BeyondTrust

Assistance technique à distance
Guide d’administration 21.1

TC:4/29/2021

Table des matières

Interface d'administration Remote Support

Ce guide offre un aperçu détaillé de **/login** et a pour objectif de vous aider à administrer les utilisateurs BeyondTrust et votre logiciel BeyondTrust. Le Serveur d'accès à distance sécurisé sert de point d'administration et de gestion central de votre logiciel BeyondTrust et vous permet de vous connecter depuis n'importe quel endroit disposant d'un accès internet pour télécharger la console du technicien d'assistance.

Utilisez ce guide uniquement après que l'administrateur a procédé à l'installation et à la configuration initiales du Serveur d'accès à distance sécurisé, comme l'explique le Guide d'installation matérielle du Serveur d'accès à distance sécurisé à l'adresse www.beyondtrust.com/docs/remote-support/getting-started/deployment/hardware/. Une fois BeyondTrust correctement installé, vous pouvez immédiatement commencer à fournir une assistance technique aux clients. Si vous avez besoin d'aide, contactez : www.beyondtrust.com/support.

Connexion à l'interface d'administration

Connexion

Connectez-vous à l'interface d'administration de l'utilisateur en allant à l'URL de votre serveur, suivie de **/login**. L'interface d'administration de l'utilisateur permet aux administrateurs de créer des comptes d'utilisateur et de configurer les paramètres du logiciel.

Bien que l'URL de votre serveur puisse être n'importe quel DNS enregistré, il est plus que probable qu'il s'agisse d'un sous-domaine du domaine principal de votre entreprise (par ex. support.example.com/login).

Nom d'utilisateur par défaut : **admin**

Mot de passe par défaut : **password**

Remote Support BeyondTrust étant distribué sous licence par utilisateurs concurrents, vous pouvez configurer autant de comptes que nécessaire, chacun ayant un nom d'utilisateur et un mot de passe uniques.

> ***Remarque :*** *pour des raisons de sécurité, le nom d'utilisateur et le mot de passe d'administration utilisés pour l'interface /appliance sont différents de ceux utilisés pour l'interface /login et doivent être gérés séparément.*

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

> *Pour plus d'informations sur l'authentification à deux facteurs, veuillez consulter Comment utiliser l'authentification à deux facteurs avec Remote Support BeyondTrust à l'adresse www.beyondtrust.com/docs/remote-support/how-to/2-factor-authentication/.*

> ***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 des codes par e-mail est désactivée de façon permanente.*

Utiliser l'authentification de navigateur intégrée

Si Kerberos a été correctement configuré pour une authentification unique, vous pouvez cliquer sur le lien pour utiliser l'authentification de navigateur intégrée, ce qui vous permet d'entrer directement dans l'interface Web sans avoir à saisir vos informations d'authentification.

> *Pour plus d'informations, veuillez consulter la section Serveur Kerberos pour authentification unique à l'adresse https://www.beyondtrust.com/docs/remote-support/how-to/integrations/security-providers/kerberos/index.htm.*

Vous avez oublié votre mot de passe ?

Ce lien est visible si la réinitialisation du mot de passe a été activée sur la page **/login > Gestion > Sécurité** et le serveur SMTP a été configuré pour votre site. Pour réinitialiser le mot de passe, cliquez sur le lien, saisissez et confirmez votre adresse e-mail, puis cliquez sur **Envoyer**. Si plusieurs utilisateurs partagent la même adresse e-mail, vous devez confirmer votre nom d'utilisateur. Vous recevrez alors

un lien par e-mail qui vous renvoie à la page de connexion. Sur l'écran de connexion, saisissez et confirmez votre nouveau mot de passe, puis cliquez sur **Modifier le mot de passe**.

Accord de connexion

Les administrateurs peuvent restreindre l'accès à l'écran de connexion en activant un accord de connexion devant impérativement être validé pour pouvoir continuer. L'accord de connexion peut être activé et personnalisé sur la page **/login > Gestion > Configuration du Site**.

État

Informations : consultation des informations logicielles Remote Support BeyondTrust

État | Informations

État du site

La page principale de l'interface /login Remote Support de BeyondTrust permet d'avoir un aperçu général des informations sur les statistiques de votre Serveur d'accès à distance sécurisé. Lorsque vous contactez l'BeyondTrust Technical Support pour des mises à jour de logiciel ou des résolutions de problèmes, il se peut que l'on vous demande d'envoyer par e-mail une capture d'écran de cette page.

Fuseau horaire

Un administrateur peut sélectionner le fuseau horaire approprié dans le menu déroulant. La date et l'heure du serveur seront ainsi définies en fonction de la région sélectionnée.

Nombre total de Jump Clients autorisés

Vérifiez le nombre total de Jump Clients actifs et passifs qui sont autorisés sur votre système. Si vous avez besoin de davantage de Jump Clients, contactez l'BeyondTrust Technical Support.

Licences d'assistance technique complètes

Consultez le nombre de licences disponibles sur votre Serveur d'accès à distance sécurisé. Si vous avez besoin de davantage de licences, contactez le service commercial de BeyondTrust.

Licences d'assistance technique de messagerie instantanée

Consultez le nombre de licences de messagerie instantanée disponibles sur votre Serveur d'accès à distance sécurisé. Si vous avez besoin de davantage de licences, contactez le service commercial de BeyondTrust.

Redémarrer le logiciel Remote Support

Vous pouvez redémarrer le logiciel BeyondTrust à distance. Ne redémarrez votre logiciel que si cela vous a été demandé par l'BeyondTrust Technical Support.

Logiciel client

Ceci est le nom d'hôte auquel les logiciels clients BeyondTrust se connectent. Si le nom d'hôte tenté par un logiciel client doit changer, prévenez l'BeyondTrust Technical Support des changements requis afin qu'elle puisse créer une mise à jour logicielle.

Clients connectés

Consultez le nombre et le type de clients logiciels BeyondTrust connectés à votre Serveur d'accès à distance sécurisé.

Clients GIAPT

Consultez le nombre de gestionnaires d'informations d'authentification de point de terminaison BeyondTrust (GIAPT) connectés à votre Serveur d'accès à distance sécurisé. Vous pouvez également consulter les informations liées à l'emplacement et la durée de connexion de chaque GIAPT.

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

> ***Remarque :*** *lorsque plusieurs GIAPT sont connectés au site BeyondTrust, le Serveur d'accès à distance sécurisé achemine les demandes vers le GIAPT ayant été le plus longtemps connecté au serveur.*

Techniciens d'assistance : consultation des techniciens d'assistance connectés et envoi de messages

État	Techniciens d'assistance

Techniciens d'assistance connectés

Consultez une liste des techniciens d'assistance connectés sur la console du technicien d'assistance, leur durée de connexion et s'ils exécutent des sessions d'assistance technique ou de présentation.

Mettre fin à la session

Vous pouvez mettre fin à la connexion d'un technicien d'assistance à la console du technicien d'assistance.

Envoyer un message aux techniciens d'assistance

Envoyez un message à tous les techniciens d'assistance connectés via une fenêtre contextuelle dans la console du technicien d'assistance.

Disponibilité étendue des techniciens d'assistance

Consultez les techniciens d'assistance ayant activé le mode disponibilité étendue. L'activation du mode disponibilité étendue utilise une licence.

Désactiver la disponibilité étendue

Vous pouvez désactiver la disponibilité étendue d'un technicien d'assistance afin de libérer une licence.

Nouveautés : consultation des informations relatives à la version du logiciel

État	Nouveautés

Nouveautés

Passez facilement en revue les fonctionnalités de BeyondTrust disponibles avec chaque nouvelle version. Tenez-vous informé des nouvelles fonctions disponibles pour tirer le meilleur parti de votre déploiement BeyondTrust.

La première fois que vous vous connectez à l'interface d'administration après une mise à niveau du logiciel BeyondTrust, la page **Nouveautés** est mise en évidence et vous informe des nouvelles fonctions disponibles sur votre site. Vous devez être un administrateur pour voir cet onglet.

Les informations affichées sur la page **Nouveautés** sont également accessibles aux techniciens d'assistance dans la console du technicien d'assistance dans le menu **Aide > À propos**.

Pour plus d'informations, veuillez consulter la section Listes de mises à jour et de fonctions à l'adresse https://www.beyondtrust.com/docs/remote-support/updates/index.htm.

Mon compte : modification du mot de passe et du nom d'utilisateur, et téléchargement de la Console du technicien d'assistance ainsi que d'autres logiciels

Mon compte

Mon compte

Console Web du technicien d'assistance

Lancez la console Web du technicien d'assistance, une console du technicien d'assistance basée sur le Web. Accédez à des systèmes distants depuis votre navigateur sans avoir à télécharger et à installer complètement la console du technicien d'assistance.

Console du technicien d'assistance

Choisir une plate-forme

Choisissez le système d'exploitation sur lequel vous souhaitez installer ce logiciel. Ce menu déroulant sélectionne par défaut l'installeur approprié détecté pour votre système d'exploitation.

> *Pour plus d'informations, veuillez consulter le Guide de la Console Web du technicien d'assistance à l'adresse https://www.beyondtrust.com/docs/remote-support/getting-started/rep-web/index.htm.*

Télécharger la Console du technicien d'assistance

Téléchargez l'installeur de la console du technicien d'assistance BeyondTrust afin de fournir une assistance technique à distance.

Pour installer la console du technicien d'assistance sans afficher de fenêtre, d'indicateur de chargement, d'erreur ou autres alertes visibles, ajoutez **/S** à la fin de la commande de l'EXE. Pour le déploiement en masse, BeyondTrust recommande d'utiliser l'installeur MSI.

Pour les administrateurs système devant déployer l'installeur de la console sur un grand nombre de systèmes, l'installeur Microsoft peut être utilisé avec l'outil de gestion de système de votre choix. Dans votre invite de commande, lorsque vous composez la commande pour installer la console avec un MSI, modifiez pour indiquer le répertoire de téléchargement du MSI et saisissez la commande figurant à la page **Mon compte**.

Vous pouvez inclure des paramètres facultatifs pour l'installation du MSI.

- **INSTALLDIR=** accepte tout chemin d'accès à un répertoire valide dans lequel vous voulez installer la console.
- **RUNATSTARTUP=** accepte **0** (par défaut) ou **1**. Si vous saisissez 1, la console s'exécutera à chaque démarrage de l'ordinateur.
- **ALLUSERS=** accepte **“”** (par défaut) ou **1**. **“”** est la valeur par défaut. Cet attribut n'est nécessaire que pour spécifier des installations par machine individuelle.

ALLUSERS="" donne une installation pour un seul utilisateur. Ceci force la console du technicien d'assistance à s'installer dans le même contexte qui est utilisé pour exécuter l'installation MSI. Cela n'est pas idéal si le système « Local System » est utilisé pour exécuter l'installation, comme c'est souvent le cas avec des outils de déploiement en masse. Il est impossible de cibler l'installation sur un utilisateur spécifique grâce aux paramètres MSI, donc si vous déployez le MSI avec un système de déploiement automatisé en utilisant l'indicateur d'installation d'utilisateur unique, le système de déploiement doit exécuter l'installation MSI dans le contexte du même utilisateur qui doit se connecter à la console.

- **SHOULDAUTOUPDATE=1** Si vous n'installez que pour l'utilisateur actuel, vous pouvez opter pour une mise à jour automatique de la console chaque fois que le site est mis à niveau en saisissant une valeur de **1** ; une valeur de **0** (par défaut) empêche la mise à jour automatique et la console devra être réinstallée manuellement lorsque le site sera mis à niveau. Si vous installez la console pour tous les utilisateurs, elle ne se mettra pas automatiquement à jour.
- La commande **QUIET** exécute l'installeur sans afficher de fenêtre, d'indicateur de chargement, d'erreur ou d'alerte visible.

Remarque : *si vous utilisez **ALLUSERS=1** avec **SHOULDAUTOUPDATE=1**, la console du technicien d'assistance ne se mettra pas automatiquement à jour. Si vous utilisez **SHOULDAUTOUPDATE=1** sans **ALLUSERS=1**, la console du technicien d'assistance devrait se mettre à jour automatiquement sans demander d'informations d'authentification en dehors de celles de l'utilisateur BeyondTrust et de l'utilisateur Windows actif. Aucune information d'authentification admin nécessaire.*

IMPORTANT !

Lorsqu'une console du technicien d'assistance est installée par MSI, certaines informations doivent quand même être récupérées auprès du serveur. Au cours de la première connexion, un jeton est fourni à la console du technicien d'assistance et est utilisé pour demander des mises à jour logicielles. Si aucun utilisateur ne se connecte à la console du technicien d'assistance avant que le serveur soit mis à niveau, ou si le MSI d'une version précédente est utilisé pour installer la console du technicien d'assistance, la console ne réussira pas à se mettre à jour, car elle ne dispose pas du jeton nécessaire. Si cela se produit, l'erreur suivante s'affiche

« Erreur de communication avec le serveur lors de la mise à jour du logiciel. Veuillez mettre à niveau votre logiciel en le téléchargeant depuis le site internet. (1.1gws) »

Pour cette raison, si plus d'une console du technicien d'assistance sont déployées en masse par MSI, veuillez faire le nécessaire pour faire en sorte que les utilisateurs s'authentifient avec leurs consoles au moins une fois avant l'installation de mises à jour sur le Serveur d'accès à distance sécurisé.

Pour plus d'informations, veuillez consulter :

- *Console du technicien d'assistance BeyondTrust à l'adresse https://www.beyondtrust.com/docs/remote-support/getting-started/rep-console/index.htm*
- *Déploiement en masse du logiciel BeyondTrust sur Mac à l'adresse https://www.beyondtrust.com/docs/remote-support/how-to/mass-deploy-mac/index.htm*

Modifier votre mot de passe

BeyondTrust vous recommande de changer régulièrement votre mot de passe.

Nom d'utilisateur, Mot de passe actuel, Nouveau mot de passe

Vérifiez que vous êtes connecté au compte dont vous souhaitez changer le mot de passe, puis saisissez votre mot de passe actuel. Créez et confirmez un nouveau mot de passe pour votre compte. Vous pouvez définir le mot de passe de votre choix, tant que la chaîne reste conforme à la règle définie sur la page **/login > Gestion > Sécurité**.

Modifiez vos paramètres d'e-mail

Adresse e-mail

Définissez une adresse e-mail où envoyer les notifications, comme les réinitialisations de mot de passe ou le mode Disponibilité étendue.

Mot de passe

Saisissez le mot de passe de votre compte /login, pas celui de votre e-mail.

Langue d'e-mail préférée

Si plus d'une langue est activée sur ce site, sélectionnez la langue dans laquelle envoyer les e-mails.

Modifier vos noms affichés

Nom affiché privé

Votre nom tel qu'il s'affiche dans toutes les communications internes entre techniciens d'assistance, les rapports de transcription de messagerie instantanée, les rapports d'activité d'équipe, etc.

Nom affiché public

Votre nom tel qu'il s'affiche pour les utilisateurs.

> ***Remarque :*** *ces deux champs sont synchronisés par défaut. Le texte saisi dans le champ* ***Nom affiché privé*** *est donc automatiquement copié dans le champ* ***Nom affiché public****. Pour modifier votre nom affiché public, saisissez simplement le nom sous lequel vous souhaitez apparaître pour les utilisateurs. Pour resynchroniser les champs, saisissez deux fois le même texte.*

Authentification à deux facteurs

Activer l'authentification à deux facteurs

Activez l'authentification à deux facteurs (2FA) pour améliorer le niveau de sécurité des utilisateurs accédant à /login et à la console du technicien d'assistance BeyondTrust. Cliquez sur **Activer l'authentification à deux facteurs**, puis utilisez l'appli d'authentification de votre choix, comme BeyondTrust Verify ou Google Authenticator pour scanner le code QR affiché sur la page. Vous pouvez aussi saisir manuellement le code alphanumérique sous le code QR dans votre appli d'authentification.

L'application enregistre automatiquement le compte et vous propose des codes. Saisissez votre mot de passe et le code généré par l'application sélectionnée, puis cliquez sur **Activer**. Veuillez noter qu'après avoir été généré, un code n'est valable que pendant 60 secondes. Une fois connecté, vous avez la possibilité de changer d'application d'authentification ou de désactiver l'authentification 2FA.

Remarque : *si votre administrateur a imposé l'option 2FA, il est impossible de la désactiver.*

Pour plus d'informations sur l'authentification à deux facteurs, veuillez consulter Comment utiliser l'authentification à deux facteurs avec Remote Support BeyondTrust à l'adresse www.beyondtrust.com/docs/remote-support/how-to/2-factor-authentication/.

Mode disponibilité étendue

Activer ou désactiver

Activez ou désactivez le mode Disponibilité étendue en cliquant sur le bouton **Activer/Désactiver**. Le mode disponibilité étendue vous permet de recevoir des invitations par e-mail de la part d'autres utilisateurs demandant de partager une session lorsque vous n'êtes pas connecté à la console.

Pour plus d'informations, consultez la section Utiliser la disponibilité étendue pour rester accessible lorsque vous n'êtes pas connecté à l'adresse https://www.beyondtrust.com/docs/remote-support/getting-started/rep-console/extended-availability.htm.

Changer votre photo

Changer ou supprimer la photo associée à ce compte. Cette photo est affichée dans la fenêtre de messagerie instantanée du client d'utilisateur et sur l'interface d'administration **/login**. L'image utilisée doit être au format .png ou .jpeg, ne pas faire plus d'un Mo et avoir des dimensions minimales de 80x80 pixels. Cliquez sur **Choisir le fichier** pour sélectionner une image. Une fois que le fichier d'image choisi est affiché, cliquez sur **Transférer** pour l'utiliser, ou sur **Annuler** si vous ne voulez pas garder l'image que vous avez sélectionnée. Si l'image sélectionnée a les bonnes dimensions, un message s'affiche, indiquant que le transfert a réussi.

Pour plus d'informations, veuillez visiter Client d'utilisateur : Interface de Session d'assistance technique à l'adresse https://www.beyondtrust.com/docs/remote-support/getting-started/customer-client/customer-support-interface.htm.

Téléchargement de pilotes

Carte à puce virtuelle

Choisir une architecture Windows

Choisissez le système d'exploitation sur lequel vous souhaitez installer ce logiciel. Ce menu déroulant sélectionne par défaut l'installeur approprié détecté pour votre système d'exploitation.

Si vous devez utiliser une carte à puce locale sur un système distant faisant l'objet d'une assistance technique, vous devez installer le pilote de carte à puce virtuelle Remote Support BeyondTrust sur les systèmes du technicien d'assistance et du client. Téléchargez et distribuez le pilote approprié de carte à puce virtuelle de technicien d'assistance (Installeur VSC de technicien d'assistance) pour tous les techniciens d'assistance de votre centre d'assistance qui ont besoin de la fonction de carte à puce virtuelle à distance. Le pilote peut être installé manuellement ou avec un outil de déploiement de logiciel. Une fois le pilote installé, il crée un service : Remote Support VSC Representative Service.

Configuration

Options : gérer les options de file d'attente des sessions, l'enregistrement des sessions, la configuration des SMS

Configuration | **Options**

Options de mise en attente de session d'assistance technique

Exiger des sessions terminées à la déconnexion ou fermeture

Si vous cochez **Exiger des sessions terminées à la déconnexion ou fermeture**, les utilisateurs ne pourront pas se déconnecter de la console s'ils ont des onglets de session ouverts.

Règles de retournement de session

Il existe cinq règles à suivre lorsque la connexion à une session d'un technicien d'assistance est perdue ou terminée : (1) Si la session est partagée, elle est transférée vers le technicien d'assistance qui a partagé la session le plus longtemps. Si elle n'est pas partagée, elle est transférée à (2) la dernière file d'attente dans laquelle elle se trouvait, (3) la file d'attente dans laquelle elle est entrée, ou (4) une file d'attente de récupération désignée. Ce deuxième ensemble de règles peut être activé ou désactivé pour les sessions standard (sous surveillance), les sessions de Jump (autonomes), ou les deux. (5) Enfin, si aucun technicien d'assistance n'est trouvé, la session se termine.

> ***Remarque :*** *si la session se trouve dans une file d'attente persistante, la logique ci-dessus ne s'applique pas. Vous pouvez activer les files d'attente persistantes sur la page* ***Configuration > Équipes d'assistance technique****.*

Activer les règles 2, 3 et 4 pour les sessions normales et/ou les Jump Sessions

Activez les trois règles de retournement du milieu pour des sessions initiées par les utilisateurs et/ou des sessions autonomes.

> *Pour plus d'information, veuillez consulter Consultation de Session d'assistance technique en attente à l'adresse https://www.beyondtrust.com/docs/remote-support/getting-started/rep-console/queues.htm.*

Options Equilibrium

Afficher les données de session dans toutes les boîtes de dialogue d'alerte

Lorsqu'une session est attribuée, le technicien d'assistance reçoit une alerte. Si l'option **Afficher les données de session dans toutes les boîtes de dialogue d'alerte** est cochée, toutes les alertes d'attribution de session afficheront les informations de demande d'assistance technique.

Pour plus d'informations, veuillez consulter Acceptation d'une session pour démarrer l'assistance technique à l'adresse https://www.beyondtrust.com/docs/remote-support/getting-started/rep-console/accepting-a-session.htm.

Options d'enregistrement de session d'assistance technique

Activer le Partage d'écran / Enregistrement de la fonction Montrer mon écran / Enregistrement de l'interpréteur de commandes

Indiquez si les sessions de partage d'écran, les sessions Montrer mon écran et/ou les sessions interpréteur de commandes doivent être automatiquement enregistrées sous forme de vidéos.

Partage d'écran / Résolution de l'enregistrement de la fonction Montrer mon écran / Résolution de l'enregistrement de l'interpréteur de commandes

Définissez la résolution à laquelle visionner l'enregistrement de session.

***Remarque :** tous les enregistrements sont enregistrés en format brut ; le choix de la résolution affecte uniquement la lecture.*

Activer l'enregistrement automatique des informations système

Choisissez si les informations système doivent être automatiquement récupérées depuis l'ordinateur distant au début de la session pour qu'elles soient disponibles plus tard dans les détails du rapport de session.

Enregistrement des informations système pour plateformes mobiles

Lorsque les plateformes mobiles sont prises en charge, choisissez **Standard** pour afficher uniquement une sélection de données, ou **Étendu** pour afficher toutes les données disponibles.

***Remarque :** ces paramètres de niveau site peuvent être remplacés par des paramètres de site public et des préférences utilisateur, tels que configurés dans la page **Portails publics > Client d'utilisateur**.*

Options d'enregistrement de présentation

Activer l'enregistrement de partage d'écran

Choisissez si les présentations doivent automatiquement être enregistrées en vidéo.

***Remarque :** lorsque vous commencez une présentation et que vous attendez que les participants la rejoignent, l'enregistrement ne commencera que quand le premier participant rejoint la présentation. Si personne ne rejoint la présentation, l'enregistrement de session ne sera pas créé.*

Résolution d'enregistrement de partage d'écran

Définissez la résolution à laquelle visionner l'enregistrement de présentation.

Options pair-à-pair

Désactivé(e)

Désactive les connexions pair-à-pair. Pour activer cette fonction, vous devez choisir un serveur pour négocier la session. Lorsque le partage d'écran, le transfert de fichiers ou l'interpréteur distant est détecté, la connexion pair-à-pair est tentée. Si elle réussit, cela crée une connexion directe entre le technicien d'assistance et les systèmes clients, tout en continuant d'envoyer un second flux de données au serveur à des fins d'audit. Si pour une raison quelconque la connexion pair-à-pair ne peut pas être établie, le trafic de session redevient par défaut une connexion gérée par le serveur.

Utiliser le serveur hébergé pair-à-pair de BeyondTrust

Ceci est le réglage par défaut. Les clients BeyondTrust tentent d'atteindre une connexion pair-à-pair à travers le serveur hébergé par BeyondTrust. Ceci nécessite que vos clients BeyondTrust puissent envoyer des demandes de connexion sortantes UDP 3478 à stun.bomgar.com. Ce réglage devrait fonctionner dans la plupart des situations.

Utiliser le serveur comme serveur pair-à-pair

Si votre organisation requiert des paramètres de sécurité spécifiques pour le trafic, vous pouvez utiliser le serveur comme serveur pair-à-pair. Ceci nécessite que votre Serveur d'accès à distance sécurisé puisse accepter les demandes de connexion entrantes UDP 3478 par vos clients BeyondTrust. Vous devez vous assurer que les pare-feu entre les clients et le Serveur d'accès à distance sécurisé autorisent le passage de l'UDP 3478.

> *Pour plus d'informations, veuillez consulter la section Administration du serveur : Restrictions relatives aux comptes, réseaux et ports, configuration de Syslog, activation de l'accord de connexion, et réinitialisation des comptes administrateur à l'adresse https://www.beyondtrust.com/docs/remote-support/getting-started/deployment/web/security-appliance-administration.htm.*

Options relatives aux e-mails d'invitation

Activer les e-mails client pour les invitations d'assistance technique et de présentation

Lorsque ceci est activé, les techniciens d'assistance peuvent envoyer des e-mails d'assistance technique et d'invitation à des présentations à partir du client d'e-mail local (par exemple : Outlook). Ces e-mails sont envoyés en utilisant le compte e-mail du technicien d'assistance. Le technicien d'assistance peut voir et modifier l'e-mail si nécessaire.

Activer les e-mails serveur pour les invitations d'assistance technique

Si ceci est activé, les techniciens d'assistance peuvent envoyer des e-mails d'invitation à partir du Serveur d'accès à distance sécurisé plutôt qu'à partir de leur client e-mail local. Une fenêtre de dialogue demande au technicien d'assistance de spécifier le destinataire de l'e-mail. Le technicien d'assistance ne peut pas prévisualiser ou modifier le sujet ou le texte de l'e-mail. L'adresse e-mail à partir de laquelle les e-mails côté serveur sont envoyés peut être personnalisée pour chaque portail sur la page **Portails publics > Client d'utilisateur**. L'adresse spécifiée sur la page **Gestion > Configuration e-mail** peut également être utilisée.

Pour plus d'informations, consultez Génération d'une clé de session en vue de démarrer une Session d'assistance technique à l'adresse https://www.beyondtrust.com/docs/remote-support/getting-started/rep-console/session-keys.htm.

Passerelle SMS

URL de la passerelle SMS

Saisissez une URL de passerelle SMS sécurisée depuis votre FAI ou un fournisseur de passerelle tiers pour offrir aux techniciens d'assistance la possibilité d'envoyer des clés d'accès à l'assistance technique par SMS. Envoyez des messages d'assistance technique par SMS à un appareil mobile depuis la console du technicien d'assistance. Les SMS envoyés de la sorte à d'autres périphériques mobiles recevront un lien de session. La communication SMS n'est pas journalisée dans le serveur.

Problèmes : gestion des problèmes d'assistance technique

Configuration | **Problèmes**

Problèmes d'assistance technique

Créez des problèmes d'assistance technique pour simplifier l'expérience de votre utilisateur lors d'une demande d'assistance technique sur le portail public. Les problèmes créés peuvent être configurés pour apparaître sur le menu déroulant du formulaire de soumission de problème, et inclure une liste des problèmes d'assistance technique que vos utilisateurs rencontreront probablement.

Étant donné que les problèmes doivent être acheminés vers les Équipes d'assistance technique, vous devez créer des équipes avant de créer des problèmes d'assistance technique.

> *Pour plus d'informations, veuillez consulter la section Configurer les paramètres d'équipe à l'adresse https://www.beyondtrust.com/docs/remote-support/how-to/equilibrium/configure-team-settings.htm.*

> *Pour plus d'informations, veuillez consulter la section Attribuer des compétences aux problèmes à l'adresse https://www.beyondtrust.com/docs/remote-support/how-to/equilibrium/assign-skills-issue.htm.*

Ajouter un nouveau problème d'assistance technique, modifier, supprimer

Créer un nouveau problème, modifier un problème existant ou supprimer un problème existant.

Ajouter ou modifier un problème d'assistance technique

Description

Ajoutez une brève description d'un problème que vous vous attendez à voir dans une demande d'assistance technique. Si le formulaire de soumission de problème est activé, cette description est visible aux utilisateurs, et elle est utilisée pour aider les techniciens d'assistance à déterminer rapidement à quel type de problème l'utilisateur est confronté. La description peut aussi être visible pour les techniciens d'assistance demandant de l'aide depuis la session d'assistance technique.

Nom de code

Définissez également un nom de code, qui sera utilisé à des fins d'intégration. Dans le cas contraire, le système en crée un automatiquement.

Acheminer vers

Utilisez le menu déroulant **Acheminer vers** pour associer ce problème à une équipe spécifique.

Priorité

Définissez la priorité du problème sur **Haute**, **Moyenne** ou **Basse**, selon la façon dont vous souhaitez que le problème soit traité par le système. La priorité par défaut est définie sur **Moyenne**.

Autoriser les techniciens d'assistance technique à demander de l'aide pour ce problème

Cochez ensuite la case si vous souhaitez que les techniciens d'assistance puissent demander de l'aide pour ce problème au cours d'une session. Lorsque cette option est sélectionnée, le problème est ajouté à la liste de la fenêtre **Demander de l'aide** de la console du technicien d'assistance lorsque l'option **Partage de session** est activée.

Compétences requises

Les problèmes peuvent être associés aux compétences exigées pour mieux les résoudre. Les compétences peuvent être définies comme **Plus prisées**, **Moins prisées** ou **Ignorées** selon le niveau de connaissances requis pour résoudre un problème donné. Ceci déterminera la façon dont les demandes d'assistance technique sont acheminées et traitées par le système.

Équipes d'assistance technique : regroupement des techniciens d'assistance en équipes

Configuration | Équipes d'assistance technique

Gérer des équipes d'assistance technique

Le regroupement des techniciens Service client en équipes améliore l'efficacité en désignant un leader au sein des groupes de techniciens d'assistance et en facilitant l'orientation des utilisateurs vers le technicien d'assistance le mieux à même de résoudre un problème donné. Dans la console du technicien d'assistance, chaque équipe apparaît comme une file d'attente séparée pour les session d'assistance technique en attente.

Ajouter une nouvelle équipe, modifier, supprimer

Créer une nouvelle équipe, modifier ou supprimer une équipe existante. La suppression d'une équipe ne supprime pas ses comptes d'utilisateurs, mais uniquement l'équipe à laquelle ils sont associés.

Paramètres Equilibrium

Gérez l'acheminement automatique de session pour cette équipe en utilisant equilibrium.

Ajouter ou modifier des équipes d'assistance technique

Nom d'équipe

Créez un nom unique permettant d'identifier cette équipe.

Nom de code

Définissez également un nom de code, qui sera utilisé à des fins d'intégration. Dans le cas contraire, le système en crée un automatiquement.

Commentaires

Ajoutez des commentaires sur la fonction de cette équipe.

File d'attente persistante

Si cette option est cochée, chaque session d'assistance technique reste dans cette file d'attente même lorsqu'aucun technicien d'assistance n'est disponible. Une session dans cette file d'attente y reste jusqu'à ce qu'un technicien d'assistance ou une opération de l'API la prenne en charge. Cette option offre davantage de souplesse en matière de gestion personnalisée de l'attribution des sessions.

Règles de groupe

Notez toutes les règles de groupe attribuant des membres à cette équipe. Cliquez sur le lien renvoyant vers la page **Règles de groupe** afin de vérifier les membres des règles ou d'en assigner.

Accès au portail

Les techniciens d'assistance peuvent uniquement accéder aux portails auxquels leur équipe a été autorisée à accéder. Les options d'accès au portail permettent aux membres d'une équipe d'accéder à tous les portails ou à certains d'entre eux.

Les membres de cette équipe sont autorisés à accéder à tous les portails

Cochez la case pour permettre aux membres de l'équipe sélectionnée d'accéder à tous les portails.

Autorisez les membres de cette équipe à accéder aux portails suivants :

Cette possibilité n'apparaît que si l'option ci-dessus n'est pas cochée. Cochez la case de chaque portail auquel les membres de l'équipe sélectionnée peuvent accéder. Les membres d'une équipe doivent toujours avoir accès au portail par défaut. Les portails non cochés n'apparaissent pas dans la liste des options de portail lorsque le technicien d'assistance génère une clé de session.

Membres de l'équipe

Lancez une recherche pour ajouter des utilisateurs à cette équipe. Vous pouvez déterminer le rôle de chaque membre, tel que **Membre de l'équipe**, **Chef d'équipe** ou **Responsable d'équipe**. Ces rôles représentent une part significative de la fonction **Tableau de bord** de la console du technicien d'assistance.

Dans le tableau ci-dessous, consultez les membres d'équipe existants. Vous pouvez filtrer la vue en saisissant une chaîne dans la zone de texte **Filtrer par nom**. Vous pouvez aussi modifier les paramètres d'un utilisateur ou supprimer un membre de l'équipe.

Pour ajouter un groupe d'utilisateurs à une équipe, consultez **Utilisateurs et sécurité > Règles de groupe** et assignez ce groupe à une ou à plusieurs équipes dans un rôle donné.

> ***Remarque :***
> *il est possible que les options **Modifier** et **Supprimer** de certains utilisateurs aient été désactivées. Cela arrive lorsqu'on ajoute un utilisateur par le biais d'une règle de groupe.*
>
> *Cliquez sur le lien de la règle de groupe pour modifier la règle de façon globale. Les changements apportés à une règle de groupe s'appliquent à l'ensemble des membres de celle-ci.*
>
> *Vous pouvez aussi ajouter un utilisateur à l'équipe, en ignorant ses paramètres tels qu'il sont définis ailleurs.*

Paramètres Equilibrium

Algorithme de routage

Si cela est défini sur **Le moins occupé**, une session dans cette file d'attente sera assignée au technicien d'assistance le moins occupé qui est disponible pour prendre des sessions depuis cette file d'attente. Si l'option est définie sur **Correspondance de compétences, le moins occupé**, si une session a besoin de compétences et se trouve dans la file d'attente, cette session sera assignée au technicien

d'assistance ayant les meilleures compétences correspondant au problème et disponible pour prendre des sessions depuis cette file d'attente.

Délai d'alerte

Un technicien d'assistance dispose d'autant de temps que défini ici pour accepter ou refuser une session attribuée. Si le technicien d'assistance refuse la session ou ne répond pas avant l'expiration du délai, la session est réattribuée au prochain technicien d'assistance ayant la meilleure correspondance disponible pour accepter des sessions de cette file d'attente.

Règle de session en attente

Vous pouvez également créer une **règle de session en attente**. Lorsque cette option est activée, elle définit la durée pendant laquelle une session peut rester dans la file d'attente. Indiquez ensuite la procédure à appliquer en cas de dépassement du temps d'attente défini : vous pouvez choisir de transférer les sessions vers une file d'attente de dépassement ou de les marquer comme étant en souffrance. Une session qui devient en souffrance déclenche une alerte sonore, clignote dans la file d'attente, déclenche le clignotement de la file d'attente elle-même, et affiche une notification contextuelle. Ces notifications peuvent être modifiées dans les paramètres de la console du technicien d'assistance.

> *Pour plus d'informations, veuillez consulter Equilibrium pour l'acheminement automatique de session à l'adresse https://www.beyondtrust.com/docs/remote-support/how-to/equilibrium/index.htm.*

Paramètres du tableau de bord

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 au cas par cas pour chaque équipe. Ainsi, un utilisateur peut être en mesure d'administrer un autre utilisateur dans une équipe, sans pouvoir administrer ce même utilisateur dans une autre.*

Surveillance des membres de l'équipe depuis le tableau de bord

Si l'option est activée, un chef ou responsable d'équipe peut surveiller les membres de l'équipe depuis le tableau de bord. Choisissez une sélection pour **désactiver** la possibilité de surveiller, restreindre la surveillance à la **Console du technicien d'assistance uniquement**, ou autoriser un chef ou responsable d'équipe à surveiller **tout l'écran** d'un membre de l'équipe. La surveillance affecte tous les responsables et chefs d'équipe de toutes les équipes du site.

Activer l'indicateur de surveillance

Si cette option est cochée, un membre de l'équipe dont l'écran est surveillé verra une icône de surveillance sur son écran.

Activer le transfert de session et la reprise du contrôle sur le tableau de bord

Si cette option est cochée, un chef d'équipe peut prendre le contrôle ou transférer les sessions d'un membre d'équipe. De la même façon, un responsable d'équipe peut administrer les membres et les chefs de l'équipe.

> *Pour plus d'informations, veuillez consulter Surveillance des membres d'une équipe dans le tableau de bord à l'adresse https://www.beyondtrust.com/docs/remote-support/getting-started/rep-console/dashboard.htm.*

Compétences : attribution des problèmes aux techniciens d'assistance

Configuration | **Compétences**

Compétences

Les compétences font partie des domaines de compétence couverts par vos techniciens d'assistance. En tant qu'administrateur, vous devez créer une liste de ces compétences qui sont classées dans de vastes catégories selon leur importance. Ces compétences racines peuvent se voir attribuer un nombre de sous-compétences. Par exemple, la compétence racine pour « Antivirus » peut contenir une liste de logiciels courants d'antivirus qui possèdent chacun une sous-compétence particulière indispensable pour traiter de façon correcte un problème d'assistance technique de l'utilisateur lié à un antivirus.

Les techniciens d'assistance associés à une compétence donnée sont répertoriés à droite. Si aucun technicien d'assistance n'est associé à une compétence, allez dans **Utilisateurs et sécurité > Utilisateurs**, sélectionnez un utilisateur à modifier, puis cliquez sur les **Paramètres de disponibilité** pour configurer les compétences.

> ***Remarque :*** *afin de pouvoir créer et modifier des compétences, cette autorisation doit être définie par utilisateur. Allez dans* ***Utilisateurs et sécurité > Utilisateurs****, faites défiler jusqu'à la section* ***Autorisations*** *et assurez-vous que la permission* ***Autorisé à modifier les compétences*** *est cochée. Les administrateurs se voient accorder automatiquement cette autorisation.*

Pour créer ou modifier des compétences, allez dans **Configuration > Compétences**.

Nouvelle compétence racine

Pour commencer, créez une liste de compétences racines en tant que catégories générales.

Nouvelle compétence

Ajoutez des compétences sous les compétences racines.

Modifier, supprimer

Modifier ou supprimer un élément existant.

Modifier le classement

Si vous avez besoin de changer la place d'une compétence racine, cliquez sur **Modifier le classement**. Vous pourrez alors déplacer les compétences dans le classement.

Compétences

Les compétences racines et leurs sous-catégories s'affichent dans l'arborescence des **Compétences**. Vous pouvez utiliser les flèches orange pour afficher ou masquer chaque section.

Les compétences racines sont classées dans l'ordre de la plus importante à la moins importante. Lorsque le système Equilibrium est activé, il essaie d'abord de faire correspondre toutes les compétences racines, mais si cela n'est pas possible, il commence par les compétences racines les plus basses du classement, une par une, jusqu'à trouver une correspondance.

Nom affiché

Créez un nom unique permettant d'identifier cette compétence.

Nom de code

Définissez également un nom de code, qui sera utilisé à des fins d'intégration. Dans le cas contraire, le système en crée un automatiquement.

> *Pour plus d'informations, veuillez consulter la section Configurer des compétences pour acheminer des problèmes à ces techniciens d'assistance à l'adresse https://www.beyondtrust.com/docs/remote-support/how-to/equilibrium/configure-skills.htm.*

Importer les compétences de l'utilisateur

Une fois créées, les compétences peuvent être attribuées à des techniciens d'assistance depuis la page **Utilisateurs et sécurité > Utilisateurs**.

Lorsque vous gérez un très grand nombre de techniciens d'assistance et/ou de compétences, il peut être plus simple d'assigner les compétences à des techniciens d'assistance grâce à l'importation en masse. Utilisez la fonction **Choisir le fichier** pour charger un fichier CSV avec les noms d'utilisateur et les compétences associées. Le fichier CSV doit utiliser le format suivant :

```
"username1", "skill_code_name"
"username1", "skill_code_name2"
"username2", "skill_code_name"
```

Remarque : les compétences répertoriées pour un technicien d'assistance donné sur le fichier d'importation remplaceront toutes les compétences déjà associées à cet utilisateur. Si vous avez besoin de supprimer toutes les compétences associées à un utilisateur en particulier, laissez le nom de code de la compétence vide ("username3", "").

> *Pour plus d'informations, veuillez consulter la section Configurer des compétences pour acheminer des problèmes à ces techniciens d'assistance à l'adresse https://www.beyondtrust.com/docs/remote-support/how-to/equilibrium/configure-skills.htm.*

> *Pour plus d'informations, veuillez consulter la section Attribuer des compétences à des techniciens d'assistance à l'adresse https://www.beyondtrust.com/docs/remote-support/how-to/equilibrium/assign-skills-rep.htm.*

> *Pour plus d'informations, veuillez consulter la section Algorithme d'acheminement de compétences à l'adresse https://www.beyondtrust.com/docs/remote-support/how-to/equilibrium/skills-routing-algorithms.htm.*

Parrain d'accès : création de groupes d'utilisateurs avec privilèges

Configuration | **Parrain d'accès**

Groupes de parrains d'accès

Créez des groupes de parrains d'accès pour permettre à un technicien ayant des autorisations limitées de 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.

Ajouter un nouveau groupe de parrains d'accès, modifier, supprimer

Créez un nouveau groupe, modifiez un groupe existant ou supprimez un groupe existant.

Ajouter ou modifier les groupes de parrains d'accès

Nom

Créez un nom unique permettant d'identifier ce groupe. Ce nom doit aider les techniciens d'assistance à déterminer le bon groupe de parrains d'accès auquel demander de l'assistance technique.

Description

Ajoutez une brève description pour résumer la fonction de ce groupe.

Membres du groupe

Ajoutez à ce groupe des techniciens d'assistance ayant moins de privilèges comme Demandeurs et des techniciens d'assistance ayant plus de privilèges comme Parrains.

Pour en savoir plus, veuillez consulter Acceptation d'une demande d'accès à des fins d'accroissement des droits à l'adresse https://www.beyondtrust.com/docs/remote-support/getting-started/rep-console/access-requests.htm.

Bouton assistance technique : déployer un Bouton assistance technique pour un démarrage rapide de sessions

Configuration | **Boutons assistance technique**

Assistant de déploiement en masse de plus d'un Bouton assistance technique

Le déploiement d'un Bouton assistance technique sur l'ordinateur du client installe un client d'utilisateur sur sa machine, procurant une méthode rapide et efficace pour démarrer des sessions d'assistance technique. Le Bouton assistance technique ne maintient PAS la connexion au Serveur d'accès à distance sécurisé, mais permet à l'utilisateur d'envoyer une demande d'assistance technique. En fonction de la configuration du Bouton assistance technique et du site d'assistance technique, cliquer sur le Bouton assistance technique peut connecter le client à un technicien ou à une équipe d'assistance technique prédéfinis, lui permettre de saisir une clé de session, ou lui permettre de soumettre un formulaire de soumission de problème. Un Bouton assistance technique peut être installé sur des ordinateurs Windows, Mac et Linux.

Pour plus d'informations, veuillez consulter Gestion de Bouton assistance technique à l'adresse https://www.beyondtrust.com/docs/remote-support/getting-started/rep-console/support-button-management-interface.htm.

Pour plus d'informations, veuillez visiter Bouton assistance technique : Demande d'assistance technique rapide à l'adresse https://www.beyondtrust.com/docs/remote-support/getting-started/customer-client/support-button.htm.

Description

Créez un nom unique permettant d'identifier ce Bouton assistance technique. Ce nom est utile pour la gestion d'un Bouton assistance technique déployé.

Portail public

Sélectionnez le portail public que cet élément devra utiliser pour se connecter à une session d'assistance technique. Si une règle de session est associée à ce portail public, celle-ci peut affecter les autorisations des sessions démarrées avec cet élément.

Langue

Si ce site utilise plus d'une langue, définissez la langue que ce Bouton assistance technique doit utiliser. Un Bouton assistance technique ne détecte pas la langue locale lors de son exécution ; il utilise la langue par défaut attribuée lors du déploiement.

Équipe

Précisez si l'ouverture d'une session à l'aide de ce Bouton assistance technique place l'utilisateur dans votre file d'attente personnelle ou dans la file d'attente d'une équipe.

Un Bouton assistance technique déployé est valide pendant

Définissez la durée de vie du bouton. Le client ne peut utiliser ce bouton pour démarrer des sessions que pendant la durée spécifiée. Si l'utilisateur clique sur ce bouton alors qu'il a expiré, un message de clé de session non valide s'affiche et le navigateur s'actualise en affichant votre portail d'assistance technique. Ce délai n'affecte PAS la durée pendant laquelle l'installeur reste actif ni la durée d'une session.

Mode d'installation

Choisissez d'installer le Bouton assistance technique pour un utilisateur unique ou pour tous les utilisateurs du système distant. Il n'est possible de déployer un Bouton assistance technique pour tous les utilisateurs uniquement sur les plateformes Windows. Notez également qu'en cas de modification du profil d'un Bouton assistance technique, un Bouton assistance technique à utilisateur unique intégrera automatiquement ces changements à sa prochaine connexion, tandis qu'un Bouton assistance technique déployé pour l'ensemble des utilisateurs devra être redéployé pour que les modifications prennent effet. Il est conseillé de redéployer un Bouton assistance technique déployé pour utilisateurs multiples après chaque mise à niveau du logiciel BeyondTrust. Notez qu'il est impossible de supprimer un Bouton assistance technique déployé pour tous les utilisateurs d'un système à partir de la console du technicien d'assistance ; ils doivent être désinstallés directement depuis l'ordinateur cible.

Profil

Sélectionnez un profil à utiliser depuis le menu déroulant.

Créer

Cliquez pour créer le Bouton assistance technique.

Télécharger maintenant

Plate-forme

Choisissez le système d'exploitation sur lequel vous souhaitez installer ce logiciel. Ce menu déroulant sélectionne par défaut l'installeur approprié détecté pour votre système d'exploitation.

Pour les administrateurs système devant déployer l'installeur de Bouton assistance technique sur un nombre conséquent de systèmes, l'option MSI peut être utilisée avec l'outil de gestion de système de votre choix. Dans votre invite de commande, lorsque vous composez la commande pour installer le Bouton assistance technique avec un MSI, modifiez pour indiquer le répertoire de téléchargement du MSI et saisissez la commande figurant à la page **Bouton assistance technique**.

> ***Remarque :*** *notez que, contrairement à la console du technicien d'assistance, un Bouton assistance technique installé à partir d'un MSI se met à jour automatiquement.*

Lors de l'installation d'un exécutable de Bouton assistance technique sur des machines distantes Windows, vous pouvez spécifier l'emplacement où vous souhaitez que le Bouton assistance technique s'installe. Si le dossier d'installation que vous spécifiez n'existe pas, il sera créé, si l'installation dispose des autorisations suffisantes sur le système local. Vous pouvez spécifier le dossier d'installation en utilisant le package d'installation MSI, ou le package d'installation EXE. Cela nécessite BeyondTrust 15.1.3 ou une version supérieure. L'installation des chemins personnalisés n'est pas prise en charge sur les systèmes Mac ou Linux.

La syntaxe pour l'installation EXE est :

```
bomgar-scc-w07dc30w8ff8h51116g785zgh151hdfe8y6z7jgc408c90 --cb-install-dir "C:\Bouton assistance technique"
```

où `bomgar-scc-w07dc30w8ff8h51116g785zgh151hdfe8y6z7jgc408c90` est le nom de fichier de votre client d'installation exécutable et `"C:\Bouton assistance technique"` est le chemin d'installation que vous souhaitez utiliser.

La syntaxe pour l'installation MSI est

```
msiexec /i bomgar-scc-win64.msi KEY_INFO=w0hdc301hd18wxj8xjfd8z6jzyefz7wzd1gwwd6c408c90 INSTALLDIR="C:\Bouton assistance technique"
```

où `bomgar-scc-win64.msi` est le nom de fichier de votre paquet d'installation MSI, `w0hdc301hd18wxj8xjfd8z6jzyefz7wzd1gwwd6c408c90` est la clé de votre paquet d'installation, et `"C:\Bouton assistance technique"` est le chemin d'installation que vous souhaitez utiliser.

Pour installer un Bouton assistance technique sans afficher de fenêtre, d'indicateur de chargement, d'erreur ou autres alertes visibles, ajoutez **--silent** à la fin de la commande de l'EXE ou **/quiet** à la fin de la commande MSI.

Téléchargement

Vous pouvez télécharger l'installeur immédiatement si vous comptez le distribuer en utilisant un outil de gestion de systèmes ou si vous êtes sur l'ordinateur auquel vous aurez besoin d'accéder.

> ***Remarque :*** *étant donné que certains navigateurs exigent que l'installeur soit enregistré avant d'être exécuté, il peut être difficile de savoir si le Bouton assistance technique a bien été installé. Le fichier* ***bomgar-scc-{uid}.exe*** *téléchargé n'est pas le bouton à proprement parler, mais plutôt l'installeur du bouton. Ce fichier doit être exécuté pour terminer l'installation.*

Déployer auprès des destinataires de messagerie

E-mail

Vous pouvez également envoyer par e-mail l'installeur à un ou plusieurs utilisateurs distants. Des destinataires multiples peuvent installer le client à partir du même lien.

Profils de Bouton assistance technique - Ajouter

Créer un nouveau profil, modifier un profil existant, ou supprimer un profil existant. Vous pouvez modifier le profil du Bouton assistance technique par défaut, mais pas le supprimer.

Nom

Créez un nom unique permettant d'identifier ce profil. Ce nom doit aider un technicien d'assistance à décider à quel profil attribuer un Bouton assistance technique.

Icône

Transférez le fichier contenant l'icône de bouton personnalisé. Le fichier doit être au format PNG et ne doit pas dépasser 150 Ko avec une hauteur et une largeur minmales de 128 pixels. La hauteur et la largeur doivent par ailleurs être identiques.

Titre

Le titre est utilisé comme titre de l'icône de bureau.

Titre court

Le titre court sera utilisé si le système d'exploitation de l'utilisateur limite la longueur des titres.

Emplacements de déploiement

Sélectionnez l'emplacement de déploiement du Bouton assistance technique (sur le bureau ou dans le menu). Notez que seuls les systèmes Windows, Mac et Linux permettent le déploiement au sein du menu.

Permettre l'accès direct à la file d'attente

Déterminez si le client peut se servir du Bouton assistance technique pour se connecter directement à une file d'attente spécifiée (la file d'attente est spécifiée par le menu déroulant **Équipe** de l'assistant de déploiement en masse de Bouton assistance technique).

Générateur de fichiers de registre Bouton assistance technique intégré

Utilisez le **Générateur intégré de fichiers de registre de Bouton assistance technique** pour créer des fichiers de registre qui intégreront le Bouton assistance technique dans la barre de titre d'une application. Un Bouton assistance technique intégré permet aux techniciens d'assistance de faciliter le chemin d'accès à l'assistance pour des applications spécifiques. Par exemple, si votre équipe d'assistance technique traite fréquemment des problèmes relatifs à Microsoft Outlook, vous pouvez intégrer un Bouton assistance technique au sein de ce logiciel. Vous pouvez ensuite configurer ce Bouton assistance technique intégré pour qu'il pointe vers un problème spécifique, de sorte que lorsqu'un client l'utilise une session démarre immédiatement avec l'équipe la plus qualifiée pour résoudre les problèmes liés à Outlook. Un Bouton assistance technique intégré n'est disponible que sous Windows.

Pour créer un Bouton assistance technique intégré, un Bouton assistance technique classique doit d'abord être déployé sur le système distant. Si nécessaire, vous pouvez configurer le profil du Bouton assistance technique de sorte à ne créer de raccourci ni sur le bureau ni dans le menu.

Mode d'installation

Choisissez d'installer pour un utilisateur unique ou pour tous les utilisateurs d'un système.

Nom de l'exécutable

Indiquez le nom du logiciel dans lequel vous souhaitez intégrer un Bouton assistance technique. sans spécifier le chemin d'accès au fichier.

Problème

Vous pouvez facultativement choisir un problème qui sera associé aux sessions démarrées au moyen de ce Bouton assistance technique intégré. ou sélectionner l'option **Aucun problème attribué**.

Afficher l'enquête initiale

Cocher l'option **Afficher l'enquête préalable** demande au client de décrire son problème avant de démarrer une session. Si cette option n'est pas cochée, la session démarrera immédiatement, sans autre intervention de l'utilisateur.

Clé externe

Vous pouvez ajouter une clé externe à associer aux sessions démarrées grâce à ce Bouton assistance technique intégré.

Supprimer

Supprimer une application existante de ce fichier de registre.

Ajouter une ligne

Pour ajouter plusieurs applications à un fichier de registre, cliquez sur **Ajouter une nouvelle ligne**, puis renseignez les informations relatives à la nouvelle application.

Importer un fichier de registre

Pour modifier la fonctionnalité d'un Bouton assistance technique intégré, importez le fichier de registre puis modifiez-en les entrées. Une fois terminé, cliquez sur **Créer un fichier de registre**. Exécutez ensuite ce fichier de registre afin d'écraser les anciennes entrées.

Créer un fichier de registre

Après avoir ajouté tous les exécutables auxquels vous souhaitez intégrer un Bouton assistance technique, cliquez sur **Créer un fichier de registre**. Vous serez alors invité à enregistrer un fichier de registre sur votre système. À l'aide d'Active Directory ou d'un outil de déploiement, déployez le fichier de registre sur tous les systèmes distants nécessitant un Bouton assistance technique intégré. Une fois le fichier de registre exécuté, l'utilisateur distant devra se déconnecter puis se reconnecter pour créer l'entrée de registre du Bouton assistance technique.

> ***Remarque :*** *il est conseillé d'enregistrer une copie de tous les fichiers de registre générés. Les informations relatives à ces fichiers ne sont pas enregistrées sur le Serveur d'accès à distance sécurisé.*

À présent, lorsque l'une des applications répertoriées est lancée, un Bouton assistance technique apparaîtra dans l'angle supérieur droit de la fenêtre, à côté du bouton de réduction. Cliquer sur ce Bouton assistance technique intégré entraîne le lancement d'une session, tel que défini par le profil et les paramètres de fichier de registre associés.

> ***Remarque :*** *l'exécution d'un fichier de registre de Bouton assistance technique sur un système comprenant déjà des entrées de registre de Bouton assistance technique écrasera les entrées d'origine. Par conséquent, si vous avez intégré un Bouton assistance technique dans une application et que vous souhaitez l'intégrer à une autre, le nouveau fichier de registre doit contenir le nom des deux exécutables. Si le nouveau fichier de registre ne comprend que le nom du nouvel exécutable, le Bouton assistance technique intégré apparaîtra uniquement dans la nouvelle application.*

Pour supprimer un Bouton assistance technique intégré d'une application sans l'ajouter à une autre, vous devez modifier le registre. Dans le bloc-notes ou dans n'importe quel autre éditeur de texte similaire, ouvrez le fichier de registre initialement déployé, et insérez un tiret devant chaque clé de registre à supprimer. Enregistrez ensuite le fichier de registre et redéployez-le afin de supprimer les entrées marquées. L'exemple suivant présente une entrée de registre marquée pour suppression.

```
[-HKEY_LOCAL_MACHINE\Software\Test]
```

> *Pour plus d'informations sur les entrées de registre, visitez l'adresse https://support.microsoft.com/kb/310516.*

Remarque : *le fait de désinstaller un Bouton assistance technique entraîne sa suppression dans tous les programmes intégrés, mais ne supprime pas les entrées de registre. Par conséquent, si un autre Bouton assistance technique est installé pour le même site, celui-ci hérite des entrées de registre précédentes et apparaîtra dans les mêmes logiciels.*

Pour plus d'informations, veuillez consulter Gestion de Bouton assistance technique à l'adresse https://www.beyondtrust.com/docs/remote-support/getting-started/rep-console/support-button-management-interface.htm.

Champs personnalisés : créer et modifier des champs pour la soumission de problème du portail public

Configuration | **Champs personnalisés**

Champs personnalisés

Vous pouvez configurer jusqu'à 30 champs personnalisés. Les valeurs de champs personnalisées peuvent être créées et configurées pour des sessions d'assistance technique individuelles grâce à la configuration d'envoi de problème du portail public, ainsi qu'avec certaines opérations d'API. Ils sont visibles dans la console du technicien d'assistance BeyondTrust.

Créer un nouveau champ, modifier, supprimer

Créer, modifier ou supprimer un champ personnalisé. Les champs personnalisés supprimés ne s'affichent plus dans la console du technicien d'assistance ou les rapports de session.

Ajouter ou modifier un champ personnalisé

Nom affiché

Créez un nom unique permettant d'identifier ce champ.

Nom de code

Définissez également un nom de code, qui sera utilisé à des fins d'intégration. Dans le cas contraire, le système en crée un automatiquement.

Afficher dans la console du technicien d'assistance

Cochez cette case si vous voulez que ce champ s'affiche dans la console du technicien d'assistance.

> ***Remarque :*** *pour choisir les problèmes à afficher dans le portail public, ainsi que leur ordre d'affichage, allez dans* ***Portails publics > Utiliser l'enquête de soumission de problème****. Ajoutez ou modifiez un site public, puis choisissez* ***Utiliser l'enquête de soumission de problème****. Choisissez les champs disponibles à afficher.*

Jump

Jump Clients : gestion des paramètres et installation de Jump Clients pour un accès autonome

Assistant de déploiement en masse de Jump Clients

L'assistant de déploiement en masse permet aux administrateurs et aux utilisateurs privilégiés de déployer des Jump Clients sur un ou plusieurs ordinateurs distants pour pouvoir y accéder ultérieurement en mode autonome.

> *Pour plus d'informations, veuillez consulter Guide Jump Client Remote Support : Accès sans surveillance aux systèmes de n'importe quel réseau à l'adresse https://www.beyondtrust.com/docs/remote-support/how-to/jump-clients/index.htm.*

Groupe de Jump

Dans le menu déroulant, indiquez si vous souhaitez attacher le Jump Client à votre liste personnelle d'éléments de Jump ou à un groupe de Jump partagé avec d'autres utilisateurs. Si vous l'attachez à votre liste personnelle d'éléments de Jump, vous serez le seul à pouvoir accéder à cet ordinateur distant par le biais de ce Jump Client. Si vous l'attachez au groupe de Jump partagé, ce Jump Client deviendra accessible à tous les membres de ce groupe de Jump.

Autoriser le remplacement lors de l'installation

Certains paramètres de l'assistant de déploiement en masse autorisent le remplacement, et vous permettent donc d'utiliser la ligne de commande pour définir des paramètres spécifiques au déploiement, avant l'installation.

L'installeur est valide pour

Le programme d'installation n'est valable que pendant la durée indiquée dans le menu déroulant **L'installeur est valide pour**. N'oubliez pas de laisser suffisamment de temps pour l'installation. En cas de tentative d'exécution de l'installeur de Jump Client une fois ce délai écoulé, l'installation échoue et un nouvel installeur de Jump Client doit être créé. De plus, si l'installateur est exécuté dans le temps imparti mais que le Jump Client n'est pas en mesure de se connecter au serveur durant cet intervalle, le Jump Client se désinstalle, et un nouvel installeur doit être lancé. Le délai de validité peut être défini sur un laps de temps allant de 10 minutes à 1 an. Ce délai n'affecte pas la durée pendant laquelle le Jump Client demeure actif.

En plus d'expirer après la période donnée par l'option **L'installeur est valide pour**, les packages de déploiement en masse de Jump Client deviennent non valides lorsque leur Serveur d'accès à distance sécurisé est mis à niveau. La seule exception à cette règle est les mises à jour directes qui modifient le nombre de licences ou leur date d'expiration. Toute autre mise à jour, même si elle ne change pas le numéro de version du serveur, rend non valides les installeurs de Jump Client d'avant la mise à niveau. Si ces installeurs sont des packages MSI, ils peuvent toujours être utilisés pour désinstaller les Jump Clients si nécessaire.

Une fois qu'un Jump Client a été installé, il reste en ligne et actif jusqu'à ce qu'il soit désinstallé du système local par un utilisateur connecté, par un technicien d'assistance depuis l'interface de Jump de la console du technicien d'assistance, ou par un script de

désinstallation. Un technicien d'assistance ne peut supprimer un Jump Client que s'il a reçu les autorisations nécessaires de son admin dans l'interface /login.

Portail public

Sélectionnez le portail public que cet élément devra utiliser pour se connecter à une session d'assistance technique. Si une règle de session est associée à ce portail public, celle-ci peut affecter les autorisations des sessions démarrées avec cet élément.

Nom

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.

Commentaires

Ajoutez des **commentaires** qui peuvent s'avérer utiles pour rechercher et identifier des ordinateurs distants. Il est à noter que les Jump Clients déployés avec cet installeur affichent les mêmes commentaires définis au préalable, sauf si vous cochez **Autoriser le remplacement pendant l'installation** et que vous utilisez les paramètres disponibles pour modifier l'installeur pour des installations individuelles.

Balise

L'ajout d'une **balise** permet d'organiser vos Jump Clients en catégories à l'intérieur de la console du technicien d'assistance.

Règle de Jump

Vous pouvez appliquer une **règle de Jump** à ce Jump Client. Les règles de Jump sont configurées sur la page **Jump > Règles de Jump** et déterminent les périodes pendant lesquelles un utilisateur peut accéder à ce Jump Client. En l'absence de toute règle de Jump, le Jump Client est accessible en continu.

Règle de session utilisateur présent et Règle de session utilisateur absent

Sélectionnez les règles de session à appliquer à ce Jump Client. Les règles de session affectées à ce Jump Client 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 de l'utilisateur est déterminée par le biais du paramètre de Jump Client **Utiliser l'état de l'écran pour détecter la présence de l'utilisateur**. La présence de l'utilisateur est détectée au démarrage de la session de Jump Client. 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.

Type de connexion

Définissez le **type de connexion** sur **Active** ou **Passive** pour les Jump Clients déployés.

Proxy de Jumpoint

Si vous avez un ou plusieurs Jumpoints définis comme proxy, vous pouvez sélectionner un Jumpoint comme proxy pour ces connexions de Jump Client. Ainsi, lorsque ces Jump Clients sont installés sur des ordinateurs sans connexion Internet native, ils peuvent utiliser le Jumpoint pour se connecter au Serveur d'accès à distance sécurisé. Les Jump Clients doivent être installés sur le même réseau que le Jumpoint sélectionné comme proxy pour les connexions.

Tenter une installation avec des droits accrus si le client offre cette possibilité

Si l'option **Tenter une installation avec des droits accrus si le client offre cette possibilité** est sélectionnée, le programme d'installation tente de s'exécuter avec les droits d'administration, en installant le Jump Client en tant que service système. Si la tentative d'installation avec des droits accrus échoue ou si cette option est désélectionnée, le programme d'installation s'exécute avec des droits utilisateur, en installant le Jump Client en tant qu'application. Notez que cette option n'est valable que pour les systèmes d'exploitation Windows et Mac.

> ***Remarque :*** *un Jump Client attaché en mode utilisateur n'est disponible que lorsque cet utilisateur est connecté. À l'inverse, un Jump Client attaché en mode service, avec des droits accrus, permet un accès permanent au système, indépendamment de l'utilisateur connecté.*

Demander des informations d'authentification d'accroissement de droits si nécessaire

Si l'option **Demander des informations d'authentification d'accroissement de droits si nécessaire** est sélectionnée, le programme d'installation invite l'utilisateur à indiquer les informations d'authentification d'un compte d'administration si le système exige que ces informations d'authentification soient fournies de manière indépendante ; dans le cas contraire, le Jump Client est installé avec des droits d'utilisateur. Notez que cette option ne concerne que les installations avec droits accrus.

Minimise le Client d'utilisateur au démarrage de la session

En choisissant l'option **Minimise le Client d'utilisateur au démarrage de la session**, le client d'utilisateur ne passe pas au premier plan et reste réduit dans la barre des tâches ou le dock lorsqu'une session est lancée par l'un de ces Jump Clients.

Mot de passe/Confirmer le mot de passe

Vous pouvez également définir un **mot de passe** pour ces Jump Clients. Dans ce cas, la saisie du mot de passe est obligatoire pour pouvoir modifier ou utiliser l'un des Jump Clients.

Aide pour le déploiement en masse

Pour les administrateurs système devant déployer le programme d'installation de Jump Client sur un grand nombre de systèmes, l'exécutable Windows, Mac ou Linux, ou le MSI Windows peut être utilisé avec l'outil de gestion de système de votre choix. Vous pouvez inclure un chemin d'accès personnalisé valide pour le répertoire d'installation du Jump Client.

Vous pouvez également remplacer certains paramètres d'installation en fonction de vos besoins spécifiques. Ces paramètres peuvent être spécifiés pour le MSI et l'EXE en utilisant un outil d'administration système ou l'interface en ligne de commande. Lors de la configuration du remplacement de certaines options d'installation spécifiques pendant l'installation, vous pouvez utiliser les paramètres facultatifs suivants pour modifier l'installeur de Jump Client pour différentes installations. Notez que si un paramètre est passé en ligne de commande mais qu'il n'est pas marqué pour remplacement dans l'interface d'administration /login, l'installation échoue. Dans ce cas, consultez le journal des événements du système d'exploitation à la recherche des erreurs d'installation.

> ***Remarque :*** *il est courant de recevoir un message d'erreur lors de l'installation, concernant un problème de mise en page ou d'apparence. Cela peut être ignoré.*

Paramètre de ligne de commande	Valeur	Description
--install-dir	<directory_path>	Spécifie un nouveau répertoire accessible en écriture dans lequel

		installer le Jump Client. Ce paramètre est pris en charge sur les systèmes Windows et Linux uniquement. En cas de définition d'un répertoire d'installation personnalisé, assurez-vous que ce répertoire n'existe pas déjà et que l'emplacement spécifié est disponible en écriture.
--jc-name	<name...>	Si le remplacement est autorisé, ce paramètre de ligne de commande définit le nom du Jump Client.
--jc-jump-group	utilisateur :<username> jumpgroup:<jumpgroup-code-name>	Si le remplacement est autorisé, ce paramètre de ligne de commande prévaut sur le groupe de Jump défini dans l'assistant de déploiement en masse.
--jc-public-site-address	<public-site-address-hostname>	Si le remplacement est autorisé, ce paramètre de ligne de commande associe le Jump Client au portail public présentant le nom d'hôte spécifié en tant qu'adresse de site. Si aucun portail public ne comporte le nom d'hôte comme adresse de site, le Jump Client utilise le site public par défaut.
--jc-session-policy-present	<session-policy-code-name>	Si le remplacement est autorisé, ce paramètre de ligne de commande définit la règle de session du Jump Client contrôlant la règle d'autorisation au cours d'une session d'assistance technique lorsque l'utilisateur est présent.
--jc-session-policy-not-present	<session-policy-code-name>	Si le remplacement est autorisé, ce paramètre de ligne de commande définit la règle de session du Jump Client contrôlant la règle d'autorisation au cours d'une session d'assistance technique lorsque l'utilisateur est absent.
--jc-jump-policy	<jump-policy-code-name>	Si le remplacement est autorisé, ce paramètre de ligne de commande définit la règle de Jump contrôlant l'accès au Jump Client.
--jc-tag	<tag-name>	Si le remplacement est autorisé, ce paramètre de ligne de commande définit lla balise du Jump Client.
--jc-comments	<comments ... >	Si le remplacement est autorisé, ce paramètre de ligne de commande définit les commentaires du Jump Client.
--silent		Avec cette commande, l'installeur n'affiche ni fenêtre, ni indicateur de chargement, ni erreur, ni aucune autre alerte visible.

Remarque :
lors du déploiement d'un installeur MSI sous Windows à l'aide de la commande msiexec, les paramètres ci-avant peuvent être spécifiés comme suit :

1. *Suppression des tirets de début (--)*
2. *Conversion des tirets restants en tirets bas (_)*
3. *Attribution d'une valeur à l'aide du signe égal (=)*

Exemple MSI :

```
msiexec /i bomgar-scc-win32.msi KEY_INFO=w0dc3056g7ff8d1j68ee6wi6dhwzfefggyezh7c40jc90
jc_jump_group=jumpgroup:server_support jc_tag=servers
```

Lors du déploiement d'un installeur EXE, les paramètres ci-dessus peuvent être spécifiés comme suit :

- *Ajout de tirets*
- *Ajouter un espace entre le paramètre et la valeur au lieu d'un signe égal*

Exemple EXE :

```
bomgar-scc-[unique id].exe --jc-jump-group jumpgroup:servers --jc-tag servers
```

Autres règles à prendre en compte :

- ***installdir** possède un tiret dans la version EXE, mais aucun dans la version MSI.*
- ***/quiet** est utilisé dans la version MSI à la place de **--silent** dans la version EXE.*

Pour plus d'informations, veuillez consulter la section Déploiement en masse du logiciel BeyondTrust sur Mac à l'adresse https://www.beyondtrust.com/docs/remote-support/how-to/mass-deploy-mac/index.htm.

Télécharger ou installer le client maintenant

Plate-forme

Choisissez le système d'exploitation sur lequel vous souhaitez installer ce logiciel. Ce menu déroulant sélectionne par défaut l'installeur approprié détecté pour votre système d'exploitation.

***Remarque :** contrairement à la console du technicien d'assistance, les Jump Clients installés à partir d'un MSI se mettent à jour automatiquement.*

***Remarque :** pour installer un Jump Client en mode service sur un système Linux, l'installeur de Jump Client doit être exécuté en racine, mais le service Jump Client ne doit pas être exécuté dans le contexte d'utilisateur racine. Un Jump Client en mode service permet à l'utilisateur de démarrer une session même si aucun utilisateur distant n'est connecté, et de déconnecter l'utilisateur distant actuel et de se connecter avec des informations d'authentification différentes. Un Jump Client Linux installé en mode utilisateur ne peut pas être accru lors d'une session.*

Utilisez la syntaxe suivante pour ajouter des autorisations d'exécutable au fichier, où {uid} est un identificateur unique composé de lettres et de chiffres :

1. Ajoutez des autorisations d'exécutable au fichier :

```
sudo chmod +x ./Downloads/bomgar-scc-[uid].desktop
```

2. Exécutez l'installeur en tant qu'utilisateur racine en utilisant la commande **sudo** :

```
sudo sh ./Downloads/bomgar-scc-[uid].desktop
```

Télécharger/Installer

Vous pouvez télécharger l'installeur immédiatement si vous comptez le distribuer en utilisant un outil de gestion de systèmes ou si vous êtes sur l'ordinateur auquel vous aurez besoin d'accéder.

> ***Remarque :*** *après l'exécution de l'installeur, le Jump Client tente de se connecter au serveur. Lorsqu'il y parvient, le Jump Client apparaît dans l'interface de Jump de la console du technicien d'assistance. Si le Jump Client n'est pas en mesure d'accéder au serveur, il tentera de se connecter jusqu'à ce qu'il y parvienne. S'il ne parvient pas à se connecter dans le temps défini par* ***L'installeur est valide pour****, le Jump Client se désinstalle du système distant et doit être relancé.*

Déployer auprès des destinataires de messagerie

E-mail

Vous pouvez également envoyer par e-mail l'installeur à un ou plusieurs utilisateurs distants. Des destinataires multiples peuvent installer le client à partir du même lien.

> *Pour en savoir plus sur l'assistant de déploiement en masse, consultez Déployer des Jump Clients lors d'une session d'assistance technique ou avant l'assistance technique à l'adresse https://www.beyondtrust.com/docs/remote-support/how-to/jump-clients/deploying.htm.*

Statistiques des Jump Clients

Un administrateur peut choisir les statistiques à afficher pour tous les Jump Clients à l'échelle du site. Ces statistiques sont affichées dans la console du technicien d'assistance ; elles comprennent le processeur, l'utilisateur de la console, le taux d'utilisation du disque, une miniature de l'écran distant et le temps de disponibilité.

Intervalle de mise à jour des statistiques de Jump Client actif

L'**intervalle de mise à jour des statistiques du Jump Client** détermine à quelle fréquence ces statistiques sont mises à jour. Le fait de définir les statistiques affichées et leur fréquence d'affichage permet souvent de réguler la quantité de bande passante utilisée. Plus vous déployez de Jump Clients actifs, moins les statistiques sont nombreuses et plus l'intervalle risque d'être long.

Mise à niveau

Bande passante maximale pour les mises à niveau simultanées de Jump Client

Vous pouvez encore réguler la bande passante utilisée lors des mises à jour à l'aide du paramètre **Bande passante maximale pour les mises à niveau de Jump Client simultanées**. La bande passante de mise à niveau maximale est de 100 Mio/s.

> ***Remarque :*** *ce paramètre n'affecte pas les mises à niveau de la console du technicien d'assistance ou les déploiements d'un Bouton assistance technique.*

Nombre maximum de mises à niveau de Jump Client simultanées

De même, définissez le nombre maximum de Jump Clients à mettre à jour en même temps. Notez que si vous avez déployé un grand nombre de Jump Clients, il se peut que vous deviez en limiter le nombre pour réguler la quantité de bande passante consommée. Le nombre maximum autorisé est de 500.

> ***Remarque :*** *ce paramètre n'affecte pas les mises à niveau de la console du technicien d'assistance ou les déploiements d'un Bouton assistance technique.*

Taux de connexions global pour les Jump Clients

Le paramètre **Taux de connexions global pour les Jump Clients** détermine le taux maximum de Jump Clients par seconde autorisés à se connecter au serveur en même temps qu'une mise à niveau ou après une importante perte de réseau. La valeur par défaut est de 50 connexions, et le maximum autorisé est de 300.

Maintenance

Nombre de jours avant que les Jump Clients non connectés soient effacés automatiquement

Si un Jump Client est déconnecté et ne se reconnecte pas au Serveur d'accès à distance sécurisé pendant le nombre de jours spécifié par le paramètre **Nombre de jours avant que les Jump Clients non connectés soient effacés automatiquement**, il sera automatiquement désinstallé de l'ordinateur cible et supprimé de l'interface de Jump dans la console du technicien d'assistance.

> ***Remarque :*** *ce paramètre est partagé avec le Jump Client en temps normal. Ainsi, même s'il ne parvient pas à communiquer avec le site, il se désinstalle au moment configuré. Si ce paramètre est modifié après qu'un Jump Client se soit déconnecté du serveur, il se désinstallera au moment configuré précédemment.*

> ***Remarque :*** *le réglage doit être configuré pour quinze jours ou plus.*

Nombre de jours avant que les Jump Clients non connectés soient considérés comme perdus

Si un Jump Client est déconnecté et ne se reconnecte pas au Serveur d'accès à distance sécurisé pendant le nombre de jours spécifié par le paramètre **Nombre de jours avant que les Jump Clients non connectés soient considérés comme perdus**, il sera identifié comme perdu dans la console du technicien d'assistance. Aucune action spécifique n'est effectuée sur le Jump Client à ce moment. 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.

Remarque : *pour vous permettre d'identifier les Jump Clients perdus avant qu'ils soient automatiquement supprimés, ce champ doit contenir un chiffre inférieur au champ de suppression ci-dessus.*

Remarque : *le réglage doit être configuré pour quinze jours ou plus.*

Astuce: *les Jumps simultanés peuvent être autorisés ou refusés en configurant un Jump Client dans la section* ***Jump > Éléments de Jump > Paramètres de Jump****. Lorsqu'ils sont autorisés, plusieurs utilisateurs peuvent accéder au même Jump Client sans avoir à être invités à rejoindre une session par un autre utilisateur. Dans le cas contraire, un seul utilisateur à la fois est en mesure d'utiliser un Jump vers un Jump Client. S'il souhaite accéder à la session, un second utilisateur doit obtenir une invitation de la part de l'utilisateur ayant ouvert la session.*

Pour plus d'informations, consultez la section Configurer les paramètres du Jump Client à l'adresse https://www.beyondtrust.com/docs/remote-support/how-to/jump-clients/settings.htm.

Comportement du Jump Client désinstallé

L'option **Comportement du Jump Client désinstallé** définit comment un Jump Client supprimé par un utilisateur final est géré par la console du technicien d'assistance. Selon l'option sélectionnée dans le menu déroulant, l'élément supprimé peut être signalé comme désinstallé et conservé dans la liste, ou retiré de la liste d'éléments de Jump dans la console du technicien d'assistance. Si le Jump Client n'est pas en mesure de contacter le Serveur d'accès à distance sécurisé lors de l'installation, l'élément affecté se maintient hors ligne.

Restreindre la désinstallation/désactivation locale des Jump Clients

Limiter la désinstallation/désactivation locales des Jump Clients limite la capacité de l'utilisateur distant à désinstaller ou désactiver des Jump Clients depuis le menu contextuel, diminuant la nécessité de réinstaller des Jump Clients qui n'auraient pas dû être désinstallés. Lorsque cette option est activée, seuls les utilisateurs disposant de privilèges appropriés sur la machine cible sont autorisés à désinstaller le Jump Client via le menu de suppression de programmes du système hôte.

Divers

Type de connexion par défaut pour Jump Client

Avec **Type de connexion par défaut pour Jump Client**, définissez si les Jump Clients attachés pendant une session lancée par un client doivent être actifs ou passifs par défaut.

Port de Jump Client passif

L'option **Port de Jump Client passif** indique le port qu'un Jump Client passif doit utiliser pour écouter une commande de « réveil » émise par le serveur. Le port par défaut est 5832. Vérifiez que la configuration du pare-feu autorise le trafic entrant sur ce port pour les hôtes présentant des Jump Clients passifs. Une fois activés, les Jump Clients se connectent toujours au serveur via le port 80 ou la sortie 443.

Autoriser les techniciens d'assistance à tenter de réveiller les Jump Clients

Autoriser les techniciens d'assistance à tenter de réveiller les Jump Clients permet de réveiller un Jump Client spécifique en transmettant des paquets WOL (Wake-on-LAN) par le biais d'un autre Jump Client du même réseau. Après chaque tentative, cette option devient indisponible pendant 30 secondes. Notez que la technologie WOL doit être activée sur l'ordinateur cible et le réseau associé pour que cela fonctionne. Les informations de passerelle par défaut du Jump Client sont utilisées pour déterminer si d'autres Jump Clients résident sur le même réseau. Lors de l'envoi d'un paquet WOL, l'utilisateur dispose d'une option avancée pour fournir un mot de passe pour les environnements WOL nécessitant un mot de passe WOL sécurisé.

Utiliser l'état de l'écran pour détecter la présence de l'utilisateur

Utiliser l'état de l'écran pour détecter la présence de l'utilisateur permet de définir la façon dont la présence de l'utilisateur est déterminée. La présence de l'utilisateur est utilisée pour choisir entre les règles de session Utilisateur présent et Utilisateur absent. Lorsque cette option est activée, l'utilisateur est considéré comme étant présent uniquement s'il est connecté, que l'écran n'est pas verrouillé et que l'économiseur d'écran n'est pas en fonction. Sinon, l'utilisateur est considéré comme étant présent dès lors qu'il est connecté, quel que soit l'état de l'écran.

Groupes de Jump : définir les éléments de Jump accessibles aux techniciens d'assistance

Groupes de Jump

Un groupe de Jump est une façon d'organiser les éléments de Jump : on attribue à certains membres un certain niveau d'accès à ces éléments. Les utilisateurs sont associés à des groupes de Jump depuis cette page ou depuis la page **Utilisateurs et sécurité > Règles de groupe**.

Ajouter un nouveau groupe de Jump, modifier, supprimer

Créez un nouveau groupe, modifiez un groupe existant ou supprimez un groupe existant.

Groupe de Jump - Ajouter ou modifier

Nom

Créez un nom unique permettant d'identifier ce groupe. Ce nom est utile lorsqu'on ajoute des éléments de Jump à un groupe ou lorsqu'on souhaite savoir quels utilisateurs et quelles règles de groupe font partie d'un groupe de Jump.

Nom de code

Définissez également un nom de code, qui sera utilisé à des fins d'intégration. Dans le cas contraire, le système en crée un automatiquement.

Commentaires

Ajoutez une brève description pour résumer la fonction de ce groupe de Jump.

Règles de groupe

Cette option affiche une liste de règles de groupe qui associent des utilisateurs à ce groupe de Jump.

Utilisateurs autorisés

Lancez une recherche pour ajouter des utilisateurs à ce groupe de Jump. Il est possible de paramétrer le **Nouveau rôle de membre** de chaque utilisateur pour définir son type d'autorisation vis-à-vis des éléments de Jump dans ce groupe de Jump. Vous pouvez aussi utiliser les rôles d'élément de Jump par défaut de l'utilisateur défini sur la page **Utilisateurs et sécurité > Règles de groupe** ou sur la page **Utilisateurs et sécurité > Utilisateurs**. Le rôle d'élément de Jump est un ensemble prédéfini d'autorisations relatives à la gestion et à l'utilisation d'un élément de Jump.

Les utilisateurs de groupes de Jump existants figurent dans un tableau, avec leur rôle assigné et des informations qui accordent ce rôle. Vous pouvez filtrer la vue en saisissant une chaîne dans la zone de texte **Filtrer par nom**. Vous pouvez aussi modifier les paramètres d'un utilisateur ou supprimer l'utilisateur du groupe de Jump.

Pour ajouter des groupes d'utilisateurs à un groupe de Jump, consultez **Utilisateurs et sécurité > Règles de groupe** et associez ce groupe à un ou à plusieurs groupes de Jump.

Remarque : *il est possible que les options* ***Modifier*** *et* ***Supprimer*** *de certains utilisateurs aient été désactivées. Cela arrive lorsqu'on ajoute un utilisateur par le biais d'une règle de groupe ou lorsque le rôle d'élément de Jump du système d'un utilisateur n'est pas défini sur* ***Aucun accès****. Cliquez sur le lien de la règle de groupe pour modifier la règle de façon globale. Les changements apportés à une règle de groupe s'appliquent également à l'ensemble des membres de ce groupe. Cliquez sur le lien de l'utilisateur pour modifier le rôle d'élément de Jump du système de l'utilisateur. Les changements apportés à un rôle d'élément de Jump du système de l'utilisateur s'appliquent également à l'ensemble des autres groupes de Jump dans lesquels cet utilisateur n'a pas été associé en tant que membre. Vous pouvez aussi ajouter un utilisateur au groupe, en ignorant paramètres tels qu'il sont définis ailleurs.*

Pour plus d'informations, veuillez consulter la section Utiliser des groupes de Jump pour définir les éléments de Jump accessibles aux utilisateurs à l'adresse https://www.beyondtrust.com/docs/remote-support/how-to/jumpoint/jump-groups.htm.

Règles de Jump : définir les plannings pour les Jump Clients

Jump | Règles de Jump

Règles de Jump

Les règles de Jump sont utilisées pour contrôler à quels moments certains éléments de Jump sont accessibles en mettant en place des calendriers.

> *Pour plus d'informations sur la création et l'utilisation de règles de Jump, veuillez consulter la section Créer des règles de Jump à appliquer aux éléments de Jump à l'adresse https://www.beyondtrust.com/docs/remote-support/how-to/jumpoint/policies.htm.*

Ajouter, modifier, supprimer

Créer une nouvelle règle, modifier ou supprimer une règle existante.

Ajouter ou modifier une règle

Nom affiché

Créez un nom unique permettant d'identifier cette règle. Ce nom doit aider les utilisateurs à identifier cette règle lors de son assignation à des Jump Clients.

Nom de code

Définissez également un nom de code, qui sera utilisé à des fins d'intégration. Dans le cas contraire, le système en crée un automatiquement.

Description

Ajoutez une brève description pour résumer la fonction de cette règle.

Planning de Jump : Activé

Définissez un planning pour déterminer à quel moment l'accès aux éléments de Jump est autorisé selon cette règle. Définissez le fuseau horaire à utiliser pour ce planning, puis ajoutez une ou plusieurs entrées de planification. Pour chaque entrée, indiquez l'heure et la date de début ainsi que l'heure et la date de fin.

Ainsi, si la période commence à 8 h et se termine à 17 h, un utilisateur peut lancer une session à l'aide de cet élément de Jump durant cet intervalle, et il pourra également continuer à travailler après l'heure de fin. Si un utilisateur tente d'accéder à cet élément de Jump après 17 heures, il recevra une notification l'informant que le planning n'autorise pas le démarrage d'une session. Si nécessaire, l'utilisateur peut choisir d'outrepasser la restriction du planning et lancer la session malgré tout.

Forcer l'arrêt de la session lorsque le planning ne permet pas l'accès

Si un contrôle d'accès plus strict est requis, cochez **Forcer l'arrêt de la session lorsque le planning ne permet pas l'accès**. Ceci force la déconnexion de la session à l'heure de fin définie. Dans ce cas, l'utilisateur reçoit des notifications récurrentes à partir de 15 minutes avant d'être déconnecté.

Rôles d'élément de Jump : configurer les groupes d'autorisation pour les éléments de Jump

Rôles d'élément de Jump

Le rôle d'élément de Jump est un ensemble prédéfini d'autorisations relatives à la gestion et à l'utilisation d'un élément de Jump. Les rôles d'élément de Jump sont attribués aux utilisateurs depuis la page **Jump > Rôles d'élément de Jump** ou depuis la page **Utilisateurs et sécurité > Règles de groupe**.

Si plusieurs rôles sont attribués à un utilisateur, le rôle le plus spécifique est toujours utilisé. Voici l'ordre de spécificité des rôles d'élément de Jump (du plus spécifique au moins spécifique) :

- Le rôle attribué à la relation entre un utilisateur et un groupe de Jump sur la page **Jump > Rôles d'élément de Jump**.
- Le rôle attribué à la relation entre un utilisateur et un groupe de Jump sur la page **Utilisateurs et sécurité > Règles de groupe**.
- Les **Rôles d'élément de Jump** attribués à un utilisateur depuis la page **Utilisateurs et sécurité > Utilisateurs** ou la page **Utilisateurs et sécurité > Règles de groupe**.

Ajouter un nouveau rôle d'élément de Jump, modifier, supprimer

Créez un nouveau rôle, modifiez un rôle existant ou supprimez un rôle existant.

Ajouter ou modifier un rôle d'élément de Jump

Nom

Créez un nom unique permettant d'identifier ce rôle. Ce nom est utile lorsqu'on associe un rôle d'élément de Jump à un utilisateur ou à un groupe d'utilisateurs dans un groupe de Jump.

Description

Ajoutez une brève description pour résumer la fonction de ce rôle.

Autorisations

Groupe de Jump ou éléments de Jump personnels

Créer et déployer de nouveaux éléments de Jump

Permet à l'utilisateur de créer des éléments de Jump et de les installer sur des systèmes distants.

Déplacer et copier des éléments de Jump

Permet à l'utilisateur de déplacer ou de copier des éléments de Jump d'un groupe de Jump à un autre groupe de Jump. Cette autorisation doit être activée sur les deux groupes de Jump. Les éléments de Jump copiés peuvent être modifiés.

Supprimer des éléments de Jump existants

Permet à l'utilisateur de supprimer des éléments de Jump.

Élément de Jump

Démarrer les sessions

Permet à l'utilisateur d'effectuer un Jump vers des ordinateurs distants.

Modifier une balise

Permet à l'utilisateur de modifier un champ de balise d'élément de Jump.

Modifier des commentaires

Permet à l'utilisateur de modifier un champ de commentaires d'élément de Jump.

Modifier le portail public

Permet à l'utilisateur de définir le portail public auquel un élément de Jump est associé.

Modifier une règle de Jump

Permet à l'utilisateur de définir, le cas échéant, la règle de Jump à associer à un élément de Jump.

Modifier une règle de session

Permet à l'utilisateur de définir, le cas échéant, la règle de session à associer à un élément de Jump. Toute modification de la règle de session peut affecter les autorisations associées à la session.

Modifier la connectivité et l'authentification

Permet à l'utilisateur de modifier la connexion et les informations d'authentification associées à un élément de Jump, notamment les champs comme le nom d'hôte, le Jumpoint, le port et le nom d'utilisateur, entre autres.

Modifier le comportement et l'expérience

Permet à l'utilisateur de modifier le comportement des éléments de Jump, notamment les champs comme le type de connexion, la taille de l'affichage et le type de terminal, entre autres.

Jump Clients uniquement

Définir les mots de passe

Permet à l'utilisateur de protéger les Jump Clients par un mot de passe.

Contourner les mots de passe

Permet à l'utilisateur d'accéder à des Jump Clients protégés par un mot de passe sans en connaître le mot de passe.

> *Pour plus d'informations, veuillez consulter la section Utiliser les rôles d'éléments de Jump pour créer les groupes d'autorisation des éléments de Jump à l'adresse https://www.beyondtrust.com/docs/remote-support/how-to/jumpoint/jump-item-roles.htm.*

Jumpoint : configuration d'un accès autonome à un réseau

Jump | **Jumpoint**

Gestion de Jumpoint

La technologie Jump de BeyondTrust permet à un utilisateur d'accéder à des ordinateurs sur un réseau distant sans avoir à préinstaller un logiciel sur chaque machine. Il suffit d'installer un agent Jumpoint unique à n'importe quel endroit du réseau pour pouvoir accéder à chaque ordinateur de ce réseau en mode autonome.

Ajouter un nouveau Jumpoint, modifier, supprimer

Créer un nouveau Jumpoint, modifier ou supprimer un Jumpoint existant.

Redéployer

Désinstaller un Jumpoint existant et télécharger un installeur pour remplacer le Jumpoint existant par un nouveau. Les raccourcis de Jump associés au Jumpoint existant utiliseront le nouveau Jumpoint une fois qu'il est installé.

> ***Remarque :*** *lorsqu'un Jumpoint existant est remplacé, sa configuration n'est pas sauvegardée. Le nouveau Jumpoint doit être reconfiguré.*

Activer la navigation réseau

L'option permettant d'**autoriser la navigation réseau** se trouve au bas de la page **Jumpoint**. Si l'option est cochée, un utilisateur autorisé peut consulter et sélectionner des systèmes dans l'arborescence des répertoires réseau. Si l'option est décochée, l'utilisateur ne peut accéder à un système via un Jumpoint qu'en indiquant le nom d'hôte ou l'adresse IP du système. Dans tous les cas, l'utilisateur doit fournir des informations d'authentification valides au système distant avant d'obtenir l'accès.

Ajouter ou modifier des Jumpoints

Nom

Créez un nom unique permettant d'identifier ce Jumpoint. Ce nom doit aider les utilisateurs à trouver ce Jumpoint lorsqu'ils ont besoin de démarrer une session avec un ordinateur sur le même réseau.

Nom de code

Définissez également un nom de code, qui sera utilisé à des fins d'intégration. Dans le cas contraire, le système en crée un automatiquement.

Commentaires

Ajoutez des commentaires pour identifier la fonction de ce Jumpoint.

Désactivé(e)

Si cette option est cochée, ce Jumpoint n'est pas disponible pour établir des connexions de Jump.

En cluster

Si cela est coché, vous pourrez ajouter plusieurs nœuds redondants du même Jumpoint sur différents systèmes hôtes. Ceci garantit que le Jumpoint sera toujours disponible tant qu'au moins un nœud est en ligne.

Activer la méthode de Shell Jump

Si vous souhaitez que les utilisateurs puissent se connecter à des appareils réseau SSH et Telnet à travers ce Jumpoint, cochez la case **Activer la méthode de Shell Jump**.

Règles de groupe

Cette option affiche une liste de règles de groupe permettant aux utilisateurs d'accéder à ce Jumpoint.

Utilisateurs autorisés

Nouveau nom de membre

Lancez une recherche pour ajouter des utilisateurs à ce Jumpoint. Selon leur niveau d'autorisation, les utilisateurs peuvent utiliser ce Jumpoint pour lancer une session et/ou créer des éléments de Jump se connectant via ce Jumpoint.

Le tableau du bas affiche les utilisateurs des Jumpoints existants. Vous pouvez filtrer la vue en saisissant une chaîne dans la zone de texte **Filtrer par nom**. Vous pouvez aussi supprimer l'utilisateur du Jumpoint.

Pour ajouter un groupe d'utilisateurs à un Jumpoint, consultez **Utilisateurs et sécurité > Règles de groupe** et associez ce groupe à un ou à plusieurs Jumpoints.

> ***Remarque :***
> *il est possible que l'option **Supprimer** de certains utilisateurs ait été désactivée. Cela arrive lorsqu'on ajoute un utilisateur par le biais d'une règle de groupe.*
>
> *Cliquez sur le lien de la règle de groupe pour modifier la règle de façon globale. Les changements apportés à une règle de groupe s'appliquent à l'ensemble des membres de celle-ci.*
>
> *Vous pouvez aussi ajouter un utilisateur au Jumpoint, en ignorant ses paramètres tels qu'ils sont définis ailleurs.*

> *Pour plus d'informations, veuillez consulter Configurer et installer un Jumpoint à l'adresse https://www.beyondtrust.com/docs/remote-support/how-to/jumpoint/installation.htm.*

Éléments de Jump : importation de raccourcis d'éléments de Jump

Jump | Éléments de Jump

Assistant d'importation en masse de raccourcis de Jump

Créez des raccourcis de Jump pour lancer des sessions d'assistance technique standard, pour lancer une session de protocole de bureau à distance ou des sessions VNC, pour effectuer un Shell Jump vers des appareils réseau prenant en charge SSH ou Telnet, ou pour lancer des sessions Intel® vPro.

Lors de la création d'un grand nombre de raccourcis de Jump, il peut être plus aisé de les importer par le biais d'une feuille de calcul plutôt que de les ajouter un par un dans la console du technicien d'assistance.

Pour plus d'informations, veuillez consulter la section Utiliser des raccourcis de Jump pour effectuer un Jump vers des systèmes distants à l'adresse https://www.beyondtrust.com/docs/remote-support/how-to/jumpoint/jump-shortcuts.htm.

Télécharger un modèle adapté pour importer des raccourcis de Jump

Dans la liste déroulante de la **section Assistant d'importation en masse de raccourcis de Jump**, sélectionnez le type d'élément de Jump que vous souhaitez ajouter, puis cliquez sur **Télécharger modèle**. En utilisant le texte du modèle CSV comme en-têtes de colonnes, ajoutez les informations pour chaque raccourci de Jump que vous voulez importer. Les champs optionnels peuvent être remplis ou laissés vides.

Transférer le modèle d'assistant d'importation en masse de raccourcis de Jump

Importer des raccourcis de Jump

Une fois que vous avez fini de remplir le modèle, utilisez **Importer des raccourcis de Jump** pour transférer le fichier CSV contenant les informations d'éléments de Jump. Vous pouvez transférer un fichier d'une taille maximale de 5 Mo à la fois. Seul un type d'élément de Jump peut être inclus dans chaque fichier CSV.

Raccourci de Jump local - Aide

Paramètre	Description
Nom de l'hôte	Le nom d'hôte du point de terminaison auquel cet élément de Jump doit accéder. Cette chaîne contient 128 caractères au maximum.
Nom	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.
Groupe de Jump	Le nom de code du groupe de Jump avec lequel cet élément de Jump doit être associé. ***Remarque :** lorsqu'on utilise la méthode d'importation, un élément de Jump ne peut pas être associé à une liste personnelle d'éléments de Jump.*

Paramètre	Description
Balise (optionnelle)	Vous pouvez organiser vos éléments de Jump en catégories en ajoutant une balise. Cette chaîne contient 1 024 caractères au maximum.
Commentaires (optionnels)	Vous pouvez ajouter des commentaires à vos éléments de Jump. Cette chaîne contient 1 024 caractères au maximum.
Règle de Jump (optionnelle)	Le nom de code d'une règle de Jump. Vous pouvez spécifier une règle de Jump pour gérer l'accès à cet élément de Jump.
Portail public (optionnel)	Le portail public que l'élément de Jump devra utiliser pour se connecter.
Règle de session client présent (facultatif)	Le nom de code d'une règle de session. Vous pouvez spécifier une règle de session pour gérer les autorisations disponibles sur cet élément de Jump lorsqu'un client est présent.
Règle de session client absent (facultatif)	Le nom de code d'une règle de session. Vous pouvez spécifier une règle de session pour gérer les autorisations disponibles sur cet élément de Jump lorsqu'un client est absent.

Raccourci de Jump distant - Aide

Paramètre	Description
Nom de l'hôte	Le nom d'hôte du point de terminaison auquel cet élément de Jump doit accéder. Cette chaîne contient 128 caractères au maximum.
Jumpoint	Le nom de code du Jumpoint à travers lequel l'on accède au point de terminaison.
Nom	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.
Groupe de Jump	Le nom de code du groupe de Jump avec lequel cet élément de Jump doit être associé. ***Remarque :*** *lorsqu'on utilise la méthode d'importation, un élément de Jump ne peut pas être associé à une liste personnelle d'éléments de Jump.*
Balise (optionnelle)	Vous pouvez organiser vos éléments de Jump en catégories en ajoutant une balise. Cette chaîne contient 1 024 caractères au maximum.
Commentaires (optionnels)	Vous pouvez ajouter des commentaires à vos éléments de Jump. Cette chaîne contient 1 024 caractères au maximum.
Règle de Jump (optionnelle)	Le nom de code d'une règle de Jump. Vous pouvez spécifier une règle de Jump pour gérer l'accès à cet élément de Jump.
Portail public (optionnel)	Le portail public que l'élément de Jump devra utiliser pour se connecter.
Règle de session client présent (facultatif)	Le nom de code d'une règle de session. Vous pouvez spécifier une règle de session pour gérer les autorisations disponibles sur cet élément de Jump lorsqu'un client est présent.
Règle de session client absent (facultatif)	Le nom de code d'une règle de session. Vous pouvez spécifier une règle de session pour gérer les autorisations disponibles sur cet élément de Jump lorsqu'un client est absent.

Raccourci de Jump VNC local - Aide

Paramètre	Description
Nom de l'hôte	Le nom d'hôte du point de terminaison auquel cet élément de Jump doit accéder. Cette chaîne contient 128 caractères au maximum.
Port (optionnel)	Un numéro de port valide entre **100** et **65535**. Sélectionne par défaut **5900**.
Nom	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.
Groupe de Jump	Le nom de code du groupe de Jump avec lequel cet élément de Jump doit être associé. ***Remarque :*** *lorsqu'on utilise la méthode d'importation, un élément de Jump ne peut pas être associé à une liste personnelle d'éléments de Jump.*
Balise (optionnelle)	Vous pouvez organiser vos éléments de Jump en catégories en ajoutant une balise. Cette chaîne contient 1 024 caractères au maximum.
Commentaires (optionnels)	Vous pouvez ajouter des commentaires à vos éléments de Jump. Cette chaîne contient 1 024 caractères au maximum.
Règle de Jump (optionnelle)	Le nom de code d'une règle de Jump. Vous pouvez spécifier une règle de Jump pour gérer l'accès à cet élément de Jump.
Portail public (optionnel)	Le portail public que l'élément de Jump devra utiliser pour se connecter.

Raccourci de Jump VNC distant - Aide

Paramètre	Description
Nom de l'hôte	Le nom d'hôte du point de terminaison auquel cet élément de Jump doit accéder. Cette chaîne contient 128 caractères au maximum.
Jumpoint	Le nom de code du Jumpoint à travers lequel l'on accède au point de terminaison.
Port (optionnel)	Un numéro de port valide entre **100** et **65535**. Sélectionne par défaut **5900**.
Nom	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.
Groupe de Jump	Le nom de code du groupe de Jump avec lequel cet élément de Jump doit être associé. ***Remarque :*** *lorsqu'on utilise la méthode d'importation, un élément de Jump ne peut pas être associé à une liste personnelle d'éléments de Jump.*
Balise (optionnelle)	Vous pouvez organiser vos éléments de Jump en catégories en ajoutant une balise. Cette chaîne contient 1 024 caractères au maximum.
Commentaires (optionnels)	Vous pouvez ajouter des commentaires à vos éléments de Jump. Cette chaîne contient 1 024 caractères au maximum.

Paramètre	Description
Règle de Jump (optionnelle)	Le nom de code d'une règle de Jump. Vous pouvez spécifier une règle de Jump pour gérer l'accès à cet élément de Jump.
Portail public (optionnel)	Le portail public que l'élément de Jump devra utiliser pour se connecter.

Raccourci de Jump RDP distant - Aide

Paramètre	Description
Nom de l'hôte	Le nom d'hôte du point de terminaison auquel cet élément de Jump doit accéder. Cette chaîne contient 128 caractères au maximum.
Jumpoint	Le nom de code du Jumpoint à travers lequel l'on accède au point de terminaison.
Nom d'utilisateur (optionnel)	Le nom d'utilisateur avec lequel se connecter.
Domaine (optionnel)	Le domaine où se trouve le point de terminaison.
Qualité (optionnelle)	La qualité à laquelle afficher le système distant. Peut être **basse** (niveaux de gris 2 bits pour une consommation de bande passante minimale), **meilleure_perf** (par défaut - couleur 8 bits pour performances rapides), **perf_et_qual** (16 bits pour une qualité d'image et des performances moyennes), **meilleure_qual** (32 bits pour une résolution d'image maximale), ou **video_opt** (codec VP9 pour une vidéo plus fluide). Notez que ce réglage ne peut plus être modifié une fois la session de protocole de bureau à distance démarrée.
Session de console (optionnelle)	**1** : Démarre une session de console. **0** : Démarre nouvelle session (par défaut).
Ignorer un certificat non approuvé (optionnel)	**1** : Ignore les avertissements de certificat. **0** : Affiche un avertissement si le certificat du serveur ne peut pas être vérifié.
Nom	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.
Groupe de Jump	Le nom de code du groupe de Jump avec lequel cet élément de Jump doit être associé. ***Remarque :*** *lorsqu'on utilise la méthode d'importation, un élément de Jump ne peut pas être associé à une liste personnelle d'éléments de Jump.*
Balise (optionnelle)	Vous pouvez organiser vos éléments de Jump en catégories en ajoutant une balise. Cette chaîne contient 1 024 caractères au maximum.
Commentaires (optionnels)	Vous pouvez ajouter des commentaires à vos éléments de Jump. Cette chaîne contient 1 024 caractères au maximum.
Règle de Jump (optionnelle)	Le nom de code d'une règle de Jump. Vous pouvez spécifier une règle de Jump pour gérer l'accès à cet élément de Jump.
Portail public (optionnel)	Le portail public que l'élément de Jump devra utiliser pour se connecter.

Raccourci de Jump RDP local - Aide

Paramètre	Description
Nom de l'hôte	Le nom d'hôte du point de terminaison auquel cet élément de Jump doit accéder. Cette chaîne contient 128 caractères au maximum.
Nom d'utilisateur (optionnel)	Le nom d'utilisateur avec lequel se connecter.
Domaine (optionnel)	Le domaine où se trouve le point de terminaison.
Qualité (optionnelle)	La qualité à laquelle afficher le système distant. Peut être **basse** (niveaux de gris 2 bits pour une consommation de bande passante minimale), **meilleure_perf** (par défaut - couleur 8 bits pour performances rapides), **perf_et_qual** (16 bits pour une qualité d'image et des performances moyennes), **meilleure_qual** (32 bits pour une résolution d'image maximale), ou **video_opt** (codec VP9 pour une vidéo plus fluide). Notez que ce réglage ne peut plus être modifié une fois la session de protocole de bureau à distance démarrée.
Session de console (optionnelle)	**1** : Démarre une session de console. **0** : Démarre nouvelle session (par défaut).
Ignorer un certificat non approuvé (optionnel)	**1** : Ignore les avertissements de certificat. **0** : Affiche un avertissement si le certificat du serveur ne peut pas être vérifié.
Nom	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.
Groupe de Jump	Le nom de code du groupe de Jump avec lequel cet élément de Jump doit être associé. ***Remarque :*** *lorsqu'on utilise la méthode d'importation, un élément de Jump ne peut pas être associé à une liste personnelle d'éléments de Jump.*
Balise (optionnelle)	Vous pouvez organiser vos éléments de Jump en catégories en ajoutant une balise. Cette chaîne contient 1 024 caractères au maximum.
Commentaires (optionnels)	Vous pouvez ajouter des commentaires à vos éléments de Jump. Cette chaîne contient 1 024 caractères au maximum.
Règle de Jump (optionnelle)	Le nom de code d'une règle de Jump. Vous pouvez spécifier une règle de Jump pour gérer l'accès à cet élément de Jump.
Portail public (optionnel)	Le portail public que l'élément de Jump devra utiliser pour se connecter.

Raccourci de Shell Jump - Aide

Paramètre	Description
Nom de l'hôte	Le nom d'hôte du point de terminaison auquel cet élément de Jump doit accéder. Cette chaîne contient 128 caractères au maximum.
Jumpoint	Le nom de code du Jumpoint à travers lequel l'on accède au point de terminaison.

Paramètre	Description
Nom d'utilisateur (optionnel)	Le nom d'utilisateur avec lequel se connecter.
Protocole	Peut être **ssh** ou **telnet**.
Port (optionnel)	Un numéro de port valide entre **1** et **65535**. Se règle par défaut sur **22** si le protocole est **ssh**, ou **23** si le protocole est **Telnet**.
Type de terminal (optionnel)	Peut être **xterm** (par défaut) ou **VT100**.
Persistance (optionnelle)	Le nombre de secondes entre chaque paquet envoyé pour empêcher une session inactive de s'arrêter. Peut être compris entre **0** et **300**. **Zéro** désactive la persistance (réglé par défaut).
Nom	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.
Groupe de Jump	Le nom de code du groupe de Jump avec lequel cet élément de Jump doit être associé. ***Remarque :*** *lorsqu'on utilise la méthode d'importation, un élément de Jump ne peut pas être associé à une liste personnelle d'éléments de Jump.*
Balise (optionnelle)	Vous pouvez organiser vos éléments de Jump en catégories en ajoutant une balise. Cette chaîne contient 1 024 caractères au maximum.
Commentaires (optionnels)	Vous pouvez ajouter des commentaires à vos éléments de Jump. Cette chaîne contient 1 024 caractères au maximum.
Règle de Jump (optionnelle)	Le nom de code d'une règle de Jump. Vous pouvez spécifier une règle de Jump pour gérer l'accès à cet élément de Jump.
Règle de session (optionnelle)	Le nom de code d'une règle de session. Vous pouvez spécifier une règle de session pour gérer les autorisations disponibles sur cet élément de Jump.
Portail public (optionnel)	Le portail public que l'élément de Jump devra utiliser pour se connecter.

Raccourci Intel vPro - Aide

Paramètre	Description
Nom de l'hôte	Le nom d'hôte du point de terminaison auquel cet élément de Jump doit accéder. Cette chaîne contient 128 caractères au maximum.
Jumpoint	Le nom de code du Jumpoint à travers lequel l'on accède au point de terminaison.
Nom	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.
Groupe de Jump	Le nom de code du groupe de Jump avec lequel cet élément de Jump doit être associé.

Paramètre	Description
	Remarque : *lorsqu'on utilise la méthode d'importation, un élément de Jump ne peut pas être associé à une liste personnelle d'éléments de Jump.*
Balise (optionnelle)	Vous pouvez organiser vos éléments de Jump en catégories en ajoutant une balise. Cette chaîne contient 1 024 caractères au maximum.
Commentaires (optionnels)	Vous pouvez ajouter des commentaires à vos éléments de Jump. Cette chaîne contient 1 024 caractères au maximum.
Règle de Jump (optionnelle)	Le nom de code d'une règle de Jump. Vous pouvez spécifier une règle de Jump pour gérer l'accès à cet élément de Jump.
Portail public (optionnel)	Le portail public que l'élément de Jump devra utiliser pour se connecter.

Pour plus d'informations, veuillez consulter la section Utiliser des raccourcis de Jump pour effectuer un Jump vers des systèmes distants à l'adresse https://www.beyondtrust.com/docs/remote-support/how-to/jumpoint/jump-shortcuts.htm.

Paramètres d'élément de Jump

Jumps simultanés

Pour Jump Client, Jump local, Jump distant, VNC local, VNC distant, Intel® vPro

Définissez les **Jumps simultanés** sur **Rejoindre une session existante** pour offrir à plusieurs utilisateurs le moyen d'accéder au même élément de Jump sans avoir à être invités à rejoindre une session active par un autre utilisateur. Le premier utilisateur à accéder à cet élément de Jump conserve la propriété de la session. Les utilisateurs dans une session de Jump partagée peuvent se voir et discuter.

Choisissez l'option **Interdire Jump** si vous souhaitez qu'un seul utilisateur à la fois soit en mesure d'effectuer un Jump vers un élément de Jump. S'il souhaite accéder à la session, un second utilisateur doit obtenir une invitation de la part de l'utilisateur ayant ouvert la session.

Ce réglage s'applique aux types d'éléments de Jump suivants :

- Jump Client
- Jump local
- Jump distant
- VNC local
- VNC distant
- Shell Jump
- Intel® vPro

Pour un RDP distant, RDP local

Définissez les **Jumps simultanés** sur **Démarrer une nouvelle session** pour offrir à plusieurs utilisateurs le moyen d'accéder au même élément de Jump sans avoir à être invités à rejoindre une session active par un autre utilisateur. Pour les RDP, plusieurs utilisateurs peuvent accéder à un élément de Jump, mais chacun d'entre eux démarre une session indépendante.

Choisissez l'option **Interdire Jump** si vous souhaitez qu'un seul utilisateur à la fois soit en mesure d'effectuer un Jump vers un élément de Jump. S'il souhaite accéder à la session, un second utilisateur doit obtenir une invitation de la part de l'utilisateur ayant ouvert la session.

Ce paramètre ne s'applique qu'aux types d'éléments de Jump RDP distant et local.

Vault pour Remote Support

Détection : domaines, comptes et points de terminaison

Vault | **Détection**

BeyondTrust Vault est un magasin d'informations d'authentification sur serveur permettant la détection et l'accès à des informations d'authentification privilégiées. Vous pouvez ajouter manuellement des informations d'authentification privilégiées, ou vous pouvez utiliser l'outil de détection intégré pour scanner et importer les comptes Active Directory et locaux dans BeyondTrust Vault.

Pour plus d'informations, veuillez consulter le Livre blanc technique de BeyondTrust Vault à l'adresse https://www.beyondtrust.com/docs/remote-support/how-to/vault/index.htm.

Détection : Nouvelle tâche

Avec l'add-on BeyondTrust Vault, vous pouvez détecter les comptes Active Directory, les comptes locaux et les points de terminaison. Les Jumpoints sont utilisés pour scanner les points de terminaison et détecter les comptes associés à ces derniers.

Pour en savoir plus sur les Jumpoints, veuillez consulter le Guide de Jumpoint Remote Support BeyondTrust à l'adresse https://www.beyondtrust.com/docs/remote-support/how-to/jumpoint/index.htm.

Cliquez sur **Nouvelle tâche de détection** pour lancer une détection. Les options sont :

- **Domaine Windows** : détectez des points de terminaison, des comptes de domaine et des comptes locaux accessibles depuis un Jumpoint sur un domaine Windows.
- **Comptes locaux Windows sur les Jump Clients** : détectez des comptes Windows locaux sur les machines pour lesquelles un Jump Client en mode service, actif est actuellement en ligne.

***Remarque :** l'option **Comptes locaux Windows sur les Jump Clients** s'affiche uniquement si vous disposez d'une autorisation pour des **Jump Clients** située dans **Utilisateurs et sécurité > Utilisateurs > Autorisations du technicien d'assistance > Technologie Jump**. Si vous rencontrez des problèmes, contactez l'administrateur de votre site.*

Cliquez sur **Continuer** pour lancer le processus de détection.

Si vous avez sélectionné **Domaine Windows**, suivez les étapes de la section **Ajouter un domaine**. Si vous avez sélectionné **Comptes locaux Windows sur les Jump Clients**, suivez les étapes dans la section **Détection : Critère de recherche de Jump Client**.

Ajouter un domaine

Nom de DNS

Saisissez le nom DNS pour votre environnement.

Jumpoint

Choisissez un Jumpoint existant situé dans l'environnement où vous souhaitez détecter des comptes.

Compte de gestion

Sélectionnez le compte de gestion nécessaire au lancement de la tâche de détection. Choisissez d'utiliser un nouveau compte, lequel nécessitera la saisie d'un **nom d'utilisateur**, d'un **mot de passe** et d'une **confirmation du mot de passe**. Ou alors, choisissez d'utiliser un compte existant détecté lors d'une précédente tâche ou ajouté manuellement dans la section **Comptes**. Une fois qu'un compte est sélectionné, cliquez sur **Continuer** pour lancer la tâche de détection.

Détection : Critère de recherche de Jump Client

Saisissez un ou plusieurs critères de recherche pour trouver des Jump Clients actifs que vous aimeriez utiliser pour détecter des comptes locaux Windows. Toutes les recherches dans le champ texte sont partielles et insensibles à la casse. Les Jump Clients qui correspondent à tous les critères de recherche seront affichés sur la page suivant afin que vous puissiez effectuer une sélection avant le début de la détection.

> ***Remarque :***
> *Les types suivants de Jump Clients ne peuvent pas être utilisés pour la détection d'un compte local et ne seront pas inclus dans les résultats de recherche :*
>
> - *Jump Clients actuellement hors ligne ou désactivés*
> - *Jump Clients qui ne s'exécutent pas en tant que service accru*
> - *Jump Clients qui sont installés dans un contrôleur de domaine*
> - *Jump Clients passifs*

Groupes de Jump

Les administrateurs peuvent rechercher des Jump Clients via leurs groupes de Jump et leurs attributs. Si l'utilisateur n'est membre d'aucun groupe de Jump, la section de sélection **Groupes de Jump** est grisée et une info-bulle ou une note s'affiche indiquant que l'utilisateur doit être membre d'au moins un groupe de Jump pour poursuivre le processus de détection de Jump Client. Ceci est similaire au fonctionnement de la détection de domaine lorsqu'un utilisateur n'est pas membre d'un Jumpoint pendant la détection ou n'est pas membre d'un groupe de Jump lors de l'importation d'un point de terminaison.

Vous pouvez rechercher **Tous vos groupes de Jump partagés** ou des **Groupes de Jump spécifiques**.

Attributs de Jump Client

Vous pouvez sélectionner un ou plusieurs groupes de Jump partagés. Les groupes de Jump privés ne sont pas pris en charge.

Un ou plusieurs attributs de Jump Client peuvent être saisis. Si plusieurs critères de recherche sont saisis, seuls les Jump Clients correspondant à tous les critères sont utilisés pour la détection.

Les attributs suivants peuvent être utilisés comme critères de recherche :

- **Nom** : Le nom du Jump Client tel qu'il apparaît dans la colonne **Nom** dans la Console du technicien d'assistance.
- **Nom d'hôte** : Le nom d'hôte du Jump Client tel qu'il apparaît dans la colonne **Nom d'hôte/IP** de la Console du technicien d'assistance.

- **FQDN** : Le nom de domaine complet du Jump Client, tel qu'il apparaît sous l'étiquette **FQDN** du volet de détails du Jump Client dans la Console du technicien d'assistance.
- **Balise** : La balise du Jump Client telle qu'elle apparaît dans la colonne **Balise** de la console du technicien d'assistance.
- **IP publique/privée** : Les adresses IP publique et privée du Jump Client, telles qu'elle apparaîssent sous l'étiquette **IP publique** du volet de détails du Jump Client dans la Console du technicien d'assistance. Les Jump Clients dont l'adresse IP commence par la valeur de recherche donnée correspondront.

Cliquez sur **Continuer** pour lancer la détection.

Détection : Sélectionner des Jump Clients

Cet écran affiche les Jump Clients qui seront utilisés pour la détection. Sélectionnez-en un ou plusieurs puis cliquez sur **Lancer la détection**.

Résultats de la détection

Les résultats fournissent une liste de **Points de terminaison** et de **Comptes locaux** détectés. Sélectionnez-en un ou plusieurs puis cliquez sur **Importer la sélection**.

Importer les éléments détectés

Une liste des sélections que vous avez effectuées s'affiche.

Groupe de comptes

Sélectionnez à partir du groupe de comptes que vous souhaitez importer, puis cliquez sur **Lancer l'importation**. Un avertissement s'affiche, indiquant que ce processus ne peut pas être arrêté une fois qu'il a commencé. Cliquez sur **Oui** pour poursuivre ou sur **Non** pour annuler.

Importation en cours

Un message s'affiche indiquant que l'importation a été effectuée. Une liste des **points de terminaison** et des **comptes locaux** s'affiche.

Comptes

Chercher des comptes partagés/personnels

Si vous obtenez une liste étendue de comptes détectés, utilisez le champ **Rechercher** pour chercher des comptes par **Nom**, **Point de terminaison** ou **Description** (par **Nom** et **Description** pour les comptes personnels uniquement).

Basculez entre les comptes **Partagé** et **Personnel**. Sélectionnez un ou plusieurs comptes. Cliquez sur **...** pour **Provoquer la rotation du mot de passe**, **Modifier** ou **Supprimer** le compte. Vous pouvez aussi cliquer sur **Provoquer la rotation** en haut de page pour provoquer la rotation du mot de passe des comptes sélectionnés.

Tâches de détection (Domaine Windows)

Consultez les tâches de détection en cours pour un domaine spécifique, ou vérifiez les résultats des tâches de détection ayant réussi ou échoué.

Consulter les résultats

Consultez les résultats de la tâche de détection dans la section **Résultats de la détection**, incluant les points de terminaison détectés, les comptes locaux détectés et les comptes de domaine trouvés sur le domaine. Pour chaque élément détecté, un **nom** et une **description** seront fournis. Vous pouvez sélectionner les points de terminaison et comptes à importer et stocker dans votre instance BeyondTrust Vault. Cochez la case à côté de chaque élément de la liste que vous souhaitez importer, puis cliquez sur **Importer la sélection**.

> *Pour plus d'informations, veuillez consulter Détecter des domaines, des points de terminaison et des comptes avec BeyondTrust Vault à l'adresse https://www.beyondtrust.com/docs/remote-support/how-to/vault/discovery.htm.*

Comptes : gérer les comptes Vault

Vault | **Comptes**

Consultez et gérez les informations de tous les comptes détectés et ajoutés manuellement. Les informations disponibles pour les comptes partagés comprennent :

- **Type** : Le type de compte, à savoir, si c'est un compte de domaine ou un compte local, ou bien un compte à mot de passe générique.
- **Nom** : Le nom du compte.
- **Groupe** : Le nom du groupe de comptes auquel le compte appartient.
- **Point de terminaison** : Le point de terminaison auquel le compte est associé.
- **Description** : Description brève au sujet du compte.
- **Dernière extraction** : La dernière fois que le compte a été extrait.
- **Âge du mot de passe** : L'âge du mot de passe.

> ***Astuce:*** *Vous pouvez filtrer la liste des comptes partagés affichée à l'aide des filtres en fonction du* ***Groupe*** *et de l'****Âge du mot de passe****.*

Sur la base de cette information, vous pouvez procéder à différentes actions, incluant l'extraction/l'archivage d'informations d'authentification et la rotation d'informations d'authentification.

Les informations disponibles pour les comptes personnels comprennent :

- **Type** : Le type de compte, à savoir, si c'est un compte de domaine ou un compte local, ou bien un compte à mot de passe générique.
- **Nom** : Le nom du compte.
- **Propriétaire** : Le nom de la personne qui a créé et possède le compte.
- **Description** : Description brève au sujet du compte.
- **Âge du mot de passe** : L'âge du mot de passe.

> ***Astuce:*** *Vous pouvez filtrer la liste des comptes partagés affichée à l'aide des filtres en fonction du* ***Propriétaire*** *et de l'****Âge du mot de passe****.*

Comptes

Ajouter un compte

Cliquez sur **Ajouter** pour ajouter manuellement un compte partagé ou générique personnel à BeyondTrust Vault.

Chercher des comptes partagés

Recherchez un compte partagé ou groupe de comptes spécifique en fonction du **Nom**, du **Nom du point de terminaison** ou de la **Description**.

Extraction/Archivage d'un compte partagé

Cliquez sur **Extraction** pour voir et utiliser les informations d'authentification. Lorsque sélectionné, l'invite du **Mot de passe du compte** apparaît, affichant les informations d'authentification pendant 60 secondes pour vous permettre de copier le mot de passe. Une fois l'invite fermée, l'option **Archivage** devient alors disponible. Lorsque vous avez fini d'utiliser le compte, cliquez sur **Archivage** pour archiver à nouveau le mot de passe dans le système.

> *Pour plus d'informations, veuillez consulter Extraire des informations d'authentification depuis l'interface /login à l'adresse https://www.beyondtrust.com/docs/remote-support/how-to/vault/check-out.htm.*

Menu à points de suspension pour les comptes partagés

Cliquez sur **...** pour voir plus d'actions, telles que **Rotation du mot de passe**, **Modifier** et **Supprimer**. Lorsque vous sélectionnez **Rotation du mot de passe**, le système procède automatiquement à une rotation ou un changement du mot de passe. Lorsque vous sélectionnez **Modifier**, vous pouvez seulement modifier les informations du compte. L'option **Supprimer** supprime le compte de la liste **Comptes**.

Chercher des comptes personnels

Recherchez un compte personnel ou groupe de comptes spécifique en fonction du **Nom** ou de la **Description**.

Afficher le mot de passe pour un compte personnel

Cliquez sur **Afficher le mot de passe** pour voir et utiliser les informations d'authentification. Lorsque sélectionné, l'invite du **Mot de passe du compte** apparaît, affichant les informations d'authentification pendant 60 secondes pour vous permettre de copier le mot de passe.

Modifier le compte personnel

Cliquez sur **Modifier le compte** pour modifier les informations du compte, à savoir **Nom**, **Description**, **Nom d'utilisateur** et **Mot de passe**.

Ajouter un compte générique partagé

L'option **Ajouter > Compte générique partagé** vous permet d'ajouter des comptes sans avoir à lancer une tâche de détection. Au lieu de cela, vous pouvez saisir manuellement les informations à propos du compte. Cette option est utile dans les situations où un compte partagé ou une combinaison de nom d'utilisateur/mot de passe peut être utilisé pour accéder à de nombreux systèmes différents.

Nom

Saisissez un nom pour le compte.

Description

Saisissez une description brève et facile à mémoriser du compte.

Nom d'utilisateur

Fournissez le nom d'utilisateur du compte.

Authentification

Sélectionnez la méthode d'authentification pour le compte : **Mot de passe** ou **Clé privée SSH**.

> ***Remarque :*** *si vous sélectionnez une clé privée SSH pour l'authentification, vous devez fournir une clé privée pour le compte au format OpenSSH. Facultativement, vous pouvez inclure la phrase secrète associée à la clé privée.*

Mot de passe et confirmation du mot de passe

Si la méthode d'authentification sélectionnée est **Mot de passe**, vous devez saisir le mot de passe du compte et le confirmer.

Clé privée SSH

Si la méthode d'authentification **Clé privée SSH** est sélectionnée, vous devez saisir la clé privée SSH du compte.

Phrase secrète de clé SSH

Si applicable, saisissez la phrase secrète de la clé privée SSH.

Permettre les extractions simultanées

Si le compte peut être extrait et utilisé par de multiples utilisateurs ou sessions à la fois, sélectionnez cette option.

Groupe de comptes

Sélectionnez un groupe dans la liste pour ajouter le compte partagé à un groupe de comptes. Si aucun groupe n'est sélectionné, le compte est ajouté au groupe système **Aucun**.

Utilisateurs du compte

Nouveau nom d'utilisateur

Sélectionnez les utilisateurs autorisés à accéder à ce compte.

Nouveau rôle de membre

L'un de ces deux rôles peut être assigné aux utilisateurs :

- **Injecter** (valeur par défaut) : Les utilisateurs dotés de ce rôle peuvent utiliser ce compte dans des sessions Remote Support.
- **Injecter et extraire** : Les utilisateurs dotés de ce rôle peuvent utiliser ce compte dans des sessions Remote Support et peuvent extraire le compte sur **/login**. L'autorisation d'**extraction** n'a pas d'effet sur les comptes génériques SSH.

> ***Remarque :*** *le **rôle de compte Vault** est visible dans la liste des utilisateurs ajoutés au compte Vault.*

Remarque : *lors d'une mise à niveau vers une installation Remote Support BeyondTrust avec la fonction Extraction configurable du Vault, toutes les* ***appartenances de compte Vault*** *existantes qui étaient configurées dans les règles de groupe avant la mise à niveau verront leur* ***rôle de compte Vault*** *défini par défaut sur* ***Injecter et extraire*** *après la mise à niveau.*

IMPORTANT !

Prévalence des rôles de compte Vault *: les rôles de compte Vault peuvent être assignés à la fois aux utilisateurs et aux règles de groupe. Cela signifie qu'un même utilisateur peut avoir différents rôles pour un seul compte Vault. Un rôle peut être assigné par les règles de groupe de l'utilisateur, tandis qu'un autre peut l'être en vertu de l'accès explicite de l'utilisateur au compte Vault. Dans de tels cas, le système utilise le rôle le plus spécifique pour cet utilisateur. Par conséquent, le système autorisera le rôle assigné par la page* ***Modifier le compte Vault*** *à outrepasser le rôle assigné par la règle de groupe de l'utilisateur. Lorsque le rôle est remplacé de cette manière, le mot outrepassé apparaît sur la page* ***Modifier le compte Vault*** *en ce qui concerne les règles de groupe associées à l'utilisateur. Ce comportement est conforme avec l'ordre de prévalence pour les rôles d'élément de Jump.*

Remarque : *les comptes utilisateur avec la permission* ***Autorisé à administrer Vault*** *sont implicitement autorisés à accéder à tous les comptes Vault.*

Ajouter un compte personnel

L'option **Ajouter > Compte générique personnel** vous permet d'ajouter des comptes.

Nom

Saisissez un nom pour le compte.

Description

Saisissez une description brève et facile à mémoriser du compte.

Nom d'utilisateur

Fournissez le nom d'utilisateur du compte.

Authentification

Sélectionnez la méthode d'authentification pour le compte : **Mot de passe** ou **Clé privée SSH**.

Remarque : *si une clé SSH est sélectionnée pour l'authentification, vous devez fournir une clé privée pour le compte au format OpenSSH. Facultativement, vous pouvez inclure la phrase secrète associée à la clé privée.*

Mot de passe et confirmation du mot de passe

Si la méthode d'authentification sélectionnée est **Mot de passe**, vous devez saisir le mot de passe du compte et le confirmer.

Clé privée SSH

Si la méthode d'authentification **Clé privée SSH** est sélectionnée, vous devez saisir la clé privée SSH du compte.

Phrase secrète de clé SSH

Si applicable, saisissez la phrase secrète de la clé privée SSH.

Modifier un compte local

Nom

Consultez ou modifiez le nom utilisé pour le compte.

Description

Consultez ou modifiez la description du compte.

Nom d'utilisateur

Consultez le nom d'utilisateur associé au compte.

Mot de passe et confirmation du mot de passe

Saisissez un nouveau mot de passe pour le compte, ou laissez le champ vide pour conserver le mot de passe existant. Confirmez le mot de passe saisi.

Âge du mot de passe

Consultez l'âge du mot de passe existant.

Rotation automatique des informations d'authentification après l'archivage

Définir des comptes locaux pour une rotation automatique après utilisation

Permettre les extractions simultanées

Si le compte peut être extrait et utilisé par de multiples utilisateurs ou sessions à la fois, sélectionnez cette option.

Groupe de comptes

Sélectionnez un groupe dans la liste pour ajouter le compte partagé à un groupe de comptes. Si aucun groupe n'est sélectionné, le compte est ajouté au groupe système **Aucun**.

Nom du point de terminaison

Consultez quels points de terminaison sont associés au compte.

Nom d'hôte du point de terminaison

Consultez le nom d'hôte des points de terminaison associés.

Utilisateurs du compte

Sélectionnez les utilisateurs autorisés à accéder à ce compte.

> ***Remarque :*** *les comptes utilisateur avec la permission* ***Autorisé à administrer Vault*** *sont implicitement autorisés à accéder à tous les comptes Vault.*

Modifier un compte de domaine

Nom

Consultez ou modifiez le nom utilisé pour le compte.

Description

Consultez ou modifiez la description du compte.

Nom d'utilisateur

Consultez le nom d'utilisateur associé au compte.

Mot de passe et confirmation du mot de passe

Saisissez un nouveau mot de passe pour le compte, ou laissez le champ vide pour conserver le mot de passe existant. Confirmez le mot de passe saisi.

Voir l'historique de mot de passe

Afficher la date et l'heure des modifications de mot de passe. Cliquez sur **Révéler** pour afficher temporairement le mot de passe. Cliquez sur **Utiliser** pour que le mot de passe de ce compte soit celui-ci.

Âge du mot de passe

Consultez l'âge du mot de passe existant.

Rotation automatique des informations d'authentification après l'archivage

Si vous souhaitez qu'une rotation des informations d'authentification ait lieu de façon automatique après archivage, sélectionnez cette option.

> ***Remarque :*** *les informations d'authentification Active Directory sont les seules qui prennent en charge la rotation automatique.*

Permettre les extractions simultanées

Si le compte peut être extrait et utilisé par de multiples utilisateurs ou sessions à la fois, sélectionnez cette option.

Nom unique

Consultez le nom unique du compte.

Groupe de comptes

Sélectionnez un groupe dans la liste pour ajouter le compte partagé à un groupe de comptes. Si aucun groupe n'est sélectionné, le compte est ajouté au groupe système **Aucun**.

Utilisateurs du compte

Sélectionnez les utilisateurs autorisés à accéder à ce compte.

> ***Remarque :*** *les comptes utilisateur avec la permission* ***Autorisé à administrer Vault*** *sont implicitement autorisés à accéder à tous les comptes Vault.*

Modifier un compte générique personnel (mot de passe)

Nom

Consultez ou modifiez le nom utilisé pour le compte.

Description

Consultez ou modifiez la description du compte.

Nom d'utilisateur

Consultez le nom d'utilisateur associé au compte.

Mot de passe et confirmation du mot de passe

Saisissez un nouveau mot de passe pour le compte, ou laissez le champ vide pour conserver le mot de passe existant. Confirmez le mot de passe saisi.

Groupes de comptes Vault : ajouter et gérer des groupes de comptes

Vault | **Groupes de comptes**

Les comptes Vault partagés peuvent être ajoutés à un groupe de comptes pour permettre aux administrateurs Vault d'accorder aux utilisateurs l'accès à plusieurs comptes Vault partagés plus efficacement. Les groupes de comptes peuvent également être utilisés pour associer un groupe de comptes Vault partagés à une règle de groupe.

> ***Remarque :*** *un compte vault partagé ne peut appartenir qu'à un seul groupe à la fois et les comptes vault personnels ne peuvent pas être ajoutés à un groupe de comptes.*

Groupes de comptes

Ajouter, afficher et gérer des groupes de comptes.

Ajouter un groupe de comptes

Cliquez sur **Ajouter** pour ajouter un groupe de comptes, ajouter des comptes Vault au groupe et accorder aux utilisateurs l'accès au groupe de comptes Vault partagés.

Chercher des groupes de comptes

Recherchez un groupe de comptes spécifique en fonction du **Nom** ou de la **Description**.

Ajouter un groupe de comptes

L'option **Ajouter un groupe de comptes** vous permet d'ajouter des groupes de comptes dans le but d'accorder aux utilisateurs l'accès à plusieurs comptes Vault à la fois.

Nom

Saisissez un nom pour le groupe de comptes.

Description

Saisissez une description brève et facile à mémoriser du groupe de comptes.

Règles de groupe

Si le groupe de comptes a été ajouté à des règles de groupe, ces dernières sont répertoriées ici, avec leurs rôles de compte Vault.

Comptes

Groupe de comptes sources

Filtrez la liste des comptes disponibles à ajouter au groupe en sélectionnant un groupe dans la liste **Groupe de comptes sources**.

Rechercher le groupe de comptes sélectionnés

Filtrez la liste des comptes disponibles à ajouter au groupe en recherchant un groupe de comptes. Vous pouvez chercher par **Nom**, **Point de terminaison** et **Description**.

Comptes n'étant pas dans un groupe

Liste des comptes Vault disponibles en vue de leur ajout au groupe de comptes.

Ajouter

Sélectionnez des comptes dans la liste des groupes disponibles, puis cliquez sur **Ajouter** pour les ajouter à la liste **Comptes dans ce groupe**.

Supprimer

Sélectionnez des comptes dans la liste **Comptes dans ce groupe**, puis cliquez sur **Supprimer** pour les supprimer du groupe de comptes.

Recherche ce groupe de comptes

Filtrez la liste **Comptes dans ce groupe** en cherchant un groupe de comptes en fonction de **Nom**, **Point de terminaison** et **Description**.

Comptes dans ce groupe

Liste des comptes Vault qui existent dans ce groupe de comptes.

Utilisateurs autorisés

Nouveau nom d'utilisateur

Sélectionnez les utilisateurs autorisés à accéder à ce compte.

Nouveau rôle de membre

Sélectionnez le rôle de compte Vault pour le nouvel utilisateur, puis cliquez sur **Ajouter**. L'un de ces deux rôles peut être assigné aux utilisateurs :

- **Injecter** (valeur par défaut) : Les utilisateurs dotés de ce rôle peuvent utiliser ce compte dans des sessions Remote Support.
- **Injecter et extraire** : Les utilisateurs dotés de ce rôle peuvent utiliser ce compte dans des sessions Remote Support et peuvent extraire le compte sur **/login**. L'autorisation d'**extraction** n'a pas d'effet sur les comptes génériques SSH.

> ***Remarque :*** *le* ***rôle de compte Vault*** *est visible dans la liste des utilisateurs ajoutés au compte Vault.*

Points de terminaison : gérer les points de terminaison détectés

Vault | **Points de terminaison**

Points de terminaison

Consultez les informations sur tous les points de terminaison détectés, telles que le nom et le nom de domaine du système, ainsi que les informations à propos des comptes associés à ces systèmes.

Recherche de points de terminaison

Recherchez un point de terminaison spécifique ou un groupe de points de terminaison sur la base du **nom**, du **nom d'hôte**, de la **description** ou du **nom du Jumpoint**.

Comptes

Consultez le nombre de comptes trouvés pendant la détection ainsi que les points de terminaison qui y sont associés. Cliquez sur l'option **Comptes** pour voir les comptes associés au système.

Modifier

Modifiez les informations du point de terminaison, à savoir le **Nom**, la **Description**, le **Nom d'hôte** et le **Jumpoint**.

Supprimer

Supprimez le point de terminaison de la liste des **points de terminaison**.

Gérer les comptes privilégiés utilisés sur les points de terminaison

Consultez et gérez les informations de tous les comptes détectés et ajoutés manuellement. Les informations disponibles incluent :

- **Type** : Le type de compte, à savoir, si c'est un compte de domaine ou un compte local.
- **Nom** : Le nom du compte.
- **Point de terminaison** : Le point de terminaison auquel le compte est associé.
- **Dernière extraction** : La dernière fois que le compte a été extrait.
- **Âge du mot de passe** : L'âge du mot de passe.

Sur la base de cette information, vous pouvez procéder à différentes actions, incluant l'extraction/l'archivage d'informations d'authentification et la rotation d'informations d'authentification.

Domaines : gérer des domaines avec Vault

Vault | **Domaines**

Domaines

Ajoutez, consultez et gérez des informations sur vos domaines.

Ajouter, modifier, supprimer

Ajoutez un nouveau domaine, modifiez un domaine existant ou supprimez un domaine existant.

Nom de domaine

Consultez le nom du domaine.

Jumpoint

Consultez le Jumpoint utilisé pour détecter des comptes et points de terminaison sur le domaine.

Compte de gestion

Consultez le compte de gestion associé au Jumpoint et au domaine.

Détecter

Cliquez sur **Détecter** pour que le Jumpoint commence à scanner et détecter des points de terminaison et des comptes sur le domaine.

Ajouter ou modifier un domaine

Nom DNS

Saisissez le **nom DNS** du domaine.

Jumpoint

Choisissez un Jumpoint existant situé dans l'environnement où vous souhaitez détecter des comptes.

Compte de gestion

Sélectionnez le compte de gestion nécessaire au lancement de la tâche de détection pour ce domaine. Choisissez d'utiliser un nouveau compte, lequel nécessitera la saisie d'un **nom d'utilisateur**, d'un **mot de passe** et d'une **confirmation du mot de passe**. Ou alors, choisissez d'utiliser un compte existant détecté lors d'une précédente tâche ou ajouté manuellement dans la section **Comptes**.

Options : planifier la rotation des mots de passe

Vault | **Options**

Gestion automatique des mots de passe

Activer la rotation planifiée des mots de passe

Cochez l'option **Activer la rotation planifiée des mots de passe** pour provoquer une rotation automatique des mots de passe des comptes Vault lorsqu'ils atteignent un âge maximal spécifié.

Âge maximum du mot de passe

Spécifiez le nombre maximal de jours pendant lesquels un mot de passe peut être en place pour des comptes Vault avant qu'il ne soit automatiquement mis en rotation.

Console du technicien d'assistance

Paramètres de la console du technicien d'assistance : gestion des paramètres par défaut de la console du technicien d'assistance

Gestion des paramètres de la Console du technicien d'assistance

Vous pouvez configurer les paramètres par défaut de la console du technicien d'assistance pour l'ensemble de votre base d'utilisateurs, afin d'obtenir une expérience utilisateur de console du technicien d'assistance homogène et d'augmenter l'efficacité de votre équipe. Vous pouvez forcer des paramètres, permettre aux utilisateurs de les outrepasser, ou ne pas les gérer. Si vous sélectionnez **Non gérés**, la configuration BeyondTrust par défaut s'affiche à des fins d'examen.

Chaque paramètre d'**activation** et de **désactivation** inclut une option d'administration permettant l'application forcée du paramètre. Les paramètres forcés prennent effet lors de la prochaine connexion de l'utilisateur et ne permettent pas la configuration dans la console. Les paramètres non forcés peuvent être outrepassés par un utilisateur dans la fenêtre des paramètres de la console du technicien d'assistance.

> *Pour plus d'informations, consultez Modification des paramètres et préférences de la console du technicien d'assistance à l'adresse https://www.beyondtrust.com/docs/remote-support/getting-started/rep-console/settings.htm.*

Un paramètre forcé ne peut pas être outrepassé, sauf si un administrateur décoche l'option **Forcé** pour ce paramètre dans l'interface d'administration **/login**.

Choisissez les paramètres par défaut pour vos utilisateurs, puis cliquez sur le bouton **Enregistrer** au bas de la page.

Notez que les paramètres enregistrés ne prennent effet qu'à la connexion à la console. Même si vous enregistrez et appliquez les modifications avec le bouton **Appliquer maintenant** situé en haut de page (voir plus loin), l'utilisateur n'utilisera les nouveaux paramètres qu'après connexion.

Si, par exemple, vous souhaitez définir des paramètres par défaut pour les nouveaux utilisateurs tout en conservant les paramètres définis pour les utilisateurs existants, enregistrez vos paramètres gérés sans les appliquer. De cette manière, toutes les nouvelles connexions à la console du technicien d'assistance démarreront avec vos paramètres gérés par défaut. Les paramètres forcés seront appliqués aux utilisateurs existants à la prochaine connexion, mais tous les autres paramètres resteront identiques.

Paramètres globaux

Correcteur orthographique activé

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.

Désactiver l'attribution automatique de session lors de la connexion

Si l'attribution automatique de session est désactivée à la connexion, aucune session n'est automatiquement attribuée à l'utilisateur tant que ceux-ci n'en décident pas autrement.

Barre latérale de session configurable

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.

Boutons de démarrage rapide

Pour plus d'informations, veuillez consulter la section Interface d'utilisateur de la Console du technicien d'assistance à l'adresse https://www.beyondtrust.com/docs/remote-support/getting-started/rep-console/representative-console-overview.htm.

***Remarque :** utilisez l'option **Forcé** pour que les techniciens d'assistance ne puissent outrepasser les paramètres gérés par défaut.*

Démarrer une session

Afficher un bouton **Démarrer** en haut de la console du technicien d'assistance. Cliquer sur ce bouton permet à l'utilisateur de consulter les moyens dont dispose votre client pour démarrer une session d'assistance technique.

Clé de session

Afficher un bouton de création de clé de session en haut de la console du technicien d'assistance.

Bouton assistance techniques

Afficher un bouton pour lancer l'interface de gestion de Bouton assistance technique en haut de la console du technicien d'assistance.

Shell Jump

Afficher un bouton pour lancer une session Shell Jump en haut de la console du technicien d'assistance.

Jump

Afficher un bouton pour lancer une session Jump locale ou distante en haut de la console du technicien d'assistance.

Intel® vPro

Afficher un bouton pour lancer l'accès à une session vPro Jumpoint préparée en haut de la console du technicien d'assistance.

RDP

Afficher un bouton pour lancer une session RDP en haut de la console du technicien d'assistance.

VNC

Afficher un bouton pour lancer une session VNC en haut de la console du technicien d'assistance.

Démarrer la présentation

Afficher un bouton pour planifier ou commencer immédiatement une nouvelle présentation en haut de la console du technicien d'assistance.

Alertes

Alertes sonores - Émettre un signal sonore lors de la réception d'un message instantané

Choisissez si une alerte sonore doit retentir lorsque l'utilisateur reçoit un message instantané. Si cela n'est pas géré, ou si cela est activé mais non forcé, l'utilisateur peut désigner un son personnalisé au format WAV de 1 Mo maximum.

Alertes visuelles - Faire clignoter l'icône de l'application lors de la réception d'un message instantané

Choisissez si l'icône de l'application doit clignoter lorsque l'utilisateur reçoit un message instantané.

Afficher les messages d'état dans la messagerie instantanée des équipes d'assistance technique

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.

Notifications contextuelles

Files d'attente d'équipe

Choisissez si un utilisateur doit recevoir un avertissement contextuel pour les messages instantanés reçus dans la messagerie instantanée de l'équipe d'assistance technique.

Session d'assistance techniques

Choisissez si un utilisateur doit recevoir un avertissement contextuel pour les messages instantanés reçus dans une session d'assistance technique

Alertes sonores - Émettre un signal sonore lors de l'ajout d'une session dans une file d'attente

Choisissez si une alerte sonore doit retentir lorsqu'une session arrive dans une des files d'attente d'un utilisateur.

Alertes sonores - Émettre un signal sonore pour signaler les sessions en souffrance dans les files d'attente d'équipe

Choisissez si une alerte sonore doit retentir lorsqu'une session est en souffrance dans la file d'attente d'une équipe d'assistance technique.

Alertes visuelles - Faire clignoter l'icône de l'application lors de l'ajout d'une session dans une file d'attente

Choisissez si l'icône de l'application doit clignoter lorsqu'une session arrive dans l'une des files d'attente d'un utilisateur.

Alertes visuelles - Faire clignoter l'icône de l'application pour signaler les sessions en souffrance dans les files d'attente d'équipe

Choisissez si l'icône de l'application doit clignoter lorsqu'une session est en souffrance dans la file d'attente d'une équipe d'assistance technique.

Avertir lorsqu'un nouvel utilisateur arrive dans la file d'attente personnelle

Définissez si un utilisateur doit être prévenu lorsqu'une session arrive dans sa file d'attente personnelle.

Notifications contextuelles

Les notifications contextuelles s'affichent indépendamment de la console du technicien d'assistance et par-dessus les autres fenêtres. Si les notifications contextuelles sont activées mais non forcées ou laissées non gérées, l'utilisateur pourra choisir la façon dont il reçoit des notifications.

File d'attente personnelle - Nouvelles sessions, sessions transférées, sessions partagées

Choisissez si un utilisateur doit recevoir un avertissement contextuel pour les nouvelles sessions, les sessions transférées ou les sessions partagées dans cette file d'attente.

Files d'attente d'équipe - Nouvelles sessions, sessions transférées, sessions partagées, sessions en souffrance

Choisissez si un utilisateur doit recevoir un avertissement contextuel pour les nouvelles sessions, les sessions transférées, les sessions partagées ou les sessions en souffrance dans cette file d'attente.

Comportement contextuel - Emplacement et durée

Définissez l'emplacement et la durée par défaut des avertissements contextuels.

Alerte d'attribution de Session d'assistance technique

Alertes sonores - Émettre un signal sonore lors de l'attribution d'une session

Choisissez si une alerte sonore doit retentir lorsqu'une session est attribuée automatiquement à un utilisateur.

Signal sonore d'expiration d'une attribution

Choisissez si une alerte sonore doit retentir lorsqu'une invitation de session attribuée automatiquement est sur le point d'arriver à expiration. L'alerte peut être un fichier audio ou l'alerte sonore du système. Si cela n'est pas géré, ou si cela est activé mais non forcé, l'utilisateur peut désigner un son personnalisé au format WAV de 1 Mo maximum.

Session d'assistance techniques

Demander automatiquement le partage d'écran

Indiquez si vous souhaitez que les sessions de vos utilisateurs démarrent avec la messagerie instantanée uniquement ou avec une demande immédiate de partage d'écran.

Détacher automatiquement

Choisissez si vous souhaitez que les sessions s'ouvrent sous forme d'onglets dans la console du technicien d'assistance ou détacher les sessions automatiquement dans de nouvelles fenêtres.

Demander l'accroissement si le bureau sécurisé de l'utilisateur est activé

Lorsqu'il est probable que les utilisateurs rencontrent des problèmes d'assistance technique à cause du bureau sécurisé du client, vous pouvez autoriser la demande d'accroissement des privilèges afin que vos utilisateurs disposent de droits d'administrateur au démarrage de la session.

Qualité par défaut

Définissez la qualité par défaut pour les sessions de partage d'écran.

Échelle par défaut

Définissez la taille d'écran par défaut pour les sessions de partage d'écran.

Passer automatiquement en mode plein écran au démarrage du partage d'écran

L'utilisateur peut passer automatiquement en mode plein écran au démarrage du partage d'écran.

Réduire automatiquement la barre latérale en mode plein écran

Lorsque le partage d'écran passe en mode plein écran, la barre de discussion peut disparaître automatiquement.

Montrer mon écran

Minimiser automatiquement la fenêtre lorsque vous montrez votre écran

Lorsqu'un utilisateur montre son écran à un client, vous pouvez choisir de laisser la console du technicien d'assistance ouverte ou de la réduire dans la barre des tâches de l'utilisateur.

Interpréteur de commandes

Nombre de lignes d'historique de commande disponible

Vous pouvez définir le nombre de lignes à enregistrer dans l'historique de l'interpréteur de commandes. La valeur par défaut est de 500 lignes.

Enregistrer

Cliquez sur **Enregistrer** pour enregistrer tous les paramètres configurés. Le message de confirmation **Le profil de paramètres a été modifié** s'affiche alors dans le haut de la page. Tous les utilisateurs se connectant à la console du technicien d'assistance après que vous avez enregistré un nouveau profil recevront les nouveaux paramètres en tant que paramètres par défaut.

Appliquer les paramètres Console du technicien d'assistance

Appliquer maintenant

Pour appliquer les paramètres par défaut à l'ensemble de votre base d'utilisateurs, cliquez sur **Appliquer maintenant**. Le message de confirmation « **Le profil de paramètres a été appliqué.** » s'affiche alors dans le haut de la page.

Suite à l'application de nouveaux paramètres pour votre base d'utilisateurs, ceux-ci recevront une alerte de confirmation lors de leur première connexion à la console du technicien d'assistance après que vous avez appliqué les paramètres. Cette alerte leur indique que leurs paramètres ont été modifiés et leur permet uniquement d'accuser réception de l'alerte ou d'ouvrir leur fenêtre de paramètres de console du technicien d'assistance pour voir les changements.

Liens personnalisés : ajouter des raccourcis d'URL à la Console du technicien d'assistance

Console du technicien d'assistance | **Liens personnalisés**

Liens personnalisés

Créer des liens vers des sites auxquels vos utilisateurs peuvent accéder lors des sessions. Ceux-ci peuvent être, par exemple, un lien vers une base de connaissances pouvant faire l'objet d'une recherche, pour donner aux utilisateurs l'opportunité de rechercher une solution au problème du client, ou un système de gestion de la relation client (GRC) avec des fonctions de réaffectation. Dans ce cas, le lien peut ouvrir le système GRC sur une page où l'utilisateur peut remplir un formulaire de réaffectation pour une équipe qui n'utilise pas BeyondTrust.

Les liens créés ici deviennent disponibles par le bouton **Liens** de la console du technicien d'assistance.

Ajouter, modifier, supprimer

Créer un nouveau lien, modifier ou supprimer un lien existant.

Ajouter ou modifier un lien personnalisé

Nom

Créez un nom unique permettant d'identifier ce lien.

URL

Ajoutez l'URL vers laquelle ce lien personnalisé doit renvoyer. Utilisez les macros répertoriées sous ce champ dans la page /login pour personnaliser le texte selon vos besoins.

> *Pour plus d'informations, veuillez consulter la section Vue d'ensemble des sessions d'assistance technique et outils à l'adresse https://www.beyondtrust.com/docs/remote-support/getting-started/rep-console/support-session-overview.htm.*

Messages prédéfinis : création de messages pour la messagerie instantanée

Console du technicien d'assistance | **Messages prédéfinis**

Pour plus d'informations, veuillez consulter la section Messagerie instantanée avec un utilisateur lors d'une session à l'adresse https://www.beyondtrust.com/docs/remote-support/getting-started/rep-console/chat.htm.

Messages prédéfinis

Vous pouvez créer des messages prédéfinis à utiliser lors des sessions de messagerie instantanée. L'utilisation de messages prédéfinis permet de réduire le temps de réponse et aide à normaliser les communications entre les techniciens d'assistance et les utilisateurs. Vous pouvez filtrer votre affichage en sélectionnant une catégorie ou une équipe dans la liste déroulante située en haut de la page.

Ajouter, modifier, supprimer

Créer un nouveau message, modifier un message existant, ou supprimer un message existant.

Ajouter ou modifier les messages prédéfinis

Titre

Créez un nom unique permettant d'identifier ce message.Ce nom doit aider les techniciens d'assistance à trouver le message qu'ils souhaitent envoyer.

Message

Créez le texte qui apparaîtra dans la messagerie instantanée de l'utilisateur. Vous pouvez utiliser BBCode pour du formatage basique, comme l'ajout de caractères gras, de couleurs ou de liens hypertextes. Cliquez sur **Formatage de BBCode pris en charge** pour afficher une liste de codes et les applications qui en résultent.

***Astuce:** les messages doivent être relativement courts afin qu'ils puissent être lus sans faire défiler la fenêtre du client d'utilisateur. Ceci s'applique aux modes client natif et cliquer-pour-messagerie instantanée.*

Catégorie

Sélectionnez la catégorie dans laquelle répertorier cet objet.

Disponibilité d'équipe

Sélectionnez les équipes d'assistance technique qui doivent pouvoir utiliser cet élément.

Catégories de messages prédéfinis

Ajouter, modifier, supprimer

Créez une nouvelle catégorie, modifiez une catégorie existante, ou supprimez une catégorie existante.

Ajouter ou modifier une catégorie

Nom

Créez un nom unique permettant d'identifier cette catégorie.Ce nom doit aider les techniciens d'assistance à trouver le message qu'ils souhaitent envoyer.

Catégorie parent

Vous pouvez également sélectionner une catégorie parent pour contenir des catégories.

Catégories enfants

Voir les noms des catégories enfants et leurs liens.

Messages

Voir les liens vers les messages dans cette catégorie.

Scripts prédéfinis : création de scripts pour le partage d'écran ou les sessions d'interpréteur de commandes

Console du technicien d'assistance | **Scripts prédéfinis**

Scripts prédéfinis

Créez des scripts personnalisés à utiliser pour le partage d'écran et des sessions d'interpréteur de commandes. Le script s'affiche dans l'interface du partage d'écran ou de l'interpréteur de commandes lors de son exécution. L'exécution d'un script dans l'interface de partage d'écran affichera le script en cours d'exécution sur l'écran distant. Le script s'exécutera dans le contexte de l'utilisateur connecté lorsque la session n'est pas accrue, et il s'exécutera en tant que système local si la session est accrue. Vous pouvez filtrer votre affichage en sélectionnant une catégorie ou une équipe dans la liste déroulante située en haut de la page.

Pour plus d'informations, veuillez consulter la section Vue d'ensemble des sessions d'assistance technique et outils à l'adresse https://www.beyondtrust.com/docs/remote-support/getting-started/rep-console/support-session-overview.htm.

Pour plus d'informations, veuillez consulter la section Accès à l'interpréteur de commandes distant à l'adresse https://www.beyondtrust.com/docs/remote-support/getting-started/rep-console/command-shell.htm.

Ajouter, modifier, supprimer

Créer un nouveau script, modifier ou supprimer un script existant.

Ajouter ou modifier un script prédéfini

Nom du script

Créez un nom unique permettant d'identifier ce script. Ce nom doit aider les utilisateurs à trouver le script qu'ils souhaitent exécuter.

Description

Ajoutez une brève description pour résumer la fonction de ce script. Cette description s'affiche à l'invite pour confirmer que l'utilisateur souhaite exécuter le script sélectionné.

Séquence de commande

Écrivez la séquence de commandes. Les scripts doivent être rédigés au format ligne de commande, comme pour la rédaction d'un fichier de lot ou d'un script d'interpréteur. Veuillez noter que seule la dernière ligne du script peut être interactive ; vous ne pouvez pas mettre en pause le script ou demander une saisie au milieu du script.

Dans le script lui-même, référencez un fichier de ressources associé à l'aide de **%RESOURCE_FILE%** en veillant à insérer les guillemets. Remarque : la séquence de commande est sensible à la casse.

Vous pouvez accéder au répertoire temporaire du fichier de ressources à l'aide de **%RESOURCE_DIR%**. Lorsque vous exécutez un script avec un fichier de ressources associé, celui-ci est temporairement chargé sur l'ordinateur de l'utilisateur.

Disponibilité d'équipe

Sélectionnez les équipes d'assistance technique qui doivent pouvoir utiliser cet élément.

Catégories

Sélectionnez les catégories dans lesquelles répertorier cet objet.

Fichier de ressources

Vous pouvez sélectionner un fichier de ressources à associer à ce script.

Mode d'accroissement des droits

Choisissez si ce script doit être disponible à l'exécution en mode de droits accrus uniquement, en mode de droits non accrus, ou dans les deux cas.

Disponible en Partage d'écran en lecture seule, en tant qu'action spéciale

Si cette option est cochée, ce script peut être exécuté même lorsque l'utilisateur est uniquement autorisé à voir mais pas à contrôler l'ordinateur distant.Notez que lorsque l'utilisateur est en partage d'écran en mode affichage seul, le client reçoit une invite pour autoriser le lancement du script.

> ***Remarque :*** *si l'utilisateur est autorisé à utiliser des scripts prédéfinis, tous les scripts prédéfinis sont disponibles en partage d'écran en contrôle total, que l'option soit cochée ou pas.*

> *Pour plus d'informations, veuillez consulter la section Partage d'écran avec l'utilisateur distant à des fins de consultation et de contrôle à l'adresse https://www.beyondtrust.com/docs/remote-support/getting-started/rep-console/screen-sharing.htm.*

Catégories

Ajouter une catégorie, supprimer

Créer une nouvelle catégorie ou supprimer une catégorie existante.

Ressources

Choisir et transférer une ressource

Ajoutez les fichiers de ressources auxquels vous souhaitez avoir accès dans vos scripts. La taille de fichier maximale autorisée est de 250 Mo, avec un espace de stockage maximum de 1 Go.

Supprimer

Supprimez un fichier de ressources existant.

Actions spéciales : création d'actions spéciales personnalisées

Console du technicien d'assistance | **Actions spéciales**

Pour plus d'informations, veuillez consulter la section Partage d'écran avec l'utilisateur distant à des fins de consultation et de contrôle à l'adresse https://www.beyondtrust.com/docs/remote-support/getting-started/rep-console/screen-sharing.htm.

Actions spéciales

Créer des actions spéciales personnalisées afin d'accélérer vos processus. Notez qu'il est possible de créer des actions spéciales personnalisées pour les systèmes Windows, Mac et Linux.

Ajouter, modifier, supprimer

Créer une nouvelle action, modifier une action existante ou supprimer une action existante.

Ajouter ou modifier une action spéciale

Nom de l'action

Créez un nom unique permettant d'identifier cette action. Au cours d'une session, un utilisateur peut voir ce nom dans le menu déroulant d'actions spéciales.

Commande

Dans le champ **Commande**, entrez le chemin d'accès complet de l'application à exécuter. N'utilisez pas de guillemets, le système les ajoute automatiquement. Les systèmes Windows peuvent utiliser les macros prédéfinies. Si la commande n'est pas trouvable sur le système distant, cette action spéciale personnalisée n'apparaîtra pas dans la liste d'actions spéciales de l'utilisateur.

Arguments

Si la commande accepte les arguments de ligne de commande, vous pouvez alors en spécifier. Si nécessaire, vous pouvez utiliser des guillemets pour les arguments, et les arguments des systèmes Windows peuvent utiliser les macros prédéfinies.

Pour plus d'informations sur les arguments Windows, recherchez « commutateurs de ligne de commande » sur le site Web docs.microsoft.com/fr-fr/.

Confirmer

Si vous cochez la case **Confirmer**, les utilisateurs seront invités à confirmer qu'ils veulent exécuter cette action spéciale avant qu'elle se lance. Dans le cas contraire, la sélection de cette action spéciale personnalisée dans le menu au cours d'une session entraîne son exécution immédiate.

Exécuter avec des droits accrus

Cocher cette option permet de n'afficher l'action spéciale que lorsque le client d'utilisateur s'exécute avec des droits accrus. Lorsque vous exécutez une action personnalisée avec des droits accrus, vous serez invité à l'exécuter en tant qu'utilisateur système ou à fournir les informations d'authentification d'un autre compte valide du système distant.

Paramètres des actions spéciales

Afficher les actions spéciales préexistantes

Si vous souhaitez activer les actions spéciales par défaut fournies par BeyondTrust, cochez la case **Afficher les actions spéciales préexistantes**. Si vous ne souhaitez activer que vos actions spéciales personnalisées, décochez-la.

> ***Remarque :*** *les actions spéciales* ***Sécurité de Windows (Ctrl-Alt-Suppr)*** *et* ***Options de contrôle de l'alimentation*** *ne peuvent pas être désactivées. Notez également que le fait de désactiver les actions spéciales préexistantes ne désactive pas les actions spéciales définies par défaut pour les appareils mobiles.*

Utilisateurs et sécurité

Utilisateurs : ajout d'autorisations utilisateur pour un technicien d'assistance ou un administrateur

Comptes utilisateurs

Affichez les informations sur tous les utilisateurs qui ont accès à votre Serveur d'accès à distance sécurisé, y compris les utilisateurs locaux et ceux qui y ont accès par l'intégration du fournisseur de sécurité.

Ajouter, modifier, supprimer

Créer un nouveau compte, modifier un compte existant, ou supprimer un compte existant. Vous ne pouvez pas supprimer votre propre compte.

Chercher des utilisateurs

Rechez un utilisateur spécifique selon les critères **Authentifié(e) la dernière fois en tant que**, **Nom affiché public**, **Nom affiché privé** et **Adresse e-mail**.

Fournisseur de sécurité

Sélectionnez le fournisseur de sécurité que vous souhaitez chercher.

Synchroniser

Synchronisez les utilisateurs et les groupes associés avec un fournisseur de sécurité externe. La synchronisation se produit automatiquement une fois par jour. Cliquer sur ce bouton force une synchronisation manuelle.

Choisir les colonnes visibles

Utilisez le menu déroulant pour sélectionner les colonnes à afficher.

Rapport sur les comptes utilisateur

Exportez des informations détaillées sur vos utilisateurs à des fins d'audit. Collectez des informations détaillées sur l'ensemble des utilisateurs, sur les utilisateurs d'un fournisseur de sécurité spécifique ou sur les utilisateurs locaux uniquement. Les informations collectées incluent les données affichées sous le bouton « Afficher les détails », ainsi que les appartenances et les autorisations des équipes et des règles de groupe.

Ajouter ou modifier un utilisateur

Après avoir effectué vos modifications, cliquez sur **Enregistrer** pour enregistrer vos modifications auprès de cet utilisateur.

Nom d'utilisateur

Identificateur unique servant à vous connecter.

Noms affichés

Le nom de l'utilisateur tel qu'il apparaît sur le site public, dans la messagerie instantanée, etc. Les utilisateurs peuvent utiliser un nom affiché public, pour les échanges avec les clients, et un nom affiché privé, pour toutes les communications internes.

Rang d'affichage

Saisissez un numéro d'identification unique ou laissez ce champ vide pour sélectionner automatiquement le numéro disponible suivant. Ce numéro affecte l'ordre dans lequel les utilisateurs sont répertoriés sur le site public.

Photo

Envoyez une photo qui sera utilisée comme avatar pour le technicien d'assistance et qui sera affichée dans la fenêtre de messagerie instantanée du client d'utilisateur et sur l'interface d'administration **/login**. L'image utilisée doit être au format .png ou .jpeg, ne pas faire plus d'un Mo et avoir des dimensions minimales de 80x80 pixels. Cliquez sur **Choisir une photo** pour sélectionner une image. Définissez les dimensions de l'image en utilisant le curseur et les boutons **Ajuster dans la boîte** et **Remplir toute la boîte**. Une fois satisfait du résultat, cliquez sur **Rogner** pour l'utiliser, ou sur **Annuler** si vous ne voulez pas garder l'image que vous avez sélectionnée. Cliquez sur **Changer la photo** pour sélectionner une nouvelle image ou sur **Supprimer la photo** afin de supprimer l'avatar pour cet utilisateur.

La photo peut également être changée ou supprimée depuis la page **/login > Mon compte**.

> *Pour plus d'informations, veuillez visiter Client d'utilisateur : Interface de Session d'assistance technique à l'adresse https://www.beyondtrust.com/docs/remote-support/getting-started/customer-client/customer-support-interface.htm.*

Adresse e-mail

Définissez une adresse e-mail où envoyer les notifications, comme les réinitialisations de mot de passe ou le mode Disponibilité étendue.

Mot de passe

Le mot de passe utilisé avec le nom d'utilisateur pour la connexion. Vous pouvez définir le mot de passe de votre choix, tant que la chaîne reste conforme à la règle définie sur la page **/login > Gestion > Sécurité**.

Doit changer son mot de passe lors de la prochaine connexion

Si cette option est sélectionnée, l'utilisateur doit réinitialiser son mot de passe lors de sa prochaine connexion.

Le mot de passe n'expire jamais

Si cette option est sélectionnée, le mot de passe n'expire jamais.

Date d'expiration du mot de passe

Avec ceci, le mot de passe expirera à une date donnée.

Langue d'e-mail préférée

Si plus d'une langue est activée sur ce site, sélectionnez la langue dans laquelle envoyer les e-mails.

Paramètres du compte

Authentification à deux facteurs : Connexion avec une appli d'authentification :

Choisissez si l'utilisateur doit impérativement utiliser une appli d'authentification ou si le choix lui est laissé (réglage par défaut). Si cette option est définie sur **Obligatoire**, la prochaine fois que l'utilisateur tentera de se connecter à l'interface d'administration ou à la console du technicien d'assistance, un écran s'affichera pour demander qu'il active l'authentification à deux facteurs.

> *Pour plus d'informations sur l'authentification à deux facteurs, veuillez consulter Comment utiliser l'authentification à deux facteurs avec Remote Support BeyondTrust à l'adresse www.beyondtrust.com/docs/remote-support/how-to/2-factor-authentication/.*

Le compte n'expire jamais

Lorsque cette option est sélectionnée, le compte n'expire jamais.

Date d'expiration du compte

Avec ceci, le compte expirera à une date donnée.

Compte désactivé

Désactive le compte pour que l'utilisateur ne puisse plus se connecter. Une désactivation ne supprime PAS le compte.

Autorisé à modifier ses noms affichés

Permet aux utilisateurs de changer leurs noms affichés.

Autorisé à modifier sa photo

Permet aux utilisateurs de changer la photo de leur avatar, qui s'affiche sur l'interface d'administration **/login** et dans la fenêtre de messagerie instantanée du client d'utilisateur.

Autorisé à apparaître sur le site public

Affiche le nom de l'utilisateur sur tous les sites publics sur lesquels la liste des techniciens d'assistance est activée.

Commentaires

Ajoutez des commentaires pour identifier la fonction de ce compte.

Autorisations générales

Administration

Administrateur

Accorde des droits d'administration complets à l'utilisateur.

Autorisé à administrer Vault

Permet à l'utilisateur de gérer tous les aspects de l'add-on Vault de BeyondTrust.

Autorisé à définir les mots de passe

Permet à l'utilisateur de définir des mots de passe et de débloquer des comptes pour les utilisateurs locaux ne disposant pas de droits d'administrateur.

Autorisé à modifier les Jumpoints

Permet à l'utilisateur de créer ou de modifier des Jumpoints. Cette option n'affecte pas la capacité de l'utilisateur à accéder à des ordinateurs distants via un Jumpoint, qui est configurée par Jumpoint ou règle de groupe.

Autorisé à modifier le site public

Permet à l'utilisateur de créer et de modifier les configurations du site public, de modifier les modèles HTML, d'afficher l'interface de traduction, etc.

Autorisé à modifier les annonces aux utilisateurs

Permet aux techniciens d'assistance de créer et de modifier des messages utilisés pour notifier les utilisateurs, lorsqu'ils demandent une assistance technique, en cas d'interruptions informatiques à grand impact.

Autorisé à modifier le magasin de fichiers

Permet à l'utilisateur d'ajouter ou de supprimer des fichiers depuis le magasin de fichiers.

Autorisé à modifier les messages prédéfinis

Permet à l'utilisateur de créer ou de modifier des messages de messagerie instantanée prédéfinis.

Autorisé à modifier les équipes d'assistance technique

Permet à l'utilisateur de créer ou de modifier des équipes d'assistance technique.

Autorisé à modifier les groupes de Jump

Permet à l'utilisateur de créer ou de modifier les groupe de Jump.

Autorisé à modifier les problèmes

Permet à l'utilisateur de créer et de modifier des problèmes.

Autorisé à modifier les compétences

Permet à l'utilisateur de créer et de modifier des compétences.

Autorisé à modifier les profils Bouton assistance technique

Permet à l'utilisateur de personnaliser les profils de Bouton assistance technique.

Autorisé à modifier les scripts prédéfinis

Permet à l'utilisateur de créer ou de modifier des scripts prédéfinis en vue de les utiliser dans des sessions de partage d'écran ou d'interpréteur de commandes.

Autorisé à modifier les liens de technicien d'assistance personnalisés

Permet à l'utilisateur de créer ou de modifier des liens personnalisés.

Autorisé à modifier les parrains d'accès

Permet à l'utilisateur de créer ou de modifier des équipes de parrains d'accès.

Autorisé à modifier les profils iOS

Permet à l'utilisateur de créer, modifier et envoyer du contenu d'un profil Apple iOS pour le distribuer aux utilisateurs d'appareils iOS.

Rapport en cours

Autorisé à consulter les rapports : Session d'assistance technique

Permet à l'utilisateur d'établir des rapports sur l'activité de session d'assistance technique, en visualisant uniquement les sessions pour lesquelles il était le technicien d'assistance principal, les sessions où l'une de ses équipes était l'équipe principale ou l'un des membres de son équipe était le technicien d'assistance principal, ou toutes les sessions.

Autorisé à voir les enregistrements de session d'assistance technique

Permet à l'utilisateur d'afficher les enregistrements vidéo des sessions de partage d'écran, des sessions Montrer mon écran et des sessions d'interpréteur de commandes.

:Autorisé à consulter les rapports sur l'utilisation des licences

Permet à l'utilisateur d'établir des rapports sur l'utilisation des licences BeyondTrust.

Autorisé à consulter les rapports Vault

Permet à l'utilisateur de lancer des rapports sur l'activité de Vault, de voir toutes les données d'événement ou seulement ses propres données.

Autorisé à consulter les rapports sur les sessions de présentation

Permet à l'utilisateur d'établir des rapports sur l'activité de présentation, en visualisant uniquement les présentations dans lesquelles il était le présentateur, un autre membre de son équipe était le présentateur, ou toutes les présentations.

Accès API

Autorisé à utiliser les rapports API

Permet d'utiliser les informations d'authentification de l'utilisateur pour extraire des rapports XML via l'API.

Pour plus d'informations, consultez le guide de l'API de rapport à l'adresse https://www.beyondtrust.com/docs/remote-support/how-to/integrations/api/reporting/index.htm.

***Remarque :** il est préférable d'utiliser les comptes API créés dans **Gestion > Configuration de l'API**.*

Autorisé à utiliser les API de commande

Permet d'utiliser les informations d'authentification de l'utilisateur pour exécuter des commandes via l'API.

Pour plus d'informations, consultez le guide de l'API de commande à l'adresse https://www.beyondtrust.com/docs/remote-support/how-to/integrations/api/command/index.htm.

***Remarque :** il est préférable d'utiliser les comptes API créés dans **Gestion > Configuration de l'API**.*

Autorisé à utiliser l'API d'état en temps réel

Permet d'utiliser les informations d'authentification de l'utilisateur pour extraire des données en utilisant l'API d'état en temps réel.

Pour plus d'informations, veuillez consulter la section API d'état en temps réel à l'adresse https://www.beyondtrust.com/docs/remote-support/how-to/integrations/api/real-time-state/index.htm.

Autorisations du technicien d'assistance

Autorisé à fournir une assistance technique à distance

Permet à l'utilisateur d'utiliser la console du technicien d'assistance pour exécuter une session d'assistance technique. Si l'assistance technique est activée, les options appartenant à l'assistance à distance seront également disponibles. Désactivez ce paramètre pour les utilisateurs uniquement autorisés à effectuer des présentations.

Gestion de session

Autorisé à générer des clés de session pour toute session d'assistance technique au sein de la console du technicien d'assistance

Permet à l'utilisateur de générer des clés de session en vue d'autoriser les utilisateurs à démarrer des sessions directement avec lui.

> *Pour plus d'informations, veuillez consulter Génération d'une clé de session en vue de démarrer une session d'assistance technique à l'adresse https://www.beyondtrust.com/docs/remote-support/getting-started/rep-console/session-keys.htm.*

Autorisé à générer des clés d'accès pour envoyer des profils iOS

Permet à l'utilisateur de générer des clés d'accès pour offrir du contenu iOS aux utilisateurs d'appareils iOS.

> *Pour plus d'informations, veuillez consulter Génération d'une clé d'accès au profil Apple iOS à l'adresse https://www.beyondtrust.com/docs/remote-support/getting-started/rep-console/apple-ios-access-key-management-interface.htm.*

Autorisé à accepter manuellement des sessions d'une file d'attente d'équipe

Permet à l'utilisateur de sélectionner et de démarrer des sessions qui se trouvent dans l'une des files d'attente de son équipe.

> *Pour plus d'informations, veuillez consulter Acceptation d'une session pour démarrer l'assistance technique à l'adresse https://www.beyondtrust.com/docs/remote-support/getting-started/rep-console/accepting-a-session.htm.*

Autorisé à transférer les sessions aux équipes auxquelles il n'appartient pas

Permet à l'utilisateur de transférer des sessions vers d'autres équipes que la sienne. Si elle est désactivée, l'interaction d'utilisateur est limitée aux équipes qui lui ont été attribuées.

> *Pour plus d'informations, veuillez consulter la section Vue d'ensemble des sessions d'assistance technique et outils à l'adresse https://www.beyondtrust.com/docs/remote-support/getting-started/rep-console/support-session-overview.htm.*

Autorisé à partager les sessions avec des équipes auxquelles il n'appartient pas

Permet à l'utilisateur d'inviter un ensemble moins limité d'utilisateurs pour partager des sessions, pas seulement des membres de son équipe. Combinée à la permission de disponibilité étendue, cette permission développe les capacités de partage de session.

> *Pour plus d'informations, veuillez consulter la section Vue d'ensemble des sessions d'assistance technique et outils à l'adresse https://www.beyondtrust.com/docs/remote-support/getting-started/rep-console/support-session-overview.htm.*

Autorisé à inviter des techniciens service client externes

Permet à l'utilisateur d'inviter un utilisateur tiers à participer à une session d'assistance technique de manière ponctuelle.

> *Pour plus d'informations, veuillez consulter la section Inviter un technicien d'assistance externe à rejoindre une session à l'adresse https://www.beyondtrust.com/docs/remote-support/getting-started/rep-console/rep-invite.htm.*

Autorisé à utiliser la fonctionnalité Obtenir session suivante

Permet à l'utilisateur de prendre en charge la plus ancienne session de toutes ses équipes placée dans la file d'attente, en cliquant simplement sur un bouton.

> *Pour plus d'informations, veuillez consulter Acceptation d'une session pour démarrer l'assistance technique à l'adresse https://www.beyondtrust.com/docs/remote-support/getting-started/rep-console/accepting-a-session.htm.*

Autorisé à activer le mode disponibilité étendue

Permet à l'utilisateur de recevoir des invitations par e-mail de la part d'autres utilisateurs demandant de partager une session, même lorsqu'il n'est pas connecté à la console du technicien d'assistance.

> *Pour plus d'informations, consultez la section Utiliser la disponibilité étendue pour rester accessible lorsque vous n'êtes pas connecté à l'adresse https://www.beyondtrust.com/docs/remote-support/getting-started/rep-console/extended-availability.htm.*

Autorisé à modifier la clé externe

Permet à l'utilisateur de modifier la clé externe depuis le volet d'informations d'une session dans la console du technicien d'assistance.

> *Pour plus d'informations, veuillez consulter la section Vue d'ensemble des sessions d'assistance technique et outils à l'adresse https://www.beyondtrust.com/docs/remote-support/getting-started/rep-console/support-session-overview.htm.*

Equilibrium

> *Pour plus d'informations, veuillez consulter Equilibrium pour l'acheminement automatique de session à l'adresse https://www.beyondtrust.com/docs/remote-support/how-to/equilibrium/index.htm.*

Autorisé à refuser les attributions de session

Permet au technicien d'assistance de se définir comme non disponible pour les sessions attribuées via Equilibrium.

Ne pas attribuer de sessions si le technicien d'assistance participe à au moins

Définit le nombre minimal de sessions auxquelles le technicien d'assistance doit assister avant que les sessions ne soient plus automatiquement attribuées via Equilibrium.

Ne pas attribuer de sessions si le technicien d'assistance est inactif depuis au moins

Définit la période minimale pendant laquelle le technicien d'assistance doit avoir été inactif pour que les sessions ne soient plus automatiquement attribuées via Equilibrium.

Partage d'écran entre techniciens d'assistance

Pour plus d'informations, veuillez consulter Partager votre écran avec un autre technicien d'assistance à l'adresse https://www.beyondtrust.com/docs/remote-support/getting-started/rep-console/representative-screensharing.htm.

Autorisé à montrer son écran aux autres techniciens d'assistance

Permet à l'utilisateur de partager son écran avec un autre utilisateur sans que l'utilisateur récepteur ait besoin de rejoindre une session. Cette option est disponible même si l'utilisateur n'est pas dans une session.

Autorisé à accorder le contrôle lorsqu'il montre son écran à d'autres techniciens d'assistance

Permet à l'utilisateur partageant son écran d'accorder le contrôle de son clavier et de sa souris à l'utilisateur regardant son écran.

Bouton assistance techniques

Pour plus d'informations, veuillez consulter la section Vue d'ensemble des sessions d'assistance technique et outils à l'adresse https://www.beyondtrust.com/docs/remote-support/getting-started/rep-console/support-session-overview.htm.

Autorisé à déployer et gérer tout Bouton assistance technique dans une file d'attente personnelle

Permet à l'utilisateur de déployer et de gérer tout Bouton assistance technique personnel. Ce paramètre affecte le déploiement de tout Bouton assistance technique depuis l'interface Web et la console du technicien d'assistance. Pour pouvoir déployer un Bouton assistance technique à partir d'une session, l'autorisation de session **Déploiement de Bouton assistance technique** doit également être activée.

Autorisé à gérer tout Bouton assistance technique d'équipe

Autorise l'utilisateur à modifier tout Bouton assistance technique déployé dans les équipes dont il fait partie. Si l'utilisateur est le chef ou le responsable de l'équipe, il peut aussi modifier tout Bouton assistance technique personnel de n'importe quel membre.

Pour plus d'informations, veuillez consulter Gestion de Bouton assistance technique à l'adresse https://www.beyondtrust.com/docs/remote-support/getting-started/rep-console/support-button-management-interface.htm.

Autorisé à modifier le portail public associé à tout Bouton assistance technique

Permet à l'utilisateur de définir le portail public qu'un Bouton assistance technique doit utiliser pour se connecter. Dans la mesure où les portails publics peuvent faire l'objet de règles de session, toute modification du portail peut affecter les autorisations associées à la session.

Autorisé à déployer chaque Bouton assistance technique d'équipe

Permet à l'utilisateur de déployer un Bouton assistance technique d'équipe pour les équipes dont il fait partie. Ce paramètre affecte le déploiement de tout Bouton assistance technique depuis l'interface Web et la console du technicien d'assistance. Pour pouvoir déployer un Bouton assistance technique à partir d'une session, l'autorisation de session **Déploiement de Bouton assistance technique** doit également être activée.

Technologie Jump

Méthodes de Jump autorisées

Permet à l'utilisateur d'effectuer un Jump vers des ordinateurs en utilisant les méthodes de **Jump Clients**, **Jump local**, **VNC local**, **RDP local**, **Jump distant**, **VNC distant**, **RDP distant**, **Shell Jump** et/ou **Intel vPro**.

Rôles d'élément de Jump

Le rôle d'élément de Jump est un ensemble prédéfini d'autorisations relatives à la gestion et à l'utilisation d'un élément de Jump. Pour chaque option, cliquez sur le bouton **Modifier** pour ouvrir le rôle d'élément de Jump dans un nouvel onglet.

Le rôle **Par défaut** n'est utilisé que lorsque **Utiliser les paramètres par défaut de l'utilisateur** est défini pour cet utilisateur dans un groupe de Jump.

Le rôle **Personnel** ne s'applique qu'aux éléments de Jump attachés à la liste personnelle d'éléments de Jump d'un utilisateur.

Le rôle **Équipe** ne s'applique qu'aux éléments de Jump attachés à la liste personnelle d'éléments de Jump d'un membre de l'équipe doté d'un rôle inférieur. Ainsi, un chef d'équipe peut visualiser les éléments de Jump d'un responsable ou d'un membre de son équipe, et un responsable d'équipe peut visualiser les éléments de Jump personnels d'un membre de son équipe.

Le rôle **Système** s'applique au reste des éléments de Jump du système. Pour la plupart des utilisateurs, ce rôle est en principe défini sur **Aucun accès**. S'il est défini sur une autre option, l'utilisateur est ajouté à des groupes de Jump auxquels il ne devrait pas être assigné, et, dans la console du technicien d'assistance, il est en mesure de visualiser la liste personnelle d'éléments de Jump de membres n'appartenant pas à son équipe.

> *Pour plus d'informations, veuillez consulter Utiliser les rôles d'éléments de Jump pour créer des groupes d'autorisations pour les Jump Clients à l'adresse https://www.beyondtrust.com/docs/remote-support/how-to/jump-clients/jump-item-roles.htm.*

Présentation

Autorisé à effectuer des présentations

Permet au technicien d'assistance d'effectuer des présentations à l'intention d'un ou de plusieurs participants.

> *Pour plus d'informations, veuillez consulter Réaliser une présentation pour des participants distants à l'adresse https://www.beyondtrust.com/docs/remote-support/getting-started/rep-console/presentation.htm.*

Autorisé à accorder le contrôle à un participant de la présentation

Permet au technicien d'assistance d'accorder le contrôle de son ordinateur à un participant au cours d'une présentation. Ce paramètre affecte uniquement les présentations et n'a aucun impact sur la fonction Montrer mon écran d'une session d'assistance technique. Un seul participant à la fois peut avoir le contrôle. Le technicien d'assistance conserve le contrôle du remplacement.

> *Pour plus d'informations, veuillez consulter la section Client de participant à une présentation : Rejoindre une présentation à l'adresse https://www.beyondtrust.com/docs/remote-support/getting-started/customer-client/customer-presentation-interface.htm.*

Console du technicien d'assistance

Délai d'inactivité

Définissez le délai pendant lequel le technicien d'assistance peut être inactif avant d'être déconnecté de la console du technicien d'assistance. Cette autorisation peut utiliser le paramètre défini pour le site ou peut remplacer ce paramètre.

Autorisations relatives aux sessions autonomes et non autonomes

Règle de session

Définissez les règles de demande et d'autorisation devant s'appliquer aux sessions de cet utilisateur. Sélectionnez une règle de session existante ou définissez des autorisations personnalisées pour cet utilisateur. Notez que l'option **Non défini** entraîne l'utilisation de la règle globale par défaut. Ces autorisations peuvent être remplacées par une règle de niveau supérieur.

Utiliser les mêmes autorisations pour les sessions non autonomes

Pour utiliser les mêmes autorisations pour les sessions autonomes et les sessions non autonomes, cochez la case **Utiliser les mêmes autorisations pour les sessions non autonomes**. Décochez cette case si vous souhaitez définir des autorisations distinctes pour les sessions autonomes et les sessions non autonomes. Vous pouvez également copier les autorisations d'un type de session à l'autre.

Description

Affichez la description d'une règle de permission de session prédéfinie.

Demande d'outil d'assistance technique

> *Pour en savoir plus, veuillez consulter Client d'utilisateur : Interface de session d'assistance technique à l'adresse https://www.beyondtrust.com/docs/remote-support/getting-started/customer-client/customer-support-interface.htm.*

Règles de demande

Vous pouvez choisir de demander à l'utilisateur l'autorisation d'utiliser les fonctions d'assistance technique ci-après. Sélectionnez **Aucune demande** pour ne jamais envoyer de demande, **Toujours demander** pour toujours envoyer une demande ou **Demander pour certains outils** pour choisir les autorisations pour lesquelles envoyer une demande. Lorsque l'option **Demander pour certains outils** est sélectionnée, l'option **Demander l'accord de l'utilisateur** apparaît en dessous de chaque outil, avec les choix **Jamais** et **Toujours**. En cas de sélection de **Non défini**, cette option est définie par la règle de priorité inférieure suivante. Ce réglage peut être remplacé par une règle de priorité supérieure.

Autorisé à demander une fois

Si l'option **Partage d'écran** est définie sur **Voir et contrôler** et que l'envoi de demandes est activé, cette option est disponible. Cochez cette case pour permettre à la fonction de partage d'écran d'accéder à tous les outils au cours de la session, sans demande supplémentaire.

Options de demande

Définissez le délai d'attente de réponse à une demande avant l'envoi de la réponse par défaut **Refuser** ou **Autoriser**. En cas de sélection de **Non défini**, cette option est définie par la règle de priorité inférieure suivante. Ce réglage peut être remplacé par une règle de priorité supérieure.

Partage d'écran

Règles de partage d'écran

Permet à l'utilisateur de voir ou de contrôler l'écran distant. En cas de sélection de **Non défini**, cette option est définie par la règle de priorité inférieure suivante. Ce réglage peut être remplacé par une règle de priorité supérieure.

> *Pour plus d'informations, veuillez consulter la section Partage d'écran avec l'utilisateur distant à des fins de consultation et de contrôle à l'adresse https://www.beyondtrust.com/docs/remote-support/getting-started/rep-console/screen-sharing.htm.*

Autorisé à montrer son écran à l'utilisateur

Permet à l'utilisateur de partager son écran avec le client au cours d'une session d'assistance technique.

> *Pour plus d'informations, veuillez consulter la section Montrer mon écran : Inversion du partage d'écran à l'adresse https://www.beyondtrust.com/docs/remote-support/getting-started/customer-client/show-my-screen.htm.*

Restrictions d'utilisateur autorisées

Définissez si l'utilisateur peut interrompre l'entrée souris et clavier du système distant. L'utilisateur peut aussi empêcher l'affichage du bureau distant.

> *Pour plus d'informations, veuillez consulter la section Interaction client restreinte : Écran de confidentialité et désactivation de l'entrée de l'utilisateur distant à l'adresse https://www.beyondtrust.com/docs/remote-support/getting-started/customer-client/privacy-screen.htm.*

Comportement de demande de partage d'applications

Déterminez si une demande de partage d'écran ne doit jamais ou toujours faire l'objet d'une demande auprès du client pour sélectionner les applications à partager, ou si l'utilisateur peut choisir de faire une demande de partage d'applications ou non. Sélectionner **Toujours** ou **Décision du technicien d'assistance** vous permet aussi de prédéfinir les restrictions de partage d'application.

> *Pour plus d'informations, veuillez consulter la section Partage d'application : Restriction des éléments visibles par le technicien d'assistance à l'adresse https://www.beyondtrust.com/docs/remote-support/getting-started/customer-client/application-sharing.htm.*

Sens de synchronisation du presse-papiers

Sélectionnez la manière dont le contenu du presse-papiers circule entre les techniciens d'assistance et les utilisateurs finaux. Les options sont :

- **Non autorisé :** Le technicien d'assistance n'est pas autorisé à utiliser le presse-papiers, aucune icône de presse-papiers ne s'affiche dans la console du technicien d'assistance et les commandes couper-coller ne fonctionnent pas.
- **Autorisé du technicien d'assistance vers l'utilisateur :** Le technicien d'assistance peut envoyer le contenu du presse-papiers au client, mais ne peut pas le coller à partir du presse-papiers de l'utilisateur final. Seule l'icône Envoyer le presse-papiers s'affiche dans la console du technicien d'assistance.
- **Envoyer dans les deux sens :** Le contenu du presse-papiers peut circuler dans les deux sens. Les icônes du presse-papiers Envoyer et Obtenir s'affichent dans la console du technicien d'assistance.

> *Pour plus d'informations sur le Mode de synchronisation du presse-papiers, veuillez consulter « Sécurité : Gestion des paramètres de sécurité », page 205 de sécurité.*

Partage de navigateur

Règles de partage de navigateur

Permet à l'utilisateur de consulter la même page Web que le client regarde, sans avoir le contrôle et sans voir d'autres applications. En cas de sélection de **Non défini**, cette option est définie par la règle de priorité inférieure suivante. Ce réglage peut être remplacé par une règle de priorité supérieure.

> *Pour plus d'informations, veuillez consulter la section Partage d'écran avec l'utilisateur distant à des fins de consultation et de contrôle à l'adresse https://www.beyondtrust.com/docs/remote-support/getting-started/rep-console/screen-sharing.htm.*

Annotations

Règles d'annotation

Permet à l'utilisateur d'utiliser les outils d'annotation pour dessiner sur l'écran du système distant. En cas de sélection de **Non défini**, cette option est définie par la règle de priorité inférieure suivante. Ce réglage peut être remplacé par une règle de priorité supérieure.

Pour plus d'informations, veuillez consulter la section Utiliser les annotations pour dessiner sur l'écran distant à l'adresse https://www.beyondtrust.com/docs/remote-support/getting-started/rep-console/annotations.htm.

Transfert de fichiers

Règles de transfert de fichiers

Permet à l'utilisateur d'envoyer des fichiers vers le système distant, de télécharger des fichiers depuis le système distant, ou les deux. En cas de sélection de **Non défini**, cette option est définie par la règle de priorité inférieure suivante. Ce réglage peut être remplacé par une règle de priorité supérieure.

Chemins accessibles sur le système de fichiers de l'utilisateur

Permettre à l'utilisateur de transférer des fichiers de et vers n'importe quel répertoire sur le système distant ou uniquement les répertoires spécifiés.

Chemins accessibles sur le système de fichiers du technicien d'assistance

Permettre à l'utilisateur de transférer des fichiers de et vers n'importe quel répertoire sur son système local ou uniquement les répertoires spécifiés.

Pour plus d'informations, veuillez consulter la section Transfert de fichiers vers et depuis le système distant à l'adresse https://www.beyondtrust.com/docs/remote-support/getting-started/rep-console/file-transfer.htm.

Interpréteur de commandes

Règles de l'interpréteur de commandes

Permet à l'utilisateur de saisir des commandes sur l'ordinateur distant par l'intermédiaire d'une interface en ligne de commande virtuelle. En cas de sélection de **Non défini**, cette option est définie par la règle de priorité inférieure suivante. Ce réglage peut être remplacé par une règle de priorité supérieure.

***Remarque :** l'accès à l'interpréteur de commandes ne peut pas être restreint lors de sessions de Shell Jump.*

Pour plus d'informations, veuillez consulter la section Accès à l'interpréteur de commandes distant à l'adresse https://www.beyondtrust.com/docs/remote-support/getting-started/rep-console/command-shell.htm.

Informations système

Règles relatives aux informations système

Permet à l'utilisateur de consulter les informations système de l'ordinateur distant. En cas de sélection de **Non défini**, cette option est définie par la règle de priorité inférieure suivante. Ce réglage peut être remplacé par une règle de priorité supérieure.

Autorisé à utiliser les actions relatives aux informations système

Permet à l'utilisateur d'interagir avec les processus et les programmes sur le système distant sans avoir recours au partage d'écran. Le technicien d'assistance peut ainsi désinstaller des programmes, supprimer des processus ou encore démarrer, arrêter, mettre en pause, reprendre et redémarrer des services.

> *Pour plus d'informations, veuillez consulter la section Consulter les informations du système distant à l'adresse https://www.beyondtrust.com/docs/remote-support/getting-started/rep-console/system-info.htm.*

Accès au registre

Règles d'accès au registre

Permet à l'utilisateur d'agir sur le registre d'un système Windows distant sans avoir recours au partage d'écran. Le technicien d'assistance peut ainsi afficher, ajouter, supprimer, modifier, rechercher et importer/exporter des clés.

> *Pour plus d'informations, veuillez consulter la section Accès à l'éditeur de registre distant à l'adresse https://www.beyondtrust.com/docs/remote-support/getting-started/rep-console/registry-editor.htm.*

Scripts prédéfinis

Règles de script prédéfini

Permet à l'utilisateur d'exécuter des scripts prédéfinis créés pour ses équipes. Notez que lorsque l'utilisateur est en partage d'écran en mode affichage seul, le client reçoit une invite pour autoriser le lancement du script.En cas de sélection de **Non défini**, cette option est définie par la règle de priorité inférieure suivante. Ce réglage peut être remplacé par une règle de priorité supérieure.

> *Pour plus d'informations, veuillez consulter la section Accès à l'interpréteur de commandes distant à l'adresse https://www.beyondtrust.com/docs/remote-support/getting-started/rep-console/command-shell.htm.*

Accroissement des droits

Règles d'accroissement des droits

Permet à l'utilisateur de tenter d'accroître les droits du client d'utilisateur pour s'exécuter avec des droits administratifs sur le système distant. En cas de sélection de **Non défini**, cette option est définie par la règle de priorité inférieure suivante. Ce réglage peut être

remplacé par une règle de priorité supérieure.

> *Pour plus d'informations, veuillez consulter la section Accroître le client à l'adresse https://www.beyondtrust.com/docs/remote-support/getting-started/rep-console/elevation.htm.*

Déploiement de Bouton assistance technique

Règles de déploiement de Bouton assistance technique

Permet à l'utilisateur de déployer ou de supprimer un Bouton assistance technique au cours d'une session. Les emplacements de déploiement possibles dépendent des paramètres de Bouton assistance technique ci-dessus. En cas de sélection de **Non défini**, cette option est définie par la règle de priorité inférieure suivante. Ce réglage peut être remplacé par une règle de priorité supérieure.

> *Pour plus d'informations, veuillez consulter la section Vue d'ensemble des sessions d'assistance technique et outils à l'adresse https://www.beyondtrust.com/docs/remote-support/getting-started/rep-console/support-session-overview.htm.*

Attachement/Détachement de Jump Clients

Règles d'attachement/détachement de Jump Clients

Permet à l'utilisateur d'attacher ou de détacher un Jump Client au cours d'une session. Les emplacements de déploiement possibles dépendent des paramètres de Jump Client précédents. En cas de sélection de **Non défini**, cette option est définie par la règle de priorité inférieure suivante. Ce réglage peut être remplacé par une règle de priorité supérieure.

> *Pour plus d'informations, veuillez consulter la section Vue d'ensemble des sessions d'assistance technique et outils à l'adresse https://www.beyondtrust.com/docs/remote-support/getting-started/rep-console/support-session-overview.htm.*

Messagerie instantanée

> *Pour plus d'informations, veuillez consulter la section Messagerie instantanée avec un utilisateur lors d'une session à l'adresse https://www.beyondtrust.com/docs/remote-support/getting-started/rep-console/chat.htm.*

Règles de messagerie instantanée

Permet à l'utilisateur de discuter avec le client distant. En cas de sélection de **Non défini**, cette option est définie par la règle de priorité inférieure suivante. Ce réglage peut être remplacé par une règle de priorité supérieure.

Autorisé à charger des URL dans le navigateur Web de l'utilisateur

Permet à l'utilisateur d'entrer une URL dans la zone de messagerie instantanée, puis de cliquer sur le bouton **Charger l'URL** pour ouvrir automatiquement un navigateur Web à cette adresse sur l'ordinateur distant.

Autorisé à envoyer des fichiers à l'aide de l'interface de messagerie instantanée

Permet à l'utilisateur d'envoyer des fichiers via l'interface de messagerie instantanée.

> *Pour en savoir plus, veuillez consulter Client d'utilisateur : Interface de session d'assistance technique à l'adresse https://www.beyondtrust.com/docs/remote-support/getting-started/customer-client/customer-support-interface.htm.*

Paramètres de disponibilité

Pool de licences d'assistance technique complète

Choisissez le pool de licences auquel ce technicien d'assistance doit appartenir. Lorsque ce technicien d'assistance se connecte à la console du technicien d'assistance, une licence est utilisée dans le pool de licences désigné. Si **Aucun** est sélectionné, le technicien d'assistance pourra se connecter à la console du technicien d'assistance seulement si une ou plusieurs licences non assignées à des pools de licences sont disponibles.

Compétences

Désigne les compétences assignées à cet utilisateur. Lorsque vous utilisez la correspondance de compétences pour Equilibrium, les sessions seront assignées à l'utilisateur le plus compétent pour traiter un problème en particulier.

> *Pour plus d'informations, veuillez consulter la section Attribuer des compétences à des techniciens d'assistance à l'adresse https://www.beyondtrust.com/docs/remote-support/how-to/equilibrium/assign-skills-rep.htm.*

Planning de connexion

Restreindre la connexion du technicien d'assistance selon le planning suivant

Définissez un planning afin de déterminer les périodes pendant lesquelles les utilisateurs peuvent se connecter à la console du technicien d'assistance. Définissez le fuseau horaire à utiliser pour ce planning, puis ajoutez une ou plusieurs entrées de planification. Pour chaque entrée, indiquez l'heure et la date de début ainsi que l'heure et la date de fin.

Par exemple, si la période définie commence à 8 h et se termine à 17 h, un utilisateur peut se connecter à n'importe quel moment au cours de cette période et peut continuer à travailler passée l'heure de fin. Il ne sera toutefois pas autorisé à se reconnecter après 17 h.

Forcer la déconnexion lorsque le planning ne permet pas l'ouverture d'une session

Si un contrôle d'accès plus strict est requis, cochez cette option. Ceci force la déconnexion de l'utilisateur à l'heure de fin définie. Dans ce cas, l'utilisateur reçoit des notifications récurrentes à partir de 15 minutes avant d'être déconnecté. Lorsque l'utilisateur est déconnecté, toutes les sessions possédées suivront les règles de récupération.

Comptes utilisateur pour réinitialisation des mots de passe : autoriser les techniciens d'assistance à gérer les mots de passe utilisateur

Utilisateurs et sécurité | **Utilisateurs**

Comptes utilisateurs

Les administrateurs peuvent déléguer, grâce à une autorisation d'utilisateur, la réinitialisation des mots de passe des utilisateurs locaux et des comptes d'utilisateurs bloqués à un autre utilisateur sans lui accorder les droits d'administrateur complets. Notez que les utilisateurs locaux peuvent tout de même réinitialiser leurs propres mots de passe.

Lorsqu'un utilisateur privilégié non administrateur accède à la page **Utilisateurs et sécurité > Utilisateurs** dans l'interface d'administration /login, il verra une version limitée de l'écran **Utilisateurs** contenant des liens **Modifier le mot de passe** pour les utilisateurs non administrateurs. Un utilisateur privilégié ne peut pas modifier ou supprimer des comptes d'utilisateur. Les utilisateurs privilégiés ne sont pas autorisés à réinitialiser les mots de passe des administrateurs ni les mots de passe des utilisateurs fournisseurs de sécurité.

> ***Remarque :*** *cela n'a aucune incidence sur l'interface utilisateur pour les administrateurs disposant de l'autorisation* ***Autorisé à définir les mots de passe****.*

Chercher des utilisateurs

Rechez un utilisateur spécifique selon les critères **Authentifié(e) la dernière fois en tant que**, **Nom affiché public**, **Nom affiché privé** et **Adresse e-mail**.

Choisir les colonnes visibles

Utilisez le menu déroulant pour sélectionner les colonnes à afficher.

Réinitialiser

Si un utilisateur échoue une ou plusieurs fois à se connecter, cliquez sur le bouton **Réinitialiser** à côté de son nom pour remettre le chiffre à 0.

Modifier le mot de passe

Changez le mot de passe pour un utilisateur non administrateur.

Modifier le mot de passe

Nom d'utilisateur

Identificateur unique servant à vous connecter. Ce champ ne peut pas être modifié.

Noms affichés

Le nom de l'utilisateur tel qu'il apparaît sur le site public, dans la messagerie instantanée, etc. Les utilisateurs peuvent utiliser un nom affiché public, pour les échanges avec les clients, et un nom affiché privé, pour toutes les communications internes. Ce champ ne peut pas être modifié.

Adresse e-mail

L'adresse e-mail à laquelle sont envoyées les notifications par e-mail, notamment les réinitialisations de mot de passe ou les alertes de mode disponibilité étendue. Ce champ ne peut pas être modifié.

Commentaires

Commentaires sur le compte. Ce champ ne peut pas être modifié.

Mot de passe

Le nouveau mot de passe à assigner à ce compte d'utilisateur. Vous pouvez définir le mot de passe de votre choix, tant que la chaîne reste conforme à la règle définie sur la page **/login > Gestion > Sécurité**.

Envoyer le lien de réinitialisation de mot de passe à l'utilisateur par e-mail

Envoyez un lien par e-mail à l'utilisateur pour réinitialiser le mot de passe de son compte. Cette fonction nécessite une configuration SMTP valide pour votre serveur, qui s'effectue sur la page **/login > Gestion > Configuration e-mail**.

Doit changer son mot de passe lors de la prochaine connexion

Si cette option est sélectionnée, l'utilisateur doit réinitialiser son mot de passe lors de sa prochaine connexion.

Invitation d'un technicien d'assistance : création de profils pour l'invitation de techniciens d'assistance externes à des sessions

E-mail d'invitation du technicien d'assistance

Avec l'invitation d'un technicien d'assistance, un utilisateur privilégié peut inviter un utilisateur externe à rejoindre une session de manière ponctuelle. L'e-mail d'invitation est envoyé aux techniciens d'assistance externes lorsque vous les invitez à rejoindre une session.

Sélectionnez un site public à modifier

Dans le menu déroulant en haut de la page, sélectionnez le site public pour lequel vous voulez modifier l'e-mail d'invitation du technicien d'assistance.

Objet

Personnalisez l'objet de cet e-mail. Vous pouvez traduire ce texte dans les langues que vous avez activées. Pour revenir au texte par défaut, supprimez le texte du champ puis enregistrez le champ vide.

Corps

Personnalisez le texte de cet e-mail. Utilisez les macros répertoriées sous ce champ dans la page /login pour personnaliser le texte selon vos besoins. Vous pouvez traduire ce texte dans les langues que vous avez activées. Pour revenir au texte par défaut, supprimez le texte du champ puis enregistrez le champ vide.

Pour plus d'informations, veuillez consulter la section Inviter un technicien d'assistance externe à rejoindre une session à l'adresse https://www.beyondtrust.com/docs/remote-support/getting-started/rep-console/rep-invite.htm.

Fournisseurs de sécurité : activer LDAP, Active Directory, RADIUS, Kerberos, SAML pour techniciens d'assistance et SAML pour portails publics

Fournisseurs de sécurité

Vous pouvez configurer votre Serveur d'accès à distance sécurisé pour qu'il authentifie des utilisateurs auprès de serveurs LDAP, RADIUS, Kerberos ou SAML existants et pour qu'il attribue des privilèges en fonction de la hiérarchie et des paramètres de groupe préexistants déjà spécifiés dans vos serveurs. Kerberos permet une authentification unique, tandis que RSA et d'autres mécanismes d'authentification à deux facteurs par RADIUS fournissent un niveau de sécurité supplémentaire.

Ajouter

Créez une nouvelle configuration de fournisseur de sécurité. Depuis la liste déroulante, sélectionnez LDAP, RADIUS, Kerberos, SAML pour techniciens d'assistance ou SAML pour portails publics.

Modifier l'ordre

Cliquez sur ce bouton pour déplacer les fournisseurs de sécurité afin de définir leur priorité. Vous pouvez déplacer des serveurs à l'intérieur d'une grappe ; les grappes peuvent être déplacées dans leur intégralité. Cliquez sur **Enregistrer l'ordre** pour que les changements de priorité prennent effet.

Synchroniser

Synchronisez les utilisateurs et les groupes associés avec un fournisseur de sécurité externe. La synchronisation se produit automatiquement une fois par jour. Cliquer sur ce bouton force une synchronisation manuelle.

Désactiver

Désactiver la connexion de ce fournisseur de sécurité. Ceci est utile pour les maintenances planifiées, lorsque vous voulez qu'un serveur soit hors ligne mais non effacé.

Afficher le journal

Affichez l'historique d'état pour la connexion d'un fournisseur de sécurité.

Modifier, supprimer

Modifier un fournisseur existant ou supprimer un fournisseur existant.

> ***Remarque :*** *si vous modifiez le fournisseur de sécurité local et sélectionnez une règle par défaut qui ne dispose pas d'autorisations d'administrateur, un message d'avertissement s'affiche. Assurez-vous que les autres utilisateurs disposent des autorisations d'administrateur avant de continuer.*

Dupliquer le nœud

Créez une copie d'une configuration de fournisseur de sécurité en cluster existante. Ceci sera ajouté en tant que nouveau nœud dans le même cluster.

Mettre à niveau vers le cluster

Mettez à niveau un fournisseur de sécurité sur un cluster de fournisseur de sécurité. Pour ajouter d'autres fournisseurs de sécurité à ce cluster, copiez un nœud existant.

Copier

Créez une copie d'une configuration de fournisseur de sécurité existante. Ceci sera ajouté comme fournisseur de sécurité de niveau principal et non pas comme faisant partie d'un cluster.

Ajouter ou modifier un fournisseur de sécurité : LDAP

Nom

Créez un nom unique permettant d'identifier ce fournisseur.

Activé

Si cette case est cochée, votre Serveur d'accès à distance sécurisé peut chercher ce fournisseur de sécurité lorsqu'un utilisateur tente de se connecter à la console du technicien d'assistance ou à **/login**. Si elle n'est pas cochée, le fournisseur ne sera pas recherché.

Authentification utilisateur

Cela permet à ce fournisseur d'être utilisé pour authentifier les utilisateurs. Si cette option est désactivée, ce fournisseur peut être utilisé uniquement pour rechercher des autorisations d'utilisateur dans des groupes.

Garder les informations d'utilisateur synchronisées avec le serveur LDAP

Les noms affichés sont définis d'après les **Paramètres de schéma d'utilisateur** définis ci-dessous. Si vous comptez synchroniser l'attribut de la photo d'un utilisateur, cette option doit être cochée.

Paramètres d'autorisation

Synchronisation : Activer le cache d'objet LDAP

Si ceci est coché, les objets LDAP visibles pour le serveur sont mis en cache et synchronisés toutes les nuits, ou manuellement si désiré. Lorsque cette option est utilisée, un nombre plus faible de connexions est établi avec le serveur LDAP pour des raisons administratives, ce qui peut potentiellement améliorer la vitesse et l'efficacité.

Si cette option est décochée, les changements apportés au serveur LDAP sont disponibles immédiatement, sans besoin de synchronisation. Cependant, lorsque vous apportez des changements aux règles d'utilisateur à travers l'interface d'administration, quelques connexions LDAP courtes peuvent avoir lieu si c'est nécessaire.

Pour les fournisseurs qui avaient le paramètre de synchronisation activé, désactiver l'option de synchronisation provoquera l'effacement de tous les enregistrements mis en cache qui ne sont pas en cours d'utilisation.

Rechercher des groupes

Choisissez d'utiliser ce fournisseur de sécurité uniquement pour l'authentification d'utilisateurs, seulement pour les recherches de groupes, ou pour les deux. **Authentification utilisateur** doit être sélectionné si vous souhaitez désactiver la recherche de groupe.

Règle de groupe par défaut *(Visible uniquement si l'authentification d'utilisateur est autorisée)*

Chaque utilisateur qui s'authentifie auprès d'un serveur externe doit être membre d'au moins une règle de groupe pour pouvoir s'authentifier sur votre Serveur d'accès à distance sécurisé, en se connectant sur l'interface /login ou sur la console du technicien d'assistance. Vous pouvez sélectionner une règle de groupe par défaut à appliquer à tous les utilisateurs autorisés à s'authentifier auprès du serveur configuré.

> ***Remarque :*** *si une règle par défaut est définie, alors n'importe quel utilisateur qui s'authentifie sur ce serveur peut potentiellement avoir accès au niveau de cette règle par défaut. Il est donc recommandé de définir le défaut sur une règle avec le minimum de privilèges, pour empêcher les utilisateurs d'obtenir des autorisations que vous ne souhaitez pas qu'ils aient.*

> ***Remarque :*** *si un utilisateur est dans une règle de groupe par défaut et qu'il est ensuite spécifiquement ajouté à une autre règle de groupe, les paramètres pour la règle spécifique prendront toujours le pas sur les paramètres par celle par défaut, même si la règle spécifique a une priorité plus basse que celle par défaut, et même si les paramètres de la règle par défaut n'autorisent pas le remplacement.*

Paramètres de connexion *(non visible pour les clusters)*

Nom de l'hôte

Saisissez le nom d'hôte du serveur sur lequel se trouve le magasin d'annuaire externe.

> ***Remarque :*** *si vous allez utiliser **LDAPS** ou **LDAP avec TLS**, le nom d'hôte doit correspondre au nom d'hôte utilisé dans le nom du sujet du certificat SSL public de votre serveur LDAP ou au composant DNS de son nom de sujet alternatif.*

Port

Spécifiez le port de votre serveur LDAP. Il s'agit généralement du port **389** pour LDAP ou du port **636** pour LDAPS. BeyondTrust permet également le catalogue global sur le port **3268** pour LDAP ou **3269** pour LDAPS.

Chiffrement

Sélectionnez le type de cryptage à utiliser lors de la communication avec le serveur LDAP. Pour des raisons de sécurité, **LDAPS** ou **LDAP avec TLS** est recommandé.

> ***Remarque :*** *le LDAP envoie et reçoit des données en texte clair depuis le serveur LDAP, ce qui peut exposer des informations de comptes utilisateurs confidentielles au reniflage de paquets. LDAPS, et LDAP avec un cryptage TLS, cryptent*

les données utilisateur lors de leur transfert ; ces méthodes sont donc recommandées, plutôt que le LDAP classique. Le LDAP avec TLS utilise la fonction StartTLS pour initier une connexion de LDAP en texte clair, mais la fait ensuite passer en connexion cryptée. Le LDAPS initie la connexion sur une connexion cryptée sans envoyer aucune donnée en texte clair.

Si vous sélectionnez **LDAPS** ou **LDAP avec TLS**, vous devez transférer le certificat SSL racine utilisé par votre serveur LDAP. Ceci est nécessaire pour garantir la validité du serveur et la sécurité des données. Le certificat racine doit être au format PEM.

***Remarque :** si le nom de sujet du certificat SSL public du serveur LDAP ou le composant DNS de son nom de sujet alternatif ne correspond pas à la valeur du champ **Nom de l'hôte**, le fournisseur sera considéré comme inaccessible. Vous pouvez cependant utiliser un certificat à caractère générique pour certifier plusieurs sous-domaines du même site. Par exemple, un certificat pour ***.example.com** certifiera à la fois **support.example.com** et **remote.example.com**.*

Informations d'authentification de liaison

Spécifiez un nom d'utilisateur et un mot de passe grâce auxquels votre Serveur d'accès à distance sécurisé peut se lier et effectuer une recherche sur le magasin d'annuaires LDAP.

Si votre serveur prend en charge les liaisons anonymes, vous aurez la possibilité de lier sans spécifier un nom d'utilisateur et un mot de passe. La liaison anonyme est considérée comme non sécurisée et est désactivée par défaut sur la plupart des serveurs LDAP.

Méthode de connexion

Si vous utilisez un magasin de répertoire externe sur le même réseau LAN que votre Serveur d'accès à distance sécurisé, il se peut que les deux systèmes puissent communiquer directement. Dans ce cas, vous pouvez laisser l'option **Proxy à partir du serveur via l'agent de connexion** décochée et poursuivre.

Si les deux systèmes ne peuvent pas communiquer directement, par exemple si votre serveur de répertoire externe se trouve derrière un pare-feu, vous devez utiliser un agent de connexion. Télécharger l'agent de connexion Win32 permet à votre serveur de répertoire et votre Serveur d'accès à distance sécurisé de communiquer par une connexion sortante chiffrée en SSL sans configuration de pare-feu. L'agent de connexion peut être téléchargé sur le serveur de répertoire ou sur un serveur séparé sur le même réseau que votre serveur de répertoire (recommandé).

Dans le cas ci-dessus, cochez **Proxy à partir du serveur via l'agent de connexion**. Créer un **Mot de passe de l'agent de connexion** à utiliser lors du processus d'installation de l'agent de connexion. Cliquez ensuite sur **Télécharger l'agent de connexion**, lancez l'installeur et suivez les instructions de l'assistant d'installation. Lors de l'installation, vous serez invité à saisir le nom du fournisseur de sécurité et le mot de passe de l'agent de connexion que vous avez créé ci-dessus.

Type de répertoire *(non visible pour les clusters)*

Pour aider à la configuration de la connexion réseau entre votre Serveur d'accès à distance sécurisé et votre fournisseur de sécurité, vous pouvez sélectionner un type de répertoire comme modèle. Ceci pré-remplit les champs de configuration ci-dessous avec des données standard, mais celles-ci doivent être modifiées pour correspondre à la configuration spécifique de votre fournisseur de sécurité. Le LDAP Active Directory est le type de serveur le plus commun, mais vous pouvez configurer BeyondTrust pour qu'il communique avec la plupart des types de fournisseurs de sécurité.

Paramètres du cluster *(Visible uniquement pour les clusters)*

Algorithme de sélection des membres

Sélectionnez la méthode de recherche des nœuds dans ce cluster.

Du haut vers le bas essaie en premier le serveur ayant la plus haute priorité dans le cluster. Si ce serveur n'est pas disponible ou si le compte n'est pas trouvé, le serveur ayant la priorité suivante est essayé. La recherche se déplace dans la liste des serveurs en cluster jusqu'à ce que le compte soit trouvé ou qu'il soit déterminé que le compte n'existe sur aucun des serveurs spécifiés et disponibles.

En alternance est conçu pour équilibrer la charge entre plusieurs serveurs. L'algorithme choisit aléatoirement quel serveur essayer en premier. Si ce serveur n'est pas disponible, ou si le compte n'est pas trouvé, un autre serveur aléatoire est essayé. La recherche se poursuit aléatoirement parmi les serveurs restants dans le cluster jusqu'à ce que le compte soit trouvé ou qu'il soit déterminé que le compte n'existe sur aucun des serveurs spécifiés et disponibles.

Délai de nouvelle tentative

Réglez la durée devant s'écouler avant de pouvoir tenter à nouveau d'utiliser un membre de cluster indisponible.

Paramètres de schéma d'utilisateur

Remplacer les valeurs de cluster *(Visible uniquement pour les nœuds du cluster)*

Si cette option n'est pas cochée, ce nœud de cluster utilisera les mêmes paramètres de schéma que le cluster. Si cette option est cochée, vous pouvez modifier les paramètres de schéma ci-dessous.

Nom unique de base de recherche

Déterminez le niveau dans la hiérarchie de votre annuaire, spécifiée par un nom unique, où le Serveur d'accès à distance sécurisé devra commencer à chercher des utilisateurs. En fonction de la taille de votre magasin d'annuaires et des utilisateurs nécessitant des comptes BeyondTrust, vous pourrez améliorer les performances en désignant l'unité organisationnelle spécifique dans votre magasin d'annuaires qui requiert l'accès. Si vous n'êtes pas sûr, ou si les utilisateurs recouvrent plusieurs unités organisationnelles, vous pouvez aussi spécifier le nom unique de la racine de votre magasin d'annuaires.

Requête utilisateur

Spécifiez les informations de requête que le Serveur d'accès à distance sécurisé doit utiliser pour trouver un utilisateur LDAP lorsque l'utilisateur tente de se connecter. Le champ **Requête utilisateur** accepte une requête LDAP standard (RFC 2254 - Représentation en chaîne des filtres de recherche LDAP). Vous pouvez modifier la chaîne de requête pour personnaliser la façon dont vos utilisateurs se connectent et quels types de noms d'utilisateurs sont acceptés. Pour spécifier quelle valeur à l'intérieur de la chaîne doit correspondre au nom d'utilisateur, remplacer cette valeur par *****.

Requête de navigation

La requête de navigation influence la façon dont les résultats sont affichés lors de la navigation par règles de groupe. Ceci filtre les résultats afin que seuls certains d'entre eux soient affichés dans la liste déroulante de sélection de membres lors de l'ajout de membres dans une règle de groupe.

Classes d'objets

Spécifiez des classes d'objets valides pour un utilisateur dans votre magasin d'annuaires. Seuls les utilisateurs possédant une ou plusieurs de ces classes d'objets seront autorisés à s'authentifier. Ces classes d'objets sont également utilisées avec les noms d'attribut ci-dessous pour indiquer à votre Serveur d'accès à distance sécurisé le schéma que le serveur LDAP utilise pour identifier les utilisateurs. Vous pouvez indiquer plusieurs classes d'objets, une par ligne.

Noms d'attribut

Spécifiez les champs à utiliser pour l'identificateur unique et les noms affichés d'un utilisateur.

Identificateur unique

Ce champ nécessite un identificateur unique pour l'élément. Bien que le nom unique puisse servir d'identificateur, le nom unique d'un utilisateur peut changer fréquemment au cours de la vie de l'utilisateur, avec un changement de nom ou d'emplacement, ou avec le changement de nom du magasin LDAP. Ainsi, la plupart des serveurs LDAP incorporent un champ unique pour chaque élément qui ne change pas pour la durée de vie de l'utilisateur. Si vous utilisez le nom unique comme identifiant unique et que le nom unique d'un utilisateur change, cet utilisateur sera considéré comme un nouvel utilisateur, et tout changement apporté spécifiquement au compte utilisateur BeyondTrust de cet individu ne sera pas reporté sur le nouvel utilisateur. Si votre serveur LDAP n'inclut pas d'identificateur unique, utilisez un champ dont il est peu probable que la valeur soit identique pour un autre utilisateur.

E-mail

L'attribut E-mail synchronise l'adresse e-mail de l'utilisateur depuis LDAP. Veuillez noter que les caractères spéciaux **?** et **!** ne peuvent pas être utilisés.

Photo

Ce champ vous permet de configurer des fournisseurs LDAP pour synchroniser les photos des techniciens d'assistance depuis LDAP. Par défaut, les modèles de paramètres pour Active Directory, Novell eDirectory et OpenLDAP utilisent tous l'attribut ***:jpegPhoto**. Les administrateurs peuvent modifier l'attribut si nécessaire. Si aucun attribut n'est spécifié, aucune photo ne sera récupérée depuis LDAP.

Les photos dans LDAP doivent être stockées en tant qu'images JPEG en données binaires brutes ou en données encodées en Base64. Remote Support BeyondTrust détecte automatiquement l'encodage et le décode selon les besoins.

Utiliser le même attribut pour les noms affichés publics et privés

Si cette option est cochée, vous pouvez spécifier des valeurs séparées pour les noms privé et public de l'utilisateur.

Noms affichés

Ces valeurs déterminent les champs qui devraient être utilisés en tant que nom privé et nom public de l'utilisateur.

Paramètres de schéma de groupe *(Visible uniquement lors de recherches de groupe)*

Nom unique de base de recherche

Déterminez le niveau dans la hiérarchie de votre annuaire, spécifiée par un nom unique, où le Serveur d'accès à distance sécurisé devra commencer à chercher des groupes. En fonction de la taille de votre magasin d'annuaires et des groupes nécessitant un accès au Serveur d'accès à distance sécurisé, vous pourrez améliorer les performances en désignant l'unité organisationnelle spécifique dans

votre magasin d'annuaire qui requiert l'accès. Si vous n'êtes pas sûr, ou si les groupes recouvrent plusieurs unités organisationnelles, vous pouvez aussi spécifier le nom unique de la racine de votre magasin d'annuaire.

Requête de navigation

La requête de navigation influence la façon dont les résultats sont affichés lors de la navigation par règles de groupe. Ceci filtre les résultats afin que seuls certains d'entre eux soient affichés dans la liste déroulante de sélection de membres lors de l'ajout de membres dans une règle de groupe.

Classes d'objets

Spécifiez des classes d'objets valides pour un groupe dans votre magasin d'annuaires. Seuls les groupes possédant une ou plusieurs de ces classes d'objets seront retournés. Ces classes d'objets sont également utilisées avec les noms d'attribut ci-dessous pour indiquer à votre Serveur d'accès à distance sécurisé le schéma que le serveur LDAP utilise pour identifier les groupes. Vous pouvez saisir plusieurs classes d'objets de groupes, une par ligne.

Noms d'attribut

Spécifiez les champs à utiliser pour l'identificateur unique, et le nom affiché d'un groupe.

Identificateur unique

Ce champ nécessite un identificateur unique pour l'élément. Bien que le nom unique puisse servir d'identificateur, le nom unique d'un groupe peut changer fréquemment au cours de la vie du groupe, avec un changement d'emplacement, ou avec le changement de nom du magasin LDAP. Ainsi, la plupart des serveurs LDAP incorporent un champ unique pour chaque élément qui ne change pas pour la durée de vie du groupe. Si vous utilisez le nom unique comme identificateur unique et que le nom unique d'un groupe change, ce groupe sera considéré comme un nouveau groupe, et toutes les règles de groupes définies pour ce groupe ne seront pas reportées sur le nouveau groupe. Si votre serveur LDAP n'inclut pas d'identificateur unique, utilisez un champ dont il est peu probable que la valeur soit identique pour un autre groupe.

Nom affiché

Cette valeur détermine quel champ doit être utilisé comme nom affiché du groupe.

Relations utilisateurs-groupes

Relations

Ce champ appelle une requête pour déterminer quels utilisateurs appartiennent à quels groupes ou, inversement, quels groupes contiennent quels utilisateurs.

Effectuer une recherche de groupes récursive

Vous pouvez choisir d'effectuer une recherche de groupes récursive. Ceci lancera une requête pour un utilisateur, puis des requêtes pour tous les groupes auxquels l'utilisateur appartient, puis des requêtes pour tous les groupes auxquels ces groupes appartiennent, et ainsi de suite, jusqu'à ce que tous les groupes possibles associés à cet utilisateur aient été trouvés.

Lancer une recherche récursive peut avoir un impact considérable sur les performances, car le serveur continuera à émettre des requêtes jusqu'à ce qu'il trouve des informations sur tous les groupes. Si cela prend trop de temps, l'utilisateur ne pourra peut-être pas se connecter.

Une recherche non récursive n'émettra qu'une requête par utilisateur. Si votre serveur LDAP a un champ spécial contenant tous les groupes auxquels l'utilisateur appartient, la recherche récursive n'est pas nécessaire. La recherche récursive est également inutile si votre système de répertoire ne prend pas en charge les membres de groupes ou les groupes.

Tester les paramètres

Nom d'utilisateur et mot de passe

Saisissez un nom d'utilisateur et un mot de passe pour un compte qui existe sur le serveur que vous testez. Ce compte doit correspondre aux critères de connexion spécifiés dans la configuration ci-dessus.

Essayer d'obtenir des attributs d'utilisateur et des appartenances de groupes si les informations d'authentification sont acceptées

Si cette option est cochée, votre test d'informations d'authentification réussi tentera également de vérifier les attributs d'utilisateur et la recherche de groupe.

> ***Remarque :*** *pour que ces fonctions soient testées avec succès, elles doivent être prises en charge et configurées dans votre fournisseur de sécurité.*

Tester

Si votre serveur est correctement configuré et que vous avez saisi un nom d'utilisateur et un mot de passe de test valides, vous recevrez un message de confirmation. Sinon, vous verrez un message d'erreur et un journal qui vous aidera à résoudre le problème.

> *Pour plus d'informations, veuillez consulter la section Créer et configurer le fournisseur de sécurité LDAP à l'adresse https://www.beyondtrust.com/docs/remote-support/how-to/integrations/security-providers/ldap-users/configure-settings.htm.*

Ajouter ou modifier un fournisseur de sécurité : RADIUS

Nom

Créez un nom unique permettant d'identifier ce fournisseur.

Activé

Si cette case est cochée, votre Serveur d'accès à distance sécurisé peut chercher ce fournisseur de sécurité lorsqu'un utilisateur tente de se connecter à la console du technicien d'assistance ou à **/login**. Si elle n'est pas cochée, le fournisseur ne sera pas recherché.

Conserver le nom affiché synchronisé avec le système distant

Ces valeurs déterminent les champs qui devraient être utilisés en tant que nom privé et nom public de l'utilisateur.

Paramètres d'autorisation

N'autoriser que les utilisateurs suivants

Vous pouvez choisir d'autoriser l'accès seulement aux utilisateurs spécifiés sur votre serveur RADIUS. Saisissez chaque nom d'utilisateur séparé par un saut de ligne. Une fois qu'ils auront été saisis, ces utilisateurs seront disponibles dans le dialogue **Ajouter membre de règle** lors de la modification de règle de groupe sur la page **/login > Utilisateurs et sécurité > Règles de groupe**.

Si vous laissez ce champ vide, tous les utilisateurs qui s'authentifient grâce à votre serveur RADIUS seront autorisés ; si vous les autorisez tous, vous devez aussi spécifier une règle de groupe par défaut.

Règle de groupe par défaut

Chaque utilisateur qui s'authentifie auprès d'un serveur externe doit être membre d'au moins une règle de groupe pour pouvoir s'authentifier sur votre Serveur d'accès à distance sécurisé, en se connectant sur l'interface /login ou sur la console du technicien d'assistance. Vous pouvez sélectionner une règle de groupe par défaut à appliquer à tous les utilisateurs autorisés à s'authentifier auprès du serveur configuré.

Recherche de groupe LDAP

Si vous voulez que les utilisateurs de ce fournisseur de sécurité soient associés à leurs groupes sur un serveur LDAP séparé, choisissez un ou plusieurs serveurs de groupe LDAP à utiliser pour la recherche de groupe.

Paramètres de connexion

Nom de l'hôte

Saisissez le nom d'hôte du serveur sur lequel se trouve le magasin d'annuaire externe.

Port

Spécifiez le port d'authentification pour votre serveur RADIUS. C'est en général le port **1812**.

Délai d'attente (secondes)

Définissez la durée d'attente maximale d'une réponse du serveur. Notez bien que si la réponse est **Réponse-Accepter** ou **Réponse-Demande**, alors RADIUS attendra pendant l'intégralité de la durée spécifiée ici avant d'authentifier le compte. Il est ainsi conseillé de garder cette valeur à un niveau aussi bas que possible, en fonction de vos paramètres réseau. Une valeur idéale est de 3-5 secondes, la valeur maximum étant de trois minutes.

Méthode de connexion

Si vous utilisez un magasin de répertoire externe sur le même réseau LAN que votre Serveur d'accès à distance sécurisé, il se peut que les deux systèmes puissent communiquer directement. Dans ce cas, vous pouvez laisser l'option **Proxy à partir du serveur via l'agent de connexion** décochée et poursuivre.

Si les deux systèmes ne peuvent pas communiquer directement, par exemple si votre serveur de répertoire externe se trouve derrière un pare-feu, vous devez utiliser un agent de connexion. Télécharger l'agent de connexion Win32 permet à votre serveur de répertoire et votre Serveur d'accès à distance sécurisé de communiquer par une connexion sortante chiffrée en SSL sans configuration de pare-feu.

L'agent de connexion peut être téléchargé sur le serveur de répertoire ou sur un serveur séparé sur le même réseau que votre serveur de répertoire (recommandé).

Dans le cas ci-dessus, cochez **Proxy à partir du serveur via l'agent de connexion**. Créer un **Mot de passe de l'agent de connexion** à utiliser lors du processus d'installation de l'agent de connexion. Cliquez ensuite sur **Télécharger l'agent de connexion**, lancez l'installeur et suivez les instructions de l'assistant d'installation. Lors de l'installation, vous serez invité à saisir le nom du fournisseur de sécurité et le mot de passe de l'agent de connexion que vous avez créé ci-dessus.

Secret partagé

Fournissez un nouveau secret partagé pour que votre Serveur d'accès à distance sécurisé et votre serveur RADIUS puissent communiquer.

Paramètres du cluster *(Visible uniquement pour les clusters)*

Algorithme de sélection des membres

Sélectionnez la méthode de recherche des nœuds dans ce cluster.

Du haut vers le bas essaie en premier le serveur ayant la plus haute priorité dans le cluster. Si ce serveur n'est pas disponible ou si le compte n'est pas trouvé, le serveur ayant la priorité suivante est essayé. La recherche se déplace dans la liste des serveurs en cluster jusqu'à ce que le compte soit trouvé ou qu'il soit déterminé que le compte n'existe sur aucun des serveurs spécifiés et disponibles.

En alternance est conçu pour équilibrer la charge entre plusieurs serveurs. L'algorithme choisit aléatoirement quel serveur essayer en premier. Si ce serveur n'est pas disponible, ou si le compte n'est pas trouvé, un autre serveur aléatoire est essayé. La recherche se poursuit aléatoirement parmi les serveurs restants dans le cluster jusqu'à ce que le compte soit trouvé ou qu'il soit déterminé que le compte n'existe sur aucun des serveurs spécifiés et disponibles.

Délai de nouvelle tentative

Réglez la durée devant s'écouler avant de pouvoir tenter à nouveau d'utiliser un membre de cluster indisponible.

Tester les paramètres

Nom d'utilisateur et mot de passe

Saisissez un nom d'utilisateur et un mot de passe pour un compte qui existe sur le serveur que vous testez. Ce compte doit correspondre aux critères de connexion spécifiés dans la configuration ci-dessus.

Essayer d'obtenir des attributs d'utilisateur et des appartenances de groupes si les informations d'authentification sont acceptées

Si cette option est cochée, votre test d'informations d'authentification réussi tentera également de vérifier les attributs d'utilisateur et la recherche de groupe.

> ***Remarque :*** *pour que ces fonctions soient testées avec succès, elles doivent être prises en charge et configurées dans votre fournisseur de sécurité.*

Tester

Si votre serveur est correctement configuré et que vous avez saisi un nom d'utilisateur et un mot de passe de test valides, vous recevrez un message de confirmation. Sinon, vous verrez un message d'erreur et un journal qui vous aidera à résoudre le problème.

> *Pour plus d'informations, veuillez consulter la section Créer et configurer le fournisseur de sécurité RADIUS à l'adresse https://www.beyondtrust.com/docs/remote-support/how-to/integrations/security-providers/radius/configure-settings.htm.*

Ajouter ou modifier un fournisseur de sécurité : Kerberos

Nom

Créez un nom unique permettant d'identifier ce fournisseur.

Activé

Si cette case est cochée, votre Serveur d'accès à distance sécurisé peut chercher ce fournisseur de sécurité lorsqu'un utilisateur tente de se connecter à la console du technicien d'assistance ou à **/login**. Si elle n'est pas cochée, le fournisseur ne sera pas recherché.

Conserver le nom affiché synchronisé avec le système distant

Ces valeurs déterminent les champs qui devraient être utilisés en tant que nom privé et nom public de l'utilisateur.

Retirer le domaine des noms principaux

Sélectionnez cette option pour supprimer la partie DOMAINE du nom principal d'utilisateur lors de la construction du nom d'utilisateur BeyondTrust.

Paramètres d'autorisation

Mode de gestion des utilisateurs

Sélectionnez les utilisateurs pouvant s'authentifier auprès de votre Serveur d'accès à distance sécurisé. **Autoriser tous les utilisateurs** autorise toute personne actuellement authentifiée par votre KDC (Key Distribution Center). **Autoriser uniquement les noms principaux d'utilisateurs indiqués dans la liste** n'autorise que les noms principaux d'utilisateurs spécifiquement désignés. **Autoriser uniquement les noms principaux d'utilisateurs qui correspondent à la regex** autorise uniquement les utilisateurs correspondant à une expression régulière compatible Perl (PCRE).

Règle de groupe par défaut

Chaque utilisateur qui s'authentifie auprès d'un serveur externe doit être membre d'au moins une règle de groupe pour pouvoir s'authentifier sur votre Serveur d'accès à distance sécurisé, en se connectant sur l'interface /login ou sur la console du technicien d'assistance. Vous pouvez sélectionner une règle de groupe par défaut à appliquer à tous les utilisateurs autorisés à s'authentifier auprès du serveur configuré.

Mode de gestion SPN

Autoriser uniquement les SPN indiqués dans la liste

Si la case n'est pas cochée, tous les Noms principaux du service (SPN) pour ce fournisseur de sécurité sont autorisés. Si la case est cochée, sélectionnez des SPN spécifiques dans une liste de SPN actuellement configurés.

Recherche de groupe LDAP

Si vous voulez que les utilisateurs de ce fournisseur de sécurité soient associés à leurs groupes sur un serveur LDAP séparé, choisissez un ou plusieurs serveurs de groupe LDAP à utiliser pour la recherche de groupe.

> *Pour plus d'informations, veuillez consulter la section Configurer le Serveur d'accès à distance sécurisé pour l'authentification Kerberos à l'adresse https://www.beyondtrust.com/docs/remote-support/how-to/integrations/security-providers/kerberos-configuration/index.htm.*

Ajouter ou modifier un fournisseur de sécurité : SAML pour techniciens d'assistance

Nom

Le nom de votre fournisseur SAML est auto-généré et ne peut pas être modifié pour le moment.

Activé

Si cette case est cochée, votre Serveur d'accès à distance sécurisé peut chercher ce fournisseur de sécurité lorsqu'un utilisateur tente de se connecter à la console du technicien d'assistance ou à **/login**. Si elle n'est pas cochée, le fournisseur ne sera pas recherché.

Paramètres du fournisseur d'identité

Métadonnées

Le fichier de métadonnées contient toutes les informations nécessaires à l'installation initiale de votre fournisseur SAML et doit être téléchargé à partir de votre fournisseur d'identité. Enregistrez le fichier XML, puis cliquez sur **Transférer des métadonnées de fournisseur d'identité** pour sélectionner et transférer le fichier sélectionné.

ID d'entité

Identificateur unique pour le fournisseur d'identité que vous utilisez.

Certificat du serveur

Ce certificat sera utilisé pour vérifier la signature de l'affirmation envoyée par le fournisseur d'identité.

> ***Remarque :*** *les champs pour l'**ID d'entité**, l'**URL de service d'authentification unique** et le **Certificat** sont automatiquement remplis à partir du fichier de métadonnées du fournisseur d'identité. Si vous ne pouvez pas obtenir de fichier de métadonnées de votre fournisseur, ces informations peuvent être saisies manuellement.*

URL de service d'authentification unique

Lorsque vous souhaitez vous connecter à BeyondTrust au moyen de SAML, c'est vers cette URL que vous serez automatiquement redirigé afin de pouvoir vous connecter.

Liaison de protocole URL SSO

Cela détermine si un utilisateur poste, ou s'il est redirigé vers l'URL d'authentification. Ceci devrait être laissé par défaut sur la redirection, sauf si quelque chose d'autre est requis par le fournisseur d'identité.

Paramètres du fournisseur de service

Télécharger les métadonnées du fournisseur de service

Téléchargez les métadonnées BeyondTrust qui doivent ensuite être transférées à votre fournisseur d'identité.

ID d'entité

Ceci est votre URL BeyondTrust. Elle identifie de façon unique le fournisseur de service.

Clé privée

Si nécessaire, vous pouvez déchiffrer les messages envoyés par le fournisseur d'identité, s'ils prennent en charge et requièrent le chiffrement. Cliquez sur **Choisir le fichier** pour transférer la clé privée nécessaire au déchiffrement des messages envoyés par le fournisseur d'identité.

Paramètres d'attributs d'utilisateur

Les attributs SAML sont utilisés pour approvisionner les utilisateurs dans BeyondTrust. Les valeurs par défaut correspondent aux applications certifiées par BeyondTrust avec différents fournisseurs d'identité. Si vous créez votre propre connecteur SAML, il se peut que vous ayez besoin de modifier les attributs pour qu'ils correspondent à ce qui est envoyé par votre fournisseur d'identité. Si votre fournisseur d'identité requiert une insensibilité à la casse pour l'attribut NameID, sélectionnez **Utiliser une comparaison non sensible à la casse pour les NameID**.

Paramètres d'autorisation

Nom d'attribut de recherche de groupe

Ceci est le nom de l'attribut SAML contenant les noms des groupes auxquels les utilisateurs devraient appartenir. Le nom par défaut des applications BeyondTrust est « Groupes ».

Délimiteur

si la valeur d'attribut contient plusieurs noms de groupes, vous devez spécifier le délimiteur utilisé pour séparer leurs noms. Si le délimiteur est laissé vide, la valeur d'attribut peut contenir plusieurs nœuds XML contenant chacun un nom différent.

Groupes disponibles

Permet à une liste de groupes prédéfinie d'être associée au fournisseur de sécurité. Cette liste peut ensuite être utilisée pour associer un groupe à la règle de groupe appropriée.

Règle de groupe par défaut

Sélectionnez le groupe par défaut auquel les utilisateurs seront assignés. les utilisateurs se verront attribuer des paramètres définis dans la règle de groupe par défaut seulement s'ils n'appartiennent pas à une autre règle de groupe qui définit ces paramètres.

> *Pour plus d'informations, veuillez consulter la section SAML pour l'authentification unique à l'adresse https://www.beyondtrust.com/docs/remote-support/how-to/integrations/security-providers/saml/index.htm.*

Ajouter ou modifier un fournisseur de sécurité : SAML pour portails publics

Nom

Le nom de votre fournisseur SAML est auto-généré et ne peut pas être modifié pour le moment.

Activé

Si cette case est cochée, votre Serveur d'accès à distance sécurisé peut chercher ce fournisseur de sécurité lorsqu'un utilisateur tente de se connecter au portail public. Si elle n'est pas cochée, le fournisseur ne sera pas recherché.

Paramètres du fournisseur d'identité

Métadonnées

Le fichier de métadonnées contient toutes les informations nécessaires à l'installation initiale de votre fournisseur SAML et doit être téléchargé à partir de votre fournisseur d'identité. Enregistrez le fichier XML, puis cliquez sur **Transférer des métadonnées de fournisseur d'identité** pour sélectionner et transférer le fichier sélectionné.

ID d'entité

Identificateur unique pour le fournisseur d'identité que vous utilisez.

Certificat du serveur

Ce certificat sera utilisé pour vérifier la signature de l'affirmation envoyée par le fournisseur d'identité.

> ***Remarque :*** *les champs pour l'**ID d'entité**, l'**URL de service d'authentification unique** et le **Certificat** sont automatiquement remplis à partir du fichier de métadonnées du fournisseur d'identité. Si vous ne pouvez pas obtenir de fichier de métadonnées de votre fournisseur, ces informations peuvent être saisies manuellement.*

URL de service d'authentification unique

Lorsque vous souhaitez vous connecter à BeyondTrust au moyen de SAML, c'est vers cette URL que vous serez automatiquement redirigé afin de pouvoir vous connecter.

Liaison de protocole URL SSO

Cela détermine si un utilisateur poste, ou s'il est redirigé vers l'URL d'authentification. Ceci devrait être laissé par défaut sur la redirection, sauf si quelque chose d'autre est requis par le fournisseur d'identité.

Paramètres du fournisseur de service

Télécharger les métadonnées du fournisseur de service

Téléchargez les métadonnées BeyondTrust qui doivent ensuite être transférées à votre fournisseur d'identité.

ID d'entité

Ceci est votre URL BeyondTrust. Elle identifie de façon unique le fournisseur de service.

Clé privée

Si nécessaire, vous pouvez déchiffrer les messages envoyés par le fournisseur d'identité, s'ils prennent en charge et requièrent le chiffrement. Cliquez sur **Choisir le fichier** pour transférer la clé privée nécessaire au déchiffrement des messages envoyés par le fournisseur d'identité.

Paramètres d'attributs d'utilisateur

Les attributs SAML sont utilisés pour approvisionner les utilisateurs dans BeyondTrust. Les valeurs par défaut correspondent aux applications certifiées par BeyondTrust avec différents fournisseurs d'identité. Si vous créez votre propre connecteur SAML, il se peut que vous ayez besoin de modifier les attributs pour qu'ils correspondent à ce qui est envoyé par votre fournisseur d'identité. Les attributs SAML peuvent aussi être associés aux sessions du client en ajoutant des champs personnalisés avec des noms de code correspondant sur la page **Champs personnalisés** dans **/login**.

> *Pour plus d'informations, veuillez consulter la section SAML pour l'authentification unique à l'adresse https://www.beyondtrust.com/docs/remote-support/how-to/integrations/security-providers/saml/index.htm.*

Règles de session : Configuration de règles de demande et d'autorisation de session

Règles de session

Les règles de session permettent de personnaliser les autorisations de sécurité des sessions pour correspondre à des scénarios spécifiques. Les règles de session peuvent être appliquées aux utilisateurs, aux sites publics et aux Jump Clients.

> *Pour plus d'informations, reportez-vous à la section Utilisation des règles de Session d'assistance technique à l'adresse www.beyondtrust.com/docs/remote-support/how-to/session-policies/.*

La section **Règles de session** répertorie toutes les règles disponibles. Cliquez sur la flèche située en regard d'une règle pour connaître les éléments auxquels elle est associée, sa disponibilité pour les utilisateurs, les invitations de techniciens d'assistance et les Jump Clients, ainsi que les outils d'assistance technique et les demandes configurés.

Ajouter, modifier, supprimer

Créer une nouvelle règle, modifier ou supprimer une règle existante.

Copier

Pour accélérer la création de règles de groupe semblables, cliquez sur **Copier** pour créer une nouvelle règle avec des réglages identiques. Vous pouvez ensuite modifier cette nouvelle règle pour répondre à vos exigences spécifiques.

Ajouter ou modifier une règle de session

Après avoir effectué vos modifications, cliquez sur **Enregistrer** pour rendre cette règle disponible.

Nom affiché

Créez un nom unique permettant d'identifier cette règle. Ce nom facilite l'assignation d'une règle de session aux utilisateurs, portails publics et Jump Clients.

Nom de code

Définissez également un nom de code, qui sera utilisé à des fins d'intégration. Dans le cas contraire, le système en crée un automatiquement.

Description

Ajoutez une brève description pour résumer la fonction de cette règle. La description s'affiche lors de l'application d'une règle à des comptes utilisateur, règles de groupe et invitations de technicien d'assistance.

Disponibilité

Utilisateurs

Choisissez si cette règle peut être attribuée à des utilisateurs (comptes d'utilisateurs et règles de groupe).

Invitation d'un technicien d'assistance

Choisissez si cette règle peut être sélectionnée par les utilisateurs lors de l'invitation d'utilisateurs externes à rejoindre une session.

Éléments de Jump

Choisissez si cette règle peut être associée à un élément de Jump.

Dépendances

Si cette règle de session est déjà utilisée, le nombre d'utilisateurs, de portails publics et de Jump Clients associés est également indiqué.

Autorisations

Vous pouvez choisir d'activer ou de désactiver toutes les autorisations suivantes, ou encore de les définir sur **Non défini**. Les règles de session sont appliquées à une session de manière hiérarchisée, les Jump Clients étant prioritaires, suivis des portails d'assistance technique, des utilisateurs, et enfin de la règle globale par défaut. S'il existe plusieurs règles s'appliquant à une session, la règle présentant la priorité la plus haute prévaut sur toutes les autres. Par exemple, si la règle appliquée à un Jump Client définit une autorisation, alors aucune autre règle ne peut modifier cette autorisation pour la session. Pour qu'une autorisation puisse être définie par une règle de niveau inférieur, elle doit être définie sur **Non défini**.

> *Pour plus d'informations et d'exemples, reportez-vous à la section Utilisation des règles de Session d'assistance technique à l'adresse www.beyondtrust.com/docs/remote-support/how-to/session-policies/.*

Indiquez les outils devant être activés ou désactivés par cette règle, ainsi que ceux devant faire l'objet d'une demande d'autorisation au client.

Demande d'outil d'assistance technique

> *Pour en savoir plus, veuillez consulter Client d'utilisateur : Interface de session d'assistance technique à l'adresse https://www.beyondtrust.com/docs/remote-support/getting-started/customer-client/customer-support-interface.htm.*

Règles de demande

Vous pouvez choisir de demander à l'utilisateur l'autorisation d'utiliser les fonctions d'assistance technique ci-après. Sélectionnez **Aucune demande** pour ne jamais envoyer de demande, **Toujours demander** pour toujours envoyer une demande ou **Demander pour certains outils** pour choisir les autorisations pour lesquelles envoyer une demande. Lorsque l'option **Demander pour certains outils** est sélectionnée, l'option **Demander l'accord de l'utilisateur** apparaît en dessous de chaque outil, avec les choix **Jamais** et **Toujours**. En cas de sélection de **Non défini**, cette option est définie par la règle de priorité inférieure suivante. Ce réglage peut être remplacé par une règle de priorité supérieure.

Autorisé à demander une fois

Si l'option **Partage d'écran** est définie sur **Voir et contrôler** et que l'envoi de demandes est activé, cette option est disponible. Cochez cette case pour permettre à la fonction de partage d'écran d'accéder à tous les outils au cours de la session, sans demande supplémentaire.

Options de demande

Définissez le délai d'attente de réponse à une demande avant l'envoi de la réponse par défaut **Refuser** ou **Autoriser**. En cas de sélection de **Non défini**, cette option est définie par la règle de priorité inférieure suivante. Ce réglage peut être remplacé par une règle de priorité supérieure.

Partage d'écran

Règles de partage d'écran

Permet à l'utilisateur de voir ou de contrôler l'écran distant. En cas de sélection de **Non défini**, cette option est définie par la règle de priorité inférieure suivante. Ce réglage peut être remplacé par une règle de priorité supérieure.

> *Pour plus d'informations, veuillez consulter la section Partage d'écran avec l'utilisateur distant à des fins de consultation et de contrôle à l'adresse https://www.beyondtrust.com/docs/remote-support/getting-started/rep-console/screen-sharing.htm.*

Autorisé à montrer son écran à l'utilisateur

Permet à l'utilisateur de partager son écran avec le client au cours d'une session d'assistance technique.

> *Pour plus d'informations, veuillez consulter la section Montrer mon écran : Inversion du partage d'écran à l'adresse https://www.beyondtrust.com/docs/remote-support/getting-started/customer-client/show-my-screen.htm.*

Restrictions d'utilisateur autorisées

Définissez si l'utilisateur peut interrompre l'entrée souris et clavier du système distant. L'utilisateur peut aussi empêcher l'affichage du bureau distant.

> *Pour plus d'informations, veuillez consulter la section Interaction client restreinte : Écran de confidentialité et désactivation de l'entrée de l'utilisateur distant à l'adresse https://www.beyondtrust.com/docs/remote-support/getting-started/customer-client/privacy-screen.htm.*

Comportement de demande de partage d'applications

Déterminez si une demande de partage d'écran ne doit jamais ou toujours faire l'objet d'une demande auprès du client pour sélectionner les applications à partager, ou si l'utilisateur peut choisir de faire une demande de partage d'applications ou non. Sélectionner **Toujours** ou **Décision du technicien d'assistance** vous permet aussi de prédéfinir les restrictions de partage d'application.

Pour plus d'informations, veuillez consulter la section Partage d'application : Restriction des éléments visibles par le technicien d'assistance à l'adresse https://www.beyondtrust.com/docs/remote-support/getting-started/customer-client/application-sharing.htm.

Sens de synchronisation du presse-papiers

Sélectionnez la manière dont le contenu du presse-papiers circule entre les techniciens d'assistance et les utilisateurs finaux. Les options sont :

- **Non autorisé :** Le technicien d'assistance n'est pas autorisé à utiliser le presse-papiers, aucune icône de presse-papiers ne s'affiche dans la console du technicien d'assistance et les commandes couper-coller ne fonctionnent pas.
- **Autorisé du technicien d'assistance vers l'utilisateur :** Le technicien d'assistance peut envoyer le contenu du presse-papiers au client, mais ne peut pas le coller à partir du presse-papiers de l'utilisateur final. Seule l'icône Envoyer le presse-papiers s'affiche dans la console du technicien d'assistance.
- **Envoyer dans les deux sens :** Le contenu du presse-papiers peut circuler dans les deux sens. Les icônes du presse-papiers Envoyer et Obtenir s'affichent dans la console du technicien d'assistance.

Pour plus d'informations sur le Mode de synchronisation du presse-papiers, veuillez consulter « Sécurité : Gestion des paramètres de sécurité », page 205 de sécurité.

Partage de navigateur

Règles de partage de navigateur

Permet à l'utilisateur de consulter la même page Web que le client regarde, sans avoir le contrôle et sans voir d'autres applications. En cas de sélection de **Non défini**, cette option est définie par la règle de priorité inférieure suivante. Ce réglage peut être remplacé par une règle de priorité supérieure.

Pour plus d'informations, veuillez consulter la section Partage d'écran avec l'utilisateur distant à des fins de consultation et de contrôle à l'adresse https://www.beyondtrust.com/docs/remote-support/getting-started/rep-console/screen-sharing.htm.

Annotations

Règles d'annotation

Permet à l'utilisateur d'utiliser les outils d'annotation pour dessiner sur l'écran du système distant. En cas de sélection de **Non défini**, cette option est définie par la règle de priorité inférieure suivante. Ce réglage peut être remplacé par une règle de priorité supérieure.

Pour plus d'informations, veuillez consulter la section Utiliser les annotations pour dessiner sur l'écran distant à l'adresse https://www.beyondtrust.com/docs/remote-support/getting-started/rep-console/annotations.htm.

Transfert de fichiers

Règles de transfert de fichiers

Permet à l'utilisateur d'envoyer des fichiers vers le système distant, de télécharger des fichiers depuis le système distant, ou les deux. En cas de sélection de **Non défini**, cette option est définie par la règle de priorité inférieure suivante. Ce réglage peut être remplacé par une règle de priorité supérieure.

Chemins accessibles sur le système de fichiers de l'utilisateur

Permettre à l'utilisateur de transférer des fichiers de et vers n'importe quel répertoire sur le système distant ou uniquement les répertoires spécifiés.

Chemins accessibles sur le système de fichiers du technicien d'assistance

Permettre à l'utilisateur de transférer des fichiers de et vers n'importe quel répertoire sur son système local ou uniquement les répertoires spécifiés.

> *Pour plus d'informations, veuillez consulter la section Transfert de fichiers vers et depuis le système distant à l'adresse https://www.beyondtrust.com/docs/remote-support/getting-started/rep-console/file-transfer.htm.*

Interpréteur de commandes

Règles de l'interpréteur de commandes

Permet à l'utilisateur de saisir des commandes sur l'ordinateur distant par l'intermédiaire d'une interface en ligne de commande virtuelle. En cas de sélection de **Non défini**, cette option est définie par la règle de priorité inférieure suivante. Ce réglage peut être remplacé par une règle de priorité supérieure.

> ***Remarque :** l'accès à l'interpréteur de commandes ne peut pas être restreint lors de sessions de Shell Jump.*

> *Pour plus d'informations, veuillez consulter la section Accès à l'interpréteur de commandes distant à l'adresse https://www.beyondtrust.com/docs/remote-support/getting-started/rep-console/command-shell.htm.*

Informations système

Règles relatives aux informations système

Permet à l'utilisateur de consulter les informations système de l'ordinateur distant. En cas de sélection de **Non défini**, cette option est définie par la règle de priorité inférieure suivante. Ce réglage peut être remplacé par une règle de priorité supérieure.

Autorisé à utiliser les actions relatives aux informations système

Permet à l'utilisateur d'interagir avec les processus et les programmes sur le système distant sans avoir recours au partage d'écran. Le technicien d'assistance peut ainsi désinstaller des programmes, supprimer des processus ou encore démarrer, arrêter, mettre en pause, reprendre et redémarrer des services.

> *Pour plus d'informations, veuillez consulter la section Consulter les informations du système distant à l'adresse https://www.beyondtrust.com/docs/remote-support/getting-started/rep-console/system-info.htm.*

Accès au registre

Règles d'accès au registre

Permet à l'utilisateur d'agir sur le registre d'un système Windows distant sans avoir recours au partage d'écran. Le technicien d'assistance peut ainsi afficher, ajouter, supprimer, modifier, rechercher et importer/exporter des clés.

> *Pour plus d'informations, veuillez consulter la section Accès à l'éditeur de registre distant à l'adresse https://www.beyondtrust.com/docs/remote-support/getting-started/rep-console/registry-editor.htm.*

Scripts prédéfinis

Règles de script prédéfini

Permet à l'utilisateur d'exécuter des scripts prédéfinis créés pour ses équipes. Notez que lorsque l'utilisateur est en partage d'écran en mode affichage seul, le client reçoit une invite pour autoriser le lancement du script.En cas de sélection de **Non défini**, cette option est définie par la règle de priorité inférieure suivante. Ce réglage peut être remplacé par une règle de priorité supérieure.

> *Pour plus d'informations, veuillez consulter la section Accès à l'interpréteur de commandes distant à l'adresse https://www.beyondtrust.com/docs/remote-support/getting-started/rep-console/command-shell.htm.*

Accroissement des droits

Règles d'accroissement des droits

Permet à l'utilisateur de tenter d'accroître les droits du client d'utilisateur pour s'exécuter avec des droits administratifs sur le système distant. En cas de sélection de **Non défini**, cette option est définie par la règle de priorité inférieure suivante. Ce réglage peut être remplacé par une règle de priorité supérieure.

> *Pour plus d'informations, veuillez consulter la section Accroître le client à l'adresse https://www.beyondtrust.com/docs/remote-support/getting-started/rep-console/elevation.htm.*

Déploiement de Bouton assistance technique

Règles de déploiement de Bouton assistance technique

Permet à l'utilisateur de déployer ou de supprimer un Bouton assistance technique au cours d'une session. Les emplacements de déploiement possibles dépendent des paramètres de Bouton assistance technique ci-dessus. En cas de sélection de **Non défini**, cette option est définie par la règle de priorité inférieure suivante. Ce réglage peut être remplacé par une règle de priorité supérieure.

> *Pour plus d'informations, veuillez consulter la section Vue d'ensemble des sessions d'assistance technique et outils à l'adresse https://www.beyondtrust.com/docs/remote-support/getting-started/rep-console/support-session-overview.htm.*

Attachement/Détachement de Jump Clients

Règles d'attachement/détachement de Jump Clients

Permet à l'utilisateur d'attacher ou de détacher un Jump Client au cours d'une session. Les emplacements de déploiement possibles dépendent des paramètres de Jump Client précédents. En cas de sélection de **Non défini**, cette option est définie par la règle de priorité inférieure suivante. Ce réglage peut être remplacé par une règle de priorité supérieure.

> *Pour plus d'informations, veuillez consulter la section Vue d'ensemble des sessions d'assistance technique et outils à l'adresse https://www.beyondtrust.com/docs/remote-support/getting-started/rep-console/support-session-overview.htm.*

Messagerie instantanée

> *Pour plus d'informations, veuillez consulter la section Messagerie instantanée avec un utilisateur lors d'une session à l'adresse https://www.beyondtrust.com/docs/remote-support/getting-started/rep-console/chat.htm.*

Règles de messagerie instantanée

Permet à l'utilisateur de discuter avec le client distant. En cas de sélection de **Non défini**, cette option est définie par la règle de priorité inférieure suivante. Ce réglage peut être remplacé par une règle de priorité supérieure.

Autorisé à charger des URL dans le navigateur Web de l'utilisateur

Permet à l'utilisateur d'entrer une URL dans la zone de messagerie instantanée, puis de cliquer sur le bouton **Charger l'URL** pour ouvrir automatiquement un navigateur Web à cette adresse sur l'ordinateur distant.

Autorisé à envoyer des fichiers à l'aide de l'interface de messagerie instantanée

Permet à l'utilisateur d'envoyer des fichiers via l'interface de messagerie instantanée.

> *Pour en savoir plus, veuillez consulter Client d'utilisateur : Interface de session d'assistance technique à l'adresse https://www.beyondtrust.com/docs/remote-support/getting-started/customer-client/customer-support-interface.htm.*

Exporter la règle

Vous pouvez exporter une règle de session à partir d'un site et importer ces autorisations dans une règle sur un autre site. Modifiez la règle que vous souhaitez exporter et faites défiler jusqu'au bas de la page. Cliquez sur **Exporter la règle** et enregistrez le fichier.

Importer une règle

Vous pouvez importer ces paramètres de règles vers les autres sites BeyondTrust prenant en charge l'importation de règles de session. Créez une nouvelle règle de session, puis accédez au bas de la page. Naviguez jusqu'au fichier de la règle, puis cliquez sur **Importer la règle**. Une fois le fichier de la règle chargé, la page s'actualisera pour vous permettre d'effectuer des modifications. Cliquez alors sur **Enregistrer la règle** pour rendre la règle disponible.

Simulateur de règle de session

La priorisation des règles pouvant s'avérer complexe, vous pouvez utiliser le **simulateur de règle de session** pour déterminer le résultat. Vous pouvez également utiliser ce simulateur pour déterminer pourquoi une autorisation n'est pas disponible alors qu'elle devrait l'être.

Technicien d'assistance

Commencez en sélectionnant l'utilisateur effectuant la session. La liste déroulante inclut les règles de comptes d'utilisateur et d'invitation de techniciens d'assistance.

Méthode de démarrage de session

Sélectionnez la méthode de démarrage de la session à utiliser pour cette simulation.

Portail public

Si vous avez sélectionné **Portail public**, indiquez le portail public à utiliser pour cette simulation de session initiée par le client.

Bouton assistance technique

Si vous avez sélectionné **Bouton assistance technique**, recherchez un Bouton assistance technique déployé par profil, portail public associé, file d'attente associée, nom d'ordinateur ou description. Le portail public associé sera automatiquement sélectionné au-dessus.

Jumpoint ou Jump local

Dans la mesure où les Jumps locaux et les Jumpoints sont toujours associés au portail public par défaut, aucune configuration supplémentaire n'est requise.

Jump Client, raccourci de Jump local, raccourci de Jump distant, raccourci de Jump VNC local, raccourci de Jump VNC distant, raccourci de Jump RDP distant, raccourci de Jump RDP local, raccourci de Shell Jump, raccourci Intel® vPro

Rechercher un Jump Client attaché ou un raccourci de Jump par nom, commentaires, groupe de Jump, balise, ou portail public associé. Le portail public associé sera automatiquement sélectionné au-dessus.

Utilisateur présent

Si vous avez sélectionné **Jump Client**, vous pouvez choisir si l'utilisateur doit apparaître comme étant présent ou non.

Simuler

Cliquez sur **Simuler**. La zone située en dessous affiche en lecture seule les autorisations configurables par règle de session. Vous pouvez ainsi voir quelles autorisations sont accordées ou refusées d'après la hiérarchie de règles, ainsi que la règle associée à chaque autorisation.

Règles de groupe : Application d'autorisations utilisateur à des groupes d'utilisateurs

Règles de groupe

La page **Règles de groupe** vous permet de définir des groupes d'utilisateurs qui partagent des privilèges communs.

Ajouter, modifier, supprimer

Créer une nouvelle règle, modifier ou supprimer une règle existante.

> ***Remarque :*** *si vous modifiez la règle de groupe qui est celle par défaut pour le fournisseur local, ou qui comporte des utilisateurs administrateurs locaux et que vous supprimez les autorisations d'administrateur, un message d'avertissement s'affiche. Assurez-vous que les autres utilisateurs disposent des autorisations d'administrateur avant de continuer.*

Copier

Pour accélérer la création de règles de groupe semblables, cliquez sur **Copier** pour créer une nouvelle règle avec des réglages identiques. Vous pouvez ensuite modifier cette nouvelle règle pour répondre à vos exigences spécifiques.

Modifier l'ordre

Cliquez sur le bouton **Modifier l'ordre** pour faire glisser et déposer les règles de groupe afin de définir leur priorité. Cliquez sur **Enregistrer l'ordre** pour que les changements de priorité prennent effet. Lorsque plusieurs règles s'appliquent à un utilisateur donné, les autorisations prennent effet en commençant en haut de la liste **Règles de groupe**, puis en descendant dans la liste. Si une autorisation entre en conflit avec une autorisation appliquée par une règle de groupe située plus haut dans la liste, l'autorisation la plus basse écrasera la plus élevée, à moins que la plus élevée n'ait été définie en tant que **Final**. En bref, les règles de groupe qui apparaissent plus bas dans la liste ont une priorité fonctionnelle plus élevée que celles qui sont plus haut.

Ajouter ou modifier une règle

Après avoir effectué vos modifications, cliquez sur **Enregistrer** pour enregistrer vos modifications dans cette règle de groupe.

Nom de la règle

Créez un nom unique permettant d'identifier cette règle.

Membres de la règle

Pour attribuer des membres, cliquez sur le bouton **Ajouter** pour ouvrir une zone de sélection. Sélectionnez des utilisateurs dans votre système local, ou sélectionnez des utilisateurs ou des groupes entiers à partir des fournisseurs de sécurité configurés. Pour ajouter des utilisateurs et des groupes d'un magasin d'annuaires externe, vous devez d'abord configurer la connexion sur la page **/login >**

Utilisateurs et sécurité > Fournisseurs de sécurité. Si une tentative d'ajout d'un utilisateur d'un fournisseur de sécurité configuré n'est pas valide, le message d'erreur de journal de synchronisation apparaîtra ici et dans le journal.

Paramètres du compte

Quels paramètres de compte cette règle de groupe doit-elle contrôler ?

Décidez si un paramètre doit être **Défini** dans cette règle. Dans l'affirmative, vous pouvez sélectionner **Final** pour empêcher des règles de priorité inférieure d'outrepasser la valeur d'autorisation définie par cette règle. Sélectionnez **Tout** pour définir tous les paramètres dans cette section.

Authentification à deux facteurs : Connexion avec une appli d'authentification :

Choisissez si l'utilisateur doit impérativement utiliser une appli d'authentification ou si le choix lui est laissé (réglage par défaut). Si cette option est définie sur **Obligatoire**, la prochaine fois que l'utilisateur tentera de se connecter à l'interface d'administration ou à la console du technicien d'assistance, un écran s'affichera pour demander qu'il active l'authentification à deux facteurs.

> *Pour plus d'informations sur l'authentification à deux facteurs, veuillez consulter Comment utiliser l'authentification à deux facteurs avec Remote Support BeyondTrust à l'adresse www.beyondtrust.com/docs/remote-support/how-to/2-factor-authentication/.*

Expiration du compte : Le compte n'expire jamais

Lorsque cette option est sélectionnée, le compte n'expire jamais.

Expiration du compte : Date d'expiration du compte

Avec ceci, le compte expirera à une date donnée.

Activation du compte : Compte désactivé

Désactive le compte pour que l'utilisateur ne puisse plus se connecter. Une désactivation ne supprime PAS le compte.

Modification du nom affiché : Autorisé à modifier ses noms affichés

Permet aux utilisateurs de changer leurs noms affichés.

Modification de photo : Autorisé à modifier sa photo

Permet aux utilisateurs de changer la photo de leur avatar, qui s'affiche sur l'interface d'administration **/login** et dans la fenêtre de messagerie instantanée du client d'utilisateur.

Apparaître sur le site public : Autorisé à apparaître sur le site public

Affiche le nom de l'utilisateur sur tous les sites publics sur lesquels la liste des techniciens d'assistance est activée.

Commentaires

Ajoutez des commentaires pour identifier la fonction de ce compte.

Autorisations générales

Quels paramètres globaux cette règle de groupe doit-elle contrôler ?

Décidez si un paramètre doit être **Défini** dans cette règle. Dans l'affirmative, vous pouvez sélectionner **Final** pour empêcher des règles de priorité inférieure d'outrepasser la valeur d'autorisation définie par cette règle. Sélectionnez **Tout** pour définir tous les paramètres dans cette section.

Administration

Privilèges administratifs : Administrateur

Accorde des droits d'administration complets à l'utilisateur.

Privilèges administratifs Vault : Autorisé à administrer Vault

Permet à l'utilisateur de gérer tous les aspects de l'add-on Vault de BeyondTrust.

Paramètres de mot de passe : Autorisé à définir les mots de passe

Permet à l'utilisateur de définir des mots de passe et de débloquer des comptes pour les utilisateurs locaux ne disposant pas de droits d'administrateur.

Modification d'un Jumpoint : Autorisé à modifier les Jumpoints

Permet à l'utilisateur de créer ou de modifier des Jumpoints. Cette option n'affecte pas la capacité de l'utilisateur à accéder à des ordinateurs distants via un Jumpoint, qui est configurée par Jumpoint ou règle de groupe.

Modification du site public : Autorisé à modifier le site public

Permet à l'utilisateur de créer et de modifier les configurations du site public, de modifier les modèles HTML, d'afficher l'interface de traduction, etc.

Modification des annonces aux utilisateurs : Autorisé à modifier les annonces aux utilisateurs

Permet aux techniciens d'assistance de créer et de modifier des messages utilisés pour notifier les utilisateurs, lorsqu'ils demandent une assistance technique, en cas d'interruptions informatiques à grand impact.

Modification du magasin de fichiers : Autorisé à modifier le magasin de fichiers

Permet à l'utilisateur d'ajouter ou de supprimer des fichiers depuis le magasin de fichiers.

Modification de message prédéfini : Autorisé à modifier les messages prédéfinis

Permet à l'utilisateur de créer ou de modifier des messages de messagerie instantanée prédéfinis.

Modification d'équipe d'assistance : Autorisé à modifier les équipes d'assistance technique

Permet à l'utilisateur de créer ou de modifier des équipes d'assistance technique.

Modification d'un groupe de Jump : Autorisé à modifier les groupes de Jump

Permet à l'utilisateur de créer ou de modifier les groupe de Jump.

Modification de problème : Autorisé à modifier les problèmes

Permet à l'utilisateur de créer et de modifier des problèmes.

Modification de compétence : Autorisé à modifier les compétences

Permet à l'utilisateur de créer et de modifier des compétences.

Bouton assistance technique Modification de profil : Autorisé à modifier les profils Bouton assistance technique

Permet à l'utilisateur de personnaliser les profils de Bouton assistance technique.

Modification de script prédéfini : Autorisé à modifier les scripts prédéfinis

Permet à l'utilisateur de créer ou de modifier des scripts prédéfinis en vue de les utiliser dans des sessions de partage d'écran ou d'interpréteur de commandes.

Modification de lien personnalisé de technicien d'assistance : Autorisé à modifier les liens de technicien d'assistance personnalisés

Permet à l'utilisateur de créer ou de modifier des liens personnalisés.

Modification de parrain d'accès : Autorisé à modifier les parrains d'accès

Permet à l'utilisateur de créer ou de modifier des équipes de parrains d'accès.

Modification de profil iOS : Autorisé à modifier les profils iOS

Permet à l'utilisateur de créer, modifier et envoyer du contenu d'un profil Apple iOS pour le distribuer aux utilisateurs d'appareils iOS.

Rapport en cours

Accès aux sessions et rapports d'équipe : Autorisé à consulter les rapports : Session d'assistance technique

Permet à l'utilisateur d'établir des rapports sur l'activité de session d'assistance technique, en visualisant uniquement les sessions pour lesquelles il était le technicien d'assistance principal, les sessions où l'une de ses équipes était l'équipe principale ou l'un des membres de son équipe était le technicien d'assistance principal, ou toutes les sessions.

Accès aux sessions et rapports d'équipe : Autorisé à voir les enregistrements de session d'assistance technique

Permet à l'utilisateur d'afficher les enregistrements vidéo des sessions de partage d'écran, des sessions Montrer mon écran et des sessions d'interpréteur de commandes.

Accès aux rapports sur l'utilisation des licences : :Autorisé à consulter les rapports sur l'utilisation des licences

Permet à l'utilisateur d'établir des rapports sur l'utilisation des licences BeyondTrust.

Accès aux rapports Vault : Autorisé à consulter les rapports Vault

Permet à l'utilisateur de lancer des rapports sur l'activité de Vault, de voir toutes les données d'événement ou seulement ses propres données.

Accès aux rapports sur la présentation : Autorisé à consulter les rapports sur les sessions de présentation

Permet à l'utilisateur d'établir des rapports sur l'activité de présentation, en visualisant uniquement les présentations dans lesquelles il était le présentateur, un autre membre de son équipe était le présentateur, ou toutes les présentations.

Accès API

Accès à l'API de rapport : Autorisé à utiliser les rapports API

Permet d'utiliser les informations d'authentification de l'utilisateur pour extraire des rapports XML via l'API.

Pour plus d'informations, consultez le guide de l'API de rapport à l'adresse https://www.beyondtrust.com/docs/remote-support/how-to/integrations/api/reporting/index.htm.

***Remarque :** il est préférable d'utiliser les comptes API créés dans **Gestion > Configuration de l'API**.*

Accès à l'API de commande : Autorisé à utiliser les API de commande

Permet d'utiliser les informations d'authentification de l'utilisateur pour exécuter des commandes via l'API.

Pour plus d'informations, consultez le guide de l'API de commande à l'adresse https://www.beyondtrust.com/docs/remote-support/how-to/integrations/api/command/index.htm.

***Remarque :** il est préférable d'utiliser les comptes API créés dans **Gestion > Configuration de l'API**.*

Accès API temps réel : Autorisé à utiliser l'API d'état en temps réel

Permet d'utiliser les informations d'authentification de l'utilisateur pour extraire des données en utilisant l'API d'état en temps réel.

Pour plus d'informations, veuillez consulter la section API d'état en temps réel à l'adresse https://www.beyondtrust.com/docs/remote-support/how-to/integrations/api/real-time-state/index.htm.

Autorisations du technicien d'assistance

Autorisé à fournir une assistance technique à distance

Permet à l'utilisateur d'utiliser la console du technicien d'assistance pour exécuter une session d'assistance technique. Si l'assistance technique est activée, les options appartenant à l'assistance à distance seront également disponibles. Désactivez ce paramètre pour les utilisateurs uniquement autorisés à effectuer des présentations.

Gestion de session

Autorisé à générer des clés de session pour toute session d'assistance technique au sein de la console du technicien d'assistance

Permet à l'utilisateur de générer des clés de session en vue d'autoriser les utilisateurs à démarrer des sessions directement avec lui.

> *Pour plus d'informations, veuillez consulter Génération d'une clé de session en vue de démarrer une session d'assistance technique à l'adresse https://www.beyondtrust.com/docs/remote-support/getting-started/rep-console/session-keys.htm.*

Autorisé à générer des clés d'accès pour envoyer des profils iOS

Permet à l'utilisateur de générer des clés d'accès pour offrir du contenu iOS aux utilisateurs d'appareils iOS.

> *Pour plus d'informations, veuillez consulter Génération d'une clé d'accès au profil Apple iOS à l'adresse https://www.beyondtrust.com/docs/remote-support/getting-started/rep-console/apple-ios-access-key-management-interface.htm.*

Autorisé à accepter manuellement des sessions d'une file d'attente d'équipe

Permet à l'utilisateur de sélectionner et de démarrer des sessions qui se trouvent dans l'une des files d'attente de son équipe.

> *Pour plus d'informations, veuillez consulter Acceptation d'une session pour démarrer l'assistance technique à l'adresse https://www.beyondtrust.com/docs/remote-support/getting-started/rep-console/accepting-a-session.htm.*

Autorisé à transférer les sessions aux équipes auxquelles il n'appartient pas

Permet à l'utilisateur de transférer des sessions vers d'autres équipes que la sienne. Si elle est désactivée, l'interaction d'utilisateur est limitée aux équipes qui lui ont été attribuées.

> *Pour plus d'informations, veuillez consulter la section Vue d'ensemble des sessions d'assistance technique et outils à l'adresse https://www.beyondtrust.com/docs/remote-support/getting-started/rep-console/support-session-overview.htm.*

Autorisé à partager les sessions avec des équipes auxquelles il n'appartient pas

Permet à l'utilisateur d'inviter un ensemble moins limité d'utilisateurs pour partager des sessions, pas seulement des membres de son équipe. Combinée à la permission de disponibilité étendue, cette permission développe les capacités de partage de session.

> *Pour plus d'informations, veuillez consulter la section Vue d'ensemble des sessions d'assistance technique et outils à l'adresse https://www.beyondtrust.com/docs/remote-support/getting-started/rep-console/support-session-overview.htm.*

Autorisé à inviter des techniciens service client externes

Permet à l'utilisateur d'inviter un utilisateur tiers à participer à une session d'assistance technique de manière ponctuelle.

> *Pour plus d'informations, veuillez consulter la section Inviter un technicien d'assistance externe à rejoindre une session à l'adresse https://www.beyondtrust.com/docs/remote-support/getting-started/rep-console/rep-invite.htm.*

Autorisé à utiliser la fonctionnalité Obtenir session suivante

Permet à l'utilisateur de prendre en charge la plus ancienne session de toutes ses équipes placée dans la file d'attente, en cliquant simplement sur un bouton.

> *Pour plus d'informations, veuillez consulter Acceptation d'une session pour démarrer l'assistance technique à l'adresse https://www.beyondtrust.com/docs/remote-support/getting-started/rep-console/accepting-a-session.htm.*

Autorisé à activer le mode disponibilité étendue

Permet à l'utilisateur de recevoir des invitations par e-mail de la part d'autres utilisateurs demandant de partager une session, même lorsqu'il n'est pas connecté à la console du technicien d'assistance.

> *Pour plus d'informations, consultez la section Utiliser la disponibilité étendue pour rester accessible lorsque vous n'êtes pas connecté à l'adresse https://www.beyondtrust.com/docs/remote-support/getting-started/rep-console/extended-availability.htm.*

Autorisé à modifier la clé externe

Permet à l'utilisateur de modifier la clé externe depuis le volet d'informations d'une session dans la console du technicien d'assistance.

> *Pour plus d'informations, veuillez consulter la section Vue d'ensemble des sessions d'assistance technique et outils à l'adresse https://www.beyondtrust.com/docs/remote-support/getting-started/rep-console/support-session-overview.htm.*

Equilibrium

Pour plus d'informations, veuillez consulter Equilibrium pour l'acheminement automatique de session à l'adresse https://www.beyondtrust.com/docs/remote-support/how-to/equilibrium/index.htm.

Autorisé à refuser les attributions de session

Permet au technicien d'assistance de se définir comme non disponible pour les sessions attribuées via Equilibrium.

Ne pas attribuer de sessions si le technicien d'assistance participe à au moins

Définit le nombre minimal de sessions auxquelles le technicien d'assistance doit assister avant que les sessions ne soient plus automatiquement attribuées via Equilibrium.

Ne pas attribuer de sessions si le technicien d'assistance est inactif depuis au moins

Définit la période minimale pendant laquelle le technicien d'assistance doit avoir été inactif pour que les sessions ne soient plus automatiquement attribuées via Equilibrium.

Partage d'écran entre techniciens d'assistance

Pour plus d'informations, veuillez consulter Partager votre écran avec un autre technicien d'assistance à l'adresse https://www.beyondtrust.com/docs/remote-support/getting-started/rep-console/representative-screensharing.htm.

Autorisé à montrer son écran aux autres techniciens d'assistance

Permet à l'utilisateur de partager son écran avec un autre utilisateur sans que l'utilisateur récepteur ait besoin de rejoindre une session. Cette option est disponible même si l'utilisateur n'est pas dans une session.

Autorisé à accorder le contrôle lorsqu'il montre son écran à d'autres techniciens d'assistance

Permet à l'utilisateur partageant son écran d'accorder le contrôle de son clavier et de sa souris à l'utilisateur regardant son écran.

Bouton assistance techniques

Pour plus d'informations, veuillez consulter la section Vue d'ensemble des sessions d'assistance technique et outils à l'adresse https://www.beyondtrust.com/docs/remote-support/getting-started/rep-console/support-session-overview.htm.

Autorisé à déployer et gérer tout Bouton assistance technique dans une file d'attente personnelle

Permet à l'utilisateur de déployer et de gérer tout Bouton assistance technique personnel. Ce paramètre affecte le déploiement de tout Bouton assistance technique depuis l'interface Web et la console du technicien d'assistance. Pour pouvoir déployer un Bouton assistance

technique à partir d'une session, l'autorisation de session **Déploiement de Bouton assistance technique** doit également être activée.

Autorisé à gérer tout Bouton assistance technique d'équipe

Autorise l'utilisateur à modifier tout Bouton assistance technique déployé dans les équipes dont il fait partie. Si l'utilisateur est le chef ou le responsable de l'équipe, il peut aussi modifier tout Bouton assistance technique personnel de n'importe quel membre.

> *Pour plus d'informations, veuillez consulter Gestion de Bouton assistance technique à l'adresse https://www.beyondtrust.com/docs/remote-support/getting-started/rep-console/support-button-management-interface.htm.*

Autorisé à modifier le portail public associé à tout Bouton assistance technique

Permet à l'utilisateur de définir le portail public qu'un Bouton assistance technique doit utiliser pour se connecter. Dans la mesure où les portails publics peuvent faire l'objet de règles de session, toute modification du portail peut affecter les autorisations associées à la session.

Autorisé à déployer chaque Bouton assistance technique d'équipe

Permet à l'utilisateur de déployer un Bouton assistance technique d'équipe pour les équipes dont il fait partie. Ce paramètre affecte le déploiement de tout Bouton assistance technique depuis l'interface Web et la console du technicien d'assistance. Pour pouvoir déployer un Bouton assistance technique à partir d'une session, l'autorisation de session **Déploiement de Bouton assistance technique** doit également être activée.

Technologie Jump

Méthodes de Jump autorisées

Permet à l'utilisateur d'effectuer un Jump vers des ordinateurs en utilisant les méthodes de **Jump Clients**, **Jump local**, **VNC local**, **RDP local**, **Jump distant**, **VNC distant**, **RDP distant**, **Shell Jump** et/ou **Intel vPro**.

Rôles d'élément de Jump

Le rôle d'élément de Jump est un ensemble prédéfini d'autorisations relatives à la gestion et à l'utilisation d'un élément de Jump. Pour chaque option, cliquez sur le bouton **Modifier** pour ouvrir le rôle d'élément de Jump dans un nouvel onglet.

Le rôle **Par défaut** n'est utilisé que lorsque **Utiliser les paramètres par défaut de l'utilisateur** est défini pour cet utilisateur dans un groupe de Jump.

Le rôle **Personnel** ne s'applique qu'aux éléments de Jump attachés à la liste personnelle d'éléments de Jump d'un utilisateur.

Le rôle **Équipe** ne s'applique qu'aux éléments de Jump attachés à la liste personnelle d'éléments de Jump d'un membre de l'équipe doté d'un rôle inférieur. Ainsi, un chef d'équipe peut visualiser les éléments de Jump d'un responsable ou d'un membre de son équipe, et un responsable d'équipe peut visualiser les éléments de Jump personnels d'un membre de son équipe.

Le rôle **Système** s'applique au reste des éléments de Jump du système. Pour la plupart des utilisateurs, ce rôle est en principe défini sur **Aucun accès**. S'il est défini sur une autre option, l'utilisateur est ajouté à des groupes de Jump auxquels il ne devrait pas être assigné, et, dans la console du technicien d'assistance, il est en mesure de visualiser la liste personnelle d'éléments de Jump de membres n'appartenant pas à son équipe.

> *Pour plus d'informations, veuillez consulter Utiliser les rôles d'éléments de Jump pour créer des groupes d'autorisations pour les Jump Clients à l'adresse https://www.beyondtrust.com/docs/remote-support/how-to/jump-clients/jump-item-roles.htm.*

Présentation

Autorisé à effectuer des présentations

Permet au technicien d'assistance d'effectuer des présentations à l'intention d'un ou de plusieurs participants.

> *Pour plus d'informations, veuillez consulter Réaliser une présentation pour des participants distants à l'adresse https://www.beyondtrust.com/docs/remote-support/getting-started/rep-console/presentation.htm.*

Autorisé à accorder le contrôle à un participant de la présentation

Permet au technicien d'assistance d'accorder le contrôle de son ordinateur à un participant au cours d'une présentation. Ce paramètre affecte uniquement les présentations et n'a aucun impact sur la fonction Montrer mon écran d'une session d'assistance technique. Un seul participant à la fois peut avoir le contrôle. Le technicien d'assistance conserve le contrôle du remplacement.

> *Pour plus d'informations, veuillez consulter la section Client de participant à une présentation : Rejoindre une présentation à l'adresse https://www.beyondtrust.com/docs/remote-support/getting-started/customer-client/customer-presentation-interface.htm.*

Console du technicien d'assistance

Délai d'inactivité

Définissez le délai pendant lequel le technicien d'assistance peut être inactif avant d'être déconnecté de la console du technicien d'assistance. Cette autorisation peut utiliser le paramètre défini pour le site ou peut remplacer ce paramètre.

Autorisations relatives aux sessions autonomes et non autonomes

Règles de sessions surveillées et sans surveillance

Règle de session

Définissez les règles de demande et d'autorisation devant s'appliquer aux sessions de cet utilisateur. Sélectionnez une règle de session existante ou définissez des autorisations personnalisées pour cet utilisateur. Notez que l'option **Non défini** entraîne l'utilisation de la règle globale par défaut. Ces autorisations peuvent être remplacées par une règle de niveau supérieur.

Utiliser les mêmes autorisations pour les sessions non autonomes

Pour utiliser les mêmes autorisations pour les sessions autonomes et les sessions non autonomes, cochez la case **Utiliser les mêmes autorisations pour les sessions non autonomes**. Décochez cette case si vous souhaitez définir des autorisations distinctes pour les sessions autonomes et les sessions non autonomes. Vous pouvez également copier les autorisations d'un type de session à l'autre.

Description

Affichez la description d'une règle de permission de session prédéfinie.

Demande d'outil d'assistance technique

Pour en savoir plus, veuillez consulter Client d'utilisateur : Interface de session d'assistance technique à l'adresse https://www.beyondtrust.com/docs/remote-support/getting-started/customer-client/customer-support-interface.htm.

Règles de demande

Vous pouvez choisir de demander à l'utilisateur l'autorisation d'utiliser les fonctions d'assistance technique ci-après. Sélectionnez **Aucune demande** pour ne jamais envoyer de demande, **Toujours demander** pour toujours envoyer une demande ou **Demander pour certains outils** pour choisir les autorisations pour lesquelles envoyer une demande. Lorsque l'option **Demander pour certains outils** est sélectionnée, l'option **Demander l'accord de l'utilisateur** apparaît en dessous de chaque outil, avec les choix **Jamais** et **Toujours**. En cas de sélection de **Non défini**, cette option est définie par la règle de priorité inférieure suivante. Ce réglage peut être remplacé par une règle de priorité supérieure.

Autorisé à demander une fois

Si l'option **Partage d'écran** est définie sur **Voir et contrôler** et que l'envoi de demandes est activé, cette option est disponible. Cochez cette case pour permettre à la fonction de partage d'écran d'accéder à tous les outils au cours de la session, sans demande supplémentaire.

Options de demande

Définissez le délai d'attente de réponse à une demande avant l'envoi de la réponse par défaut **Refuser** ou **Autoriser**. En cas de sélection de **Non défini**, cette option est définie par la règle de priorité inférieure suivante. Ce réglage peut être remplacé par une règle de priorité supérieure.

Partage d'écran

Règles de partage d'écran

Permet à l'utilisateur de voir ou de contrôler l'écran distant. En cas de sélection de **Non défini**, cette option est définie par la règle de priorité inférieure suivante. Ce réglage peut être remplacé par une règle de priorité supérieure.

Pour plus d'informations, veuillez consulter la section Partage d'écran avec l'utilisateur distant à des fins de consultation et de contrôle à l'adresse https://www.beyondtrust.com/docs/remote-support/getting-started/rep-console/screen-sharing.htm.

Autorisé à montrer son écran à l'utilisateur

Permet à l'utilisateur de partager son écran avec le client au cours d'une session d'assistance technique.

> *Pour plus d'informations, veuillez consulter la section Montrer mon écran : Inversion du partage d'écran à l'adresse https://www.beyondtrust.com/docs/remote-support/getting-started/customer-client/show-my-screen.htm.*

Restrictions d'utilisateur autorisées

Définissez si l'utilisateur peut interrompre l'entrée souris et clavier du système distant. L'utilisateur peut aussi empêcher l'affichage du bureau distant.

> *Pour plus d'informations, veuillez consulter la section Interaction client restreinte : Écran de confidentialité et désactivation de l'entrée de l'utilisateur distant à l'adresse https://www.beyondtrust.com/docs/remote-support/getting-started/customer-client/privacy-screen.htm.*

Comportement de demande de partage d'applications

Déterminez si une demande de partage d'écran ne doit jamais ou toujours faire l'objet d'une demande auprès du client pour sélectionner les applications à partager, ou si l'utilisateur peut choisir de faire une demande de partage d'applications ou non. Sélectionner **Toujours** ou **Décision du technicien d'assistance** vous permet aussi de prédéfinir les restrictions de partage d'application.

> *Pour plus d'informations, veuillez consulter la section Partage d'application : Restriction des éléments visibles par le technicien d'assistance à l'adresse https://www.beyondtrust.com/docs/remote-support/getting-started/customer-client/application-sharing.htm.*

Sens de synchronisation du presse-papiers

Sélectionnez la manière dont le contenu du presse-papiers circule entre les techniciens d'assistance et les utilisateurs finaux. Les options sont :

- **Non autorisé :** Le technicien d'assistance n'est pas autorisé à utiliser le presse-papiers, aucune icône de presse-papiers ne s'affiche dans la console du technicien d'assistance et les commandes couper-coller ne fonctionnent pas.
- **Autorisé du technicien d'assistance vers l'utilisateur :** Le technicien d'assistance peut envoyer le contenu du presse-papiers au client, mais ne peut pas le coller à partir du presse-papiers de l'utilisateur final. Seule l'icône Envoyer le presse-papiers s'affiche dans la console du technicien d'assistance.
- **Envoyer dans les deux sens :** Le contenu du presse-papiers peut circuler dans les deux sens. Les icônes du presse-papiers Envoyer et Obtenir s'affichent dans la console du technicien d'assistance.

> *Pour plus d'informations sur le Mode de synchronisation du presse-papiers, veuillez consulter « Sécurité : Gestion des paramètres de sécurité », page 205 de sécurité.*

Partage de navigateur

Règles de partage de navigateur

Permet à l'utilisateur de consulter la même page Web que le client regarde, sans avoir le contrôle et sans voir d'autres applications. En cas de sélection de **Non défini**, cette option est définie par la règle de priorité inférieure suivante. Ce réglage peut être remplacé par une règle de priorité supérieure.

> *Pour plus d'informations, veuillez consulter la section Partage d'écran avec l'utilisateur distant à des fins de consultation et de contrôle à l'adresse https://www.beyondtrust.com/docs/remote-support/getting-started/rep-console/screen-sharing.htm.*

Annotations

Règles d'annotation

Permet à l'utilisateur d'utiliser les outils d'annotation pour dessiner sur l'écran du système distant. En cas de sélection de **Non défini**, cette option est définie par la règle de priorité inférieure suivante. Ce réglage peut être remplacé par une règle de priorité supérieure.

> *Pour plus d'informations, veuillez consulter la section Utiliser les annotations pour dessiner sur l'écran distant à l'adresse https://www.beyondtrust.com/docs/remote-support/getting-started/rep-console/annotations.htm.*

Transfert de fichiers

Règles de transfert de fichiers

Permet à l'utilisateur d'envoyer des fichiers vers le système distant, de télécharger des fichiers depuis le système distant, ou les deux. En cas de sélection de **Non défini**, cette option est définie par la règle de priorité inférieure suivante. Ce réglage peut être remplacé par une règle de priorité supérieure.

Chemins accessibles sur le système de fichiers de l'utilisateur

Permettre à l'utilisateur de transférer des fichiers de et vers n'importe quel répertoire sur le système distant ou uniquement les répertoires spécifiés.

Chemins accessibles sur le système de fichiers du technicien d'assistance

Permettre à l'utilisateur de transférer des fichiers de et vers n'importe quel répertoire sur son système local ou uniquement les répertoires spécifiés.

> *Pour plus d'informations, veuillez consulter la section Transfert de fichiers vers et depuis le système distant à l'adresse https://www.beyondtrust.com/docs/remote-support/getting-started/rep-console/file-transfer.htm.*

Interpréteur de commandes

Règles de l'interpréteur de commandes

Permet à l'utilisateur de saisir des commandes sur l'ordinateur distant par l'intermédiaire d'une interface en ligne de commande virtuelle. En cas de sélection de **Non défini**, cette option est définie par la règle de priorité inférieure suivante. Ce réglage peut être remplacé par une règle de priorité supérieure.

Remarque : *l'accès à l'interpréteur de commandes ne peut pas être restreint lors de sessions de Shell Jump.*

Pour plus d'informations, veuillez consulter la section Accès à l'interpréteur de commandes distant à l'adresse https://www.beyondtrust.com/docs/remote-support/getting-started/rep-console/command-shell.htm.

Informations système

Règles relatives aux informations système

Permet à l'utilisateur de consulter les informations système de l'ordinateur distant. En cas de sélection de **Non défini**, cette option est définie par la règle de priorité inférieure suivante. Ce réglage peut être remplacé par une règle de priorité supérieure.

Autorisé à utiliser les actions relatives aux informations système

Permet à l'utilisateur d'interagir avec les processus et les programmes sur le système distant sans avoir recours au partage d'écran. Le technicien d'assistance peut ainsi désinstaller des programmes, supprimer des processus ou encore démarrer, arrêter, mettre en pause, reprendre et redémarrer des services.

Pour plus d'informations, veuillez consulter la section Consulter les informations du système distant à l'adresse https://www.beyondtrust.com/docs/remote-support/getting-started/rep-console/system-info.htm.

Accès au registre

Règles d'accès au registre

Permet à l'utilisateur d'agir sur le registre d'un système Windows distant sans avoir recours au partage d'écran. Le technicien d'assistance peut ainsi afficher, ajouter, supprimer, modifier, rechercher et importer/exporter des clés.

Pour plus d'informations, veuillez consulter la section Accès à l'éditeur de registre distant à l'adresse https://www.beyondtrust.com/docs/remote-support/getting-started/rep-console/registry-editor.htm.

Scripts prédéfinis

Règles de script prédéfini

Permet à l'utilisateur d'exécuter des scripts prédéfinis créés pour ses équipes. Notez que lorsque l'utilisateur est en partage d'écran en mode affichage seul, le client reçoit une invite pour autoriser le lancement du script.En cas de sélection de **Non défini**, cette option est définie par la règle de priorité inférieure suivante. Ce réglage peut être remplacé par une règle de priorité supérieure.

> *Pour plus d'informations, veuillez consulter la section Accès à l'interpréteur de commandes distant à l'adresse https://www.beyondtrust.com/docs/remote-support/getting-started/rep-console/command-shell.htm.*

Accroissement des droits

Règles d'accroissement des droits

Permet à l'utilisateur de tenter d'accroître les droits du client d'utilisateur pour s'exécuter avec des droits administratifs sur le système distant. En cas de sélection de **Non défini**, cette option est définie par la règle de priorité inférieure suivante. Ce réglage peut être remplacé par une règle de priorité supérieure.

> *Pour plus d'informations, veuillez consulter la section Accroître le client à l'adresse https://www.beyondtrust.com/docs/remote-support/getting-started/rep-console/elevation.htm.*

Déploiement de Bouton assistance technique

Règles de déploiement de Bouton assistance technique

Permet à l'utilisateur de déployer ou de supprimer un Bouton assistance technique au cours d'une session. Les emplacements de déploiement possibles dépendent des paramètres de Bouton assistance technique ci-dessus. En cas de sélection de **Non défini**, cette option est définie par la règle de priorité inférieure suivante. Ce réglage peut être remplacé par une règle de priorité supérieure.

> *Pour plus d'informations, veuillez consulter la section Vue d'ensemble des sessions d'assistance technique et outils à l'adresse https://www.beyondtrust.com/docs/remote-support/getting-started/rep-console/support-session-overview.htm.*

Attachement/Détachement de Jump Clients

Règles d'attachement/détachement de Jump Clients

Permet à l'utilisateur d'attacher ou de détacher un Jump Client au cours d'une session. Les emplacements de déploiement possibles dépendent des paramètres de Jump Client précédents. En cas de sélection de **Non défini**, cette option est définie par la règle de priorité inférieure suivante. Ce réglage peut être remplacé par une règle de priorité supérieure.

Pour plus d'informations, veuillez consulter la section Vue d'ensemble des sessions d'assistance technique et outils à l'adresse https://www.beyondtrust.com/docs/remote-support/getting-started/rep-console/support-session-overview.htm.

Messagerie instantanée

Pour plus d'informations, veuillez consulter la section Messagerie instantanée avec un utilisateur lors d'une session à l'adresse https://www.beyondtrust.com/docs/remote-support/getting-started/rep-console/chat.htm.

Règles de messagerie instantanée

Permet à l'utilisateur de discuter avec le client distant. En cas de sélection de **Non défini**, cette option est définie par la règle de priorité inférieure suivante. Ce réglage peut être remplacé par une règle de priorité supérieure.

Autorisé à charger des URL dans le navigateur Web de l'utilisateur

Permet à l'utilisateur d'entrer une URL dans la zone de messagerie instantanée, puis de cliquer sur le bouton **Charger l'URL** pour ouvrir automatiquement un navigateur Web à cette adresse sur l'ordinateur distant.

Autorisé à envoyer des fichiers à l'aide de l'interface de messagerie instantanée

Permet à l'utilisateur d'envoyer des fichiers via l'interface de messagerie instantanée.

Pour en savoir plus, veuillez consulter Client d'utilisateur : Interface de session d'assistance technique à l'adresse https://www.beyondtrust.com/docs/remote-support/getting-started/customer-client/customer-support-interface.htm.

Paramètres de disponibilité

Quels paramètres de disponibilité cette règle de groupe doit-elle contrôler ?

Décidez si un paramètre doit être **Défini** dans cette règle. Dans l'affirmative, vous pouvez sélectionner **Final** pour empêcher des règles de priorité inférieure d'outrepasser la valeur d'autorisation définie par cette règle. Sélectionnez **Tout** pour définir tous les paramètres dans cette section.

Pool de licences d'assistance technique complète

Choisissez le pool de licences auquel ce technicien d'assistance doit appartenir. Lorsque ce technicien d'assistance se connecte à la console du technicien d'assistance, une licence est utilisée dans le pool de licences désigné. Si **Aucun** est sélectionné, le technicien d'assistance pourra se connecter à la console du technicien d'assistance seulement si une ou plusieurs licences non assignées à des pools de licences sont disponibles.

Planning de connexion

Restreindre la connexion du technicien d'assistance selon le planning suivant

Définissez un planning afin de déterminer les périodes pendant lesquelles les utilisateurs peuvent se connecter à la console du technicien d'assistance. Définissez le fuseau horaire à utiliser pour ce planning, puis ajoutez une ou plusieurs entrées de planification. Pour chaque entrée, indiquez l'heure et la date de début ainsi que l'heure et la date de fin.

Par exemple, si la période définie commence à 8 h et se termine à 17 h, un utilisateur peut se connecter à n'importe quel moment au cours de cette période et peut continuer à travailler passée l'heure de fin. Il ne sera toutefois pas autorisé à se reconnecter après 17 h.

Forcer la déconnexion lorsque le planning ne permet pas l'ouverture d'une session

Si un contrôle d'accès plus strict est requis, cochez cette option. Ceci force la déconnexion de l'utilisateur à l'heure de fin définie. Dans ce cas, l'utilisateur reçoit des notifications récurrentes à partir de 15 minutes avant d'être déconnecté. Lorsque l'utilisateur est déconnecté, toutes les sessions possédées suivront les règles de récupération.

Composition

Quels paramètres d'appartenance cette règle de groupe doit-elle contrôler ?

Décidez si un paramètre doit être **Défini** dans cette règle. Dans l'affirmative, vous pouvez sélectionner **Final** pour empêcher des règles de priorité inférieure d'outrepasser la valeur d'autorisation définie par cette règle. Sélectionnez **Tout** pour définir tous les paramètres dans cette section.

Ajouter une appartenance des équipes d'assistance technique

Lancez une recherche pour trouver les équipes auxquelles les membres de cette règle de groupe devraient appartenir. Vous pouvez définir les rôles **Membre de l'équipe**, **Chef d'équipe** ou **Responsable d'équipe**. Ces rôles représentent une part significative de la fonction **Tableau de bord** de la console du technicien d'assistance. Cliquez sur **Ajouter**.

Les équipes ajoutées figurent dans un tableau. Il est possible de modifier le rôle d'un membre d'une équipe ou de supprimer l'équipe de la liste.

Supprimer une appartenance des équipes d'assistance technique

Recherchez les équipes dont les membres de cette règle de groupe devraient être supprimés, puis cliquez sur **Ajouter**. Les équipes supprimées figurent dans un tableau. Il est possible de supprimer une équipe de la liste.

Ajouter une appartenance à un Jumpoint

Recherchez les Jumpoints auxquels les membres de cette règle de groupe devraient pouvoir accéder, puis cliquez sur **Ajouter**. Les Jumpoints ajoutés figurent dans un tableau. Il est possible de supprimer un Jumpoint de la liste.

Supprimer des appartenances à un Jumpoint

Recherchez les Jumpoints dont les membres de cette règle de groupe ne devraient pas être supprimés, puis cliquez sur **Ajouter**. Les Jumpoints supprimés figurent dans un tableau. Il est possible de supprimer un Jumpoint de la liste.

Ajouter des appartenances de groupe de Jump

Recherchez les groupes de Jump auxquels les membres de cette règle de groupe devraient appartenir. Il est possible de paramétrer le rôle d'élément de Jump de chaque utilisateur pour définir son type d'autorisation vis-à-vis des éléments de Jump dans ce groupe de Jump. Vous pouvez aussi utiliser les rôles d'élément de Jump par défaut de l'utilisateur définis dans cette règle de groupe ou sur la page **Utilisateurs et sécurité > Utilisateurs**. Le rôle d'élément de Jump est un ensemble prédéfini d'autorisations relatives à la gestion et à l'utilisation d'un élément de Jump.

> *Pour plus d'informations, reportez-vous à la section Rôles d'élément de Jump : configurer les groupes d'autorisation pour les éléments de Jump à l'adresse www.beyondtrust.com/docs/remote-support/getting-started/admin/jump-item-roles.htm.*

Vous pouvez aussi appliquer une règle de Jump pour gérer l'accès aux éléments de Jump dans ce groupe de Jump.

Les groupe de Jump ajoutés figurent dans un tableau. Il est possible de modifier les paramètres d'un groupe de Jump ou de supprimer le groupe de Jump de la liste.

Supprimer des appartenances de groupe de Jump

Recherchez les groupes de Jump dont les membres de cette règle de groupe devraient être supprimés, puis cliquez sur **Ajouter**. Les groupe de Jump supprimés figurent dans un tableau. Il est possible de supprimer un groupe de Jump de la liste.

Ajouter des appartenances à un compte Vault

Recherchez un compte, sélectionnez le **Rôle de compte de Vault**, puis cliquez sur **Ajouter** pour accorder aux membres de la règle l'accès au compte de Vault sélectionné. Les utilisateurs peuvent voir leurs appartenances ajoutées par d'autres règles de groupe. Consultez **Vault > Comptes** pour voir tous les membres de chaque groupe. Les utilisateurs peuvent assigner aux comptes Vault l'un des deux rôles :

- **Injecter** (valeur par défaut) : Les utilisateurs dotés de ce rôle peuvent utiliser ce compte dans des sessions Remote Support.
- **Injecter et extraire** : Les utilisateurs dotés de ce rôle peuvent utiliser ce compte dans des sessions Remote Support et peuvent extraire le compte sur **/login**. L'autorisation d'**extraction** n'a pas d'effet sur les comptes génériques SSH.

> ***Remarque :** activez l'autorisation **Ajouter des appartenances à un compte Vault** pour assigner un **rôle de compte Vault** à un compte Vault dans une règle de groupe. Le **rôle de compte Vault** est visible dans la liste des comptes ajoutés à la règle de groupe.*

Ajouter des appartenances à un groupe de comptes Vault

Recherchez un groupe de comptes, sélectionnez le **Rôle de compte Vault** puis cliquez sur **Ajouter** pour accorder aux membres de la règle l'accès au groupe de comptes Vault. Les utilisateurs peuvent voir leurs appartenances ajoutées par d'autres règles de groupe. Consultez **Vault > Comptes** pour voir tous les membres de chaque groupe. Les utilisateurs peuvent assigner au groupe de comptes Vault l'un des deux rôles :

- **Injecter** (valeur par défaut) : Les utilisateurs dotés de ce rôle peuvent utiliser ce compte dans des sessions Remote Support.
- **Injecter et extraire** : Les utilisateurs dotés de ce rôle peuvent utiliser ce compte dans des sessions Remote Support et peuvent extraire le compte sur **/login**. L'autorisation d'**extraction** n'a pas d'effet sur les comptes génériques SSH.

> ***Remarque :*** *activez l'autorisation* ***Ajouter un groupe de comptes Vault*** *pour assigner un* ***Rôle de compte Vault*** *à un groupe de comptes Vault dans une règle de groupe. Le* ***rôle de compte Vault*** *est visible dans la liste des groupes de comptes ajoutés à la règle de groupe.*

Exporter la règle

Vous pouvez exporter une règle de groupe à partir d'un site et importer ces autorisations dans une règle sur un autre site. Modifiez la règle que vous souhaitez exporter et faites défiler jusqu'au bas de la page. Cliquez sur **Exporter la règle** et enregistrez le fichier.

> ***Remarque :*** *lors de l'exportation d'une règle de groupe, seuls le nom de la règle, les paramètres du compte et les autorisations sont exportés. Les membres de la règle, les appartenances à des équipes et des Jumpoints ne sont pas inclus dans l'exportation.*

Importer une règle

Vous pouvez importer des paramètres de règles de groupe exportés dans les autres sites BeyondTrust prenant en charge l'importation de règles de groupe. Créez une nouvelle règle de groupe ou modifiez une règle existante dont vous souhaitez remplacer les autorisations, et faites défiler jusqu'au bas de la page. Naviguez jusqu'au fichier de la règle, puis cliquez sur **Sélectionner un fichier de règle**. Une fois le fichier de la règle chargé, la page s'actualisera pour vous permettre d'effectuer des modifications. Cliquez sur **Enregistrer** pour mettre en application la règle de groupe.

> ***Remarque :*** *l'importation d'un fichier de règle dans une règle de groupe existante remplacera toutes les autorisations précédemment définies, sauf les membres de la règle, et les appartenances à des équipes et des Jumpoints.*

Keytab Kerberos : gestion du keytab Kerberos

Gestion du keytab Kerberos

BeyondTrust prend en charge une fonctionnalité d'authentification unique au moyen du protocole d'authentification Kerberos. Cela permet aux utilisateurs de s'authentifier sur le Serveur d'accès à distance sécurisé sans avoir à entrer leurs informations d'authentification. L'authentification Kerberos s'applique à la fois à l'interface Web /login et à la console du technicien d'assistance.

Pour intégrer Kerberos à votre Serveur d'accès à distance sécurisé, Kerberos doit avoir été déployé ou être en cours de déploiement. Les conditions requises sont les suivantes :

- Vous devez avoir un centre de distribution de clés (KDC) opérationnel.
- Les horloges doivent être synchronisées sur tous les clients, le KDC et le Serveur d'accès à distance sécurisé. L'utilisation d'un serveur NTP (Network Time Protocol) est un moyen facile d'y parvenir.
- Vous devez avoir créé un nom principal du service (SPN) sur le KDC pour votre Serveur d'accès à distance sécurisé.

Noms principaux configurés

La section **Noms principaux configurés** répertorie tous les SPN disponibles pour chaque keytab transféré.

Une fois que des SPN sont disponibles, vous pouvez configurer un fournisseur de sécurité Kerberos depuis la page **Fournisseurs de sécurité** et définir les principaux utilisateurs pouvant s'authentifier sur le Serveur d'accès à distance sécurisé via Kerberos.

Importer un keytab

Choisir le fichier

Exportez le keytab pour le SPN depuis votre KDC et chargez-le sur le Serveur d'accès à distance sécurisé.

> *Pour plus d'informations, veuillez consulter la section Serveur Kerberos pour authentification unique à l'adresse https://www.beyondtrust.com/docs/remote-support/how-to/integrations/security-providers/kerberos/index.htm.*

Licences : assigner des techniciens d'assistance à des pools de licences

Pools de licences d'assistance technique complète

Configurez des pools de licence pour refléter la structure de votre organisation d'assistance technique et veillez à ce que chaque pool dispose du nombre de licences exact qui lui est accordé. Le tableau montre le nombre de licences réservées et le nombre maximum de licences autorisé pour chaque pool, ainsi que le nombre d'utilisateurs affectés à ce pool. Notez que ce nombre ne reflète pas les utilisateurs affectés par une règle de groupe ou les techniciens d'assistance invités.

Ajouter, modifier, supprimer

Créer un nouveau pool, modifier un pool existant ou supprimer un pool existant.

Ajouter ou modifier le pool de licences d'assistance technique complète

Nom

Créez un nom unique permettant d'identifier ce pool. Ce nom doit aider les administrateurs à affecter des utilisateurs ou des groupes à un pool de licences.

Description

Ajoutez une brève description pour résumer la fonction de ce pool.

Licences réservées

Le nombre de licences devant être réservées pour ce pool. Si toutes les autres licences sont utilisées et qu'un technicien qui ne fait pas partie du pool tente de se connecter sur la console du technicien d'assistance, la connexion lui sera refusée. La note ci-dessous montre combien de licences non réservées sont encore disponibles et peuvent être affectées.

Nombre maximal de licences

Le nombre maximum de licences pouvant être utilisées par les utilisateurs de ce pool. Si le nombre maximum de licences est déjà utilisé par les utilisateurs de ce pool et qu'un autre technicien faisant partie de ce pool tente de se connecter à la console du technicien d'assistance, la connexion lui sera refusée. Si vous ne souhaitez pas définir un maximum, cochez **Illimitée**.

Pool de licences dédiées aux techniciens d'assistance invités

Mêmes autorisations que le technicien d'assistance hôte

Lorsqu'un technicien d'assistance envoie une invitation d'un technicien d'assistance à un technicien externe, le technicien invité devra utiliser une licence du même pool que le technicien d'assistance qui a envoyé la demande.

Utiliser le pool suivant pour tous les techniciens d'assistance invités

Lorsqu'un technicien d'assistance envoie une invitation d'un technicien d'assistance à un technicien externe, le technicien invité devra utiliser une licence du pool spécifié. Si cette option est définie sur **Aucun**, la licence utilisée sera choisie parmi les licences non réservées.

Notification d'utilisation des licences

Activer des alertes sur seuil de licences

Recevez un e-mail lorsque le nombre de licences en cours d'utilisation atteint le seuil défini ci-dessous.

Options relatives aux alertes sur seuil de licences

Définissez le seuil de licence pour un nombre total ou un pourcentage de licences en cours d'utilisation. Définissez le délai minimum devant s'écouler avant qu'un autre e-mail puisse être envoyé.

Activer les alertes de refus de connexion

Si cette option est cochée, une alerte est envoyée par e-mail chaque fois qu'un technicien d'assistance ne parvient pas à se connecter en raison d'un nombre insuffisant de licences, d'emplacements réservés ou que la limite maximum de licences a été atteinte.

Contact pour les alertes de licences

Saisissez une ou plusieurs adresses auxquelles les e-mails doivent être envoyés. Séparez les adresses avec une espace. Cette fonction nécessite une configuration SMTP valide pour votre serveur, qui s'effectue sur la page **/login > Gestion > Configuration e-mail**.

Rapports

Assistance technique : faire un rapport sur l'activité des sessions

Rapports d'assistance technique

Les administrateurs et les utilisateurs avec privilèges peuvent générer de vastes rapports exhaustifs et appliquer des filtres spécifiques en vue de personnaliser les informations contenues dans les rapports en fonction des besoins précis.

Type de rapport

Générez des rapports d'activité d'après quatre types de rapports distincts : **Session**, **Résumé**, **Enquête de satisfaction de l'utilisateur** et **Enquête de satisfaction du technicien d'assistance**.

Filtres

Appliquez des options de filtre selon les besoins en vue de générer des rapports encore plus personnalisés à partir des types de rapport de base. Activez un ou plusieurs filtres selon vos désirs, mais seules les sessions qui correspondent à tous les filtres sélectionnés s'afficheront.

Identifiant de session ou numéro de séquence

Cet identificateur unique exige que vous indiquiez l'identifiant (LSID) ou le numéro de séquence pour la session unique que vous recherchez. Ceci est souvent utile si vous possédez un système de tickets externe ou une intégration GRC. Vous ne pouvez pas combiner ce filtre à un autre.

Période

Sélectionnez une date de début pour l'extraction de données de rapport. Sélectionnez ensuite le nombre de jours pour lequel extraire votre rapport, ou une date de fin.

Utilisateur

Filtrez les sessions par nom d'utilisateur, nom de l'entreprise, nom de l'ordinateur, adresse IP publique ou adresse IP privée.

Site public

Filtrez pour axer votre rapport sur un site public donné.

Technicien d'assistance

Utilisez le menu déroulant pour choisir le type de participation du technicien d'assistance que vous souhaitez inclure. Choisissez des sessions où un technicien d'assistance a rejoint, aucun technicien d'assistance n'a rejoint, ou un technicien d'assistance spécifique a participé, ou n'importe quel technicien d'assistance d'une équipe a participé, y compris des sessions qui n'ont jamais été associées à l'équipe spécifiée.

Équipe

Utilisez le menu déroulant pour choisir le type de participation de l'équipe que vous souhaitez inclure. Choisissez des sessions qui ont été assignées à au moins une équipe, des sessions qui n'ont jamais été assignées à une équipe, ou des sessions qui ont été assignées à une équipe spécifique.

Clé externe

Filtrez pour rapporter des sessions qui ont utilisé la même clé externe donnée.

N'inclure que les sessions terminées

Filtrez pour inclure uniquement les sessions qui ont été terminées. Ceci exclut les sessions toujours en cours.

Regrouper par *(Visible seulement pour les rapports récapitulatifs)*

Choisissez de regrouper les données des rapports récapitulatifs par technicien d'assistance, par équipe ou par site public.

Résultats de rapport de Session d'assistance technique

Afficher toutes les sessions qui correspondent aux critères spécifiés sur la page précédente. Les rapports de session comprennent des informations de session de base, ainsi que des liens vers les détails de session, les transcriptions de la messagerie instantanée, et les enregistrements vidéo des sessions de partage d'écran, des sessions Montrer mon écran et des sessions d'interpréteur de commandes. Cliquez sur **Choisir les colonnes visibles** pour choisir les informations à afficher.

Détails sur la Session d'assistance technique

Les rapports de session détaillent la transcription complète de la discussion, le nombre de fichiers transférés et les permissions demandées et accordées. D'autres informations incluent le site public via lequel la session a été exécutée, la durée de la session, le nom et l'adresse IP des ordinateurs locaux et distants, et les informations sur le système distant (le cas échéant). Les rapports peuvent être consultés en ligne ou être téléchargés sur le système local.

Si l'enregistrement de session est activé, lisez une vidéo des sessions individuelles, avec une annotation précisant qui contrôlait la souris et le clavier à tout moment au cours de la session. De même, si l'enregistrement de la fonction Montrer mon écran est activé, vous pouvez afficher et télécharger des vidéos du système du technicien d'assistance pendant une session Montrer mon écran. Si l'enregistrement de l'invite de commande est activé, vous pouvez également visionner les enregistrements de tous les interpréteurs de commandes qui ont été exécutés pendant la session. Tous les enregistrements sont conservés sur le Serveur d'accès à distance sécurisé dans un format brut et sont convertis dans un format compressé lors du visionnage ou du téléchargement.

Rapport récapitulatif

Les rapports récapitulatifs fournissent une vision d'ensemble de l'activité pendant une certaine période, classée par technicien d'assistance, équipe ou site public. Les statistiques regroupent le nombre total de sessions exécutées, le nombre moyen de sessions par jour de la semaine et leur durée moyenne.

Rapport d'enquête de satisfaction de l'utilisateur ou d'enquête de satisfaction du technicien d'assistance

Afficher les rapports sur les réponses à vos enquêtes personnalisées, délimitées par site public. Une colonne est ajoutée pour chaque question que vous incluez à vos enquêtes. Elle est intitulée en fonction du nom désigné dans le champ **En-tête de rapport**. Pour les questionnaires à choix multiples, la **valeur enregistrée** est affichée comme réponse. Si les techniciens d'assistance ont également accès à l'enquête de satisfaction du technicien d'assistance lors de la session, et que l'administrateur l'a utilisée pour créer un flux de travail détaillé, ces questions et/ou ces champs, ainsi que les réponses des techniciens d'assistance sont aussi affichées dans le rapport.

Rapport sur l'activité d'équipe

Affichez toutes les activités d'équipe qui correspondent aux critères spécifiés sur la page précédente. Les rapports d'activité d'équipe incluent des informations sur les utilisateurs lorsqu'ils se connectent à et se déconnectent de la console du technicien d'assistance, les messages instantanés échangés entre membres d'équipe, les actions de partage d'écran d'utilisateur à utilisateur telles qu'elles sont répertoriées dans la messagerie instantanée, et les fichiers partagés et téléchargés.

Période

Sélectionnez une date de début pour l'extraction de données de rapport. Sélectionnez ensuite le nombre de jours pour lequel extraire votre rapport, ou une date de fin.

Équipe

Spécifiez l'équipe dont vous souhaitez voir les résultats.

Présentation : faire un rapport sur l'activité des présentations

Rapports | **Présentation**

Présentations

Début de période, fin de période

Sélectionnez une date de début pour l'extraction de données de rapport. Sélectionnez ensuite le nombre de jours pour lequel extraire votre rapport, ou une date de fin.

Résultats de rapport de présentation

Afficher toutes les présentations qui correspondent aux critères spécifiés sur la page précédente. Les rapports de présentations comprennent des informations de présentations de base, ainsi que des liens vers les détails de présentations, les transcriptions de la messagerie instantanée et les enregistrements vidéo. Cliquez sur **Choisir les colonnes visibles** pour choisir les informations à afficher.

Licences : faire un rapport sur les pics d'utilisation des licences

Rapports | Licences

Rapport de licences de technicien d'assistance

Période

Sélectionnez une date de début pour l'extraction de données de rapport. Sélectionnez ensuite le nombre de jours pour lequel extraire votre rapport, ou une date de fin.

Grouper par

Choisissez de regrouper le rapport sur les pics d'utilisation des licences par heure, par jour ou par mois.

Rapport sur l'utilisation des licences

Consultez les rapports sur les moments de pics d'utilisation des licences. Consultez le nombre de techniciens d'assistance connectés, le nombre de techniciens d'assistance en mode de disponibilité étendue, et le nombre total de licences en cours d'utilisation.

Vault : Rapports sur le compte Vault et l'activité du technicien d'assistance

Rapports | Vault

Rapport d'activité du compte Vault

Période

Sélectionnez une date de début pour l'extraction de données de rapport. Sélectionnez ensuite le nombre de jours pour lequel extraire votre rapport, ou une date de fin.

Compte

Pour voir tous les événements impliquant un compte Vault BeyondTrust stocké spécifique, saisissez le nom du compte, ou sélectionnez le compte dans la liste dynamique de la fenêtre pop-up.

Effectué par

Pour voir tous les événements impliquant un utilisateur spécifique, saisissez le nom d'utilisateur ou une partie de celui-ci, puis sélectionnez l'utilisateur dans la liste. Pour voir tous les événements exécutés par le système, cliquez dans la zone, puis sélectionnez **Système** dans la liste. Pour voir tous les événements impliquant un compte API, saisissez **api** dans la zone, puis sélectionnez le compte api dans la liste.

Remarque : *si un utilisateur a été rendu anonyme en vue de satisfaire à des normes de conformité, le rapport* ***d'activité du compte Vault*** *peut contenir des pseudonymes pour les données utilisateurs ou indiquer que des informations ont été supprimées. Pour en savoir plus sur l'anonymisation des données et la suppression pour cause de mise en conformité, veuillez consulter la section Conformité : Anonymiser les données pour satisfaire aux normes de conformité à l'adresse https://www.beyondtrust.com/docs/remote-support/getting-started/admin/compliance.htm.*

Pour plus d'informations, veuillez consulter le Livre blanc technique de BeyondTrust Vault à l'adresse https://www.beyondtrust.com/docs/remote-support/how-to/vault/index.htm.

Résultats de rapport d'activité de compte Vault

Étant donné que les utilisateurs peuvent obtenir un accès distinct pour utiliser et extraire des comptes, le **Rapport d'activité du compte Vault** distingue ces deux types d'activité. Cela permet aux administrateurs de faire la différence entre un utilisateur qui est en mesure d'afficher le mot de passe du compte et un utilisateur qui ne peut qu'injecter des informations d'identification dans une session.

Dans le **Rapport d'activité du compte Vault**, la colonne **Données** indique des informations associées avec l'événement. L'événement **Informations d'authentification extraites** contient un lien **Détails** dans la nouvelle colonne **Données** quand les informations

d'authentification sont extraites lors d'une session. Ce lien redirige vers le **Rapport des détails de session d'assistance technique** dans laquelle les informations d'authentification ont été utilisées.

> ***Remarque :*** *si les informations d'authentification sont extraites depuis* ***/login****, alors aucun lien* ***Détails*** *n'est présent dans la colonne* ***Données****.*

Conformité : anonymiser des données pour répondre aux normes de conformité

Rapports | **Conformité**

IMPORTANT !

*L'onglet de **conformité** est désactivé par défaut. Si votre organisation a besoin de cette fonction, veuillez contacter l'assistance technique BeyondTrust à l'adresse https://www.beyondtrust.com/docs/index.htm#support.*

Anonymisation du technicien d'assistance

Les informations concernant les techniciens d'assistance et les actions effectuées pendant les sessions d'assistance technique peuvent être rendues anonymes pour satisfaire aux réglementations en matière de confidentialité et aux normes de conformité.

Pour anonymiser les données, sélectionnez un technicien d'assistance puis cliquez sur **Chercher l'activité du technicien d'assistance**. Le système renvoie une liste d'informations trouvées pour ce technicien d'assistance, ainsi qu'une proposition de terme de remplacement généré aléatoirement pour remplacer les informations. Vous pouvez également choisir d'**Ajouter un élément personnalisé**. Ceci vous permet de saisir et de rechercher des informations personnalisées, comme des numéros de compte.

Pour modifier le texte de remplacement, cliquez sur le bouton **Modifier**. Dans l'invite **Modifier un remplacement**, définissez le **Remplacement** souhaité. Choisissez de **Modifier dans Tout l'historique** ou **Modifier dans Seulement cette session**.

La liste se met à jour avec le nouveau terme de remplacement et affiche « L'ensemble des sessions d'assistance technique, des sessions de présentation, de l'activité d'équipe et des événements de compte Vault pour ce technicien d'assistance sera marqué comme anonymisé à : [date et heure] ». Après avoir vérifié les termes de remplacement et la date, cliquez sur **Supprimer l'utilisateur et anonymiser** pour commencer le processus d'anonymisation pour tout le logiciel. Avant de commencer le processus d'anonymisation, vous devez saisir votre nom affiché pour confirmer que vous souhaitez effectuer cette action.

IMPORTANT !

Tous les enregistrements de session sont supprimés suite à la demande d'anonymisation.

Anonymisation du client

Les informations concernant les clients bénéficiant d'une assistance technique et les actions effectuées pendant les sessions d'assistance technique peuvent être rendues anonymes pour satisfaire aux réglementations en matière de confidentialité et aux normes de conformité.

Pour anonymiser les données, saisissez le nom du client, le nom de l'ordinateur ou l'adresse IP dans le champ. Cochez la case **Correspondance partielle** si vous voulez que les correspondances partielles soient listées. Cliquez ensuite sur **Chercher l'activité du client**. Si des données sont trouvées, le système renvoie une liste d'informations trouvées pour ce client, ainsi qu'une proposition de terme de remplacement généré aléatoirement pour remplacer les informations. Vous pouvez également choisir d'**Ajouter un élément personnalisé**. Ceci vous permet de saisir et de rechercher des informations personnalisées, comme des numéros de compte.

Pour modifier le texte de remplacement, cliquez sur le bouton **Modifier**. Dans l'invite **Modifier un remplacement**, définissez le **Remplacement** souhaité. Choisissez de **Modifier dans Tout l'historique** ou **Modifier dans Seulement cette session**.

La liste se met à jour avec le nouveau terme de remplacement et affiche « Les sessions d'assistance technique et les sessions de présentation sélectionnées seront marquées comme anonymisées à : [date et heure]. » Après avoir vérifié les termes de remplacement et l'horodatage, cliquez sur **Anonymiser les sessions sélectionnées** pour lancer le processus d'anonymisation pour tout le logiciel. Avant de commencer le processus d'anonymisation, vous devez saisir votre nom affiché pour confirmer que vous souhaitez effectuer cette action.

IMPORTANT !

Tous les enregistrements de session sont supprimés suite à la demande d'anonymisation.

État

Vérifiez les informations sur la tâche d'anonymisation, parmi lesquelles les termes trouvés, les termes de remplacement, le type de données anonymisées et l'état de la tâche.

L'état de la tâche est automatiquement actualisé toutes les 15 secondes, et l'état des demandes terminées reste disponible pendant 24 heures.

Remarque : *les informations d'état sont également disponibles dans les rapports de* ***Détail de session d'assistance technique*** *et de* ***Détail de session de présentation****.*

Remarque : *pour les environnements où la reprise en séquence ou Atlas est configuré, l'anonymisation des données n'est terminée qu'une fois que tous les nœuds ou les serveurs de sauvegarde ont été synchronisés.*

Portails publics

Sites publics : personnalisation du portail d'assistance technique

Sites publics

Configurez un ou plusieurs sites publics pour votre Serveur d'accès à distance sécurisé. Un site public est un site Web dans lequel vos clients peuvent démarrer une session et vers lequel l'ensemble du trafic de session est redirigé.

Ajouter un nouveau site, modifier, supprimer

Créer un nouveau site, modifier un site existant ou supprimer un site existant.

Ajouter ou modifier un site public

Nom

Créez un nom unique permettant d'identifier ce site. Ce nom vous aide à déterminer le portail public par lequel un client est arrivé. Le nom du site par défaut ne peut pas être modifié.

Adresses de sites

Chaque site doit avoir au moins un DNS ou une adresse IP permettant d'accéder à votre Serveur d'accès à distance sécurisé. Plusieurs noms d'hôte peuvent orienter vers un seul site, mais un nom d'hôte ne peut pas être utilisé pour plusieurs sites.

Profil Bouton assistance technique par défaut

Choisissez le profil de Bouton assistance technique à utiliser pour ce site public (par défaut ou personnalisé). Les profils des boutons sont configurés sur la page **Configuration > Bouton assistance technique**.

Modèle public

Configurez la mise en page et la disposition de la page en sélectionnant un modèle Web public, configuré à partir de la page **Portails publics > Modèles HTML**.

> *Pour plus d'informations, veuillez consulter la section Personnaliser le modèle Web du site public à l'adresse https://www.beyondtrust.com/docs/remote-support/how-to/customize-portals/html-templates.htm.*

Exiger l'authentification SAML

Si **SAML pour portails publics** est configuré sur la page **Utilisateurs et sécurité > Fournisseurs de sécurité**, cette option peut être sélectionnée. Si cette option est sélectionnée, les clients doivent s'authentifier auprès d'un fournisseur d'identité avant qu'une session ne soit lancée à l'aide du portail d'assistance public.

Afficher les annonces aux utilisateurs

Vous pouvez choisir d'afficher les avis d'utilisateur sur le site public. Si cette option est sélectionnée, les avis sont affichés sur le portail public, avertissant les utilisateurs des problèmes potentiels qu'ils peuvent rencontrer, et pour lesquels aucune assistance technique n'est exigée pour le moment. De cette façon, les utilisateurs ne rejoignent jamais la file d'attente de l'assistance technique, ce qui permet aux techniciens d'assistance de concentrer leur attention sur les utilisateurs ayant besoin d'assistance. Les avis d'utilisateur sont configurés sur la page **Portails publics > Avis d'utilisateur**.

> ***Remarque :*** *le même avis d'utilisateur peut être utilisé à travers plusieurs sites, ou sur un portail personnalisé. Le XML pour le portail public contient une section dans laquelle toutes les notifications actuelles sont indiquées. Cela garantit que les messages sont toujours synchronisés à travers plusieurs sites.*

> *Pour plus d'informations, veuillez consulter la section Choix des options de connexion à l'adresse https://www.beyondtrust.com/docs/remote-support/how-to/customize-portals/connection-options.htm.*

Liste des techniciens d'assistance

Utiliser la liste des techniciens d'assistance

La liste des techniciens d'assistance affiche le nom de tous les techniciens d'assistance connectés, triée d'après le numéro d'affichage. Lorsqu'un client clique sur un nom et exécute le client d'utilisateur, une session apparaît immédiatement dans la file d'attente personnelle de ce technicien d'assistance.

Choisissez si cette option de lancement de session doit être disponible pour le portail d'assistance technique. Choisissez si cette option doit être activée pour le site public et l'API, activée pour l'API mais masquée sur le site public, ou désactivée.

> ***Remarque :*** *un technicien effectuant une présentation est par défaut supprimé de la liste des techniciens d'assistance bien que cette exclusion puisse être remplacée en sélectionnant* ***Apparaît dans la liste des techniciens d'assistance*** *dans la console du technicien d'assistance.*

Afficher le texte d'aide

Choisissez si vous souhaitez afficher un texte d'aide pour cette option sur le site public. Vous pouvez personnaliser le texte affiché. Pour revenir au texte par défaut, supprimez le texte du champ puis enregistrez le champ vide.

Démarrer une session avec Cliquer-pour-messagerie instantanée

Choisissez si les sessions démarrées avec cette méthode doivent commencer par le cliquer-pour-messagerie instantanée, en démarrant sous la forme de discussions en ligne plutôt que par le client d'utilisateur.

Liste des présentations

Utiliser la liste des présentations

La liste des présentations affiche les présentations actives. Pour qu'une présentation soit répertoriée ici, le technicien d'assistance doit avoir démarré la présentation et choisi d'afficher la présentation sur le site public. Lorsqu'un client clique sur le nom d'une présentation et exécute le client, il rejoint immédiatement cette présentation.

Afficher le texte d'aide

Choisissez si vous souhaitez afficher un texte d'aide pour cette option sur le site public. Vous pouvez personnaliser le texte affiché. Pour revenir au texte par défaut, supprimez le texte du champ puis enregistrez le champ vide.

Clés de session

Utiliser les clés de session

Vous pouvez générer une clé de session pour une session d'assistance technique ou une présentation et la donner à votre client au préalable, en lui demandant de la soumettre sur votre site public. L'exécution du client d'utilisateur depuis une clé de session place l'utilisateur dans la file d'attente avec le technicien d'assistance qui a généré la clé.

Choisissez si cette option de lancement de session doit être disponible pour le portail d'assistance technique. Choisissez si cette option doit être activée pour le site public et l'API, activée pour l'API mais masquée sur le site public, ou désactivée.

Afficher le texte d'aide

Choisissez si vous souhaitez afficher un texte d'aide pour cette option sur le site public. Vous pouvez personnaliser le texte affiché. Pour revenir au texte par défaut, supprimez le texte du champ puis enregistrez le champ vide.

Démarrer une session avec Cliquer-pour-messagerie instantanée

Choisissez si les sessions démarrées avec cette méthode doivent commencer par le cliquer-pour-messagerie instantanée, en démarrant sous la forme de discussions en ligne plutôt que par le client d'utilisateur.

Demander avant de télécharger le client d'utilisateur Remote Support

Si vous cochez l'option de demande d'accord du client, l'utilisateur distant doit confirmer qu'il souhaite démarrer une session d'assistance technique ou rejoindre une présentation avant de commencer le téléchargement du client BeyondTrust. Si vous décochez cette option, le téléchargement du client démarre dès que le client envoie la clé de session ou suit le lien de clé de session.

Enquête de soumission de problème

Utiliser l'enquête de soumission de problème

L'utilisateur peut remplir une enquête de soumission de problème pour demander de l'assistance technique.

Choisissez si cette option de lancement de session doit être disponible pour le portail d'assistance technique. Choisissez si cette option doit être activée pour le site public et l'API, activée pour l'API mais masquée sur le site public, ou désactivée.

Sélection de la file d'attente de sessions

Si vous avez déterminé que cette enquête doit afficher les problèmes courants, votre client peut sélectionner le type de problème auquel il est confronté. Il est ensuite placé dans la file d'attente de l'équipe qui possède ce problème.

Si vous déterminez que l'enquête doit répertorier les techniciens d'assistance disponibles, votre utilisateur est placé dans la file d'attente personnelle du technicien d'assistance sélectionné. Notez que tous les techniciens d'assistance sont affichés, indépendamment de l'équipe à laquelle ils appartiennent.

Afficher les problèmes de toutes les équipes

Sélectionnez **Afficher les problèmes de toutes les équipes** pour répertorier tous les problèmes configurés, ou sélectionnez les équipes dont vous voulez afficher les problèmes sur ce site.

Champs disponibles/affichés

Sélectionnez à partir des champs disponibles les informations que les champs doivent afficher sur ce site. Allez dans **Configuration > Champs personnalisés** pour créer et gérer ces champs.

Afficher le texte d'aide

Choisissez si vous souhaitez afficher un texte d'aide pour cette option sur le site public. Vous pouvez personnaliser le texte affiché. Pour revenir au texte par défaut, supprimez le texte du champ puis enregistrez le champ vide.

Démarrer une session avec Cliquer-pour-messagerie instantanée

Choisissez si les sessions démarrées avec cette méthode doivent commencer par le cliquer-pour-messagerie instantanée, en démarrant sous la forme de discussions en ligne plutôt que par le client d'utilisateur.

> ***Remarque :*** *un autre type de session d'assistance technique est le partage de navigateur collaboratif, qui permet à votre client de cliquer sur un lien depuis un site Web pour vous permettre de voir et d'annoter le navigateur Web distant uniquement. Le partage de navigateur collaboratif doit être configuré grâce à l'API BeyondTrust.*

> *Pour plus d'informations, veuillez consulter le Guide du programmeur d'API à l'adresse www.beyondtrust.com/docs/remote-support/how-to/integrations/api.*

Page de destination post-session

Activer la page de destination post-session

Indiquez pour chaque site si vous souhaitez afficher une enquête de satisfaction de l'utilisateur sur la page de destination BeyondTrust, rediriger votre client vers une URL externe ou ne pas diriger l'utilisateur vers une page

> *Pour plus d'informations, veuillez consulter Personnaliser le message de désinstallation et les enquêtes de satisfaction à l'adresse https://www.beyondtrust.com/docs/remote-support/how-to/customize-portals/post-session-behavior.htm.*

Questions disponibles/affichées

Si vous activez la page de destination BeyondTrust, sélectionnez les questions à inclure dans l'enquête. Les questions sont configurées sur la page **Portails publics > Enquêtes de satisfaction**.

Autoriser les utilisateurs à télécharger la transcription de la messagerie instantanée et l'enregistrement de session.

Si vous activez la page d'accueil de BeyondTrust, vous pouvez également choisir de fournir au client un lien pour télécharger la transcription de la messagerie instantanée et l'enregistrement vidéo de la session.

URL de destination externe

Si vous activez une page d'accueil personnalisée, définissez l'URL externe d'arrivée vers laquelle les utilisateurs doivent être dirigés après une session d'assistance technique.

Enquête de satisfaction du technicien d'assistance

Activer l'enquête de satisfaction du technicien d'assistance

Vous pouvez choisir d'afficher une enquête de satisfaction du technicien d'assistance. L'enquête de satisfaction s'affichera lorsqu'une session est terminée. Il est également possible de permettre au technicien d'assistance d'accéder à l'enquête de satisfaction lors d'une session. Cette option permet aux administrateurs d'utiliser l'enquête pour créer des flux de travail détaillés contenant des liens Web externes avec des ressources, et pour garantir que les techniciens d'assistance enregistrent des informations spécifiques ou suivent un nombre prédéfini d'étapes d'assistance technique. L'option pour afficher l'enquête pendant une session est configurée sur la page **Portails publics > Enquêtes de satisfaction**.

> *Pour plus d'informations, veuillez consulter la section Enquête de satisfaction du technicien d'assistance à l'adresse https://www.beyondtrust.com/docs/remote-support/getting-started/rep-console/representative-exit-survey.htm.*

Questions disponibles/affichées

Si vous activez l'enquête de satisfaction du technicien d'assistance, sélectionnez les questions à afficher. Les questions sont configurées sur la page **Portails publics > Enquêtes de satisfaction**.

Planning : définir les heures d'ouverture du portail public

Portails publics | **Planifier**

Plannings réguliers du portail

Configurez un ou plusieurs plannings d'heures d'ouverture pour vos portails publics. En dehors des heures d'ouverture, les méthodes de lancement de session autres que les clés de session n'apparaissent pas sur votre site public, et un message indiquant que le site est fermé s'affiche.

Ajouter, modifier ou supprimer un nouveau planning

Créez un nouveau planning, modifier ou supprimer un planning existant.

Ajouter/modifier un planning

Nom du planning

Créez un nom unique permettant d'identifier ce planning.

Message de portail fermé

Créez le texte à afficher en dehors des heures d'ouverture. Les messages peuvent contenir des macros indiquant les prochaines heures d'ouverture. Vous pouvez utiliser des macros ainsi que BBCode pour du formatage basique, comme l'ajout de caractères gras, de couleurs ou de liens hypertextes. Cliquez sur **Macros** ou **BBCode** pour afficher une liste de codes et les applications qui en résultent.

Planifier

Définissez un planning afin de déterminer quand les clients peuvent lancer des sessions d'assistance technique. Définissez le fuseau horaire à utiliser pour ce planning, puis ajoutez une ou plusieurs entrées de planification. Pour chaque entrée, indiquez l'heure et la date de début ainsi que l'heure et la date de fin.

Par exemple, si la période commence à 8 h et se termine à 17 h, un client peut lancer une session durant cet intervalle. Les sessions déjà en cours peuvent dépasser la fin du planning. Si les clés de session sont activées, un technicien d'assistance peut en envoyer une à un client pour lancer une session, même en dehors du planning du site public.

Appliquer aux sites publics suivants

Si vous disposez de plus d'un site public, sélectionnez ceux qui doivent suivre ce planning.

Utilise ces jours fériés

Sélectionnez les heures non ouvrées créées pouvant s'appliquer à ce planning. Les associations créées ici s'appliquent aussi aux paramètres du planning d'heures non ouvrés.

Plannings du portail pour les jours fériés

Lorsqu'un planning d'heures non ouvrées est appliqué à un planning régulier, les heures du planning d'heures non ouvrées remplacent les heures d'ouverture normales. Les plannings d'heures non ouvrées peuvent être utilisés pour définir les jours fériés, les jours contenant moins d'heures ouvertes, et même les jours contenant davantage d'heures ouvertes.

Ajouter, modifier ou supprimer des heures non ouvrées

Créez un nouveau planning d'heures non ouvrées, modifiez ou supprimez-en un déjà existant.

Ajouter/modifier un jour férié

Nom du jour férié

Créez un nom unique permettant d'identifier ce planning d'heures non ouvrées.

Date

Définissez la date à laquelle ce planning d'heures non ouvrées doit s'appliquer.

Message de portail fermé

Créez le texte à afficher en dehors des heures normales pour cette date. Vous pouvez utiliser des macros ainsi que BBCode pour du formatage basique, comme l'ajout de caractères gras, de couleurs ou de liens hypertextes. Cliquez sur **Macros** ou **BBCode** pour afficher une liste de codes et les applications qui en résultent.

Planifier

Sélectionnez **Fermé toute la journée** ou définissez une heure d'ouverture et une heure de fermeture.

Appliquer aux plannings de portails suivants

Sélectionnez un planning normal qui a été créé et auquel ce planning d'heures non ouvrées doit s'appliquer. Les associations créées ici s'appliquent aussi aux paramètres du planning normal du portail.

> *Pour plus d'informations, veuillez consulter la section Afficher les avis d'utilisateur et les heures d'ouverture sur le portail public à l'adresse https://www.beyondtrust.com/docs/remote-support/how-to/customize-portals/portal-messages.htm.*

Modèles HTML : personnalisation de l'interface Web

Portails publics | **Modèles HTML**

Modèle Web du site public

Personnalisez les modèles HTML de votre site public afin d'établir une cohérence avec le reste de votre site Web.

Ajouter ou modifier un modèle

En haut de la page, sélectionnez un modèle existant à modifier ou sélectionnez **Ajouter** pour créer un nouveau modèle.

Nom

Lors de la création de modèles supplémentaires, attribuez un nom unique à chacun afin de pouvoir les identifier en vue de les modifier ou de les appliquer à un site public.

Modèle HTML

Les macros remplacent les données en temps réel, telles que les options de lancement de session et la liste déroulante des langues disponibles. Cela vous permet de positionner ces éléments n'importe où sur la page.

BeyondTrust vous recommande de ne modifier le site public que si vous maîtrisez le format HTML.

Revenir à la version HTML par défaut initiale

Après avoir personnalisé le site, vous pouvez rétablir l'état initial du site public en cliquant sur **Revenir à la version HTML par défaut initiale** en bas de la fenêtre de codage.

Icône Aide

Modifier l'icône d'aide

Vous pouvez charger une nouvelle image servant d'icône d'aide sur le portail public.

Revenir à l'icône d'aide par défaut d'origine

Pour restaurer l'icône d'aide initiale de BeyondTrust pour un modèle, cliquez sur le bouton **Revenir à l'icône d'aide par défaut initiale**.

Pour plus d'informations, veuillez consulter la section Personnaliser le modèle Web du site public à l'adresse https://www.beyondtrust.com/docs/remote-support/how-to/customize-portals/html-templates.htm.

Avis d'utilisateur : création de messages pour le système de notification des utilisateurs

Portails publics | **Annonces aux utilisateurs**

Annonces aux utilisateurs

Prévenez les clients, lorsqu'ils demandent une assistance technique, en cas d'interruptions informatiques à large impact pour éviter de submerger vos techniciens d'assistance BeyondTrust. Ces messages peuvent être définis pour expirer à une heure prédéterminée et appliqués à un ou plusieurs portails publics.

Une fois créés, les avis d'utilisateur sont affichés sur le portail public et la fenêtre de lancement de Bouton assistance technique, afin que les clients reçoivent les informations dont ils ont besoin avant même de démarrer une session. Les avis apparaissent également dans la fenêtre de messagerie instantanée du client d'utilisateur au début d'une session, et lorsqu'elles sont envoyées depuis l'interface /login.

Les administrateurs et les techniciens d'assistance autorisés peuvent créer jusqu'à 10 messages par portail, avec 1 020 caractères maximum.

Même si les messages ne peuvent pas être configurés par langue, vous pouvez créer différents messages pour les langues prises en charge sur le même portail.

Les administrateurs peuvent créer et modifier les avis d'utilisateur et également accorder ce droit aux techniciens d'assistance sans privilège administratif.

Ajouter une nouvelle annonce aux utilisateurs, modifier, supprimer

Créer une nouvelle annonce, modifier une annonce existante ou supprimer une annonce existante.

Envoyer

Envoyer une annonce d'utilisateur à toutes les sessions en attente.

Ajouter ou modifier une annonce aux utilisateurs

Nom

Créez un nom unique permettant d'identifier cette annonce. Ce nom n'est pas montré à l'utilisateur.

Texte de l'annonce

Créez le texte qui apparaîtra dans le client d'utilisateur, sur le portail public et dans tout Bouton assistance technique. Vous pouvez utiliser des macros ainsi que BBCode pour du formatage basique, comme l'ajout de caractères gras, de couleurs ou de liens hypertextes. Cliquez sur **Macros** ou **BBCode** pour afficher une liste de codes et les applications qui en résultent.

> ***Remarque :*** *les messages doivent être relativement courts afin qu'ils puissent être lus sans faire défiler la fenêtre du client d'utilisateur. Ceci s'applique aux modes client natif et cliquer-pour-messagerie instantanée.*

Expire le

Saisissez une date pour l'expiration de l'avis. Si vous sélectionnez **Pas de date d'expiration**, l'avis restera sur votre site jusqu'à ce qu'il soit supprimé manuellement. Les avis expirés sont automatiquement supprimés 24 heures après leur date d'expiration.

Sites publics

Si vous disposez de plus d'un site public, sélectionnez ceux qui afficheront l'annonce. Vous pouvez sélectionner plusieurs portails.

> *Pour plus d'informations, veuillez consulter la section Afficher les avis d'utilisateur et les heures d'ouverture sur le portail public à l'adresse https://www.beyondtrust.com/docs/remote-support/how-to/customize-portals/portal-messages.htm.*

Magasin de fichiers : téléchargement de fichiers de ressources

Portails publics | **Magasin de fichiers**

À propos

Utilisez le magasin de fichiers en ligne pour enregistrer les fichiers que vous devez référencer depuis votre modèle HTML, tels que des fichiers d'image et des feuilles de style. Vous pouvez également utiliser le magasin de fichiers comme point d'accès centralisé pour les fichiers fréquemment utilisés au cours des sessions d'assistance technique.

Accessibilité

Montrer la liste des fichiers du magasin de fichiers sous /files

Si cette option est cochée, tous les fichiers chargés ici sont accessibles en naviguant vers le nom d'hôte de votre site d'assistance technique suivie de /files (par exemple : support.example.com/files).

Voir le magasin de fichiers

Si l'option ci-dessus est cochée, cliquez sur ce bouton pour voir votre magasin de fichiers en ligne.

Statistiques du magasin de fichiers

Consultez le nombre de fichiers transférés, la capacité maximum disponible et la taille maximale de fichier.

Contenu

Transfert

Naviguez pour trouver des fichiers et transférez-les vers votre magasin de fichiers.

Fichiers dans le Magasin de fichiers

Consultez une liste des fichiers transférés vers votre magasin de fichiers.

Supprimer les fichiers sélectionnés

Sélectionnez un ou plusieurs fichiers dans la liste ci-dessus et cliquez sur ce bouton pour les supprimer de votre magasin de fichiers.

Pour plus d'informations, veuillez consulter la section Personnaliser le portail d'assistance technique BeyondTrust à l'adresse https://www.beyondtrust.com/docs/remote-support/how-to/customize-portals/file-store.htm.

Profil de configuration iOS : ajout de profils de configuration Apple

Portails publics | Configuration iOS

profil de configuration iOS

BeyondTrust prend en charge la distribution de profils de configuration Apple iOS, permettant ainsi aux techniciens Service client de proposer aux utilisateurs de périphériques iOS des profils publics et privés configurés par l'administrateur à télécharger sur leur iPhone®, iPad™ ou iPod touch®.

Pour plus d'informations, veuillez consulter la section Profils de configuration iOS à l'adresse https://www.beyondtrust.com/docs/remote-support/getting-started/customer-client/apple-ios/iosconfigurationprofiles.htm.

IMPORTANT !

*Afin de s'assurer que les profils de configuration sont téléchargés vers les périphériques iOS sur une connexion HTTPS cryptée, vous devez cocher la case **Forcer le site public à utiliser HTTPS** sur la page **Gestion > Sécurité** de l'interface d'administration /login. Dans le cas contraire, les téléchargements s'effectueront sur des connexions HTTP non cryptées.*

Pour administrer les paramètres Apple iOS, vous devez utiliser un compte admin. Pour créer ou modifier des profils de configuration Apple iOS, vous devez avoir l'autorisation du compte utilisateur **Autorisé à modifier les profils iOS**. Pour qu'un technicien d'assistance puisse donner aux clients l'accès aux profils de configuration privés, il doit disposer de l'autorisation de compte **Autorisé à générer des clés d'accès pour envoyer des profils iOS**. Dans l'interface d'administration /login, sélectionnez **Utilisateurs et sécurité > Utilisateurs** et/ou **Règles de groupe** pour modifier les autorisations de compte.

Après avoir configuré et exporté un profil de configuration à partir de l'utilitaire de configuration iPhone gratuit d'Apple, utilisez l'interface d'administration /login dans BeyondTrust pour rendre le profil accessible. L'utilitaire de configuration iPhone est disponible sur le site Web d'assistance technique iPhone d'Apple.

Ajouter un nouveau profil, Modifier, Supprimer

Créer un nouveau profil, modifier un profil existant, ou supprimer un profil existant.

Ajouter ou modifier un profil de configuration iOS

Nom

Créez un nom unique permettant d'identifier ce profil. Le nom de ce profil de configuration iOS doit aider l'utilisateur à sélectionner le profil qui convient lorsqu'il parcourt votre portail d'assistance technique.

Fichier

Transférez le profil Apple iOS que vous venez de créer avec le logiciel iPhone Configuration Utility. Notez que le profil Apple iOS sous-jacent doit être altéré pour modifier le contenu des profils de périphérique iOS que vous souhaitez distribuer aux utilisateurs de périphériques iOS.

Description

Ajoutez une brève description pour résumer la fonction de ce profil.

Public

Cochez la case **Public** pour que le profil apparaisse dans une liste visible par tous les utilisateurs iOS qui naviguent sur votre portail public. Notez que les utilisateurs iOS ne verront pas une liste des techniciens d'assistance traditionnelle ou une boîte de soumission de problème lorsqu'ils parcourent le portail public.

En ne cochant pas la case **Public**, vous avez la possibilité de restreindre l'accès au profil iOS que vous avez créé. Pour télécharger le contenu d'un profil privé, les utilisateurs doivent saisir la clé d'accès que vous avez générée dans la console du technicien d'assistance.

Paramètres

Sélectionnez un site public à modifier

Dans le menu déroulant, sélectionnez le site public dont vous voulez régler les paramètres.

Lien vers les profils de configuration iOS activé.

Si cette option est sélectionnée, les utilisateurs sur appareils iOS verront un lien vers le portail des profils de configuration iOS lorsqu'ils accèdent au site public. Cette page affiche tous les profils publics disponibles et fournit une zone de saisie de texte dans laquelle les clients peuvent soumettre une clé d'accès fournie par leur technicien d'assistance, et être dirigés vers un profil de configuration privé.

Portail

Titre

Personnalisez le titre de la page du portail iOS. Vous pouvez traduire ce texte dans les langues que vous avez activées. Pour revenir au texte par défaut, supprimez le texte du champ puis enregistrez le champ vide.

Message

Personnalisez le texte qui sera affiché sur la page du portail iOS. Vous pouvez traduire ce texte dans les langues que vous avez activées. Pour revenir au texte par défaut, supprimez le texte du champ puis enregistrez le champ vide.

E-mail d'invitation

Lorsqu'un technicien d'assistance génère une clé d'accès au profil Apple iOS à partir de la console du technicien d'assistance, la clé d'accès peut être envoyée par e-mail à l'utilisateur iOS.

Objet

Personnalisez l'objet de cet e-mail. Vous pouvez traduire ce texte dans les langues que vous avez activées. Pour revenir au texte par défaut, supprimez le texte du champ puis enregistrez le champ vide.

Message

Personnalisez le texte de cet e-mail. Utilisez les macros répertoriées sous ce champ dans la page /login pour personnaliser le texte selon vos besoins. Vous pouvez traduire ce texte dans les langues que vous avez activées. Pour revenir au texte par défaut, supprimez le texte du champ puis enregistrez le champ vide.

> *Pour plus d'informations, veuillez consulter la section Gérer les profils de configuration Apple iOS à l'adresse https://www.beyondtrust.com/docs/remote-support/getting-started/customer-client/apple-ios/manageprofilespage.htm.*

Enquêtes : activation des enquêtes de satisfaction de l'utilisateur et du technicien d'assistance

Portails publics | Enquêtes de satisfaction

Enquête de satisfaction de l'utilisateur ou enquête de satisfaction du technicien d'assistance

Configurez les questions à implémenter dans les enquêtes de satisfaction du technicien d'assistance et du client, qui sont utiles pour contrôler le niveau de satisfaction et les taux de résolution des incidents. Les questions sont attribuées aux enquêtes d'un site d'assistance technique sur la page **Portails publics > Sites publics**.

Autoriser les techniciens d'assistance à modifier l'enquête au cours d'une session d'assistance technique

Autorisez le technicien d'assistance à accéder à l'enquête lors de la session. Les administrateurs peuvent utiliser l'enquête pour créer des flux de travail détaillés contenant des liens Web externes avec des ressources, et pour garantir que les techniciens d'assistance enregistrent des informations spécifiques ou suivent un nombre prédéfini d'étapes d'assistance technique.

Ajouter une nouvelle question, modifier, supprimer

Créer une nouvelle question, modifier une question existante ou supprimer une question existante.

Prévisualisation de l'enquête

Prévisualisez la façon dont toutes les questions d'enquête apparaîtront pour vos utilisateurs. La prévisualisation de l'enquête de technicien d'assistance montre le format basique, mais les styles ont une apparence différente dans la console du technicien d'assistance.

Enquête de satisfaction de l'utilisateur ou enquête de satisfaction du technicien d'assistance : Ajouter une nouvelle question

Type de question

Vous avez le choix entre différents types de questions, y compris des boutons radio, des cases à cocher, des menus déroulants, des zones de texte et des zones de saisie de texte.

Texte de question

Entrez le texte de la question tel que vous souhaitez le voir apparaître dans l'enquête.

Nom de la question

Attribuez un nom à la question pour le formatage interne.

En-tête de rapport

Attribuez un en-tête à la question pour l'identifier dans vos rapports d'enquête.

Réponse obligatoire

Pour les enquêtes de satisfaction des techniciens d'assistance, déterminez si le technicien d'assistance doit répondre à la question avant de fermer la session.

Style CSS

Vous pouvez définir un style CSS pour une question d'enquête de satisfaction de l'utilisateur. Cette option est proposée pour le développement Web. Il est conseillé aux utilisateurs qui ne maîtrisent pas les formats HTML et CSS de laisser ces champs vierges.

Classes CSS

Vous pouvez définir des classes CSS pour une question d'enquête de satisfaction de l'utilisateur. Cette option est proposée pour le développement Web. Il est conseillé aux utilisateurs qui ne maîtrisent pas les formats HTML et CSS de laisser ces champs vierges.

ID HTML

Vous pouvez définir un identifiant HTML pour une question d'enquête de satisfaction de l'utilisateur. Cette option est proposée pour le développement Web. Il est conseillé aux utilisateurs qui ne maîtrisent pas les formats HTML et CSS de laisser ces champs vierges.

Autoriser les sélections multiples

Pour un menu déroulant, vous pouvez choisir d'autoriser plusieurs sélections.

Taille de la zone de texte

Pour une zone de texte, définissez la taille du champ de saisie.

Nb de caract. max de la réponse

Pour une zone de texte, réglez le nombre maximum de caractères pouvant être utilisés.

Taille de la zone de texte

Pour une zone de saisie de texte, définissez la taille du champ de saisie.

Ordre d'affichage

Choisissez l'ordre d'apparition des questions dans l'enquête. Les chiffres inférieurs apparaissent en premier.

Valeur par défaut

Pour une zone de texte ou une zone de saisie de texte, vous pouvez insérer un texte par défaut dans le champ.

Apparait sur le site public par défaut

Si vous sélectionnez cette option, cette question sera automatiquement ajoutée à l'enquête pour votre site d'assistance technique par défaut. Une enquête ne peut comporter plus de dix questions. Par conséquent, vous recevez un message d'erreur si vous essayez d'enregistrer une question qui dépasse cette limite sur votre enquête de satisfaction du site par défaut. Pour créer une question à utiliser dans une autre enquête de satisfaction, décochez la case, puis enregistrez.

Valeur affichée

Pour chaque option disponible dans un groupe de boutons radio, de cases à cocher ou dans un menu déroulant, assignez une valeur d'affichage qui apparaîtra à l'utilisateur.

Valeur enregistrée

Pour chaque option disponible dans un groupe de boutons radio, de cases à cocher ou dans un menu déroulant, assignez une valeur enregistrée qui sera conservée dans les rapports sur l'enquête de satisfaction.

Sélectionnée par défaut

Pour un groupe de boutons radio, un groupe de cases à cocher ou un menu déroulant, vous pouvez choisir d'avoir une option sélectionnée par défaut.

Ordre d'affichage

Pour un groupe de boutons radio, un groupe de cases à cocher ou un menu déroulant, définissez l'ordre dans lequel ces options apparaissent sous la question.

Tri croissant

Pour un groupe de boutons radio, un groupe de cases à cocher ou un menu déroulant, classez les options par ordre croissant.

Tri décroissant

Pour un groupe de boutons radio, un groupe de cases à cocher ou un menu déroulant, classez les options par ordre décroissant.

Ajouter une option

Ajoutez plusieurs options à un groupe de boutons radio, un groupe de cases à cocher ou un menu déroulant

Aperçu de la question

Prévisualisez la façon dont cette question apparaîtra pour vos utilisateurs. La prévisualisation d'une question d'enquête de technicien d'assistance montre le format basique, mais les styles ont une apparence différente dans la console du technicien d'assistance.

Pour plus d'informations, veuillez consulter Personnaliser le message de désinstallation et les enquêtes de satisfaction à l'adresse https://www.beyondtrust.com/docs/remote-support/how-to/customize-portals/post-session-behavior.htm.

Pour en savoir plus, veuillez consulter Enquête de satisfaction de l'utilisateur : envoyer un avis à l'adresse https://www.beyondtrust.com/docs/remote-support/getting-started/customer-client/customer-exit-survey.htm.

Pour plus d'informations, veuillez consulter la section Enquête de satisfaction du technicien d'assistance à l'adresse https://www.beyondtrust.com/docs/remote-support/getting-started/rep-console/representative-exit-survey.htm.

Client d'utilisateur : modification de l'e-mail d'invitation, des options d'affichage et des options de connexion

Portails publics | **Client d'utilisateur**

Sélectionnez un site public à modifier

Dans le menu déroulant, sélectionnez le site public dont vous voulez régler les paramètres.

E-mail d'invitation

Créez un e-mail personnalisé avec des instructions uniques de session d'assistance technique pour chaque site public.

Adresse de l'expéditeur

Vous avez la possibilité d'utiliser le champ **Adresse de l'expéditeur** pour créer des invitations par e-mail générées par le système plutôt qu'une invitation utilisant le client e-mail local du technicien d'assistance. Si elles sont configurées de cette façon, les invitations de session sont envoyées depuis une adresse centralisée pour tout le système (par exemple : « admin@support.example.com »). Ceci peut être utile si vos techniciens d'assistance ont des restrictions d'e-mail d'entreprise pour des raisons de sécurité ou de respect de la vie privée. Si le champ **Adresse de l'expéditeur** est laissé vide, c'est l'adresse de l'expéditeur configurée sur la page Configuration e-mail qui sera utilisée.

> ***Remarque :*** *pour activer les e-mails sur tout le système, assurez-vous que la case* ***Activer les e-mails serveur pour les invitations d'assistance technique*** *est cochée sur la page* ***/login > Configuration > Options****.*

Objet

Personnalisez l'objet de cet e-mail. Vous pouvez traduire ce texte dans les langues que vous avez activées. Pour revenir au texte par défaut, supprimez le texte du champ puis enregistrez le champ vide.

Corps

Personnalisez le texte de cet e-mail. Utilisez les macros répertoriées sous ce champ dans la page /login pour personnaliser le texte selon vos besoins. Vous pouvez traduire ce texte dans les langues que vous avez activées. Pour revenir au texte par défaut, supprimez le texte du champ puis enregistrez le champ vide.

Accords de l'utilisateur

> *Pour en savoir plus, veuillez consulter Client d'utilisateur : Interface de session d'assistance technique à l'adresse https://www.beyondtrust.com/docs/remote-support/getting-started/customer-client/customer-support-interface.htm.*

Sessions de client complet

Afficher l'accord d'utilisation avant les sessions du client complet

Personnalisez le texte de cet accord. Vous pouvez traduire ce texte dans les langues que vous avez activées. Pour revenir au texte par défaut, supprimez le texte du champ puis enregistrez le champ vide.

Titre

Personnalisez le titre de l'accord. L'utilisateur final voit cela dans la barre de titre de l'invite. Vous pouvez traduire ce texte dans les langues que vous avez activées. Pour revenir au texte par défaut, supprimez le texte du champ puis enregistrez le champ vide.

Délai d'attente d'acceptation

Si l'utilisateur n'accepte pas l'accord dans le **Délai d'attente d'acceptation**, la session se terminera. Cela s'applique uniquement aux sessions sans surveillance.

Texte

Saisissez le texte pour l'accord d'utilisateur pour le client natif. Vous pouvez traduire ce texte dans les langues que vous avez activées. Pour revenir au texte par défaut, supprimez le texte du champ puis enregistrez le champ vide.

Sessions cliquer-pour-messagerie instantanée

Afficher l'accord d'utilisation avant les sessions Cliquer-pour-messagerie instantanée

Activez un accord que l'utilisateur doit accepter avant d'accéder à une session cliquer-pour-messagerie instantanée.

Sessions sans surveillance

Afficher l'accord d'utilisateur avant les sessions non autonomes

Activer un accord qui doit être accepté avant de lancer une session sans surveillance.

Titre

Personnalisez le titre de l'accord. L'utilisateur final voit cela dans la barre de titre de l'invite. Vous pouvez traduire ce texte dans les langues que vous avez activées. Pour revenir au texte par défaut, supprimez le texte du champ puis enregistrez le champ vide.

Délai d'attente d'acceptation

Si le client n'accepte pas l'accord dans le **Délai d'attente d'acceptation**, la session prend fin. Ceci s'applique aux sessions client natif et cliquer-pour-messagerie instantanée.

Comportement automatique

Déterminez si les points de terminaison sans surveillance acceptent ou rejettent automatiquement les sessions lancées par le biais d'un Jump Client, d'un Jump distant et d'éléments de Jump.

Texte

Saisissez le texte pour l'accord d'utilisateur pour le client natif. Vous pouvez traduire ce texte dans les langues que vous avez activées. Pour revenir au texte par défaut, supprimez le texte du champ puis enregistrez le champ vide.

Options d'affichage

Afficher les invites

Vous pouvez définir la façon dont les invites utilisateur s'affichent au cours des sessions d'assistance technique, en choisissant de les afficher sous forme de liens hypertexte dans la fenêtre de messagerie instantanée ou sous forme de fenêtres contextuelles au-dessus de cette fenêtre. Notez que l'option d'affichage sous forme de fenêtres contextuelles ne s'applique pas aux clients mobiles ni aux sessions cliquer-pour-messagerie instantanée.

Minimiser le client d'utilisateur à l'ouverture pour les sessions non autonomes.

Choisissez de démarrer discrètement le client d'utilisateur réduit et sans prendre la main dans les sessions lancées par l'utilisateur.

Lors de l'attachement d'un Jump Client, fixez le comportement par défaut de manière à ce que les clients d'utilisateurs lancés depuis ce Jump Client soient minimisés à l'ouverture.

Choisissez de démarrer discrètement le client d'utilisateur réduit et sans prendre la main dans les sessions de Jump Client.

Minimisez le client d'utilisateur à l'ouverture pour les sessions démarrées en Jump local ou Jumpoint.

Choisissez de démarrer discrètement le client d'utilisateur réduit et sans prendre la main dans les sessions Jump local ou Jumpoint.

Afficher l'invite d'enregistrement de session avant les sessions du client complet

Si cette option est cochée, l'utilisateur est invité à autoriser l'enregistrement de session au début de chaque session. S'il accepte, la session est enregistrée, tel que défini pour le portail public. S'il refuse, la session se poursuit sans enregistrement. Cette option s'applique à l'enregistrement du partage d'écran, de l'interpréteur de commandes et des informations système.

Afficher les annonces aux utilisateurs dans le client d'utilisateur

Si cette option est cochée, jusqu'à ce que la session soit acceptée, le client d'utilisateur affichera les deux avis d'utilisateur déjà actifs lors de la demande de session ainsi que les avis d'utilisateur créés et envoyés. Chaque avis sera accompagné d'un lien pour terminer la session si l'avis traite un problème connu pour lequel l'utilisateur a demandé une assistance technique.

Messages

Message de bienvenue

Afficher le message de bienvenue avant la session

Le message de bienvenue à l'utilisateur s'affiche dans la fenêtre de messagerie instantanée lorsque la session est dans la file d'attente. Vous pouvez traduire ce texte dans les langues que vous avez activées. Pour revenir au texte par défaut, supprimez le texte du champ

puis enregistrez le champ vide.

Informez les utilisateurs sur le statut de leur session en leur fournissant des commentaires concernant leur place dans la file d'attente et l'estimation du temps d'attente. Grâce à ces informations, les utilisateurs auront plus de chances de rester dans la file d'attente et obtenir le service dont ils ont besoin.

Le temps d'attente et la place sont calculés par file d'attente. La place d'un utilisateur dans la file d'attente est déterminée par l'âge de la session sur la base du premier arrivé, premier servi. Le temps d'attente est calculé à l'aide du plus récent modèle de sessions entrées dans la file d'attente et auxquelles a répondu un technicien d'assistance. Un minimum de cinq sessions est nécessaire pour fournir suffisamment de données pour un calcul fiable du temps d'attente.

Les messages sont configurés à l'aide de macros. Copiez les macros **%POSITION_IN_QUEUE%** et **%ESTIMATED_WAIT_TIME%** dans la zone de texte.

> ***Remarque :*** *les macros se développent dans des phrases complètes décrivant la place de l'utilisateur dans la file d'attente, ainsi que le temps d'attente estimé qu'il reste à l'utilisateur.*

Message de mise en attente

Afficher le message de mise en attente

Le message d'attente s'affiche à intervalles définis jusqu'à ce qu'un technicien d'assistance accepte la session. Vous pouvez traduire ce texte dans les langues que vous avez activées. Pour revenir au texte par défaut, supprimez le texte du champ puis enregistrez le champ vide.

Informez les utilisateurs sur le statut de leur session en leur fournissant des commentaires concernant leur place dans la file d'attente et l'estimation du temps d'attente. Grâce à ces informations, les utilisateurs auront plus de chances de rester dans la file d'attente et obtenir le service dont ils ont besoin.

Le temps d'attente et la place sont calculés par file d'attente. La place d'un utilisateur dans la file d'attente est déterminée par l'âge de la session sur la base du premier arrivé, premier servi. Le temps d'attente est calculé à l'aide du plus récent modèle de sessions entrées dans la file d'attente et auxquelles a répondu un technicien d'assistance. Un minimum de cinq sessions est nécessaire pour fournir suffisamment de données pour un calcul fiable du temps d'attente.

Les messages sont configurés à l'aide de macros. Copiez les macros **%POSITION_IN_QUEUE%** et **%ESTIMATED_WAIT_TIME%** dans la zone de texte.

> ***Remarque :*** *les macros se développent dans des phrases complètes décrivant la place de l'utilisateur dans la file d'attente, ainsi que le temps d'attente estimé qu'il reste à l'utilisateur.*

Intervalle du message de mise en attente

Indiquez le nombre de minutes devant s'écouler entre deux envois de messages d'attente.

Texte

Saisissez le texte pour le message de mise en attente.

Message orphelin

Afficher le message de session orpheline

Si un utilisateur demande une session lorsqu'aucun technicien d'assistance n'est disponible, un message de session orpheline peut être affiché. Vous pouvez traduire ce texte dans les langues que vous avez activées. Pour revenir au texte par défaut, supprimez le texte du champ puis enregistrez le champ vide.

Et ouvrir cette URL

Si une session est perdue, le navigateur Web de l'utilisateur peut être automatiquement ouvert sur une URL spécifiée, comme une base de connaissances ou une page de contact.

Texte

Saisissez le texte pour le message orphelin.

Bannière de la fenêtre de messagerie instantanée

Changer la bannière de la messagerie instantanée

Transférez une bannière d'image pour la fenêtre du client d'utilisateur. Ce fichier doit être un fichier Bitmap (BMP) Windows 256 couleurs (8 bits), doté d'une résolution de 480 pixels. La hauteur recommandée pour l'image est de 40 pixels. Dès que vous envoyez une nouvelle bannière, toutes les nouvelles sessions utilisent cette image. Les sessions déjà ouvertes ne sont pas affectées.

Revenir au défaut

Revenez à la bannière par défaut. Dès que vous revenez à l'image par défaut, toutes les nouvelles sessions l'utilisent. Les sessions déjà ouvertes ne sont pas affectées.

Filigrane

Afficher à l'écran un indicateur lorsqu'un technicien d'assistance est en session avec le client (Windows® uniquement).

Cochez la case pour ajouter un filigrane à l'écran durant une session.

Changer le filigrane

Envoyez une image de filigrane personnalisée à afficher sur l'écran du client. Cette image personnalisée remplace le filigrane par défaut de BeyondTrust. Cette image doit être un fichier .png ou .bmp avec des dimensions entre 32x32 et 256x256 pixels. Pour de meilleurs résultats, la taille recommandée est de 128x128 pixels. Vous pouvez redimensionner l'image sélectionnée en utilisant le curseur ou en cliquant sur le bouton **Ajuster à la boîte** ou **Remplir toute la boîte**. Cliquez sur **Enregistrer le filigrane** pour enregistrer les modifications ou sur **Annuler les changements** si vous ne voulez pas garder l'image que vous avez sélectionnée.

Lorsque le filigrane est affiché sur l'écran du client, une transparence de 40 % est appliquée, ce qui vous permet d'envoyer une image complètement opaque sans qu'il y ait de risque qu'elle obstrue l'affichage du bureau du client.

Remarque : *si vous envoyez une image qui est déjà partiellement transparente, une transparence supplémentaire de 40 % y sera appliquée, ce qui pourrait rendre l'image plus transparente que souhaité.*

Remarque : *une fois que les clients ont mis à niveau vers BeyondTrust Remote Support 17.1, le filigrane pour tous les portails publics revient par défaut au nouveau filigrane.*

Pour en savoir plus, veuillez consulter Modifier l'apparence du Client d'utilisateur à l'adresse https://www.beyondtrust.com/docs/remote-support/how-to/customize-portals/customer-client-appearance.htm.

Revenir au défaut

Revenir à l'image par défaut. Dès que vous revenez à l'image par défaut, toutes les nouvelles sessions l'utilisent. Les sessions déjà ouvertes ne sont pas affectées.

Règle de session

Règle de session

Vous pouvez affecter une règle de session aux sessions associées au site public sélectionné dans le haut de cette page. Cette règle de session peut affecter les autorisations des sessions démarrées via ce site.

Pour plus d'informations, veuillez consulter la section Définir les autorisations d'attachement et de détachement des Jump Clients à l'adresse https://www.beyondtrust.com/docs/remote-support/how-to/jump-clients/permissions.htm.

Options d'enregistrement

Activer l'enregistrement de partage d'écran

Pour le site public sélectionné dans le haut de cette page, indiquez si vous souhaitez enregistrer les sessions de partage d'écran. Vous pouvez activer ou désactiver les enregistrements, ou utiliser le paramètre configuré pour le site via la page **Configuration > Options**. Ce paramètre peut être remplacé par une préférence utilisateur, telle que configurée ci-dessus par le paramètre **Afficher l'invite d'enregistrement de session avant les sessions du client complet**.

Activer l'enregistrement de l'interpréteur de commandes

Pour le site public sélectionné dans le haut de cette page, indiquez si vous souhaitez enregistrer les sessions d'interpréteur de commandes. Vous pouvez activer ou désactiver les enregistrements, ou utiliser le paramètre configuré pour le site via la page **Configuration > Options**. Ce paramètre peut être remplacé par une préférence utilisateur, telle que configurée ci-dessus par le paramètre **Afficher l'invite d'enregistrement de session avant les sessions du client complet**.

Activer l'enregistrement automatique des informations système

Pour le site public sélectionné dans le haut de cette page, indiquez si vous souhaitez enregistrer les informations système au début d'une session. Vous pouvez activer ou désactiver les enregistrements, ou utiliser le paramètre configuré pour le site via la page **Configuration > Options**. Ce paramètre peut être remplacé par une préférence utilisateur, telle que configurée ci-dessus par le paramètre **Afficher l'invite d'enregistrement de session avant les sessions du client complet**.

Comportement d'après-session

Message personnalisé de désinstallation

Une fois la session terminée, et si aucun Jump Client n'est installé, les utilisateurs seront informés que le logiciel BeyondTrust a été désinstallé. Vous pouvez traduire ce texte dans les langues que vous avez activées. Pour revenir au texte par défaut, supprimez le texte du champ puis enregistrez le champ vide.

> *Pour plus d'informations, veuillez consulter Personnaliser le message de désinstallation et les enquêtes de satisfaction à l'adresse https://www.beyondtrust.com/docs/remote-support/how-to/customize-portals/post-session-behavior.htm.*

Options de connexion

Délai de reconnexion

Déterminez le délai avant qu'un client d'utilisateur déconnecté puisse à nouveau se connecter.

Limiter l'accès de l'utilisateur à l'ordinateur en cas de perte de la connexion du client d'utilisateur ou de déconnexion de l'ensemble des techniciens d'assistance de la session

Si la connexion de la session est perdue, l'entrée souris et clavier du système distant peut être temporairement désactivée, pour reprendre lorsque la connexion est restaurée ou quand la session est terminée.

Comportement de fin de session

Si vous ne pouvez pas vous reconnecter dans le temps que vous avez défini dans **Délai de reconnexion**, choisissez l'action à effectuer. Pour empêcher un utilisateur final d'accéder à des privilèges non autorisés après une session avec des droits accrus, réglez le client pour qu'il déconnecte automatiquement l'utilisateur final de l'ordinateur Windows distant à la fin de la session, qu'il verrouille l'ordinateur distant, ou qu'il ne fasse rien.

Autoriser les techniciens d'assistance à remplacer ce paramètre session par session

Vous pouvez autoriser un utilisateur à outrepasser le paramètre de fin de session dans l'onglet **Résumé** de la console au cours d'une session.

Cliquer-pour-messagerie instantanée

Demande de nom

Personnalisez la demande de nom pour afficher une question ou une déclaration spécifique lorsqu'un utilisateur lance une session cliquer-pour-messagerie instantanée. Le texte par défaut est : « Veuillez indiquer votre nom ».

Demande d'accroissement des droits

Personnalisez le message que l'utilisateur voit lors d'une demande d'accroissement d'une session cliquer-pour-messagerie instantanée. Le texte par défaut est : « %REP_NAME% demande l'accroissement des privilèges vers une assistance technique distante complète qui autoriserait plus de fonctionnalités, comme le partage d'écran et le transfert de fichiers. Le système vous demandera d'exécuter une application qui vous sera envoyée. Souhaitez-vous continuer ? »

> ***Remarque :*** *la macro* ***%REP_NAME%*** *sera remplacée par le nom affiché public du technicien d'assistance à l'origine de la demande d'accroissement.*

Injection <head> HTML

Les utilisateurs qui ont l'autorisation **Autorisé à modifier les sites publics** peuvent insérer du code HTML personnalisé dans l'élément <head> de la page qui affiche le client HTML5 de cliquer-pour-messagerie instantanée.

Autres options

Accroissement automatique des droits

Choisissez de quelle façon traiter l'accroissement des droits du client d'utilisateur sur un système Windows distant. Lorsque l'option **Ne jamais tenter d'accroître les droits** est sélectionnée, le client d'utilisateur ne tente en aucun cas de s'exécuter avec les droits d'administration, sauf demande expresse du technicien d'assistance. Lorsque l'option **Tenter d'accroître les droits uniquement lorsque cela ne nécessite pas l'intervention de l'utilisateur** est sélectionnée, le client d'utilisateur tente de s'exécuter avec les droits d'administration, mais uniquement lorsque cela ne requiert pas d'intervention de la part de l'utilisateur. Lorsque l'option **Toujours tenter d'accroître les droits** est sélectionnée, le client d'utilisateur tente toujours de s'exécuter avec les droits d'administration ; au début de chaque session, l'utilisateur distant peut être invité à autoriser ou non l'accroissement des droits.

Autoriser l'utilisateur à limiter les applications partagées durant le partage d'écran lorsque cela n'est pas demandé explicitement

Si vous choisissez d'autoriser l'utilisateur à limiter les applications partagées, votre utilisateur pourra définir les applications que vous pouvez voir ou non pendant une session de partage d'écran. Si cette option est désélectionnée, les utilisateurs reçoivent cette option uniquement si le technicien d'assistance la demande explicitement ou s'il n'est autorisé qu'à demander un contrôle limité.

Autoriser le technicien d'assistance à outrepasser la règle d'injection de Ctrl-Alt-Suppr (CAS) désactivée du client (uniquement Windows Vista® et versions supérieures)

En prenant en charge Windows Vista ou une version supérieure, le technicien d'assistance peut tenter de remplacer une règle d'injection Séquence d'attention sécurisée désactivée d'un utilisateur afin d'envoyer une commande Ctrl-Alt-Suppr.

Autoriser l'utilisateur à envoyer des fichiers à l'aide de l'interface de messagerie instantanée

Si vous souhaitez empêcher les transferts de fichiers depuis l'utilisateur vers le technicien d'assistance, vous pouvez désactiver la fonctionnalité utilisateur d'envoi de fichiers pour les sessions de messagerie instantanée.

Autoriser le client d'utilisateur à désactiver temporairement l'accélération matérielle pendant le partage d'écran

Vous pouvez autoriser le client d'utilisateur à détecter lorsqu'un pilote de carte vidéo génère une utilisation intensive du processeur de l'ordinateur distant ; dans ce cas, le client d'utilisateur peut temporairement désactiver l'accélération matérielle au cours du partage d'écran afin d'accélérer la connexion à l'assistance technique à distance.

Présentation : modification des e-mails d'invitation et des options d'affichage

Portails publics | **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.*

Pour plus d'informations, veuillez consulter Réaliser une présentation pour des participants distants à l'adresse https://www.beyondtrust.com/docs/remote-support/getting-started/rep-console/presentation.htm.

Pour plus d'informations, veuillez consulter la section Client de participant à une présentation : Rejoindre une présentation à l'adresse https://www.beyondtrust.com/docs/remote-support/getting-started/customer-client/customer-presentation-interface.htm.

Participant à une présentation

E-mail d'invitation à une présentation programmée

Remarque : *une seule configuration de client du participant à la présentation est actuellement disponible. Les clients du participant à la présentation ne peuvent pas être configurés par site public.*

Envoyez un e-mail pour inviter des participants à une présentation planifiée pour plus tard.

*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 Configuration e-mail : Configurer le logiciel pour envoyer des e-mails à l'adresse https://www.beyondtrust.com/docs/remote-support/getting-started/admin/email-configuration.htm.*

Objet

Personnalisez l'objet de cet e-mail. Vous pouvez traduire ce texte dans les langues que vous avez activées. Pour revenir au texte par défaut, supprimez le texte du champ puis enregistrez le champ vide.

Corps

Personnalisez le texte de cet e-mail. Utilisez les macros répertoriées sous ce champ dans la page /login pour personnaliser le texte selon vos besoins. Vous pouvez traduire ce texte dans les langues que vous avez activées. Pour revenir au texte par défaut, supprimez le texte

du champ puis enregistrez le champ vide.

E-mail d'invitation à une présentation en cours

Envoyez un e-mail pour inviter des participants à une présentation déjà en cours.

Objet

Personnalisez l'objet de cet e-mail. Vous pouvez traduire ce texte dans les langues que vous avez activées. Pour revenir au texte par défaut, supprimez le texte du champ puis enregistrez le champ vide.

Corps

Personnalisez le texte de cet e-mail. Utilisez les macros répertoriées sous ce champ dans la page /login pour personnaliser le texte selon vos besoins. Vous pouvez traduire ce texte dans les langues que vous avez activées. Pour revenir au texte par défaut, supprimez le texte du champ puis enregistrez le champ vide.

Client de participant à une présentation

Options d'affichage

Afficher l'accord de participation avant les sessions

L'accord du participant s'affiche avant le téléchargement du client BeyondTrust, garantissant qu'il a connaissance de la fonctionnalité de partage d'écran du programme.

Afficher le message de bienvenue avant la session

Le **message de bienvenue** accueille le participant, lui demande de patienter jusqu'au démarrage de la présentation, et fournit des détails sur la conférence audio si vous les avez configurés dans la barre latérale de présentation de technicien d'assistance. Vous pouvez traduire ce texte dans les langues que vous avez activées. Pour revenir au texte par défaut, supprimez le texte du champ puis enregistrez le champ vide.

Texte

Personnalisez le texte de cet accord. Vous pouvez traduire ce texte dans les langues que vous avez activées. Pour revenir au texte par défaut, supprimez le texte du champ puis enregistrez le champ vide.

Délai d'expiration

Si le présentateur n'est pas en ligne au moment où la présentation est supposée démarrer, le **Délai d'expiration** détermine combien de temps le participant peut attendre avant d'être déconnecté.

Afficher le message de participant orphelin

Si le présentateur n'est pas en ligne au moment où la présentation est supposée démarrer et qu'il ne la rejoint pas avant le délai d'expiration, les participants pourront recevoir ce message. Vous pouvez traduire ce texte dans les langues que vous avez activées. Pour

revenir au texte par défaut, supprimez le texte du champ puis enregistrez le champ vide.

Bannière de la fenêtre de messagerie instantanée

Changer la bannière du participant

Transférez une bannière d'image pour la fenêtre du client d'utilisateur. Ce fichier doit être un fichier Bitmap (BMP) Windows 256 couleurs (8 bits), doté d'une résolution de 480 pixels. La hauteur recommandée pour l'image est de 40 pixels. Dès que vous envoyez une nouvelle bannière, toutes les nouvelles sessions utilisent cette image. Les sessions déjà ouvertes ne sont pas affectées.

Revenir au défaut

Revenez à la bannière par défaut. Dès que vous revenez à l'image par défaut, toutes les nouvelles sessions l'utilisent. Les sessions déjà ouvertes ne sont pas affectées.

Comportement d'après-session

Message personnalisé de désinstallation

À la fin de la présentation, votre participant est informé que BeyondTrust a été désinstallé. Vous pouvez traduire ce texte dans les langues que vous avez activées. Pour revenir au texte par défaut, supprimez le texte du champ puis enregistrez le champ vide.

Localisation

Messagerie instantanée en temps réel: Traduire les messages de la messagerie instantanée entre le technicien d'assistance et le client

Localisation | **Messagerie instantanée en temps réel**

Pour plus d'informations, veuillez consulter la section Site public : Demande d'assistance technique à l'adresse https://www.beyondtrust.com/docs/remote-support/getting-started/customer-client/public-site.htm.

Traduction en temps réel de la messagerie instantanée

Lors d'une telle activation, les messages entre le client et un technicien d'assistance sont traduits en temps réel. Les clients qui démarrent des sessions au moyen du portail public peuvent sélectionner leur langue dans le menu déroulant situé en haut de la page. Les techniciens d'assistance peuvent choisir la langue qu'ils souhaitent depuis la page **Paramètres > Paramètres globaux** dans l'console du technicien d'assistance.

Pour que la traduction en temps réel soit disponible, saisissez l'URL de votre API GeoFluent. Pour les États-Unis, utilisez https://api.geofluent.com ; pour l'Europe, utilisez https://api-eu.geofluent.com. Ce champ peut être modifié. Indiquez ensuite votre **clé d'API** et votre **secret**, puis cliquez sur **Enregistrer**. Pour activer la fonction, cochez **Activer la traduction en temps réel de la messagerie instantanée**.

Pour plus d'informations, veuillez consulter la section Messagerie instantanée avec un utilisateur lors d'une session à l'adresse https://www.beyondtrust.com/docs/remote-support/getting-started/rep-console/chat.htm.

***Remarque :** vous devez d'abord créer un compte GeoFluent afin de pouvoir utiliser cette fonction. Pour plus d'informations, veuillez visiter https://www.lionbridge.com/.*

Paires de langues

Le tableau indique toutes les paires linguistiques disponibles pour la fonction de traduction en temps réel, depuis la langue A vers la langue B.

***Remarque :** la liste n'indique que les paires linguistiques auxquelles vous vous êtes abonné dans GeoFluent.*

Langues : gérer les langues installées

Localisation | Langues

Langues

BeyondTrust prend actuellement en charge l'anglais, l'allemand, l'espagnol d'Amérique latine, l'espagnol européen, le finnois, le français européen, l'italien, le néerlandais, le portugais brésilien, le portugais européen, le suédois, le turc, le japonais, le chinois simplifié, le chinois traditionnel et le russe. BeyondTrust prend en charge les jeux de caractères internationaux.

> ***Remarque :*** *en raison du temps nécessaire pour procéder à la traduction, la sortie des modules linguistiques s'effectue avec un léger décalage par rapport à la version anglaise, et ce, quelle que soit la version du logiciel. Notez également que pour certaines fonctions, la localisation est limitée à des caractères codés sur 1 octet. L'utilisation de caractères codés sur 2 octets (certains modules linguistiques) peut modifier le comportement attendu de certaines fonctions. L'interface de configuration Jumpoint BeyondTrust n'est pas traduite pour le moment.*

Activé

Si plus d'un paquet de langues est installé, cochez la case pour chaque langue que vous souhaitez activer. Cocher cette option signifie que cette langue sera disponible à partir du menu déroulant dans l'interface d'administration, la console du technicien d'assistance et le site public.

Langue par défaut

Si plus d'un paquet de langues est installé, sélectionnez une langue à afficher par défaut. Cliquez sur **Mettre à jour les langues** pour enregistrer les modifications.

Installation des modules linguistiques

Les modules linguistiques doivent être installés et activés par l'admin BeyondTrust. L'assistance technique BeyondTrust peut intégrer des modules linguistiques aux mises à jour logicielles à la demande des clients. Avant de demander un module linguistique, vérifiez qu'il n'est pas déjà installé et que la version active actuelle le prend en charge. Pour chercher des langues et obtenir les mises à jour nécessaires, suivez ces étapes :

1. Connectez-vous à l'interface Web **/login** de BeyondTrust en tant qu'utilisateur administrateur.
2. Allez sur l'onglet **Localisation** et cherchez les langues voulues.
3. Si les langues sont dans la liste, cochez la case de celles que vous souhaitez installer.
4. Si les langues ne sont pas dans la liste, contactez l'assistance technique pour qu'une mise à jour les intégrant soit créée.
5. Installez les mises à jour nécessaires et vérifiez si les langues voulues apparaissent dans BeyondTrust.

Les clients peuvent choisir la langue qu'ils veulent dans le menu déroulant **Langue** sur le portail public et sur la page d'enquête de satisfaction. Les techniciens d'assistance peuvent choisir la langue voulue sur l'écran de connexion. Les admins et les techniciens d'assistance peuvent choisir leur langue dans le menu déroulant de **/login** et **/appliance**.

Remarque : *il est possible d'utiliser dans la messagerie instantanée d'une session une langue qui n'est pas prise en charge par BeyondTrust, mais qui est prise en charge par GeoFluent. Veuillez consulter la section sur les paramètres facultatifs dans le Guide de l'API pour plus d'informations.*

Rechercher : affichage d'un texte personnalisé dans les langues activées

Localisation | Langues

Rechercher

Affichez tous les messages personnalisables sur une page. Entrez un mot ou une phrase dans la zone de recherche pour restreindre le champ. Cliquez sur le message que vous souhaitez modifier pour le voir s'afficher dans toutes les langues disponibles. Chaque message peut être modifié individuellement depuis cette page.

La **chaîne par défaut** ne peut pas être modifiée et sert uniquement de référence pour vos messages personnalisés. Si vous devez rétablir le texte initial d'un message, supprimez tout le texte de cette zone de texte et enregistrez le message vide. Le texte par défaut dans cette langue s'affiche de nouveau.

Gestion

Logiciel : Téléchargement d'une sauvegarde et mise à niveau logicielle

Paramètres de sauvegarde

L'enregistrement régulier d'une copie de sauvegarde de vos paramètres logiciels fait partie des meilleures pratiques de la reprise après sinistre. BeyondTrust vous recommande de sauvegarder la configuration de votre Serveur d'accès à distance sécurisé chaque fois que vous en modifiez les paramètres. En cas de problème matériel, un fichier de sauvegarde accélère la reprise et, si nécessaire, permet à BeyondTrust de vous donner accès à des services hébergés temporairement tout en conservant les paramètres de votre plus récente sauvegarde.

Mot de passe de sauvegarde

Créez un mot de passe pour protéger votre fichier de sauvegarde logicielle. Si vous choisissez de définir un mot de passe, vous ne pouvez pas revenir à la sauvegarde sans fournir le mot de passe.

Inclure les données de rapport de la session enregistrée

Si cette option est cochée, votre fichier de sauvegarde comportera les journaux de session. Si cette option est décochée, les données de rapport de session ne seront pas incluses dans la sauvegarde.

Télécharger la sauvegarde

Enregistrez une copie sécurisée de votre configuration logicielle. Enregistrez ce fichier dans un emplacement sûr.

Sauvegarder la clé de chiffrement Vault

La clé de chiffrement Vault est utilisée pour chiffrer et déchiffrer toutes les informations d'authentification Vault stockées sur votre Serveur d'accès à distance sécurisé. Si vous avez besoin de restaurer les données de configuration d'une sauvegarde sur un nouveau serveur, vous devez également restaurer la clé de chiffrement Vault à partir d'une sauvegarde pour être en mesure d'utiliser les informations d'authentification chiffrées Vault contenues dans la sauvegarde de la configuration.

Mot de passe de sauvegarde

Créez un mot de passe pour protéger votre fichier de sauvegarde logicielle. Si vous choisissez de définir un mot de passe, vous ne pouvez pas revenir à la sauvegarde sans fournir le mot de passe.

Télécharger la clé de chiffrement Vault

Cliquez sur le bouton **Télécharger la clé de chiffrement Vault** pour télécharger la clé de chiffrement Vault pour l'utiliser plus tard.

> ***Remarque :*** *la clé de chiffrement Vault doit être protégée par un mot de passe.*

Restaurer les paramètres

Fichier de sauvegarde de la configuration

Si vous avez besoin de rétablir une sauvegarde, naviguez jusqu'au dernier fichier de sauvegarde que vous avez enregistré.

Mot de passe de la sauvegarde de la configuration

Si vous avez créé un mot de passe pour votre fichier de sauvegarde, saisissez-le ici.

Fichier de sauvegarde de la clé de chiffrement Vault

Pour fournir la clé de chiffrement Vault correspondant à la sauvegarde de la configuration, choisissez le fichier de sauvegarde de la clé de chiffrement Vault.

Mot de passe de la sauvegarde de la clé de chiffrement Vault

Saisissez le mot de passe que vous avez utilisé pour télécharger la clé de chiffrement Vault BeyondTrust.

Transférer une sauvegarde

Transférez le fichier de sauvegarde sur votre Serveur d'accès à distance sécurisé et restaurez les paramètres de votre site comme ils étaient sur la sauvegarde.

> ***Remarque :*** *la restauration de la sauvegarde du site ne rétablit pas l'icône d'aide à l'image présente au moment de la sauvegarde et ne supprime pas les fichiers ajoutés depuis. Notez que tous les fichiers ne sont pas sauvegardés, seuls les 50 premiers fichiers de moins de 200 Ko le sont.*

> *Pour plus d'informations, veuillez consulter la section Procédures de sauvegarde à l'adresse https://www.beyondtrust.com/docs/remote-support/how-to/disaster-recovery/back-up-procedures.htm.*

Envoyer la mise à jour

Cliquez sur **Choisir le fichier** pour envoyer manuellement les nouveaux packages de logiciels provenant de BeyondTrust. Vous serez invité à confirmer que vous souhaitez télécharger le progiciel. La section **Mise à jour téléchargée** affiche des informations supplémentaires pour vérifier que vous avez téléchargé les programmes. Cliquez sur **Installer** si vous souhaitez terminer l'installation, ou sur **Supprimer la mise à jour** si vous souhaitez effacer la zone de mise à jour. Si le progiciel mis à jour contient uniquement des licences supplémentaires, vous pouvez installer la mise à jour sans redémarrer le serveur. Une fois que vous avez confirmé que vous souhaitez procéder à l'installation, cette page affiche une barre de progression vous informant de la progression générale de l'installation. Les mises à jour effectuées ici mettent automatiquement à jour l'ensemble des sites et licences sur votre Serveur d'accès à distance sécurisé.

Remarque : *l'administrateur de votre Serveur d'accès à distance sécurisé peut également utiliser la fonction* ***Rechercher les mises à jour*** *de l'interface serveur pour rechercher automatiquement et installer les nouveaux packages logiciels.*

Sécurité : Gestion des paramètres de sécurité

Mots de passe

Longueur minimum du mot de passe

Définissez des règles pour la longueur des mots de passe des comptes d'utilisateurs locaux.

Expiration du mot de passe par défaut

Définissez à quelle fréquence les mots de passe des comptes d'utilisateurs locaux doivent expirer.

Verrouillage du compte au bout de

Définissez le nombre de saisies incorrectes d'un mot de passe avant blocage du compte.

Exiger des mots de passe complexes

Définissez des règles pour la complexité des mots de passe des comptes d'utilisateurs locaux.

Autoriser la réinitialisation du mot de passe

Autorisez les utilisateurs ayant une adresse e-mail configurée à réinitialiser leurs mots de passe. Le lien fourni dans les e-mails de réinitialisation de mot de passe est valide jusqu'à ce qu'un des événements suivants se produise :

- Vingt-quatre heures se sont écoulées.
- Le lien a été cliqué, et le mot de passe a bien été réinitialisé.
- Le système envoie un autre lien à l'adresse e-mail.

Durée du verrouillage du compte

Définissez la durée d'attente d'un utilisateur bloqué avant qu'il puisse se reconnecter. Vous pouvez aussi demander à un administrateur de débloquer son compte.

Console du technicien d'assistance

Mettre fin à la session si le compte est en cours d'utilisation

Si un utilisateur essaie de se connecter à la console du technicien d'assistance avec un compte en cours d'utilisation et que la case **Mettre fin à la session** est cochée, la connexion précédente est interrompue pour autoriser la nouvelle connexion.

Autoriser l'enregistrement des informations de connexion

Autorisez ou non la console du technicien d'assistance à mémoriser les informations d'authentification d'un utilisateur.

Déconnecter un technicien d'assistance inactif au bout de

Définissez le délai d'attente avant qu'un utilisateur inactif ne soit déconnecté d'une console du technicien d'assistance, afin de permettre à un autre utilisateur d'y accéder.

Activer l'alerte et la notification de déconnexion sur les délais d'inactivité dépassés

Définissez sur un utilisateur doit recevoir une invite avant d'être déconnecté en raison de son inactivité. La première notification se produit 30 secondes avant la déconnexion, et la seconde lorsque la déconnexion a eu lieu.

Méthode d'authentification par défaut de la console du technicien d'assistance

Sélectionnez la méthode d'authentification par défaut. La méthode d'authentification sélectionnée ici sera automatiquement sélectionnée sur la page de connexion lorsque le technicien d'assistance se connectera à la console du technicien d'assistance la prochaine fois que le paramètre aura été modifié. Les techniciens d'assistance peuvent au besoin sélectionner une méthode différente.

Vous pouvez modifier le paramètre à tout moment. Cependant, vous devez vous déconnecter de la console du technicien d'assistance et vous reconnecter pour voir le changement.

Retirer un technicien d'assistanced'une session après une inactivité

Cette option oblige un utilisateur à abandonner la session après une période d'inactivité définie. Ceci aide les clients BeyondTrust à satisfaire aux initiatives de conformité en matière d'inactivité. L'utilisateur reçoit une notification 1 minute avant la déconnexion et a la possibilité de réinitialiser le délai d'attente.

Un utilisateur est considéré comme actif dans une session lorsqu'un fichier est en cours de transfert, par le biais de onglet de transfert ou de l'interface de la messagerie, ou lorsqu'il clique sur la souris ou qu'il appuie sur un bouton de l'onglet de session. Le simple déplacement de la souris n'est pas considéré comme une activité. Dès l'interruption d'une activité, le compteur d'inactivité est mis en marche.

Autoriser la Console du technicien d'assistance mobile et la Console Web du technicien d'assistance à se connecter

Donnez aux utilisateurs la possibilité d'accéder à des systèmes distants à travers l'appli de la console du technicien d'assistance pour iOS et Android, ainsi qu'à travers la console Web du technicien d'assistance, une console du technicien d'assistance sur navigateur.

Afficher la vue en miniature dans la Console du technicien d'assistance

Lors d'une assistance technique apportée à un client ayant plusieurs écrans, cette option permet à l'utilisateur de voir des miniatures de tous les écrans disponibles. Ces miniatures ne sont pas enregistrées dans l'enregistrement de la session. Décochez cette case pour afficher des rectangles à la place des miniatures.

Autoriser les techniciens d'assistance à faire des captures d'écran distantes

Vous pouvez autoriser les utilisateurs à effectuer des captures d'écran du bureau distant depuis la console du technicien d'assistance.

Autoriser les techniciens d'assistance à contrôler la fenêtre du client d'utilisateur

L'activation de ce paramètre permet au technicien d'assistance d'agir en tant qu'utilisateur dans la fenêtre du client d'utilisateur, notamment en saisissant dans la messagerie instantanée, en envoyant des fichiers et en interagissant avec des liens et des boutons.

Lorsque ce paramètre est désactivé, le contrôle de la fenêtre du client d'utilisateur par le technicien d'assistance se limite à la déplacer et à la réduire.

Lors d'une demande d'accroissement des droits, autorisez la saisie des informations d'authentification

Lors de l'accroissement d'une session pour qu'elle ait des droits d'administration, autorisez les utilisateurs à saisir manuellement les informations d'authentification, à les injecter à partir d'une banque de mots de passe ou à les fournir via une carte à puce virtuelle. Cela permet aux utilisateurs d'utiliser des informations d'authentification privilégiées autorisées pour accroitre le contexte du client d'utilisateur. Une fois accru, le client d'utilisateur s'exécutera dans le contexte du système local.

Autoriser le redémarrage avec des informations d'authentification cachées

Dans une session d'assistance technique s'exécutant avec les droits administratifs sur un ordinateur Windows distant, cela permet à un technicien d'assistance de redémarrer la machine distante sans l'assistance du client en demandant à l'utilisateur de saisir ses informations d'authentification avant le redémarrage. Ces informations d'authentification peuvent être enregistrées pendant la durée de la session d'assistance technique, permettant à la machine de se connecter automatiquement lorsqu'elle est redémarrée plusieurs fois.

Mode de synchronisation du presse-papiers

Le **Mode de synchronisation du presse-papiers** détermine comment les utilisateurs sont autorisés à synchroniser les presse-papiers lors d'une session de partage d'écran. Les paramètres disponibles sont les suivants :

- **Automatique :** Les presse-papiers du client et du technicien d'assistance sont automatiquement synchronisés lorsque l'un ou l'autre change.
- **Mises à jour manuelles :** Le technicien d'assistance doit cliquer sur l'une des icônes du presse-papiers sur la console du technicien d'assistance pour envoyer du contenu ou extraire du contenu du presse-papiers du point de terminaison.

vous DEVEZ redémarrer le logiciel sur la page d'état pour que ce paramètre prenne effet.

Les administrateurs peuvent empêcher les techniciens d'assistance d'accéder au presse-papiers, les autoriser à envoyer des données au point de terminaison ou à accéder dans les deux sens (envoyer et recevoir des données). Ces paramètres contrôlent les icônes de presse-papiers que le technicien d'assistance voit dans la console du technicien d'assistance lorsque le mode **Manuel** est sélectionné, ainsi que le déroulement de la synchronisation en mode **Automatique**.

Un contrôle granulaire de l'accès au presse-papiers peut être défini pour les règles de session et celles de groupe, ainsi qu'être octroyé à des techniciens d'assistance spécifiques. Veuillez consulter les liens ci-dessous pour chaque cas particulier :

- **« Utilisateurs : ajout d'autorisations utilisateur pour un technicien d'assistance ou un administrateur », page 93 : Utilisateurs et sécurité > Utilisateurs > Ajouter > Autorisations relatives aux sessions autonomes et non autonomes > Partage d'écran**
- **« Règles de session : Configuration de règles de demande et d'autorisation de session », page 128 : Utilisateurs et sécurité > Règles de session > Ajouter > Autorisation > Partage d'écran**
- **« Règles de groupe : Application d'autorisations utilisateur à des groupes d'utilisateurs », page 137 : Utilisateurs et sécurité > Règles de groupe > Ajouter > Autorisations relatives aux sessions non autonomes [défini]**

Clé de session

Longueur de clé de session

La **Longueur de clé de session** peut être réglée selon tout nombre de caractères, entre 7 et 20.

Clé de session à utilisation unique

Si l'option **Clé de session à utilisation unique** est cochée, une clé de session ne peut pas être utilisée plus d'une fois pour créer une session d'assistance technique.

Délai d'expiration maximum d'une clé de session

Durée de vie maximale d'une clé de session détermine la durée maximale pendant laquelle une clé de session peut rester valide. Dans la console du technicien d'assistance, un utilisateur peut définir la durée de vie de chaque clé de session générée, sans dépasser celle définie sur cette page. Si le client n'utilise pas la clé de session dans le délai imparti, elle expire et l'utilisateur devra émettre une nouvelle clé de session pour lancer une session.

Portail public

Forcer le site public à utiliser le HTTPS

Il est possible d'obtenir une sécurité supplémentaire avec **Forcer le site public à utiliser SSL (https)**. L'utilisation de HTTPS force la connexion Internet vers votre portail public d'assistance technique à utiliser le cryptage SSL, ajoutant une couche de sécurité supplémentaire pour empêcher les utilisateurs non autorisés d'accéder aux comptes.

Bloquez les ressources externes, les scripts inline et les styles inline sur le site public

Empêchez votre site public de charger des ressources externes, d'exécuter des scripts inline ou d'afficher des styles inline. Cette option est activée en envoyant l'en-tête HTTP Content-Security-Policy (CSP) avec la valeur **default-src 'self'**.

L'en-tête CSP ordonne au navigateur d'ignorer les ressources comme les images, les polices de caractère, les feuilles de style, les scripts, les cadres et d'autres sous-ressources venant d'ailleurs que son domaine d'origine. Il ignorera également les scripts et les styles inline, qu'ils soient inclus dans l'en-tête ou le corps de la page. Ceci affecte également les scripts et les styles inline ajoutés de façon dynamique lors de l'exécution avec JavaScript.

Toutes les ressources que vous souhaitez utiliser doivent être transférées sur le serveur dans **Portails publics > Magasin de fichiers**. N'activez pas cette option si vous avez personnalisé le modèle de votre site public pour qu'il utilise des scripts inline, des styles inline ou des ressources externes à votre site BeyondTrust.

Activer le démarrage de session simplifié

Tentez de démarrer des sessions en utilisant ClickOnce ou Java. Si cette option est décochée, le client d'utilisateur doit être téléchargé et lancé manuellement.

Désactiver l'indexation du site public

Cochez **Désactiver l'indexation du site public** pour empêcher les moteurs de recherche d'indexer les sites publics hébergés sur votre Serveur d'accès à distance sécurisé.

Divers

Nombre de jours de conservation des informations enregistrées

Dans **Nombre de jours de conservation des informations enregistrées**, définissez la durée pendant laquelle les informations de journalisation doivent être stockées sur le serveur. Ces informations comprennent les données de rapport de la session ainsi que les enregistrements. Vous pouvez conserver les données de rapport et d'enregistrement d'une session sur un Serveur d'accès à distance sécurisé pendant 90 jours au maximum. Il s'agit de la valeur par défaut pour une nouvelle installation. Il arrive que les enregistrements de certaines sessions ne soient pas disponibles, même lorsque la limite de conservation n'est pas dépassée. Les contraintes liées à l'espace du disque ou le paramètre **Nombre de jours de conservation des informations enregistrées** peuvent être à l'origine de ce problème.

Le Serveur d'accès à distance sécurisé exécute un script de maintenance chaque jour pour vérifier que l'utilisation du disque est inférieure à 90 %. Si cette limite est dépassée, le script supprime les enregistrements de session selon une formule donnée jusqu'à ce que l'utilisation du disque soit inférieure à 90 %. Si le paramètre **Nombre de jours de conservation des informations enregistrées** a été modifié récemment, il est possible qu'il ne soit pris en compte qu'après un délai de 24 heures.

> *Lorsqu'on souhaite conserver les données ou les enregistrements au-delà du délai fixé, BeyondTrust conseille d'utiliser le Client d'intégration (www.beyondtrust.com/docs/remote-support/how-to/integrations/ic) ou l'API de rapport (www.beyondtrust.com/docs/remote-support/how-to/integrations/api/reporting).*

Clé pré-partagée de communication entre serveurs

Entrez un mot de passe dans le champ **Clé pré-partagée de communication entre instances** pour établir une relation de confiance entre deux serveurs. Des clés correspondantes sont requises pour la configuration de deux serveurs ou plus pour des fonctions, telles que la reprise en séquence ou le clustering. La clef doit comporter au moins 6 caractères et contenir au moins une lettre majuscule, une lettre minuscule, un chiffre et un caractère spécial.

Activer la récupération de l'historique de la messagerie instantanée

Cochez cette case pour que la fenêtre de messagerie instantanée récupère les messages de discussion si une session est interrompue puis reprise.

Exige la vérification de client Remote Support lors des tentatives d'accroissement

Vous devez fournir une vérification de client Remote Support lors des accroissements.

Validation du certificat SSL

Vous pouvez également demander à ce que la **Validation du certificat SSL** force le logiciel BeyondTrust (y compris chaque console du technicien d'assistance, chaque client d'utilisateur, les clients de présentation et les Jump Clients) à vérifier que la chaîne du certificat est reconnue, que le certificat n'a pas expiré et que le nom du certificat correspond au nom d'hôte du Serveur d'accès à distance sécurisé. Si la chaîne du certificat ne peut être correctement validée, la connexion est impossible.

Si la vérification du certificat a été désactivée puis activée, toutes les consoles et tous les clients sont automatiquement mis à niveau lors de leur prochaine connexion. Notez que les agents de connexion LDAP ne sont pas automatiquement mis à niveau, mais doivent être réinstallés pour permettre à ce paramètre de prendre effet.

Lorsque la **Validation du certificat SSL** est activée, des contrôles de sécurité sont effectués en complément de la sécurité intégrée de BeyondTrust afin de valider la chaîne du certificat SSL utilisée pour sécuriser les communications. Il est vivement conseillé d'activer la validation SSL. Si la validation du certificat est désactivée, un message d'avertissement apparaît sur votre interface d'administration. Vous pouvez le masquer pendant trente jours.

Remarque : *pour activer la validation du certificat SSL, vous devez fournir votre certificat SSL à BeyondTrust pour qu'il soit incorporé à votre logiciel BeyondTrust.*

Pour plus d'informations, veuillez consulter la section Certificats SSL et Remote Support BeyondTrust à l'adresse https://www.beyondtrust.com/docs/remote-support/how-to/sslcertificates/index.htm.

Restrictions de réseau

Déterminez quels réseaux IP peuvent accéder à /login, à /api et à la console du technicien d'assistance sur votre Serveur d'accès à distance sécurisé. Si vous activez des restrictions réseau, vous pouvez également définir les réseaux sur lesquels une console du technicien d'assistance ou plusieurs peuvent être utilisées.

Définir les règles réseau pour les interfaces suivantes :

Interface d'administration (/login) et interface API (/api)

- **Toujours appliquer des restrictions réseau** : lorsque sélectionnée, vous avez la possibilité de créer soit une liste blanche contenant uniquement les réseaux autorisés, soit une liste noire contenant les réseaux auxquels l'accès est refusé. Lorsque cette option est sélectionnée, vous pouvez déterminer quelles restrictions, le cas échéant, devraient s'appliquer aux consoles d'accès bureau, mobile et Web.
- **Ne jamais appliquer de restrictions réseau** : lorsque sélectionnée, aucune restriction n'est appliquée et aucune autre option ne permet d'appliquer de restrictions pour les consoles bureau, mobile et Web.

Console du technicien d'assistance mobile et de bureau

- **Toujours appliquer des restrictions réseaux** : lorsque sélectionnée, elle hérite des restrictions réseau mises en place pour l'interface d'administration.
- **Ne jamais appliquer de restrictions réseau** : lorsque cette option est sélectionnée, aucune restriction n'est appliquée aux consoles bureau et mobile, mais vous avez la possibilité d'appliquer des restrictions pour la console du technicien d'assistance.
- **N'appliquer des restrictions réseau que pour la première authentification d'un utilisateur** : cela applique les restrictions sélectionnées ci-dessus, mais seulement lors de la première connexion d'un utilisateur.

Console Web (/console)

- **Toujours appliquer des restrictions réseau** : lorsque cette option est sélectionnée, la console du technicien d'assistance hérite des restrictions mises en place pour l'interface d'administration.
- **Ne jamais appliquer de restrictions réseau** : lorsque cette option est sélectionnée, aucune restriction n'est appliquée à la console du technicien d'assistance, même si des restrictions sont en place pour les autres méthodes de console d'accès.

Pour plus d'informations, veuillez consulter le Guide de la Console Web du technicien d'assistance à l'adresse https://www.beyondtrust.com/docs/remote-support/getting-started/rep-web/index.htm.

Définissez vos restrictions réseau :

Saisissez les préfixes d'adresse réseau, à raison d'un par ligne. Le masque de réseau est facultatif, et peut être fourni soit sous forme décimale pointée, soit sous forme d'un entier représentant un ensemble de bits de masquage (bitmask). Les entrées sans masque de réseau sont considérées comme des adresses IP seules.

- **Liste blanche** : n'autoriser que les réseaux spécifiés.
- **Liste noire** : bloquer les réseaux spécifiés.

Restrictions de ports pour l'interface Web d'administration

Définissez les ports d'accès à l'interface /login.

Configuration du proxy

Configurez un serveur proxy pour contrôler le flux de données pour les informations envoyées par le serveur. Cela s'applique aux événements sortants et aux appels d'API.

Protocole proxy

Configurez les types de proxy HTTP ou HTTPS pour la connectivité sortante à partir du serveur.

Activer la configuration du proxy

Cochez la case pour activer les paramètres de proxy sortant.

Hôte proxy

Saisissez l'adresse IP ou le nom d'hôte de votre serveur proxy.

Port proxy

Saisissez le port qu'utilise votre serveur proxy. Le port par défaut est **1080**.

Nom d'utilisateur et mot de passe de proxy

Si votre serveur proxy requiert une authentification, indiquez un nom d'utilisateur et un mot de passe.

Tester

Cliquez sur **Tester** pour vous assurer que les paramètres de configuration sont correctement saisis. Le résultat actuel du test est affiché dans la zone **Dernier résultat du test**. Les messages d'erreur indiquent ce qui doit être corrigé dans les paramètres de configuration.

Configuration du site : configuration des ports HTTP et activation de l'accord de connexion

Gestion | Configuration du Site

Ports HTTP

Port HTTP et port HTTPS

Il est possible pour les techniciens de réseaux expérimentés qui travaillent dans des environnements réseau non standard de changer les ports de trafic de BeyondTrust. Ces paramètres ne doivent être ajustés que lorsque des ports autres que les ports standard 80 et 443 sont utilisés pour l'accès Web.

Accord de connexion à /login

Activer l'accord de connexion

Vous pouvez activer un accord de connexion que les utilisateurs devront accepter pour pouvoir accéder à l'interface d'administration /login. Cet accord configurable permet de spécifier des restrictions et des règles de politique interne relatives aux connexions utilisateur.

Titre de l'accord

Personnalisez le titre de l'accord. Vous pouvez traduire ce texte dans les langues que vous avez activées. Pour revenir au texte par défaut, supprimez le texte du champ puis enregistrez le champ vide.

Texte de l'accord

Saisissez le texte pour l'accord de connexion. Vous pouvez traduire ce texte dans les langues que vous avez activées. Pour revenir au texte par défaut, supprimez le texte du champ puis enregistrez le champ vide.

Configuration e-mail : configuration de l'envoi des e-mails

Gestion | **Configuration e-mail**

Adresse e-mail

Remarque : *lorsqu'un serveur est désigné comme étant un serveur de sauvegarde ou un nœud de trafic, la configuration des e-mails pour ce serveur sera remplacée par celle définie sur le serveur maître principal.*

Adresse de l'expéditeur

Définissez l'adresse e-mail à partir de laquelle seront envoyés les messages automatiques de votre Serveur d'accès à distance sécurisé.

Serveur relais SMTP

Configurez votre Serveur d'accès à distance sécurisé pour qu'il fonctionne avec votre serveur relais SMTP, afin d'envoyer automatiquement des notifications par e-mail de certains événements.

Serveur relais SMTP

Indiquez le nom d'hôte ou l'adresse IP de votre serveur relais SMTP.

Port SMTP

Indiquez le port SMTP sur lequel contacter ce serveur.

Cryptage SMTP

Selon vos paramètres de serveur SMTP, choisissez **TLS**, **STARTTLS** ou **Aucun**.

Nom d'utilisateur SMTP

Si votre serveur SMTP requiert une authentification, indiquez un nom d'utilisateur.

Mot de passe SMTP

Si votre serveur SMTP requiert une authentification, indiquez un mot de passe.

Contact administrateur

Adresses e-mail du contact administrateur par défaut

Saisissez une ou plusieurs adresses auxquelles les e-mails doivent être envoyés. Séparez les adresses avec une espace.

Envoyer un avis de communication tous les jours

Vous pouvez demander à recevoir un avis de communication quotidien du Serveur d'accès à distance sécurisé pour vérifier le bon fonctionnement des alertes.

Envoyer un e-mail de test lorsque les paramètres sont enregistrés

Si vous souhaitez recevoir un e-mail de test pour vérifier immédiatement la bonne configuration de vos paramètres SMTP, cochez cette option avant de cliquer sur le bouton **Enregistrer**.

En plus de l'e-mail de test et des avis de communication qui peuvent être configurés ci-dessus, des e-mails sont envoyés pour les évènements suivants :

- Lors de toute opération de reprise en séquence, la version de produit du nœud principal ne correspond pas à la version de produit du nœud de sauvegarde.
- Lors d'un contrôle d'état de reprise en séquence, l'un des problèmes suivants est détecté.
    - Le serveur actuel est le nœud principal et une adresse IP partagée est configurée dans /login, mais l'interface réseau n'est pas activée.
    - Une adresse IP partagée est configurée dans /login, mais n'est pas répertoriée comme adresse IP dans /appliance.
    - Le nœud de sauvegarde n'a pas pu contacter ni le nœud principal ni aucune des adresses IP de test configurées sur la page **Gestion > Reprise en séquence**.
    - Le nœud de sauvegarde n'a pu contacter aucune des adresses IP de test configurées sur la page **Gestion > Reprise en séquence**.
    - Les opérations de sauvegarde du nœud de sauvegarde ont été désactivées sur la page **Gestion > Reprise en séquence**.
    - Le nœud de sauvegarde n'a pas réussi à se sonder lui-même, ce qui indique qu'il ne fonctionne pas correctement.
    - Le nœud de sauvegarde n'a pas réussi à contacter le nœud principal en utilisant le nom d'hôte du nœud principal.
    - La reprise en séquence automatique est désactivée, et le nœud de sauvegarde n'a pas réussi à sonder le nœud principal.
    - La reprise en séquence automatique est activée, et le nœud de sauvegarde n'a pas réussi à sonder le nœud principal. Le nœud de sauvegarde deviendra automatiquement le nœud principal si le nœud principal ne répond pas.
    - La reprise en séquence automatique est activée, et le nœud de sauvegarde devient automatiquement le nœud principal parce que le nœud principal est resté inactif pendant trop longtemps.
    - Le nœud principal n'a pas réussi à synchroniser des données avec le nœud de sauvegarde au cours des 24 dernières heures.

Événements sortants : configuration des événements déclenchant l'envoi de messages

Destinataires HTTP

Vous pouvez configurer votre Serveur d'accès à distance sécurisé pour qu'il envoie des messages à un serveur HTTP ou à une adresse e-mail lorsque différents événements sont déclenchés.

Les variables envoyées par le Serveur d'accès à distance sécurisé arrivent par la méthode HTTP POST et sont accessibles via la méthode utilisée pour récupérer les données POST dans votre langage de codage. Si le serveur ne vous adresse pas une réponse HTTP 200 pour indiquer la réussite de l'opération, le Serveur d'accès à distance sécurisé remet l'événement dans la file d'attente et réessaie ultérieurement.

Ajouter, modifier, supprimer

Créer un nouveau destinataire, modifier ou supprimer un destinataire existant.

Ajouter ou modifier un destinataire HTTP

Activé

Vous pouvez décocher **Activé(e)** pour interrompre rapidement les messages pour le gestionnaire d'événements que vous avez mis en place, comme dans le cas d'un test d'intégration planifié.

Nom

Créez un nom unique permettant d'identifier ce destinataire.

URL

Saisissez une URL de destination pour ce gestionnaire d'événements sortants.

Utiliser un certificat AC

Lorsque vous utilisez une connexion HTTPS, vous devez transférer le certificat racine de l'autorité de certificat annoncé par le serveur d'évènements sortants.

Envoyer des champs personnalisés

Choisissez si les champs personnalisés et leurs valeurs doivent être envoyés avec l'événement sortant.

Événements à transmettre

Choisissez les événements qui doivent déclencher l'envoi de messages.

Intervalle entre tentatives

Définissez combien de fois il faut relancer après un échec de connexion.

Durée totale des tentatives

Si un événement continue d'échouer malgré les différentes tentatives, déterminez au bout de combien de temps abandonner.

Contact e-mail

Entrez une ou plusieurs adresses de messagerie auxquelles envoyer une notification en cas d'erreur.

Transmettre une alerte par e-mail

Déterminez au bout de combien de temps un e-mail doit être envoyé ; si le problème est résolu avant la fin de ce délai et si l'événement aboutit, aucune notification d'erreur n'est envoyée.

Retransmettre les alertes e-mail

Définissez à quelle fréquence envoyer des e-mails d'erreur si l'échec se prolonge.

Destinataires de messagerie

Ajouter, modifier, supprimer

Créer un nouveau destinataire, modifier ou supprimer un destinataire existant.

Durée totale des tentatives

Si un événement continue d'échouer malgré les différentes tentatives, déterminez au bout de combien de temps abandonner.

Ajouter ou modifier le destinataire de l'e-mail

Avant de configurer le Serveur d'accès à distance sécurisé pour envoyer des messages d'événement à une adresse e-mail, vérifiez que votre Serveur d'accès à distance sécurisé est bien configuré pour utiliser le serveur relais SMTP. Accédez à la page **Gestion > Configuration e-mail** pour vérifier les paramètres.

Activé

Utilisez la case **Activé(e)** pour interrompre rapidement les messages pour le gestionnaire d'événements que vous avez mis en place, comme dans le cas d'un test d'intégration planifié.

Nom

Créez un nom unique permettant d'identifier ce destinataire.

E-mail

Saisissez l'adresse e-mail à laquelle doit être envoyée la notification des événements sélectionnés. Vous pouvez configurer jusqu'à dix adresses e-mail séparées par des virgules.

Clé externe requise

Si cette option est cochée, les e-mails ne seront envoyés que pour les sessions possédant une clé externe lors de la survenue de l'événement.

Événements à transmettre

Choisissez les événements qui doivent déclencher l'envoi de messages.

Objet

Personnalisez l'objet de cet e-mail. Vous pouvez traduire ce texte dans les langues que vous avez activées. Pour revenir au texte par défaut, supprimez le texte du champ puis enregistrez le champ vide.

Corps

Personnalisez le texte de cet e-mail. Utilisez les macros répertoriées sous ce champ dans la page /login pour personnaliser le texte selon vos besoins. Vous pouvez traduire ce texte dans les langues que vous avez activées. Pour revenir au texte par défaut, supprimez le texte du champ puis enregistrez le champ vide.

> *Pour plus d'informations, veuillez consulter le Guide de référence des événements sortants -- Variables et macros à l'adresse https://www.beyondtrust.com/docs/remote-support/how-to/integrations/outbound-events/index.htm.*

Cluster : configuration de la technologie Atlas pour l'équilibrage de charge

Gestion > Cluster

État

Les déploiements géographiques à grande échelle tirent parti de la technologie de cluster BeyondTrust Atlas, établissant un site BeyondTrust unique sur plusieurs serveurs, appelés nœuds dans un cluster. Le nœud serveur maître/serveur principal est le site de la plupart des tâches d'administration. Le nœud de trafic est un Serveur d'accès à distance sécurisé qui participe à l'acheminement efficace de votre trafic d'assistance technique.

Sur le nœud maître principal, vous pouvez configurer le maître principal lui-même et les nœuds de trafic.

> *Vous trouverez plus d'informations sur Atlas dans le Guide de la technologie BeyondTrust Atlas, disponible à l'adresse https://www.beyondtrust.com/docs/remote-support/how-to/atlas.*

Statut actuel

Confirme le rôle de l'instance de site depuis laquelle vous avez accédé à la page.

Nœud(s) maître(s)

Affiche une liste de tous les nœuds maîtres disponibles.

Synchroniser maintenant

Synchronisez les serveurs en cluster.

Démanteler le cluster

Démantelez le cluster, ce qui supprime chaque serveur de son rôle dans le cluster.

Historique de l'état

Affichez ou masquez le journal des messages de serveur en cluster.

Nœuds de trafic

Méthode de sélection des nœuds de trafic

Ce menu est utilisé pour définir la sélection d'un nœud de trafic pour la connexion d'un technicien d'assistance ou d'un client d'utilisateur. Les méthodes disponibles pour définir la connexion sont les suivantes : **Aléatoire**, **Recherche d'enregistrement**, **Recherche d'enregistrement SRV**, **Anycast IP** et **Décalage horaire**. La méthode de connexion choisie dépend en grande partie de votre infrastructure réseau, entre autres considérations complexes.

Ajouter, modifier, supprimer

Créer un nouveau nœud, modifier un nœud existant, ou supprimer un nœud existant.

Accepte les nouvelles connexions de clients

Vérifiez que cette option est cochée sans quoi les clients ne pourront pas utiliser le nœud de trafic.

Ajouter le nœud de trafic

Accepte les nouvelles connexions de clients

Si activé, les nouvelles connexions d'utilisateurs pourront passer par ce nœud. Si vous désactivez les nouvelles connexions d'utilisateur pour ce nœud, les connexions existantes ne sont pas affectées.

> ***Remarque :*** *si cette option n'est pas cochée, les utilisateurs ne pourront pas utiliser le nœud de trafic.*

Nom

Créez un nom unique permettant d'identifier ce nœud.

Adresse publique

Saisissez le nom d'hôte que vous avez mis comme DNS pour ce nœud, et le port sur lequel les clients vont communiquer avec le nœud.

Décalage horaire

S'utilise uniquement si la **méthode de sélection des nœuds de trafic** est définie sur **Décalage horaire**. Ce processus implique la détection du paramètre de fuseau horaire de la machine hôte et l'utilisation de ce paramètre pour associer le nœud de trafic approprié qui possède le décalage horaire le plus proche. Le décalage horaire est dérivé du paramètre de fuseau horaire du client par rapport au temps universel coordonné (UTC).

Adresse interne

Il peut s'agir de la même adresse que celle utilisée pour l'adresse publique. Des configurations avancées peuvent la définir en option sur un autre nom d'hôte pour une communication inter-serveur.

Préfixes d'adresse réseau

Cette zone peut rester vierge.

Pour les configurations avancées, saisissez les préfixes d'adresse réseau, à raison d'un par ligne, sous la forme **ip.add.re.ss[/masque de réseau]**. Le masque de réseau est facultatif et peut être fourni sous forme décimale pointée ou sous forme d'un entier représentant un ensemble de bits de masquage (bitmask). Si le masque de réseau n'est pas indiqué, une adresse IP unique est supposée.

Si ce champ est renseigné, le nœud maître tente d'assigner un client à ce nœud de trafic si l'adresse IP du client correspond à l'un des préfixes d'adresse réseau. Si l'adresse IP du client correspond à plusieurs préfixes d'adresse réseau de nœuds de trafic, le client est assigné au nœud de trafic ayant la plus longue correspondance de préfixe. Si les préfixes d'adresse réseau correspondants ont une longueur identique, l'un des nœuds de trafic correspondants est choisi aléatoirement. Si l'adresse IP d'un client ne correspond à aucun préfixe d'adresse réseau, le client utilisera la méthode de sélection configurée.

Configuration du nœud maître

Nœud maître primaire

Nom

Créez un nom unique permettant d'identifier ce nœud.

Adresse publique

Saisissez le nom d'hôte que vous avez mis comme DNS pour ce nœud, et le port sur lequel les clients vont communiquer avec le nœud.

Adresse interne

Il peut s'agir de la même adresse que celle utilisée pour l'adresse publique. Des configurations avancées peuvent la définir en option sur un autre nom d'hôte pour une communication inter-serveur.

Sauvegarde du nœud maître

L'instance de site actuelle est la principale dans une relation de reprise en séquence. Si les rôles de reprise en séquence sont inversés, l'instance de site de sauvegarde devient le nouveau nœud maître du cluster. Vous pouvez configurer la configuration des nœuds du cluster pour l'instance de sauvegarde ci-dessous. L'instance de site de sauvegarde sera automatiquement retirée du cluster si la relation de reprise en séquence est rompue.

Nom

Créez un nom unique permettant d'identifier ce nœud.

Adresse publique

Saisissez le nom d'hôte que vous avez mis comme DNS pour ce nœud, et le port sur lequel les clients vont communiquer avec le nœud.

Adresse interne

Il peut s'agir de la même adresse que celle utilisée pour l'adresse publique. Des configurations avancées peuvent la définir en option sur un autre nom d'hôte pour une communication inter-serveur.

Reprise de client maximum sur le maître

Permet au nombre de clients que vous définissez de revenir au maître pour contrôler le trafic si nécessaire.

Lorsqu'un client est dans l'incapacité de choisir un nœud de trafic par défaut viable (pour des raisons d'erreurs de configuration temporaires, de problèmes de DNS, d'incompatibilités logicielles, etc.), il devra se résoudre à utiliser le nœud maître comme nœud de trafic par défaut. Pour éviter de surcharger le trafic réseau sur le nœud maître, cette valeur sert à limiter le nombre de clients pouvant se replier simultanément sur le nœud maître.

Reprise en séquence : configuration d'un serveur de sauvegarde pour la reprise en séquence

Gestion > Reprise en séquence

Pour plus d'informations, veuillez consulter la section Configuration de la reprise en séquence à l'adresse https://www.beyondtrust.com/docs/remote-support/how-to/failover/index.htm.

Configuration

Mise en place d'une relation de reprise en séquence

Informations de connexion du nouveau site de sauvegarde

Nom de l'hôte ou adresse IP

Saisissez le nom d'hôte ou l'adresse IP du Serveur d'accès à distance sécurisé que vous souhaitez utiliser comme sauvegarde dans une relation de reprise en séquence.

Port

Saisissez le port TLS permettant à ce serveur principal de se connecter au serveur de sauvegarde.

Rapporter les informations de connexion à ce site primaire

Nom de l'hôte ou adresse IP

Saisissez le nom d'hôte ou l'adresse IP de ce Serveur d'accès à distance sécurisé que vous souhaitez utiliser comme serveur principal dans une relation de reprise en séquence.

Port

Saisissez le port TLS permettant au serveur de sauvegarde de se connecter au serveur principal.

État

Statut de cet hôte

Afficher le nom d'hôte de ce site, ainsi que son état d'instance de site principal ou d'instance de site de sauvegarde.

Statut de l'hôte pair

Afficher le nom d'hôte de ce site, ainsi que son état d'instance de site principal ou d'instance de site de sauvegarde. Afficher également la date et l'heure de la dernière vérification d'état.

Historique de l'état

Développez ou réduisez un tableau des évènements d'état qui se sont produits.

État de l'instance de site principal ou de sauvegarde

Un texte confirme que vous vous trouvez sur l'instance de site principal ou sur l'instance de site de sauvegarde de votre site hôte.

Synchroniser maintenant

Forcer manuellement une synchronisation de données du serveur principal vers le serveur de sauvegarde.

Devenir sauvegarde/principal

Alternez les rôles avec le serveur pair, ce qui force une reprise en séquence pour une opération de maintenance ou un événement de reprise en séquence connu.

Cochez cette case pour extraire une synchronisation des données de l'instance de site sur example.com tout en devenant la sauvegarde/principale.

Pour synchroniser les données du serveur pair avant d'échanger les rôles, cochez cette case. Si cette option est sélectionnée, tous les utilisateurs du serveur principal sont déconnectés pendant la synchronisation et aucune opération n'est possible pendant l'opération d'échange.

Cochez cette case pour devenir une sauvegarde même si l'instance du site pair sur example.com ne peut être contactée.

Sur l'instance de site principal, vous pouvez passer en site de sauvegarde même si le serveur pair ne peut être contacté. Si cette option est désélectionnée, la reprise en séquence est annulée si les deux serveurs ne peuvent être maintenus en synchronisation en termes de rôles de reprise en séquence (un serveur principal et un serveur de sauvegarde).

Par exemple, si vous savez que le serveur de sauvegarde est en ligne mais que le serveur principal ne peut le contacter en raison d'un problème de connexion réseau, vous pouvez sélectionner cette option afin de faire du serveur principal le serveur de sauvegarde en attendant de restaurer la connexion réseau. Dans cet exemple, vous devez également accéder au serveur de sauvegarde afin d'en faire le serveur principal.

Rompre les relations de reprise en séquence

Brisez la relation de la reprise en séquence, ce qui supprime chaque serveur de son rôle principal ou de sauvegarde.

Configuration de l'instance de site principal ou de sauvegarde

IP partagées

Contrôlez les adresses IP partagées que l'instance de site utilise au cas où une reprise en séquence viendrait à se produire. Il suffit pour cela de cocher la case de l'adresse IP de reprise en séquence. Si vous modifiez la relation entre les sites, les adresses IP sélectionnées seront désactivées lorsque le site principal deviendra site de sauvegarde, et seront activées lors de l'opération inverse. Vous devrez copier manuellement ce réglage sur le site pair, car il n'est pas partagé.

Paramètres de sauvegarde

Les paramètres que vous configurez ici deviennent actifs lorsque l'instance de site que vous configurez passe en mode sauvegarde.

Sur l'instance de site principal, sélectionnez **Paramètres de sauvegarde** pour afficher ou masquer la page affichant les champs de configuration.

Activer les opérations de sauvegarde

Activez ou désactivez les sauvegardes de site.

Délai d'attente de l'instance du site principal

Déterminez l'intervalle avant qu'un site principal inaccessible passe en reprise en séquence.

Intervalle de synchronisation automatique des données

Vous pouvez contrôler l'intervalle de synchronisation automatique.

Limite de bande passante de la synchronisation des données

Définissez les paramètres de bande passante pour la synchronisation de données.

Activer la reprise en séquence automatique

Activer ou désactiver la reprise en séquence automatique.

IP test de connectivité réseau

Indiquez des adresses IP pour le site de sauvegarde, afin de déterminer si la sauvegarde ne peut pas atteindre le site principal, car le site principal est hors-ligne ou parce que la sauvegarde a perdu sa connexion réseau.

Configuration de l'API : activation de l'API XML et configuration de champs personnalisés

Gestion > Configuration de l'API

Configuration de l'API

Activer l'API XML

Vous pouvez choisir d'activer l'API XML BeyondTrust, qui permet d'exécuter des rapports et des commandes, comme le démarrage ou le transfert de sessions depuis des applications externes, ainsi que de sauvegarder automatiquement votre configuration logicielle.

Remarque : *seuls les appels d'**API de commande**, **de génération de rapports** et **de script client** sont activés/désactivés par ce paramètre. Les autres appels d'API doivent être configurés sous **Portails publics**.*

Pour plus d'informations, veuillez consulter le Guide du programmeur d'API à l'adresse www.beyondtrust.com/docs/remote-support/how-to/integrations/api.

Activer l'API d'archivage

Choisissez d'activer l'API d'archivage d'état pour télécharger des journaux de l'état du Serveur d'accès à distance sécurisé et des évènements qui se sont déroulés à une date donnée.

Comptes d'API

Un compte API stocke tous les paramètres d'authentification et d'autorisation pour le client d'API. Au moins un compte d'API est nécessaire pour utiliser l'API, soit en conjonction avec le client d'intégration, soit avec une application tierce, soit avec votre propre logiciel.

Ajouter, modifier, supprimer

Créer un nouveau compte, modifier un compte existant, ou supprimer un compte existant.

Ajouter ou modifier un compte d'API

Activé

Si cette option est cochée, ce compte est autorisé à s'authentifier auprès de l'API. Lorsqu'un compte est désactivé, tous les jetons OAuth associés au compte sont immédiatement désactivés.

Nom

Créez un nom unique permettant d'identifier ce compte.

Identifiant client OAuth

l'ID client OAuth et le secret de client sont utilisés pour créer des jetons OAuth, nécessaires pour l'authentification à l'API.

L'ID client OAuth est un identificateur unique généré par le serveur. Il ne peut pas être modifié. L'ID client est considérée comme information publique et peut donc être partagée sans compromettre la sécurité de l'intégration.

Commentaires

Ajoutez des commentaires pour identifier la fonction de ce compte.

Secret de client OAuth

Le secret de client OAuth est généré par le serveur grâce à un générateur de nombres pseudo-aléatoire sécurisé cryptographiquement.

> ***Remarque :*** *le secret de client ne peut pas être modifié, mais il peut être généré à nouveau sur la page* ***Modifier****. Générer un nouveau secret de client et enregistrer le compte rend immédiatement invalides tous les jetons OAuth associés à ce compte. Tout appel d'API utilisant ces jetons ne pourra pas accéder à l'API.*

Autorisations

Sélectionnez les zones de l'API que ce compte a le droit d'utiliser.

API de commande

Pour l'API de commande, choisissez de refuser l'accès, d'autoriser l'accès en lecture seule ou d'autoriser l'accès complet.

API de rapport

Pour la section API de rapport, définissez si ce compte a accès aux rapports et enregistrements de sessions d'assistance technique, aux rapports et enregistrements de sessions de présentation, aux rapports d'utilisation de licences, aux rapports d'archives et aux rapports d'activité de compte Vault.

API de sauvegarde

Définissez si ce compte peut utiliser l'API de sauvegarde.

Configuration de l'API

Définissez si ce compte peut utiliser l'API de configuration et, le cas échéant, si elle peut gérer des comptes Vault.

API d'état en temps réel

Définissez si ce compte peut utiliser l'API d'état en temps réel.

API de gestionnaire d'informations d'authentification de point de terminaison

Définissez si ce compte peut utiliser l'API du gestionnaire d'informations d'authentification de point de terminaison.

Restrictions de réseau

Répertoriez les préfixes d'adresse réseau à partir desquels ce compte peut s'authentifier.

> ***Remarque :*** *les comptes API ne sont pas restreints par les préfixes réseau configurés sur la page* ***/login > Gestion > Sécurité****. Ils sont uniquement restreints par les préfixes de réseau configurés pour le compte d'API.*

Liste blanche d'adresses réseau

Saisisse les adresses réseau que vous voulez placer en liste blanche.

Assistance technique : contacter l'BeyondTrust Technical Support

Gestion | **Assistance technique**

Comment contacter l'assistance technique BeyondTrust

La page d'assistance technique contient toutes les coordonnées pour contacter le technicien d'assistance BeyondTrust Technical Support.

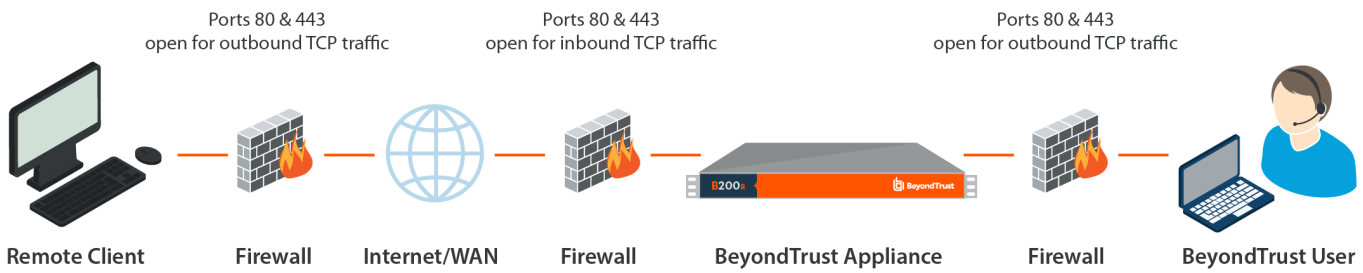
Assistance technique avancée de BeyondTrust

Si un technicien de l'BeyondTrust Technical Support doit accéder à votre serveur, il vous fournira des codes d'assistance technique, d'accès et de remplacement à saisir sur cette page pour créer un tunnel d'assistance technique entièrement crypté créé par le serveur et pointant vers BeyondTrust pour une résolution rapide des problèmes complexes.

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 .
- Des logiciels de sécurité internet tels que des pare-feu ne doivent pas bloquer le téléchargement des fichiers exécutables BeyondTrust. Sont concernés notamment McAfee Security, Norton Security et Zone Alarm. Si vous disposez d'un logiciel pare-feu, vous pouvez constater quelques problèmes de connexion. Afin d'éviter ces problèmes, configurez votre pare-feu de façon à autoriser les fichiers exécutables suivants, où {uid} est un identificateur unique composé de lettres et de chiffres :
    - bomgar-scc-{uid}.exe
    - bomgar-scc.exe
    - bomgar-pac-{uid}.exe
    - bomgar-pac.exe

  Pour obtenir une assistance au niveau de la configuration de votre pare-feu, veuillez contacter le fabricant du logiciel du pare-feu.
- Des exemples de règles de pare-feu basées sur l'emplacement du serveur 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.

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, veuillez contacter : www.beyondtrust.com/support.

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