BOMGAR™

Privileged Access
Privileged Web

TC :4/26/2018

Table des matières

Guide de la console d'accès Privileged Web **3**

Exigences de la console d'accès Privileged Web **4**

Lancement de la console d'accès Privileged Web à travers /login **5**

Utilisation d'éléments de Jump pour accéder à des points de terminaison dans la console d'accès Privileged Web **7**

Connexion aux points de terminaison en utilisant l'injection d'informations d'authentification **10**

Configuration requise 10

Authentification depuis l'API de script client **15**

Retour à une session active dans la console d'accès Privileged Web **16**

Recherche de points de terminaison 16

Contrôler le point de terminaison distant grâce au partage d'écran en utilisant Privileged Web **18**

Ouvrir l'interpréteur de commandes sur le point de terminaison distant en utilisant la console Privileged Web **20**

Transfert de fichiers vers et depuis le point de terminaison distant **22**

Partage d'une session avec d'autres utilisateurs en utilisant la console d'accès Privileged Web **24**

Inviter un utilisateur externe à rejoindre une session Privileged Web **26**

Suppression d'un membre d'une session de la console d'accès Privileged Web **27**

Fermeture de la session de console d'accès Privileged Web **28**

Téléchargement du bureau natif depuis la console d'accès Privileged Web **29**

Guide de la console d'accès Privileged Web

Avec la console d'accès Privileged Web Bomgar, 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 console d'accès basée sur le Web. 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 console d'accès Privileged Web et de la façon dont cette console d'accès basée sur le Web 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 du serveur Bomgar, qui sont expliquées dans le Guide d'installation matérielle du serveur Bomgar. Si vous avez besoin d'aide, veuillez contacter l'assistance technique de Bomgar : help.bomgar.com.*

Exigences de la console d'accès Privileged Web

Pour exécuter la console d'accès Privileged Web sur votre système, votre serveur Bomgar doit utiliser la version logicielle 15.3 ou supérieure. La console d'accès Privileged Web est prise en charge sur les plate-formes et navigateurs suivants :

Plates-formes

- Windows
- Macintosh
- Linux

Navigateurs

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

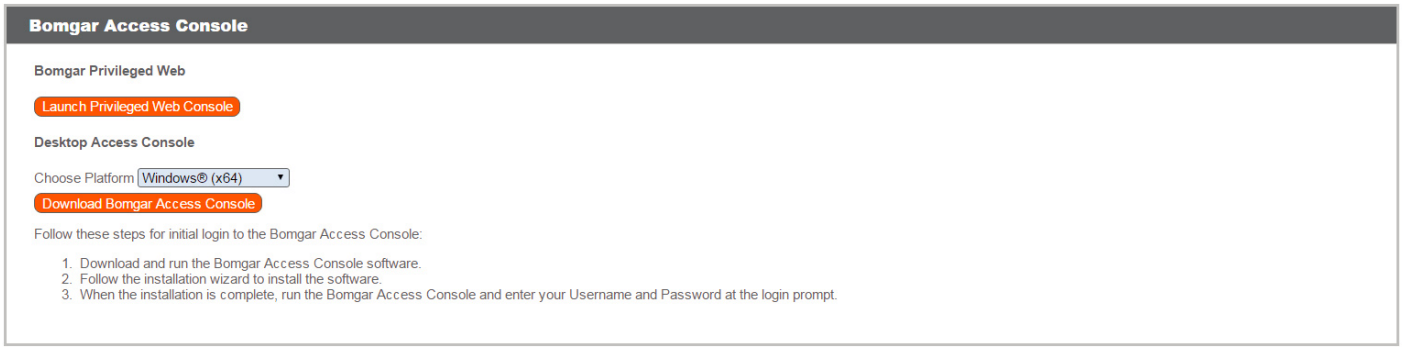
IMPORTANT !

Votre serveur Bomgar doit être équipé d'un certificat SSL valide signé par une autorité de certificat. Une fois que vous avez appliqué un certificat SSL signé par une autorité de certification à votre serveur Bomgar, contactez l'assistance technique de Bomgar. Votre technicien service client créera une nouvelle version logicielle s'intégrant à votre certificat SSL. Avec cette version mise à jour installée sur votre serveur, vous pouvez exécuter la console d'accès Bomgar sur votre appareil pour accéder à vos points de terminaison depuis pratiquement n'importe où.

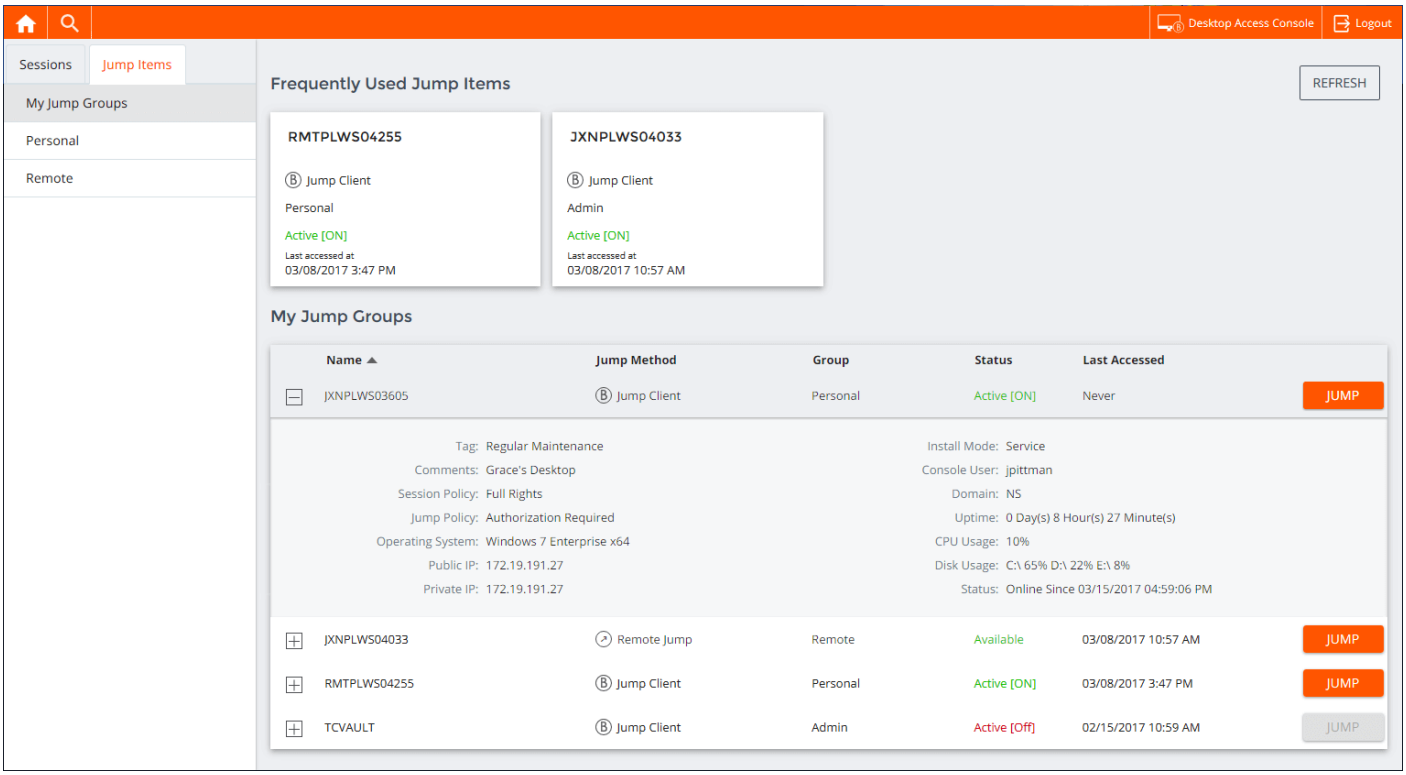
Lancement de la console d'accès Privileged Web à travers /login

La console d'accès Privileged Web vous permet d'utiliser une console d'accès basée sur le Web pour accéder de façon sécurisée à vos points de terminaison en vous y connectant à distance par le biais du serveur Bomgar. Pour commencer à utiliser la console d'accès Privileged Web pour accéder à des points de terminaison, suivez les étapes décrites ci-dessous :

Remarque : *par défaut, le bouton* ***Lancer la console d'accès de Privileged Web*** *n'est pas disponible. Vous devez aller dans* ***Gestion > Sécurité*** *et cocher* ***Permettre à la console d'accès Bomgar et à la console d'accès Privileged Web Bomgar de se connecter*** *pour activer la console.*



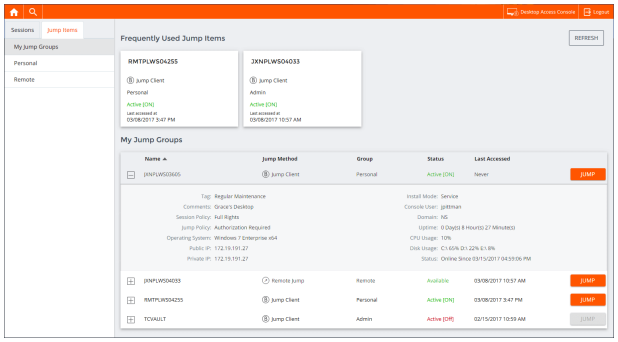
1. Dans la barre d'adresse de votre navigateur, saisissez le nom d'hôte de votre site Bomgar suivi de /login (exemple : access.example.com/login).
2. Saisissez le nom d'utilisateur et le mot de passe associés à votre compte utilisateur Bomgar.
3. Cliquez sur **Connexion**.
4. Une fois que vous êtes connecté à l'interface d'administration /login, cliquez sur l'onglet **Mon compte**.
5. Cliquez sur le bouton **Lancement de la console d'accès Privileged Web** situé dans la section **Console d'accès Bomgar**.
6. La console d'accès de Privileged Web s'ouvrira dans un nouvel onglet, et vous pourrez commencer à accéder à des points de terminaison.



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

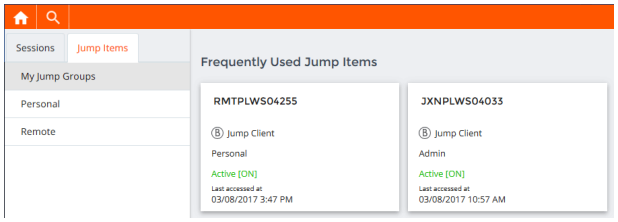
Utilisation d'éléments de Jump pour accéder à des points de terminaison dans la console d'accès Privileged Web

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 :

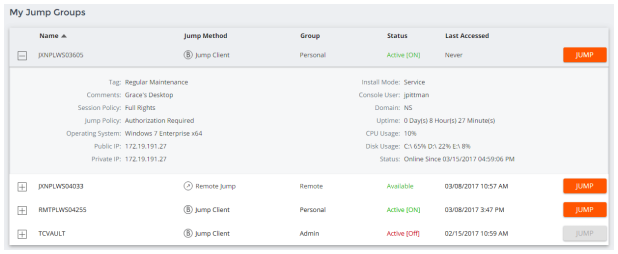
- Trouvez et sélectionnez un point de terminaison dans la liste **Mes groupes de Jump**.
- Choisissez un groupe de Jump et sélectionnez un point de terminaison dans la liste des points de terminaison de ce groupe.
- Sélectionnez une session dans la liste des **éléments de Jump fréquemment utilisés**.

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****.*

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

1. Sélectionnez un emplacement puis cliquez sur le bouton **Tout 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.

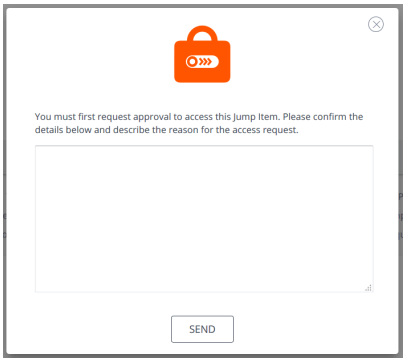


3. Cliquez sur le bouton **JUMP** pour lancer une session avec le point de terminaison.

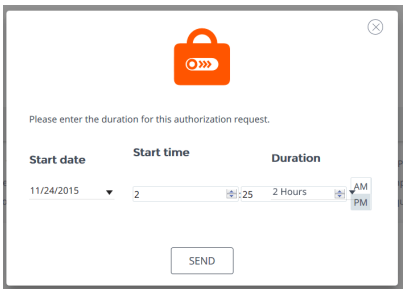
Autorisation pour utilisateur final et tierce partie

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.bomgar.com/docs/privileged-access/getting-started/admin/jump-policies.htm.

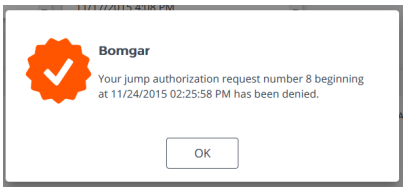
1. Après avoir cliqué sur le bouton **JUMP** et sollicité l'accès, une invite vous demande de justifier votre demande d'accès au système.



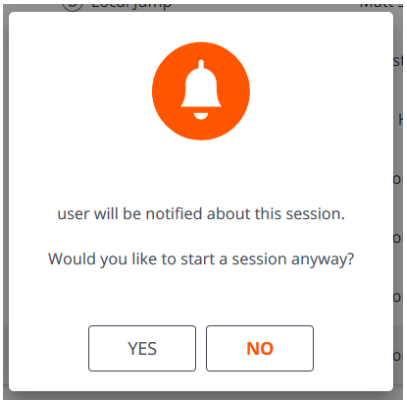
2. Vous devez ensuite indiquer à quel moment et pour combien de temps vous accéderez au système.
3. Une fois la requête soumise, la tierce partie ou la personne responsable de l'approbation des demandes d'accès est prévenue par e-mail et peut accepter ou refuser la demande. Bien que d'autres approbateurs 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.



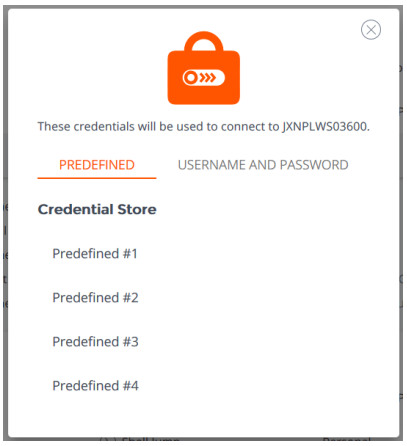
4. Après qu'une autorisation a été établie, une notification d'autorisation apparaît dans les informations de l'élément de Jump, affichant « approuvée » ou « refusée ». Si l'accès est autorisé, vous pouvez appuyer sur le bouton Jump pour accéder au système.



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.



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.bomgar.com/docs/privileged-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 console d'accès Privileged Web, vous pouvez utiliser les informations d'authentification d'un magasin d'informations d'authentification pour vous connecter au point de terminaison ou pour lancer des applications en tant qu'admin.

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

Remarque : *vous n'avez pas de banque de mots de passe ? Vous pouvez en apprendre davantage sur* ***Bomgar Vault*** *à l'adresse https://www.bomgar.com/vault.*

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 Bomgar (GIAPT). Le GIAPT Bomgar vous permet de configurer rapidement votre connexion à un magasin d'informations d'authentification, comme une banque de mots de passe.

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

Configuration requise

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

Remarque : *lors de l'installation du gestionnaire d'informations d'authentification de point de terminaison pour être utilisé avec Bomgar Vault, nous recommandons de l'installer sur une machine ayant une adresse IP fixe, pour éviter de possibles problèmes avec la liste blanche d'IP de Vault pour l'API.*

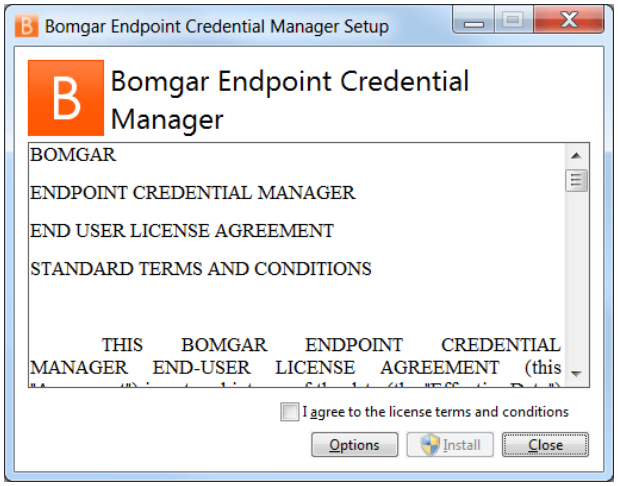
1. Pour commencer, téléchargez le gestionnaire d'informations d'authentification de point de terminaison (GIAPT) Bomgar auprès de l'assistance technique Bomgar à l'adresse ssc.bomgar.com. Lancez l'assistant de configuration du gestionnaire d'informations d'authentification de point de terminaison Bomgar.

2. Acceptez les conditions générales du CLUF. Cochez la case si vous acceptez, puis cliquez sur **Installer**.

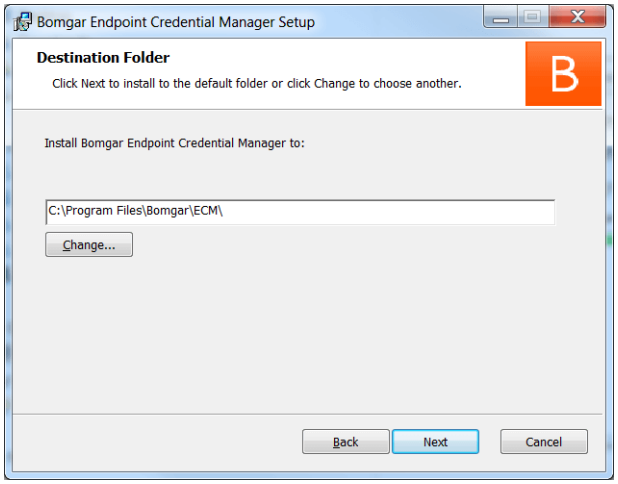
   Remarque : *vous ne pourrez pas poursuivre l'installation si vous n'acceptez pas le CLUF.*

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

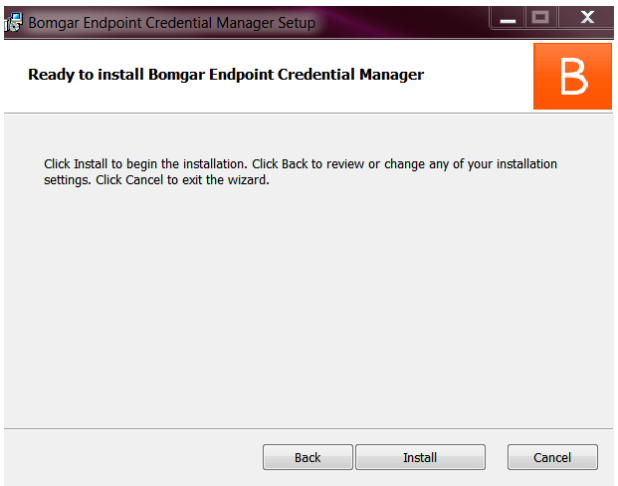
3. Cliquez sur **Installer**.



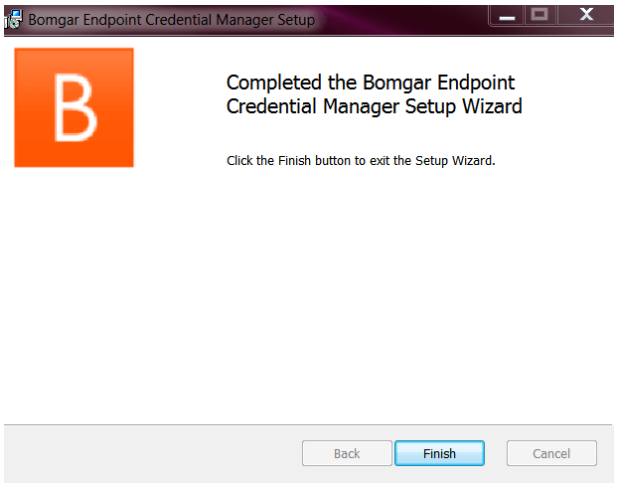
4. Choisissez un emplacement pour le gestionnaire d'informations d'authentification, puis cliquez sur **Suivant**.
5. Sur l'écran suivant, vous pouvez lancer l'installation ou vérifier les étapes précédentes.



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



7. L'installation prend quelques instants. Sur cet écran, cliquez sur **Terminé**.



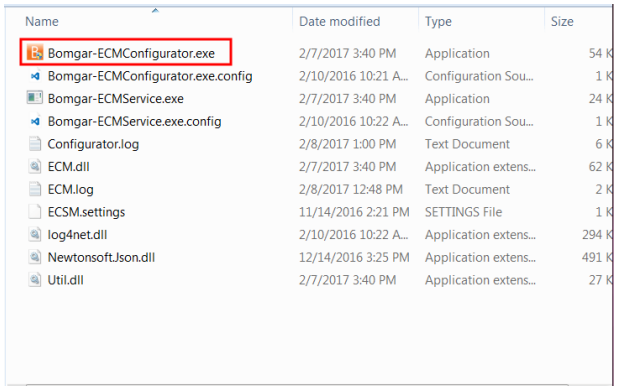
Remarque : *pour optimiser le temps de disponibilité, les administrateurs peuvent installer jusqu'à 5 GIAPT sur plusieurs machines Windows pour communiquer avec le même site sur le serveur Bomgar. Une liste des GIAPT connectés au site du serveur est disponible sur* ***/login > État > Information > Clients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

Remarque : *lorsque plusieurs GIAPT sont connectés au site Bomgar, le serveur Bomgar achemine les demandes vers le GIAPT ayant été le plus longtemps connecté au serveur.*

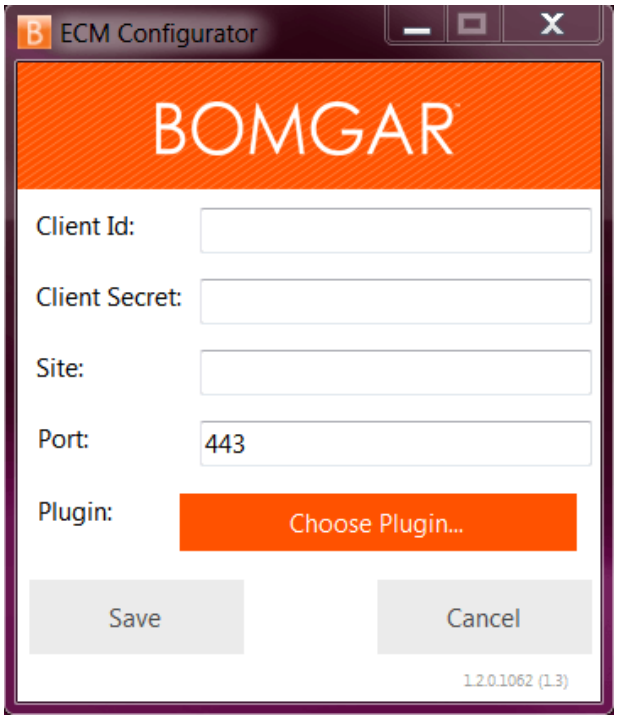
Configurer une connexion à votre magasin d'informations d'authentification

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

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



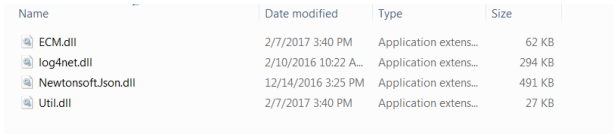
3. Lorsque le configurateur GIAPT s'ouvre, remplissez les champs. Tous les champs sont obligatoires.



Saisissez les valeurs suivantes :

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

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



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

IMPORTANT

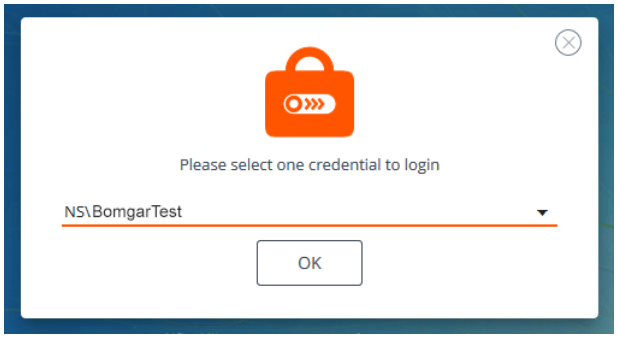
Pour appliquer de nouveaux paramètres à la configuration, redémarrez le service GIAPT.

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 console d'accès Privileged Web peut commencer à utiliser des informations d'authentification dans le magasin d'informations d'authentification pour se connecter à des points de terminaison.

1. Connectez-vous à la console d'accès Privileged Web.
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 GIAPT.

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



Authentification depuis l'API de script client

Cette fonction permet aux utilisateurs de se connecter à la console d'accès Privileged Web et d'effectuer un Jump vers un point de terminaison en utilisant l'API de script client PA (https://www.bomgar.com/docs/privileged-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 serveur.

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 console d'accès du bureau lorsqu'on accède à l'URL de l'API du script client avec **type=web_console**, l'utilisateur sera alors connecté à la console d'accès Privileged Web et déconnecté de la console d'accès du 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 console d'accès Privileged Web et que l'API appelle **type=rep**, l'utilisateur sera connecté à la console d'accès du bureau et déconnecté de la console d'accès Privileged Web.

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 console d'accès Privileged Web, la demande ci-dessus exécute la commande dans l'onglet du navigateur qui exécute la console d'accès Privileged Web. 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 console d'accès Privileged Web, 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 alors redirigé vers la console d'accès Privileged Web, 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 console d'accès de Privileged Web affiche un message d'erreur.

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 plusieurs sessions d'accès en cours, vous avez la possibilité de revenir à n'importe quelle autre session à tout moment. Pour revenir à un point de terminaison auquel vous avez déjà accédé dans une autre session, suivez les étapes décrites ci-dessous :

1. Cliquez sur le menu déroulant **Sessions**.

> ***Remarque :*** *le nombre qui apparaît dans le menu déroulant* ***Sessions*** *indique le nombre de sessions actives auxquelles vous accédez simultanément.*

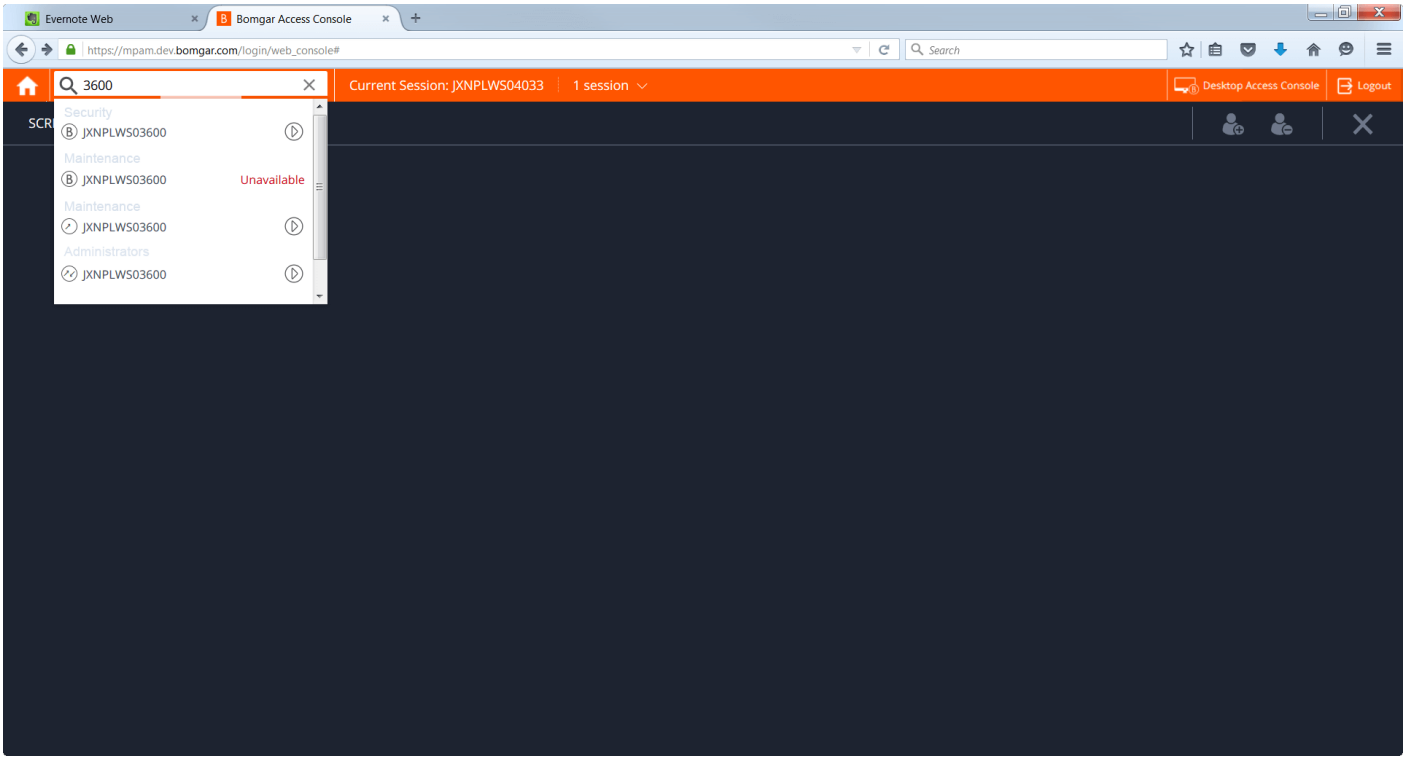
2. Sélectionnez un point de terminaison dans la liste.

3. Vous serez ensuite emmené dans la session de ce point de terminaison spécifique.

Recherche de points de terminaison

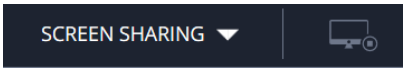
Lorsque vous utilisez la console d'accès Privileged Web, vous pouvez rechercher des points de terminaison spécifiques pendant que vous êtes dans une session d'accès. Dans les résultats de la recherche, vous pouvez aussi cliquer sur le bouton **Démarrer** pour commencer une session avec ce point de terminaison.

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 **Démarrer** pour lancer une session.



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

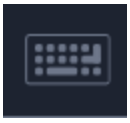
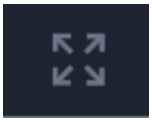
Pour voir et contrôler des systèmes distants, utilisez l'action de partage d'écran pendant une session d'accès.



1. Dans la fenêtre de session, cliquez sur le menu déroulant **Partage d'écran** et choisissez l'option **Partage d'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

	Arrêtez 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 Bomgar a désactivé l'affichage du client final. L'utilisateur final peut reprendre le contrôle à tout moment en appuyant sur **Ctrl+Alt+Suppr**. L’interaction restreinte avec le client n’est disponible que lors d’une assistance technique à un ordinateur Windows. Dans Windows Vista et les versions supérieures, le client de point de terminaison doit être accru. Sur Windows 8 et les versions supérieures, 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.
	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 Bomgar. Une fois qu'un accord de services est en place, vous pouvez télécharger le middleware requis auprès du centre de self-service de Bomgar.

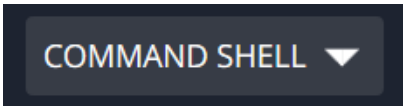
	Basculez le clavier virtuel.
	Basculez le presse-papiers.
	Sélectionnez un autre écran distant à afficher. Notez que le moniteur principal est désigné par la lettre **P**.
	Visualisez l'écran distant à sa taille réelle ou mis à l'échelle.
	Définissez le mode d'optimisation de la couleur d'affichage de l'écran distant. Si vous comptez principalement partager de la vidéo, sélectionnez **Vidéo optimisée** ; sinon, choisissez entre **Noir et blanc** (utilise moins de bande passante), **Quelques couleurs**, **Davantage de couleurs** ou **Toutes les couleurs** (utilise plus de bande passante). Les modes Vidéo optimisée et Toutes les couleurs vous permettent de voir votre fond d'écran.
	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**.

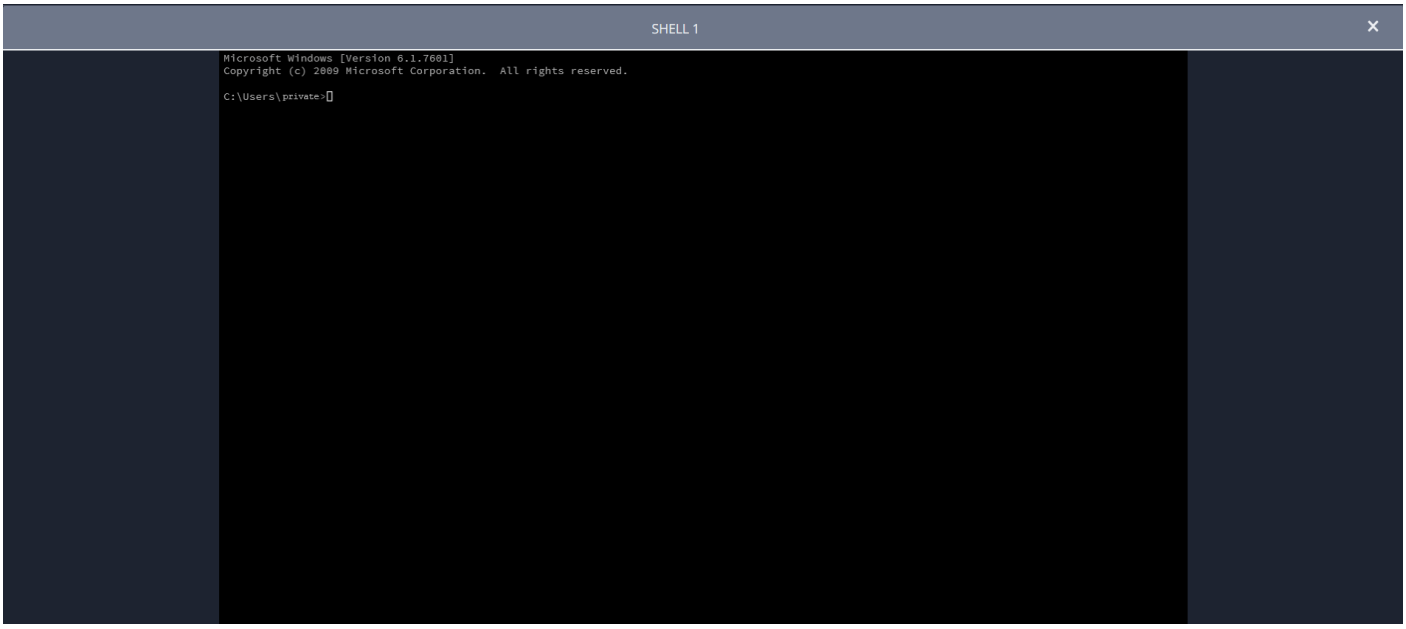
Ouvrir l’interpréteur de commandes sur le point de terminaison distant en utilisant la console Privileged Web

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.

1. Pour accéder à l'**interpréteur de commandes** pendant une session d'accès, cliquez sur le menu déroulant **Partage d'écran** dans le coin supérieur de l'écran.
2. Sélectionnez l'option **Interpréteur de commandes**.
3. Après avoir choisi l'option **Interpréteur de commandes**, les options et l'invite de commandes apparaîtront.





Outils d'interpréteur de commandes

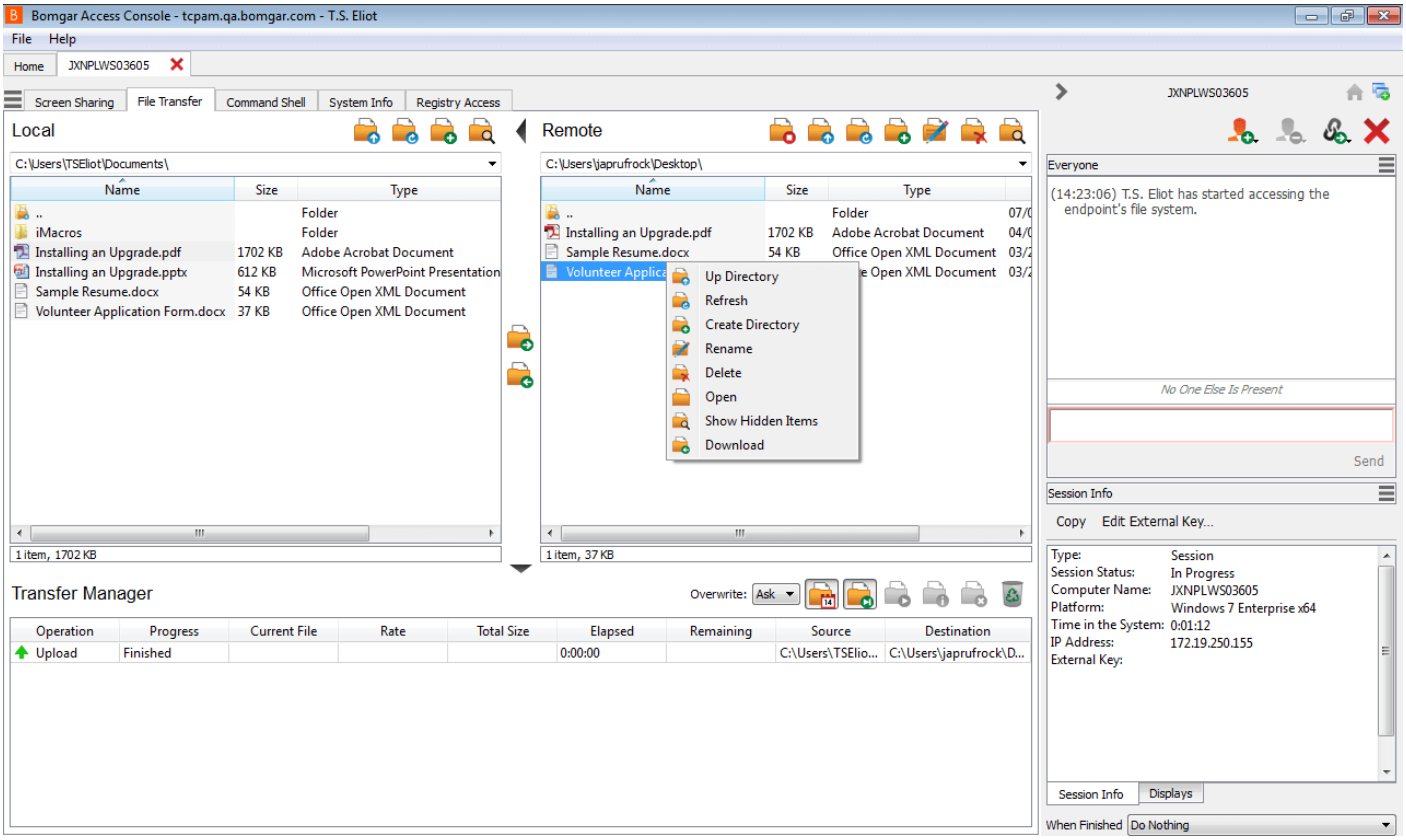
	Mettre fin à l'accès à l'invite de commande une fois que celui-ci n'est plus nécessaire.
	Ouvrir un nouvel interpréteur pour exécuter plusieurs instances d'une invite de commande ou fermer des interpréteurs individuels sans abandonner l'accès à l'invite de commande. Les interpréteurs de commandes sont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

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.

Partage d'une session avec d'autres utilisateurs en utilisant la console d'accès Privileged Web

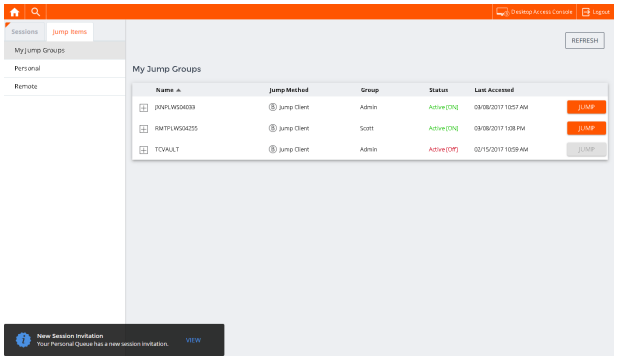
Pendant une session, vous pouvez demander à ce qu'un membre d'équipe participe à une session d'accès. Pour partager une session, suivez les étapes décrites ci-dessous.

1. Cliquez sur l'icône **Partager la session**.

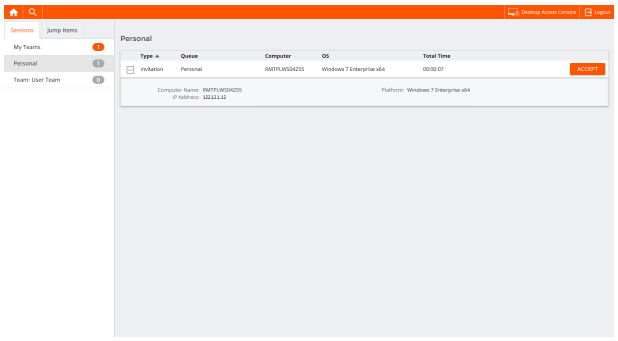
2. Sélectionnez l'équipe dont l'utilisateur fait partie dans le menu.

3. Dans le listing de l'équipe, choisissez l'utilisateur avec lequel vous souhaitez partager la session.

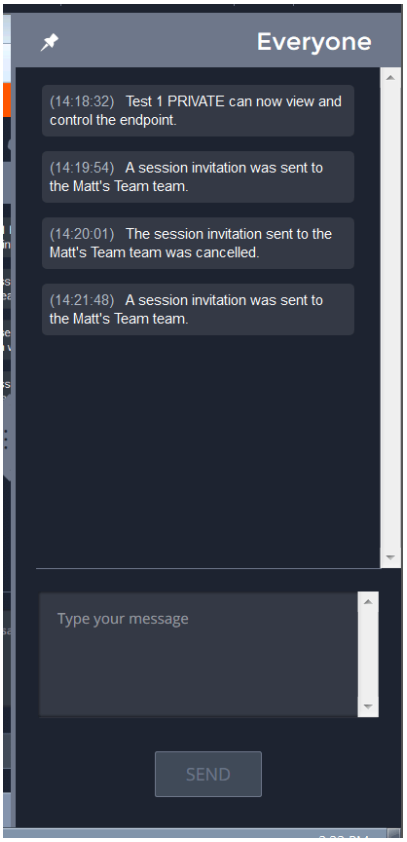
4. L'utilisateur invité verra une notification en bas à gauche de l'écran, lui indiquant qu'il a reçu une invitation pour accéder à une nouvelle session.



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 console d'accès, ou si leur mode Disponibilité étendue est activé.

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

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

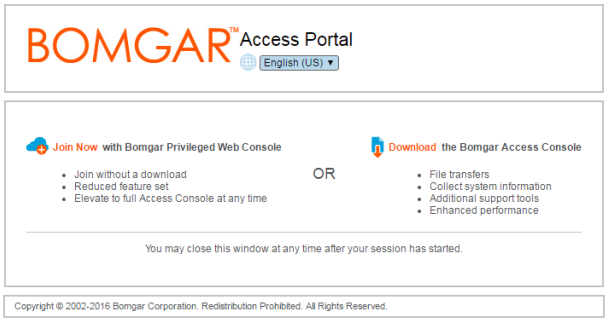
- L'utilisateur qui invite annule l'invitation.
- L'utilisateur qui invite quitte la session.
- La session se termine.
- L'utilisateur invité accepte l'invitation.

Inviter un utilisateur externe à rejoindre une session Privileged Web

Dans une session, vous pouvez demander à un utilisateur externe de participer à une session de manière ponctuelle. Pour inviter un utilisateur externe, suivez les étapes décrites ci-dessous.

1. Lorsque vous êtes dans une session, cliquez sur le bouton **Partager la session**.
2. Dans le menu, sélectionnez **Inviter un technicien d'assistance externe**.

3. Sélectionnez une règle de sécurité. Ces règles sont créées dans l'interface d'administration /login et déterminent le niveau d'autorisation dont bénéficie l'utilisateur externe. Lorsque vous sélectionnez une règle, la description complète s'affiche en dessous.
4. Saisissez le nom de l'utilisateur invité. Ce nom apparaît dans la fenêtre de messagerie instantanée et dans les rapports.
5. Saisissez ensuite des commentaires sur le motif de l'invitation de cet utilisateur.
6. Cliquez sur **Envoyer**. Une nouvelle boîte de dialogue contenant l'URL d'invitation s'affiche.
7. 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 et l'envoyer à l'utilisateur.
8. Lorsque l'utilisateur externe clique sur l'URL d'invitation d'accès, il a le choix de rejoindre la session en utilisant la console d'accès Privileged Web ou en téléchargeant et installant la console d'accès de bureau.
9. Une fois qu'il a choisi la console d'accès Privileged Web ou installé la console d'accès de bureau, il peut rejoindre la session.



Remarque : *voici quelques conseils pour utiliser la fonction d'invitation d'utilisateur externe :*

- *L'utilisateur externe n'a accès qu'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.*
- *L'utilisateur externe peut accroître vers la console d'accès de bureau. Lorsque l'utilisateur clique sur le bouton **Accroître**, un nouvel onglet de navigateur s'ouvre, redirigeant l'utilisateur vers l'URL d'invitation d'accès pour la console d'accès de bureau.*

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

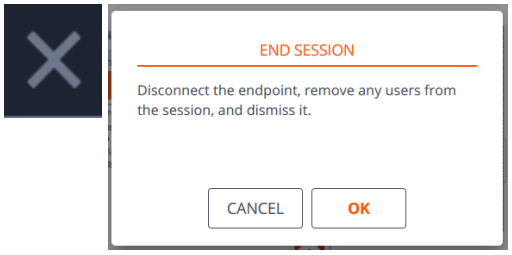
Lorsque c'est nécessaire, vous pouvez supprimer un autre utilisateur d'une session d'accès partagée. Pour supprimer un utilisateur, cliquez sur l'icône **Supprimer membre**.

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 console d'accès 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 console d'accès Privileged Web, vous pouvez à tout moment choisir de télécharger la console d'accès native de bureau sur votre ordinateur.

1. Pour télécharger la console d'accès native de bureau depuis la console d'accès Privileged Web, cliquez sur le bouton **Lancer la console d'accès native de bureau** situé 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.*