

Remote Support 22.1 Guide du technicien d'assistance



Table of Contents

Console du technicien d'assistance BeyondTrust	7
Installation de la console du technicien d'assistance	8
Connexion à la console du technicien d'assistance	9
Interface utilisateur de la console du technicien d'assistance	12
Modification des paramètres et préférences de la console du technicien d'assistance	. 14
Modification des paramètres	14
Prise en charge des utilisateurs	18
Options de démarrage de session d'assistance technique	18
Sessions initiées par le client	18
E-mail	18
URL	18
Portail Web BeyondTrust	19
bouton d'assistance technique	19
Accroissement des droits	20
Session lancée par un technicien d'assistance	20
Jump Client BeyondTrust (agent d'exécution préinstallé)	20
Jump vers (ad hoc)	21
Génération d'une clé de session en vue de démarrer une session d'assistance technique	22
Consultation des sessions d'assistance technique en attente	
Files d'attente	
Acceptation d'une session pour démarrer l'assistance technique	
Règles d'attribution de session	
Génération d'une clé d'accès au profil Apple iOS	
Interface de Jump	
Utiliser les éléments de Jump pour apporter une assistance technique à des systèmes	20
distants	28
Jump vers un élément de Jump	28
Copier des éléments de Jump	29
Accès autonome à des ordinateurs distants à l'aide de Jump Clients	30
Organiser les Jump Clients	30
Trouver un Jump Client	30



	Panneau de détails sur le Jump Client	. 30
	Wake-On-Lan (WOL)	. 30
	Copier des éléments de Jump	. 31
	Propriétés des Jump Clients	32
	Utiliser des Jump Clients pour un accès autonome à des appareils Android	34
	Attachez un Jump Client Android depuis la Console du technicien d'assistance	35
	Envoyer un lien par e-mail depuis l'interface /login pour installer un Jump Client Android	. 35
Cré	er et utiliser des raccourcis de Jump local	. 37
Cré	er et utiliser des éléments de Jump locaux ou distants	. 39
	Créer un raccourci de Jump distant	39
	Créer un raccourci de Jump local	40
	Utiliser un raccourci de Jump distant ou un raccourci de Jump local	41
Utili	iser un RDP local pour accéder à des systèmes Windows et Linux	. 43
	Assistance technique multimoniteur	44
Cré	er et utiliser des raccourcis RDP	. 45
	Créer un raccourci de RDP local	45
	Créer un raccourci de RDP distant	46
	Utiliser un raccourci de RDP	47
	Assistance technique multimoniteur	48
VNC	C vers un système distant	. 49
Cré	er et utiliser des raccourcis VNC	. 50
	Créer un raccourci VNC local	. 50
	Créer un raccourci VNC distant	51
	Utiliser un raccourci VNC	. 52
Réa	lisation d'un Shell Jump vers un périphérique réseau distant	. 53
Cré	er et utiliser des raccourcis de Shell Jump	55
	Créer un raccourci de Shell Jump	. 55
	Utiliser un raccourci de Shell Jump	. 56
Ass	sistance technique de systèmes Windows avec Intel® vPro	57
С	Outils de session vPro	. 59
Cré	er et utiliser des raccourcis de Jump Intel vPro	. 61
	Créer un raccourci Intel® vPro	61
	Utiliser un raccourci Intel® vPro	. 61



Boîte à outils	. 63
Vue d'ensemble des sessions d'assistance technique et outils	. 63
Outils de session	. 64
Connexion aux systèmes en utilisant l'injection d'informations d'authentification depuis la Console du technicien d'assistance	. 67
Installer et configurer le gestionnaire d'informations d'authentification de point de terminaison	67
Configuration requise	67
Configurer une connexion à votre magasin d'informations d'authentification	69
Utilisez l'injection d'informations d'authentification pour accéder à des systèmes distants	71
Faites votre choix parmi les informations d'authentification préférées pour injection	72
Extraire et injecter des informations d'authentification Vault	.72
Messagerie instantanée avec un utilisateur lors d'une session	. 74
Accroître le client	77
Accroissement des droits	. 78
Partage d'écran avec l'utilisateur distant à des fins de consultation et de contrôle	79
Options de partage d'écran	. 79
Outils de partage d'écran	81
Utilisation d'annotations sur l'écran distant.	. 83
Activation des annotations	83
Affichage de moniteurs multiples sur un système distant	. 85
Utilisation de l'icône Affichage	. 85
Assistance technique multimoniteur lors d'une session RDP	. 86
Utilisation de l'onglet Écrans	. 86
Transfert de fichiers vers et depuis un système distant	. 88
Outils de transfert de fichiers	90
Accès à l'interpréteur de commandes distant	91
Outils d'interpréteur de commandes	. 92
Consulter des informations relatives à un système distant	93
Outils d'informations système	. 94
Accès à l'éditeur de registre distant	. 95
Montrer mon écran à l'utilisateur	97
Outils de la fonction Montrer mon écran	98
Réaliser une présentation pour des participants distants	99



bancaire nationale ou fédérale.

Outils de présentation	. 103
Annotations	.104
Collaboration	.105
Messagerie instantanée avec d'autres techniciens d'assistance	105
Partager votre écran avec un autre technicien d'assistance	.106
Outils de partage d'écran	. 107
Utilisateur partageant	. 107
Utilisateur en visualisation	107
Acceptation d'une demande d'accès à des fins d'accroissement des droits	.108
Partage d'une session avec d'autres techniciens d'assistance	.109
Accessibilité hors connexion grâce à la fonction de disponibilité étendue	. 110
Invitation et notification par e-mail	.111
Invitation d'un technicien d'assistance externe à rejoindre une session	. 112
Gestion	114
Gérer un bouton d'assistance technique .	.114
Surveillance des membres d'une équipe dans le tableau de bord	. 117
Enquête de satisfaction du technicien d'assistance	118
Ce que votre client voit : Le client d'utilisateur BeyondTrust	119
Site public : demande d'assistance technique	120
Client d'utilisateur : interface de session d'assistance technique	122
Partage d'application : restriction des éléments visibles par le technicien d'assistance	.124
Interaction utilisateur restreinte : écran de confidentialité et désactivation de l'entrée de l'utilisateur distant	. 126
Informations d'authentification pour connexion automatique : redémarrage et reconnexion	127
Montrer mon écran : inversion du partage d'écran	128
bouton d'assistance technique : demande d'assistance technique rapide	129
Enquête de satisfaction de l'utilisateur : soumission de commentaires	. 130
Client de participant à une présentation : rejoindre une présentation	131
Ports et pare-feu	. 133
Régler les problèmes de connexion à la console du technicien d'assistance BeyondTrust	134
Avis de non-responsabilité, limitations associées à la licence et assistance technique	
Avis de non-responsabilité	. 135
Limitations associées à la licence	. 135



Assistance technique	135



Console du technicien d'assistance BeyondTrust

Ce guide est destiné à vous aider à installer la console du technicien d'assistance BeyondTrust sur votre ordinateur et à en comprendre les différentes fonctions. BeyondTrust vous permet d'apporter une assistance technique à distance à vos clients en vous y connectant par le biais du BeyondTrust Appliance B Series.

Installation de la console du technicien d'assistance

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

Sur la page **Mon compte**, téléchargez et installez la console du technicien d'assistance BeyondTrust. L'option s'adaptera par défaut à l'installeur de votre système d'exploitation.



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

Lorsque l'assistant d'installation apparaît, suivez les instructions pour installer le logiciel. Une fois la console du technicien d'assistance installée, vous pouvez choisir **Exécuter la Console du technicien d'assistance maintenant** et **Exécuter au démarrage**, puis cliquer sur **Terminer**.



Remarque : si vous choisissez Exécuter la Console du technicien d'assistance maintenant durant l'installation, une invite de connexion s'affichera sur votre écran.



Connexion à la console du technicien d'assistance

Une fois la console du technicien d'assistance BeyondTrust installée, démarrez-la à partir de son répertoire, tel que défini au cours de l'installation.



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

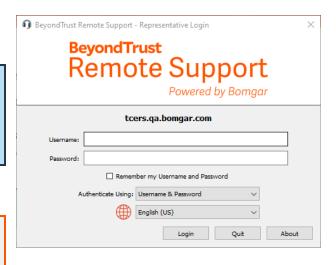
Si l'Accord de connexion a été activé, vous devez cliquer sur **Accepter** pour poursuivre.

i

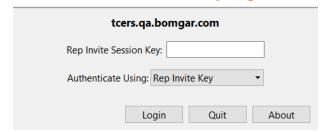
Pour en savoir plus sur la configuration, l'activation ou la désactivation de cette fonction, consultez <u>Configuration du site</u>: <u>Configuration des ports HTTP et activation de l'accord de connexion</u> à l'adresse <u>https://www.beyondtrust.com/docs/remote-support/getting-</u>

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

started/admin/site-configuration.htm.







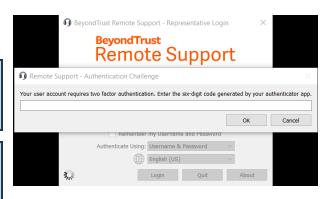
Si l'authentification à deux facteurs est activée sur votre compte, saisissez le code de l'application d'authentification.



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



Remarque: Les utilisateurs qui s'authentifiaient à l'aide de codes reçus par e-mail passeront automatiquement à l'authentification à deux facteurs (2FA). Ils ont toutefois la possibilité de continuer à utiliser des codes e-mail jusqu'à ce qu'ils enregistrent une application. Après une première utilisation de 2FA, l'option du code e-mail n'est plus disponible.





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

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

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



Si plusieurs langues sont activées pour votre site, sélectionnez celle que vous souhaitez utiliser dans la liste déroulante située en regard de l'icône de globe. Une fois connecté, pour modifier la langue sélectionnée, vous devez revenir en arrière et choisir une autre langue.

Lorsque vous êtes connecté, la console s'ouvrira, et une icône BeyondTrust apparaîtra dans la barre d'état système de votre ordinateur. Si vous fermez la console, mais restez connecté, vous pouvez rouvrir la fenêtre en double-cliquant sur l'icône dans la barre d'état système ou en cliquant avec le bouton droit sur l'icône et en sélectionnant **Montrer la fenêtre**.



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

Si vous perdez votre connexion, la console du technicien d'assistance tente de se reconnecter pendant 60 secondes. Si votre connexion est rétablie pendant ce laps de temps, votre console du technicien d'assistance rouvre, et toutes vos sessions ouvertes sont récupérées. Si votre connexion ne peut pas être rétablie pendant cette durée, vos sessions sont gérées selon les règles définies dans /login > Configuration > Options et vous serez invité à réessayer de vous connecter ou à quitter la console.

Si vous êtes connecté à une console du technicien d'assistance à un emplacement et que vous vous connectez ailleurs, vos sessions ouvertes sont maintenues.



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



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

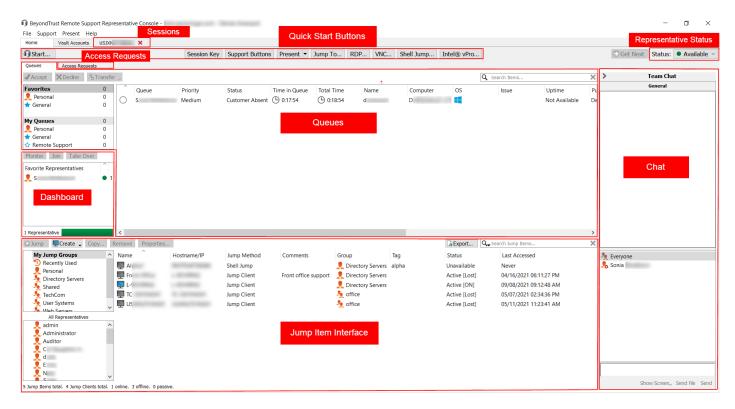




Pour plus d'informations sur les utilisateurs invités, veuillez consulter <u>Invitation d'un technicien d'assistance : Création de profils pour l'invitation de techniciens d'assistance externes à des sessions</u> à l'adresse https://www.beyondtrust.com/docs/remote-support/getting-started/admin/rep-invite.htm.



Interface utilisateur de la console du technicien d'assistance



Sessions: gérez plusieurs sessions distantes à la fois.



Remarque : les onglets de session peuvent être déplacés et réorganisés pour vous aider à organiser et hiérarchiser votre charge de travail. Cliquez et faites simplement glisser un onglet de session vers une nouvelle position. Les onglets de session peuvent également être détachés de la fenêtre principale de la console du technicien d'assistance.

Boutons de démarrage rapide : accédez rapidement aux outils fréquemment utilisés. Vous pouvez activer et désactiver ces boutons de démarrage rapide sous Fichier > Paramètres.

- Démarrage : ouvre une boîte de dialogue contenant un guide de référence rapide pour démarrer une session.
- Clé de session : démarrez des sessions à l'aide de clés de session à usage unique générées de manière aléatoire.
- bouton d'assistance technique s: consultez les détails et statistiques d'utilisation de chaque bouton d'assistance technique déployé.
- **Présentation**: partagez votre écran avec un ou plusieurs participants distants. Lancez une présentation immédiatement ou programmez-la pour une date ultérieure.
- **Jump**: Effectuez un Jump vers un ordinateur sur un réseau distant via un Jumpoint ou sur votre réseau local. La technologie Jump de BeyondTrust permet aux techniciens d'assistance avec privilèges de se connecter à un ordinateur distant sans surveillance pour démarrer une session sans l'aide d'un utilisateur final.
- RDP: démarrez une session de protocole de bureau à distance avec un système Windows distant.
- VNC : démarrez une session VNC avec un système Windows distant.
- Shell Jump: connectez-vous rapidement aux périphériques réseau SSH et Telnet par l'intermédiaire d'un Jumpoint déployé.

TC: 7/18/2022



• Intel® vPro : la technologie de gestion active Intel® permet d'assister les systèmes Intel® vPro Windows totalement fournis sous le niveau du système d'exploitation.

Files d'attente : les files d'attente répertorient les clients qui sont en attente d'assistance technique ou dans une session. Les détails sur le système distant bénéficiant d'une assistance technique apparaissent dans cette section.

Tableau de bord: les utilisateurs privilégiés peuvent voir et surveiller les sessions en cours et les membres de leur équipe de rang inférieur, permettant une supervision administrative pour aider à gérer le personnel. Les indicateurs de statut indiquent si les techniciens d'assistance sont disponibles, inactifs ou occupés, ou encore si la fonction d'attribution automatique est désactivée pour ces techniciens. Une barre, située dans le bas du tableau de bord, indique le pourcentage de techniciens d'assistance par état.

Demandes d'accès: si un technicien d'assistance est le parrain d'un ou plusieurs groupes de parrains d'accès, il verra un onglet Demandes d'accès sur la console du technicien d'assistance. Lorsqu'un technicien d'assistance fait une demande, tous les parrains du groupe de parrains d'accès sélectionné verront une nouvelle demande dans l'onglet Demandes d'accès de la console du technicien d'assistance.

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

État du technicien d'assistance : Si vous n'utilisez pas l'attribution automatique de session, vous pouvez indiquer votre état depuis ce menu déroulant. Vos responsables d'équipe voient votre état sur leur tableau de bord. Si votre administrateur a configuré des états personnalisés, vous pouvez sélectionner n'importe lequel d'entre eux ici si votre état affiche autre chose qu'un état par défaut (Disponible, Occupé ou Absent).

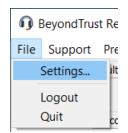
Messagerie instantanée : discutez avec d'autres utilisateurs connectés. Vous pouvez également partager votre écran avec un membre de votre équipe, sans besoin d'être en session.



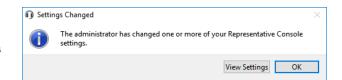
Modification des paramètres et préférences de la console du technicien d'assistance

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

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



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

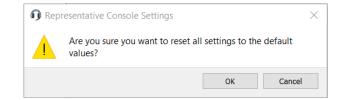


Modification des paramètres



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

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





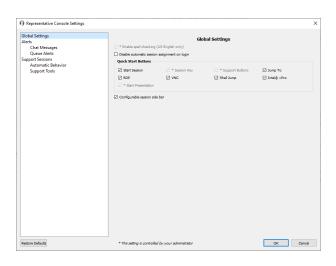
Remarque: si les paramètres par défaut sont imposés par l'administrateur, vous ne pourrez toutefois pas les configurer.



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

Si l'attribution automatique de session est désactivée lors de la connexion, les sessions ne vous sont pas automatiquement attribuées tant que vous n'en n'avez pas décidé autrement.

La sélection de l'option **Démarrer une session** sous **Boutons de démarrage rapide** entraîne l'apparition d'un bouton **Démarrer** en haut de votre console du technicien d'assistance. En cliquant sur ce bouton, vous voyez comment votre utilisateur peut démarrer une session d'assistance technique. Vous pouvez également sélectionner **Clé de session** pour afficher un bouton de génération de clé de session, et sélectionner **bouton d'assistance technique** pour afficher un bouton permettant de lancer l'interface de gestion de bouton d'assistance technique . Sélectionnez



Jump vers, **RDP**, **VNC**, **Shell Jump** et **Intel**® **vPro** pour afficher les boutons permettant de lancer ces connexions Jump respectives. L'option **Démarrer la présentation** vous permet de démarrer simplement une nouvelle présentation.

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

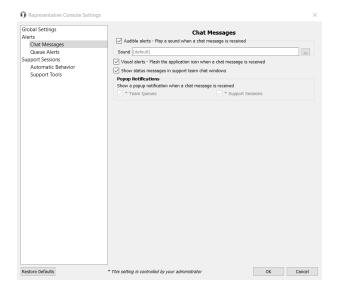
Si la traduction de la messagerie instantanée en temps réel est activée pour votre site, choisissez la langue de chat désirée dans le menu déroulant. Cela permet à la console du technicien d'assistance de savoir dans quelle langue vous écrivez afin que les messages instantanés puissent être traduits dans la langue choisie par le client et vice versa.

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

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

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

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



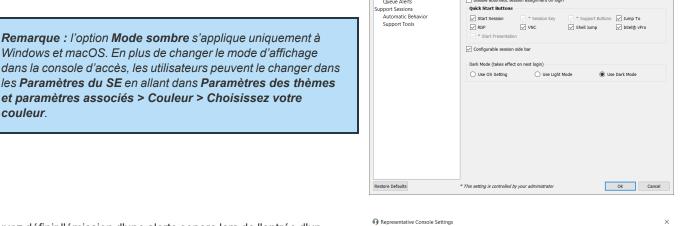
TC: 7/18/2022



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



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



Representative Console Settings

Global Settings

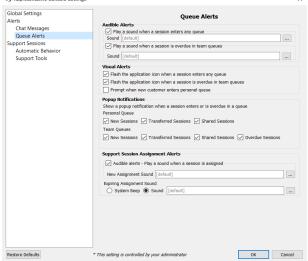
Chat Messages

Queue Alerts

Vous pouvez définir l'émission d'une alerte sonore lors de l'entrée d'un utilisateur dans l'une de vos files d'attente et/ou lors du passage d'une session en attente à l'état En souffrance. Pour télécharger un signal sonore personnalisé pour ces alertes, cliquez sur le bouton [...], puis sélectionnez un fichier WAV sur votre ordinateur. Notez que le fichier doit être inférieur à 1 Mo.

Vous pouvez également choisir de faire clignoter l'icône de l'application lors de l'entrée d'un utilisateur dans l'une de vos files d'attente et/ou lors du passage d'une session en attente à l'état En souffrance. En outre, lorsqu'un utilisateur entre dans votre file d'attente personnelle, en cliquant sur votre nom ou en saisissant une clé de session sur le site public, la session peut démarrer immédiatement ou attendre que vous l'acceptiez.

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



Disable automatic session assignment on login

Ouick Start Buttons

Vous pouvez en outre choisir d'entendre ou non une alerte sonore lorsqu'une session d'assistance technique vous est attribuée de manière automatique. Vous pouvez spécifier un signal sonore personnalisé pour les attributions de session.

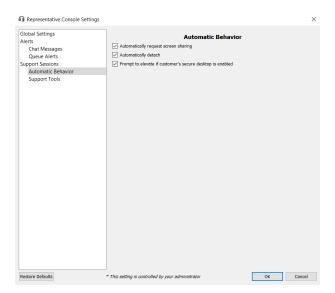
Enfin, vous pouvez choisir d'être averti lorsqu'une invitation de session attribuée automatiquement est sur le point d'expirer. Ici encore, vous pouvez définir un signal sonore personnalisé ou sélectionner l'option Signal sonore du système pour entendre le signal sonore système par défaut.



Indiquez si vous préférez démarrer vos sessions uniquement avec la messagerie instantanée ou demander immédiatement le partage d'écran.

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

Lorsqu'il est probable que vous rencontriez des problèmes à cause du bureau sécurisé de l'utilisateur, vous pouvez être invité à demander l'accroissement des privilèges afin d'exécuter la session avec des droits d'administration.



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

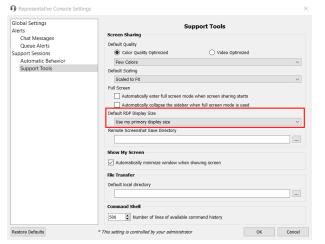
De plus, lorsque le partage d'écran commence, le système distant peut automatiquement voir son affichage et son entrée au clavier et à la souris restreints, fournissant un écran de confidentialité.

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

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

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

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

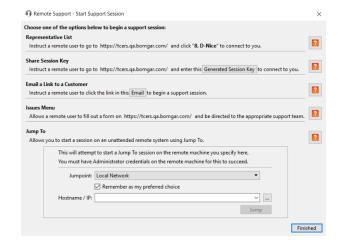




Prise en charge des utilisateurs

Options de démarrage de session d'assistance technique

Pour plus d'informations sur le démarrage d'une session, cliquez sur le bouton **Démarrer** situé en haut de la console du technicien d'assistance. Notez que les options disponibles dépendent de la configuration de votre site et des autorisations de votre compte.



Sessions initiées par le client

Vos clients disposent de plusieurs moyens pour initier une session d'assistance technique à distance avec un technicien d'assistance.

E-mail

Les techniciens d'assistance peuvent générer un e-mail contenant un lien. Pour recevoir une assistance technique, le destinataire de l'e-mail clique sur le lien, ce qui déclenche le téléchargement du client d'utilisateur sur son système. Ceci établit une connexion sécurisée vers le technicien d'assistance qui a émis l'invitation.

URL

Les techniciens d'assistance peuvent générer une URL en hyperlien pour l'utilisateur distant grâce à plusieurs méthodes, comme la messagerie instantanée.

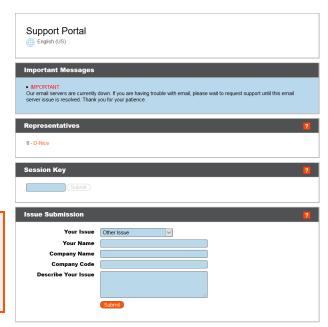


Portail Web BeyondTrust

BeyondTrust vous permet de créer des portails d'assistance technique sur internet ou des sites internet publics pour votre BeyondTrust Appliance B Series. Ces portails permettent à vos clients de demander une assistance technique avec les logiciels d'assistance technique à distance BeyondTrust. Chaque portail d'assistance technique peut être configuré pour prendre en charge l'identité et les processus de votre organisation. Ceci comprend la personnalisation des logos, et la possibilité de permettre aux clients de lancer une session BeyondTrust en utilisant la fonction cliquer-pour-messagerie instantanée.



Pour en savoir plus sur les portails d'assistance technique, veuillez consulter <u>Comment personnaliser les portails</u> <u>d'assistance technique</u> à l'adresse <u>https://www.beyondtrust.com/docs/remote-support/how-to/customize-portals/index.htm</u>.



- Techniciens d'assistance : vous pouvez présenter une liste de techniciens d'assistance connectés, permettant aux clients de cliquer sur le nom d'un technicien d'assistance pour lancer le téléchargement du client d'utilisateur. Une fois le téléchargement terminé, une session est lancée avec le technicien d'assistance.
- Clé de session : un technicien d'assistance peut générer une clé de session alphanumérique à partager avec un client. À partir de là, le client se rend sur le portail d'assistance technique et saisit la clé de session dans le champ de texte. Ceci ordonne au client d'utilisateur de télécharger et d'établir une connexion sécurisée vers le technicien d'assistance qui a émis l'invitation.
- Soumission de problème: la page du portail d'assistance technique peut être configurée pour offrir une sélection des problèmes parmi lesquels le client peut choisir lorsqu'il cherche une assistance technique. Les clients peuvent choisir un problème dans le menu déroulant pour déclencher le téléchargement du client d'utilisateur. Cette action génère une demande dans la file d'attente d'équipe associée à ce problème spécifique. Par exemple, si l'utilisateur sélectionne **Problèmes e-mail**, la demande sera dirigée vers l'équipe ou les techniciens d'assistance possédant des compétences en systèmes d'e-mail.

bouton d'assistance technique

Le bouton d'assistance technique est un raccourci sur le bureau installé à l'avance sur le poste de travail d'un client et qui lance le client d'utilisateur. Lorsque l'utilisateur clique sur le bouton d'assistance technique, il lui est demandé de saisir une clé de session ou de décrire son problème. Il peut aussi avoir la possibilité de rejoindre directement la file d'attente configurée pour le bouton d'assistance technique. Cette méthode spécifique de lancement de session peut être préinstallée sur une image standard et ne nécessite pas le téléchargement du client d'utilisateur.



Remarque: un bouton d'assistance technique ne peut pas être déployé depuis une session qui a été lancée depuis un portail public avec authentification SAML et un bouton d'assistance technique ne peut pas être utilisé pour démarrer une session avec un portail public qui requiert une authentification SAML.



Pour plus d'informations sur le bouton d'assistance technique , veuillez consulter <u>bouton d'assistance technique : Demande</u> <u>d'assistance technique rapide</u> à l'adresse <u>https://www.beyondtrust.com/docs/remote-support/getting-started/customer-client/support-button.htm.</u>

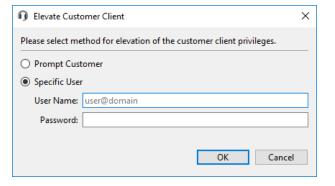


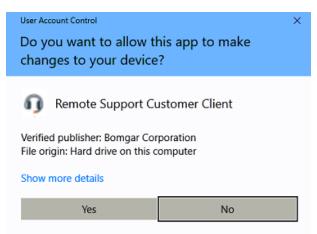
Accroissement des droits

Pour chaque méthode de lancement de session à l'initiative du client, le client d'utilisateur s'exécute dans le contexte de l'utilisateur connecté. Ainsi, l'invite du Contrôle d'accès d'utilisateur (UAC) de Windows rend plus difficile l'assistance technique. Pour permettre l'assistance technique dans ces situations, BeyondTrust offre la possibilité d'accroître les droits du client d'utilisateur. Ceci signifie simplement que le client d'utilisateur s'exécutant avec l'utilisateur connecté peut être accru au niveau d'un service système en fournissant des informations d'authentification administratives au système du client.

Ce processus génère une invite UAC non visible en partage d'écran et qui doit être résolue par le client. Cette invite ne nécessite pas d'informations d'authentification de l'utilisateur final. Ce dernier devra simplement cliquer sur **Qui**

Une fois que c'est fait, le client d'utilisateur s'exécute en tant que service système. Ainsi, toutes les invites UAC suivantes seront visibles lors du partage d'écran.





Session lancée par un technicien d'assistance

Jump Client BeyondTrust (agent d'exécution préinstallé)

Le Jump Client BeyondTrust est un service qui s'exécute et permet à un technicien d'assistance de lancer une session d'assistance technique vers un système distant spécifique à travers la console du technicien d'assistance. Ceci peut être utilisé pour lancer des sessions vers des systèmes sans surveillance, où aucun utilisateur n'est présent, ou comme méthode par défaut pour apporter une assistance technique aux clients. Bien que la session soit lancée par le technicien d'assistance, les autorisations dans BeyondTrust permettent de déterminer avec flexibilité si les techniciens d'assistance ont besoin de demander l'accès au client et peuvent même vérifier si un utilisateur connecté est présent. De plus, l'accès aux Jump Clients individuels peut être contrôlé individuellement ou par appartenance à un groupe dans BeyondTrust, et différents groupes peuvent disposer d'autorisations différentes.



Pour plus d'informations sur les Jump Clients, veuillez consulter <u>Guide Jump Client Remote Support : Accès sans surveillance à un système sur n'importe quel réseau</u> à l'adresse <u>https://www.beyondtrust.com/docs/remote-support/how-to/jump-clients/index.htm.</u>



Jump vers (ad hoc)

La deuxième méthode de lancement de session d'assistance technique amorcée par un technicien d'assistance est le Jump vers BeyondTrust. Jump vers permet aux techniciens d'assistance d'utiliser la console du technicien d'assistance pour envoyer le client d'utilisateur sur un poste de travail distant pour lancer une session d'assistance technique. Comme le téléchargement du client depuis la page d'un portail, ceci est une session ad hoc dans laquelle aucun élément n'est préinstallé et où tout est supprimé une fois la session terminée. Contrairement à la plupart des autres méthodes, cette méthode de lancement de session compte plusieurs dépendances. Tout d'abord, elle n'est disponible que sur Windows. Ensuite, elle dépend de plusieurs services Windows pour s'exécuter, et plusieurs ports TCP doivent être accessibles sur la machine distante. Pour cette raison, BeyondTrust propose une technologie appelée Jumpoints, qui peut aider au lancement sur un réseau distant.



Pour plus d'informations sur les Jumpoints, veuillez consulter <u>Guide Jumpoint Remote Support : Accès sans surveillance à des ordinateurs sur un réseau</u> à l'adresse <u>https://www.beyondtrust.com/docs/remote-support/how-to/jumpoint/index.htm.</u>



Génération d'une clé de session en vue de démarrer une session d'assistance technique

Selon les autorisations de votre compte, une méthode pour démarrer une session d'assistance technique consiste à utiliser des clés de session à usage unique, générées de manière aléatoire. Les clés de session ne sont pas utilisées pour l'authentification. Elles guident simplement le client vers l'équipe ou le technicien d'assistance approprié et ne sont valides que pour une durée limitée. Les méthodes grâce auxquelles le B Series Appliance génère des clés de session sont confidentielles. Lorsque votre utilisateur appelle avec une demande d'assistance technique, générez une nouvelle clé de session à partir :



- du menu Assistance technique de la console du technicien d'assistance
- du bouton Démarrer situé en haut de la console du technicien d'assistance
- du bouton Clé de session situé en haut de la console du technicien d'assistance
- de la combinaison Ctrl + F4 ou Commande + F4.

Définissez la durée de validité de la clé de session. Le délai d'expiration s'applique uniquement à la durée d'utilisation de la clé pour démarrer une session et n'affecte pas la durée de la session en elle-même.



Pour plus d'informations, veuillez consulter « Délai d'expiration maximum d'une clé de session » dans <u>Sécurité : gestion des paramètres de sécurité</u> à l'adresse <u>https://www.beyondtrust.com/docs/remote-support/getting-started/admin/security.htm.</u>

Vous pouvez également sélectionner le portail public par lequel vous voulez que l'utilisateur accède à la session, depuis les portails rendus disponibles par vous ou votre administrateur. La console du technicien d'assistance se souviendra de votre choix de la prochaine fois que vous générerez une clé de session.

En fonction des options sélectionnées par votre administrateur, vous pourrez envoyer l'invitation depuis votre adresse e-mail locale, une adresse e-mail du serveur, ou par SMS.

Dirigez votre utilisateur vers l'URL unique ou vers le site public où il doit saisir la clé de session. Dès l'exécution du client d'utilisateur, l'utilisateur apparaît dans votre file d'attente personnelle.



Consultation des sessions d'assistance technique en attente

Files d'attente

Les files d'attente de session fournissent des informations sur les clients en attente d'assistance technique, ainsi qu'un accès jusqu'à eux. L'onglet File d'attente **personnelle** contient les utilisateurs avec lesquels vous êtes en session ou qui attendent une session avec vous. Une session d'attente apparaîtra dans votre file d'attente personnelle si la session vous a été transférée, ou si le client a lancé la session en saisissant une clé de session que vous avez générée, en sélectionnant votre nom sur le site public ou en cliquant sur un bouton d'assistance technique auquel vous êtes lié. Cette file d'attente contient également les invitations à rejoindre une session partagée que vous avez reçues.

Vous disposez aussi de files d'attente pour toutes les équipes dont vous êtes membre. Si un client lance une session en sélectionnant un type de problème dans un formulaire de soumission de problème, ce client est placé dans la file d'attente de l'équipe qui possède ce problème. Un client est également placé dans une file d'attente d'équipe s'il clique sur un **bouton d'assistance technique** lié à une équipe. Une session peut également être placée dans une file d'attente suite à un transfert intentionnel, en raison des règles définies pour les sessions en attente, ou en cas de perte de la connexion du technicien d'assistance dans le courant d'une session. Ces files d'attente contiennent également les invitations à rejoindre une session partagée envoyées à tous les techniciens d'assistance de l'équipe.

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

Un utilisateur peut également demander de l'aide directement à partir d'une page Web, via un lien. La sélection de ce lien entraîne l'ouverture d'une session de partage de navigation, permettant au technicien d'assistance de discuter avec l'utilisateur et d'accéder à la page Web affichée sur son ordinateur. Il est possible pour les administrateurs de générer des liens personnalisés afin de diriger les sessions de navigation vers la file d'attente du technicien d'assistance ou de l'équipe appropriée. Dans les files d'attente, les sessions de partage de navigation sont identifiées à l'aide du préfixe [Browser], situé à côté du nom de l'utilisateur.

Organisez vos files d'attente en fonction de différents critères, notamment la durée d'attente de l'utilisateur, le nom de l'utilisateur, la catégorie de problème, etc. Tous les critères peuvent ne pas être disponibles selon la manière dont l'utilisateur a lancé la session. Vous pouvez rechercher une session active. Cliquez sur un élément dans la file d'attente pour consulter ses informations. Cliquez une seconde fois pour fermer la fenêtre d'informations. La console du technicien d'assistance se souviendra de l'ordre des colonnes et de l'organisation de la file d'attente des sessions la prochaine fois que la console du technicien d'assistance sera lancée.

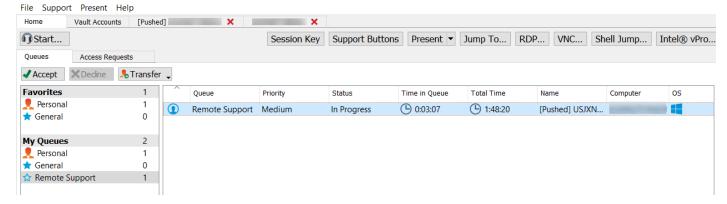
Une fois l'utilisateur placé dans la file d'attente, vous avez le choix entre cliquer deux fois sur l'entrée de l'utilisateur ou sélectionner l'entrée, puis cliquer sur le bouton **Accepter**. Le fait d'accepter une session ouvre un nouvel onglet pour cette session dans la partie supérieure de la console du technicien d'assistance. Il est possible d'exécuter plusieurs sessions simultanément. Un nouvel onglet est créé pour chaque session.



Vous trouverez d'autres moyens pour accepter les demandes d'assistance technique dans « Acceptation d'une session pour démarrer l'assistance technique », page 25.



BeyondTrust Remote Support Representative Console - tcers.qa.bomgar.com - Denise



Q Search Items



Acceptation d'une session pour démarrer l'assistance technique

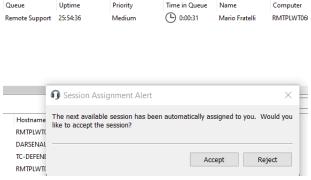
Une fois l'utilisateur dans la file d'attente, plusieurs moyens s'offrent à vous pour accepter la session. Si elle se trouve dans votre file d'attente personnelle ou que vous avez l'autorisation d'accepter manuellement des sessions depuis une file d'attente d'équipe, double-cliquez sur l'entrée de l'utilisateur ou sélectionnez-la, puis cliquez sur le bouton **Accepter**. Si vous êtes autorisé à utiliser cette fonction, commencez par la session la plus ancienne des files d'attente de votre équipe en choisissant d'obtenir la session suivante à partir :

- du menu Assistance technique de la console du technicien d'assistance
- du bouton Obtenir la suivante situé dans le haut de la console du technicien d'assistance

Règles d'attribution de session

Vous pouvez également accepter des sessions qui sont attribuées à l'aide d'Equilibrium. Lorsqu'une session est placée dans une file d'attente pour laquelle Equilibrium est activé, elle est automatiquement attribuée au technicien d'assistance le plus qualifié et le moins occupé, en fonction des compétences requises, du nombre de sessions prises en charge par ce technicien d'assistance et du temps pendant lequel il a été disponible.

Lorsqu'une session vous est attribuée, une invite apparaît pour que vous acceptiez ou rejetiez la session, en même temps qu'une alerte sonore si elle est activée. Des alertes visuelles et sonores vous avertissent que l'invitation est sur le point d'expirer. Si vous rejetez l'invitation ou si elle expire, la session est réattribuée au deuxième technicien d'assistance le plus qualifié et le moins occupé dans cette file d'attente.



Une session rejetée n'est jamais réattribuée une deuxième fois au même technicien d'assistance, à moins qu'elle ne soit transférée manuellement vers une autre file d'attente pour laquelle ce technicien d'assistance est disponible. Si une session fait le tour de tous les techniciens d'assistance disponibles pour la file d'attente sans être acceptée, elle reste dans la file d'attente jusqu'à ce que quelqu'un l'accepte ou la transfère manuellement.

Autrement, si votre administrateur a défini une règle de session en attente pour cette file d'attente, une alerte sonore et visuelle est émise pour signaler cette session en souffrance, ou la session est transférée vers une file d'attente de dépassement. Si cette file d'attente de dépassement est associée à une règle de session en attente renvoyant la session vers la première file d'attente, la session peut potentiellement passer de l'une à l'autre jusqu'à ce qu'elle soit acceptée.

Une session n'est pas attribuée à un technicien d'assistance si ce technicien d'assistance n'est pas disponible. Si vous verrouillez votre ordinateur ou basculez vers l'écran de connexion, vous êtes identifié comme indisponible. De même, les règles qui régissent les autorisations d'utilisateur vous désignent comme indisponible si vous participez à davantage de sessions que prévu ou si vous avez été inactif depuis plus longtemps que la période spécifiée. Enfin, si vous avez l'autorisation de refuser des attributions de session, vous pouvez choisir de ne pas recevoir d'attributions de session automatiques.

Le fait d'accepter une session ouvre un nouvel onglet pour cette session dans la partie supérieure de la console du technicien d'assistance. Il est possible d'exécuter plusieurs sessions simultanément. Un nouvel onglet est créé pour chaque session.



Remarque: les onglets de session peuvent être déplacés et réorganisés pour vous aider à organiser et hiérarchiser votre charge de travail. Cliquez et faites simplement glisser un onglet de session vers une nouvelle position. Les onglets de session peuvent également être détachés de la fenêtre principale de la console du technicien d'assistance.

TC: 7/18/2022

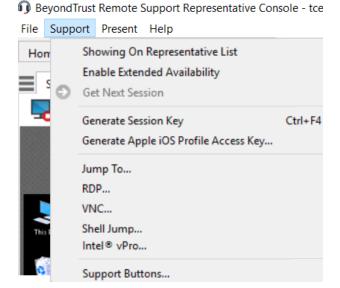


Génération d'une clé d'accès au profil Apple iOS

Pour distribuer vos profils BeyondTrust publics et privés aux utilisateurs d'appareils Apple iOS, générez une clé d'accès au profil Apple iOS à partir du menu **Assistance technique** de la console du technicien d'assistance.

Notez que la case Lien vers les profils de configuration iOS activé de la page /login > Portails publics > Configuration iOS doit être cochée pour que cette option soit disponible.

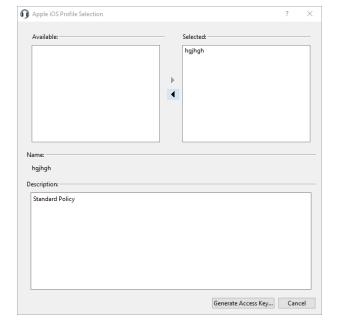
Cliquez sur **Générer une clé d'accès au profil Apple iOS** pour lancer l'interface **Sélection du profil Apple iOS**.



L'interface **Sélection du profil Apple iOS** contient les profils publics et privés précédemment configurés dans l'interface /login.

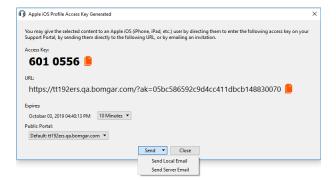
Tandis que le site public peut être défini pour afficher les profils iOS publics à quiconque connaît l'URL, la génération d'une clé d'accès est le seul moyen de permettre à un utilisateur d'accèder à un profil iOS privé.

Vous pouvez y sélectionner n'importe quel profil public ou privé pour le distribuer en toute sécurité aux utilisateurs d'appareils Apple iOS via votre portail d'assistance technique iOS consultable. Cliquez sur le bouton **Générer une clé d'accès**.





Lorsque vous cliquez sur le bouton **Clé d'accès générée**, un écran unique **Clé d'accès générée** s'ouvre contenant des options spéciales pour l'envoi d'un e-mail d'invitation à votre utilisateur de périphérique Apple iOS. En fonction des options sélectionnées par votre administrateur, vous pourrez envoyer l'invitation depuis votre adresse e-mail locale, une adresse e-mail du serveur, ou par SMS.





Interface de Jump

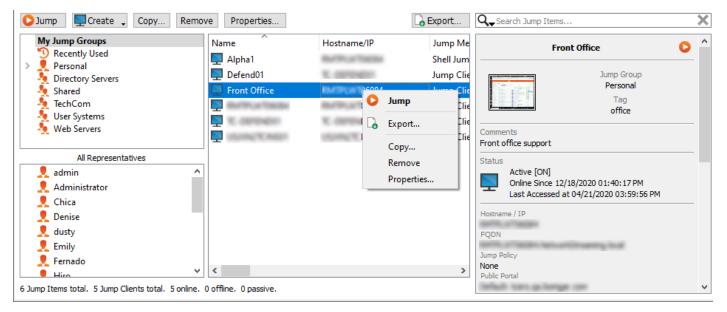
Utiliser les éléments de Jump pour apporter une assistance technique à des systèmes distants

La technologie Jump de BeyondTrust permet aux utilisateurs privilégiés de se connecter à un système distant sans surveillance pour démarrer une session sans l'aide d'un utilisateur final. Selon vos autorisations, vous pouvez effectuer un Jump vers un ordinateur de votre réseau local (LAN)/réseau privé virtuel (VPN) ou d'un réseau équipé d'un agent Jumpoint. Vous pouvez enregistrer des raccourcis de Jump pour les machines auxquelles vous accédez fréquemment. Pour effectuer un Jump vers un ordinateur non Windows ou vers un système n'appartenant à aucun réseau, vous pouvez installer un Jump Client.

L'interface de Jump apparaît dans la partie inférieure de la console du technicien d'assistance. La liste peut contenir des Jump Clients actifs et passifs ainsi que des raccourcis de Jump pour des Jumps distants, des Jumps locaux, des sessions RDP locales et distantes, des sessions VNC locales et distantes, des Shell Jumps et des Jumps Intel® vPro.

Les éléments de Jump sont répertoriés dans les groupes de Jump. Si vous êtes associé à un ou plusieurs groupes de Jump, vous pouvez accéder aux éléments de Jump de ces groupes, selon les autorisations accordées par votre administrateur. Sélectionner un groupe de Jump et cliquer sur **Créer** sélectionne automatiquement ce groupe de Jump dans la fenêtre de configuration d'élément de Jump.

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



Jump vers un élément de Jump

Parcourez les groupes ou recherchez dynamiquement les ordinateurs.

TC: 7/18/2022



Pour faciliter la navigation dans la liste des Jump Clients, vous pouvez faire glisser les colonnes pour les faire apparaître dans l'ordre de votre choix, puis trier une colonne en cliquant sur son en-tête. La console du technicien d'assistance se souviendra de l'ordre des colonnes ainsi que de leur organisation la prochaine fois que la console du technicien d'assistance sera lancée.

En plus de naviguer parmi les Jump Clients, vous pouvez effectuer une recherche basée sur plusieurs champs. Saisissez une chaîne dans le champ de recherche, puis appuyez sur **Entrée**. Pour choisir dans quels champs faire vos recherches, cliquez sur la loupe et cochez ou découchez un champ disponible. Les champs de recherche comprennent **les commentaires**, **l'utilisateur de la console**, **le domaine**, **le FQDN**, **le groupe**, **le nom d'hôte/l'IP**, **la méthode de Jump**, **le dernier accès**, **le nom**, **l'IP privée**, **l'IP publique**, **l'état**, **la balise** et **le groupe de travail**.

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



Remarque: si vous devez accéder à des éléments de Jump alors qu'aucun utilisateur n'est disponible, assurez-vous que les autorisations de session sont définies pour désactiver l'invite ou pour basculer par défaut sur **Autoriser** pour les sessions autonomes.

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

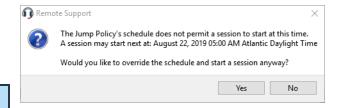


Pour plus de détails sur les scripts, veuillez consulter <u>Scripts pour Console du technicien d'assistance et API de scripts client</u> à l'adresse www.beyondtrust.com/docs/remote-support/how-to/integrations/api/client-script/index.htm.

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



Remarque: si vous avez l'autorisation de modifier les règles de Jump, l'invite vous donnera l'option d'outrepasser la planification et de démarrer une session malgré tout.



Copier des éléments de Jump

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

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

TC: 7/18/2022



Accès autonome à des ordinateurs distants à l'aide de Jump Clients

Pour accéder à un ordinateur sans l'aide d'un utilisateur final, installez un Jump Client sur ce système depuis une session ou depuis la page **Jump Clients** de l'interface d'administration. vos paramètres de compte déterminent les autorisations d'élément de Jump dont vous disposez, y compris à quels groupes de Jump vous avez accès, et quels types d'éléments de Jump vous êtes autorisé à utiliser.

Organiser les Jump Clients

Pour faciliter la navigation dans la liste des Jump Clients, vous pouvez faire glisser les colonnes pour les faire apparaître dans l'ordre de votre choix, puis trier une colonne en cliquant sur son en-tête. La console du technicien d'assistance se souviendra de l'ordre des colonnes ainsi que de leur organisation la prochaine fois que la console du technicien d'assistance sera lancée.

Trouver un Jump Client

En plus de naviguer parmi les Jump Clients, vous pouvez effectuer une recherche basée sur plusieurs champs. Saisissez une chaîne dans le champ de recherche, puis appuyez sur **Entrée**. Pour choisir dans quels champs faire vos recherches, cliquez sur la loupe et cochez ou découchez un champ disponible. Les champs de recherche comprennent **les commentaires**, **l'utilisateur de la console**, **le domaine**, **le FQDN**, **le groupe**, **le nom d'hôte/l'IP**, **la méthode de Jump**, **le dernier accès**, **le nom**, **l'IP privée**, **l'IP publique**, **l'état**, **la balise** et **le groupe de travail**.

Panneau de détails sur le Jump Client

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

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

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

Wake-On-Lan (WOL)

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



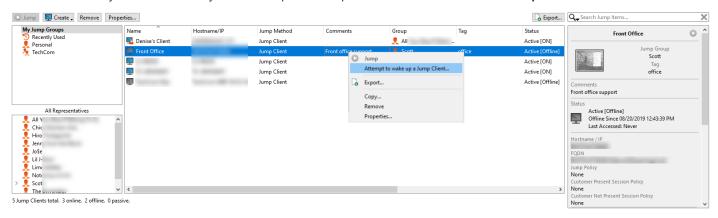
Remarque: WOL n'est pas une technologie BeyondTrust. Le logiciel BeyondTrust s'intègre aux systèmes WOL existants. Pour utiliser WOL avec BeyondTrust, la fonction WOL du système doit être activée, et le réseau doit autoriser l'envoi de paquets de WOL.

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



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

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



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

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

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

Copier des éléments de Jump

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

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

TC: 7/18/2022



Propriétés des Jump Clients

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

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

Changez le mode d'un Jump Client depuis le menu déroulant **Type de connexion**. Les Jump Clients actifs envoient des statistiques vers la B Series Appliance à intervalles définis. Les Jump Clients passifs envoient des statistiques vers la B Series Appliance une fois par jour, ou lors de l'« archivage » manuel. Selon les options choisies par votre administrateur, ces statistiques peuvent inclure plusieurs détails sur l'ordinateur distant, comme l'utilisateur connecté à la console, le système d'exploitation, le temps de fonctionnement, le processeur, le taux d'utilisation du disque et une capture d'écran de la dernière mise à jour.

Une fois un mot de passe défini pour un Jump Client, son icône indique qu'il est verrouillé, et la capture d'écran est elle aussi verrouillée. Pour Jump vers un Jump Client verrouillé, vous devez fournir son mot de passe. De même, vous devez fournir le mot de passe pour supprimer un Jump Client verrouillé via l'interface de Jump Client. Vous n'avez pas besoin du mot de passe pour vous détacher d'une session, puisque vous avez déjà fourni le mot de passe pour Jump vers la session.

Si l'option **Démarrage silencieux** est cochée, le client d'utilisateur ne s'affiche pas au premier plan et reste réduit dans la barre des tâches ou le dock au lancement d'une session.

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

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

Sélectionnez le **portail public** à travers lequel cet élément de Jump doit se connecter. Si une règle de session est associée à ce portail public, celle-ci peut affecter les autorisations des sessions démarrées avec cet élément de Jump. Le fait de pouvoir définir ou non le portail public dépend également des autorisations définies pour votre compte.

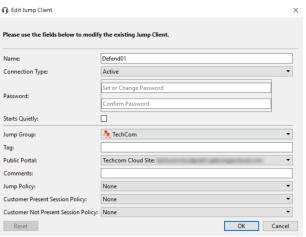
Les éléments de Jump comprennent un champ **Commentaires** pour un nom ou une description, ce qui facilite et accélère le tri, la recherche et l'identification des éléments de Jump.

Sélectionnez une **Règle de Jump** afin de définir quand les utilisateurs peuvent accéder à cet élément de Jump. Ces règles doivent être configurées par l'administrateur dans l'interface **/login**.

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

Sélectionnez les règles de session à appliquer à cet élément de Jump. Les règles de session affectées à cet élément de Jump ont la priorité lors de la configuration des autorisations de session. La **Règle de session Utilisateur présent** est appliquée lorsque l'utilisateur final est déterminé comme étant présent. Dans le cas contraire, c'est la **Règle de session Utilisateur absent** qui s'applique.

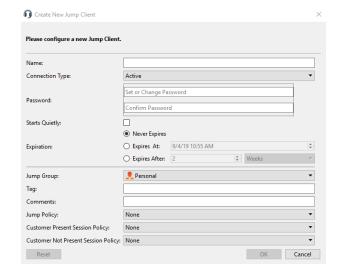
La présence du client est déterminée par le paramètre d'élément de Jump **Utiliser l'état de l'écran pour détecter la présence du client** dans l'interface /login. Lorsque cette option est activée, un client est considéré comme présent uniquement si un utilisateur est connecté, le système n'est pas verrouillé et l'économiseur d'écran ne s'exécute pas. Si l'option est désactivée, un client est considéré





comme présent si un utilisateur est connecté, quel que soit l'état de l'écran. La présence du client est détectée au démarrage de la session d'élément de Jump. La règle de session utilisée reste la même tout au long de la session, même en cas de modification de l'état de l'utilisateur. Le fait de pouvoir définir ou non une règle de session dépend là encore des autorisations définies pour votre compte.

Lors de l'attachement d'un Jump Client à partir d'une session et de la personnalisation préalable des propriétés, vous pouvez également définir l'expiration du Jump Client. Cela peut être jamais, à une heure et une date spécifiques ou après une certaine période. Un Jump Client expiré est automatiquement désinstallé du système distant et supprimé de la liste dans l'interface.



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



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



Jump Clients actifs et passifs				
Jump Client actif			Jump Client passif	
Maintient une connexion durable au B Series Appliance.			Écoute une demande d'accès à distance depuis le B Series Appliance.	
			Remarque : il peut être nécessaire de configurer le pare-feu.	
Envoie des statistiques vers le B Series Appliance à intervalles réguliers.			Envoie des statistiques au B Series Appliance une fois par jour, lord d'un archivage manuel, ou lorsqu'un nouvel utilisateur se connecte (si cette fonction est activée).	
Permet d'accéder à distance à n'importe quel système d'exploitation pris en charge par BeyondTrust.			Permet d'accéder à distance à n'importe quel système d'exploitation pris en charge par BeyondTrust.	
Le nombre de clients à installer est limité par le modèle de votre B Series Appliance.		le modèle de votre B	Cinquante mille Jump Clients passifs sont pris en charge sur tous les modèles de B Series Appliance.	
B200	B300	B400	Si vous avez besoin de davantage de Jump Clients passifs, contactez l'assistance technique à l'adresse	
Jusqu'à 1 000 Jump Clients actifs	Jusqu'à 10 000 Jump Clients actifs	Jusqu'à 25 000 Jump Clients actifs	www.beyondtrust.com/support.	
serveur virtuel RS (P)	serveur virtuel RS (M)	serveur virtuel RS (G)		
Jusqu'à 1 000 Jump Clients actifs	Jusqu'à 10 000 Jump Clients actifs	Jusqu'à 25 000 Jump Clients actifs		



Remarque : le nombre maximal de Jump Clients disponibles pour une serveur virtuel RS dépend des ressources allouées.

Utiliser des Jump Clients pour un accès autonome à des appareils Android

Une connexion persistante peut être établie avec un appareil Android Samsung ou Zebra en attachant un Jump Client à l'appareil. Ceci donne la possibilité d'avoir des sessions d'assistance technique autonomes. Vous pouvez déployer des Jump Clients en utilisant l'une des méthodes ci-dessous.



Remarque : l'utilisation de la bande passante et l'autonomie de la batterie ne sont que légèrement affectées par l'établissement d'une connexion persistante.





Remarque: les connexions persistantes à des appareils Android autonomes ne peuvent avoir lieu que lorsque le Client d'assistance technique BeyondTrust et l'Appli de Jump Client BeyondTrust sont tous deux installés depuis le Play Store de Google sur les appareils. Pour en savoir plus, veuillez consulter Télécharger le Client d'assistance technique BeyondTrust et les Applis de Jump Client BeyondTrust à l'adresse https://www.beyondtrust.com/docs/remote-support/getting-started/customer-client/android/android-download-app.htm.

Attachez un Jump Client Android depuis la Console du technicien d'assistance

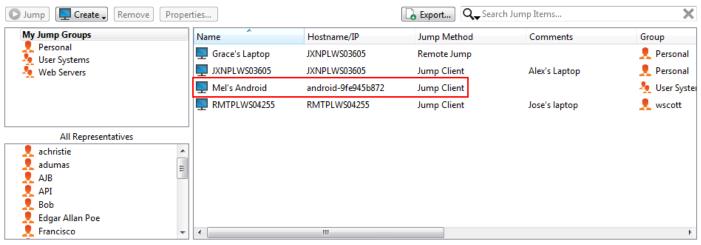
 Au cours d'une session d'assistance technique avec un appareil Android, cliquez sur l'icône Attacher comme Jump Client.



- Après l'avoir attaché, l'appareil Android apparaît comme élément de Jump dans la liste des éléments de Jump. Si l'icône Attacher un Jump Client est grisée, le Jump Client Android n'est pas installé sur l'appareil Android.
- 3. Dans le même temps, l'appli Jump Client BeyondTrust sur l'appareil affiche le client comme attaché avec la date et l'heure.



Remarque: des options sont disponibles pour que le Jump Client soit désactivé si l'appareil dépend de la batterie ou d'une connexion de données pour la connexion.

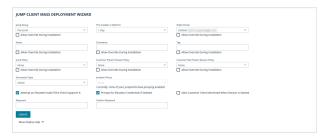


3 Jump Items total. 2 Jump Clients total. 2 online. 0 offline. 0 passive.

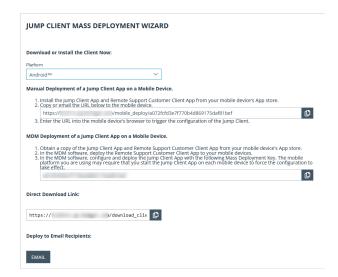
Envoyer un lien par e-mail depuis l'interface /login pour installer un Jump Client Android



 Depuis l'interface /login, allez sur Jump > Jump Clients > Assistant de déploiement en masse de Jump Clients.



- 2. Donnez les informations nécessaires pour votre Jump Client, comme le Groupe de Jump, le Portail public, etc.
- 3. Cliquez sur Créer.
- 4. Dans la section **Télécharger ou installer le client maintenant**, choisissez **Android** comme plateforme.
- 5. Vérifiez que l'appli **Jump Client BeyondTrust** est installée sur l'appareil Android. Si ce n'est pas le cas, allez sur Google Play pour télécharger l'application.



6. Pour télécharger le Jump Client sur l'appareil Android, ouvrez un navigateur sur celui-ci et allez sur l'URL fournie par l'assistant de déploiement en masse.



Remarque: vous pouvez également envoyer l'URL par e-mail à l'appareil Android en cliquant sur le lien E-mail situé dans la section Déployer auprès des destinataires de messagerie.



Remarque: Android empêche l'application d'être pleinement fonctionnelle tant que l'utilisateur n'a pas ouvert l'application au moins une fois. Cela doit être fait une fois l'application installée et avant d'essayer d'y attacher une session.



Créer et utiliser des raccourcis de Jump local



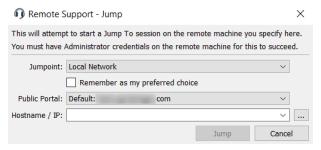
Remarque: Jumpoint est disponible uniquement pour les systèmes Windows et Linux. Des Jump Clients sont nécessaires pour l'accès à distance aux ordinateurs Mac. Pour effectuer un Jump vers un ordinateur Windows sans Jump Client, celui-ci doit être dans un domaine et le Service d'accès à distance au registre (désactivé par défaut sur Vista) doit être activé. Si vous devez accéder à des ordinateurs distants via Jumpoint alors qu'aucun utilisateur n'est disponible, assurez-vous que les autorisations de votre compte sont définies pour désactiver l'invite ou pour basculer par défaut sur Autoriser. Vous ne pouvez pas effectuer de Jump vers un appareil portable, mais la technologie Jump est disponible pour les consoles mobiles BeyondTrust.



Remarque: Les Jumpoints Linux peuvent uniquement être utilisés pour les sessions RDP et SSH/Telnet.

Pour effectuer un Jump sans client pré-installé, ouvrez la boîte de dialogue **Effectuer un Jump vers...** à partir :

- du menu Assistance technique de la console du technicien d'assistance
- du bouton Démarrer situé en haut de la console du technicien d'assistance
- du bouton Effectuer un Jump vers situé en haut de la console du technicien d'assistance



Dans la liste déroulante **Jumpoint**, sélectionnez le réseau qui héberge l'ordinateur auquel vous voulez accéder. Selon les autorisations dont vous disposez, vous pouvez effectuer un Jump vers un système du réseau local ou vers un réseau bénéficiant d'un Jumpoint.

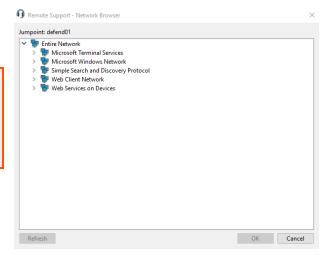
Sélectionnez le portail public auquel vous voulez associer votre session. Cela permet au système de savoir quel comportement d'accord pour l'utilisateur employer.



Pour en savoir plus, veuillez consulter <u>Client d'utilisateur</u>: <u>Modification de l'e-mail d'invitation, des options d'affichage et des options de connexion</u> à l'adresse <u>https://www.beyondtrust.com/docs/remote-support/getting-started/admin/customer-client.htm</u>.

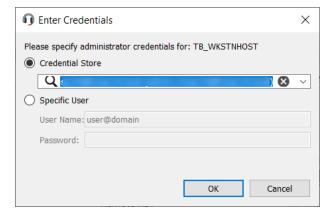
Saisissez le nom d'hôte ou l'adresse IP du système auquel vous souhaitez accéder. Si la navigation réseau est activée (/login> Jump > Jumpoint), vous pouvez également utiliser le bouton [...] pour accéder à l'arborescence de répertoires.

Une fois l'ordinateur cible localisé, cliquez sur Effectuer un Jump.





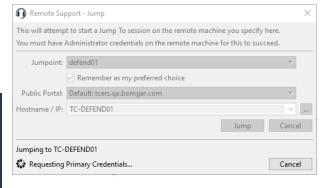
Vous devez alors fournir les informations d'authentification d'administration de l'ordinateur distant pour pouvoir effectuer le Jump. Les droits d'administration utilisés doivent correspondre à un administrateur local du système distant ou à un administrateur de domaine.



Les fichiers clients seront envoyés sur le système distant, et une session essaiera de se lancer. Selon les autorisations définies pour la session, l'utilisateur final peut être invité à accepter ou à refuser la session. En l'absence de réponse dans le délai imparti, la session démarre ou est annulée, en fonction des autorisations définies pour la session.



Remarque: si vous devez accéder à des systèmes via un Jumpoint alors qu'aucun utilisateur n'est disponible, assurezvous que les autorisations pour votre compte ainsi que pour le portail public sont définies pour désactiver l'invite ou pour basculer par défaut sur Autoriser.





Créer et utiliser des éléments de Jump locaux ou distants

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

Un Jumpoint sert de conduit pour un accès autonome aux ordinateurs d'un réseau distant connu. Un Jumpoint unique installé sur un ordinateur dans un réseau LAN est utilisé pour accéder à plusieurs systèmes, ce qui élimine le besoin de préinstaller un logiciel sur chaque ordinateur auquel on peut vouloir accéder.

Un Jump local permet à un utilisateur de se connecter à un ordinateur distant non autonome de son réseau local, Dans le réseau local, l'ordinateur de l'utilisateur BeyondTrust peut initier une session vers un système Windows ou Linux directement, sans utiliser de Jumpoint.



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

Créer un raccourci de Jump distant

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



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



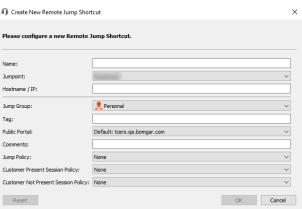
Remarque: pour voir les propriétés de plusieurs éléments de Jump, les éléments sélectionnés doivent tous être du même type (par ex. que des Jump Clients, que des Jump distants, etc.). Pour examiner les propriétés d'autres types d'éléments de Jump, veuillez consulter la section correspondante de ce guide.

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

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

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

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



TC: 7/18/2022



Sélectionnez le **portail public** à travers lequel cet élément de Jump doit se connecter. Si une règle de session est associée à ce portail public, celle-ci peut affecter les autorisations des sessions démarrées avec cet élément de Jump. Le fait de pouvoir définir ou non le portail public dépend également des autorisations définies pour votre compte.

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

Sélectionnez une **Règle de Jump** afin de définir quand les utilisateurs peuvent accéder à cet élément de Jump. Ces règles doivent être configurées par l'administrateur dans l'interface **/login**.

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

Sélectionnez les règles de session à appliquer à cet élément de Jump. Les règles de session affectées à cet élément de Jump ont la priorité lors de la configuration des autorisations de session. La **Règle de session Utilisateur présent** est appliquée lorsque l'utilisateur final est déterminé comme étant présent. Dans le cas contraire, c'est la **Règle de session Utilisateur absent** qui s'applique.

La présence du client est déterminée par le paramètre d'élément de Jump **Utiliser l'état de l'écran pour détecter la présence du client** dans l'interface /login. Lorsque cette option est activée, un client est considéré comme présent uniquement si un utilisateur est connecté, le système n'est pas verrouillé et l'économiseur d'écran ne s'exécute pas. Si l'option est désactivée, un client est considéré comme présent si un utilisateur est connecté, quel que soit l'état de l'écran. La présence du client est détectée au démarrage de la session d'élément de Jump. La règle de session utilisée reste la même tout au long de la session, même en cas de modification de l'état de l'utilisateur. Le fait de pouvoir définir ou non une règle de session dépend là encore des autorisations définies pour votre compte.

Créer un raccourci de Jump local

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



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



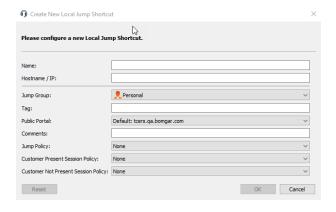
Remarque: pour voir les propriétés de plusieurs éléments de Jump, les éléments sélectionnés doivent tous être du même type (par ex. que des Jump Clients, que des Jump distants, etc.). Pour examiner les propriétés d'autres types d'éléments de Jump, veuillez consulter la section correspondante de ce guide.

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

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

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

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



TC: 7/18/2022



Sélectionnez le **portail public** à travers lequel cet élément de Jump doit se connecter. Si une règle de session est associée à ce portail public, celle-ci peut affecter les autorisations des sessions démarrées avec cet élément de Jump. Le fait de pouvoir définir ou non le portail public dépend également des autorisations définies pour votre compte.

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

Sélectionnez une **Règle de Jump** afin de définir quand les utilisateurs peuvent accéder à cet élément de Jump. Ces règles doivent être configurées par l'administrateur dans l'interface **/login**.

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

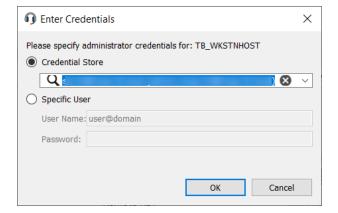
Sélectionnez les règles de session à appliquer à cet élément de Jump. Les règles de session affectées à cet élément de Jump ont la priorité lors de la configuration des autorisations de session. La **Règle de session Utilisateur présent** est appliquée lorsque l'utilisateur final est déterminé comme étant présent. Dans le cas contraire, c'est la **Règle de session Utilisateur absent** qui s'applique.

La présence du client est déterminée par le paramètre d'élément de Jump **Utiliser l'état de l'écran pour détecter la présence du client** dans l'interface /login. Lorsque cette option est activée, un client est considéré comme présent uniquement si un utilisateur est connecté, le système n'est pas verrouillé et l'économiseur d'écran ne s'exécute pas. Si l'option est désactivée, un client est considéré comme présent si un utilisateur est connecté, quel que soit l'état de l'écran. La présence du client est détectée au démarrage de la session d'élément de Jump. La règle de session utilisée reste la même tout au long de la session, même en cas de modification de l'état de l'utilisateur. Le fait de pouvoir définir ou non une règle de session dépend là encore des autorisations définies pour votre compte.

Utiliser un raccourci de Jump distant ou un raccourci de Jump local

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

Vous devez alors fournir les informations d'authentification d'administration de l'ordinateur distant pour pouvoir effectuer le Jump. Les droits d'administration utilisés doivent correspondre à un administrateur local du système distant ou à un administrateur de domaine.

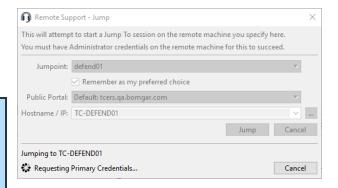




Les fichiers clients seront envoyés sur le système distant, et une session essaiera de se lancer. Selon les autorisations définies pour la session, l'utilisateur final peut être invité à accepter ou à refuser la session. En l'absence de réponse dans le délai imparti, la session démarre ou est annulée, en fonction des autorisations définies pour la session.



Remarque: si vous devez accéder à des systèmes via un Jumpoint alors qu'aucun utilisateur n'est disponible, assurezvous que les autorisations pour votre compte ainsi que pour le portail public sont définies pour désactiver l'invite ou pour basculer par défaut sur Autoriser.





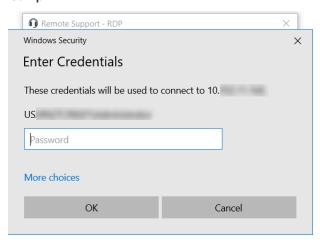
Utiliser un RDP local pour accéder à des systèmes Windows et Linux

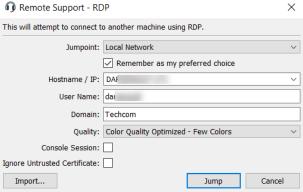
Utilisez BeyondTrust pour démarrer une session locale de protocole de bureau à distance (RDP) avec des systèmes Windows et Linux distants. Contrairement à une session RDP BeyondTrust classique, les sessions RDP locales ne passent pas à travers un Jumpoint, ce qui signifie que les utilisateurs ne peuvent effectuer de Jump que vers des systèmes à l'intérieur de leur réseau local. Pour utiliser le RDP local à travers BeyondTrust, vous devez avoir l'autorisation de compte d'utilisateur **Méthodes de Jump autorisées : RDP local sur le réseau local.**

- Pour démarrer une session RDP locale depuis la console du technicien d'assistance, ouvrez la boîte de dialogue Protocole de bureau à distance à partir du menu Assistance technique ou du bouton RDP.
- 2. Choisissez Réseau local comme option de Jumpoint.
- Saisissez le nom d'hôte ou l'adresse IP de l'ordinateur auquel vous souhaitez apporter une assistance technique.
- 4. Indiquez le nom d'utilisateur à utiliser pour la connexion.
- 5. Sélectionnez un domaine.
- 6. Définissez la qualité d'affichage de l'écran distant. Ce réglage ne peut pas être modifié pendant une session RDP.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).
- 7. Pour démarrer une session de console plutôt qu'une nouvelle session, cochez la case **Session de console**. Si le certificat du serveur ne peut pas être vérifié, vous recevrez un avertissement. Cocher l'option **Ignorer ce certificat non approuvé** vous permet de vous connecter au système distant sans voir ce message.

Les modes Vidéo optimisée et Toutes les couleurs vous permettent de voir le vrai fond d'écran.

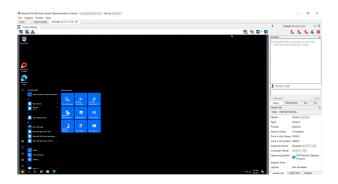
- 8. Pour importer un fichier RDP, cliquez sur le bouton **Importer**. Cela permet de pré-renseigner certains champs requis pour la connexion du protocole de bureau à distance.
- 9. Pour démarrer la session de protocole de bureau à distance, cliquez sur Jump.
- Vous êtes invité à saisir le mot de passe associé au nom d'utilisateur indiqué au préalable.







11. Votre session de protocole de bureau à distance (RDP) démarre.



Assistance technique multimoniteur

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



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



Créer et utiliser des raccourcis RDP

Utilisez BeyondTrust pour démarrer une session de protocole de bureau à distance (RDP) avec un système Windows ou Linux distant. Comme les sessions RDP sont converties en sessions BeyondTrust, les utilisateurs peuvent partager ou transférer des sessions, et celles-ci peuvent être automatiquement contrôlées et enregistrées, selon la configuration définie par l'administrateur pour votre site.

Pour utiliser le RDP local à travers BeyondTrust, vous devez être sur le même segment de réseau que le système cible et avoir l'autorisation de compte d'utilisateur **Méthodes de Jump autorisées : RDP local**.

Pour utiliser le RDP distant à travers BeyondTrust, vous devez avoir accès à un Jumpoint et avoir l'autorisation du compte d'utilisateur **Méthodes de Jump autorisées : RDP distant**.

Créer un raccourci de RDP local

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



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



Remarque : pour voir les propriétés de plusieurs éléments de Jump, les éléments sélectionnés doivent tous être du même type (par ex. uniquement des Jump Client, uniquement des Jump distants, etc.). Pour vérifier les propriétés d'autres types d'éléments de Jump, veuillez consulter la section adéquate de ce guide.

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

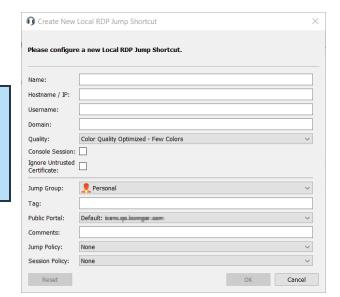
Saisissez le **nom d'hôte / IP** du système auquel vous souhaitez accéder.



Remarque: Par défaut, le serveur RDP écoute le port 3389, qui constitue donc le port par défaut pour les tentatives BeyondTrust. Si le serveur RDP distant est configuré pour utiliser un port différent, ajoutez-le à la suite du nom d'hôte ou de l'adresse IP au format <hostname>:<port> ou <ipaddress>:<port> (par exemple, 10.10.24.127:40000).

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

Définissez la **qualité** d'affichage de l'écran distant. Ce réglage ne peut pas être modifié pendant une session RDP. Définir le mode d'optimisation de la couleur d'affichage de l'écran distant. Si vous comptez principalement partager de la vidéo, sélectionnez **Vidéo optimisée**; sinon, choisissez



entre **Noir et blanc** (utilise moins de bande passante), **Quelques couleurs**, **Davantage de couleurs** ou **Toutes les couleurs** (utilise plus de bande passante). Les modes Vidéo optimisée et Toutes les couleurs vous permettent de voir votre fond d'écran.

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

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



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

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

Sélectionnez le **portail public** à travers lequel cet élément de Jump doit se connecter. Si une règle de session est associée à ce portail public, celle-ci peut affecter les autorisations des sessions démarrées avec cet élément de Jump. Le fait de pouvoir définir ou non le portail public dépend également des autorisations définies pour votre compte.

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

Sélectionnez une **Règle de Jump** afin de définir quand les utilisateurs peuvent accéder à cet élément de Jump. Ces règles doivent être configurées par l'administrateur dans l'interface **/login**.

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

Créer un raccourci de RDP distant

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



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



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

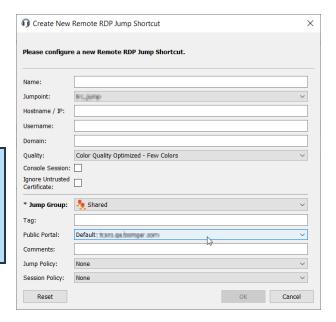
Saisissez un **Nom** pour l'élément de Jump. Ce nom identifie l'élément dans les onglets de la session. Cette chaîne contient 128 caractères au maximum.

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



Remarque: Par défaut, le serveur RDP écoute le port 3389, qui constitue donc le port par défaut pour les tentatives BeyondTrust. Si le serveur RDP distant est configuré pour utiliser un port différent, ajoutez-le à la suite du nom d'hôte ou de l'adresse IP au format <hostname>:<port> ou <ipaddress>:<port> (par exemple, 10.10.24.127:40000).

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





Définissez la **qualité** d'affichage de l'écran distant. Ce réglage ne peut pas être modifié pendant une session RDP. Définir le mode d'optimisation de la couleur d'affichage de l'écran distant. Si vous comptez principalement partager de la vidéo, sélectionnez **Vidéo optimisée**; sinon, choisissez entre **Noir et blanc** (utilise moins de bande passante), **Quelques couleurs**, **Davantage de couleurs** ou **Toutes les couleurs** (utilise plus de bande passante). Les modes Vidéo optimisée et Toutes les couleurs vous permettent de voir votre fond d'écran.

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

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

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

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

Sélectionnez le **portail public** à travers lequel cet élément de Jump doit se connecter. Si une règle de session est associée à ce portail public, celle-ci peut affecter les autorisations des sessions démarrées avec cet élément de Jump. Le fait de pouvoir définir ou non le portail public dépend également des autorisations définies pour votre compte.

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

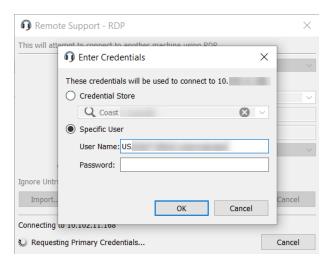
Sélectionnez une **Règle de Jump** afin de définir quand les utilisateurs peuvent accéder à cet élément de Jump. Ces règles doivent être configurées par l'administrateur dans l'interface **/login**.

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

Utiliser un raccourci de RDP

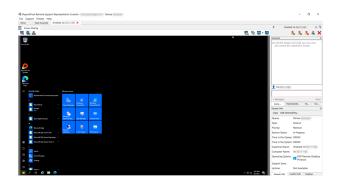
Pour utiliser un raccourci de Jump pour démarrer une session, sélectionnez simplement le raccourci dans l'interface de Jump et cliquez sur le bouton **Jump**.

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





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



Assistance technique multimoniteur

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



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



Remarque: il est possible de configurer les éléments de Jump pour permettre à plusieurs utilisateurs d'accéder au même élément de Jump en simultané. Si ce paramètre est réglé sur **Démarrer une nouvelle session**, une nouvelle session indépendante commence pour chaque utilisateur effectuant un jump vers un élément de Jump RDP spécifique. La configuration RDP sur le point de terminaison définit le comportement relatif aux connexions RDP simultanées.



Pour en savoir plus sur les Jumps simultanés, veuillez consulter <u>Paramètres d'élément de Jump</u> à l'adresse <u>www.beyondtrust.com/docs/remote-support/getting-started/admin/jump-items.htm</u>.



VNC vers un système distant

Utilisez BeyondTrust pour démarrer une session VNC avec un système distant. Comme les sessions VNC sont converties en sessions BeyondTrust, les utilisateurs peuvent partager ou transférer des sessions, et celles-ci peuvent être automatiquement contrôlées et enregistrées, selon la configuration définie par l'administrateur pour votre site.

Pour utiliser le VNC local à travers BeyondTrust, vous devez être sur le même segment de réseau que le système cible et avoir l'autorisation de compte d'utilisateur **Méthodes de Jump autorisées : VNC local**.

Pour utiliser le VNC distant à travers BeyondTrust, vous devez avoir accès à un Jumpoint et avoir l'autorisation du compte d'utilisateur **Méthodes de Jump autorisées : VNC distant**.

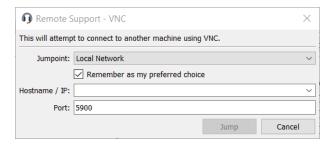
Pour démarrer une session VNC, ouvrez la boîte de dialogue VNC à partir :

- du menu Assistance technique de la console du technicien d'assistance
- du bouton VNC situé en haut de la console du technicien d'assistance

Dans la liste déroulante **Jumpoint**, sélectionnez le réseau qui héberge l'ordinateur auquel vous voulez accéder. Si vous accédez régulièrement au même Jumpoint, cochez **Enregistrer en tant que favori**. Saisissez le **nom d'hôte / IP** du système auquel vous souhaitez accéder.

par défaut, le serveur VNC écoute sur le port 5900, qui est donc le port par défaut des tentatives BeyondTrust. Si le serveur VNC distant est configuré pour utiliser un port différent, saisissez-le dans le champ **Port**.

Pour démarrer la session VNC, cliquez sur Jump.





Créer et utiliser des raccourcis VNC

Utilisez BeyondTrust pour démarrer une session VNC avec un système distant. Comme les sessions VNC sont converties en sessions BeyondTrust, les utilisateurs peuvent partager ou transférer des sessions, et celles-ci peuvent être automatiquement contrôlées et enregistrées, selon la configuration définie par l'administrateur pour votre site.

Pour utiliser le VNC local à travers BeyondTrust, vous devez être sur le même segment de réseau que le système cible et avoir l'autorisation de compte d'utilisateur **Méthodes de Jump autorisées : VNC local**.

Pour utiliser le VNC distant à travers BeyondTrust, vous devez avoir accès à un Jumpoint et avoir l'autorisation du compte d'utilisateur **Méthodes de Jump autorisées : VNC distant**.

Créer un raccourci VNC local

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



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



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

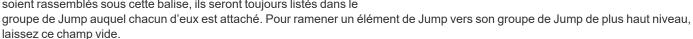
Saisissez un **Nom** pour l'élément de Jump. Ce nom identifie l'élément dans les onglets de la session. Cette chaîne contient 128 caractères au maximum.

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

par défaut, le serveur VNC écoute sur le port 5900, qui est donc le port par défaut des tentatives BeyondTrust. Si le serveur VNC distant est configuré pour utiliser un port différent, saisissez-le dans le champ **Port**.

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

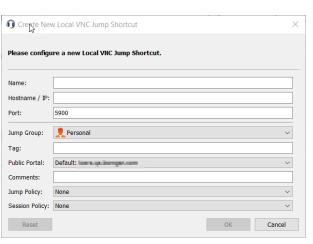
Organisez encore mieux vos éléments de Jump en saisissant le nom d'une **Balise** nouvelle ou existante. Bien que les éléments de Jump sélectionnés soient rassemblés sous cette balise, ils seront toujours listés dans le



Sélectionnez le **portail public** à travers lequel cet élément de Jump doit se connecter. Si une règle de session est associée à ce portail public, celle-ci peut affecter les autorisations des sessions démarrées avec cet élément de Jump. Le fait de pouvoir définir ou non le portail public dépend également des autorisations définies pour votre compte.

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

Sélectionnez une **Règle de Jump** afin de définir quand les utilisateurs peuvent accéder à cet élément de Jump. Ces règles doivent être configurées par l'administrateur dans l'interface **/login**.





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

Créer un raccourci VNC distant

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

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



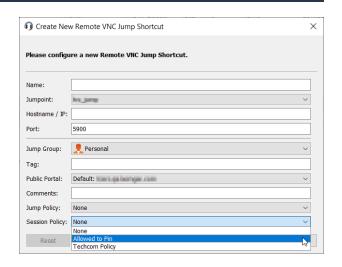
Remarque : pour voir les propriétés de plusieurs éléments de Jump, les éléments sélectionnés doivent tous être du même type (par ex. que des Jump Clients, que des Jump distants, etc.).

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

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

par défaut, le serveur VNC écoute sur le port 5900, qui est donc le port par défaut des tentatives BeyondTrust. Si le serveur VNC distant est configuré pour utiliser un port différent, saisissez-le dans le champ **Port**.

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



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

Sélectionnez le **portail public** à travers lequel cet élément de Jump doit se connecter. Si une règle de session est associée à ce portail public, celle-ci peut affecter les autorisations des sessions démarrées avec cet élément de Jump. Le fait de pouvoir définir ou non le portail public dépend également des autorisations définies pour votre compte.

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

Sélectionnez une **Règle de Jump** afin de définir quand les utilisateurs peuvent accéder à cet élément de Jump. Ces règles doivent être configurées par l'administrateur dans l'interface **/login**.

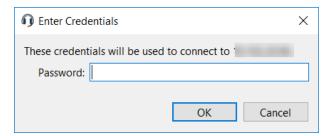
Choisissez une **règle de session** à attribuer à cet élément de Jump. La règle de session attribuée à cet élément de Jump a la priorité la plus élevée lors de la configuration des autorisations de session. Le fait de pouvoir définir ou non une règle de session dépend là encore des autorisations définies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



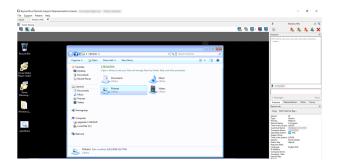
Utiliser un raccourci VNC

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

Lors de l'établissement de la connexion au serveur VNC, le système détermine si des informations d'authentification lui sont associées. Si tel est le cas, vous êtes invité à les saisir.



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





Remarque : il est possible de configurer les éléments de Jump pour permettre à plusieurs utilisateurs d'accéder au même élément de Jump en simultané. Si l'option **Rejoindre une session existante** est activée, d'autres utilisateurs sont susceptibles de rejoindre une session déjà en cours. Le propriétaire initial de la session reçoit une notification lui indiquant qu'un autre utilisateur a rejoint la session, mais il n'est pas autorisé à lui refuser l'accès.



Pour en savoir plus sur les Jumps simultanés, veuillez consulter <u>Paramètres d'élément de Jump</u> à l'adresse <u>www.beyondtrust.com/docs/remote-support/getting-started/admin/jump-items.htm.</u>



Réalisation d'un Shell Jump vers un périphérique réseau distant

La technologie Shell Jump permet de se connecter rapidement à un dispositif réseau SSH ou Telnet, afin d'en utiliser la fonction de ligne de commande. Vous pouvez, par exemple, exécuter un script normalisé sur plusieurs systèmes afin d'installer un correctif ou de résoudre un problème de réseau.

Pour effectuer un Shell Jump à travers BeyondTrust, vous devez avoir accès à un Jumpoint sur lequel Shell Jump est activé, et avoir l'autorisation de compte d'utilisateur **Méthodes de Jump autorisées : Shell Jump**.

Pour démarrer une session Shell Jump, ouvrez la boîte de dialogue Shell Jump à partir :

- du menu Assistance technique de la console du technicien d'assistance
- du bouton Shell Jump situé en haut de la console du technicien d'assistance

Votre Jumpoint peut être configuré pour un accès Shell Jump fourni uniquement.

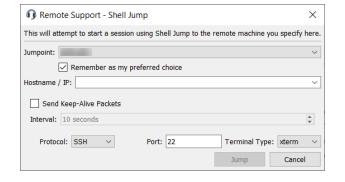
Dans la liste déroulante **Jumpoint**, sélectionnez le réseau qui héberge l'ordinateur auquel vous voulez accéder. Si vous accédez régulièrement au même Jumpoint, cochez **Enregistrer en tant que favori**. Sélectionnez le système provisionné auquel vous souhaitez accéder

Vous pouvez aussi configurer votre Jumpoint pour un accès ouvert ou un accès limité

Dans la liste déroulante **Jumpoint**, sélectionnez le réseau qui héberge l'ordinateur auquel vous voulez accéder. Si vous accédez régulièrement au même Jumpoint, cochez **Enregistrer en tant que favori**.

Pour accéder à un système fourni, cochez **Utiliser celui fourni** et sélectionnez le système dans le menu déroulant.

Vous pouvez aussi saisir le **nom d'hôte / IP** du système auquel vous souhaitez accéder. Si votre Jumpoint est configuré pour un accès limité, le système distant doit être dans la plage d'adresses IP délimitée.



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

Sélectionnez le **protocole** à utiliser, **SSH** ou **Telnet.Port** bascule automatiquement vers le port par défaut du protocole sélectionné, mais il peut être modifié en fonction de vos paramètres réseau.Sélectionnez le **type de terminal**, **xterm** ou **VT100**.

Cliquez ensuite sur Effectuer un Jump.

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

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





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



Créer et utiliser des raccourcis de Shell Jump

La technologie Shell Jump permet de se connecter rapidement à un dispositif réseau SSH ou Telnet, afin d'en utiliser la fonction de ligne de commande. Vous pouvez, par exemple, exécuter un script normalisé sur plusieurs systèmes afin d'installer un correctif ou de résoudre un problème de réseau.

Créer un raccourci de Shell Jump

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





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

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



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

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

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

Sélectionnez le protocole à utiliser, SSH ou Telnet.

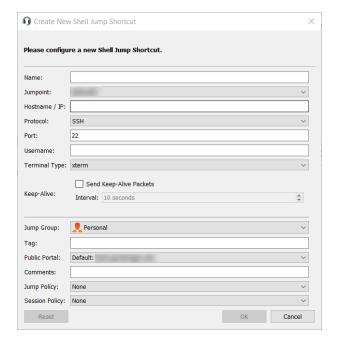
Port bascule automatiquement vers le port par défaut du protocole sélectionné, mais il peut être modifié en fonction de vos paramètres réseau.

Saisissez le nom d'utilisateur avec lequel se connecter.

Sélectionnez le type de terminal, xterm ou VT100.

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

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



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

TC: 7/18/2022



Sélectionnez le **portail public** à travers lequel cet élément de Jump doit se connecter. Si une règle de session est associée à ce portail public, celle-ci peut affecter les autorisations des sessions démarrées avec cet élément de Jump. Le fait de pouvoir définir ou non le portail public dépend également des autorisations définies pour votre compte.

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

Sélectionnez une **Règle de Jump** afin de définir quand les utilisateurs peuvent accéder à cet élément de Jump. Ces règles doivent être configurées par l'administrateur dans l'interface **/login**.

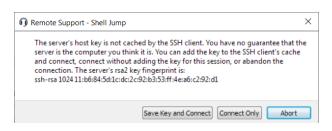
Choisissez une **règle de session** à attribuer à cet élément de Jump. La règle de session attribuée à cet élément de Jump a la priorité la plus élevée lors de la configuration des autorisations de session. Le fait de pouvoir définir ou non une règle de session dépend là encore des autorisations définies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

Utiliser un raccourci de Shell Jump

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

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

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



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



Assistance technique de systèmes Windows avec Intel® vPro

L'utilisation de la technologie de gestion active Intel[®] permet aux utilisateurs privilégiés de fournir une assistance technique aux systèmes Intel[®] vPro Windows totalement fournis sous le niveau du système d'exploitation, quel que soit le statut ou l'état de l'alimentation de ces systèmes distants. Pour utiliser Intel[®] vPro, vous devez avoir accès à un Jumpoint avec Intel[®] vPro activé et avoir l'autorisation du compte d'utilisateur **Méthodes de Jump autorisées : Intel[®] vPro**.



Remarque: les systèmes distants utilisant vPro avec AMT version 5 ou ultérieure peuvent être pris en charge par BeyondTrust.



Remarque: bien que vPro soit pris en charge par les Jumpoints en cluster, les options de configuration ne sont disponibles que pour les Jumpoints autonomes. Les Jumpoints en cluster n'ont pas d'option de configuration pour Intel® vPro.

Pour démarrer une session avec un système Intel[®] vPro, accédez à la boîte de dialogue Intel[®] vPro à partir :

- du menu Assistance technique de la console du technicien d'assistance
- du bouton Intel® vPro situé en haut de la console du technicien d'assistance

Dans la liste déroulante **Jumpoint**, sélectionnez le réseau qui héberge l'ordinateur auquel vous voulez accéder. Si vous accédez régulièrement au même Jumpoint, cochez **Enregistrer en tant que favori**. Saisissez le **nom d'hôte / IP** du système auquel vous souhaitez accéder.

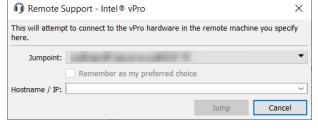
Cliquez ensuite sur Effectuer un Jump.

En fonction de votre configuration de Jumpoint, il pourra vous être demandé d'indiquer un nom d'utilisateur et un mot de passe.

Le Jumpoint détecte le matériel vPro fourni. Si les informations d'authentification fournies lors de la configuration du Jumpoint ou de la tentative de Jump correspondent à celles du système disposant de vPro, la connexion est établie.

Selon la façon dont l'ordinateur vPro est fourni, vous pouvez être invité à indiquer un code de consentement de l'utilisateur avant d'exécuter certaines actions.

Si un code de consentement est requis, une fenêtre contextuelle s'affiche sur l'écran distant. Un utilisateur final doit vous fournir ce code avant que vous puissiez accéder au matériel.

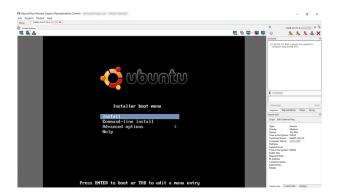








Une fois la connexion établie, vous aurez le contrôle du matériel vPro distant. Vous pouvez alors utiliser les outils de session vPro pour travailler sur le système distant.





Outils de session vPro



Réinitialisez la connexion vPro.



Éteignez ou allumez la machine hôte. Vous pouvez également redémarrer la machine hôte normalement, sur le BIOS, sur PXE ou sur une image disque sélectionnée.



Sélectionnez un fichier ISO ou IMG pour monter sur le système distant. L'emplacement du fichier est défini lors de la configuration du Jumpoint.



Démarrez ou arrêtez la consultation de l'affichage du système distant en utilisant KVM.



Envoyez Ctrl-Alt-Suppr à l'ordinateur distant.



Lors du partage d'écran, effectuez une capture d'écran du ou des écrans distants en résolution maximum, enregistrée au format PNG. Sauvegardez le fichier image sur votre système local ou votre presse-papiers. L'action de capture d'écran est enregistrée dans le journal de discussion avec un lien vers une image enregistrée localement. Le lien reste actif même après que le client a quitté la session, mais il n'est pas conservé dans le rapport de session BeyondTrust. Vous pouvez modifier le répertoire où les captures d'écran sont enregistrées en allant dans le menu **Fichier > Paramètres > Outils d'assistance technique** de la console du technicien d'assistance. Cette fonction est disponible sur Mac, Windows et Linux.



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.



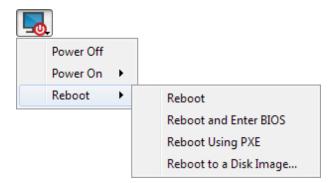
Définir le mode d'optimisation de la couleur d'affichage de l'écran distant. Si vous comptez principalement partager de la vidéo, sélectionnez **Vidéo optimisée** ; sinon, choisissez entre **Noir et blanc** (utilise moins de bande passante), **Quelques couleurs**, **Davantage de couleurs** ou **Toutes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



Affichez le bureau distant en mode plein écran ou revenez à l'affichage de l'interface.

Dans le menu **Redémarrage**, sélectionnez **Redémarrer et accéder au BIOS** pour démarrer le processus de démarrage du BIOS sur le système vPro distant. Vous aurez alors accès au BIOS pour le dépannage.

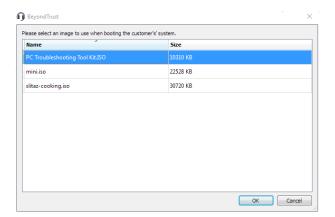
Sélectionnez **Redémarrer via PXE** pour démarrer le système distant en utilisant une interface réseau, indépendamment des périphériques de stockage de données ou des systèmes d'exploitation installés.





Redémarrer sur une image disque utilise IDE-R pour démarrer le système distant sur un fichier ISO ou IMG spécifié.

Remarque : le système distant affichera l'écran exactement tel que vous le voyez, même lorsque vous démarrez sur une autre page.





Créer et utiliser des raccourcis de Jump Intel vPro

L'utilisation de la technologie de gestion active Intel[®] permet aux utilisateurs privilégiés de fournir une assistance technique aux systèmes Intel[®] vPro Windows totalement fournis sous le niveau du système d'exploitation, quel que soit le statut ou l'état de l'alimentation de ces systèmes distants.

Créer un raccourci Intel® vPro

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



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

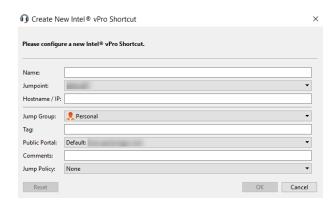


Remarque: pour voir les propriétés de plusieurs éléments de Jump, les éléments sélectionnés doivent tous être du même type (par ex. que des Jump Clients, que des Jump distants, etc.).

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

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

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



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

Sélectionnez le **portail public** à travers lequel cet élément de Jump doit se connecter. Si une règle de session est associée à ce portail public, celle-ci peut affecter les autorisations des sessions démarrées avec cet élément de Jump. Le fait de pouvoir définir ou non le portail public dépend également des autorisations définies pour votre compte.

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

Sélectionnez une **Règle de Jump** afin de définir quand les utilisateurs peuvent accéder à cet élément de Jump. Ces règles doivent être configurées par l'administrateur dans l'interface **/login**.

Utiliser un raccourci Intel® vPro

En fonction de votre configuration de Jumpoint, il pourra vous être demandé d'indiquer un nom d'utilisateur et un mot de passe.

Le Jumpoint détecte le matériel vPro fourni. Si les informations d'authentification fournies lors de la configuration du Jumpoint ou de la tentative de Jump correspondent à celles du système disposant de vPro, la connexion est établie.

TC: 7/18/2022



Selon la façon dont l'ordinateur vPro est fourni, vous pouvez être invité à indiquer un code de consentement de l'utilisateur avant d'exécuter certaines actions.

Si un code de consentement est requis, une fenêtre contextuelle s'affiche sur l'écran distant. Un utilisateur final doit vous fournir ce code avant que vous puissiez accéder au matériel.

Une fois la connexion établie, vous aurez le contrôle du matériel vPro distant. Vous pouvez alors utiliser les outils de session vPro pour travailler sur le système distant.









Remarque : il est possible de configurer les éléments de Jump pour permettre à plusieurs utilisateurs d'accéder au même élément de Jump en simultané. Si l'option **Rejoindre une session existante** est activée, d'autres utilisateurs sont susceptibles de rejoindre une session déjà en cours. Le propriétaire initial de la session reçoit une notification lui indiquant qu'un autre utilisateur a rejoint la session, mais il n'est pas autorisé à lui refuser l'accès.

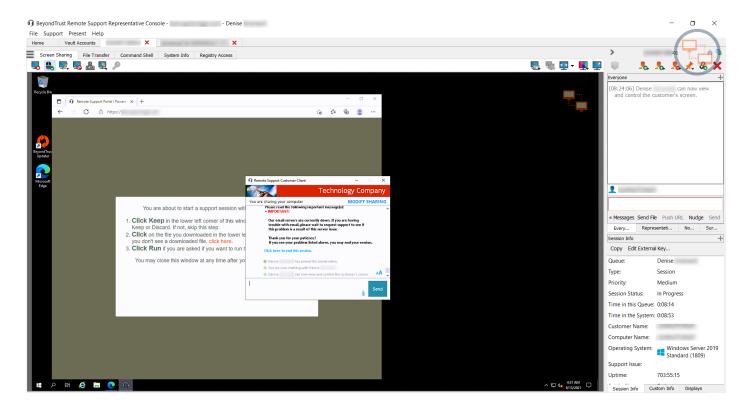


Pour en savoir plus sur les Jumps simultanés, veuillez consulter <u>Paramètres d'élément de Jump</u> à l'adresse www.beyondtrust.com/docs/remote-support/getting-started/admin/jump-items.htm.



Boîte à outils

Vue d'ensemble des sessions d'assistance technique et outils





Outils de session

_	
$\overline{}$	

Cliquez sur l'icône de menu en haut à gauche de la fenêtre de session pour accéder aux contrôles de session pour votre session. Vous pouvez aussi faire un clic droit sur l'onglet de session pour accéder aux contrôles de session.

Plusieurs de ces contrôles possèdent des icônes dédiées ailleurs dans l'interface et sont décrits ci-dessous (Accroître les droits, Transférer, Inviter, Déconnecter un participant, Déployer un bouton d'assistance technique, Déployer un Jump Client, Liens personnalisés, Fermer).

Depuis le menu, sélectionnez **Détacher l'onglet Session** pour séparer la session de la console, ou cliquez sur l'onglet de session et faites-le glisser en dehors de la fenêtre principale. L'icône de menu reste avec votre session même lorsque vous détachez l'onglet de session, ce qui vous permet de positionner l'onglet de session où vous voulez, y compris sur un écran différent, tout en conservant l'accès aux outils de session. Rattacher la session en utilisant l'option **Attacher l'onglet Session** dans le menu, ou en cliquant simplement sur le X pour fermer la fenêtre détachée.

De plus, depuis le menu, sélectionnez **Localiser la barre latérale** pour trouver la barre latérale de cette session, ce qui peut être utile si vous avez plusieurs barres latérales de session détachées (voir ci-dessous) éparpillées sur votre écran.

Vous pouvez également renommer la session ou rétablir le nom par défaut.





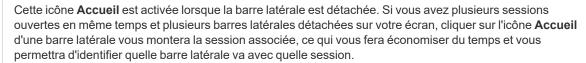
Réduisez la barre latérale pour agrandir vote espace de travail de session. Pour épingler à nouveau la barre latérale, survolez la flèche de la barre latérale réduite et cliquez sur l'icône **Épingler la barre latérale**.





Cliquez sur cette icône pour détacher la barre latérale. Une fois détachée, la barre latérale peut être placée n'importe où sur votre bureau ou sur un écran différent. La barre latérale peut aussi être redimensionnée selon vos besoins. Vous pouvez aussi redimensionner les volets de la barre latérale pour avoir plus d'espace. Cliquez sur l'icône **Attacher la barre latérale** pour rattacher la batte latérale. Lorsque la barre latérale est détachée, l'icône **Accueil** est activée (voir ci-dessous).









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







Accroissez les droits d'une session cliquer-pour-messagerie instantanée en un client d'utilisateur intégral, ou accroissez les droits du client d'utilisateur pour qu'il ait les droits d'administrateur en cliquant sur le bouton en forme de bouclier. Sélectionnez **Demander l'accord du client** pour demander les informations d'authentification d'admin à l'utilisateur distant. Si vous avez les informations d'authentification d'administrateur pour l'ordinateur distant, sélectionnez **Utilisateur spécifique** pour fournir vous-même un nom d'utilisateur et un mot de passe administratifs.

L'accroissement des droits du client d'utilisateur permet de permuter des comptes utilisateur, de déployer des Jump Clients en mode service, et de contrôler les fenêtres et les boîtes de dialogue de contrôle de compte utilisateur protégées. L'accroissement des droits ne modifie pas le contexte de l'utilisateur actif et ne revient pas à déconnecter l'utilisateur actif pour le reconnecter en tant qu'administrateur.

La fonction d'accroissement vers des droits administrateur est actuellement disponible pour les ordinateurs Windows et Mac uniquement. Un administrateur peut configurer le client d'utilisateur de sorte à demander automatiquement l'accroissement des droits lors de l'ouverture d'une session sur un système Windows.



Si vous estimez qu'une autre personne est plus compétente pour gérer une session, transférez le contrôle de cette session à une autre équipe ou un autre utilisateur. Restez comme participant ou fermez l'onglet pour laisser la session à son nouveau propriétaire. Une fois que vous avez transféré la session à un nouveau propriétaire, vos icônes **Transférer**, **Partager** et **Supprimer** seront grisées et vous ne pourrez plus effectuer ces actions, car vous n'êtes plus le propriétaire de cette session. La session persistera jusqu'à ce que le nouveau propriétaire y mette fin.



Invitez un autre utilisateur à participer à une session partagée. Vous restez propriétaire de la session, mais vous pouvez recevoir l'avis d'un ou de plusieurs membres de votre équipe ou d'un utilisateur externe.

Vous pouvez également demander à un parrain d'accès de réaliser certaines actions en votre nom.



Le propriétaire de la session peut supprimer un autre utilisateur d'une session partagée. Vous pouvez également déconnecter l'utilisateur mais conserver l'onglet de session afin d'ajouter des notes ou de consulter les dernières informations système collectées.





Si vous y êtes autorisé, installez un **bouton d'assistance technique** sur le bureau distant, ou supprimez un bouton d'assistance technique précédemment installé. Le client peut cliquer sur le **bouton d'assistance technique** pour démarrer rapidement et facilement une session d'assistance technique.





Si vous y êtes autorisé, installez un Jump Client sur l'ordinateur distant pour permettre aux membres de votre équipe ou à vous-même d'accéder ultérieurement à ce système sans l'intervention de l'utilisateur final. Désinstallez le client si vous n'avez plus besoin d'accéder à ce système en mode autonome. Pour définir les détails, tels que le mot de passe, les commentaires, le groupe, etc., sélectionnez **Personnaliser**.



Ouvrez un navigateur Internet sur votre ordinateur sur n'importe quel site défini par votre administrateur. Ce bouton peut être configuré pour inclure des informations détaillées sur la session, le client final et/ou l'utilisateur BeyondTrust qui ouvre le lien personnalisé. Si, par exemple, la clé externe correspond à l'identificateur unique d'un dossier dans votre système GRC, le fait de cliquer sur ce bouton pourrait afficher le dossier associé dans le système externe.



Lorsqu'un appareil iOS compatible est détecté, l'icône d'**actions spéciales** apparaît, permettant au technicien d'assistance d'envoyer des instructions de partage d'écran iOS à l'appareil.



Fermez complètement l'onglet de session. Si vous êtes le propriétaire de cette session, vous pouvez au choix désinstaller le client d'utilisateur depuis la machine distante ou laisser l'utilisateur dans la file d'attente pour qu'un autre technicien d'assistance poursuive la session. Vous pouvez fermer la session depuis la barre latérale, le menu de session ou l'onglet de session.



Les informations relatives au système distant, ainsi que toutes les informations fournies par l'utilisateur par le biais du formulaire de soumission de problème sont affichées dans l'angle inférieur droit de la fenêtre de session. Ceci peut inclure les éléments suivants :

- Type : le type de session.
- **Priorité** : le niveau de priorité (bas, moyen (par défaut), ou élevé) de la demande, en fonction des problèmes d'assistance technique définis par votre administrateur BeyondTrust.
- File d'attente : la file d'attente personnelle du technicien d'assistance à qui appartient la session.
- État de la session : en attente (aucun technicien d'assistance n'a rejoint la session), en cours (le technicien d'assistance et le client ont rejoint la session), ou client absent (le technicien d'assistance est arrivé mais le client est parti).
- Nom d'utilisateur : c'est le nom saisi par le client au démarrage de la session, le nom d'utilisateur de l'utilisateur connecté, le nom d'hôte de la machine du client (pour les sessions chargées et épinglées), ou le service (pour les sessions aux droits accrus).
- Nom de l'ordinateur : le nom d'hôte de la machine du client tel qu'indiqué dans les paramètres système.
- Plate-forme : le système d'exploitation de la machine du client
- Problème d'assistance technique : si un problème était sélectionné, cela indique le nom du problème sélectionné par le client.
- Temps passé dans le système : ceci mesure le temps écoulé depuis que la session est entrée dans sa première file d'attente.
- **Site public** : cela est généralement indiqué comme étant Par défaut ; cependant, si des sites non par défaut sont présents, d'autres sites peuvent être disponibles.
- Compétences requises : compétences associées avec le problème spécifique sélectionné par le client. Les compétences sont créées et associées à des problèmes par l'administrateur BeyondTrust depuis l'interface /login de BeyondTrust.
- Adresse IP: l'adresse IP publique et/ou privée du système local du client.

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

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



Pour en savoir plus sur le partage d'écran sur iOS, veuillez consulter <u>Partage d'écran avec l'appareil iOS</u> à l'adresse <u>https://www.beyondtrust.com/docs/remote-support/getting-started/customer-client/apple-ios/ios-screen-sharing.htm.</u>



Connexion aux systèmes en utilisant l'injection d'informations d'authentification depuis la Console du technicien d'assistance

Lorsque vous accédez à un élément de Jump sur Windows dans la Console du technicien d'assistance, 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 Remote Support BeyondTrust.



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

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

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



Remarque: l'ECM doit être installé sur votre système pour activer le service ECM BeyondTrust et pour utiliser l'injection d'informations d'authentification dans Remote Support BeyondTrust.

Configuration requise

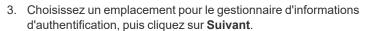
- · Windows Vista® ou supérieur, 64 bits seulement
- · .NET 4.5 ou supérieur
- Processeur: 2 GHz ou plus
- Mémoire : 2 Go ou plus
- Espace disponible sur le disque : 80 Go ou plus
- 1. Pour commencer, téléchargez le gestionnaire d'informations d'authentification de point de terminaison (ECM) BeyondTrust auprès de <u>l'assistance technique BeyondTrust</u> à l'adresse <u>https://www.beyondtrust.com/docs/index.htm#support</u>. Lancez l'assistant de configuration du gestionnaire d'informations d'authentification de point de terminaison BeyondTrust.

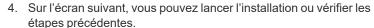


 Acceptez les conditions générales du CLUF. Cochez la case si vous acceptez, puis cliquez sur Installer. Si vous souhaitez modifier le chemin d'installation, cliquez sur le bouton Options pour le choisir.



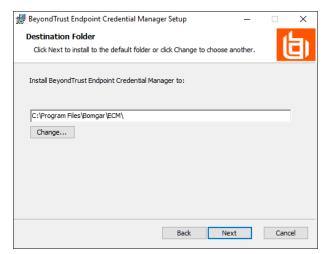
Remarque : vous ne pourrez pas poursuivre l'installation si vous n'acceptez pas le CLUF.

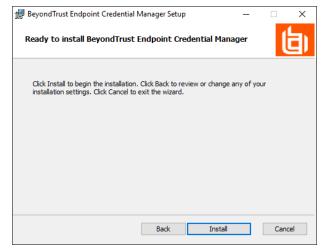




5. Cliquez sur **Installer** lorsque vous êtes prêt à commencer.

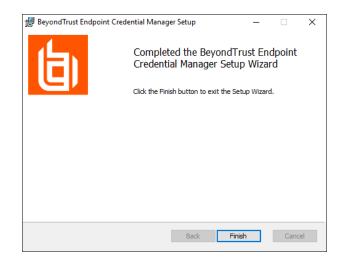








 L'installation prendra quelques instants. Sur cet écran, cliquez sur Terminé.





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 BeyondTrust Appliance B Series. Une liste des ECM connectés au site de la B Series Appliance est disponible sur /login > État > Information > Clients ECM.



Remarque : lorsque plusieurs ECM sont connectés au site BeyondTrust, le B Series Appliance achemine les demandes vers le ECM ayant été le plus longtemps connecté à la B Series Appliance.



Remarque: si vous recevez une erreur de plug-in Windows pendant l'installation, trouvez et débloquez le fichier **BomgarVaultRestPlugin.dll**.

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

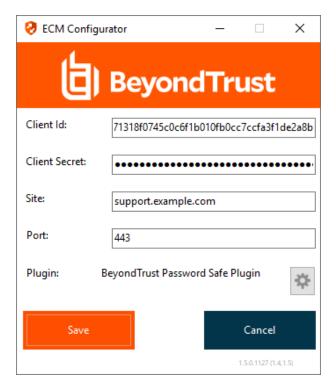
En utilisant le configurateur ECM, établissez une connexion à votre magasin d'informations d'authentification.

- 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**.
- Lancez le programme pour commencer l'établissement d'une connexion.

→ BeyondTrust-ECMConfigurator.exe	7/23/2019 2:35 PM	Application	317 KB
BeyondTrust-ECMConfigurator.exe.config	7/23/2019 2:35 PM	CONFIG File	1 KB
BeyondTrust-ECMService.exe	7/23/2019 2:35 PM	Application	26 KB
BeyondTrust-ECMService.exe.config	7/23/2019 2:35 PM	CONFIG File	2 KB
Configurator.log	11/14/2019 3:06 PM	Text Document	3 KB
ECM.dll	7/23/2019 2:35 PM	Application exten	65 KB
ECM.log	11/14/2019 3:06 PM	Text Document	4 KB
ECSM.settings	7/23/2019 2:35 PM	SETTINGS File	1 KB
log4net.dll	7/23/2019 2:35 PM	Application exten	294 KB
Newtonsoft.Json.dll	8/3/2014 9:33 PM	Application exten	491 KB
₩ Util.dll	7/23/2019 2:35 PM	Application exten	31 KB



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 d'admin pour votre magasin d'informations d'authentification.
Secret de client	La clé secrète d'admin 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.

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



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



IMPORTANT!

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

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

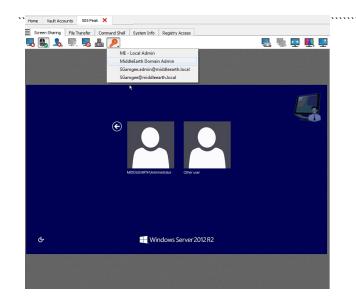
Une fois que le magasin d'informations d'authentification a été configuré et qu'une connexion a été établie, la console du technicien d'assistance peut commencer à utiliser les informations d'authentification du magasin d'informations d'authentification pour se connecter à des systèmes distants.

- 1. Connectez-vous à la console du technicien d'assistance.
- 2. Effectuez un Jump vers un système distant avec un élément de Jump installé comme service accru sur une machine Windows.
- 3. Appuyez sur le bouton **Lecture** pour commencer le partage d'écran avec le système distant. Si le système distant est sur l'écran de connexion de Windows, le bouton **Injecter des informations d'authentification** est en surbrillance.
- 4. Cliquez sur le bouton **Injecter des informations d'authentification**. Un dialogue de sélection d'informations d'authentification apparaît, répertoriant les informations d'authentification disponibles pour ECM.





- 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.
- Le technicien d'assistance est connecté au système distant.



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

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

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



Remarque: lors de l'utilisation de BeyondTrust Vault, le nombre maximal d'informations d'authentification pouvant s'afficher dans le menu déroulant est de 2 000. Lors de l'utilisation du GIAPT. la limite est de 200.

Extraire et injecter des informations d'authentification Vault

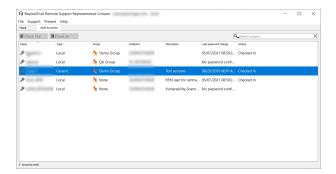
Vous pouvez facilement accéder à Remote Support Vault directement depuis la console du technicien d'assistance. Cela vous permet d'extraire ou d'injecter des informations d'authentification lorsque c'est nécessaire, durant une session ou sur votre machine locale.



TC: 7/18/2022



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

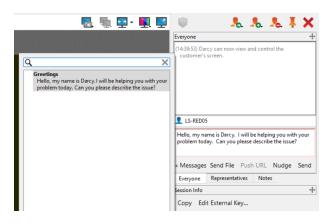




Messagerie instantanée avec un utilisateur lors d'une session

Tout au long de la session d'assistance technique, vous pouvez discuter avec votre client distant. Vous n'avez pas besoin d'une autorisation de partage d'écran pour commencer une session de messagerie instantanée. Si cette option est activée dans les paramètres de la console du technicien d'assistance, vous verrez des notifications contextuelles lorsque vous recevrez des messages instantanés. Si vous avez envoyé votre photo ou un avatar, cette image sera affichée dans la fenêtre de messagerie instantanée du client une fois la messagerie instantanée lancée.

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



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

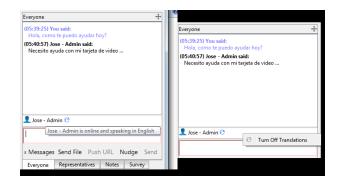
Si la traduction en temps réel de la messagerie instantanée est activée, les clients peuvent discuter avec un technicien d'assistance dans leur propre langue. Par exemple, un client dont la langue principale est l'anglais peut discuter avec un technicien d'assistance qui ne parle que néerlandais, les messages étant traduits automatiquement en temps réel.



Remarque : Actuellement, la messagerie instantanée à traduction en temps réel BeyondTrust Remote Support prend en charge l'allemand, l'espagnol (Amérique latine), l'espagnol (européen), le finnois, le français, l'italien, le japonais, le néerlandais, le polonais, le portugais (Brésil), le portugais (Portugal), le russe, le suédois, le turc, le chinois et le chinois simplifié.

Laisser le pointeur de la souris sur le nom du technicien d'assistance montre la langue utilisée pour traduire les messages envoyés au client. Dans cet exemple, le technicien d'assistance apparaît *en ligne et parlant anglais*, bien qu'il écrive en espagnol.

Vous pouvez désactiver les traductions en faisant un clic droit sur l'icône de traduction puis en cliquant sur **Désactiver les traductions**. Pour réactiver les traductions, faites un clic droit sur l'icône pus cliquez sur **Activer les traductions**. Le client ne peut pas désactiver le processus de traduction de son côté.



Si votre administrateur a configuré des messages prédéfinis, vous pouvez cliquer sur le bouton **Messages** situé en bas à gauche de la fenêtre de messagerie instantanée pour insérer des messages écrits à l'avance dans la discussion. Cliquez sur la flèche située à gauche d'une catégorie pour afficher les messages et sous-catégories associés. Saisissez du texte dans la zone de recherche afin de rechercher un message spécifique.

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

TC: 7/18/2022



Pour charger un fichier dans l'interface de messagerie instantanée, cliquez sur le bouton **Envoyer un fichier**. Le chargement d'une URL dans l'interface de messagerie instantanée ouvre automatiquement un navigateur sur le système distant et le dirige vers le site désigné. Pour charger une URL, l'adresse Web doit être le seul texte saisi dans le champ.

Pour attirer l'attention de votre client, cliquez sur **Envoyer un wizz**. Cela permet de donner la main au client d'utilisateur, d'envoyer une vibration au client d'utilisateur et de faire retentir une alerte sonore sur le système distant. Le wizz est connecté dans l'historique de la messagerie instantanée. Après avoir envoyé un wizz, vous devez patienter plusieurs secondes avant d'en envoyer un autre.

La fenêtre de messagerie instantanée enregistre non seulement les messages et l'heure à laquelle ils ont été envoyés, mais elle fait également office de journal pour tous les événements de la session, y compris les fichiers transférés et les autorisations accordées.

Si un ou plusieurs techniciens d'assistance partagent la session, vous pouvez choisir de discuter avec tous les participants ou de discuter en privé avec les techniciens d'assistance uniquement.Lorsqu'un utilisateur supplémentaire rejoint une session partagée, il a accès à tout l'historique de la discussion.

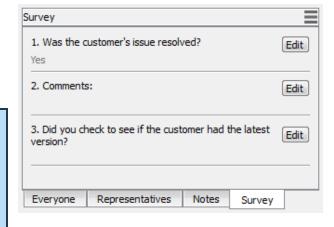
Vous pouvez aussi ajouter des notes sur la session. Si cette dernière est partagée ou transférée, ces notes peuvent être soumises par un technicien d'assistance et extraites par un autre pour une analyse rapide et confidentielle de la situation. Ces remarques sont également disponibles dans le rapport de session. Des notes peuvent être ajoutées pendant la session et également après la fin de la connexion distante.

T.5. Eliot 03/22/2015 16:16:52 PM The necessary software has been uploaded, but while it's installing, Alfred won't be able to work. I've installed a Jump Client and will finish the process once Alfred has left the office. Add Refresh Everyone Representatives Notes Survey

Votre administrateur peut aussi décider de vous autoriser à accéder à l'enquête de satisfaction du technicien d'assistance lors d'une session. Dans ce cas, l'enquête peut être utilisée comme modèle de flux de travail, ce qui permet à votre administrateur de publier une série de questions et/ou de cases à cocher, ainsi que des liens spécifiques que vous pourrez utiliser dans votre session d'assistance technique.



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





Pour plus d'informations, veuillez consulter :

• <u>Traduction de la messagerie instantanée en temps réel</u> à l'adresse <u>https://www.beyondtrust.com/docs/remote-support/videos/real-time-chat-translation.htm</u>



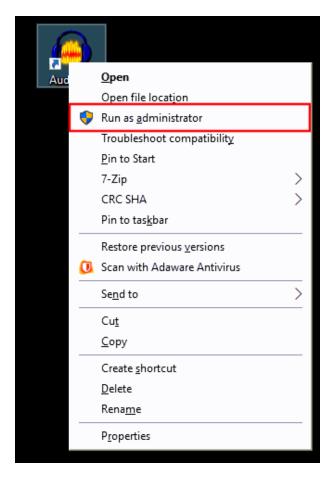


- Messagerie instantanée en temps réel : traduire les messages instantanés entre le technicien d'assistance et le client à l'adresse https://www.beyondtrust.com/docs/remote-support/getting-started/admin/real-time-chat.htm
- Référence des balises BBCode à l'adresse https://www.bbcode.org/reference.php



Accroître le client

L'accroissement des droits du client d'utilisateur permet de permuter des comptes utilisateur, de déployer des Jump Clients en mode service, et de contrôler les fenêtres et les boîtes de dialogue de contrôle de compte utilisateur protégées. L'accroissement des droits ne modifie pas le contexte de l'utilisateur actif et ne revient pas à déconnecter l'utilisateur actif pour le reconnecter en tant qu'administrateur. Une fois que vous avez accru une session, vous pouvez déconnecter l'utilisateur actuel et le reconnecter avec un compte d'administrateur, ou utiliser **Exécuter en tant qu'administrateur** pour exécuter des commandes et des programmes dans un contexte d'utilisateur administrateur.



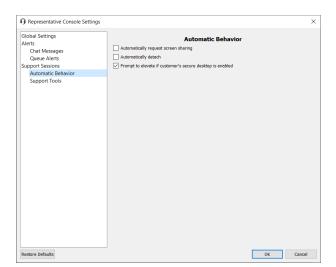
Accroissement des droits

Pour accroître les droits du client d'utilisateur afin de lui donner des droits d'administration, cliquez sur le bouton **Accroître les droits** en haut de la fenêtre de session.



Une invite pour des informations d'authentification d'administration s'affiche. Une invitation à accroître les droits apparaîtra aussi si le technicien d'assistance tente d'effectuer une action qui requiert des droits d'administration dans une session non accrue.

Vous pouvez aussi configurer les paramètres dans la console du technicien d'assistance afin que l'utilisateur de l'appareil distant soit automatiquement invité à accroître les droits si leur bureau est sécurisé. Ce paramètre se trouve dans Fichier > Paramètres > Sessions d'assistance technique > Comportement automatique. Ce paramètre peut également être configuré de façon globale dans l'interface /login sur la page Console du technicien d'assistance > Paramètres de la console du technicien d'assistance dans Gérer les paramètres de la console du technicien d'assistance.



i

Pour plus d'informations sur l'accroissement des droits, veuillez consulter les articles suivants :

- Accroître la session dans la console Web du technicien d'assistance à l'adresse https://www.beyondtrust.com/docs/remote-support/getting-started/rep-console/web/elevate.htm
- Accroître les droits dans le client d'utilisateur depuis la console du technicien d'assistance Androidà l'adresse https://www.beyondtrust.com/docs/remote-support/getting-started/rep-console/android/elevate.htm
- Accroître les droits dans le client d'utilisateur depuis la console du technicien d'assistance iOSà l'adresse https://www.beyondtrust.com/docs/remote-support/getting-started/rep-console/ios/elevate.htm
- Installer un Jump Client, un Jumpoint ou un service d'accroissement pour le lancement d'une session accrue à l'adresse https://www.beyondtrust.com/docs/remote-support/how-to/smart-card/jump-client-installation.htm



Partage d'écran avec l'utilisateur distant à des fins de consultation et de contrôle

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



Options de partage d'écran

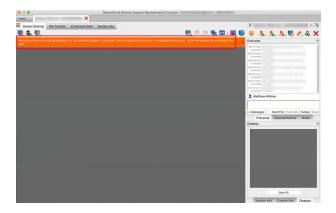
- Le fait de laisser toutes les options désélectionnées entraîne une demande de partage d'écran complet, qui offre un accès visuel et de contrôle à l'intégralité du bureau et des applications du système distant.
- Si vous cochez Accès complet, disponible uniquement lors de sessions lancées par un client, vous demanderez le partage d'écran et tous les privilèges à la fois.
- Notez que si vous cochez la case Voir uniquement, vous pourrez voir l'écran distant mais vous n'en aurez pas le contrôle.
- L'option Écran de confidentialité, disponible uniquement en cas de Jump, permet d'initier la session avec l'affichage et le contrôle du système de l'utilisateur distant désactivés. L'écran de confidentialité n'est pas disponible lors d'une assistance technique sur Windows 8.
- L'option **Sélection des applications partagées par le client**, disponible uniquement lors d'une assistance technique à un ordinateur Windows ou Mac, permet au client de limiter les applications partagées.

Si votre administrateur a défini votre compte pour exiger que l'utilisateur sélectionne les applications à partager, vous ne pouvez demander qu'un partage d'écran limité. De la même façon, vous pouvez uniquement être autorisé à demander un partage d'écran complet, ou vous pouvez être autorisé à choisir le niveau d'accès que vous souhaitez demander.



Remarque : un paramètre s'appliquant à l'intégralité du site peut autoriser votre utilisateur à limiter des applications après avoir commencé le partage d'écran, quel que soit le niveau de la demande d'accès.

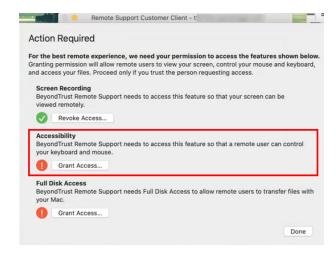
Pour les systèmes macOS Catalina (10.15) +, si le contrôle à distance n'est pas activé, cliquez sur la bannière en haut de l'onglet **Partage d'écran** pour demander au client des autorisations.



TC: 7/18/2022



Le client peut alors accorder l'accès lorsqu'il y est invité dans le client d'utilisateur, et le technicien d'assistance est dirigé vers les volets appropriés dans **Paramètres** pour mettre à jour les autorisations.



Une fois que l'utilisateur vous a donné l'autorisation, les applications autorisées sur le bureau distant apparaissent dans votre fenêtre. L'utilisateur peut choisir de vous accorder un accès Voir uniquement ou, si vos permissions l'autorisent, un contrôle total du clavier et de la souris pour que vous puissiez travailler sur l'ordinateur distant comme si vous y étiez. Vous pouvez demander à accroître votre niveau d'autorisation à tout moment au cours de la session.

Au cours d'une session en mode cliquer-pour-messagerie instantanée, vous pouvez uniquement discuter avec l'utilisateur et accéder aux informations de session de base. Si vous avez besoin d'offrir une assistance technique plus poussée, vous devez demander l'accroissement des droits de la session afin de disposer des droits complets du client d'utilisateur.





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 côté client explique clairement que le technicien d'assistance a désactivé l'affichage du client. Le client peut reprendre le contrôle à tout moment en appuyant sur **Ctrl+Alt+Suppr**.

Vous pouvez également désactiver le clavier et la souris du client tout en lui permettant de voir l'écran. Lorsque la saisie au clavier et à la souris est restreinte, une bordure orange apparaît autour des écrans du client, et un message indique que le technicien d'assistance possède le contrôle de la souris et du clavier. Le client 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 vers un ordinateur macOS ou Windows. Dans Windows Vista et les versions supérieures, le client d'utilisateur doit être accru. Sous Windows 8, l'écran de confidentialité n'est pas disponible, et le technicien d'assistance peut seulement désactiver le clavier et la souris.



Vous pouvez utiliser les outils d'annotation pour guider les utilisateurs à travers des tâches complexes et pour former des employés à distance, réduisant ainsi le nombre de rappels ainsi que les coûts de formation. Plusieurs outils sont disponibles, notamment les formes et le dessin libre. BeyondTrust InSight permet de dessiner des annotations sur une diffusion en direct depuis un appareil Android ou iOS. Notez que les annotations ont des exigences spéciales pour certaines plates-formes mobiles. Pour en savoir plus sur BeyondTrust InSight, veuillez consulter BeyondTrust InSight pour iOS ou BeyondTrust InSight pour Android.



Redémarrez le système distant en mode normal ou sans échec avec prise en charge réseau, ou éteignez-le. Vous pouvez également demander à l'utilisateur final d'entrer des informations d'authentification valides pour qu'après un redémarrage, le technicien d'assistance puisse se connecter avec les informations fournies sans que l'utilisateur soit présent. Pour plus de détails, consultez « Informations d'authentification pour connexion automatique : redémarrage et reconnexion », page 127.



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. Lors du fonctionnement mode accru, certaines actions peuvent être exécutées dans un contexte système. Vous pouvez aussi fournir les informations d'authentification d'un utilisateur administratif pour réaliser une action spéciale dans ce contexte utilisateur. Les scripts prédéfinis à la disposition de l'utilisateur apparaissent dans un menu flottant.



Vous avez accès à une liste répertoriant les lecteurs de cartes à puce disponibles sur votre système local. Utilisez une carte à puce virtuelle pour réaliser des actions administratives, exécuter des programmes dans un autre contexte utilisateur ou encore vous connecter avec d'autres informations d'authentification utilisateur. Pour utiliser les informations d'authentification de carte à puce sur un système distant, vous devez démarrer une session en utilisant un Jump Client ayant des droits accrus, un Jumpoint ou un Jump local sur réseau. Les pilotes de carte à puce virtuelle appropriés doivent néanmoins être installés à la fois sur le système local et sur le système distant, avec les services en cours d'exécution.





Lancez le partage d'écran sur appareil iOS. Pour plus de détails, veuillez consulter Assistance technique sur appareils iOS Apple à l'adresse www.beyondtrust.com/docs/remote-support/getting-started/customer-client/apple-ios/index.htm. Lors de l'assistance technique d'un système Apple OS X 10.10+ attaché à un appareil mobile Apple iOS 8.0.1+, cliquez sur ce bouton pour lancer ou terminer un partage d'écran en mode accès visuel uniquement sur l'appareil iOS connecté. Notez que ce bouton n'est visible que si vous êtes dans une session d'assistance technique de partage d'écran standard avec un système Apple OS X Yosemite, et que le bouton n'est activé que si un appareil Apple iOS 8.0.1+ est connecté au système OS X Yosemite en cours d'assistance technique.



Lors du partage d'écran, effectuez une capture d'écran du ou des écrans distants en résolution maximum, enregistrée au format PNG. Sauvegardez le fichier image sur votre système local ou votre presse-papiers. L'action de capture d'écran est enregistrée dans le journal de discussion avec un lien vers une image enregistrée localement. Le lien reste actif même après que le client a quitté la session, mais il n'est pas conservé dans le rapport de session BeyondTrust. Vous pouvez modifier le répertoire où les captures d'écran sont enregistrées en allant dans le menu **Fichier > Paramètres > Outils d'assistance technique** de la console du technicien d'assistance. Cette fonction est disponible sur Mac, Windows et Linux.



Envoyez manuellement le contenu de votre presse-papiers vers l'ordinateur distant. Cet outil n'est pas visible si vous êtes autorisé à envoyer automatiquement le contenu de votre presse-papiers ou si, au contraire, vous n'êtes pas autorisé à envoyer des informations de presse-papiers au système distant.



Recevez manuellement le contenu de votre presse-papiers depuis l'ordinateur distant. Cet outil n'est pas visible si vous êtes autorisé à recevoir automatiquement le contenu de votre presse-papiers ou si, au contraire, vous n'êtes pas autorisé à recevoir des informations de presse-papiers du système distant.



Sélectionnez un autre écran distant à afficher. Notez que le moniteur principal est désigné par la lettre P.



Visualisez l'écran distant à sa taille réelle ou mis à l'échelle.



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



Utilisation d'annotations sur l'écran distant.

Vous pouvez utiliser les outils d'annotation pour guider les utilisateurs à travers des tâches complexes et pour former des employés à distance, réduisant ainsi le nombre de rappels ainsi que les coûts de formation. Les techniciens d'assistance peuvent ainsi s'occuper des utilisateurs de façon interactive, tout en réduisant les situations de frustration potentielles et en augmentant la satisfaction des utilisateurs.

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

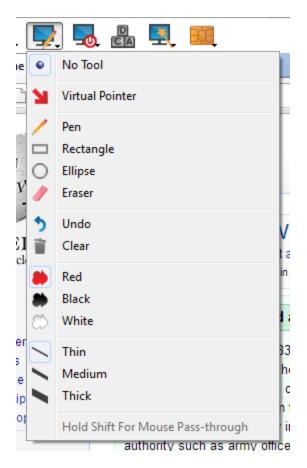
Activation des annotations

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



Cliquez sur les objets du menu déroulant pour activer le mode **Annotations**. Vous pouvez sélectionner des outils pour vous aider à guider un utilisateur à travers une série d'étapes, ou pour améliorer une session de formation. Les fonctions et outils suivants sont disponibles :

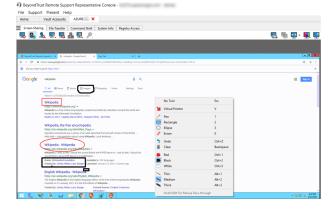
- Pointeur virtuel
- Stylo
- Outil Rectangle
- Outil Ellipse
- Effaceur
- Annuler
- Effacer
- Couleur rouge, noire ou blanche
- Trait fin, moyen ou épais





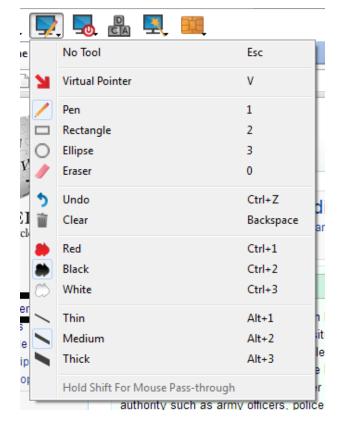
Vous pouvez sélectionner votre outil dans le menu déroulant des **Annotations**, ou en effectuant un clic droit dans la zone de l'écran distant. Si vous cliquez sur les zones en dehors de l'écran distant, le menu déroulant ne s'affichera pas.

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



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

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



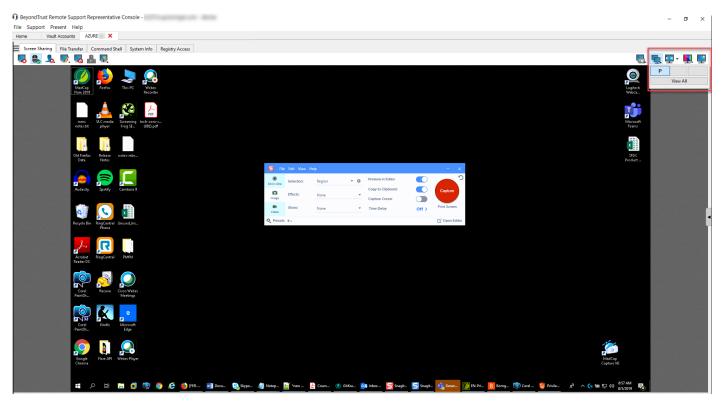
i

Les annotations sont également disponibles pendant les présentations. Pour plus d'informations, reportez-vous à « Réaliser une présentation pour des participants distants », page 99.



Affichage de moniteurs multiples sur un système distant

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



Utilisation de l'icône Affichage

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

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



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



TC: 7/18/2022



Assistance technique multimoniteur lors d'une session RDP

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



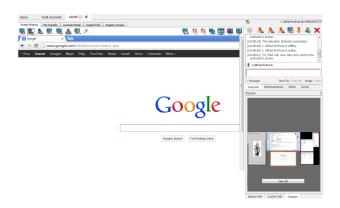


Remarque: si vous utilisez la vue plein écran tout en utilisant cette fonction, le système distant s'affiche sur tous vos moniteurs.

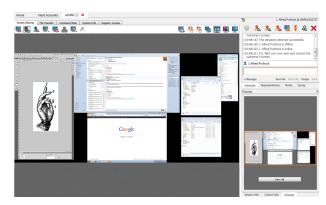
Utilisation de l'onglet Écrans

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

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



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

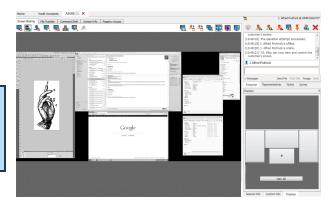




Si la session est en mode niveaux de gris, les moniteurs distants sont représentés par des rectangles plutôt que par des miniatures. La position de chaque rectangle correspond à la position configurée pour chaque moniteur sur le bureau distant.



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



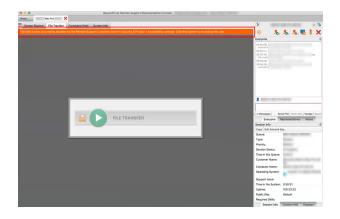


Transfert de fichiers vers et depuis un système distant

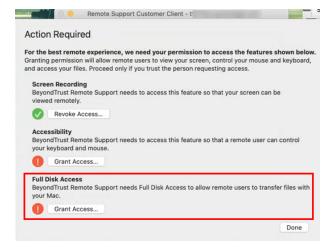
Au cours d'une session, les utilisateurs privilégiés peuvent transférer, supprimer ou renommer des fichiers, et même de répertoires entiers, depuis et vers l'ordinateur distant, depuis l'appareil distant, et depuis et vers la carte SD de l'appareil. Il n'est pas nécessaire d'avoir le contrôle total de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

Pour les systèmes macOS Catalina (10.15) +, si le partage d'écran n'est pas activé, cliquez sur la bannière en haut de l'onglet **Transfert de fichiers** pour demander au client l'autorisation de transférer des fichiers.

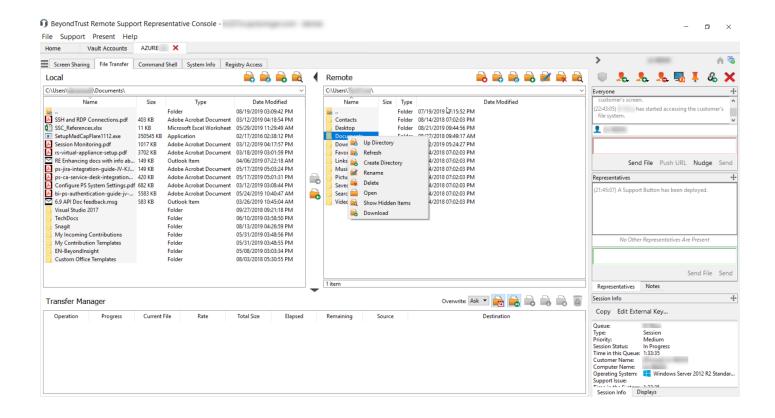


Le client peut alors accorder l'accès lorsqu'il y est invité dans le client d'utilisateur, et le technicien d'assistance est dirigé vers les volets appropriés dans **Paramètres** pour mettre à jour les autorisations.



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

<u></u>	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, Il n'est pas envoyé vers la corbeille dans un tel cas.
ā	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.
Ask ▼	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.
14	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.
<u></u>	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.
<u></u>	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.
4	Effacez toutes les informations depuis le gestionnaire des transferts.



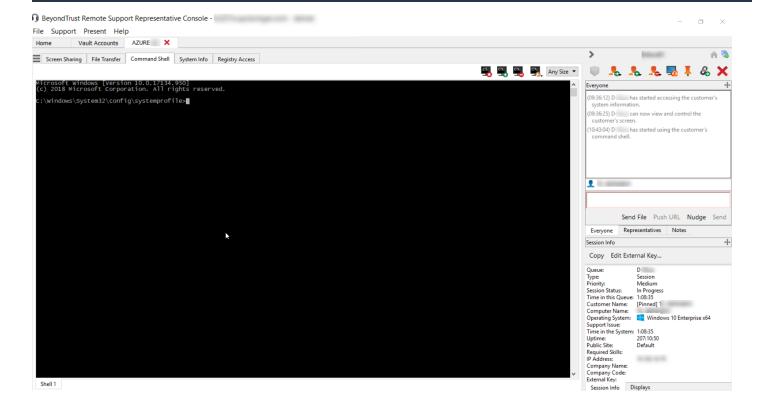
Accès à l'interpréteur de commandes distant

L'interpréteur de commandes distant permet à un utilisateur privilégié d'ouvrir une interface de ligne de commande virtuelle sur l'ordinateur distant. L'utilisateur peut ensuite saisir localement pour exécuter les commandes sur l'ordinateur distant. Vous pouvez travailler depuis plusieurs interpréteurs. Notez que les scripts à la disposition de l'utilisateur peuvent également être exécutés sur l'ordinateur distant à partir de l'interface de partage d'écran.

Votre administrateur peut aussi activer l'enregistrement de l'interpréteur distant afin de permettre la lecture ultérieure d'une vidéo à partir du rapport de session.



Remarque : La localisation est limitée à des caractères codés sur 1 octet pour cette fonction. L'utilisation de caractères codés sur 2 octets (certains modules linguistiques) peut modifier le comportement attendu de certaines fonctions.





Outils d'interpréteur de commandes

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

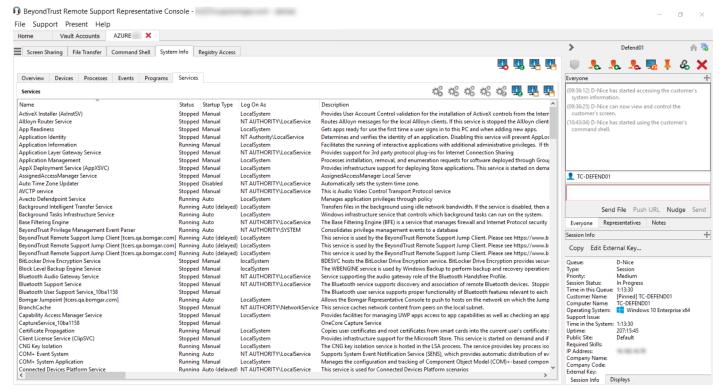


Consulter des informations relatives à un système distant

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

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







Outils d'informations système



Mettez fin à l'extraction des informations relatives au système distant. Une interruption permet toujours de voir les dernières informations mises à jour, mais pas d'extraire les données actuelles.



Actualisez l'affichage des informations système ou extrayez les informations pour les onglets auxquels vous n'avez pas encore demandé l'accès. L'actualisation peut s'effectuer pour des sections individuelles ou pour toutes les sections de l'onglet sélectionné.



Définissez l'actualisation automatique d'une catégorie d'informations système.



Copiez les informations vers le presse-papiers. Copiez des sections individuelles ou toutes les sections de l'onglet sélectionné.



Enregistrez un fichier texte des informations système sur votre ordinateur local. Vous pouvez enregistrer des sections individuelles ou toutes les sections de l'onglet sélectionné.



Mettez fin à un processus en cours d'exécution sur le système distant.



Désinstallez une application sur le système distant.



Démarrez un service arrêté sur le système distant.



Reprenez un service en pause sur le système distant.



Mettez en pause un service en cours sur le système distant.



Arrêtez un service en cours sur le système distant.

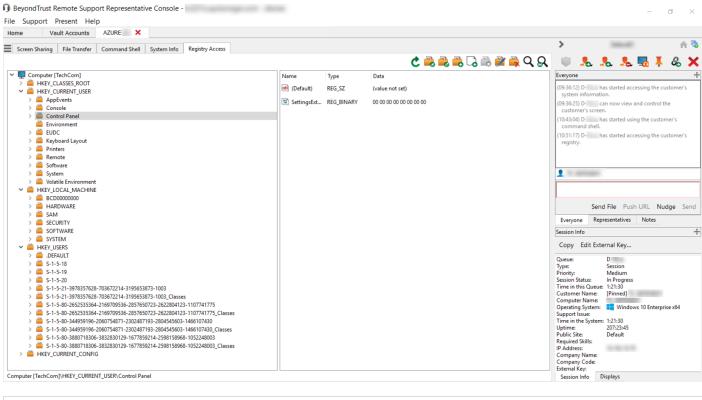


Redémarrez un service en cours sur le système distant.



Accès à l'éditeur de registre distant

Accéder au registre d'un système Windows distant sans nécessiter le partage d'écran. Dans l'éditeur de registre virtuel, vous pouvez ajouter de nouvelles clés, supprimer, modifier, rechercher, importer ou exporter des clés. L'utilisation de l'éditeur de registre virtuel sans partage d'écran permet de réduire le nombre d'interruptions pour l'utilisateur ainsi que le temps de résolution des problèmes.



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



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



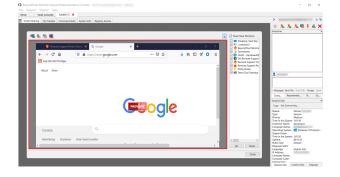
Montrer mon écran à l'utilisateur

Un technicien d'assistance avec privilèges peut à tout moment partager son écran avec un client afin d'améliorer l'efficacité des sessions d'assistance technique ou des formations.

Pour les techniciens d'assistance avec privilèges, les options **Partage d'écran** et **Montrer mon écran** sont disponibles dès le début des sessions d'assistance technique. Si vous utilisez la fonction de partage d'écran, vous devez l'interrompre pour pouvoir démarrer une session avec la fonction Montrer mon écran.



La console du technicien d'assistance affiche une prévisualisation de l'écran visible par l'utilisateur lors d'une session en direct. Lorsque vous partagez votre écran avec l'utilisateur au cours d'une session d'assistance technique, celui-ci est en mesure de voir tout le bureau ou uniquement les applications que vous avez choisi de montrer. Vous pouvez également choisir si vous souhaitez partager automatiquement ou non les nouvelles fenêtres. Notez que vous pouvez afficher ou masquer le sélecteur d'applications en cliquant sur la flèche située dans le haut de la fenêtre **Montrer mon écran**.



Cliquez sur l'icône **Montrer votre écran à l'utilisateur** située dans l'angle supérieur gauche de la fenêtre pour démarrer la session Montrer mon écran en direct. Vous pouvez continuer de discuter avec l'utilisateur pendant la session.



Remarque: l'activité de la fonction Montrer mon écran peut être enregistrée à des fins de génération de rapports (sous /login > Configuration > Options). L'enregistrement n'est pas mis à disposition de votre client sur la page de destination post-session.





Outils de la fonction Montrer mon écran





Montrez tout votre écran ou uniquement certaines applications à l'utilisateur distant ou cessez de partager votre écran.



Lors du partage de votre écran avec l'utilisateur, vous pouvez accorder ou interrompre le contrôle de votre souris et de votre clavier par l'utilisateur, comme lors d'une formation par exemple.



Remarque : le client d'utilisateur Linux ne prend pas en charge le contrôle de l'écran du technicien d'assistance.



Sélectionnez le moniteur à afficher pour la section Montrer mon écran. Le moniteur principal est désigné par la lettre **P**.



Réaliser une présentation pour des participants distants



Remarque: la fonction de présentation doit être activée lors de la création de votre site d'assistance technique. Si elle n'est pas disponible et que vous devez exécuter des présentations, veuillez contacter l'assistance ou l'administrateur de votre site.



IMPORTANT!

La fonction de présentation ne sera plus prise en charge à partir de la version Remote Support 22.1 et n'est pas incluse dans les déploiements sur nouveau site. Pour les mises à niveau, cette option est paramétrée sur ON, mais vous pouvez la désactiver avec OFF. Si vous avez un déploiement sur un nouveau site et que vous devez exécuter des présentations, veuillez contacter l'assistance ou l'administrateur de votre site.

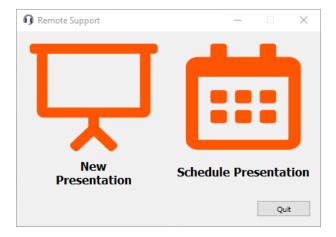
Un technicien d'assistance autorisé à effectuer des présentations, ou un technicien d'assistance disposant d'une autorisation de présentation uniquement, peut partager son écran avec un ou plusieurs participants distants. Démarrez une présentation à partir :



- du menu **Présentation** de la console du technicien d'assistance
- du bouton de démarrage rapide Présentation situé dans le haut de la console du technicien d'assistance
- De la fenêtre de sélection d'interface de présentation uniquement (techniciens d'assistance non autorisés à offrir une assistance technique).

Si vous choisissez de démarrer une présentation immédiatement à l'aide du bouton **Présentation** ou de l'option **Démarrer une présentation...** dans la console du technicien d'assistance, l'interface de **présentation** s'affiche.

Si vous ne disposez que d'une autorisation de présentation uniquement, pour démarrer une présentation, cliquez sur le bouton **Nouvelle présentation** de la fenêtre de sélection d'interface de présentation uniquement.



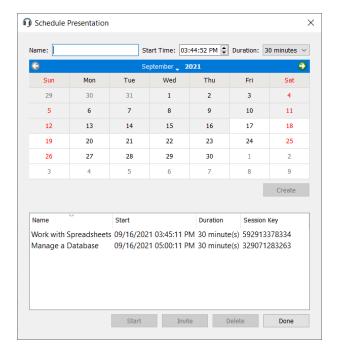


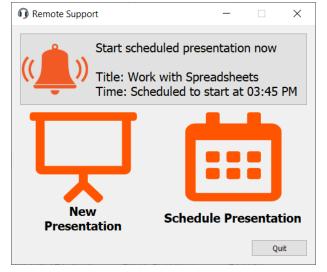
Vous pouvez aussi programmer une présentation à une date ultérieure. Un planificateur vous invite à entrer un nom pour la présentation, une heure de début et de fin, ainsi que la durée prévue de l'événement. Une fois que vous avez entré toutes ces informations, cliquez sur Créer. Votre présentation apparaît à présent dans la liste de vos présentations à venir. Les horaires des présentations ne peuvent pas se chevaucher. Si vous supprimez une présentation avant l'heure à laquelle elle était prévue, les invitations que vous avez envoyées ne sont plus valables et les participants ne peuvent pas se connecter. Lorsque vous voulez commencer une présentation programmée, sélectionnez-la dans la liste, puis cliquez sur **Démarrer** pour accéder à l'interface de présentation.

Depuis le planificateur, vous pouvez envoyer aux participants une invitation par e-mail contenant une URL unique et toutes les informations sur la conférence audio nécessaires pour la présentation ou inviter les participants à se rendre sur votre site public pour y entrer la clé de session unique. Vous pouvez également envoyer une invitation par e-mail depuis l'interface de présentation.

Lorsque le début d'une présentation programmée est imminent, un bouton s'affiche en haut de la fenêtre de sélection d'interface de présentation uniquement pour vous permettre de lancer la présentation directement. Vous pouvez également démarrer une présentation programmée à partir

de la fenêtre de planification.





L'interface de présentation comprend une barre latérale verticale discrète composée de trois sections réductibles : Invitation, Participants et Messagerie instantanée. Elle comprend également un volet latéral horizontal glissant, qui inclut une fenêtre de prévisualisation avec un voyant d'état permettant d'indiquer qu'une présentation est en cours (il change lors de la sélection du bouton de début/fin). Un sélecteur d'applications, un sélecteur d'affichage et un sélecteur de résolution, décrits ci-après, sont également disponibles.





Dans la section **Invitation**, vous pouvez entrer un nom pour la présentation ou utiliser l'entrée générique par défaut comprenant le nom du technicien d'assistance. L'interface comprend également des champs **Clé d'accès** et **URL**, et vous pouvez choisir de saisir et d'enregistrer des informations sur la conférence audio, qui seront sauvegardées d'une présentation à une autre et consignées dans la fenêtre de messagerie instantanée. Ces informations sont envoyées à tous les participants lors de leur connexion et sont à nouveau affichées au cours des présentations, après chaque modification. Si la liste des présentations est activée sur votre site public, vous pouvez sélectionner l'option **Apparaître dans la liste publique** pour afficher un lien permettant aux participants de rejoindre la présentation. Vous trouverez également des boutons permettant de **copier l'URL d'invitation** et d'**envoyer un e-mail d'invitation**.







Si le bouton **Inviter** est manquant dans la boîte de dialogue du planning de présentation, vérifiez que les e-mails côté client ont été configurés et activés sur votre instance. Pour plus d'informations, veuillez visiter <u>Configuration e-mail</u>: <u>Configurer le logiciel pour envoyer des e-mails</u> à l'adresse <u>https://www.beyondtrust.com/docs/remote-support/getting-started/admin/email-configuration.htm</u>.

La section **Participants** répertorie toutes les personnes ayant rejoint la présentation. Si vous y êtes autorisé, un bouton vous permet de transmettre (ou d'interrompre) à un participant le contrôle de votre souris et de votre clavier. Vous avez également la possibilité de déconnecter des participants de la présentation grâce à un bouton dédié.



Remarque: lorsque votre participant a le contrôle de votre souris et de votre clavier, il verra une barre rouge s'afficher dans le bas de sa fenêtre. S'il est en mode Plein écran ou Taille réelle, ces modes sont abandonnés lors de la prise de contrôle. Les participants utilisant des appareils mobiles ne peuvent pas bénéficier de cette fonctionnalité.

La section **Messagerie instantanée** de l'interface de présentation enregistre toutes les actions effectuées dans l'interface, ainsi que les messages envoyés à l'ensemble des participants ou à certains participants sélectionnés. Notez que chaque participant peut discuter avec vous uniquement ou avec vous et tous les autres participants.

Cliquer sur la flèche située au-dessus des sections de l'interface de présentation permet de passer l'interface en mode réduit, afin de n'afficher que les commandes de présentation.

Lors de la prévisualisation de la présentation ou lors de la présentation elle-même, vous pouvez ouvrir ou fermer le volet de prévisualisation/direct en cliquant sur le volet situé à gauche. Celui-ci permet notamment de sélectionner les applications à partager. Vous pouvez également choisir de présenter automatiquement ou non les nouvelles fenêtres. Si vous disposez de plusieurs moniteurs, cliquez sur l'icône correspondant à celui que vous souhaitez présenter pour le sélectionner. Notez que le moniteur principal est désigné par la lettre **P**. Vous pouvez également choisir de présenter tous les moniteurs.

Vous pouvez également choisir la profondeur de couleur de la présentation : **Bande passante limitée**, **Performance optimale**, **Performance et qualité** ou **Qualité optimale**.

Les boutons de début/fin, des moniteurs et de la profondeur de couleur restent disponibles que le volet de prévisualisation ou direct soit ouvert ou non, et que l'interface de présentation BeyondTrust soit affichée en mode réduit ou à sa taille minimale. Lors des présentations, vous disposez également d'un bouton permettant d'activer les annotations.





Outils de présentation



Démarrez la présentation. Le volet de l'interface de présentation affiche un voyant de **DIRECT** vert translucide pour les présentations en direct.



Arrêtez la présentation. Le volet de l'interface de présentation affiche un voyant de **PRÉVISUALISATION** rouge translucide.



Sélectionnez le moniteur à afficher pour la session de présentation. Le moniteur principal est désigné par la lettre P.



Affichez l'écran en échelle de gris 2 bits pour une consommation minimale de bande passante, en couleur 8 bits pour des performances rapides, 16 bits pour une qualité d'image et des performances moyennes ou 32 bits pour une résolution d'image optimale.



Activez les annotations pour la présentation en direct.



Si vous y êtes autorisé, accordez le contrôle de votre souris et de votre clavier à un participant. Ce contrôle ne peut être attribué qu'à un seul participant à la fois. Vous pouvez conserver le contrôle du remplacement ou l'annuler à tout moment. Les participants utilisant des appareils mobiles ne peuvent pas bénéficier de cette fonctionnalité. Vous ne pouvez pas transférer une présentation à un autre présentateur.



Retirez des participants de la présentation sans mettre fin à cette dernière.



Mettez fin à la présentation et fermez l'interface.



Annotations

Si vous avez l'autorisation d'utiliser les annotations, cet outil est également disponible pendant les présentations, ce qui vous permet de mettre en évidence certaines zones de l'écran et d'attirer l'attention sur des zones et des objets en particulier.

Une fois les annotations activées, cliquez avec le bouton droit de la souris dans la présentation pour accéder aux outils d'annotation. Pour désactiver les **Annotations**, sélectionnez **Aucun outil** dans le menu déroulant, ou cliquez sur **Echap**.

Parmi les outils disponibles, on trouve le dessin libre, les cercles et rectangles, effacer, annuler, supprimer, les couleurs (rouge, noir et blanc) et l'épaisseur du trait (fin/moyen/épais).





Collaboration

Messagerie instantanée avec d'autres techniciens d'assistance

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

Notez que lorsque vous revenez à votre file d'attente personnelle ou que vous sélectionnez **Toutes les files d'attente**, vous restez dans la discussion de la file d'attente que vous venez de quitter.

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

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

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

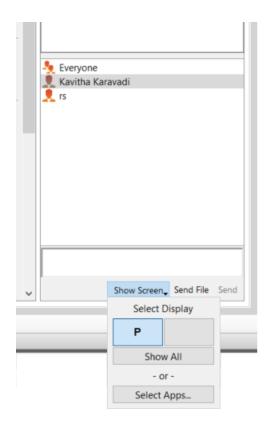




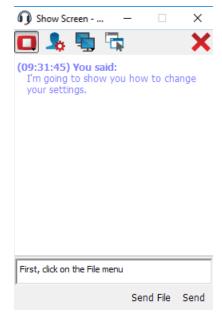
Partager votre écran avec un autre technicien d'assistance

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

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



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

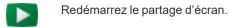




Outils de partage d'écran

Utilisateur partageant

Arrêtez temporairement le partage de votre écran avec un autre utilisateur. Cette option interrompt le partage d'écran sans fermer la fenêtre Montrer l'écran , afin de vous permettre de reprendre le partage ultérieurement.



Accordez le contrôle de la souris et du clavier à l'utilisateur regardant votre écran.

Sélectionnez le moniteur à partager avec un autre utilisateur. Notez que le moniteur principal est désigné par la lettre **P**.

Sélectionnez les applications à partager avec l'utilisateur regardant votre écran.

Fermez la session de partage d'écran. Ceci ferme l'interface de partage d'écran avec un utilisateur.

Utilisateur en visualisation

	L'utilisateur partageant son écran avec vous vous a donné le contrôle de son clavier et de sa souris.
--	---

Allumez un pointeur virtuel visible sur l'écran de l'utilisateur partageant.

Effectuez une capture de l'écran de l'utilisateur partageant à sa résolution complète.

Visualisez l'écran distant à sa taille réelle ou mis à l'échelle.

Affichez le bureau distant en mode plein écran ou revenez à l'affichage de l'interface.

Fermez la session de partage d'écran. Ceci ferme l'interface de partage d'écran avec un utilisateur.



Acceptation d'une demande d'accès à des fins d'accroissement des droits

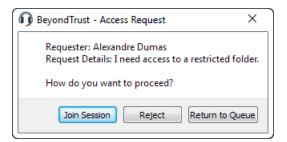
En fonction des groupes de parrains d'accès, un technicien d'assistance ayant des autorisations limitées peut demander à un technicien d'assistance ayant plus de privilèges d'effectuer en son nom certaines actions telles que l'accroissement des droits administratifs d'un client d'utilisateur ou la saisie d'informations d'authentification pour un système distant.



Si un technicien d'assistance est le parrain d'un ou plusieurs groupes de parrains d'accès, il verra un onglet **Demandes d'accès** sur la console du technicien d'assistance.

Lorsqu'un technicien d'assistance fait une demande, tous les parrains du groupe de parrains d'accès sélectionné verront une nouvelle demande dans l'onglet **Demandes d'accès** de la console du technicien d'assistance.

Lorsqu'un parrain accepte la demande, il est invité à rejoindre la session, rejeter la demande et saisir un motif de rejet, ou bien renvoyer la demande dans la file d'attente.





Partage d'une session avec d'autres techniciens d'assistance

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

Il existe plusieurs méthodes pour inviter un technicien d'assistance à rejoindre une session. Vous pouvez utiliser l'option **Demander de l'aide** pour transmettre votre demande en fonction d'un problème spécifique. Seuls les problèmes qui ont été configurés pour vous permettre de demander de l'aide s'affichent dans la liste.

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

Si vous sélectionnez **Tous les techniciens d'assistance**, l'invitation est envoyée à la file d'attente d'équipe afin que n'importe quel technicien d'assistance appartenant à cette équipe puisse rejoindre la session. Vous pouvez également envoyer plusieurs invitations si vous souhaitez que plusieurs membres d'une équipe rejoignent la session.

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

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

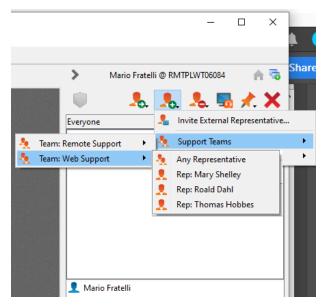
Lorsque vous invitez un utilisateur ayant la disponibilité étendue activée, il recevra une notification par e-mail.

Si vous avez envoyé une invitation et qu'elle est encore active, vous pouvez supprimer l'invitation en la sélectionnant dans le menu **Annuler l'invitation**. Seul le propriétaire de la session peut envoyer des invitations. Les invitations n'expirent pas tant que vous restez propriétaire de la session. Un utilisateur ne peut pas disposer de plusieurs invitations actives pour rejoindre une même session.

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

- · L'utilisateur qui invite annule l'invitation
- L'utilisateur invitant laisse ou transfère la propriété de la session
- · La session se termine
- · L'utilisateur invité accepte l'invitation
- · L'utilisateur invité refuse l'invitation

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





Accessibilité hors connexion grâce à la fonction de disponibilité étendue

Grâce à la disponibilité étendue, les utilisateurs privilégiés peuvent recevoir des invitations par e-mail pour partager des sessions, même s'ils ne sont pas connectés à la console. Lorsque vous envoyez une invitation, vous pouvez inviter des membres de votre équipe. Si vous y êtes autorisé, vous pouvez également inviter des utilisateurs d'équipes auxquelles vous n'appartenez pas. La capacité de partager des sessions avec des utilisateurs en dehors de vos équipes, et de recevoir des invitations à une session lorsque vous êtes déconnecté de la console, étend votre disponibilité en tant que technicien service client.

Si votre compte est configuré pour une disponibilité étendue, vous pouvez activer ou désactiver la fonctionnalité dans le menu **Assistance technique** de la console du technicien d'assistance.

File Support Present Help

Hom Showing On Representative List

Enable Extended Availability

Get Next Session

Generate Session Key Ctrl+F4

Generate Apple iOS Profile Access Key...

Jump To...

RDP...

VNC...

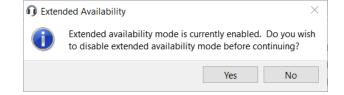
Shell Jump...

Intel® vPro...

Support Buttons...

BeyondTrust Remote Support Representative Console - tce

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





Remarque : si vous choisissez de garder la disponibilité étendue activée, un emplacement de licence vous sera réservé jusqu'à ce que la disponibilité étendue soit désactivée. Ceci vous permet d'être sûr que si vous êtes invité à rejoindre une session, la connexion ne vous sera pas refusée à cause de restrictions sur l'utilisation de licences



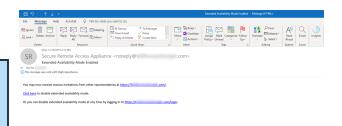
Invitation et notification par e-mail

Chaque fois que vous activez le mode disponibilité étendue, la B Series Appliance vous en informe sur l'adresse e-mail configurée dans votre compte d'utilisateur et dans la langue spécifiée le cas échéant.



Remarque : BeyondTrust n'extrait pas d'adresse e-mail des magasins d'annuaires externes LDAP. L'adresse e-mail doit être configurée dans BeyondTrust d'une des manières suivantes :

- Un administrateur peut ajouter une adresse e-mail à un compte d'utilisateur en allant sur /login > Utilisateurs et sécurité > Utilisateurs et en modifiant le compte.
- 2. L'utilisateur peut définir sa propre adresse e-mail en allant sur la page /login > Mon compte.



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

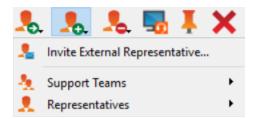
La B Series Appliance envoie également une notification par e-mail lorsque vous êtes invité à une session. Cela vous permet de rejoindre une session même sans être connecté à la console. La notification par e-mail inclut des liens permettant d'accepter ou de refuser l'invitation, tout en désactivant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





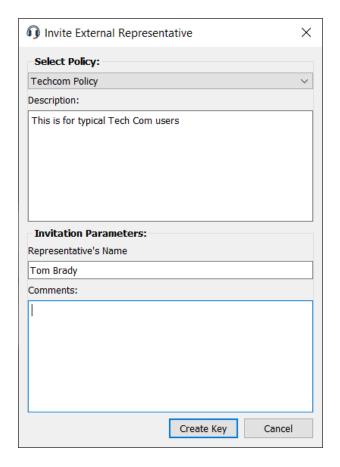
Invitation d'un technicien d'assistance externe à rejoindre une session

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

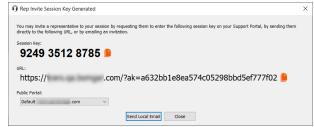


Une boîte de dialogue s'ouvre, demandant à l'utilisateur de sélectionner un profil de sécurité. Ces profils sont créés dans l'interface d'administration et déterminent le niveau d'autorisation dont bénéficiera l'utilisateur externe. Lorsque vous sélectionnez un profil, la description complète s'affiche audessous.

Saisissez le nom de l'utilisateur invité. Ce nom est visible à l'écran de l'utilisateur et apparaît dans les rapports. Saisissez ensuite des commentaires sur le motif de l'invitation de cet utilisateur. Cliquez sur **Créer une clé**. Une nouvelle boîte de dialogue contenant la clé de session et une URL directe s'affiche.



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





L'utilisateur invité n'aura accès qu'à l'onglet de session et disposera de privilèges restreints. L'utilisateur invité ne peut jamais être le propriétaire de la session. Si le technicien d'assistance qui l'a invité quitte la session sans autre propriétaire de session, le technicien d'assistance externe est déconnecté. La clé de session pour l'utilisateur invité est valide pendant deux heures ou jusqu'à ce que la session se termine.

Vous pouvez inviter plus d'un utilisateur externe à une session. N'oubliez pas que chaque technicien d'assistance externe occupe une licence BeyondTrust.



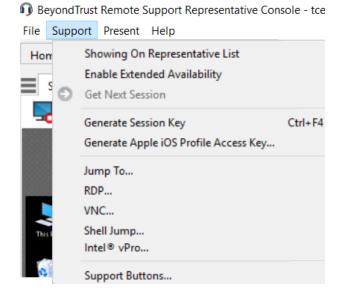
Gestion

Gérer un bouton d'assistance technique.

Un bouton d'assistance technique permet aux clients d'initier une session d'assistance technique avec l'équipe d'assistance technique qui leur a été attribuée, de saisir une clé de session ou de soumettre un problème à une file d'attente d'assistance technique. Un bouton d'assistance technique déployé peut être géré depuis l'interface de gestion de bouton d'assistance technique. Remarque : un bouton d'assistance technique déployé en masse et installé en mode système doit être supprimé en utilisant la fonction « Ajouter ou supprimer des programmes » ou des outils de gestion système.

Accédez à l'interface de gestion de bouton d'assistance technique à partir :

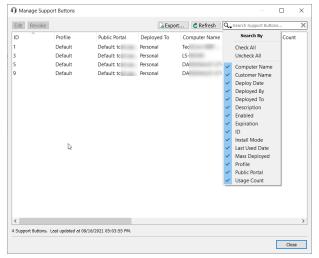
- du menu Assistance technique de la console du technicien d'assistance
- du bouton bouton d'assistance technique situé en haut de la console du technicien d'assistance



L'interface de gestion de bouton d'assistance technique affiche la liste de chaque bouton d'assistance technique déployé, ainsi que les statistiques d'utilisation correspondantes.

Les administrateurs voient chaque bouton d'assistance technique déployé, tandis que les utilisateurs avec privilèges peuvent voir les boutons associés à leur files d'attente personnelle et d'équipe.

Cliquez sur le bouton **Rechercher par** (icône de recherche) pour sélectionner les champs dans lesquels chercher. Saisissez ensuite le terme à rechercher, puis appuyez sur Entrée pour lancer la recherche. Notez que vous pouvez trier les données en cliquant sur l'en-tête d'une colonne.



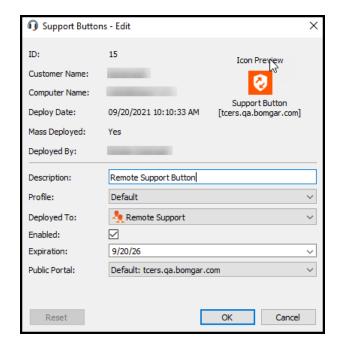


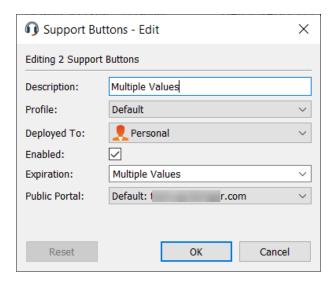
Les statistiques d'utilisation de bouton d'assistance technique incluent les points suivants :

- · Champs statiques:
 - ІГ
 - Nom d'utilisateur
 - Nom d'ordinateur
 - Date du déploiement
 - Déployé en masse (Oui/Non)
 - Déployé par (nom affiché privé du technicien d'assistance)
 - Nombre d'utilisations
 - Dernière date d'utilisation (ou Jamais en l'absence de date)
 - Mode d'installation (utilisateur ou système)
 - Prévisualisation d'icône
- Champs dynamiques (modifications autorisées):
 - Description
 - Profil
 - Déployé pour (File d'attente)
 - Activé (Oui/Non)
 - Expiration
 - Portail public

Vous pouvez également **Modifier** les champs dynamiques, **Révoquer** un bouton d'assistance technique ou **Exporter** les statistiques d'utilisation d'un bouton d'assistance technique au format *.csv. Si vous révoquez un bouton d'assistance technique déployé en masse et installé pour tous les utilisateurs d'un système, le bouton ne pourra être supprimé qu'en utilisant la fonction « Ajouter ou supprimer des programmes » ou des outils de gestion système.

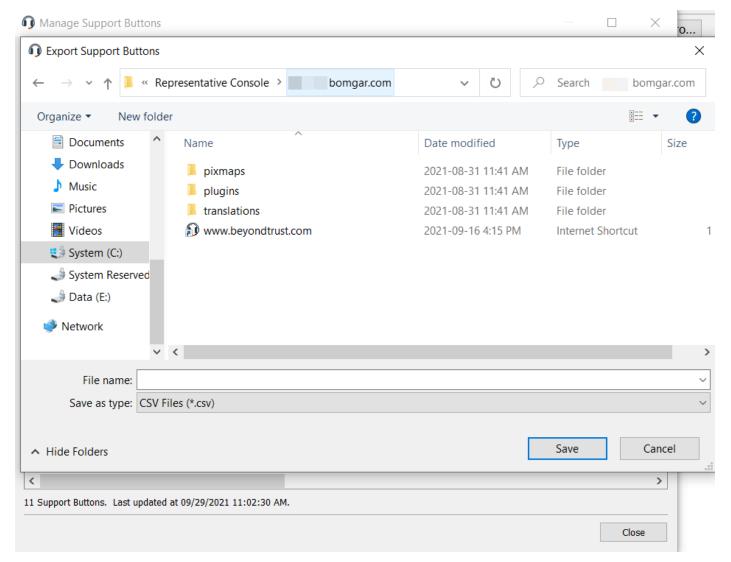
Si vous sélectionnez **Modifier** dans l'**Interface de gestion de bouton d'assistance technique**, vous pouvez modifier n'importe quel champ dynamique. Si plus d'un bouton d'assistance technique sont sélectionnés pour être modifiés, **Valeurs multiples** s'affiche dans les champs dynamiques présentant des valeurs différentes.







Si vous choisissez d'**exporter** les statistiques d'utilisation, l'écran de sélection de fichier suivant s'affiche. Vous pouvez saisir le nom de fichier de votre choix ainsi que l'emplacement d'enregistrement du fichier *.csv.





Surveillance des membres d'une équipe dans le tableau de bord

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

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

Les indicateurs de statut indiquent si les utilisateurs sont disponibles pour accepter des sessions (vert), inactifs (gris) ou occupés (jaune), ou encore si la fonction d'attribution automatique est désactivée pour eux (rouge). Si un utilisateur cumule plusieurs de ces états, l'indicateur indique l'information la plus importante, dans l'ordre suivant : fonction d'attribution automatique désactivée, occupé, inactif et disponible. Passez le curseur sur le nom de l'utilisateur pour afficher les informations détaillées. Une barre, située dans le bas du tableau de bord, indique le pourcentage d'utilisateurs par état. Passez le curseur sur cette barre pour afficher le nombre d'utilisateurs pour chaque état. Les utilisateurs ne peuvent pas modifier manuellement l'affichage de leurs états.

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

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



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

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

Une icône de surveillance peut être affichée dans l'angle du bureau de l'utilisateur en vue d'indiquer que la surveillance a lieu. Lorsque l'utilisateur déplace le curseur près de cette icône, elle se déplace dans un autre coin pour ne pas gêner la visibilité de l'écran. Sélectionnez l'utilisateur dont vous voulez voir l'écran, puis cliquez sur le bouton **Surveiller**. Ceci ouvrira une nouvelle page dans votre console, affichant soit l'intégralité de l'écran de l'ordinateur de l'utilisateur soit uniquement la console, en fonction des paramètres d'administration.

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

Au sein d'une équipe, un utilisateur ne peut administrer que les personnes ayant un rôle inférieur au sien.



Remarque : les rôles s'appliquent strictement par équipe. Ainsi, un utilisateur peut être en mesure d'administrer un autre utilisateur dans une équipe, sans pouvoir administrer ce même utilisateur dans une autre.



Enquête de satisfaction du technicien d'assistance

À la fin de la session, vous pouvez être invité à répondre à une courte enquête portant sur la session. Votre administrateur peut intégralement personnaliser les questions par le biais de l'interface d'administration et étudier les résultats à partir des rapports de session. Si une ou plusieurs questions sont obligatoires, vous n'êtes pas autorisé à fermer la session avant d'y avoir répondu.

Votre administrateur peut aussi décider de vous autoriser à accéder à l'enquête de satisfaction du technicien d'assistance lors d'une session. Dans ce cas, l'enquête peut être utilisée comme modèle de flux de travail, ce qui permet à votre administrateur de publier une série de questions et/ou de cases à cocher, ainsi que des liens spécifiques que vous pourrez utiliser dans votre session d'assistance technique.

Representative Survey		×
Please fill out the following surve	y.	
1. Was the Customer's issue resolve	ed?	
Yes		
No, will try again later		
No, impossible		
	OK	Cancel



Ce que votre client voit : Le client d'utilisateur BeyondTrust

Les clients sur des bureaux distants, des smartphones et autres appareils interagissent avec les techniciens d'assistance essentiellement à travers les clients d'utilisateur BeyondTrust.

Ils peuvent également voir des invites et des messages dans le contexte du site public ou du portail d'assistance technique. Cette section détaille les éléments que rencontre le client lors d'une session d'assistance technique à distance BeyondTrust sur un ordinateur fixe ou portable.



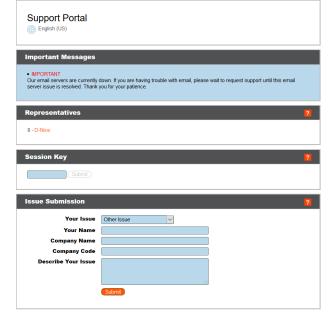


Pour plus d'informations sur la prise en charge d'autres périphériques, y compris <u>Apple iOS</u> et <u>Android</u>, consultez la page <u>https://www.beyondtrust.com/docs/remote-support/getting-started/index.htm</u>.



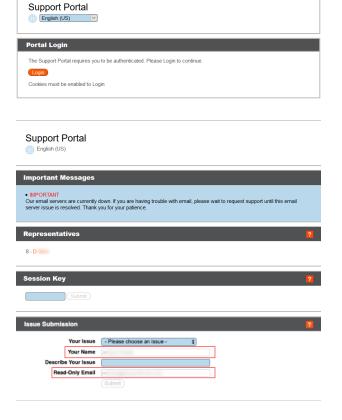
Site public : demande d'assistance technique

Le site public est le portail d'assistance de votre B Series Appliance, où vos utilisateurs viennent demander une session d'assistance technique ou rejoindre une présentation. Sur cette page, votre utilisateur peut lancer une session en cliquant sur le nom d'un technicien d'assistance, en soumettant une clé de session ou en remplissant un formulaire de soumission de problème. Vos clients peuvent également rejoindre une présentation en cliquant sur le lien correspondant ou en soumettant une clé de session.



Un client peut accéder au portail d'assistance technique public à l'aide de l'URL fournie par un technicien d'assistance. Si l'authentification SAML est configurée et activée pour le site public, le client voit apparaître la fenêtre **Connexion au portail**. Le client doit cliquer sur **Connexion**, puis fournir des informations d'authentification pour s'authentifier auprès du fournisseur d'identité.

Le client est ensuite redirigé vers la page du portail d'assistance technique où il peut soumettre sa demande d'assistance. Le nom du client et tous les champs personnalisés qui sont configurés, tels que l'adresse e-mail, sont automatiquement renseignés et ne sont pas modifiables.







Astuce: une coche verte s'affiche à côté du nom du client dans la fenêtre de messagerie instantanée de la console du technicien d'assistance pour indiquer que l'utilisateur est authentifié par le portail public.



Si la traduction en temps réel de la messagerie instantanée est activée, les clients peuvent discuter avec un technicien d'assistance dans leur propre langue. Par exemple, un client dont la langue principale est l'anglais peut discuter avec un technicien d'assistance qui ne parle que néerlandais, les messages étant traduits automatiquement en temps réel.

Si l'enquête de soumission de problème est activée, l'utilisateur sera invité à sélectionner le nom d'un technicien d'assistance ou un type de problème spécifique, en fonction des paramètres mis en place par votre administrateur. Votre client peut aussi saisir son nom, le nom de son entreprise et une description du problème rencontré. Votre administrateur a la possibilité d'inclure un champ **Code de société** pour aider au suivi du problème.

Selon la méthode de lancement de session, votre utilisateur est placé dans la file d'attente d'assistance technique du technicien d'assistance ou de l'équipe affectée au traitement de ce problème, ou votre utilisateur rejoint la présentation spécifiée.

Pour les utilisateurs de périphériques Apple iOS, votre portail d'assistance technique iOS est un référentiel sécurisé de profils publics et privés que vous avez téléchargés dans l'interface /login. Les profils privés sont accessibles uniquement si le technicien d'assistance a généré une clé d'accès iOS.

Si un avis d'utilisateur est actif pour ce site, il sera affiché dans la section **Messages importants**. Les avis peuvent alerter les utilisateurs en cas d'interruptions informatiques à large impact pour lesquelles aucune assistance technique n'est nécessaire, ce qui permet à l'utilisateur de ne plus rejoindre inutilement une session d'assistance technique.

Si un planning est défini pour ce site public et que l'heure actuelle n'est pas une heure d'ouverture, les méthodes de lancement de session autres que les clés de session n'apparaissent pas sur le site, et un message indiquant que le portail est fermé s'affiche.



Pour plus d'informations, veuillez consulter :

- SAML pour l'authentification unique à l'adresse https://www.beyondtrust.com/docs/remote-support/how-to/integrations/security-providers/saml/index.htm
- <u>Traduction de la messagerie instantanée en temps réel</u> à l'adresse <u>https://www.beyondtrust.com/docs/remote-support/videos/real-time-chat-translation.htm</u>



Client d'utilisateur : interface de session d'assistance technique

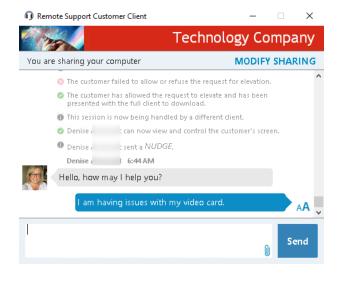
Lorsque votre client lance une session d'assistance technique avec vous, celle-ci démarre soit avec la messagerie instantanée par internet soit avec le téléchargement du client d'utilisateur complet, selon les paramètres de votre site. Si vous avez envoyé un avatar à utiliser avec votre compte, celuici sera affiché dans la fenêtre de messagerie instantanée. Veuillez noter que cela ne fonctionne qu'avec le client d'utilisateur complet, pas le client HTML.

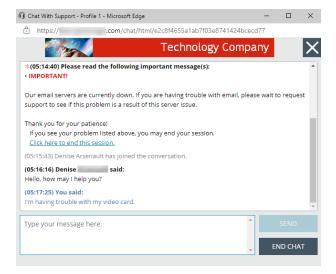
Si la session est lancée en tant que messagerie instantanée HTML5 sur internet, il sera demandé à votre client d'autoriser les notifications, ce qui activera les notifications contextuelles pour vous aider à communiquer plus efficacement avec lui.

Votre administrateur peut déterminer les messages que votre client voit avant le début de la session. Parmi les messages qui peuvent être affichés se trouvent un accord d'utilisateur, qui nécessite que ce dernier accepte les conditions d'accès à une session d'assistance technique, une invite lui permettant d'autoriser ou de refuser les enregistrements de session, ainsi qu'un message de bienvenue, qui peut inclure une estimation du temps d'attente et la place de l'utilisateur dans la file d'attente.

Si des avis d'utilisateur sont actifs, ils peuvent être affichés automatiquement ou envoyés manuellement au client d'utilisateur, ce qui permet aux utilisateurs de quitter la session s'ils rencontrent un problème connu décrit dans l'avis. Les utilisateurs qui quittent la session de cette façon ne sont pas redirigés sur la page **Enquête de satisfaction**, car aucun service n'a été fourni par un technicien d'assistance.

Un message d'attente peut s'afficher périodiquement de façon à rassurer le client sur le fait qu'il se trouve toujours dans la file d'attente et sera pris en charge rapidement. Ce message peut inclure une estimation du temps d'attente et la place de l'utilisateur dans la file d'attente.





Si aucun technicien d'assistance n'est disponible pour prendre la session, un message en alerte l'utilisateur. Si cela est configuré, le navigateur Internet de l'utilisateur peut s'ouvrir automatiquement sur une URL spécifiée, comme une base de connaissances ou une page de contact.

TC: 7/18/2022



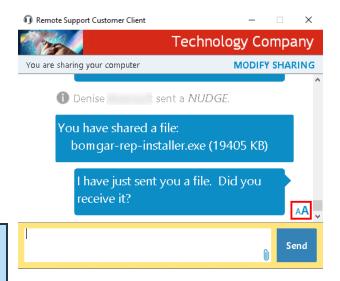
Pendant la session, l'utilisateur peut converser avec vous et demander à transmettre des fichiers à votre ordinateur. Il peut aussi modifier la taille de la police dans la fenêtre de messagerie instantanée.

Si vous envoyez un wizz, le client d'utilisateur s'affichera au premier plan et sera secoué, et une alerte sonore retentira. La fenêtre de messagerie instantanée indiquera qu'un wizz a été envoyé.

Pour stopper immédiatement le partage d'écran et annuler toutes les autorisations que le technicien d'assistance aurait pu avoir, cliquez sur le lien **ARRÊTER LE PARTAGE** sur la droite de la bannière en haut de la messagerie instantanée. L'utilisateur peut aussi choisir de mettre fin à la session en fermant la fenêtre de messagerie instantanée. Cela désinstallera le logiciel de son ordinateur.



Remarque: le lien ARRÊTER LE PARTAGE apparaît lorsque le partage d'écran se fait sans aucune restriction. Si vous autorisez le client à choisir quelles applications partager, alors MODIFIER LE PARTAGE sera affiché, permettant au client de changer ou de sélectionner les applications à partager, ou à interrompre le partage s'il le souhaite. Dans tous les cas, la session peut toujours être interrompue en fermant la fenêtre de messagerie instantanée.



Selon les paramètres du site, un filigrane peut également apparaître sur l'écran de l'utilisateur au cours de la session. Notez que ceci ne s'applique qu'aux systèmes Windows.



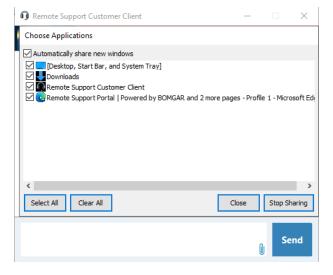
Remarque : les clients utilisant Linux doivent marquer le fichier de téléchargement du client d'utilisateur comme exécutable avant de l'installer.



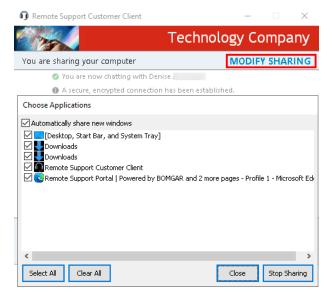


Partage d'application : restriction des éléments visibles par le technicien d'assistance

Lorsque vous demandez un partage d'écran limité, une fenêtre de sélection d'application s'affiche par-dessus la fenêtre de messagerie instantanée du client d'utilisateur.

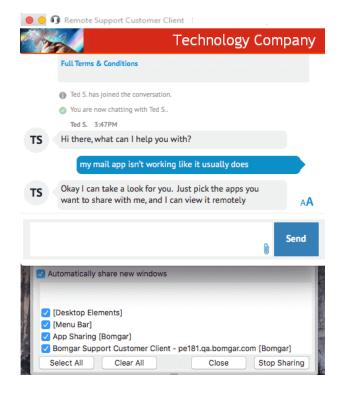


Une fois le partage d'écran accordé, la fenêtre de sélection d'application est accessible en cliquant sur le lien **Modifier le partage**.





Selon les paramètres de votre site, l'utilisateur peut toujours sélectionner des applications dans le menu volant, même si le partage d'écran limité n'a pas été expressément demandé. Le partage d'application est disponible pour l'assistance sur des ordinateurs Windows ou Mac. Des restrictions de partage d'applications prédéfinies ont peut-être été appliquées à la session d'assistance technique par l'administrateur de votre équipe d'assistance technique.





Interaction utilisateur restreinte : écran de confidentialité et désactivation de l'entrée de l'utilisateur distant

Pour faciliter l'assistance technique d'un ordinateur distant, vous pouvez éviter les interférences client en désactivant l'entrée souris et clavier de l'utilisateur distant. L'utilisateur distant pourra toujours consulter le bureau actif. Lorsque l'entrée est désactivée, chaque moniteur distant affichera une bordure orange.



Si vous devez travailler confidentiellement sur l'ordinateur distant, vous pouvez activer un écran de confidentialité de sorte que l'utilisateur distant ou des passants ne puissent pas voir ce que vous faites. Un message de courtoisie est affiché à la place. L'utilisateur 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 vers un ordinateur macOS ou Windows. Dans Windows Vista et les versions supérieures, le client d'utilisateur doit être accru. Sous Windows 8, l'écran de confidentialité n'est pas disponible, et le technicien d'assistance peut seulement désactiver le clavier et la souris.





cette fonction est activée sur l'onglet **Partage d'écran** d'une session d'assistance technique dans la console du technicien d'assistance. Pour plus d'informations, reportez-vous à « Partage d'écran avec l'utilisateur distant à des fins de consultation et de contrôle », page 79.





Informations d'authentification pour connexion automatique : redémarrage et reconnexion

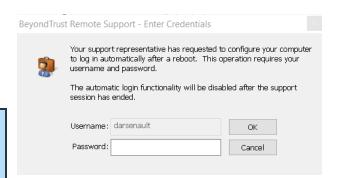
Vous pouvez demander à votre client de saisir un nom d'utilisateur et un mot de passe valides pour vous permettre de redémarrer l'ordinateur distant et de vous connecter automatiquement au système sans avoir besoin de connaître ses informations d'authentification et sans qu'il soit présent. Suivez les étapes ci-dessous pour utiliser la fonction de connexion automatique utilisant les informations d'authentification :



Remarque : pour utiliser cette fonction, votre administrateur doit avoir activé l'option de sécurité /login pour Autoriser le redémarrage avec des informations d'authentification cachées.



Astuce: avant de pouvoir utiliser cette fonction, vous devez accroître la session d'assistance technique et lancer le partage d'écran.





Remarque: les informations d'authentification sont stockées par le système d'exploitation, et pas par BeyondTrust. Nous tirons parti d'une fonction de sécurité native de Windows pour utiliser cette fonction. Les informations d'authentification ne sont jamais exposées, sous quelque forme que ce soit, sur le réseau. Cette fonction est disponible uniquement pour Windows et ne peut être utilisée sur des systèmes distants fonctionnant avec Mac OS.

- 1. Cliquez sur l'Action spéciale de contrôle de l'alimentation dans le menu.
- 2. Sélectionnez Demander les informations d'authentification d'ouverture de session automatique.
- 3. L'utilisateur devra saisir ses informations d'authentification dans l'invite.
- 4. Une fois cela fait, le texte du menu des Actions spéciales de contrôle de l'alimentation passe de Demander les informations d'authentification d'ouverture de session automatique à Effacer les informations d'authentification d'ouverture de session automatique.
- 5. Au prochain redémarrage, le système se connectera avec les informations d'authentification saisies par l'utilisateur.

TC: 7/18/2022



Montrer mon écran : inversion du partage d'écran

Lorsque vous partagez votre écran avec l'utilisateur au cours d'une session d'assistance technique, celui-ci est en mesure de voir tout le bureau ou uniquement les applications que vous avez choisi de montrer. Vous pouvez continuer de discuter avec l'utilisateur pendant ce temps.

Pour agrandir la zone d'affichage, votre utilisateur peut masquer la barre de discussion latérale en cliquant sur la flèche afficher/masquer sur le séparateur entre la barre de discussion et la fenêtre de présentation. Si l'utilisateur reçoit un message alors que la barre de discussion est masquée, la fenêtre afficher/masquer clignote en orange.

Il peut aussi gérer la fenêtre de présentation en choisissant d'afficher votre écran à sa taille réelle ou mis à l'échelle de la fenêtre du client. L'utilisateur



peut choisir d'afficher votre écran à 8 bits pour une rapidité optimale, à 16 bits pour une qualité d'image et des performances moyennes ou à 32 bits pour une résolution d'image optimale. Vous pouvez décider de partager le contrôle de la souris et du clavier avec l'utilisateur distant.

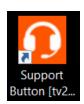


Remarque: le client d'utilisateur Linux ne prend pas en charge le contrôle de l'écran du technicien d'assistance.



bouton d'assistance technique : demande d'assistance technique rapide

Si vous avez installé un bouton d'assistance technique sur l'ordinateur de votre client, ce bouton apparaîtra sous la forme d'un raccourci sur le bureau ou dans le menu de son ordinateur. Si le bouton d'assistance technique a été personnalisé, il apparaîtra sur l'ordinateur de votre utilisateur avec une image et un titre personnalisés.



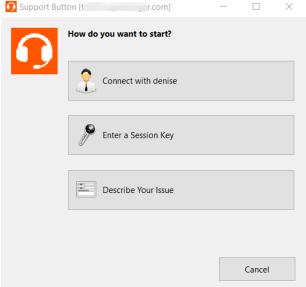
Ce bouton ouvre une boîte de dialogue invitant votre utilisateur à démarrer une session. Si ce bouton a été préconfiguré pour démarrer une session avec une équipe ou un technicien d'assistance spécifié, votre utilisateur peut commencer une session en cliquant sur le bouton **Se connecter**.

Le client peut aussi saisir une clé de session ou décrire son problème. En saisissant une clé de session, le client se connectera au technicien d'assistance qui a généré la clé, que celui-ci soit associé ou non à ce bouton d'assistance technique.



Remarque: Un bouton d'assistance technique ne peut pas être déployé depuis une session qui a été lancée depuis un portail public avec authentification SAML et un bouton d'assistance technique ne peut pas être utilisé pour démarrer une session avec un portail public qui requiert une authentification SAML.

Si une annonce d'utilisateur est active pour le site public auquel ce bouton d'assistance technique est associé, ces messages s'affichent en haut. Les avis peuvent alerter les clients en cas de problèmes informatiques à large impact pour lesquels aucune assistance technique n'est nécessaire, ce qui permet au client de ne pas rejoindre inutilement une session d'assistance technique.



Si un planning est défini pour ce site public et que l'heure actuelle n'est pas une heure d'ouverture, les méthodes de lancement de session autres que les clés de session sont supprimées du bouton d'assistance technique, et un message indiquant que le portail est fermé s'affiche.

Si vous avez intégré un bouton d'assistance technique dans une application externe, ce bouton d'assistance technique apparaît sous la forme d'un lien dans la barre de titre de l'application. Ce lien peut entraîner l'affichage de la boîte de dialogue des options d'ouverture de session, l'affichage de l'enquête de soumission de problème avec un problème présélectionné ou l'affectation de l'utilisateur à une file d'attente avec un problème présélectionné.



TC: 7/18/2022



Enquête de satisfaction de l'utilisateur : soumission de commentaires

À la fin de la session, et si aucun Jump Client n'a été installé pour un accès ultérieur, votre client est informé que vous ne pouvez plus voir son ordinateur ou y accéder, et que BeyondTrust a été entièrement désinstallé.

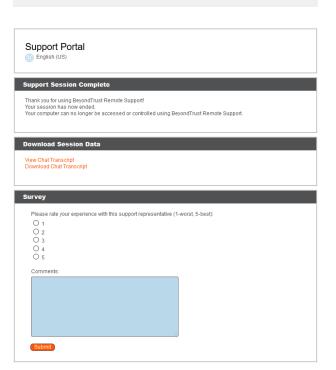
Remote Support [09/19/2019 10:23:53 PM]

Thank you for using BeyondTrust Remote Support!
Your session has now ended.
Your computer can no longer be accessed or controlled using BeyondTrust Remote Support.

OK

Si votre administrateur a activé une enquête de satisfaction, votre client sera redirigé vers une enquête visant à évaluer son expérience au cours de la session. Votre administrateur peut entièrement personnaliser cette enquête à partir de l'interface d'administration et étudier les réponses plus tard dans les rapports de session.

Autrement, si votre administrateur a configuré une URL de redirection d'après-session, une fenêtre de navigation s'ouvre sur l'ordinateur de votre client, le redirigeant vers le site spécifié.





Client de participant à une présentation : rejoindre une présentation



Remarque: la fonction de présentation doit être activée lors de la création de votre site d'assistance technique. Si elle n'est pas disponible et que vous devez exécuter des présentations, veuillez contacter l'assistance ou l'administrateur de votre site.



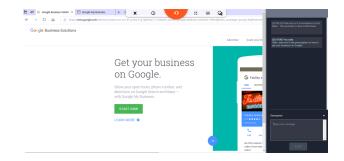
IMPORTANT!

La fonction de présentation ne sera plus prise en charge à partir de la version Remote Support 22.1 et n'est pas incluse dans les déploiements sur nouveau site. Pour les mises à niveau, cette option est paramétrée sur ON, mais vous pouvez la désactiver avec OFF. Si vous avez un déploiement sur un nouveau site et que vous devez exécuter des présentations, veuillez contacter l'assistance ou l'administrateur de votre site.

Pour rejoindre une présentation à partir d'un ordinateur, votre participant se connecte immédiatement et sans interruption à travers un navigateur utilisant HTML5. Votre participant dispose de plusieurs méthodes pour rejoindre une présentation.

Les participants peuvent également rejoindre une présentation à partir d'un appareil iOS ou Android. Pour ce faire, il doit télécharger l'application de présentation BeyondTrust. Pour plus d'informations, reportez-vous à la documentation BeyondTrust pour le périphérique concerné.

Votre administrateur peut définir les messages que votre participant verra, s'il y en a un, avant le début de la présentation. Un accord du participant et un message de bienvenue peuvent notamment s'afficher. En fonction de l'état de la présentation, le participant peut voir un message indiquant que le présentateur a mis fin à la présentation ou que la présentation est terminée et qu'il peut donc fermer le navigateur. Si personne n'est disponible pour effectuer la présentation, un message de présentation orpheline peut également être affiché.



Au cours d'une présentation, les participants peuvent voir votre bureau ou les applications sélectionnées et peuvent discuter avec vous uniquement ou avec vous et d'autres participants.

En cliquant sur l'icône B orange, les participants peuvent choisir les actions à effectuer depuis la barre d'outils. Ils peuvent quitter la session, voir les détails de la présentation, passer en plein écran, changer la taille de l'écran et activer ou désactiver le panneau de messagerie instantanée.

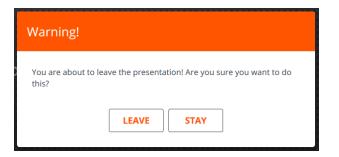


Vous pouvez aussi partager le contrôle de la souris et du clavier avec le participant. La barre d'outils et le panneau de messagerie instantanée sont verrouillés à leur emplacement lorsqu'ils ont le contrôle. Ce contrôle ne peut être attribué qu'à un seul participant à la fois. Vous pouvez toujours annuler le contrôle du participant à tout moment.

TC: 7/18/2022



À la fin de la présentation, les participants reçoivent un message leur demandant s'ils souhaitent quitter la présentation.

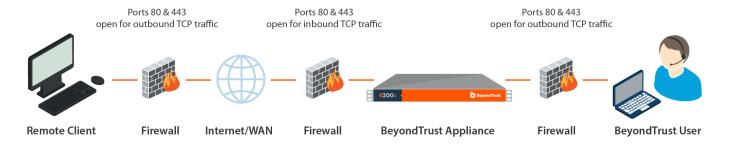




Ports et pare-feu

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

TYPICAL NETWORK SETUP



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

Pour obtenir une assistance au niveau de la configuration de votre pare-feu, veuillez contacter le fabricant du logiciel du pare-feu.

• Des exemples de règles de pare-feux basées sur l'emplacement du B Series Appliance peuvent être trouvés à l'adresse www.beyondtrust.com/docs/remote-support/getting-started/deployment/dmz/firewall-rules.htm.

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



Régler les problèmes de connexion à la console du technicien d'assistance BeyondTrust

- 1. Vérifiez que vous êtes connecté à la console du technicien d'assistance.
- 2. Si vous avez choisi d'utiliser la liste des techniciens d'assistance, assurez-vous que votre nom affiché est visible sur votre site public. Vous pouvez modifier ce statut dans le menu Assistance technique ou depuis l'icône de la barre d'état système en sélectionnant ou désélectionnant Apparaît dans la liste des techniciens d'assistance.
- 3. Essayez d'appliquer la procédure initiale de démarrage d'une session BeyondTrust sur votre propre ordinateur. Parvenez-vous à télécharger le client d'utilisateur ?
- 4. Vérifiez que l'utilisateur distant est connecté à Internet. Votre utilisateur parvient-il à accéder à votre site public?
- 5. Guidez votre utilisateur tout au long du processus que vous avez suivi pour tester le téléchargement du client d'utilisateur à l'étape 3 de ce guide de dépannage. Votre client parvient-il à télécharger le client d'utilisateur ?
- 6. Si le téléchargement ne démarre pas quand l'utilisateur clique sur votre nom, entre une clé de session ou saisit une demande d'assistance technique, demandez-lui de maintenir enfoncée la touche **Ctrl** et d'appuyer sur **F5**. En principe, cette opération vide le cache du navigateur, garantissant que l'utilisateur n'essaie pas de télécharger une version expirée du client d'utilisateur.
- 7. Si cela ne fonctionne pas et que votre utilisateur n'est pas invité à enregistrer ou exécuter un fichier, le pare-feu derrière lequel se trouve votre utilisateur peut bloquer le téléchargement. Contactez l'BeyondTrust Technical Support via www.beyondtrust.com/support pour obtenir une solution.
- 8. Demandez à votre client distant de désinstaller le client BeyondTrust, de redémarrer son ordinateur, puis de relancer le fichier exécutable.
- 9. Assurez-vous que l'utilisateur distant a désactivé les pare-feu logiciels qui pourraient bloquer les connexions sortantes. Sont concernés notamment McAfee Security, Norton Security et Zone Alarm. Ces pare-feu bloquent occasionnellement les connexions sortantes, même après leur désactivation, et devraient peut-être être désinstallés.
- 10. Il se peut également que votre client ait été invité à autoriser ou refuser/bloquer le client d'utilisateur lors de l'exécution du client téléchargé. Si le client a cliqué sur Refuser/Bloquer, demandez-lui d'ouvrir le logiciel de sécurité Internet sur son ordinateur et de changer l'entrée de bomgar-scc.exe en Autoriser/Permettre. Demandez à l'utilisateur de suivre à nouveau la procédure de téléchargement, cette fois en cliquant sur Enregistrer plutôt que sur Exécuter. Puis, demandez-lui de relancer le fichier exécutable et de cliquer sur Autoriser/Permettre. Si la session ne se connecte toujours pas, demandez au client de relancer le fichier exécutable enregistré ; il ne devrait pas recevoir de nouvelle invitation, et la session devrait se connecter.
- 11. Vérifiez si votre utilisateur se trouve derrière un serveur proxy. Assurez-vous que votre client a correctement entré ses informations d'authentification pour permettre au client d'utilisateur de se connecter à vous.
- 12. Si les étapes suivantes ne permettent pas d'établir une connexion, contactez l'BeyondTrust Technical Support à l'adresse www.beyondtrust.com/support.



Avis de non-responsabilité, limitations associées à la licence et assistance technique

Avis de non-responsabilité

Ce document est fourni exclusivement à titre informatif. BeyondTrust Corporation peut modifier ce contenu sans préavis. Le présent document n'est pas garanti être dépourvu d'erreurs, ni ne fait l'objet d'autres garanties ou conditions, orales ou implicites en vertu de la loi, y compris des garanties et conditions implicites de qualité marchande ou d'adéquation à des fins données. BeyondTrust Corporation renonce à toute responsabilité concernant le présent document et aucune obligation contractuelle n'est formulée, directement ou indirectement, par le présent document. Les technologies, fonctionnalités, services et processus décrits aux présentes peuvent faire l'objet de modifications sans préavis.

Tous droits réservés. Les autres marques déposées identifiées sur cette page sont la propriété de leurs propriétaires respectifs. BeyondTrust n'est pas une banque à charte, une société de fiducie ou une institution de dépôt. Elle n'est pas autorisée à accepter des dépôts ou des comptes en fiducie et n'est ni sous licence ni gouvernée par une autorité bancaire nationale ou fédérale.

Limitations associées à la licence

Une licence Remote Support BeyondTrust permet à un technicien d'assistance à la fois d'intervenir sur un nombre illimité d'ordinateurs distants, en mode surveillé ou non surveillé. Même si plusieurs comptes peuvent partager la même licence, il faut deux licences ou plus (une pour chacun des techniciens Service client présents) pour permettre à plusieurs techniciens Service client d'intervenir simultanément.

Assistance technique

Chez BeyondTrust, nous nous engageons à fournir une qualité de service optimale en veillant à ce que nos clients disposent de tout ce qui est nécessaire à une productivité maximale. Si vous avez besoin d'aide, contactez : www.beyondtrust.com/support.

Pour bénéficier de l'assistance technique, vous devez souscrire chaque année un plan de maintenance.