BeyondTrust

Privileged Remote Access
Console d’accès Privileged Web

TC:11/17/2022

Table of Contents

Guide de la console d'accès Privileged Web

Avec la privileged web access console BeyondTrust, les équipes d'informations et de cybersécurité peuvent accorder à des utilisateurs privilégiés un accès sécurisé distant à des systèmes critiques, même lorsque ces utilisateurs ne peuvent pas installer de logiciel dans leur propre environnement de bureau. Au lieu de cela, ils peuvent accéder à des points de terminaison à travers la access console. Ceci garantit que l'accès nécessaire peut toujours être accordé et permet aux propriétaires de systèmes de répondre aux exigences professionnelles, comme le temps de disponibilité d'un système et toute autre réglementation interne ou externe, sans compromettre les défenses mises en place pour protéger l'organisation de cyber attaques.

Dans ce guide, nous parlerons spécifiquement de la privileged web access console et de la façon dont cette access console fonctionnant sur navigateur accède aux points de terminaison et accomplit d'autres fonctions nécessaires tout en garantissant le plus haut niveau de sécurité.

> ***Remarque :*** *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. Si vous avez besoin d'aide, contactez l'BeyondTrust Technical Support à l'adresse www.beyondtrust.com/support.*

Exigences de la console d'accès Privileged Web

Pour exécuter la privileged web access console sur votre système, votre B Series Appliance doit utiliser la version logicielle 15.3 ou supérieure. La privileged web access console est prise en charge par les plates-formes et navigateurs suivants :

Plates-formes

- Windows
- Macintosh
- Linux

Navigateurs

- Chrome 46+
- Firefox 42+
- Internet Explorer 11+
- Safari 8+
- Windows Edge

IMPORTANT !

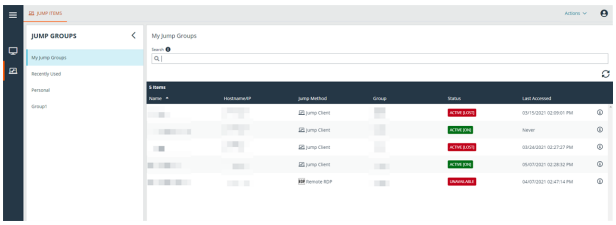
Votre B Series Appliance doit être équipée d'un certificat SSL valide signé par une autorité de certificat. Une fois que vous avez appliqué un certificat SSL signé par une AC à votre B Series Appliance, contactez l'BeyondTrust Technical Support. Votre technicien service client créera une nouvelle version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

Lancer la console d'accès Web

La privileged web access console vous permet d'accéder de façon sécurisée à vos points de terminaison en vous y connectant à distance par le biais de la B Series Appliance. Pour commencer à accéder à des points de terminaison au moyen de la privileged web access console, suivez les étapes décrites ci-dessous.

Lancer la console d'accès Web avec /console

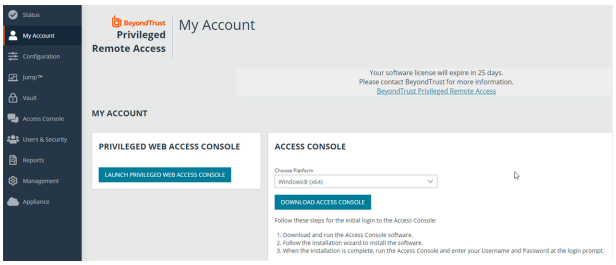
1. Dans la barre d'adresse de votre navigateur, saisissez le nom d'hôte de votre site BeyondTrust suivi de **/console**, par exemple, **access.example.com/console**).
2. Saisissez ensuite le nom d'utilisateur et le mot de passe associés à votre compte d'utilisateur BeyondTrust.
3. Cliquez sur **Connexion** pour démarrer votre session de access console basée sur le Web.



Lancer la console d'accès Web avec /login

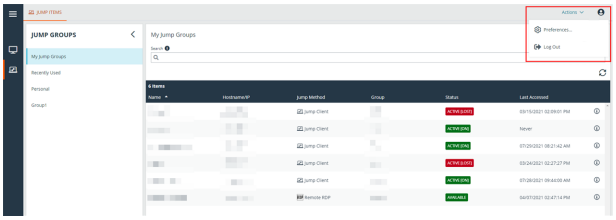
> ***Remarque :*** *par défaut, le bouton* ***Lancer la Privileged Web Access Console*** *n'est pas disponible dans l'interface d'administration /login. Vous devez aller dans* ***Gestion > Sécurité*** *et cocher* ***Permettre à la Access Console mobile et à la Privileged Web Access Console de se connecter*** *pour activer la console.*

1. Dans la barre d'adresse de votre navigateur, saisissez le nom d'hôte de votre site BeyondTrust suivi de **/login**, par exemple, **access.example.com/login**).
2. Saisissez ensuite le nom d'utilisateur et le mot de passe associés à votre compte d'utilisateur BeyondTrust.
3. Cliquez sur **Connexion**.
4. Sélectionnez **Mon compte**.
5. Cliquez sur **Lancer Privileged Web Access Console**.



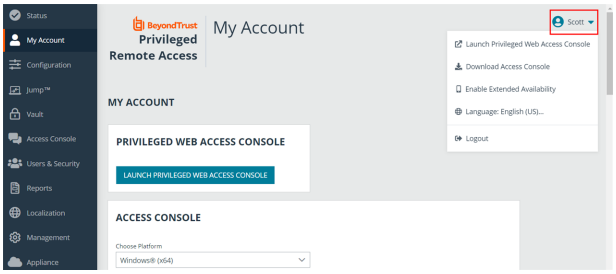
6. La privileged web access console s'ouvrira dans un nouvel onglet, et vous pourrez commencer à accéder à des points de terminaison.

   Pour quitter la access console, cliquez sur **Déconnexion** dans le coin supérieur droit de l'écran.



Lancez la Privileged Web Access Console depuis le menu déroulant Utilisateur

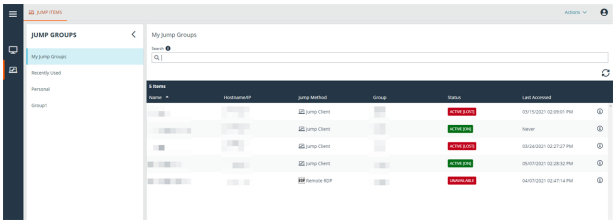
Vous pouvez également lancer la Privileged Web Access Console à partir du menu déroulant Utilisateur situé dans le coin supérieur droit de l'interface utilisateur. Ce menu est accessible à partir de n'importe quel emplacement d'onglet dans le site administratif.



> ***Remarque :*** *si plusieurs langues sont activées sur votre site, vous pouvez modifier la langue utilisée dans la Privileged Web Access Console en cliquant sur le lien* ***Langues*** *dans le menu déroulant Utilisateur et en sélectionnant la langue souhaitée. Cette langue est appliquée à la fois au site /login et à la Privileged Web Access Console.*

Utilisation d'éléments de Jump pour accéder à des points de terminaison dans la console d'accès Privileged Web

Pour accéder à un point de terminaison, installez un élément de Jump sur ce système depuis la page **Jump Clients** de l'interface d'administration /login.



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

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

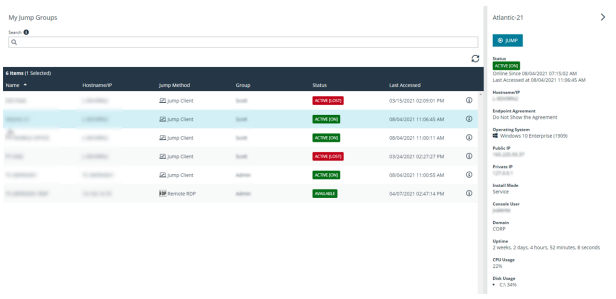
Il existe trois façons de commencer à accéder à des points de terminaison :

- Trouvez et sélectionnez un point de terminaison dans la liste **Mes groupes de Jump**.
- Choisissez un groupe de Jump et sélectionnez un point de terminaison dans la liste des points de terminaison de ce groupe.
- Sélectionnez une session dans la liste des **éléments de Jump fréquemment utilisés**.

> ***Remarque :*** *la liste des* ***éléments de Jump fréquemment utilisés*** *affiche tous les éléments de Jump auxquels vous accédez régulièrement. Pour lancer une session avec un élément fréquent, mettez le pointeur de votre souris sur la session, puis cliquez sur* ***Démarrer une session****.*

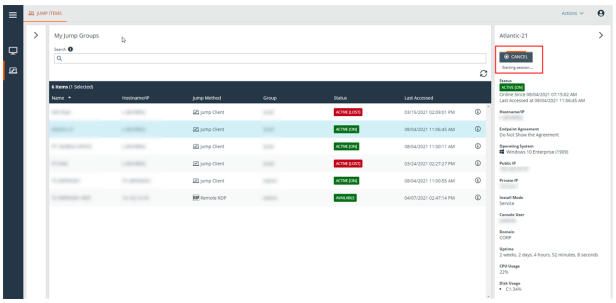
> ***Remarque :*** *La liste des éléments de Jump peut afficher un maximum de 50 éléments de Jump.*

Pour commencer à accéder aux éléments de Jump, suivez les étapes décrites ci-dessous :



1. Sélectionnez un groupe de Jump et appuyez sur le bouton **Actualiser**.
2. Une liste de tous les éléments de Jump sera créée, et vous pourrez voir les détails de chaque élément de Jump, notamment : **Nom**, **Méthode**, **Groupe**, **État** et **Dernier accès**. Pour voir plus de détails sur l'élément de Jump, cliquez sur le signe + à côté du nom de l'élément de Jump.
3. Cliquez sur le bouton **JUMP** pour lancer une session avec le point de terminaison.

4. Pour annuler une demande d'accès à un Jump, cliquez sur **Annuler**.



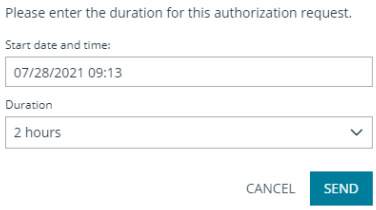
Autorisation pour utilisateur final et tierce partie

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

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

1. Après avoir cliqué sur le bouton **JUMP** et sollicité l'accès, une invite vous demande de justifier votre demande d'accès au système.

2. Vous devez ensuite indiquer à quel moment et pour combien de temps vous accéderez au système.
3. Une fois la requête soumise, la tierce partie ou la personne responsable de l'approbation des demandes d'accès est prévenue par e-mail et peut accepter ou refuser la demande. Bien que d'autres approbateurs sont susceptibles de consulter l'adresse e-mail de la personne ayant autorisé ou refusé la demande, le demandeur n'est pas en mesure de le faire.

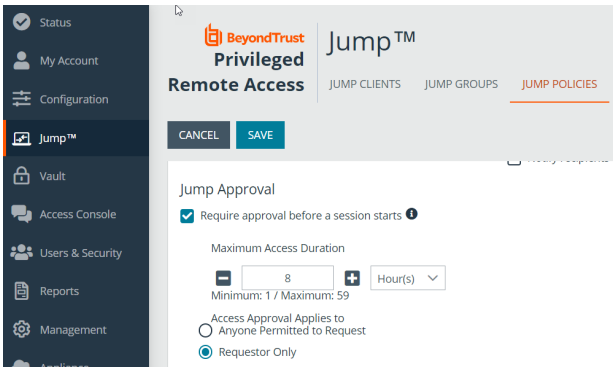


4. Après qu'une autorisation a été établie, une notification d'autorisation apparaît dans les informations de l'élément de Jump, affichant *approuvée* ou *refusée*. Si l'accès est autorisé, vous pouvez appuyer sur le bouton Jump pour accéder au système.
5. Vous verrez ensuite un message vous demandant si vous souhaitez entamer une session d'accès.
6. Si vous choisissez de commencer une session, les commentaires de l'approbateur apparaîtront, et vous pourrez commencer à accéder au système.

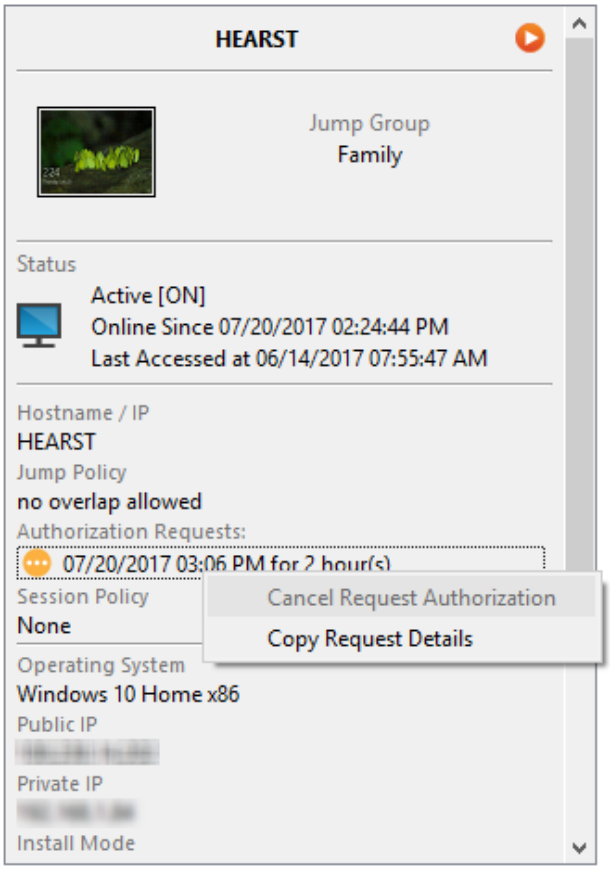
Révocation de la requête d'approbation d'accès

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 :

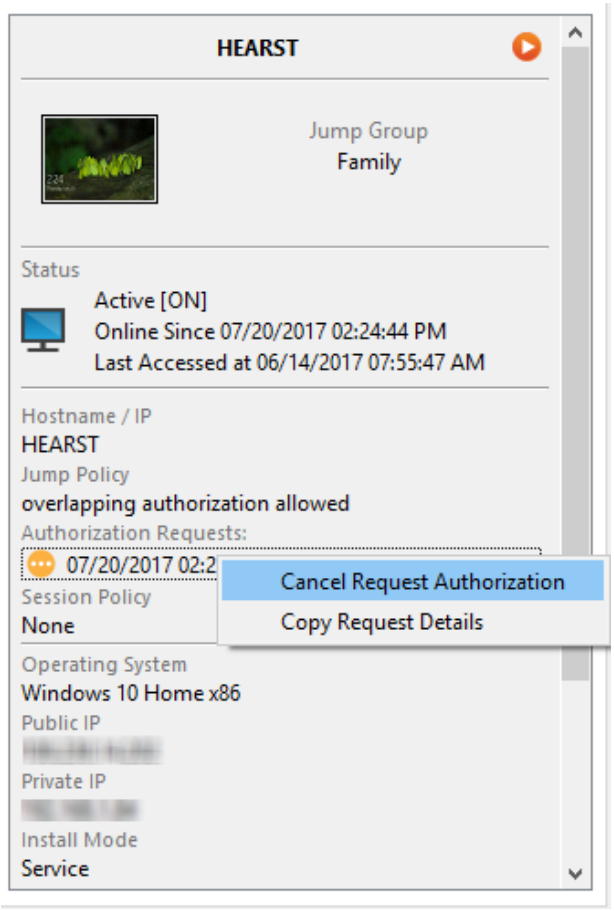
- **Toute personne autorisée à faire une requête**
- **Demandeur seulement**



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.

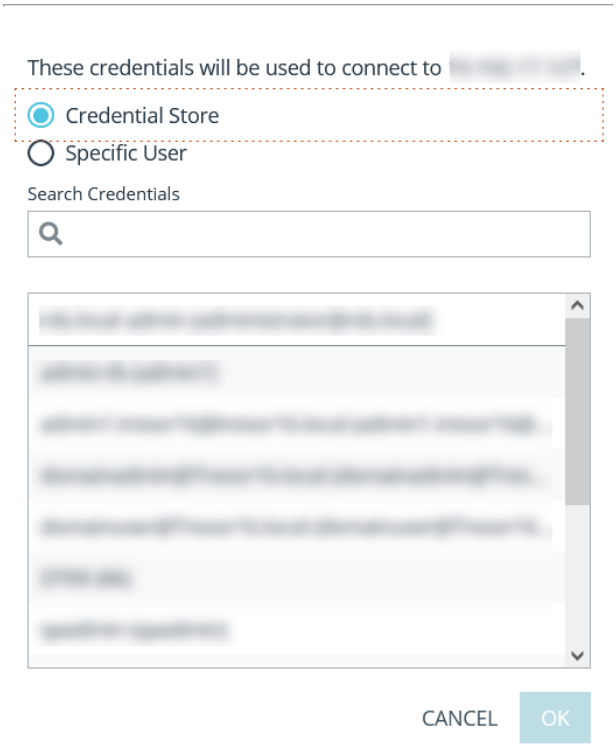


Cependant, si la règle de Jump est définie sur **Toute personne autorisée à faire une requête** et qu'une demande d'accès est actuellement approuvée pour l'utilisateur A, l'utilisateur B est autorisé à démarrer une nouvelle session avec l'élément de Jump s'il tente d'effectuer un Jump vers lui. De plus,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



Informations d'authentification pour connexion automatique

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



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

Connexion aux points de terminaison en utilisant l'injection d'informations d'authentification

Lorsque vous accédez à un élément de Jump basé sur Windows à travers la privileged web 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.

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.*

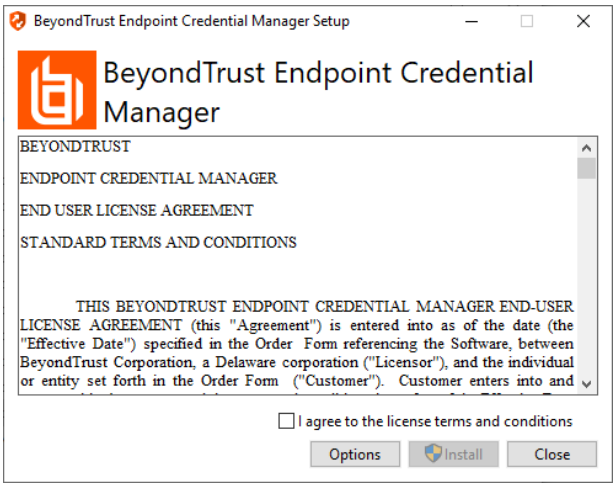
Configuration requise

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

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

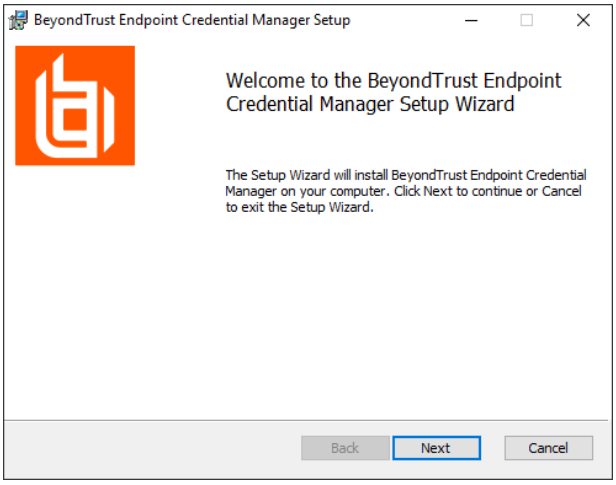
2. Lancez l'assistant de configuration du gestionnaire d'informations d'authentification de point de terminaison BeyondTrust.
3. Acceptez les conditions générales du CLUF. Cochez la case si vous acceptez, puis cliquez sur **Installer**.

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

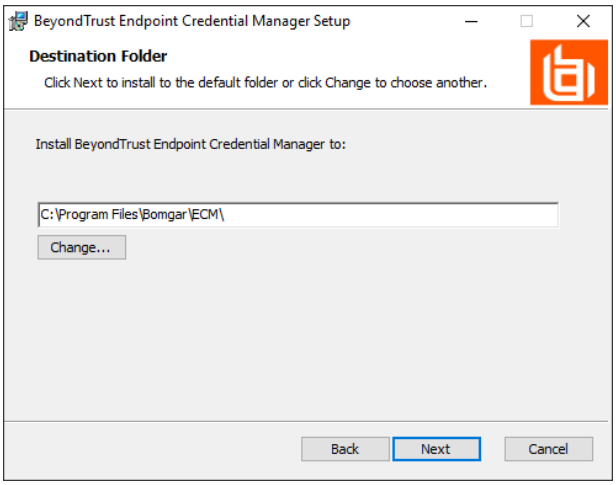


> ***Remarque :*** *vous ne pourrez pas poursuivre l'installation si vous n'acceptez pas le CLUF.*

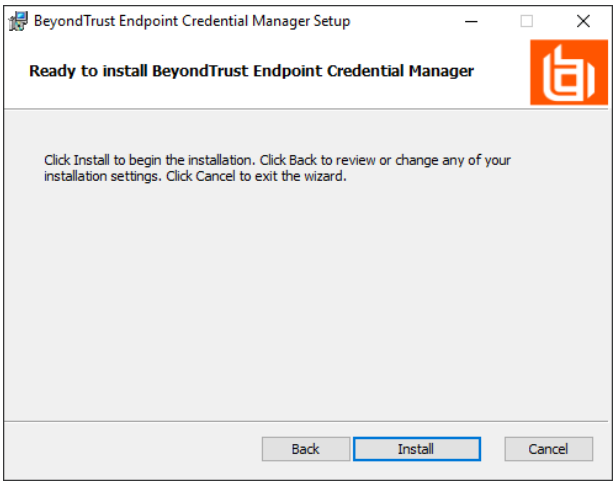
4. Cliquez sur **Suivant** dans l'écran de bienvenue.



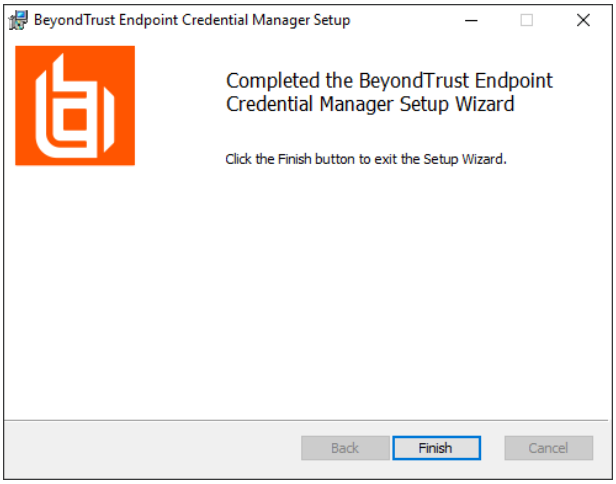
5. Choisissez un emplacement pour le gestionnaire d'informations d'authentification, puis cliquez sur **Suivant**.



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



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



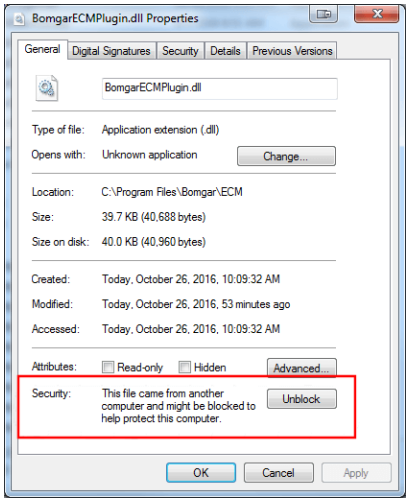
> ***Remarque :*** *pour optimiser le temps de disponibilité, les administrateurs peuvent installer jusqu'à trois ECM sur plusieurs machines Windows pour communiquer avec le même magasin d'informations d'authentification. Une liste des ECM connectés au site de l'appliance est disponible sur* ***/login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

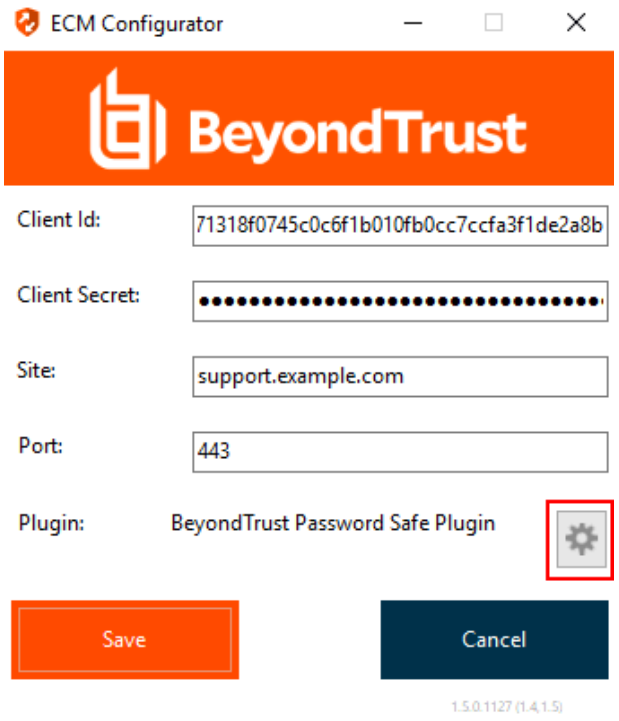
Installer et configurer le plug-in

1. Une fois que l'ECM BeyondTrust est installé, procédez à l'extraction et à la copie des fichiers du plug-in dans le répertoire d'installation (généralement **C:\Program Files\Bomgar \ECM**).
2. Exécutez le **configurateur ECM** pour installer le plug-in.

3. Le configurateur devrait automatiquement détecter le plug-in et le charger. Si c'est le cas, passez à l'étape 4 ci-dessous. Autrement, suivez ces étapes :
    - Tout d'abord, vérifiez que la DLL n'est pas bloquée. Faites un clic droit sur la DLL et sélectionnez **Propriétés**.
    - Dans l'onglet **Général** regardez au bas de l'écran. S'il y a une section **Sécurité** avec un bouton **Débloquer**, cliquez sur ce dernier.
    - Répétez ces étapes pour toutes les autres DLL fournies avec le plug-in.
    - Dans le configurateur, cliquez sur le bouton **Choisir plug-in...** et accédez à l'emplacement de la DLL du plug-in.



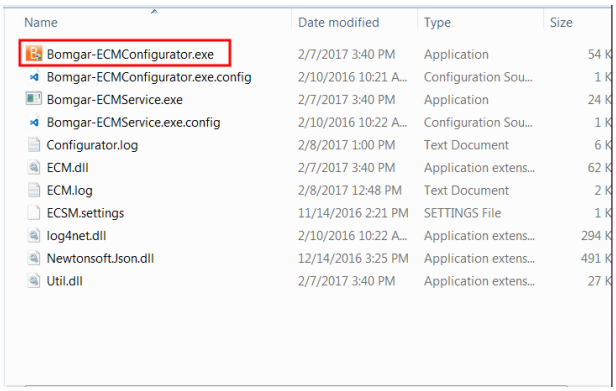
4. Cliquez sur l'icône en forme d'engrenage dans la fenêtre **Configurateur** pour configurer les paramètres du plug-in.



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

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

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

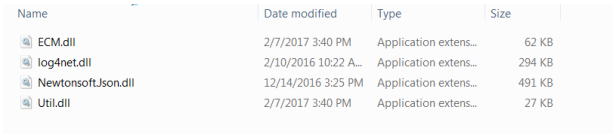


3. Lorsque le configurateur ECM s'ouvre, remplissez les champs. Tous les champs sont obligatoires.

Saisissez les valeurs suivantes :

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

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



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

IMPORTANT !

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

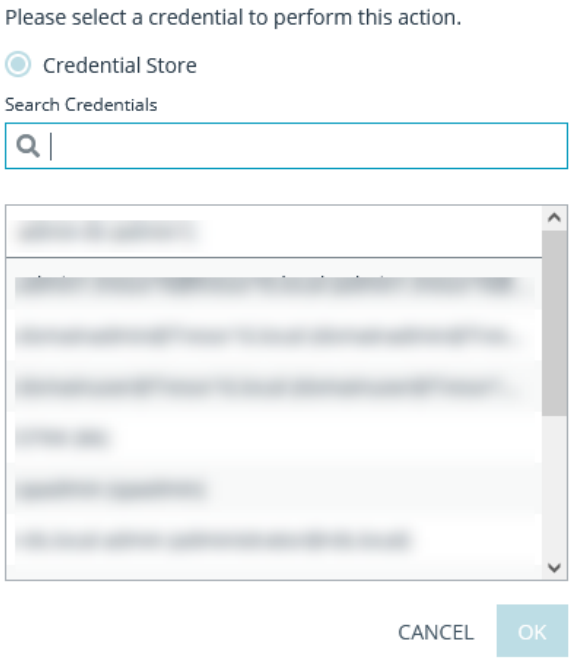
Utiliser l'injection d'informations d'authentification pour accéder à des points de terminaison

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

1. Connexion à la privileged web access console.
2. Effectuez un Jump vers un point de terminaison 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 point de terminaison. Si le point de terminaison 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.

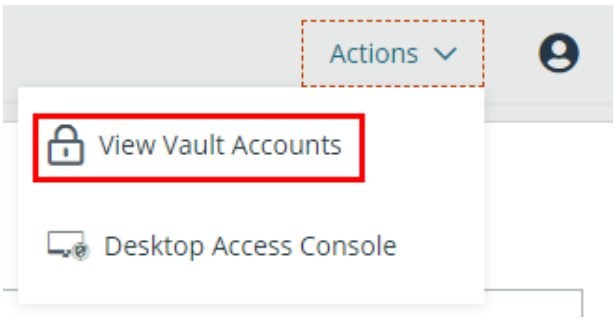
5. Sélectionnez les bonnes informations d'authentification à utiliser depuis l'ECM. Le système récupère les informations d'authentification depuis l'ECM et les injecte sur l'écran de connexion de Windows.
6. L'utilisateur est connecté au point de terminaison.



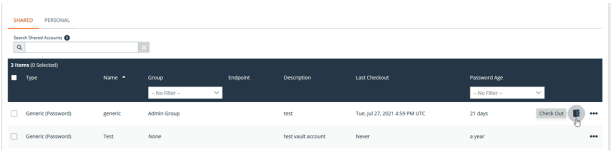
Extraire et injecter des informations d'authentification

Depuis la console d'accès Web, vous pouvez facilement accéder à Privileged Remote Access Vault dans l'interface /login pour extraire ou archiver les informations d'authentification selon les besoins, durant une session ou sur votre machine locale.

Pour accéder au vault, cliquez sur le bouton **Actions** dans la barre de navigation supérieure et sélectionnez **Afficher les comptes Vault**. Vous accédez alors directement à la page **Vault > Comptes** dans l'interface **/login** une fois connecté.



Vous pouvez alors procéder à une extraction ou une injection depuis/dans un compte Vault.



Authentification depuis l'API de script client

Cette fonction permet aux utilisateurs de se connecter à la privileged web access console et d'effectuer un Jump vers un point de terminaison en utilisant l'API de script client PRA (https://www.beyondtrust.com/docs/privileged-remote-access/how-to/integrations/api/client-script/index.htm#client-scripting-api).

L'URL de l'API de script client respecte le format suivant : **https://access.example.com/api/client_script**, access.example.com étant le nom d'hôte de votre B Series Appliance.

L'API accepte un type de client (**web_console**), une opération à effectuer (**execute**), et une commande (**start_jump_item_session**). Aucune autre commande n'est prise en charge pour le type de client **web_console**.

Si l'utilisateur est connecté à la access console de bureau lorsqu'on accède à l'URL de l'API du script client avec **type=web_console**, l'utilisateur sera alors connecté à la privileged web access console et déconnecté de la access console de bureau. Si ce comportement n'est pas souhaité, l'utilisateur doit utiliser une URL d'API de script client comportant **type=rep** au lieu de **type=web_console**.

Inversement, si l'utilisateur est connecté à la privileged web access console et que l'API appelle **type=rep**, l'utilisateur sera connecté à la access console de bureau et déconnecté de la privileged web access console.

Voici un exemple d'une requête valide d'API de script client :

```
https://access.example.com/api/client_script?type=web_console&operation=execute&action=start_jump_item_session&search_string=ABCDEF02
```

Si l'utilisateur est déjà connecté à la privileged web access console, la requête ci-dessus exécute la commande dans l'onglet du navigateur qui exécute la privileged web access console. Dans ce cas, la commande lance une session avec le Jump Client dont le nom d'hôte, les commentaires, l'IP publique ou l'IP privée correspondent à la chaîne de recherche « ABCDEF02 ».

Si l'utilisateur n'est pas déjà connecté à la privileged web access console, la demande ci-dessus ouvre un nouvel onglet du navigateur et envoie l'utilisateur sur /login pour s'authentifier (cette étape est omise si l'utilisateur est déjà connecté sur /login). L'utilisateur est ensuite redirigé vers la privileged web access console, et la commande lance une session avec le Jump Client dont le nom d'hôte, les commentaires, l'IP publique ou l'IP privée correspondent à la chaîne de recherche « ABCDEF02. ».

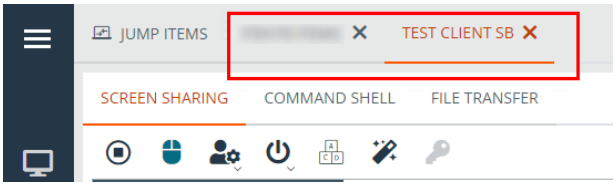
Dans les deux cas, si plus d'un élément de Jump correspond aux critères de recherche, l'utilisateur doit choisir le bon élément de Jump dans une liste. Si aucun élément de Jump ne correspond aux critères de recherche, la privileged web access console affiche un message d'erreur à l'utilisateur.

Tous les critères de recherche pour la commande **start_jump_item_session** sont pris en charge avec **type=web_console**, y compris :

- jump.method
- search_string
- client.hostname
- client.comments
- client.tag
- client.public_ip
- client.private_ip
- session.custom.<nom de code d'attribut>

Retour à une session active dans la console d'accès Privileged Web

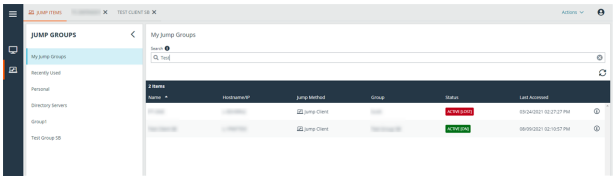
Si vous avez plus d'une access session en cours, vous avez la possibilité de revenir à n'importe laquelle de ces sessions à tout moment. Pour revenir à un point de terminaison ayant déjà fait l'objet d'un accès dans une autre session, cliquez sur la session en haut de l'écran.



Recherche de points de terminaison

Lorsque vous utilisez le privileged web access console, vous pouvez rechercher des points de terminaison spécifiques pendant que vous êtes dans une access session. Dans les résultats de la recherche, vous pouvez aussi cliquer sur le bouton **Démarrer** pour commencer une session avec ce point de terminaison.

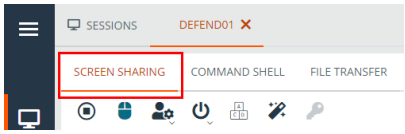
1. Cliquez sur l'icône **Rechercher** située en haut à gauche de l'écran.
2. Dans la barre de recherche, saisissez le nom du point de terminaison.
3. Dans les résultats fournis, sélectionnez le point de terminaison avec lequel vous souhaitez commencer une session, puis cliquez sur le bouton **Jump** pour lancer une session.



Contrôler le point de terminaison distant grâce au partage d'écran en utilisant Privileged Web

Pour voir et contrôler des systèmes distants, utilisez l'action de partage d'écran pendant une session d'accès.

1. Dans la fenêtre de session, cliquez sur l'onglet **Partage d'écran** en haut de l'écran. Vous pouvez aussi cliquer sur l'icône **Démarrer le partage d'écran** pour commencer à accéder au point de terminaison si le partage d'écran ne se lance pas automatiquement.
2. Utilisez l'une des actions suivantes lors d'une session pour utiliser différentes fonctions.



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.
	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.
	Basculez le clavier virtuel.
	Basculez le presse-papiers.
	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**.

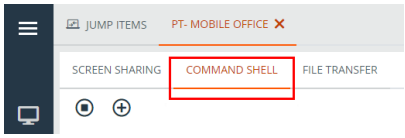
Ouvrir l'interpréteur de commandes sur le point de terminaison distant en utilisant la console Privileged Web

L'interpréteur de commandes distant permet à un utilisateur privilégié d'ouvrir une interface de ligne de commande virtuelle sur un système distant. L'utilisateur peut ensuite effectuer une saisie localement mais 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 le système distant à partir de l'interface de partage d'écran.

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

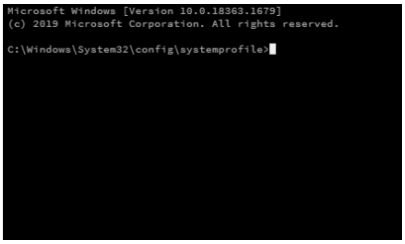
> ***Remarque :*** *selon la règle de session et le type de Jump, l'**interpréteur de commandes** peut ne pas être disponible.*

1. Pour accéder à l'**interpréteur de commandes** pendant une session d'accès, cliquez sur l'onglet **Interpréteur de commandes** dans la partie supérieure de l'écran.



2. Si vous n'êtes pas automatiquement dirigé vers l'interpréteur de commandes, cliquez sur le bouton **Démarrer l'interpréteur de commandes**.

3. Les options et l'invite de commandes apparaîtront.



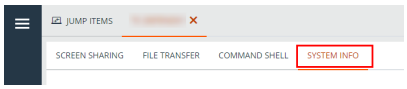
Outils d'interpréteur de commandes

	Mettez fin à l'accès à l'invite de commande une fois que celui-ci n'est plus nécessaire.
	Ouvrez 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.

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.

1. Dans la fenêtre de session, cliquez sur l'onglet **Informations système** en haut de l'écran. Vous pouvez cliquer sur le bouton **Démarrer les informations système** si les informations système ne s'ouvrent pas automatiquement.
2. Utilisez l'une des actions suivantes lors d'une session pour utiliser différentes fonctions.



Outils d'informations système

	Actualiser les informations système.
	Copier dans le presse-papiers.
	Enregistrer dans un fichier.

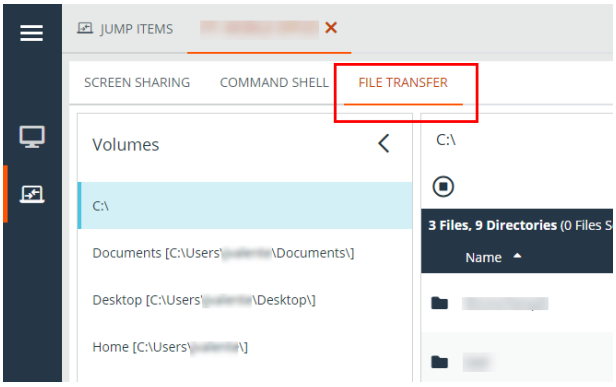
Utiliser la console Privileged Web pour transférer des fichiers vers et à partir de systèmes distants

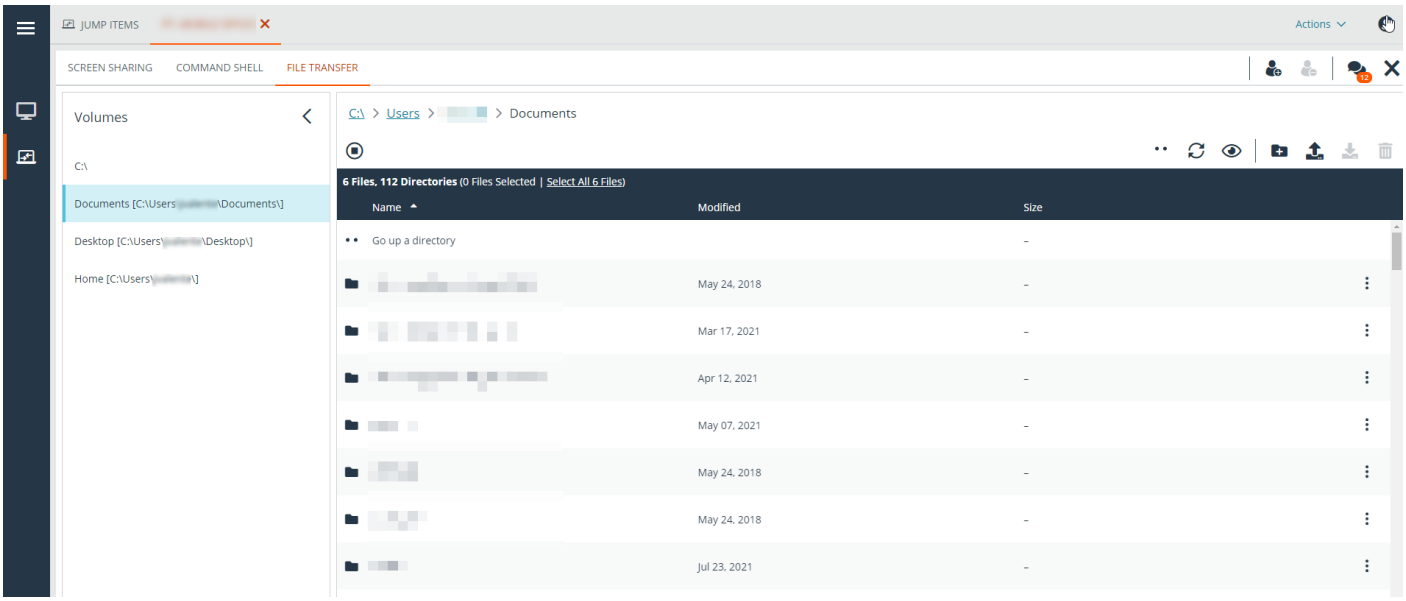
Au cours d'une session, les utilisateurs privilégiés peuvent transférer, supprimer ou renommer des fichiers, et même des répertoires entiers, depuis et vers l'ordinateur distant, depuis l'appareil distant, et depuis et vers la carte SD de l'appareil. Il n'est pas nécessaire d'avoir le contrôle total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

Selon les autorisations que l'administrateur a définies pour votre compte, vous pouvez être uniquement 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, empêchant ainsi le chargement ou le téléchargement dans certains répertoires spéficiques. Transférez les fichiers à l'aide des boutons de chargement/téléchargement. Vérifiez la progression du transfert et de la suppression en cliquant sur le signe plus au bas de l'écran. Téléchargez, renommez ou supprimez des fichiers en cliquant sur l'icône **Plus d'options**.

Pour commencer à transférer des fichiers vers un système, cliquez sur l'onglet **Transfert de fichiers** en haut de l'écran.

Sélectionnez un emplacement pour commencer la navigation dans la colonne **Volumes**. Les fils d'Ariane situés en haut montrent votre emplacement actuel. Double-cliquez sur un dossier pour l'ouvrir.





Outils de transfert de fichiers

	Mettez fin à l'accès au système de fichiers du périphérique distant.
	Remontez d'un répertoire dans le système de fichiers sélectionné.
	Actualisez votre vue du système de fichiers sélectionné.
	Affichez les fichiers masqués.
	Créez un nouveau répertoire.
	Chargez un fichier vers un répertoire.
	Téléchargez les fichiers sélectionnés depuis un répertoire.
	Supprimez les fichiers sélectionnés d'un répertoire.
	Téléchargez, renommez ou supprimez un répertoire ou un fichier.  ***Remarque :*** *la suppression d'un fichier ou d'un dossier est définitive. Il n'est pas envoyé vers la corbeille dans un tel cas.*

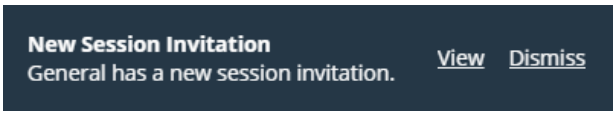
Partager une session avec des membres de l'équipe et des utilisateurs externes en utilisant la Privileged Web Access Console

Inviter des membres de l'équipe

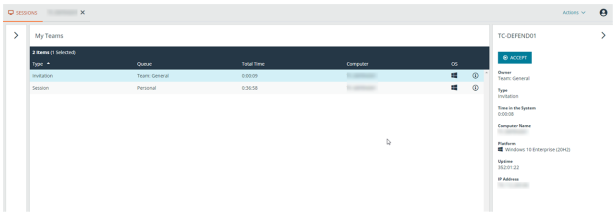
Pendant une session, vous pouvez demander à ce qu'un membre d'équipe participe à une session d'accès. Pour partager une session, suivez les étapes décrites ci-dessous.

1. Cliquez sur l'icône **Inviter d'autres utilisateurs à rejoindre la session**.
2. Sélectionnez l'équipe dont l'utilisateur fait partie dans le menu.
3. Dans le listing de l'équipe, choisissez l'utilisateur avec lequel vous souhaitez partager la session.

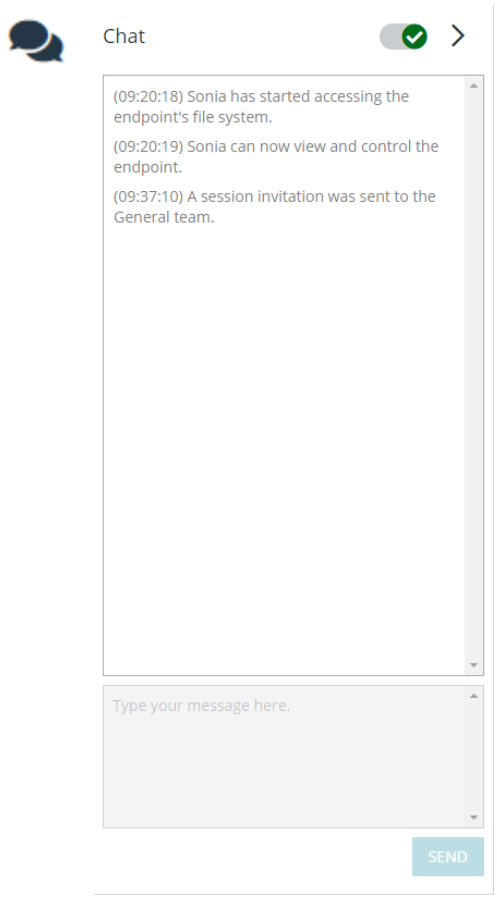
4. L'utilisateur invité verra une notification en bas à gauche de l'écran, lui indiquant qu'il a reçu une invitation pour accéder à une nouvelle session.



5. Cliquez sur **CONSULTER** sur la bannière de notification pour visualiser les informations relatives à la session. L'utilisateur peut ensuite cliquer sur **ACCEPTER** pour accéder à la session.



6. Une fois que l'utilisateur est entré dans la session, vous pouvez dialoguer avec lui en cliquant sur l'icône **Messagerie instantanée** en haut de l'écran.



Vous pouvez envoyer plusieurs invitations si vous souhaitez que plusieurs membres d'une équipe rejoignent votre session. Les utilisateurs sont répertoriés ici uniquement s'ils sont connectés à la access console, ou si leur mode Disponibilité étendue est activé.

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

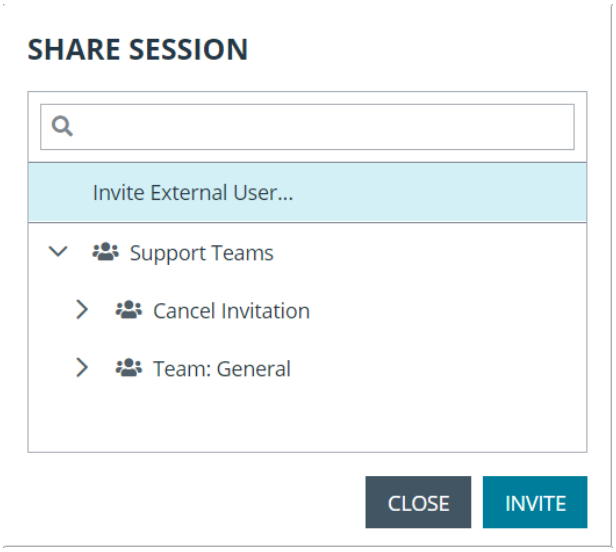
Seul le propriétaire de la session peut envoyer des invitations. Les invitations n'expirent pas tant que vous restez propriétaire de la session. Un utilisateur ne peut pas disposer de plusieurs invitations actives pour rejoindre une même session. L'invitation disparaîtra si :

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

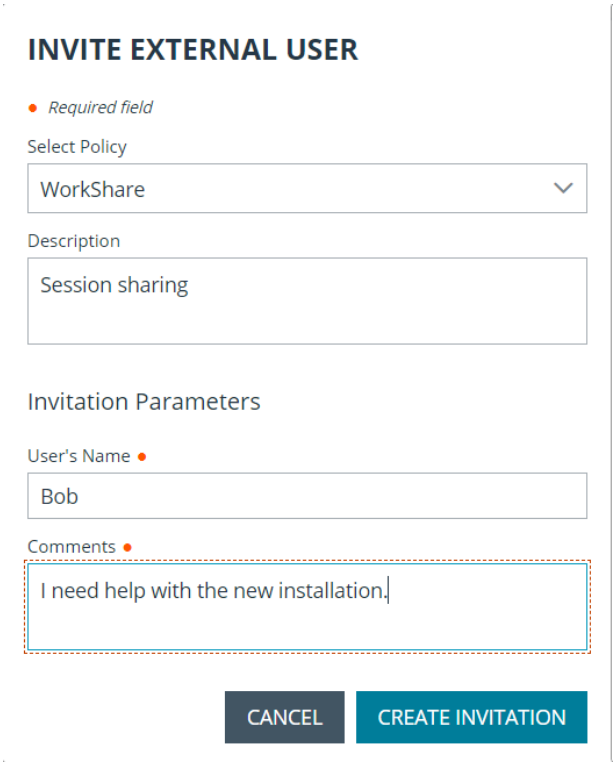
Inviter des utilisateurs externes

Vous pouvez inviter un utilisateur externe ou un fournisseur à participer à une session d'accès. Pour partager une session, suivez les étapes décrites ci-dessous :

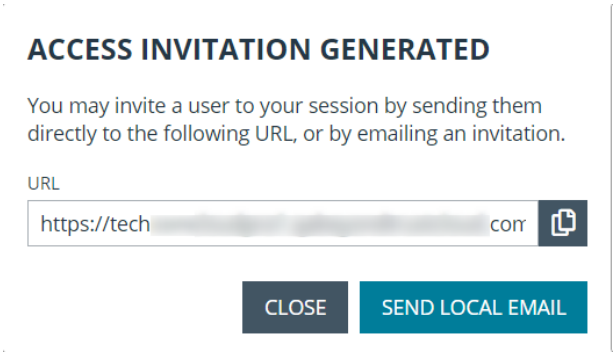
1. Cliquez sur l'icône **Inviter d'autres utilisateurs à rejoindre la session**.
2. Sélectionnez **Inviter un utilisateur externe...**.



1. Sélectionnez une règle, le cas échéant, et saisissez une brève description du type d'invitation.
2. Dans la zone **Paramètres d'invitation**, saisissez le nom de la personne invitée, ainsi que quelques commentaires pour accompagner l'invitation.
3. Cliquez sur **Créer invitation**.



Vous pouvez maintenant inviter un utilisateur externe soit en cliquant sur l'icône **Copier dans le Presse-papiers** et en fournissant à l'utilisateur le lien vers l'URL de la session, soit en envoyant une invitation par e-mail.



Suppression d'un membre d'une session de la console d'accès Privileged Web

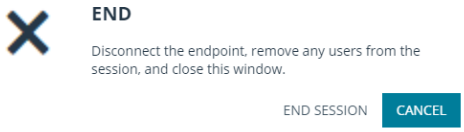
Lorsque c'est nécessaire, vous pouvez supprimer un autre utilisateur d'une session d'accès partagée. Pour supprimer un utilisateur, cliquez sur l'icône **Supprimer membre**.

Dans le menu, sélectionnez le participant que vous souhaitez supprimer. Cliquez sur **Supprimer membre**.

Remarque : *vous devez être le propriétaire de la session pour supprimer un autre membre.*

Fermeture de la session de console d'accès Privileged Web

1. Pour quitter une session d'accès, cliquez sur l'icône **X** en haut à droite de l'écran. Si vous êtes le propriétaire de la session, notez que l'action **Mettre fin à la session** fermera la page de session dans votre access console et retirera tous les membres additionnels qui partageaient la session.

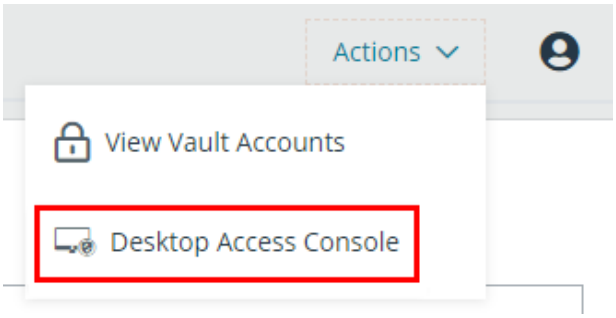


2. Vous recevrez ensuite une invite vous demandant si vous souhaitez mettre fin à la session.
3. Si vous cliquez sur **OK**, la session prendra fin, et vous serez renvoyé vers la liste de **Tous les éléments de Jump**.

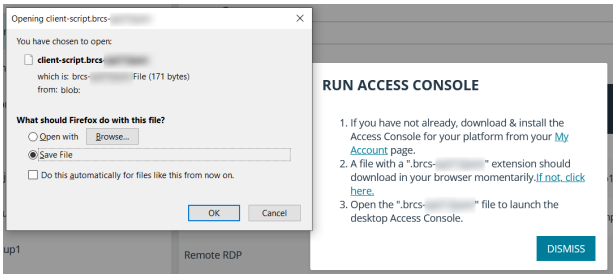
Téléchargement du bureau natif depuis la console d'accès Privileged Web

Lorsque vous travaillez dans la privileged web access console, vous pouvez à tout moment choisir de télécharger la access console native de bureau sur votre ordinateur.

1. Pour télécharger la access console native de bureau depuis la privileged web access console, sélectionnez **Access Console** de **bureau** situé sous le menu **Actif** en haut à droite de l'écran.



2. Lorsque l'installeur s'affiche, suivez les instructions pour installer le logiciel.



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