **Propriétés**.

> ***Remarque :*** *pour voir les propriétés de plusieurs éléments de Jump, les éléments sélectionnés doivent tous être du même type (que des Jump Clients, que des Jumps distants, etc.).Pour examiner les propriétés d'autres types d'éléments de Jump, veuillez consulter la section correspondante de ce guide.*

Saisissez un **Nom** pour l'élément de Jump. Ce nom identifie l'élément dans les onglets de la session. Cette chaîne contient 128 caractères au maximum.

Dans la liste déroulante **Jumpoint**, sélectionnez le réseau qui héberge l'ordinateur auquel vous voulez accéder. La access console se souviendra de votre choix de Jumpoint la prochaine fois que vous créerez ce type d'élément de Jump.Saisissez le **nom d'hôte / IP** du système auquel vous souhaitez accéder.



> ***Remarque :*** *par défaut, le serveur VNC écoute sur le port 5900, qui est donc le port par défaut des tentatives BeyondTrust. Si le serveur VNC distant est configuré pour utiliser un port différent, ajoutez-le à la suite du nom d'hôte ou de l'adresse IP au format* ***<hostname>:<port>*** *ou* ***<ipaddress>:<port>*** *(par exemple, 10.10.24.127:40000).*

Déplacez des éléments de Jump d'un groupe de Jumps à l'autre en utilisant le menu déroulant **Groupe de Jumps**. La possibilité de déplacer des éléments de Jump vers et depuis différents groupes de Jumps dépend des autorisations pour votre compte.

Organisez encore mieux vos éléments de Jump en saisissant le nom d'une **Balise** nouvelle ou existante. Bien que les éléments de Jump sélectionnés soient rassemblés sous cette balise, ils seront toujours listés dans le groupe de Jump auquel chacun d'eux est attaché. Pour ramener un élément de Jump vers son groupe de Jump de plus haut niveau, laissez ce champ vide.

Les éléments de Jump comprennent un champ **Commentaires** pour un nom ou une description, ce qui facilite et accélère le tri, la recherche et l'identification des éléments de Jump.

Pour régler le moment pendant lequel les utilisateurs sont autorisés à accéder à cet élément de Jump, si une notification d'accès doit être envoyée, ou si une autorisation ou un ID de ticket provenant de votre système de ticket externe est requis pour l'utilisation de cet élément de Jump, choisissez une **Règle de Jump**. Ces règles doivent être configurées par l'administrateur dans l'interface /login.

Utiliser un raccourci VNC

Pour utiliser un raccourci de Jump pour démarrer une session, sélectionnez simplement le raccourci dans l'interface de Jump et cliquez sur le bouton **Jump**.

Lorsque la connexion au serveur VNC est établie, le système tente de déterminer si des informations d'authentification lui sont associées. Si tel est le cas, vous êtes invité à les saisir.

Votre session VNC commence. Vous pouvez alors initier le partage d'écran afin de visualiser le bureau distant. Vous pouvez envoyer la commande Ctrl-Alt-Suppr, effectuer une capture d'écran du bureau distant et partager le contenu du presse-papiers. Vous pouvez aussi partager, transférer ou enregistrer la session VNC, selon les règles habituelles définies par les paramètres de votre compte d'utilisateur.

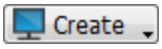
Remarque : *il est possible de configurer les éléments de Jump pour permettre à plusieurs utilisateurs d'accéder au même élément de Jump en simultané. Si l'option* ***Rejoindre une session existante*** *est activée, d'autres utilisateurs sont susceptibles de rejoindre une session déjà en cours. Le propriétaire initial de la session reçoit une notification lui indiquant qu'un autre utilisateur a rejoint la session, mais il n'est pas autorisé à lui refuser l'accès. Pour en savoir plus sur les Jumps simultanés, veuillez consulter Paramètres d'élément de Jump à l'adresse www.beyondtrust.com/docs/privileged-remote-access/getting-started/admin/jump-items.htm.*

Utiliser un Jump en tunnel par protocole pour établir une connexion TCP vers un système distant

En utilisant un Jump en tunnel par protocole, établissez une connexion TCP de votre système à un point de terminaison sur un réseau distant. Comme la connexion a lieu à travers un Jumpoint, l'administrateur peut contrôler quels utilisateurs bénéficient de l'accès, quand ils ont l'accès, et si les sessions sont enregistrées.

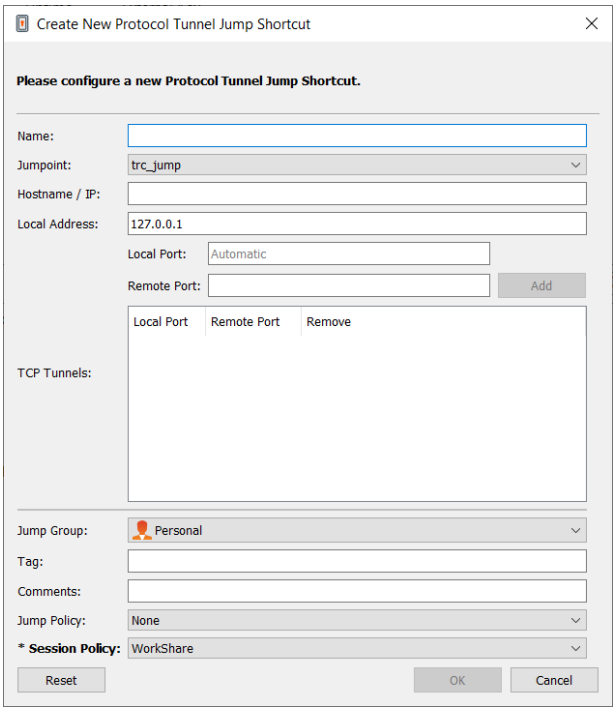
Créer un raccourci de Jump en tunnel par protocole

Pour créer un raccourci de Jump en tunnel par protocole, cliquez sur le bouton **Créer** dans l'interface de Jump. Dans le menu déroulant, sélectionnez **Jump en tunnel par protocole**. Les raccourcis de Jump en tunnel par protocole apparaissent dans l'interface de Jump avec les Jump Clients et d'autres types de raccourcis d'élément de Jump.



> ***Remarque :*** *les raccourcis de Jump en tunnel par protocole ne sont activés que si leur Jumpoint est configuré pour la méthode de Jump en tunnel par protocole sur la page* ***/login > Jump > Jumpoint****.*

Saisissez un **Nom** pour l'élément de Jump. Ce nom identifie l'élément dans les onglets de la session. Cette chaîne contient 128 caractères au maximum.



Dans la liste déroulante **Jumpoint**, sélectionnez le réseau qui héberge l'ordinateur auquel vous voulez accéder. La access console se souviendra de votre choix de Jumpoint la prochaine fois que vous créerez ce type d'élément de Jump.Saisissez le **nom d'hôte / IP** du système auquel vous souhaitez accéder.

Indiquez une **Adresse locale**. L'adresse par défaut 127.0.0.1. Si vous souhaitez vous connecter simultanément à plusieurs systèmes sur le même port distant, vous pouvez activer cette connexion en réglant chaque adresse du raccourci de Jump en tunnel par protocole sur une adresse dans la sous-plage 127.x.x.x.

Dans **Port local**, indiquez le port qui écoutera sur le système local de l'utilisateur. Si vous le laissez en automatique, la access console attribue un port libre.

Dans **Port distant**, indiquez le port auquel se connecter sur le système distant. Ceci est défini par le type de serveur auquel vous vous connectez.

Vous pouvez définir plusieurs paires de **Tunnels TCP** selon les besoins de votre configuration.

Déplacez des éléments de Jump d'un groupe de Jumps à l'autre en utilisant le menu déroulant **Groupe de Jumps**. La possibilité de déplacer des éléments de Jump vers et depuis différents groupes de Jumps dépend des autorisations pour votre compte.

Organisez encore mieux vos éléments de Jump en saisissant le nom d'une **Balise** nouvelle ou existante. Bien que les éléments de Jump sélectionnés soient rassemblés sous cette balise, ils seront toujours listés dans le groupe de Jump auquel chacun d'eux est attaché. Pour ramener un élément de Jump vers son groupe de Jump de plus haut niveau, laissez ce champ vide.

Les éléments de Jump comprennent un champ **Commentaires** pour un nom ou une description, ce qui facilite et accélère le tri, la recherche et l'identification des éléments de Jump.

Pour régler le moment pendant lequel les utilisateurs sont autorisés à accéder à cet élément de Jump, si une notification d'accès doit être envoyée, ou si une autorisation ou un ID de ticket provenant de votre système de ticket externe est requis pour l'utilisation de cet élément de Jump, choisissez une **Règle de Jump**. Ces règles doivent être configurées par l'administrateur dans l'interface /login.

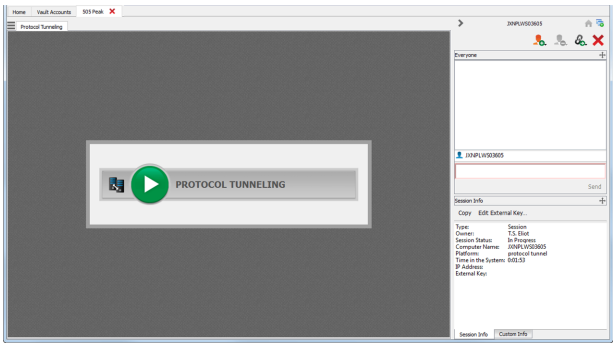
Organisez et gérez les éléments de Jump existants en en sélectionnant un ou plusieurs et en cliquant sur **Propriétés**.

> ***Remarque :*** *pour voir les propriétés de plusieurs éléments de Jump, les éléments sélectionnés doivent tous être du même type (que des Jump Clients, que des Jumps distants, etc.).Pour examiner les propriétés d'autres types d'éléments de Jump, veuillez consulter la section correspondante de ce guide.*

Utiliser un raccourci de Jump en tunnel par protocole

Pour utiliser un raccourci de Jump en tunnel par protocole pour démarrer une session, sélectionnez simplement le raccourci dans l'interface de Jump et cliquez sur le bouton **Jump**.

Une session apparaît dans votre access console. Cliquez sur le bouton **Tunnel par protocole** pour établir la connexion.

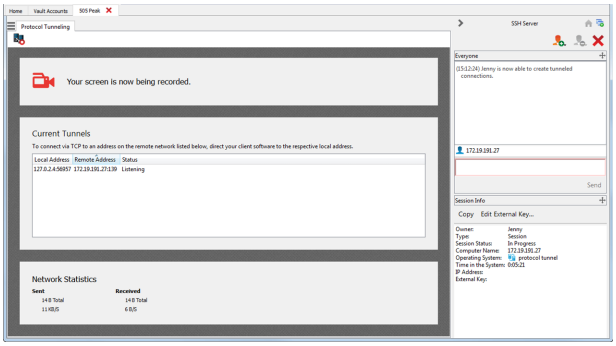


Si l'enregistrement d'écran est activé, une invite apparaît, vous informant que votre bureau sera enregistré. Cliquez sur **OK** pour continuer. Si vous cliquez sur **Annuler**, le tunnel par protocole n'est pas créé.

Si l'enregistrement d'écran est activé, un indicateur apparaît en haut de votre écran de session.

La section **Tunnels actuels** affiche les connexions actuelles et leur état. Vous pouvez aussi consulter les **Statistiques réseau** résumées.

Vous pouvez désormais ouvrir un client tiers pour effectuer des actions sur le système distant. Utilisez les ports indiqués pour vous connecter à travers le Jumpoint.



Conditions pour un bon fonctionnement

La fonction de tunnel par protocole fait passer le trafic du réseau par un tunnel d'une façon qui impose certaines restrictions sur la façon dont la communication doit se faire entre le système de l'utilisateur et le point de terminaison.

- Tout le trafic doit être en TCP.
- Un maximum de 256 connexions simultanées peuvent être gérées.
- Toutes les connexions TCP doivent provenir du point de terminaison et doivent être acceptées par le système de l'utilisateur qui écoute. Le protocole d'application ne peut pas exiger que le système de l'utilisateur établisse une connexion séparée revenant au point de terminaison.
- Toutes les connexions TCP que le point de terminaison établira en retour vers le système de l'utilisateur doivent être établies par des tunnels déjà définis dans les propriétés de l'élément de Jump en tunnel par protocole.
- Les systèmes d'exploitation interdisent en général aux processus non accrus d'écouter les ports inférieurs à 1024. Ainsi, le port local doit en général dépasser 1024. Le logiciel du point de terminaison se connecte au serveur en se connectant au port local sur lequel la access console (un processus non accru) est à l'écoute.
- Le logiciel du point de terminaison ne peut pas établir de connexions avec un système sur un réseau distant autre que celui indiqué dans les propriétés de l'élément de Jump en tunnel par protocole.
- Le protocole doit être agnostique envers le nom d'hôte que le point de terminaison utilise pour se connecter au serveur. Sinon, d'autres moyens doivent être fournis pour satisfaire aux exigences du protocole, comme l'association d'un nom d'hôte à 127.0.0.1 dans le fichier d'hôte, ou l'application d'une configuration spéciale au client de point de terminaison.
- Si la définition de tunnel a un port local différent du port distant (spécifiquement lorsque le port local doit être supérieur à 1024 parce que le port du serveur est inférieur à 1024), le protocole doit être agnostique envers le port utilisé par le client de point de terminaison pour se connecter au serveur.
- Tout protocole qui va au-delà du simple établissement d'une connexion TCP du client de point de terminaison au système de l'utilisateur requiert que l'administrateur connaisse son protocole spécifique et les conditions indiquées ci-dessus.

Utiliser un Shell Jump pour accéder à un appareil réseau distant

La technologie Shell Jump permet de se connecter rapidement à un dispositif réseau SSH ou Telnet, afin d'en utiliser la fonction de ligne de commande. Vous pouvez, par exemple, exécuter un script normalisé sur plusieurs systèmes afin d'installer un correctif ou de résoudre un problème de réseau. Les administrateurs peuvent activer le filtrage de commandes pour empêcher les utilisateurs d'utiliser accidentellement des commandes dommageables sur les points de terminaison connectés par SSH.

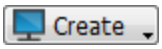
Remarque : *vous pouvez utiliser votre propre outil SSH pour le protocole SSH. Pour plus d'informations, consultez* *« Changer les paramètres et préférences dans la console d'accès », page 10.*

IMPORTANT !

Afin d'utiliser votre propre outil, vous devez activer ***Jump en tunnel par protocole*** *dans* ***/login > Utilisateurs et sécurité > Utilisateurs > Technologie Jump > Jump en tunnel par protocole****.*

Créer un raccourci de Shell Jump

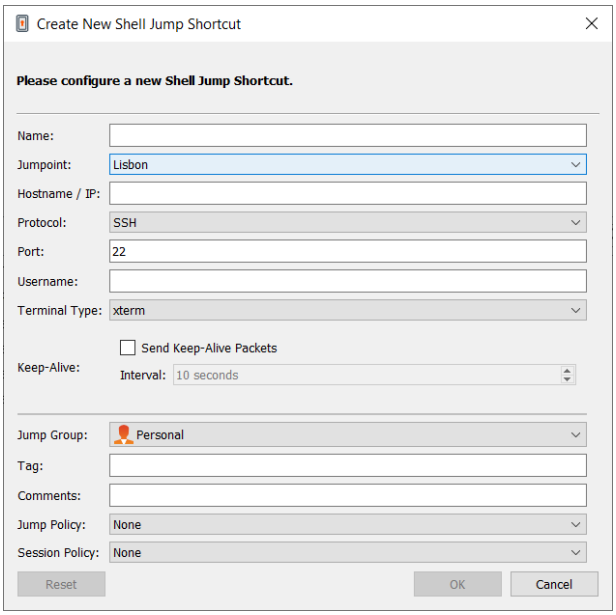
Pour créer un raccourci de Shell Jump, cliquez sur le bouton **Créer** dans l'interface de Jump. Dans le menu déroulant, sélectionnez **Shell Jump**. Les raccourcis de Shell Jump apparaissent dans l'interface de Jump avec les Jump Clients et d'autres types de raccourcis d'élément de Jump.



Remarque : *les raccourcis de Shell Jump ne sont activés que si leur Jumpoint est configuré pour un accès de Shell Jump ouvert ou limité.*

Organisez et gérez les éléments de Jump existants en en sélectionnant un ou plusieurs et en cliquant sur **Propriétés**.

Remarque : *pour voir les propriétés de plusieurs éléments de Jump, les éléments sélectionnés doivent tous être du même type (que des Jump Clients, que des Jumps distants, etc.).Pour examiner les propriétés d'autres types d'éléments de Jump, veuillez consulter la section correspondante de ce guide.*



Saisissez un **Nom** pour l'élément de Jump. Ce nom identifie l'élément dans les onglets de la session. Cette chaîne contient 128 caractères au maximum.

Dans la liste déroulante **Jumpoint**, sélectionnez le réseau qui héberge l'ordinateur auquel vous voulez accéder. La access console se souviendra de votre choix de Jumpoint la prochaine fois que vous créerez ce type d'élément de Jump.Saisissez le **nom d'hôte / IP** du système auquel vous souhaitez accéder.

Sélectionnez le **protocole** à utiliser, **SSH** ou **Telnet**.

Port bascule automatiquement vers le port par défaut du protocole sélectionné, mais il peut être modifié en fonction de vos paramètres réseau.

Saisissez le **nom d'utilisateur** avec lequel se connecter.

Sélectionnez le **type de terminal**, **xterm** ou **VT100**.

Vous pouvez également choisir d'**Envoyer des paquets de persistance** pour empêcher la clôture des sessions inactives. Indiquez le nombre de secondes devant s'écouler entre deux envois de paquets.

Déplacez des éléments de Jump d'un groupe de Jumps à l'autre en utilisant le menu déroulant **Groupe de Jumps**. La possibilité de déplacer des éléments de Jump vers et depuis différents groupes de Jumps dépend des autorisations pour votre compte.

Organisez encore mieux vos éléments de Jump en saisissant le nom d'une **Balise** nouvelle ou existante. Bien que les éléments de Jump sélectionnés soient rassemblés sous cette balise, ils seront toujours listés dans le groupe de Jump auquel chacun d'eux est attaché. Pour ramener un élément de Jump vers son groupe de Jump de plus haut niveau, laissez ce champ vide.

Les éléments de Jump comprennent un champ **Commentaires** pour un nom ou une description, ce qui facilite et accélère le tri, la recherche et l'identification des éléments de Jump.

Pour régler le moment pendant lequel les utilisateurs sont autorisés à accéder à cet élément de Jump, si une notification d'accès doit être envoyée, ou si une autorisation ou un ID de ticket provenant de votre système de ticket externe est requis pour l'utilisation de cet élément de Jump, choisissez une **Règle de Jump**. Ces règles doivent être configurées par l'administrateur dans l'interface /login.

Choisissez une **règle de session** à attribuer à cet élément de Jump. La règle de session attribuée à cet élément de Jump a la priorité la plus élevée lors de la configuration des autorisations de session. Le fait de pouvoir définir ou non une règle de session dépend là encore des autorisations définies pour votre compte.

Utiliser un raccourci de Shell Jump

Pour utiliser un raccourci de Shell Jump pour commencer une session, sélectionnez simplement le raccourci dans l'interface de Jump, puis cliquez sur le bouton **Jump**.

Si vous tentez d'effectuer un Shell Jump vers un périphérique SSH sans clé hôte en cache, vous recevrez une alerte indiquant que la clé hôte du serveur n'est pas en cache et qu'il n'y a aucune garantie que le serveur soit celui que vous pensez.

Si vous sélectionnez **Enregistrer la clé et se connecter**, la clé est mise en cache sur le système hôte du Jumpoint afin que cette alerte ne s'affiche plus pour les tentatives suivantes de Shell Jump vers ce système. L'option **Se connecter uniquement** lance la session sans mettre la clé en cache, et **Interrompre** met fin à la session Shell Jump.

Lorsque vous effectuez un Shell Jump vers un périphérique distant, une session d'interpréteur de commandes commence immédiatement avec cet appareil. Si vous effectuez un Shell Jump vers un appareil SSH approvisionné avec une clé non cryptée ou avec une clé cryptée dont le mot de passe a été mis en cache, vous n'êtes pas invité à fournir un mot de passe. Dans le cas contraire, vous devrez saisir un mot de passe. Vous pouvez ensuite envoyer des commandes au système distant.

Les administrateurs peuvent configurer le filtrage de commandes sur les éléments Shell Jump pour bloquer certaines commandes et en autoriser d'autres, dans le but d'empêcher un utilisateur d'utiliser accidentellement une commande pouvant provoquer des résultats indésirables. Dans le cas où un utilisateur essayerait d'utiliser une commande correspondant à une expression non autorisée, il se verrait présenter une invite et ne serait pas autorisé à exécuter la commande.

> ***Remarque :*** *le filtre de commandes de BeyondTrust utilise des expressions régulières étendues, ne devant pas être confondues avec egrep. Pour plus d'informations, rendez-vous à l'adresse docs.microsoft.com/en-us/cpp/standard-library/regular-expressions-cpp.*

Configurer le filtrage des invites d'interpréteur :

1. connectez-vous à l'interface /login en tant qu'utilisateur avec l'autorisation de configurer les éléments de Jump et les règles de session.
2. Rendez-vous dans **Jump > Éléments de Jump** et faites défiler vers le bas jusqu'à la section **Filtrage de Shell Jump**.
3. Dans la boîte de texte **Invites d'interpréteur reconnues**, saisissez des regex correspondant aux invites d'interpréteur de commandes sur vos systèmes de points de terminaison, une par ligne.

> ***Remarque :*** *les sauts de ligne ou les nouvelles lignes ne sont pas autorisés au sein des modèles d'invite de commande saisis. Si un système de point de terminaison utilise une invite multiligne, saisissez une expression correspondant uniquement à la ligne finale de l'invite dans la boîte de texte.*

4. Cliquez sur **Enregistrer**.

> ***Remarque :*** *après avoir saisi les regex que vous souhaitez utiliser, vous pouvez procéder à un test avec une invite d'interpréteur pour déterminer si elle correspond à l'une des regex de la liste. Cela vous permet de tester vos regex sans avoir à débuter une session. Saisissez l'expression dans la boîte de texte* ***Invite d'interpréteur*** *et cliquez sur le bouton* ***Vérifier****. Vous recevrez une notification vous indiquant si l'invite d'interpréteur que vous avez saisie correspond à l'une des regex de la liste.*

Configurer le filtrage des commandes :

1. Rendez-vous dans **Utilisateurs et sécurité > Règles de session** et créez une nouvelle règle ou modifiez-en une existante.

> ***Remarque :*** *vous pouvez également configurer cela pour les utilisateurs et/ou les règles de groupe.*

2. Localisez les paramètres **Interpréteur de commandes** dans la section Autorisations.
3. Comme vous utiliserez le filtrage de commande avec les éléments de Shell Jump, sélectionnez le bouton radio **Autoriser** pour permettre l'utilisation de l'interpréteur de commandes.
4. Choisissez entre **Autoriser toutes les commandes**, **Autoriser les modèles de commandes ci-dessous**, ou **Refuser les modèles de commandes ci-dessous** et spécifiez dans la boîte de texte quels modèles de regex vous souhaitez autoriser ou bloquer.

Remarque : *une fois que vous avez saisi les modèles de commande que vous souhaitez autoriser ou bloquer, vous pouvez tester des commandes dans la boîte de texte* ***Testeur de commandes****. Cela vous permet de tester vos filtres de commandes sans avoir à débuter une session. Cela vous permet de tester vos filtres de commandes sans avoir à débuter une session. Vous recevrez une notification vous indiquant si l'exécution d'une des commandes saisies serait autorisée sur le système distant, sur la base des regex spécifiées dans la liste.*

Les deux messages possibles sont :

- *La commande saisie sera autorisée selon vos sélections.*
- *La commande saisie sera bloquée selon vos sélections.*

Utiliser l'injection d'informations d'authentification avec SUDO sur un point de terminaison Linux

Pour utiliser l'injection d'informations d'authentification avec SUDO, un administrateur doit configurer un ou plusieurs comptes fonctionnels sur chaque point de terminaison Linux auxquels on pourra accéder par Shell Jump. Le processus pour configurer les fichiers sudoers étant complexe et différent pour chaque plate-forme, veuillez vous reporter à la documentation de votre plate-forme pour savoir comment accomplir ce processus. Chaque compte fonctionnel doit :

- Permettre l'authentification par SSH (mot de passe ou clé SSH)
- Avoir les informations d'authentification du compte stockées dans le gestionnaire d'informations d'authentification de point de terminaison
- Avoir une ou plusieurs entrées dans `/etc/sudoers` autorisant le compte fonctionnel à accéder à une ou plusieurs commandes devant être exécutées sans nécessiter un mot de passe (`NOPASSWD`).

Un administrateur doit créer un élément de Shell Jump pour le point de terminaison.

un administrateur doit ensuite configurer le gestionnaire d'informations d'authentification de point de terminaison et/ou la banque de mots de passe pour accorder aux utilisateurs l'accès aux comptes fonctionnels pour cet élément de Jump.

Lorsqu'un utilisateur effectue un Jump sur l'élément de Shell Jump, il peut choisir dans la liste de comptes fonctionnels disponibles pour ce point de terminaison. Chaque compte fonctionnel a son propre ensemble de commandes pouvant être exécutées en utilisant SUDO, comme configuré par l'administrateur sur le point de terminaison. Les informations d'authentification pour le compte sont transmises du gestionnaire d'informations d'authentification de point de terminaison au point de terminaison.

Remarque : *il est possible de configurer les éléments de Jump pour permettre à plusieurs utilisateurs d'accéder au même élément de Jump en simultané. Si l'option* ***Rejoindre une session existante*** *est activée, d'autres utilisateurs sont susceptibles de rejoindre une session déjà en cours. Le propriétaire initial de la session reçoit une notification lui indiquant qu'un autre utilisateur a rejoint la session, mais il n'est pas autorisé à lui refuser l'accès. Pour en savoir plus sur les Jumps simultanés, veuillez consulter Paramètres d'élément de Jump à l'adresse www.beyondtrust.com/docs/privileged-remote-access/getting-started/admin/jump-items.htm.*

Utiliser un Jump Web pour accéder à des services Web

Avec la prolifération des composants d'infrastructure étant passés à des interfaces basées sur le Web pour la configuration, les administrateurs informatiques sont confrontés à une situation de gestion de la sécurité de plus en plus complexe. Avec l'accès privilégié aux ressources basées sur le Web, il est difficile de contrôler, auditer et faire respecter une authentification efficace sans impacter de façon négative la productivité. Les administrateurs informatiques ont besoin d'un moyen efficace pour contrôler et auditer des ressources gérées par des interfaces Web, comme :

- Les serveurs IaaS (infrastructure comme service) hébergés en externe comme Amazon AWS, Microsoft Azure, IBM SoftLayer et Rackspace
- Les serveurs hébergés en interne gérés par des logiciels hyperviseurs comme VMware vSphere, Citrix XenServer et Microsoft Hyper-V
- Une infrastructure moderne de réseau central qui tire parti des interfaces basées sur le Web

Les capacités de gestion d'identité et d'accès varient grandement entre IaaS, fournisseurs d'hyperviseurs, et systèmes d'infrastructure centrale, et beaucoup ne proposent pas la prise en charge de l'authentification plurifactorielle, omettant ainsi ce niveau de sécurité supplémentaire. Ces disparités parmi les systèmes créent des opportunités de vulnérabilités professionnelles, comme l'utilisation abusive de comptes et d'accès, ce qui mène à des fuites de données sensibles. Jump Web BeyondTrust est la couche supplémentaire de sécurité pour authentifier ces systèmes.

IMPORTANT !

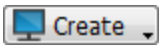
Web Jump ne prend pas en charge Flash. Assurez-vous de consulter la documentation de votre hyperviseur et de le mettre à jour vers une version prenant en charge HTML 5.

***Remarque :** l'élément de Jump Web est un add-on pour Privileged Remote Access et nécessite un achat supplémentaire.*

Créer un raccourci de Jump Web

***Remarque :** avant de créer des raccourcis de Jump Web, vérifiez que votre compte d'utilisateur peut accéder aux Jumps Web. Cette autorisation est définie dans votre compte d'utilisateur dans l'interface /login sous **Autorisations d'accès > Technologie Jump**.*

Pour créer un raccourci de Jump Web, cliquez sur le bouton **Créer** dans l'interface de Jump. Dans le menu déroulant, sélectionnez **Jump Web**. Les raccourcis de Jump Web apparaissent dans l'interface de Jump avec les Jump Clients et d'autres types de raccourcis d'éléments de Jump.



Organisez et gérez les éléments de Jump existants en en sélectionnant un ou plusieurs et en cliquant sur **Propriétés**.

***Remarque :** pour voir les propriétés de plusieurs éléments de Jump, les éléments sélectionnés doivent tous être du même type (que des Jump Clients, que des Jumps distants, etc.).Pour examiner les propriétés d'autres types d'éléments de Jump, veuillez consulter la section correspondante de ce guide.*

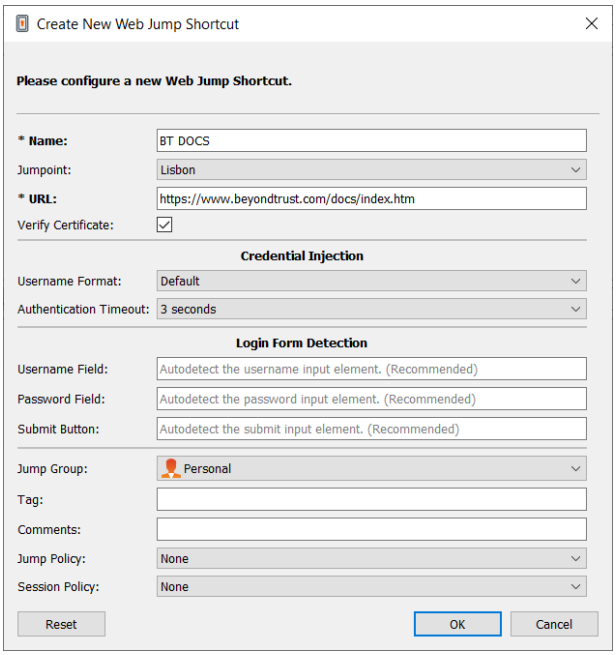
Saisissez un **Nom** pour l'élément de Jump. Ce nom identifie l'élément dans les onglets de la session. Cette chaîne contient 128 caractères au maximum.

Dans la liste déroulante **Jumpoint**, sélectionnez le Jumpoint Windows ou Linux qui héberge l'ordinateur auquel vous voulez accéder.

> ***Remarque :*** *la fonctionnalité Copier/Coller n'est pas prise en charge pour les Jumpoints Linux.*

Tapez l'**URL** du site auquel vous souhaitez accéder.

Consultez **Vérifier le certificat** si vous souhaitez que le certificat du site soit validé avant que la connexion ne soit établie. Si cette option est cochée et que des problèmes de certificat sont détectés, la session ne démarre pas.



IMPORTANT !

*Il convient de décocher **Vérifier le certificat** uniquement si vous effectuez un Jump vers un site de confiance utilisant un certificat auto-signé.*

Si vous voulez utiliser une injection d'informations d'authentification, vous devez d'abord sélectionner le **Format du nom d'utilisateur** :

- **Par défaut** : Il s'agit de la valeur par défaut pour les éléments de Jump Web nouveaux et existants. Le nom d'utilisateur n'est pas modifié avant l'injection dans la page Web et est utilisé dans le format stocké. Pour le gestionnaire d'informations d'authentification de point de terminaison (ECM), les informations d'authentification peuvent être au format UPN ou DLLN. Pour Vault, le nom d'utilisateur est toujours au format UPN.
- **Nom d'utilisateur uniquement** : Indépendamment du format stocké dans Vault ou l'ECM **(username@domain** ou **domain\username**), le domaine est supprimé et seul le nom d'utilisateur est utilisé.

Sous **Détection de formulaire de connexion**, fournissez des informations pour les trois options, comme requis :

- **Champ du nom d'utilisateur** : Ce paramètre spécifie l'indice pour le champ du nom d'utilisateur sur la page de connexion. L'injection échoue si aucun champ de nom d'utilisateur n'est trouvé. Un message d'erreur s'affiche pour indiquer qu'il est impossible de trouver le champ du nom d'utilisateur.
- **Champ du mot de passe** : Ce paramètre spécifie l'indice pour le champ du mot de passe sur la page de connexion. L'injection échoue si aucun champ de mot de passe n'est trouvé. Un message d'erreur s'affiche pour indiquer qu'il est impossible de trouver le champ du mot de passe.
- **Bouton Soumettre** : Ce paramètre spécifie l'indice pour le bouton Soumettre sur la page de connexion. L'injection échoue si aucun bouton de ce type n'est trouvé. Un message d'erreur s'affiche pour indiquer qu'il est impossible de trouver le bouton Soumettre.

> ***Remarque :*** *si ces trois champs sont laissés vides, le système le détecte automatiquement et utilise les informations nécessaires déjà enregistrées pour la connexion.*

Déplacez des éléments de Jump d'un groupe de Jumps à l'autre en utilisant le menu déroulant **Groupe de Jumps**. La possibilité de déplacer des éléments de Jump vers et depuis différents groupes de Jumps dépend des autorisations pour votre compte.

Organisez encore mieux vos éléments de Jump en saisissant le nom d'une **Balise** nouvelle ou existante. Bien que les éléments de Jump sélectionnés soient rassemblés sous cette balise, ils seront toujours listés dans le groupe de Jump auquel chacun d'eux est attaché. Pour ramener un élément de Jump vers son groupe de Jump de plus haut niveau, laissez ce champ vide.

Les éléments de Jump comprennent un champ **Commentaires** pour un nom ou une description, ce qui facilite et accélère le tri, la recherche et l'identification des éléments de Jump.

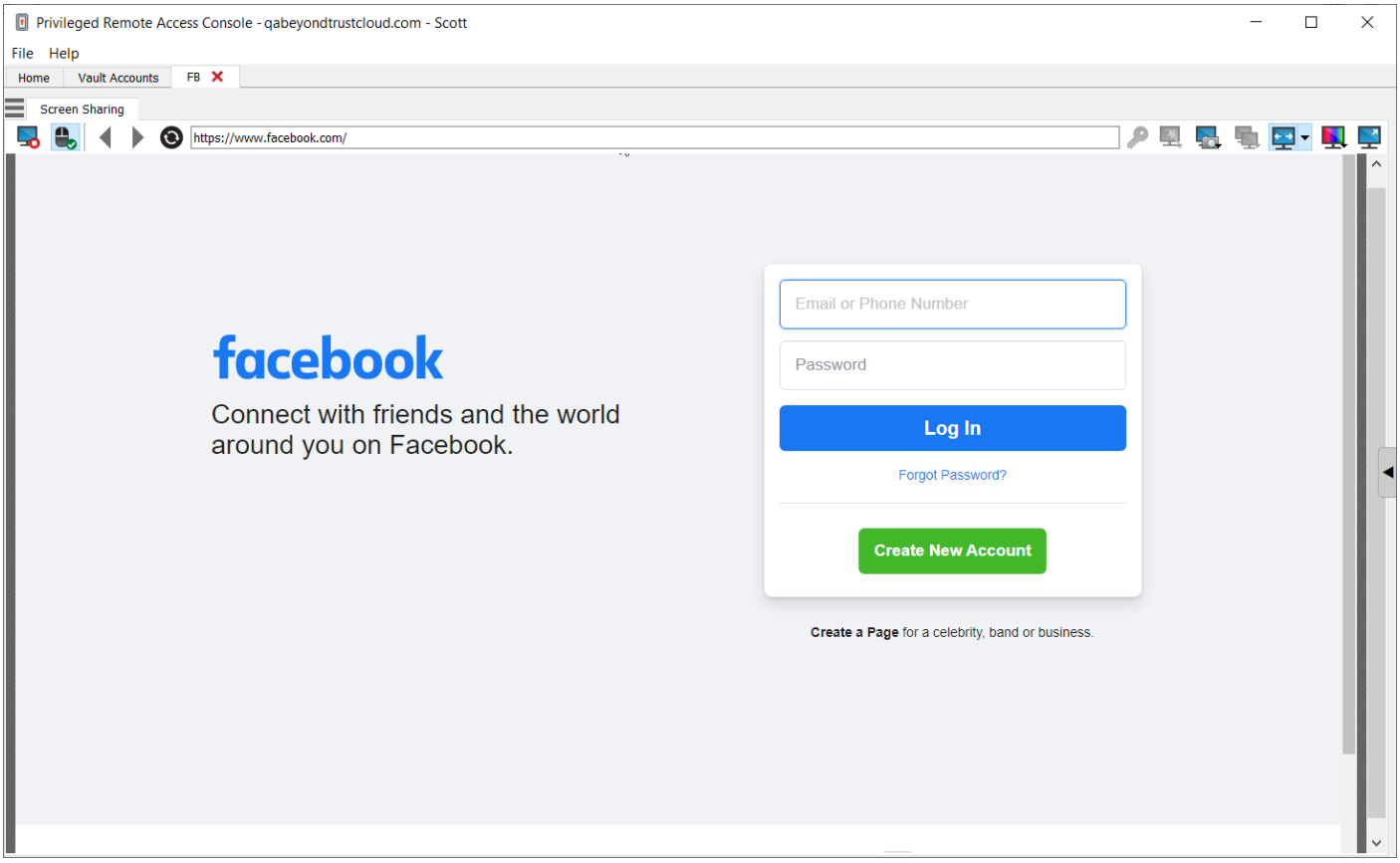
Pour régler le moment pendant lequel les utilisateurs sont autorisés à accéder à cet élément de Jump, si une notification d'accès doit être envoyée, ou si une autorisation ou un ID de ticket provenant de votre système de ticket externe est requis pour l'utilisation de cet élément de Jump, choisissez une **Règle de Jump**. Ces règles doivent être configurées par l'administrateur dans l'interface /login.

Choisissez une **règle de session** à attribuer à cet élément de Jump. La règle de session attribuée à cet élément de Jump a la priorité la plus élevée lors de la configuration des autorisations de session. Le fait de pouvoir définir ou non une règle de session dépend là encore des autorisations définies pour votre compte.

Utiliser un raccourci de Jump Web

Pour utiliser un raccourci de Jump pour démarrer une session, sélectionnez simplement le raccourci dans l'interface de Jump et cliquez sur le bouton **Jump**.

Une fois la connexion établie avec le site Web, cliquez sur le bouton de partage d'écran. L'interface de connexion du site Web apparaît. Si vous cliquez sur un lien pour télécharger un fichier depuis un site Web, une invite sur la fenêtre de messagerie vous demande d'accepter ou de refuser le téléchargement. Si vous acceptez, une fenêtre s'ouvre, et vous avez la possibilité de choisir un emplacement de téléchargement. Il en va de même pour le transfert de fichiers vers le site Web : une fenêtre s'ouvre et vous permet de choisir le fichier à transférer.



Remarque : *si le site requiert un nouvel onglet, un nouvel onglet s'ouvre. Vous ne pouvez pas ouvrir arbitrairement de nouveaux onglets.*

Astuce: *vous pouvez copier et coller du texte vers et depuis le site Web en utilisant les commandes copier/coller de votre système d'exploitation.*

Utiliser l'injection d'informations d'authentification

IMPORTANT !

L'injection d'informations d'authentification n'est pas prise en charge pour les sites non sécurisés (non HTTPS).

Lors de l'intégration de PRA BeyondTrust avec un système de banque de mots de passe, vous pouvez accéder à vos comptes de site Web sans voir l'écran de connexion et sans saisir d'informations d'authentification en utilisant l'injection d'informations d'authentification.

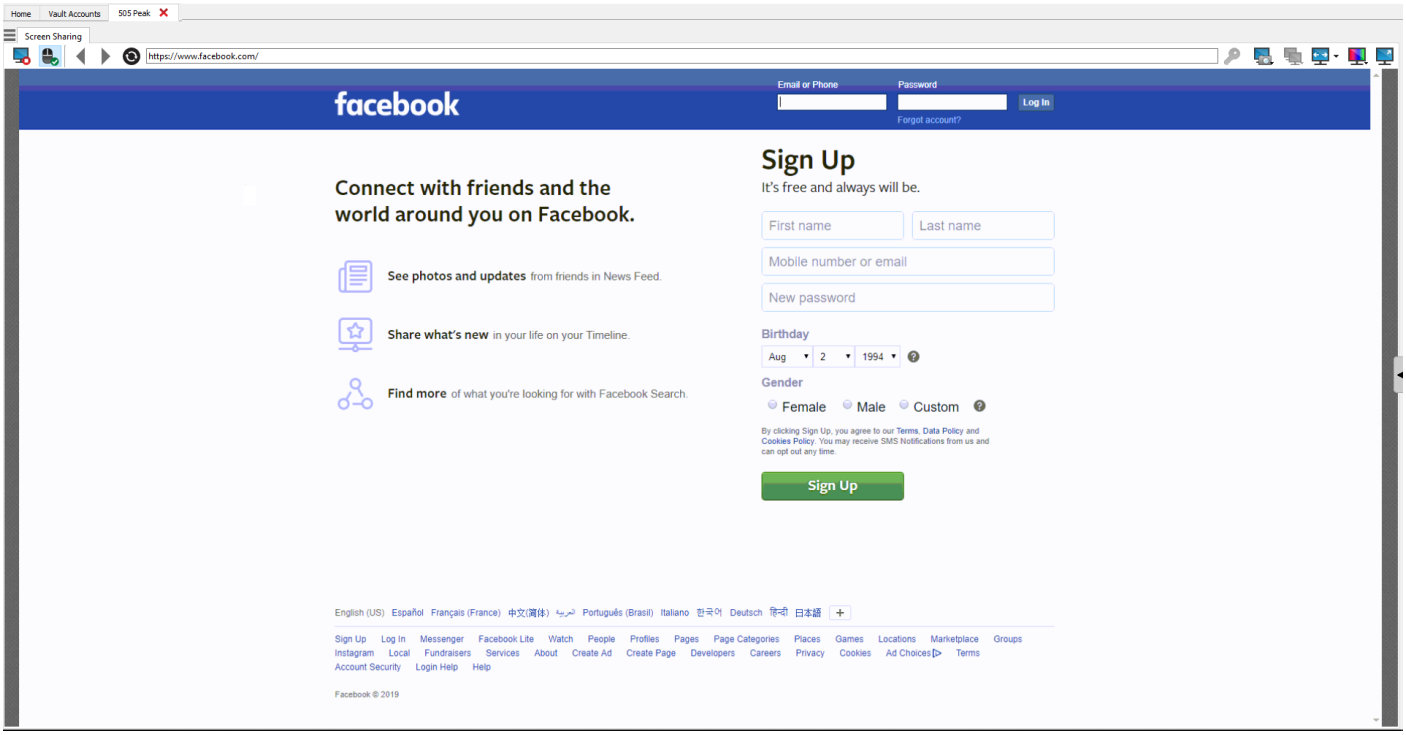
Remarque : *Web Jump prend en charge l'authentification multiétape, lors de laquelle le nom d'utilisateur et le mot de passe ne sont pas demandés sur la même page du navigateur. Jump Web prend également en charge les scénarios dans lesquels un utilisateur se connecte à une portion sans authentification d'un site Web, mais tente ensuite d'entrer dans une zone au moyen d'une authentification basique. En outre, Jump Web prend en charge les sites contenant des CAPTCHA, en permettant aux utilisateurs de saisir le CAPTCHA sans mettre fin au processus d'injection d'informations d'authentification. Une fois l'interaction avec un CAPTCHA réalisée, l'utilisateur clique sur l'icône en forme de clé dans la access console pour finaliser l'injection d'informations d'authentification.*

Remarque : *pour bénéficier de l'injection d'informations d'authentification sans interruption sur une console VMware, il est nécessaire de configurer certains paramètres.*

1. *Accédez à l'ordinateur hébergeant le Jumpoint.*
2. *Téléchargez et installez le plug-in d'intégration client dans l'URL VMware indiquée ci-dessus.*
3. *Avec les autorisations d'administrateur, ouvrez les services Windows (**services.msc**) sur l'hôte du Jumpoint.*
4. *Faites un clic droit sur le Jumpoint BeyondTrust et sélectionnez **Propriétés**.*
5. *Sur l'onglet **Connexion** sous le **Compte du système local**, cochez **Autoriser le service à interagir avec le bureau**.*
6. *Cliquez sur **OK**.*
7. *Sur le système local de l'utilisateur (où la access console est installée), démarrez un Jump Web à l'aide de l'URL VMware indiquée plus haut.*
8. *Sélectionnez **Utiliser les informations d'authentification Windows**.*
9. *Avec cette option, une invite sur le système hôte du Jumpoint autorise les services à interagir avec un programme externe. Accordez une autorisation au service.*
10. *Une invite d'injection d'informations d'authentification VMware apparaît. Décochez la case en regard du texte qui vous demande si vous souhaitez que l'invite soit affichée lorsque le programme est appelé. Cliquez sur **Accepter**.*
11. *Vous pouvez à présent effectuer des Jump Web vers la console VMware à l'aide d'informations d'authentification Windows sans une invite.*

Outils d'accès

Vue d'ensemble de session d'accès et outils



Outils de session

	Cliquez sur l'icône de menu en haut à gauche de la fenêtre de session pour accéder aux contrôles de session pour votre session. Vous pouvez aussi faire un clic droit sur l'onglet de session pour accéder aux contrôles de session. Depuis le menu, sélectionnez **Détacher l'onglet Session** pour séparer la session de la console, ou cliquez sur l'onglet de session et faites-le glisser en dehors de la fenêtre principale. L'icône de menu reste avec votre session même lorsque vous détachez l'onglet de session, ce qui vous permet de positionner l'onglet de session où vous voulez, y compris sur un écran différent, tout en conservant l'accès aux outils de session. Rattacher la session en utilisant l'option **Attacher l'onglet Session** dans le menu, ou en cliquant sur le X pour fermer la fenêtre détachée. De plus, depuis le menu, sélectionnez **Localiser la barre latérale** pour trouver la barre latérale de cette session, ce qui peut être utile si vous avez plusieurs barres latérales de session détachées (voir ci-dessous) éparpillées sur votre écran. Vous pouvez également renommer la session ou rétablir son nom par défaut à partir du menu.
 	Réduisez la barre latérale pour agrandir vote espace de travail de session. Pour épingler à nouveau la barre latérale, survolez la flèche de la barre latérale réduite et cliquez sur l'icône **Épingler la barre latérale**.

 	Cliquez sur cette icône pour détacher la barre latérale. Une fois détachée, la barre latérale peut être placée n'importe où sur votre bureau ou sur un écran différent. La barre latérale peut aussi être redimensionnée selon vos besoins. Vous pouvez aussi redimensionner les volets de la barre latérale pour avoir plus d'espace. Cliquez sur l'icône **Attacher la barre latérale** pour rattacher la batte latérale. Lorsque la barre latérale est détachée, l'icône **Accueil** est activée (voir ci-dessous).
	Cette icône **Accueil** est activée lorsque la barre latérale est détachée. Si vous avez plusieurs sessions ouvertes en même temps et plusieurs barres latérales détachées sur votre écran, cliquer sur l'icône **Accueil** d'une barre latérale vous montera la session associée, ce qui vous fera économiser du temps et vous permettra d'identifier quelle barre latérale va avec quelle session.
	il est possible de repositionner les différentes sections de widget affichées sur la barre latérale, comme la fenêtre de messagerie instantanée, le volet d'informations de session, etc. Lorsque vous survolez la barre de titre d'une section, le pointeur devient une main fermée, ce qui vous permet de faire glisser et de repositionner cette section sur la barre latérale.
	Invitez un autre utilisateur à participer à une session partagée. Vous restez propriétaire de la session, mais vous pouvez recevoir l'avis d'un ou de plusieurs membres de votre équipe ou d'un utilisateur externe.
	Le propriétaire de la session peut supprimer un autre utilisateur d'une session partagée.
	Ouvrez un navigateur Internet sur votre ordinateur sur n'importe quel site défini par votre administrateur. Ce bouton peut être configuré pour inclure des informations détaillées sur la session, le point de terminaison et/ou l'utilisateur BeyondTrust ayant cliqué sur le lien personnalisé. Si, par exemple, la clé externe correspond à l'identificateur unique d'un dossier dans votre système GRC, le fait de cliquer sur ce bouton pourrait afficher le dossier associé dans le système externe.
	Fermez complètement l'onglet de session. Vous pouvez fermer la session depuis la barre latérale, le menu de session ou l'onglet de session.

Les informations sur le système distant se trouvent en bas à droite de la fenêtre de session. Si votre administrateur a activé l'API XML, vous pouvez également désigner une clé externe à utiliser dans les rapports de session. Les attributs de session personnalisés activés par l'administrateur s'affichent dans l'onglet **Informations personnalisées**. Cliquez sur **Copier** pour copier toutes ces informations dans votre presse-papiers.

L'administrateur peut également choisir d'activer une fonction permettant de déconnecter automatiquement l'utilisateur Windows ou de verrouiller l'ordinateur distant à l'issue des sessions. Lorsque vous avez travaillé sur un système en mode autonome, il est recommandé de verrouiller l'ordinateur pour empêcher que des utilisateurs non autorisés ne puissent consulter des informations confidentielles. Définissez l'action appropriée via la liste déroulante située en bas du volet.

Connexion aux systèmes distants en utilisant l'injection d'informations d'authentification depuis la Access Console

Lorsque vous accédez à un élément de Jump basé sur Windows à travers la access console, 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'administrateur.

Avant d'utiliser l'injection d'informations d'authentification, vérifiez que vous disposez d'un magasin d'informations d'authentification ou d'une banque de mots de passe disponible pour vous connecter au Privileged Remote Access BeyondTrust.

> ***Remarque :*** *l'injection d'informations d'authentification n'est pas disponible pour les Jump Clients sur Linux ou Mac.*

Installer et configurer 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 (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 système pour activer le service ECM BeyondTrust et pour utiliser l'injection d'informations d'authentification dans Privileged Remote Access BeyondTrust.*

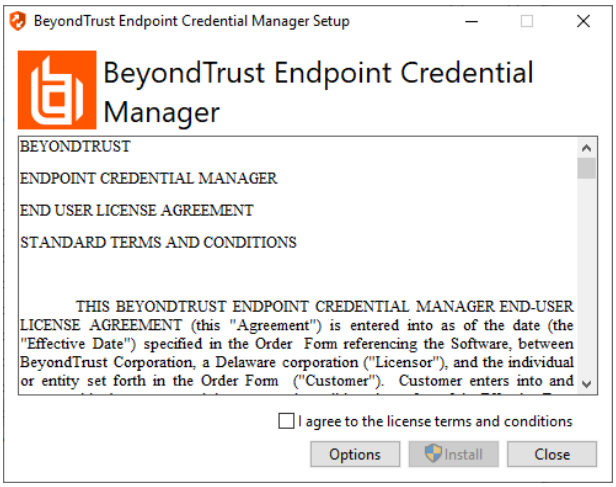
Configuration requise

- **Windows Vista® ou supérieur, 64 bits seulement**
- **.NET 4.5 ou supérieur**

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.

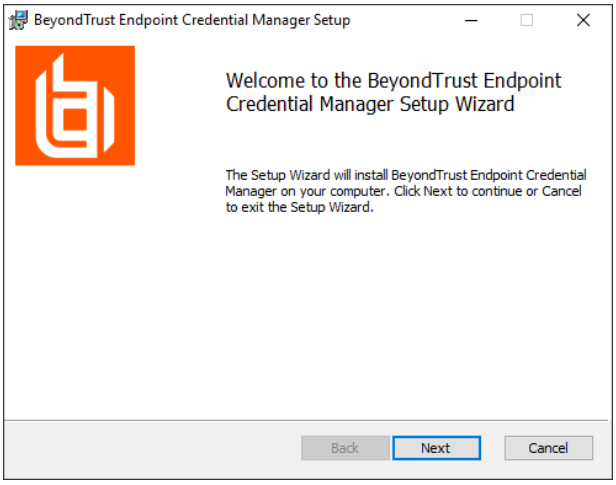
2. Lancez l'assistant de configuration du gestionnaire d'informations d'authentification de point de terminaison BeyondTrust.
3. Acceptez les conditions générales du CLUF. Cochez la case si vous acceptez, puis cliquez sur **Installer**.

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

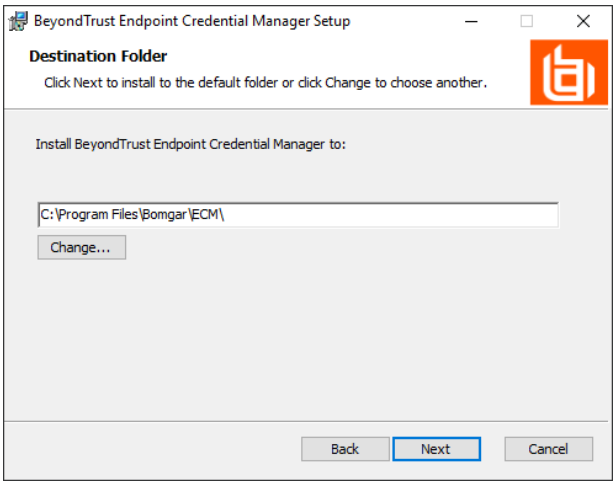


> ***Remarque :*** *vous ne pourrez pas poursuivre l'installation si vous n'acceptez pas le CLUF.*

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

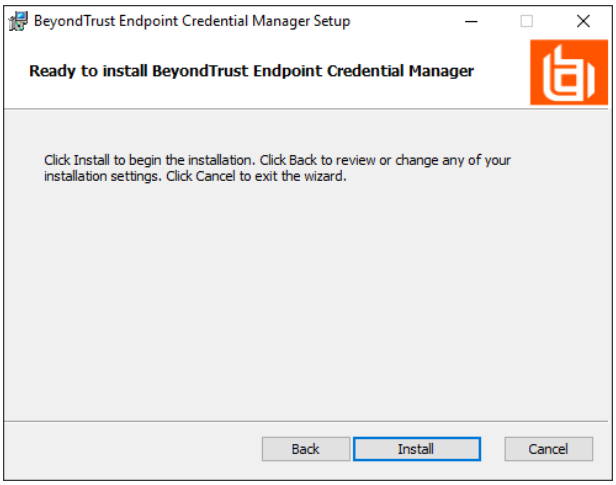


5. Choisissez un emplacement pour le gestionnaire d'informations d'authentification, puis cliquez sur **Suivant**.

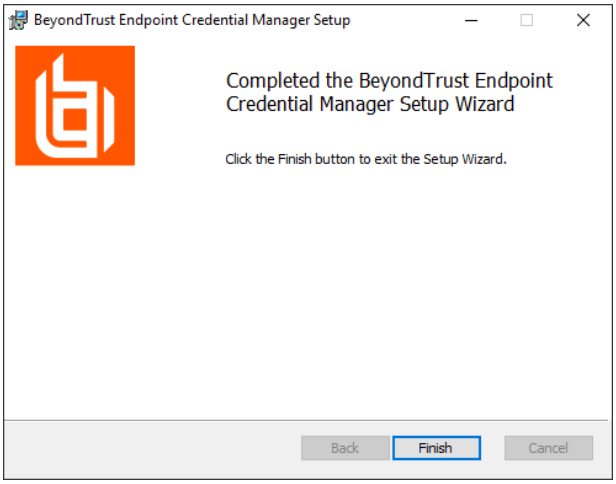


6. Sur l'écran suivant, vous pouvez lancer l'installation ou vérifier les étapes précédentes.

7. Cliquez sur **Installer** lorsque vous êtes prêt à commencer.



8. L'installation prend quelques instants. Sur cet écran, 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 de l'appliance est disponible sur* ***/login > État > Information > Clients ECM****.*

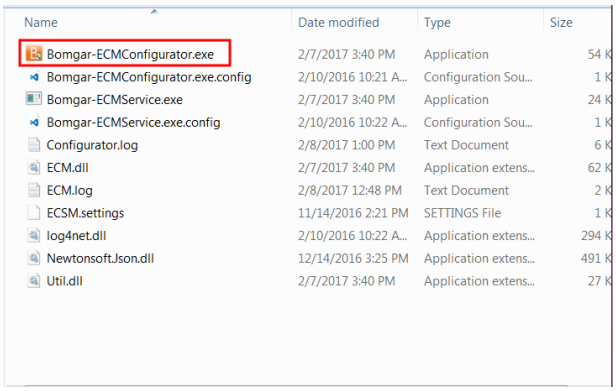
Remarque : *lorsque des ECM sont connectés dans une configuration de haute disponibilité, la BeyondTrust Appliance B Series achemine les demandes vers le groupe d'ECM ayant été le plus longtemps connectée à l'appliance.*

Remarque : *si une erreur de plug-in Windows est indiquée lors de l'installation, localisez et débloquez BeyondTrustVaultRestPlugin.dll.*

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.

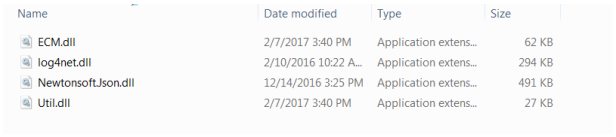


3. Lorsque le configurateur ECM s'ouvre, remplissez les champs. Tous les champs sont obligatoires.

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.*

IMPORTANT !

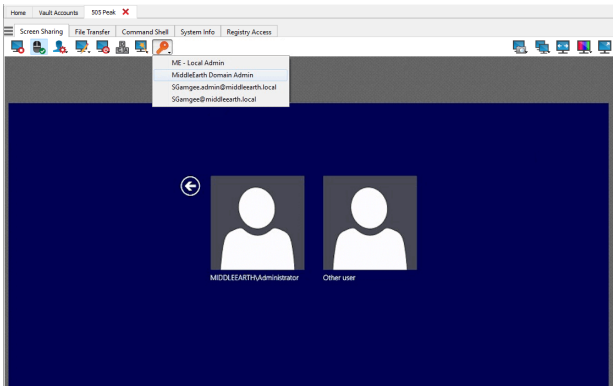
Pour appliquer de nouveaux paramètres à la configuration, redémarrez le service ECM.

Utilisez l'injection d'informations d'authentification pour accéder à des systèmes distants

Une fois que le magasin d'informations d'authentification a été configuré et qu'une connexion a été établie, la access console peut commencer à utiliser des informations d'authentification dans le magasin d'informations d'authentification pour se connecter à des systèmes distants.

1. Connexion à la access console.
2. Effectuez un Jump vers un système distant avec un élément de Jump installé comme service accru sur une machine Windows.

3. Appuyez sur le bouton **Lecture** pour commencer le partage d'écran avec le système distant. Si le système distant est sur l'écran de connexion de Windows, le bouton **Injecter des informations d'authentification** est en surbrillance.
4. Cliquez sur le bouton **Injecter des informations d'authentification**. Un dialogue de sélection d'informations d'authentification apparaît, répertoriant les informations d'authentification disponibles pour ECM.
5. Sélectionnez les bonnes informations d'authentification à utiliser depuis l'ECM. Le système récupère les informations d'authentification depuis l'ECM et les injecte sur l'écran de connexion de Windows.
6. Le technicien d'assistance est connecté au système distant.



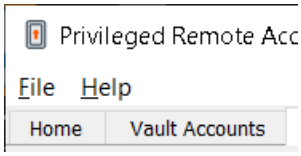
Faites votre choix parmi les informations d'authentification préférées pour injection

Après avoir utilisé un ensemble d'informations d'authentification pour vous connecter à un point de terminaison, le système stocke vos informations d'authentification préférées pour le point de terminaison ainsi que le contexte dans lequel elles ont été utilisées (pour vous connecter, pour procéder à une action spéciale, ou pour accroître ou appliquer des droits) dans la base de données de la B Series Appliance. La prochaine fois que vous utiliserez des informations d'authentification pour accéder au même point de terminaison, le menu d'injection d'informations d'authentification vous recommandera quelles informations utiliser. Les informations d'authentification sont affichées en haut de la liste d'informations d'authentification, sous **Comptes recommandés**, suivies par toutes autres informations restantes. Si aucun historique d'informations d'authentification n'existe pour un point de terminaison, la B Series Appliance affiche une liste de toutes les informations d'authentification possibles, groupées par comptes associés et non associés à l'élément de Jump. Les associations d'éléments de Jump pour les comptes et les groupes de comptes sont configurées dans /login.

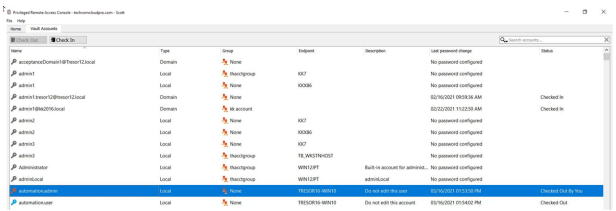
Il est recommandé de n'avoir qu'un maximum de 5 informations d'authentification dans la liste.

Extraire et injecter des informations d'authentification Vault

Vous pouvez facilement accéder à Privileged Remote Access Vault directement depuis la access console. Cela vous permet d'extraire ou d'injecter des informations d'authentification lorsque c'est nécessaire, durant une session ou sur votre machine locale.

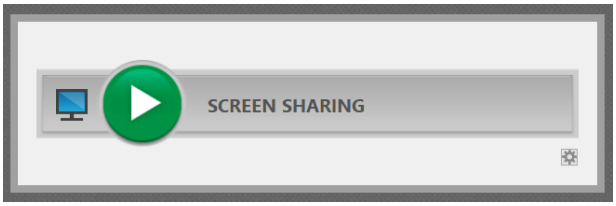


Sélectionner l'onglet **Comptes Vault** pour afficher une liste des informations d'authentification disponibles et des informations associées.



Contrôle du point de terminaison distant grâce au partage d'écran

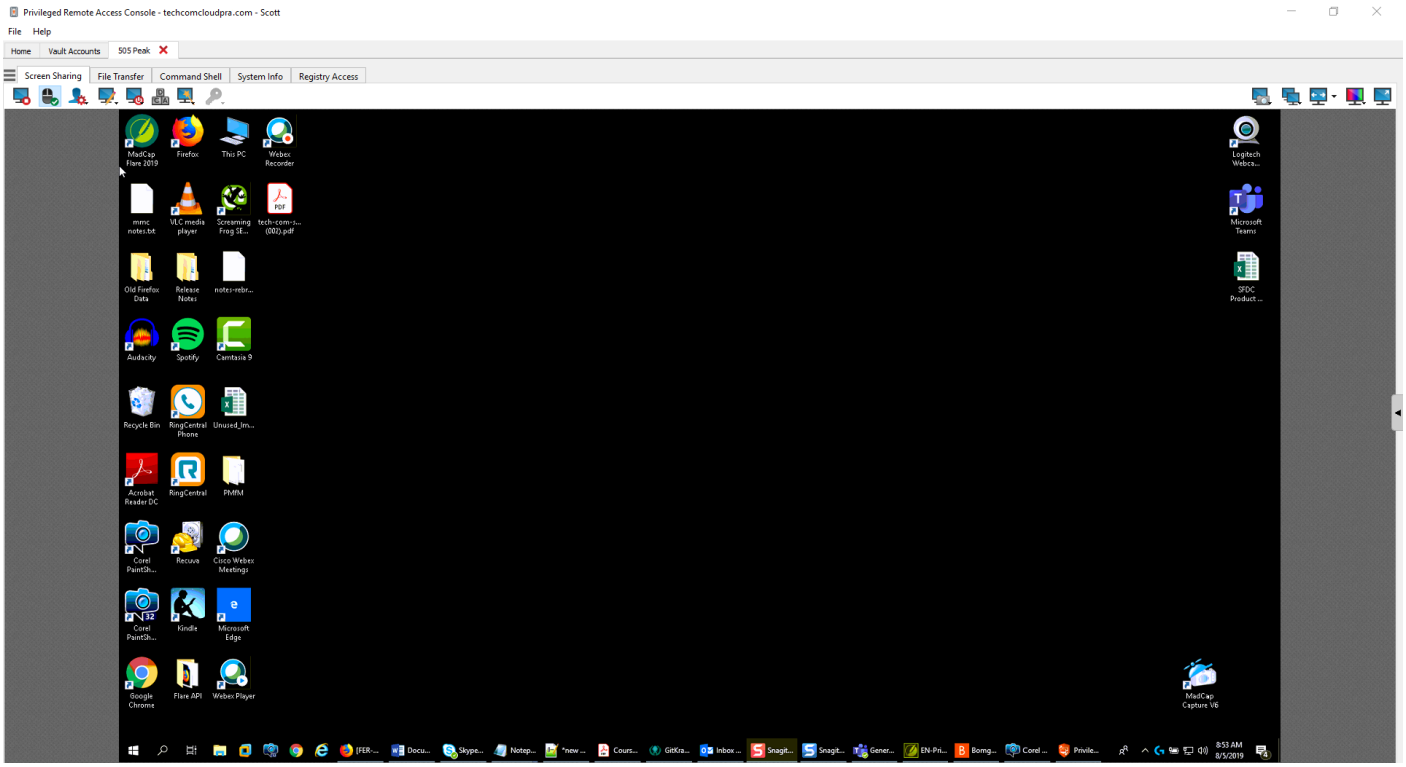
Dans la fenêtre de la session, cliquez sur le bouton **Partage d'écran** pour demander à prendre le contrôle de l'ordinateur distant si le partage d'écran ne démarre pas automatiquement. Selon vos paramètres de compte, vous pouvez voir plusieurs options disponibles sous le bouton. Cliquez sur l'icône en forme d'engrenage pour afficher toutes les options.



Une fois la session lancée, la console d'accès démarre immédiatement le partage d'écran avec le point de terminaison. En fonction du système, vous aurez le contrôle total ou uniquement des privilèges d'affichage lors du partage d'écran avec le système.

Options de partage d'écran

- Le fait de laisser toutes les options désélectionnées entraîne une demande de partage d'écran complet, qui offre un accès visuel et de contrôle à l'intégralité du bureau et des applications du système distant.
- Notez que si vous cochez la case **Voir uniquement**, vous pourrez voir l'écran distant mais vous n'en aurez pas le contrôle.
- **L'option Écran de confidentialité** lance la session avec l'affichage et le contrôle du point de terminaison désactivés. L'écran de confidentialité n'est pas disponible lors d'une assistance technique sur Windows 8.



Outils de partage d'écran

	Arrêter le partage d'écran.
	Pendant que vous regardez l'ordinateur distant, lancez ou interrompez le contrôle distant de la souris et du clavier.
	Si vos autorisations vous le permettent, vous pouvez désactiver l'affichage, ainsi que l'entrée souris et le clavier de l'utilisateur distant. L'affichage de l'écran de confidentialité de l'utilisateur final explique clairement que l'utilisateur BeyondTrust a désactivé l'affichage du client final. L'utilisateur final peut reprendre le contrôle à tout moment en appuyant sur **Ctrl+Alt+Suppr**. Vous pouvez également désactiver le clavier et la souris de l'utilisateur final tout en lui permettant de voir l'écran. Lorsque l'entrée est restreinte, une bordure orange apparaît autour des écrans de l'utilisateur final, et un message indique que l'utilisateur BeyondTrust possède le contrôle de la souris et du clavier. L'utilisateur final peut reprendre le contrôle à tout moment en appuyant sur **Ctrl+Alt+Suppr**. 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.
	Les outils d'annotation permettent une collaboration plus aisée lors de sessions partagées. Plusieurs outils sont disponibles, notamment les formes et le dessin libre.
	Redémarrez le système distant en mode normal ou sans échec avec prise en charge réseau, ou éteignez-le.
	Envoyez une commande **Ctrl-Alt-Suppr** à l'ordinateur distant.
	Pour exécuter une action spéciale sur le système distant. Les tâches disponibles varient en fonction de la configuration et du système d'exploitation distants. Les scripts prédéfinis disponibles pour l'utilisateur apparaissent dans un menu volant. Avec la fonction « Exécuter en tant que spécial » sur un système Windows®, vous pouvez choisir les informations d'authentification dans un gestionnaire d'informations d'authentification de point de terminaison. L'utilisation du gestionnaire d'informations d'authentification de point de terminaison nécessite un accord de services séparé avec BeyondTrust. Une fois qu'un accord de services est en place, vous pouvez télécharger le middleware requis auprès du portail d'assistance technique BeyondTrust.
	Vous avez accès à une liste répertoriant les lecteurs de cartes à puce disponibles sur votre système local. Utilisez une carte à puce virtuelle pour réaliser des actions administratives, exécuter des programmes dans un autre contexte utilisateur ou encore vous connecter avec d'autres informations d'authentification utilisateur. Les pilotes de carte à puce virtuelle appropriés doivent néanmoins être installés à la fois sur le système local et sur le système distant, avec les services en cours d'exécution.
	Pour relancer le partage d'écran des appareils iOS. Pour plus de détails, veuillez consulter Assistance technique sur appareils iOS Apple à l'adresse www.beyondtrust.com/docs/privileged-remote-access/getting-started/access-console/apple-ios/index.htm. Lors de l'assistance technique d'un système Apple OS X 10.10+ attaché à un appareil mobile Apple iOS 8.0.1+, cliquez sur ce bouton pour lancer ou terminer un partage d'écran en mode accès visuel uniquement sur l'appareil iOS connecté. Notez que ce bouton n'est visible que si vous êtes dans une access session de partage d'écran standard avec un système Apple OS X Yosemite, et que le bouton n'est activé que si un appareil Apple iOS 8.0.1+ est connecté au système OS X Yosemite en cours d'assistance technique.

	Se connecter au point de terminaison à l'aide d'informations d'authentification fournies par un magasin d'informations d'authentification externe. L'utilisation du gestionnaire d'informations d'authentification de point de terminaison nécessite un accord de services séparé avec BeyondTrust. Une fois qu'un accord de services est en place, vous pouvez télécharger le middleware requis auprès du portail d'assistance technique BeyondTrust. avant la version 15.2, cette fonction n'est disponible que dans les sessions lancées depuis un Jump Client aux droits accrus sur Windows®. À partir de la version 15.2, vous pouvez également utiliser un gestionnaire d'informations d'authentification de point de terminaison dans les sessions de Jump distants, les sessions de protocole de bureau à distance Microsoft®, les sessions VNC et les sessions de Shell Jump.
	Lors du partage d'écran, effectuez une capture d'écran du ou des écrans distants en résolution maximum, enregistrée au format PNG. Sauvegardez le fichier image sur votre système local ou votre presse-papiers. L'action de capture d'écran est enregistrée dans le journal de discussion avec un lien vers une image enregistrée localement. Le lien reste actif même après que le client a quitté la session, mais il n'est pas conservé dans le rapport de session BeyondTrust. Vous pouvez modifier le répertoire où les captures d'écran sont enregistrées en allant dans le menu **Fichier > Paramètres > Outils** de la access console. Cette fonction est disponible sur Mac, Windows et Linux.
	Envoyez manuellement le contenu de votre presse-papiers vers l'ordinateur distant. Cet outil n'est pas visible si vous êtes autorisé à envoyer automatiquement le contenu de votre presse-papiers ou si, au contraire, vous n'êtes pas autorisé à envoyer des informations de presse-papiers au système distant.
	Recevez manuellement le contenu de votre presse-papiers depuis l'ordinateur distant. Cet outil n'est pas visible si vous êtes autorisé à recevoir automatiquement le contenu de votre presse-papiers ou si, au contraire, vous n'êtes pas autorisé à recevoir des informations de presse-papiers du système distant.
	Sélectionnez un autre écran distant à afficher. Notez que le moniteur principal est désigné par la lettre **P**.
	Visualisez l'écran distant à sa taille réelle ou mis à l'échelle.
	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.
	Affichez le bureau distant en mode plein écran ou revenez à l'affichage de l'interface. En mode Plein écran, les touches spéciales sont transmises au système distant, notamment les touches de modification, les touches de fonction et la touche de démarrage Windows. Notez que ceci ne s'applique pas à la commande **Ctrl-Alt-Suppr**.

Utiliser les annotations pour dessiner sur l'écran distant du point de terminaison

Utilisez l'outil d'annotation pour collaborer avec d'autres utilisateurs pendant les sessions partagées. Les annotations permettent de communiquer visuellement de façon interactive, ce qui réduit les situations potentiellement frustrantes et accélère les processus.

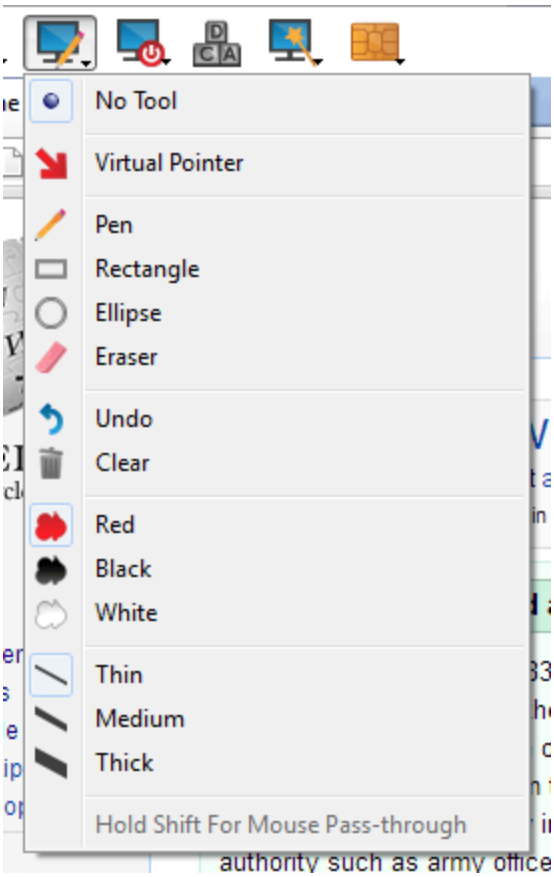
En mode annotation, vous pouvez toujours utiliser votre souris pour déplacer ou contrôler des éléments sur le bureau distant. Maintenez la touche **Maj** enfoncée pour interrompre le mode annotation.

Activation des annotations

Pour commencer à utiliser les **Annotations**, cliquez sur l'icône correspondante.

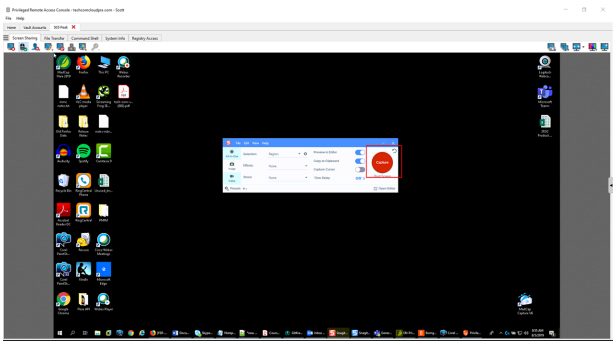
Cliquez sur les objets du menu déroulant pour activer le mode **Annotations**. Les fonctions et outils suivants sont disponibles :

- Pointeur virtuel
- Stylo
- Outil Rectangle
- Outil Ellipse
- Effaceur
- Annuler
- Effacer
- Couleur rouge, noire ou blanche
- Trait fin, moyen ou épais



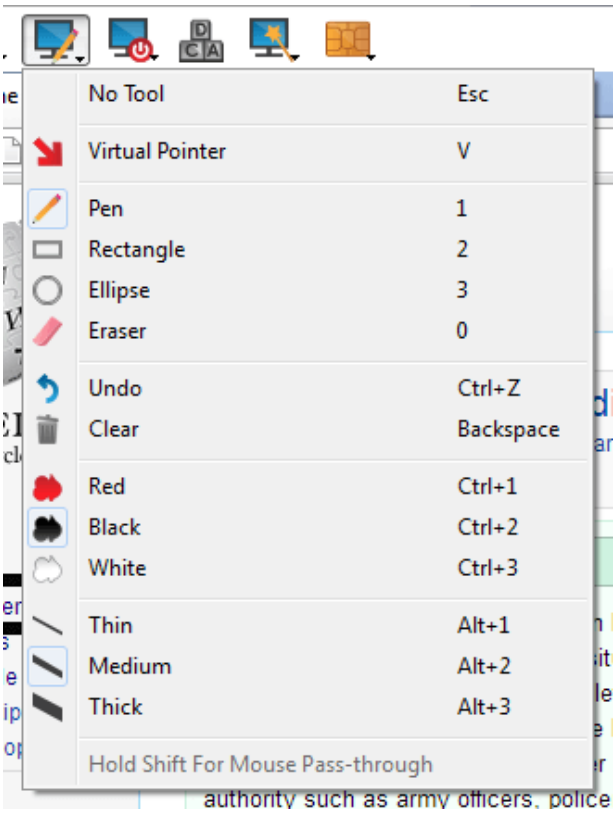
Vous pouvez sélectionner votre outil dans le menu déroulant des **Annotations**, ou en effectuant un clic droit dans la zone de l'écran distant. Si vous cliquez sur les zones en dehors de l'écran distant, le menu déroulant ne s'affichera pas.

Les annotations apparaissent sur l'écran distant pour attirer l'attention sur des points spécifiques ou mettre en évidence des zones.



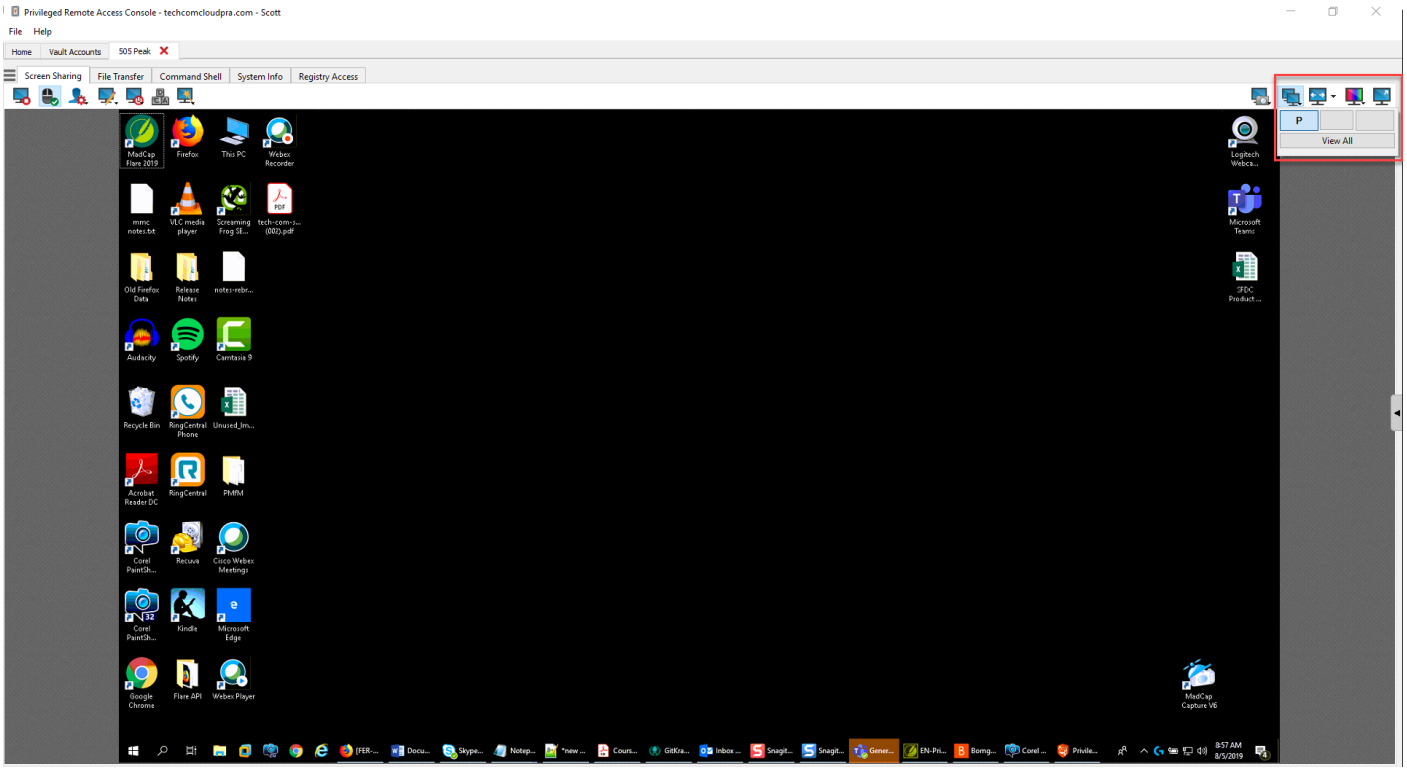
Pour désactiver les **Annotations**, sélectionnez **Aucun outil** dans le menu déroulant, ou cliquez sur **Echap**.

Toutes les annotations sur l'écran de l'utilisateur sont supprimées lorsque la session se termine.



Regarder plusieurs moniteurs sur le point de terminaison distant

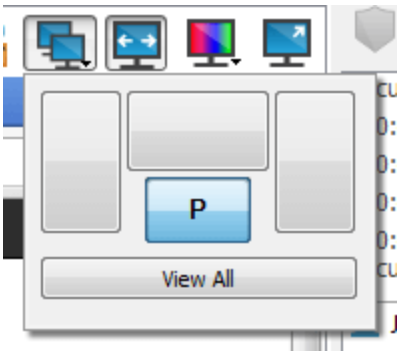
BeyondTrust prend en charge les bureaux distants configurés pour utiliser plusieurs moniteurs. Lorsque vous vous connectez pour la première fois à un bureau distant, vous voyez le moniteur principal dans l'onglet **Partage d'écran**. Si des moniteurs supplémentaires sont configurés, une icône **Affichage** sera active dans la barre d'outils **Partage d'écran**, et un onglet **Écrans** apparaîtra dans l'angle inférieur droit de la console.



Utilisation de l'icône Affichage

Sélectionnez l'icône **Affichage** pour voir tous les écrans attachés à l'ordinateur distant. Dans cette vue, les moniteurs distants sont représentés par des rectangles plutôt que par des miniatures. La position de chaque rectangle correspond à la position configurée pour chaque moniteur sur le bureau distant.

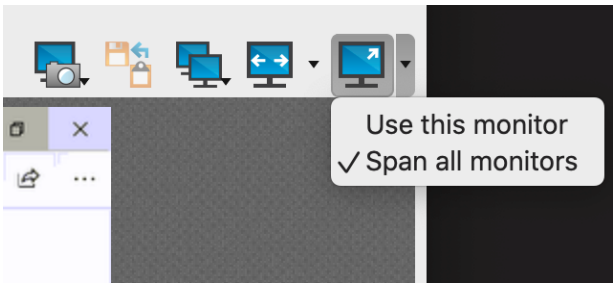
Le moniteur principal apparaît par défaut dans la fenêtre **Partage d'écran**. Pour changer d'affichage, cliquez sur le rectangle du moniteur que vous souhaitez afficher. Vous pouvez également sélectionner **Voir tous** pour afficher tous les écrans attachés à l'ordinateur distant dans la fenêtre **Partage d'écran**.



Si aucun ordinateur supplémentaire n'est attaché à l'ordinateur distant, l'icône **Affichage** sera inactive.

Assistance technique multimoniteur lors d'une session RDP

Une option vous permet d'ouvrir une connexion PRA étendue à tous les moniteurs de l'ordinateur client, quelle que soit la configuration des moniteurs client. Avec cette fonctionnalité, vous pouvez utiliser pleinement tous les moniteurs connectés à l'ordinateur client, ce qui vous permet d'ajuster le dimensionnement et la mise à l'échelle de l'écran pendant une session RDP sur plusieurs moniteurs.

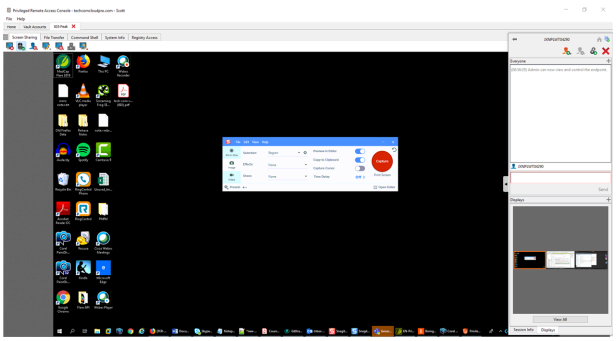


> ***Remarque :*** *si vous utilisez la vue plein écran tout en utilisant cette fonction, le système distant s'affiche sur tous vos moniteurs.*

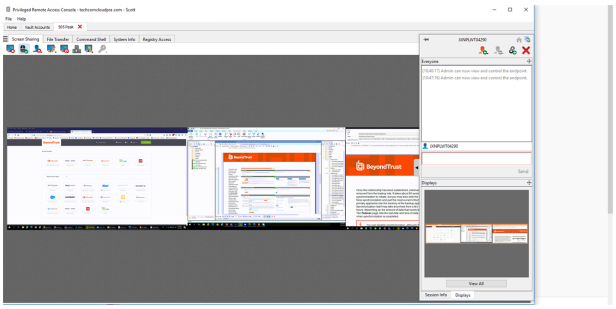
Utilisation de l'onglet Écrans

Sélectionnez l'onglet **Écrans** pour voir les miniatures de tous les écrans attachés à l'ordinateur distant. La position de chaque miniature correspond à la position configurée pour chaque écran sur le bureau distant.

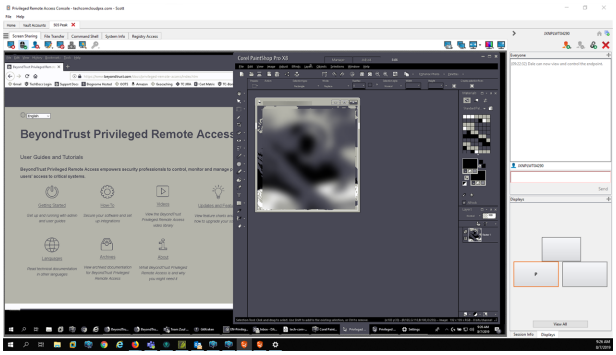
Le moniteur actuellement affiché dans l'onglet **Partage d'écran** sera mis en surbrillance.



Le moniteur principal apparaît par défaut dans la fenêtre **Partage d'écran**. Pour changer l'affichage, cliquez sur la miniature du moniteur que vous souhaitez voir. Vous pouvez également sélectionner **Voir tous** pour afficher tous les écrans attachés à l'ordinateur distant dans la fenêtre **Partage d'écran**.



Si la session est en mode niveaux de gris, les moniteurs distants sont représentés par des rectangles plutôt que par des miniatures. La position de chaque rectangle correspond à la position configurée pour chaque moniteur sur le bureau distant.



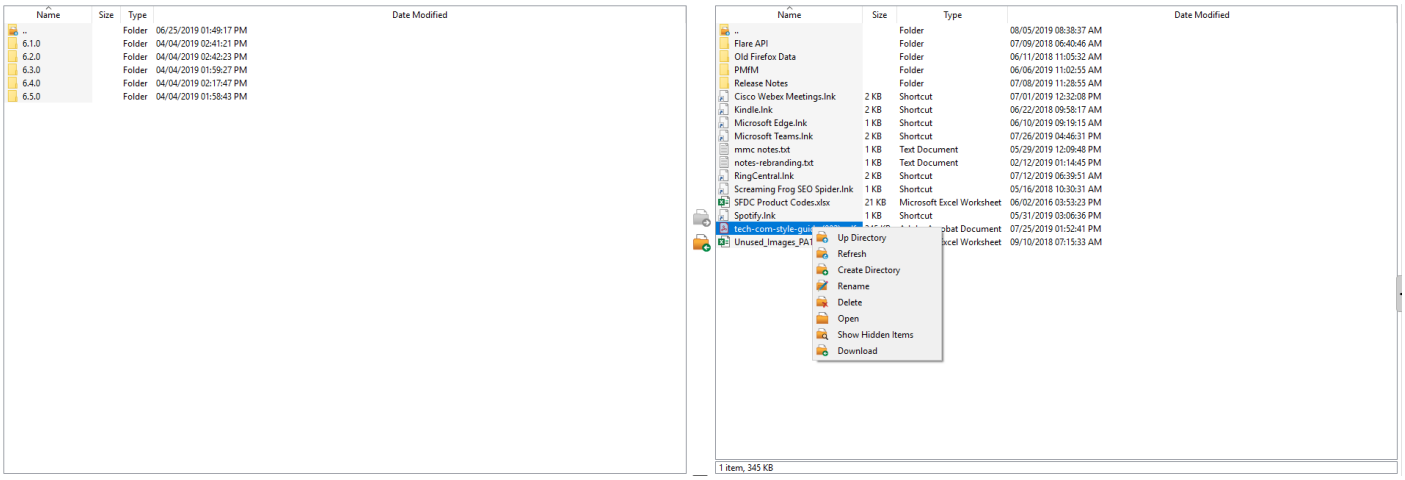
> ***Remarque :*** *le cycle d'actualisation de la miniature est d'environ trois secondes dans des conditions idéales, mais peut générer un décalage en fonction de la vitesse de connexion et du transfert de données.*

Transfert de fichiers vers et depuis le point de terminaison distant

Au cours d'une session, les utilisateurs privilégiés peuvent transférer, supprimer ou renommer des fichiers, et même de répertoires entiers, depuis et vers l'ordinateur distant, depuis l'appareil distant, et depuis et vers la carte SD de l'appareil. Il n'est pas nécessaire d'avoir le contrôle total de l'ordinateur distant pour transférer des fichiers.

Selon les autorisations que l'administrateur a définies pour votre compte, vous pouvez être autorisé à charger les fichiers vers le système distant ou à les télécharger vers votre ordinateur local. L'accès au système de fichiers peut également être restreint à certains chemins d'accès sur le système distant ou local, obligeant ainsi le chargement ou le téléchargement dans certains répertoires seulement.

Transférez les fichiers à l'aide des boutons de chargement/téléchargement ou par glisser-déplacer. Un clic droit sur un fichier entraîne l'affichage d'un menu contextuel vous permettant, entre autres, de créer un nouveau répertoire, de renommer, d'ouvrir ou de supprimer le fichier, ou encore de le télécharger directement sur votre machine.



Outils de transfert de fichiers

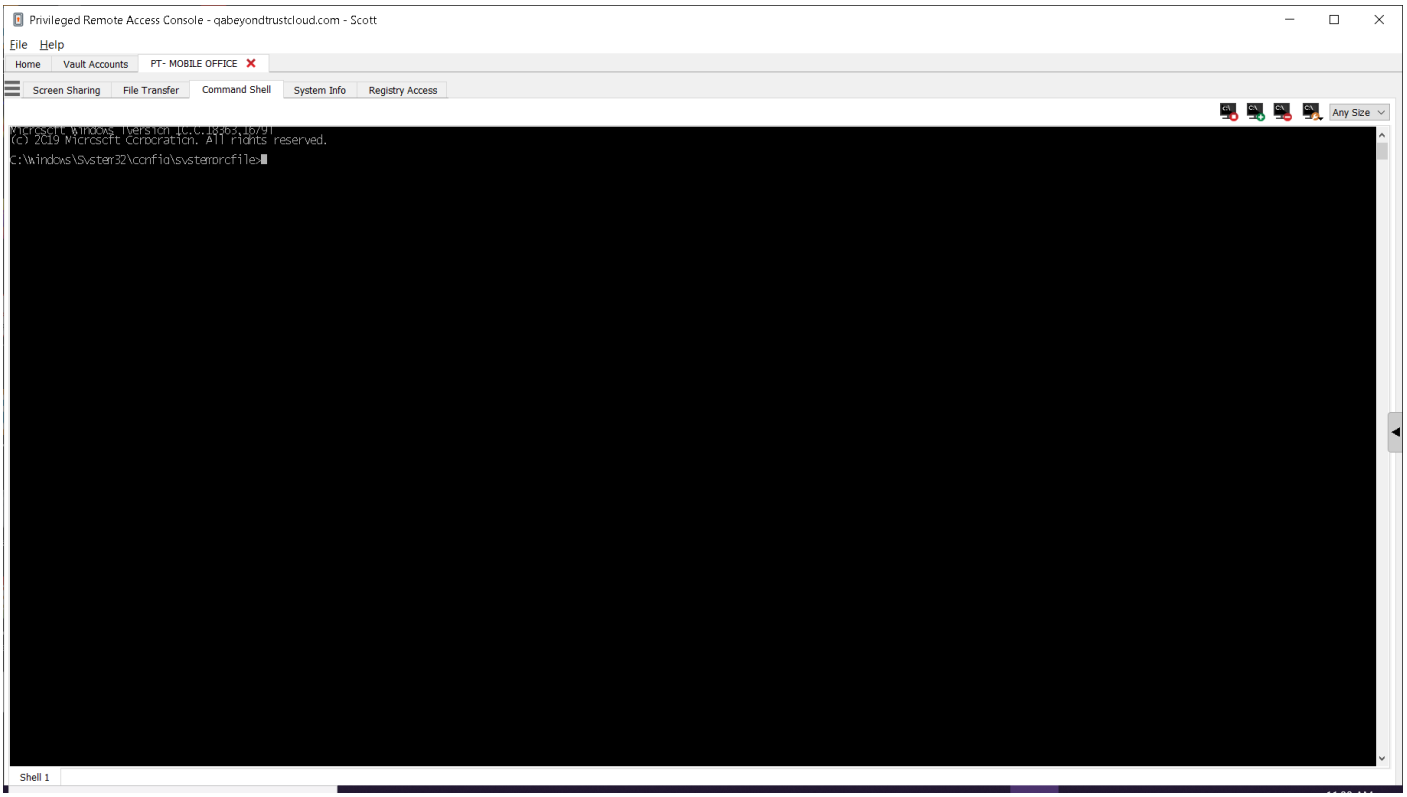
	Mettez fin à l'accès au système de fichiers du périphérique distant lorsque vous n'en avez plus besoin.
	Remontez d'un répertoire dans le système de fichiers sélectionné.
	Actualisez votre vue du système de fichiers sélectionné.
	Créez un nouveau répertoire.
	Renommez un répertoire ou un fichier.
	Supprimez un répertoire ou un fichier. Notez que cette opération entraîne la suppression définitive du fichier ou du dossier, qui n'est pas envoyé vers la corbeille.

	Affichez les fichiers masqués.
 	Sélectionnez un ou plusieurs fichiers ou répertoires, puis cliquez sur le bouton approprié pour charger les fichiers sur le système distant ou les télécharger sur votre système local. Vous pouvez également transférer les fichiers par glisser-déplacer.
	Si un fichier du même nom est déjà présent à l'emplacement où vous essayez de transférer un fichier, vous avez le choix entre remplacer le fichier existant, annuler le transfert ou être interrogé chaque fois que deux fichiers portent le même nom. Notez que si le contenu des fichiers est identique, le téléchargement est ignoré et le système affiche un message d'avertissement.
	Le fait de conserver les informations du fichier conservera l'horodatage initial du fichier. Si cette option est désactivée, l'horodatage du fichier reflète la date et l'heure du transfert.
	Si le transfert automatique de fichiers est activé, les transferts commencent dès que vous cliquez sur le bouton de chargement ou de téléchargement, ou dès qu'un fichier est déplacé d'un système de fichiers à un autre.
	Si le transfert de fichiers automatique n'est pas activé, sélectionnez dans le gestionnaire de transfert les fichiers que vous souhaitez transférer, puis cliquez sur le bouton **Démarrer** pour commencer le transfert.
	Dans le gestionnaire de transfert, sélectionnez un fichier puis cliquez sur le bouton **Détails** pour afficher les informations telles que la date et l'heure du transfert, l'origine et la destination des fichiers ainsi que le nombre d'octets transférés.
	Sélectionnez un ou plusieurs fichiers dans le gestionnaire de transfert, puis cliquez sur **Annuler** pour interrompre le transfert.
	Effacez toutes les informations depuis le gestionnaire des transferts.

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

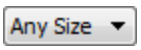
L'interpréteur de commandes distant permet aux utilisateurs privilégiés d'ouvrir une interface de ligne de commande virtuelle sur des ordinateurs distants. Les utilisateurs peuvent ensuite saisir localement pour exécuter les commandes sur le système distant. Vous pouvez travailler depuis plusieurs interpréteurs. Notez que les scripts à la disposition de l'utilisateur peuvent également être exécutés sur l'ordinateur distant à partir de l'interface de partage d'écran.

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.



Outils d'interpréteur de commandes

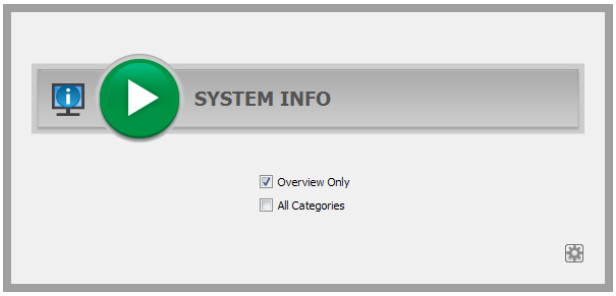
	Mettez fin à l'accès à l'invite de commande une fois que celui-ci n'est plus nécessaire.
 	Ouvrir un nouvel interpréteur pour exécuter plusieurs instances d'une invite de commande ou fermer des interpréteurs individuels sans abandonner l'accès à l'invite de commande. Les interpréteurs de commandes sont tabulés au bas de l'écran.

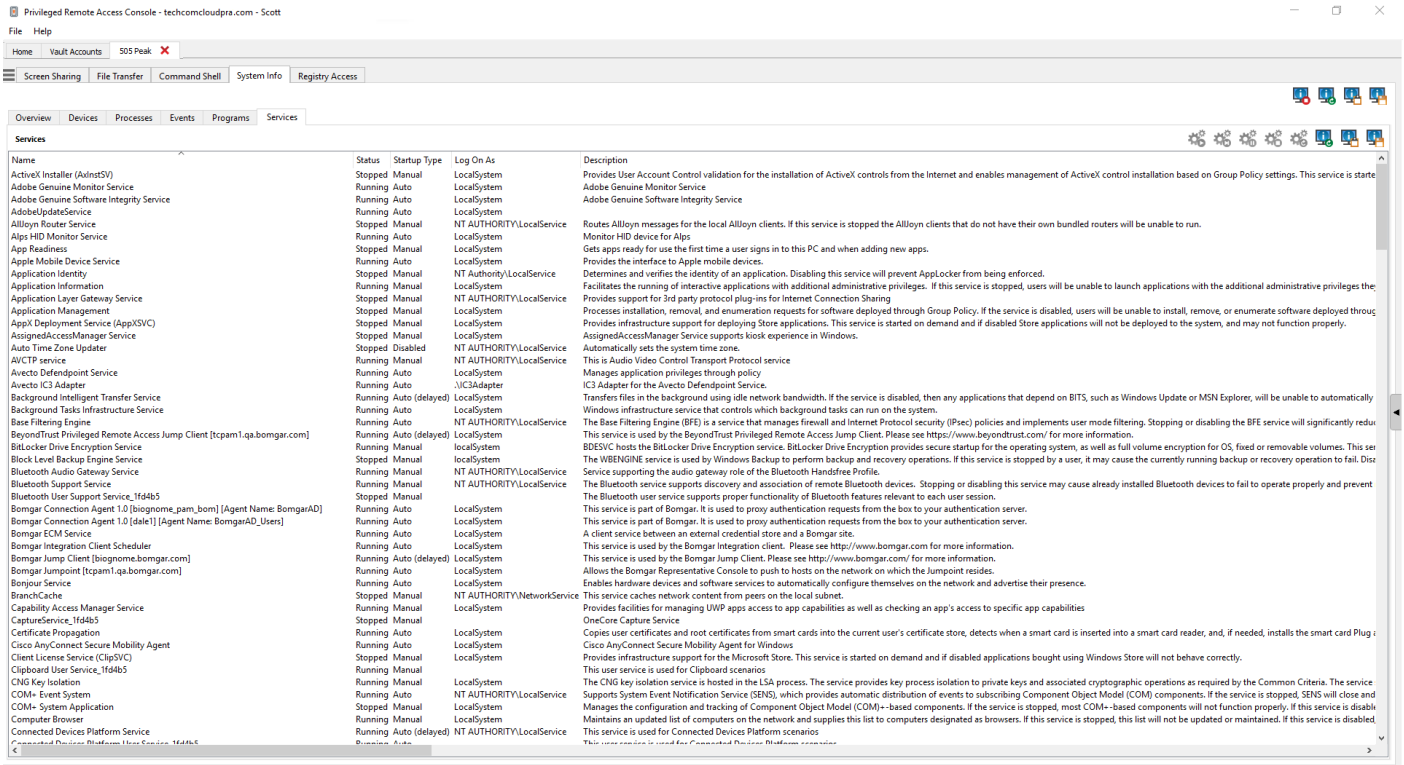
	Si vous y êtes autorisé, accédez au menu déroulant des scripts écrits auparavant. Lorsque vous sélectionnez un script à exécuter, une invite s'affiche avec une brève description du script. Lorsque vous cliquez sur **Oui**, le script s'exécute dans l'interpréteur de commandes actif.
	Accédez à des outils à utiliser dans l'invite de commandes. Collez le contenu de votre presse-papiers en sélectionnant l'option dans le menu, ou en faisant un clic droit dans la fenêtre du terminal. Copiez un fichier journal de l'interpréteur actuel dans votre presse-papiers, ou enregistrez-le sur votre ordinateur. Pour copier une partie du texte, il vous suffit de le sélectionner. Effacer toutes les lignes non affichées, ou effacer tout le contenu du terminal. Vous pouvez accéder aux outils en appuyant sur Ctrl + clic droit dans la fenêtre du terminal.
	Sélectionnez la taille d'affichage de l'écran. Vous avez le choix entre 80x50, 80x25 ou toute taille.

Consulter les informations système sur le point de terminaison distant

Les utilisateurs privilégiés peuvent voir un instantané complet des informations système du périphérique ou de l'ordinateur distant pour réduire le temps nécessaire pour un diagnostic et résoudre le problème. Les informations système disponibles varient en fonction du système d'exploitation distant et de la configuration de l'ordinateur distant. Les utilisateurs dotés des autorisations appropriées peuvent également mettre fin à des processus, démarrer, arrêter, mettre en pause, reprendre et redémarrer des services, et désinstaller des programmes.

L'extraction d'une grande quantité de données pouvant ralentir les transmissions, vous pouvez choisir de démarrer l'affichage uniquement avec l'onglet **Vue d'ensemble** ou d'extraire les données pour tous les onglets. Si vous choisissez de démarrer avec **Vue d'ensemble uniquement**, vous pouvez recueillir des données pour les autres onglets en vous rendant dans l'onglet que vous souhaitez afficher et en cliquant sur le bouton **Actualiser** en haut de cette section.



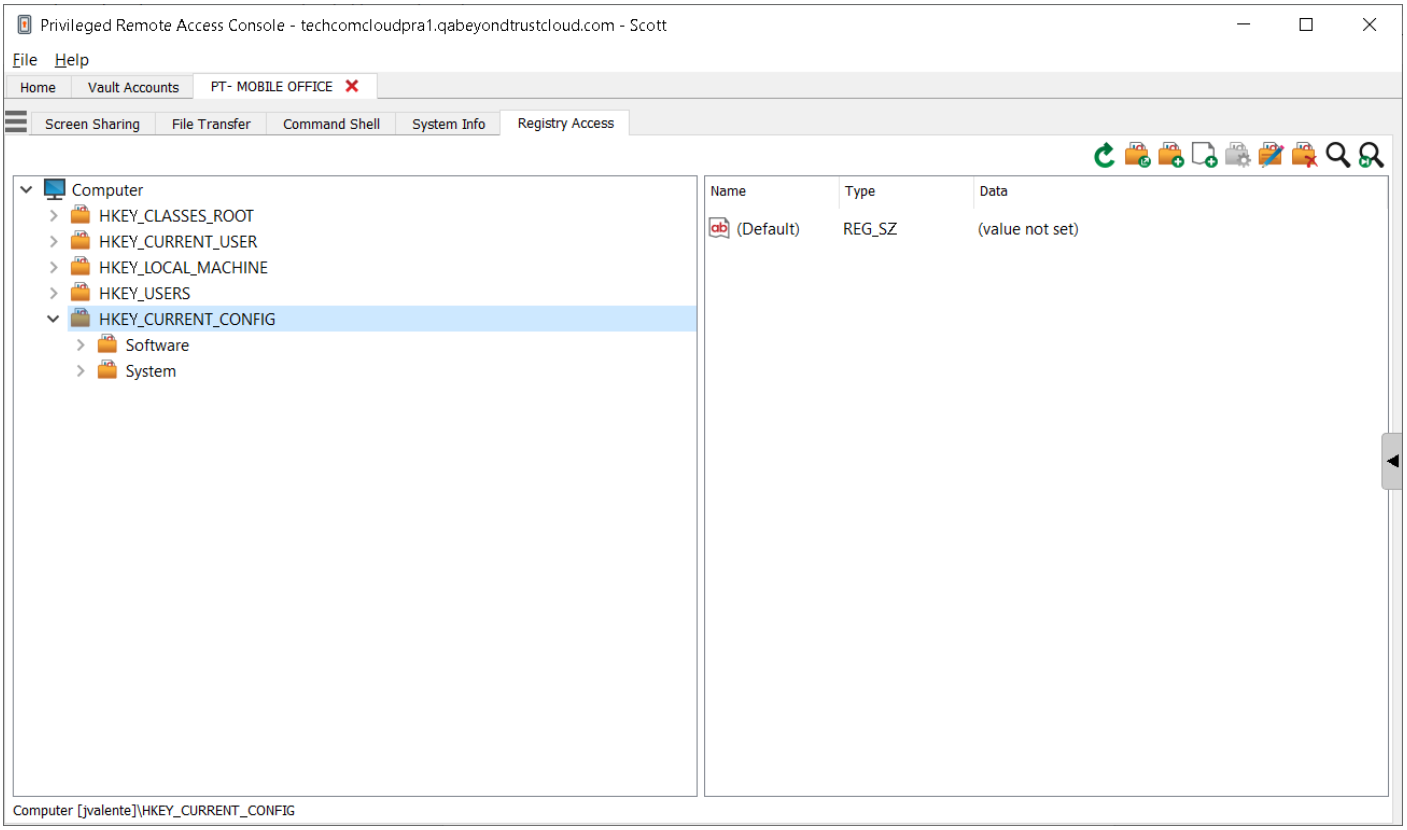


Outils d'informations système

	Mettez fin à l'extraction des informations relatives au système distant. Une interruption permet toujours de voir les dernières informations mises à jour, mais pas d'extraire les données actuelles.
	Actualisez l'affichage des informations système ou extrayez les informations pour les onglets auxquels vous n'avez pas encore demandé l'accès. L'actualisation peut s'effectuer pour des sections individuelles ou pour toutes les sections de l'onglet sélectionné.
	Définissez l'actualisation automatique d'une catégorie d'informations système.
	Copiez les informations vers le presse-papiers. Copiez des sections individuelles ou toutes les sections de l'onglet sélectionné.
	Enregistrez un fichier texte des informations système sur votre ordinateur local. Vous pouvez enregistrer des sections individuelles ou toutes les sections de l'onglet sélectionné.
	Mettez fin à un processus en cours d'exécution sur le système distant.
	Désinstallez une application sur le système distant.
	Démarrez un service arrêté sur le système distant.
	Reprenez un service en pause sur le système distant.
	Mettez en pause un service en cours sur le système distant.
	Arrêtez un service en cours sur le système distant.
	Redémarrez un service en cours sur le système distant.

Accès à l'éditeur de registre sur le point de terminaison distant

Accéder au registre d'un système Windows distant sans nécessiter le partage d'écran. Dans l'éditeur de registre virtuel, vous pouvez ajouter de nouvelles clés, supprimer, modifier, rechercher, importer ou exporter des clés.



Outils de l'éditeur de registre

	Actualiser le registre
	Importer des entrées de registre à partir d'un fichier
	Exporter des entrées de registre vers un fichier
	Créer une nouvelle clé de registre
	Créer une nouvelle valeur de registre

	Modifier la valeur de registre sélectionnée
	Renommer l'entrée de registre sélectionnée
	Supprimer l'entrée de registre sélectionnée
	Effectuer une recherche dans le registre
	Rechercher suivant.

Gestion de session et collaboration d'équipe

Afficher les sessions d'accès actives

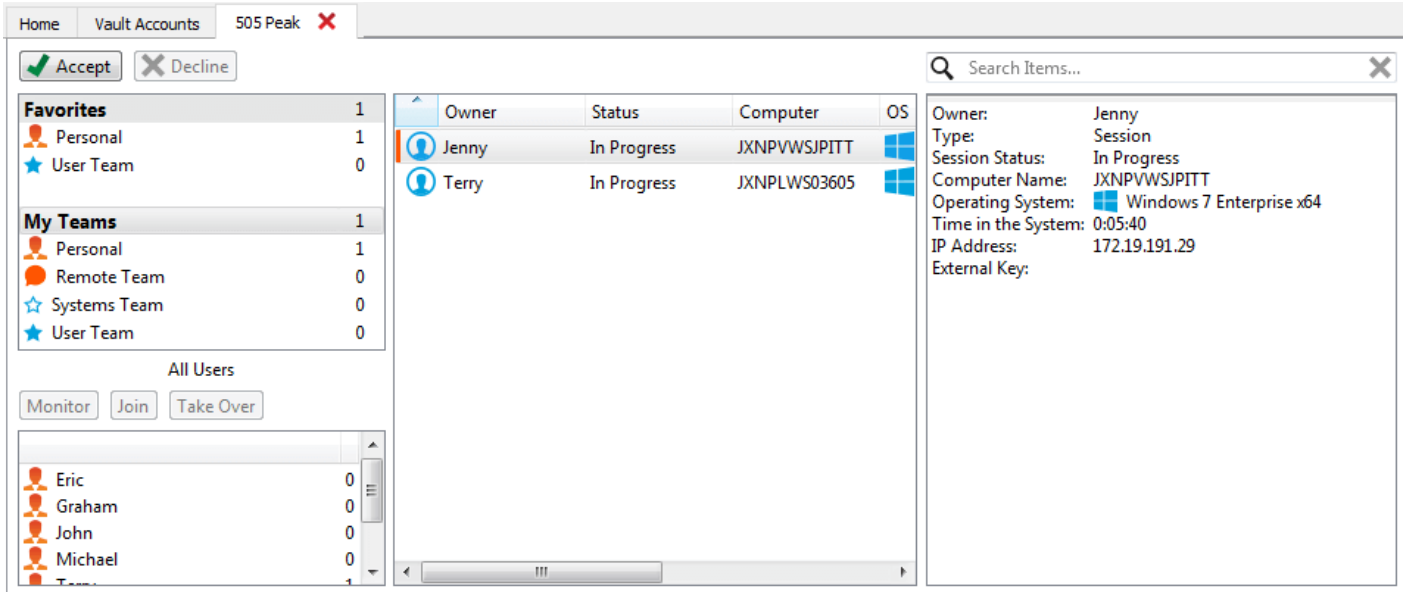
Les files d'attente de session fournissent des informations sur les sessions en cours et permettent d'y accéder. La file d'attente **personnelle** répertorie toutes les sessions actuellement en cours, ainsi que les invitations à rejoindre une session partagée que vous avez reçues.

Vous disposez aussi de files d'attente pour toutes les équipes dont vous êtes membre. Lorsqu'un autre utilisateur demande à un membre d'une équipe de rejoindre une session, son invitation apparaît dans la file d'attente de l'équipe. Si aucune équipe spécifique n'est sélectionnée, les responsables et les chefs d'équipe peuvent aussi voir les membres avec une session en cours.

Cliquez sur l'étoile à gauche du nom d'équipe pour signaler cette file d'attente comme favorite. Lorsqu'on envoie un message depuis la messagerie de l'équipe, une bulle orange apparaît à la place de l'étoile.

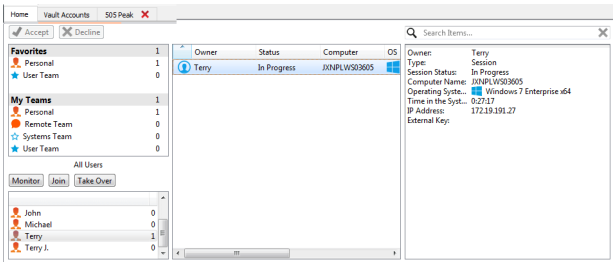
Triez vos files d'attente selon plusieurs critères, comme le temps écoulé de la session, le nom de l'ordinateur, la clé externe, etc. Vous pouvez rechercher une session active. Cliquez sur un élément dans la file d'attente pour consulter ses informations. Cliquez une seconde fois pour fermer la fenêtre d'informations. La access console se souviendra de l'ordre des colonnes et de l'organisation de la file d'attente des sessions la prochaine fois que la access console sera lancée.

Il est possible d'exécuter plusieurs sessions simultanément. En haut de la access console, un onglet apparaît pour chaque session ouverte.



Utiliser le tableau de bord pour administrer les membres d'équipe

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.



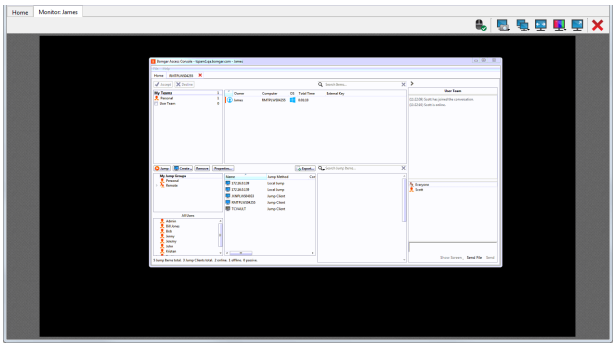
Si un utilisateur est responsable ou chef d'une ou plusieurs équipes et qu'il sélectionne l'une de ces files d'attente, le volet du tableau de bord s'affiche sous le volet de sélection de file d'attente dans l'onglet **Accueil** de la console. Ce volet répertorie tous les membres de rang inférieur connectés appartenant à l'équipe sélectionnée.

Sélectionnez un utilisateur dans le volet du tableau de bord pour afficher toutes les sessions qu'il effectue. Un responsable ou un chef d'équipe peut prendre le contrôle de la session d'un autre utilisateur de cette équipe en sélectionnant la session en question dans la file d'attente, puis en cliquant sur le bouton **Prendre le contrôle**. Ceci transfère la propriété de cette session au responsable ou chef de l'équipe ; l'utilisateur d'origine reste dans la session en tant que participant.

Le responsable d'équipe a aussi la possibilité de rejoindre une session en cours en cliquant sur le bouton **Rejoindre**. Cette démarche est similaire à celle de rejoindre une session par le biais d'une invitation, bien qu'aucune invitation ne soit requise.

> ***Remarque :*** *le chef d'équipe peut rejoindre ou reprendre la session d'un membre de l'équipe uniquement si le chef d'équipe dispose d'un accès à la session de démarrage pour l'élément de Jump qui a été utilisé pour créer la session, ou si le paramètre du tableau de bord autorisant la participation ou la reprise sans accès à la session de démarrage est coché.*

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.



Une icône est affichée dans un coin du bureau de l'utilisateur pour indiquer qu'il est surveillé. Lorsque l'utilisateur déplace le curseur près de cette icône, elle se déplace dans un autre coin pour ne pas gêner la visibilité de l'écran. Sélectionnez l'utilisateur dont vous voulez voir l'écran, puis cliquez sur le bouton **Surveiller**. Ceci ouvre un nouvel onglet dans votre console, affichant la console de l'utilisateur.

Pour pouvoir contrôler l'ordinateur de l'utilisateur, cliquez sur le bouton **Activer le contrôle souris/clavier**.

Au sein d'une équipe, un utilisateur ne peut administrer que les personnes ayant un rôle inférieur au sien. Sachez toutefois que les rôles s'appliquent strictement au cas par cas pour chaque 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.

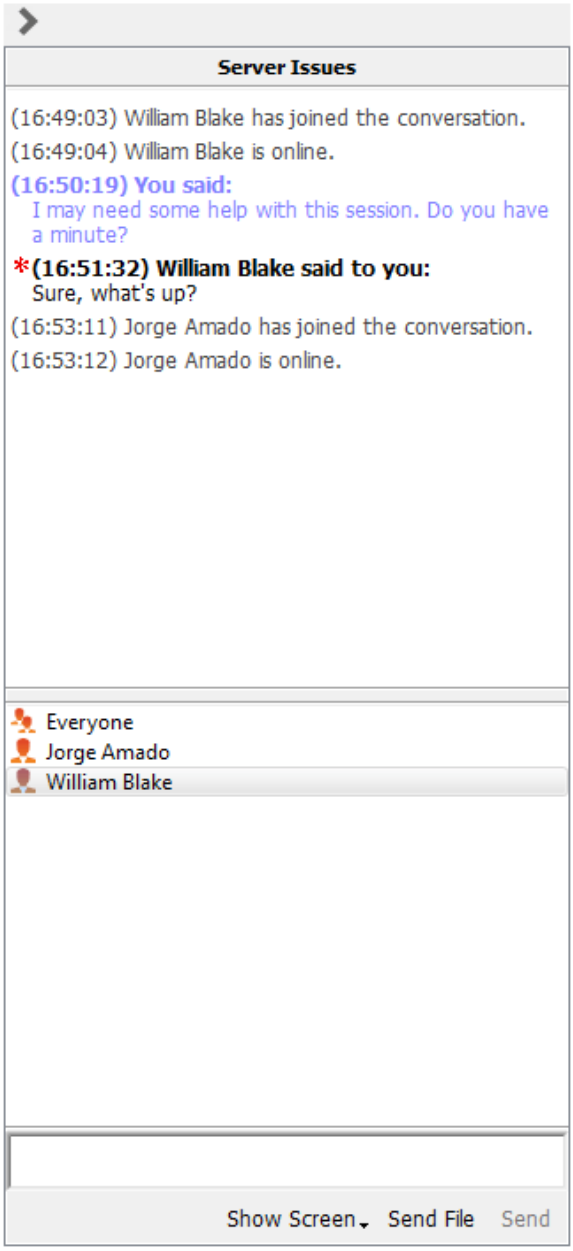
Discuter avec d'autres utilisateurs

Depuis l'onglet **Accueil** de la console, vous pouvez discuter avec d'autres utilisateurs connectés. Si vous appartenez à une ou plusieurs équipes, sélectionnez celle avec laquelle vous souhaitez discuter dans la liste des files d'attente située à gauche de l'onglet **Accueil**. Vous pouvez alors discuter avec tous les membres de cette équipe ou avec un membre en particulier.

Cliquez sur la flèche située dans l'angle supérieur gauche de la barre latérale pour réduire la barre latérale glissante. Lorsque la barre latérale est réduite, passez sur la flèche de la fenêtre cachée pour la révéler. Cliquez sur l'icône Attacher qui a remplacé la flèche dans l'angle supérieur gauche de la barre latérale pour rattacher la barre latérale glissante.

Lorsque vous saisissez un message, les mots mal orthographiés seront soulignés en rouge. Faites un clic droit pour consulter les suggestions orthographiques ou pour les ignorer pour la connexion actuelle de la console.

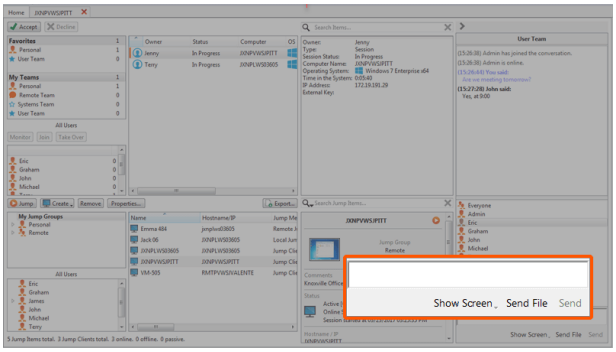
Dans les paramètres, vous pouvez choisir si la messagerie instantanée de l'équipe doit inclure les messages d'état, comme la connexion et déconnexion d'utilisateurs, ou seulement les messages instantanés envoyés entre membres de l'équipe.



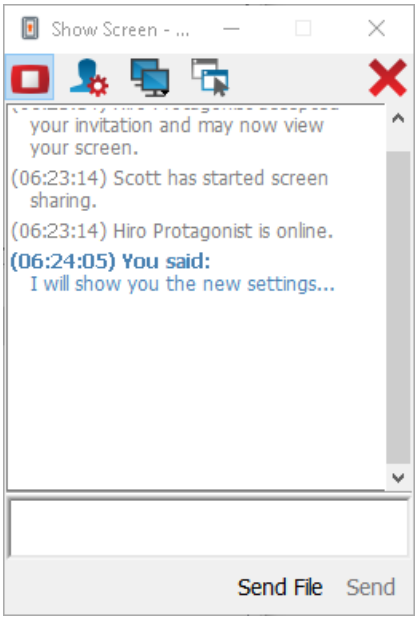
Partager votre écran avec un autre utilisateur

Si votre administrateur a activé cette autorisation, vous pouvez partager votre écran avec un autre utilisateur, sans que celui-ci ait besoin de rejoindre une session. Notez que cette option est disponible même lorsque vous n'êtes pas en session.

À partir d'une file d'attente d'équipe, sélectionnez un utilisateur, puis cliquez sur **Montrer l'écran**. Si vous travaillez avec plusieurs moniteurs, vous pouvez choisir lequel partager, ou sélectionner les applications qui seront visibles pour l'autre utilisateur. Une fois votre sélection effectuée, l'utilisateur bénéficiaire recevra une notification lui permettant d'accepter ou de refuser l'invitation.



Une fenêtre **Montrer l'écran** s'affiche, indiquant le nom de l'utilisateur qui voit votre écran. Cette fenêtre contient une messagerie instantanée et des options permettant d'arrêter le partage d'écran, de donner le contrôle à l'autre utilisateur et de sélectionner le moniteur et les applications à partager. Vous pouvez arrêter le partage d'écran tout en gardant cette fenêtre ouverte, ou fermer complètement la session de partage. Le fait de laisser la fenêtre **Montrer l'écran** ouverte permet de redémarrer ultérieurement le partage d'écran.



Outils de partage d'écran

Utilisateur partageant

	Arrêtez temporairement le partage de votre écran avec un autre utilisateur. Cette option interrompt le partage d'écran sans fermer la fenêtre **Montrer l'écran**, afin de vous permettre de reprendre le partage ultérieurement.
	Redémarrez le partage d'écran.
	Accordez le contrôle de la souris et du clavier à l'utilisateur regardant votre écran.

	Sélectionnez le moniteur à partager avec un autre utilisateur. Le moniteur principal est désigné par la lettre **P**.
	Sélectionnez les applications à partager avec l'utilisateur regardant votre écran.
	Fermez la session de partage d'écran. Ceci ferme l'interface de partage d'écran avec un utilisateur.

Utilisateur en visualisation

	L'utilisateur partageant son écran avec vous vous a donné le contrôle de son clavier et de sa souris.
	Allumez un pointeur virtuel visible sur l'écran de l'utilisateur partageant.
	Effectuez une capture de l'écran de l'utilisateur partageant à sa résolution complète.
	Visualisez l'écran distant à sa taille réelle ou mis à l'échelle.
	Affichez le bureau distant en mode plein écran ou revenez à l'affichage de l'interface.
	Fermez la session de partage d'écran. Ceci ferme l'interface de partage d'écran avec un utilisateur.

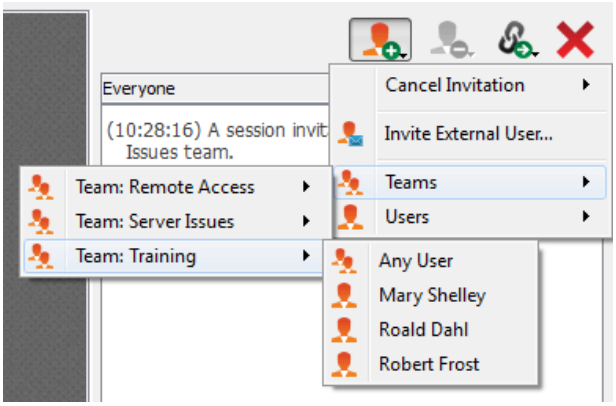
Partager une session avec d'autres utilisateurs

Invitez un autre utilisateur à rejoindre une session en cliquant sur le bouton **Partager** dans les outils de session. Par défaut, seules les équipes auxquelles vous appartenez seront répertoriées.

Vous pouvez sélectionner un utilisateur répertorié dans les équipes affichées pour l'inviter à rejoindre la session.

Si vous sélectionnez **N'importe quel utilisateur**, l'invitation est envoyée à la file d'attente d'équipe afin que n'importe quel utilisateur de l'équipe sélectionnée puisse rejoindre la session. Vous pouvez envoyer plusieurs invitations si vous souhaitez que plusieurs utilisateurs d'une équipe rejoignent votre session.

Les utilisateurs sont répertoriés ici uniquement s'ils sont connectés à la console, ou si leur mode Disponibilité étendue est activé.



Si vous êtes autorisé à partager des sessions avec les utilisateurs qui ne sont pas membres de vos équipes, des équipes supplémentaires sont affichées, à condition qu'elles comprennent au moins un membre connecté ou ayant le mode disponibilité étendue activé.

Lorsque vous invitez un utilisateur ayant la disponibilité étendue activée, il recevra une notification par e-mail.

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**. 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.

Une invitation devient inactive lorsqu'un des évènements suivants se produit :

- L'utilisateur qui invite annule l'invitation
- La session se termine
- L'utilisateur invité accepte l'invitation
- L'utilisateur invité refuse l'invitation

Lorsqu'un utilisateur supplémentaire rejoint une session partagée, il a accès à tout l'historique de la discussion.

Discuter avec d'autres utilisateurs lors d'une session partagée

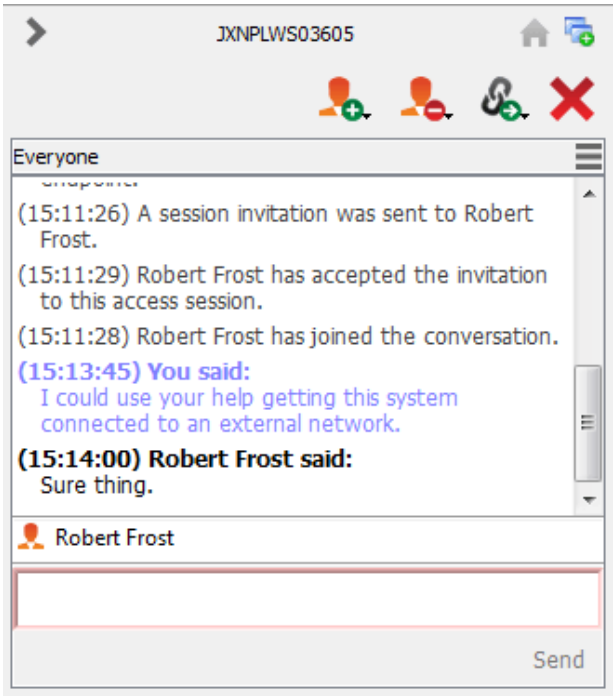
La fenêtre de messagerie instantanée fait office de journal pour tout ce qui se produit au cours de la session, y compris les fichiers transférés et les outils utilisés.

Si un ou plusieurs utilisateurs partagent la session, vous pouvez discuter avec eux. Lorsqu'un utilisateur supplémentaire rejoint une session partagée, il a accès à tout l'historique de la discussion.

Cliquez sur la flèche située dans l'angle supérieur gauche de la barre latérale pour réduire la barre latérale glissante. Lorsque la barre latérale est réduite, passez sur la flèche de la fenêtre cachée pour la révéler. Cliquez sur l'icône Attacher qui a remplacé la flèche dans l'angle supérieur gauche de la barre latérale pour rattacher la barre latérale glissante.

Lorsque vous saisissez un message, les mots mal orthographiés seront soulignés en rouge. Faites un clic droit pour consulter les suggestions orthographiques ou pour les ignorer pour la connexion actuelle de la console.

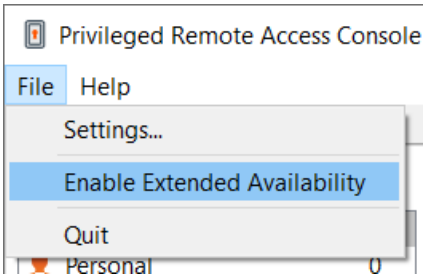
Les messages apparaissent sous forme de texte dans la fenêtre de messagerie instantanée. Vous pouvez ajouter des balises BBCode à un message ou en modifier, afin de mettre en forme le texte. Le formatage est appliqué une fois le message envoyé.



Remarque : *il est possible de repositionner les différentes sections de widget affichées sur la barre latérale, comme la fenêtre de messagerie instantanée, le volet d'informations de session, etc. Lorsque vous survolez la barre de titre d'une section, le pointeur devient une main fermée, ce qui vous permet de faire glisser et de repositionner cette section sur la barre latérale.*

Utiliser la disponibilité étendue pour rester accessible hors connexion

Grâce à la disponibilité étendue, les utilisateurs privilégiés peuvent recevoir des invitations par e-mail pour partager des sessions, même s'ils ne sont pas connectés à la console. Lorsque vous envoyez une invitation, vous pouvez inviter des membres de votre équipe. Si vous y êtes autorisé, vous pouvez également inviter des utilisateurs d'équipes auxquelles vous n'appartenez pas.



Si votre compte est configuré pour la disponibilité étendue, vous pouvez activer ou désactiver la fonctionnalité dans le menu **Fichier** de la access console.

Si vous activez la disponibilité étendue, vous verrez une notification lorsque vous vous connecterez à la console. Cette boîte de dialogue vous permet de désactiver facilement la disponibilité étendue pour éviter toute distraction, par exemple pendant une session.

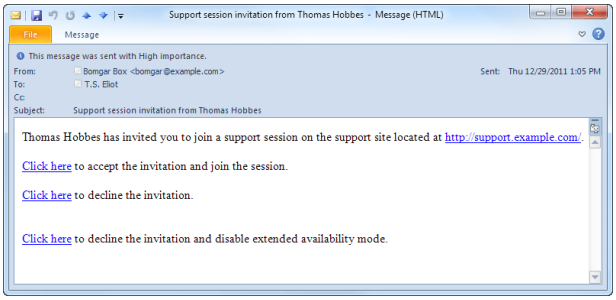
Invitation et notification par e-mail

Chaque fois que vous activez le mode disponibilité étendue, la B Series Appliance vous informera grâce à l'adresse e-mail configurée pour votre compte utilisateur.

> ***Remarque :*** *BeyondTrust n'extrait pas d'adresse e-mail des magasins d'annuaires externes LDAP. L'adresse e-mail doit être configurée dans BeyondTrust d'une des manières suivantes :*
>
> 1. *Un administrateur peut ajouter une adresse e-mail à un compte d'utilisateur en allant sur* ***/login > Utilisateurs et sécurité > Utilisateurs*** *et en modifiant le compte.*
> 2. *L'utilisateur peut définir sa propre adresse e-mail en allant sur la page* ***/login > Mon compte****.*

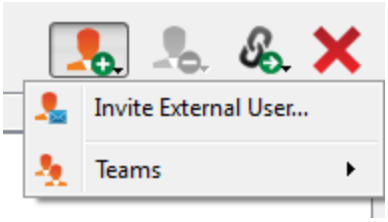
La notification inclut l'URL du site ainsi qu'un lien pour désactiver rapidement le mode disponibilité étendue.

La B Series Appliance envoie également une notification par e-mail lorsque vous êtes invité à une session. Cela vous permet de rejoindre une session même sans être connecté à la console. La notification par e-mail inclut des liens permettant d'accepter ou de refuser l'invitation, tout en désactivant le mode Disponibilité étendue.



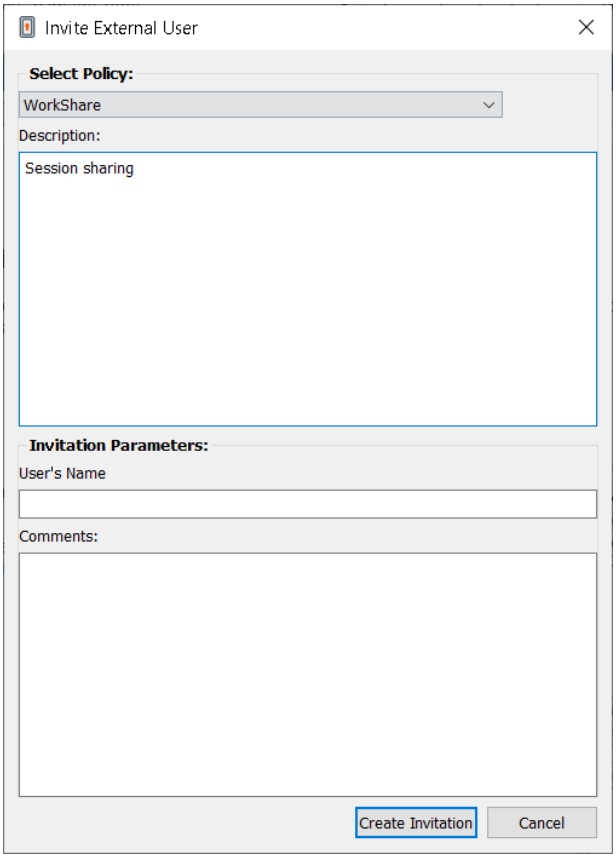
Inviter un utilisateur externe à rejoindre une session d'accès

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

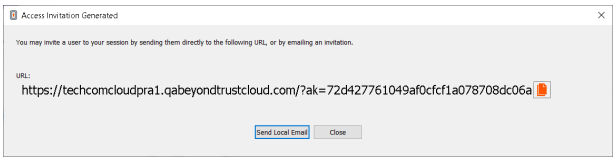


Une fenêtre de dialogue s'ouvre et demande à l'utilisateur de sélectionner une règle de session. Ces règles sont créées dans l'interface d'administration et déterminent le niveau d'autorisation dont bénéficie l'utilisateur externe. Lorsque vous sélectionnez une règle, la description complète s'affiche en dessous.

Saisissez le nom de l'utilisateur invité. Ce nom apparaîtra 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 **Créer une invitation** pour afficher une nouvelle fenêtre de dialogue contenant l'URL d'invitation.



Cliquez sur le bouton **Envoyer** pour sélectionner la façon d'envoyer la clé de session à l'utilisateur externe. 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.



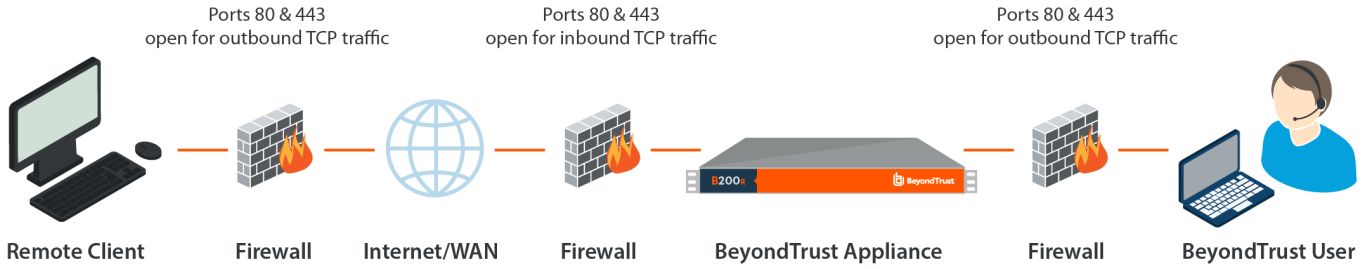
L'utilisateur externe peut uniquement accéder à l'onglet de session et dispose de privilèges restreints. L'utilisateur externe ne peut jamais être le propriétaire de la session. Lorsque l'utilisateur qui invite quitte la session, l'utilisateur externe est déconnecté.

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

Ports et pare-feu

Les solutions BeyondTrust sont conçues pour fonctionner en transparence au travers des pare-feu, et permettent une connexion avec tout ordinateur disposant d'une connexion à internet, partout dans le monde. Toutefois, avec certains réseaux hautement sécurisés, une configuration supplémentaire peut s'avérer utile.

TYPICAL NETWORK SETUP



- Les ports 80 et 443 doivent être ouverts au trafic TCP sortant sur les pare-feu de l'utilisateur et du système distant. Il est possible que davantage de ports soient disponibles en fonction de votre version. Ce schéma montre une configuration réseau type ; vous trouverez des informations supplémentaires dans le Guide d'installation matérielle de la BeyondTrust Appliance B Series à l'adresse https://www.beyondtrust.com/docs/privileged-remote-access/getting-started/deployment/hardware-sra/index.htm.
- Des logiciels de sécurité internet tels que des pare-feu ne doivent pas bloquer le téléchargement des fichiers exécutables BeyondTrust. Sont concernés notamment McAfee Security, Norton Security et Zone Alarm. Si vous disposez d'un logiciel pare-feu, vous pouvez constater quelques problèmes de connexion. Afin d'éviter ces problèmes, configurez votre pare-feu de façon à autoriser les fichiers exécutables suivants, où {uid} est un identificateur unique composé de lettres et de chiffres :
    - bomgar-scc-{uid}.exe
    - bomgar-scc.exe
    - bomgar-pac-{uid}.exe
    - bomgar-pac.exe
    - bomgar-pec-{uid}.exe
    - bomgar-pec.exe

  Pour obtenir une assistance au niveau de la configuration de votre pare-feu, veuillez contacter le fabricant du logiciel du pare-feu.
- Des exemples de règles de pare-feu basées sur l'emplacement de la B Series Appliance peuvent être trouvés à l'adresse www.beyondtrust.com/docs/privileged-remote-access/getting-started/deployment/dmz/firewall-rules.htm.

Si vous ne parvenez toujours pas à établir une connexion, contactez l'BeyondTrust Technical Support à l'adresse www.beyondtrust.com/support.