



BeyondTrust

Privileged Remote Access Installation matérielle du serveur

Table des matières

Configurer la liste des tâches du Secure Remote Access Appliance	3
Conditions requises pour un Secure Remote Access Appliance	4
Installation du Secure Remote Access Appliance	7
Allumer le Secure Remote Access Appliance	7
Configuration initiale du réseau durant la mise en place du Secure Remote Access Appliance	8
Exigence d'un certificat SSL pour le Secure Remote Access Appliance	12
Envoyez des informations sur le Secure Remote Access Appliance à l'assistance technique BeyondTrust	14
Recherche de mises à jour pour installer des logiciels PRA BeyondTrust	15
Mentions pour logiciels Open Source	16

Configurer la liste des tâches du Secure Remote Access Appliance

Cette liste des tâches sert de référence rapide pour les étapes nécessaires à la mise en place de votre Secure Remote Access Appliance. Vous trouverez des détails complets plus loin dans ce guide. Utilisez cette liste pour vérifier que vous n'oubliez aucune étape essentielle.

1. Configurez un enregistrement de DNS de type A pour le nom de domaine complet (FDQN) de votre nouveau site (par ex. access.example.com).
 - Si votre serveur se trouve dans une DMZ ou un réseau interne, un enregistrement de type A pointant vers l'adresse IP du serveur sera alors requis.
 - Si vous souhaitez apporter une assistance technique à des clients externes, alors un enregistrement DNS de type A devra également être enregistré pour l'adresse IP externe du serveur.
 - Pour des scénarios de déploiement réseau BeyondTrust, consultez [Le Secure Remote Access Appliance dans le réseau](#) à l'adresse www.beyondtrust.com/docs/deployment/dmz.
2. Installez le Secure Remote Access Appliance selon : « [Conditions requises pour un Secure Remote Access Appliance](#) », page 4.
3. Obtenez un certificat SSL correspondant à votre FDQN de DNS (par ex. access.example.com).
 - a. Pour des détails complets, consultez le [Guide de certificat SSL](#) à l'adresse www.beyondtrust.com/docs/privileged-remote-access/how-to/sslcertificates.
 - b. Importez la chaîne de certificat sur votre serveur et assignez-le à l'adresse IP du serveur.
 - c. Exportez la portion racine de la chaîne de certificat (avec les valeurs **Remis à** et **Émis par** correspondantes) sans informations de clé privée, et enregistrez le certificat racine pour la prochaine étape.
4. Envoyez par e-mail les trois éléments suivants à l'Assistance technique BeyondTrust :
 - Le nom d'hôte FDQN du DNS du serveur de l'étape 1.
 - Le segment racine du certificat SSL exporté à l'étape 3c.
 - Une capture d'écran de la page **/appliance > État > Bases**.
5. Installez le nouveau package de licence logicielle que l'Assistance technique BeyondTrust vous enverra après que vous ayez accompli les étapes 1 à 4.
 - a. Vous serez prévenu par e-mail lorsque vous devrez installer le package de licence logicielle en utilisant l'utilitaire **Rechercher les mises à jour**.
 - b. Une fois installé, naviguez vers l'interface d'administration /login (par ex. <https://access.example.com/login>).
 - c. Utilisez les informations d'authentification d'administration par défaut **admin** et **password** pour votre première connexion.

Conditions requises pour un Secure Remote Access Appliance

Ce guide vous expose la mise en place et la configuration initiale de votre Secure Remote Access Appliance. Si vous avez besoin d'aide, contactez l'Assistance technique BeyondTrust à l'adresse www.beyondtrust.com/support.

Conditions

Avant de commencer, il est important de savoir que tant que les conditions requises par le Secure Remote Access Appliance n'ont pas été satisfaites, vous ne pourrez pas atteindre votre serveur directement par son adresse IP ou son nom d'hôte, et vous ne pourrez pas rechercher des mises à jour ou l'utiliser pour fournir un accès privilégié. Le Secure Remote Access Appliance requiert au minimum ce qui suit :

- Deux prises de courant disponibles.
- Une connexion réseau haut débit.
- Un routeur ou switch réseau.
- Une adresse IP statique unique pour le Secure Remote Access Appliance.
- Un enregistrement de DNS privé de type A effectuant une résolution vers l'IP statique de votre serveur. Un enregistrement public de type A et une IP publique seront également requis si des clients externes ont besoin d'un accès au serveur.
- Un certificat SSL de serveur Web + un ou des certificats SSL intermédiaires, et une racine SSL. OU un certificat auto-signé.



Pour plus d'informations, veuillez consulter la section [Guide certificats SSL et BeyondTrust](#).

- Le package de licences logicielles BeyondTrust.

Bien que ceci réponde aux exigences minimum, des configurations plus avancées peuvent nécessiter des éléments supplémentaires. Par exemple :

- Les clients mobiles BeyondTrust nécessitent une racine SSL et un ou plusieurs certificats SSL intermédiaires.
- L'accès depuis des réseaux publics externes nécessite un enregistrement de DNS public de type A.
- L'accès depuis plusieurs enregistrements de DNS de type A nécessite plusieurs certificats de serveur Web et/ou un ou plusieurs certificats SAN ou à caractère générique.
- L'isolation du trafic client de plusieurs réseaux nécessite plusieurs adresses IP statiques.
- Les mises à jour automatiques et l'assistance technique BeyondTrust avancée nécessitent un accès sortant à l'internet public depuis le Secure Remote Access Appliance sur le port TCP 443.



IMPORTANT !

Aucun logiciel client (par ex. console d'accès, Jump Clients, Jumpoints, etc.) ne peut être téléchargé, installé ou utilisé tant que l'Assistance technique BeyondTrust n'a pas créé un package de licence logicielle pour votre serveur et que vous ne l'avez pas installé selon les instructions fournies par l'assistance technique. Comme ce package de licence est encodé avec l'enregistrement DNS de type A du serveur ainsi que son certificat SSL, ceux-ci doivent être en place avant que le package de licence puisse être terminé.

Démarrage

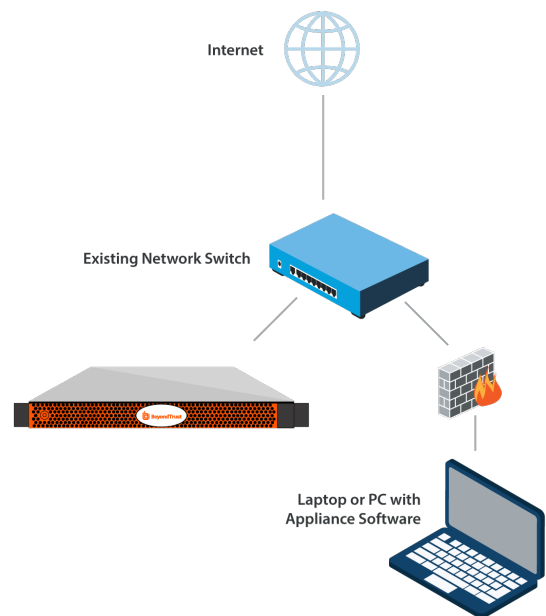
Plusieurs actions doivent être effectuées avant que le matériel BeyondTrust soit livré et installé :

1. Allouez l'espace de rack nécessaire au serveur. Assurez-vous que cet espace dispose de suffisamment d'alimentation électrique et d'accès réseau.
2. Réservez une adresse IP statique pour le serveur sur le réseau. Reportez-vous aux guides suivants pour réserver la ou les bonnes adresses IP :
 - [Secure Remote Access Appliance dans le réseau](http://www.beyondtrust.com/docs/privileged-remote-access/getting-started/deployment/dmz) - www.beyondtrust.com/docs/privileged-remote-access/getting-started/deployment/dmz
3. Configurez un enregistrement de DNS de type A pour le nom de domaine complet (FDQN) de votre nouveau site (par ex. access.example.com).



Remarque : un enregistrement de DNS de type A privé effectuant une résolution vers l'IP statique du serveur sera toujours nécessaire. Un enregistrement public de type A et une IP publique seront également requis si les clients sur des réseaux externes publics auront besoin d'un accès au serveur.

Bien que votre serveur peut fonctionner n'importe où dans votre réseau avec un accès Internet, vous devez décider où vous souhaitez installer le serveur dans le réseau avant cette étape. Si vous allez accéder à des systèmes en dehors de votre réseau, BeyondTrust vous recommande de placer votre serveur dans une DMZ ou en dehors de votre pare-feu interne. Consultez le tableau ci-dessous pour plus de détails. Pour obtenir une assistance au niveau de la configuration de votre pare-feu, veuillez contacter le fabricant du logiciel du pare-feu.



Remarque : si vous déplacez le serveur vers un autre lieu pour le connecter à Internet, vous devrez l'éteindre avant de le débrancher de sa prise d'alimentation électrique. Si vous pouvez vous connecter à l'interface d'administration /appliance, allez sur la page **État > Bases** et cliquez sur **Éteindre ce serveur**. L'extinction manuelle est possible si vous appuyez une fois sur le bouton d'alimentation. Attendez 60 secondes pour que le Secure Remote Access Appliance s'éteigne avant de le débrancher de sa source d'alimentation électrique. Lorsque vous reconnectez le serveur au nouveau lieu, vous devrez le rallumer.

Considérations pour l'emplacement réseau d'un Secure Remote Access Appliance

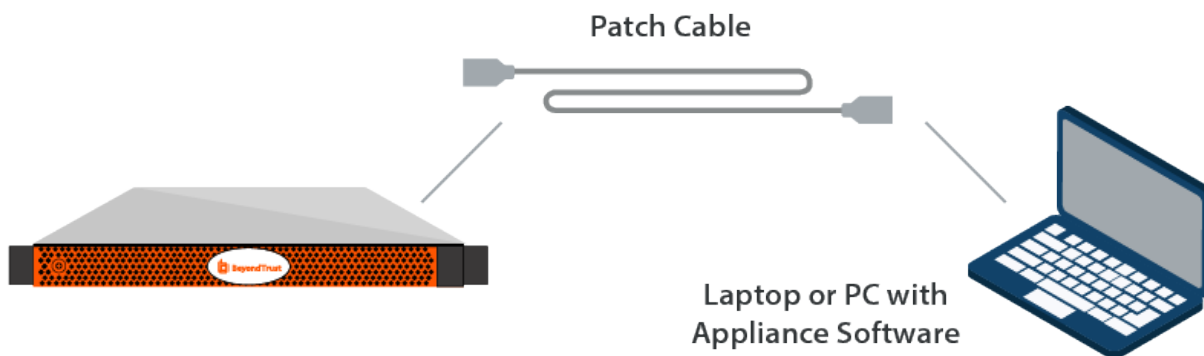
Emplacement réseau	Avantages/Inconvénients
Hors de votre pare-feu	Ne requiert pas que les ports 80 et 443 soient ouverts pour le trafic TCP entrant sur votre pare-feu. Simplifie grandement le processus d'installation, car les clients du technicien d'assistance et des clients sont construits pour renvoyer vers un DNS spécifique ; si votre DNS enregistré renvoie vers une adresse IP publique directement assignée à votre serveur, aucune installation supplémentaire n'est nécessaire de votre part pour lancer une session.

Emplacement réseau	Avantages/Inconvénients
DMZ	Peut nécessiter une configuration supplémentaire en fonction de votre (vos) routeur(s).
À l'intérieur de votre pare-feu	Nécessite une redirection de ports sur votre pare-feu et potentiellement une configuration supplémentaire de votre routage NAT et de votre DNS interne.

Installation du Secure Remote Access Appliance

Pour des instructions d'installation, veuillez vous référer au menu flottant d'instructions au sein de votre Secure Remote Access Appliance, ou consulter le [Guide utilisateur de Poweredge](http://www.beyondtrust.com/docs/privileged-remote-access/documents/infrastructure/pr-a-appliance-rail-installation.pdf) à l'adresse www.beyondtrust.com/docs/privileged-remote-access/documents/infrastructure/pr-a-appliance-rail-installation.pdf.

Allumer le Secure Remote Access Appliance



1. Branchez les câbles d'alimentation du Secure Remote Access Appliance sur une source électrique sûre. En fonction du type de serveur, vous aurez peut-être besoin de deux câbles d'alimentation. Les alimentations du serveur basculeront automatiquement au besoin entre 120 et 240 V.
2. En utilisant l'un des câbles de raccordement fournis, connectez votre ordinateur à NIC1 ou NIC2 à l'arrière du Secure Remote Access Appliance. Vous pouvez utiliser des câbles droits ou croisés. Si vous utilisez DHCP, branchez directement le câble droit au réseau, et le serveur recevra automatiquement une nouvelle adresse IP.



Remarque : BeyondTrust prend en charge le placement des deux NIC sur le même réseau pour des besoins d'association NIC. De même, les NIC peuvent être placés sur des sous-réseaux séparés pour un routage de trafic segmenté. Cependant, si vous placez les deux NIC sur le même réseau pour l'association NIC, ne configurez qu'un seul NIC. Si les deux NIC ont des adresses IP du même sous-réseau, cela produira des comportements inattendus. Lorsque plusieurs adresses IP sont requises pour un même sous-réseau, il faut assigner toutes les adresses IP à un NIC.

3. Appuyez sur le bouton d'alimentation à l'avant du serveur. Le voyant lumineux d'alimentation à droite du bouton de redémarrage s'allume, et le voyant lumineux d'activité du disque dur (à droite de la première diode) commence à clignoter. Le lancement du Secure Remote Access Appliance prendra environ 60 secondes.



Remarque : les voyants NIC1 et NIC2 peuvent s'allumer et afficher une activité même lorsque le serveur est éteint ; il est donc important de vérifier les voyants d'alimentation et de disque dur pour confirmer qu'il est allumé.

Configuration initiale du réseau durant la mise en place du Secure Remote Access Appliance

Avant de déployer le Secure Remote Access Appliance sur votre réseau, vous devez mettre en place sa configuration réseau. Vous pouvez le faire en accédant à l'interface d'administration du Secure Remote Access Appliance depuis un navigateur Internet sur votre ordinateur. Les étapes ci-dessous vous décriront ce processus. Votre processus peut varier en fonction de votre système d'exploitation.

Instructions DHCP

Si DHCP est activé pour l'emplacement du réseau que vous avez sélectionné pour votre serveur, le serveur recevra une adresse IP du réseau et il sera possible d'y accéder directement à travers cette adresse IP à **<https://<adresseip>/appliance>**. Vous pouvez trouver cette adresse IP via la console sur le port vidéo.

Utilisez le nom d'utilisateur et le mot de passe par défaut pour vous connecter.

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

Mot de passe par défaut : **password**

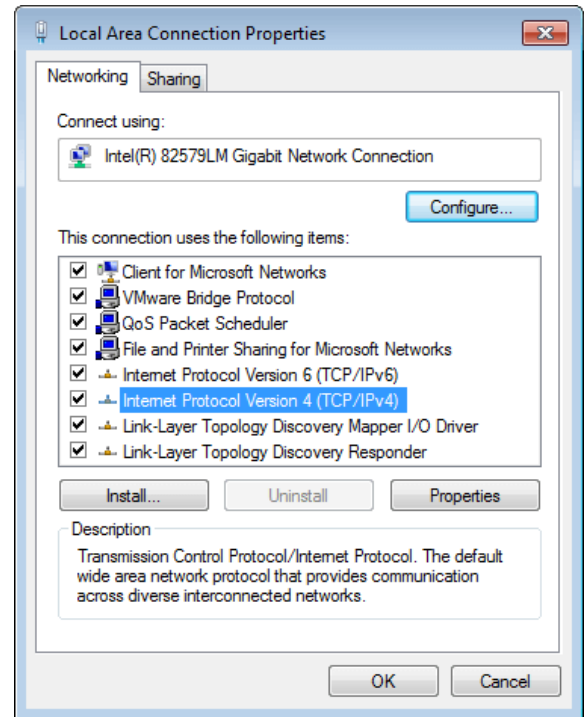
Lors de votre première connexion, vous serez invité à changer le mot de passe administratif de votre serveur.



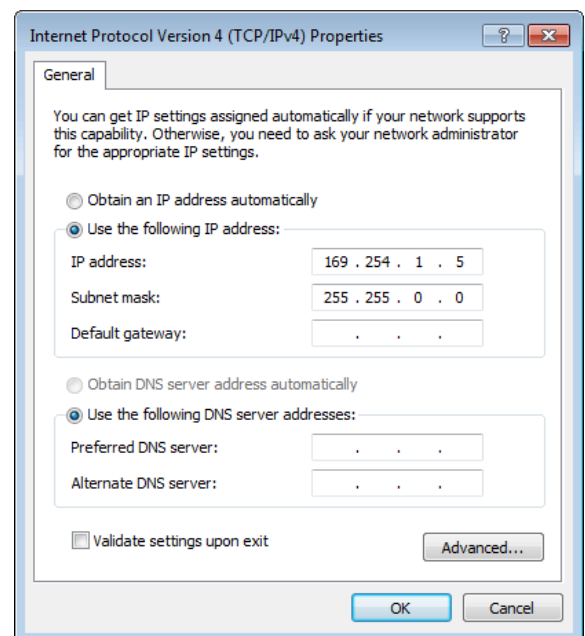
Remarque : si vous utilisez DHCP, vous pouvez sauter la section **Instructions de connexion à la zone locale** et vous rendre dans la section **Configuration /appliance**.

Instructions de connexion à la zone locale

1. Après avoir effectué la mise en place initiale de votre Secure Remote Access Appliance, allez dans la **Connexion au réseau local** de votre ordinateur puis cliquez sur **Propriétés**.
2. Sélectionnez Internet Protocol Version 4 (IPv4) et cliquez sur le bouton **Propriétés**.



3. Saisissez **169.254.1.5** comme adresse IP et **255.255.0.0** comme masque de sous-réseau. Laissez les champs Passerelle et DNS vides.

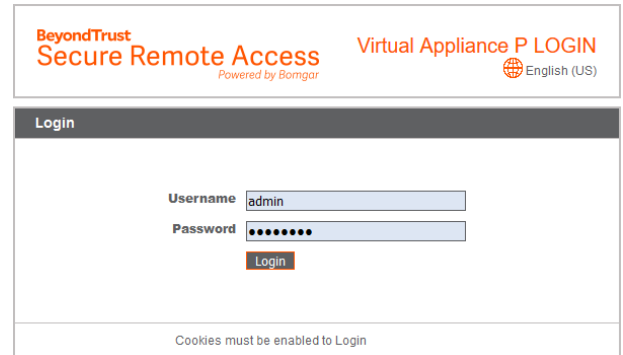


- Lancez un navigateur internet et saisissez l'adresse **https://169.254.1.1/appliance/login.ns** dans le champ d'URL. Si ceci ne fonctionne pas, essayez de remplacer le dernier chiffre de l'adresse par .2, .3 ou .4. Chargez chacune de ces adresses séparément jusqu'à ce que l'une d'elles réponde. Saisissez le nom d'utilisateur et le mot de passe par défaut, et cliquez sur **Connexion**.

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

Mot de passe par défaut : **password**

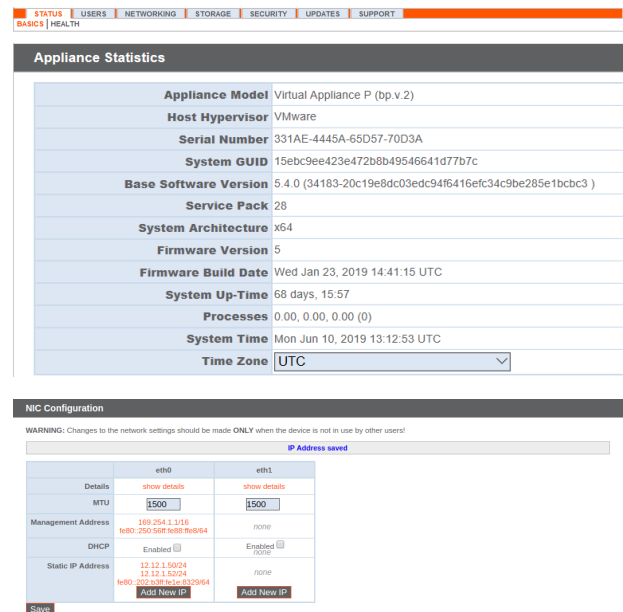
Lors de votre première connexion, vous serez invité à changer le mot de passe administratif de votre serveur.



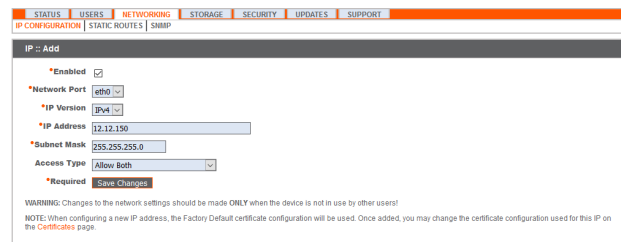
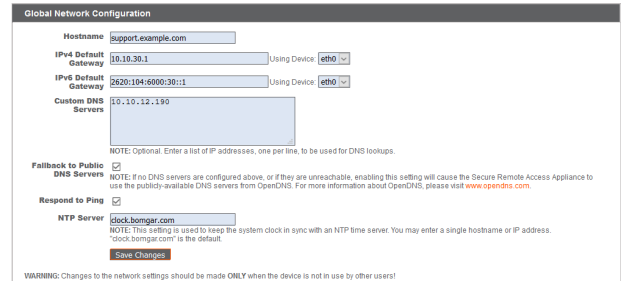
Remarque : Le Secure Remote Access Appliance utilise deux interfaces Web d'administration, /appliance et /login, pour isoler l'administration matérielle de la gestion des utilisateurs. L'interface /appliance est utilisée pour configurer les paramètres réseau et mettre à niveau le logiciel BeyondTrust. L'interface /login n'est disponible qu'après que l'Assistance technique BeyondTrust a construit le package de licences logicielles nécessaires et que ce package a été installé par le biais de /appliance. Une fois installé, /login est utilisé pour gérer les utilisateurs et les flux de travail, déployer des logiciels clients, établir des rapports sur les activités d'accès, créer et utiliser des intégrations, etc. Consultez la section [Interface admin Privileged Remote Access BeyondTrust](https://www.beyondtrust.com/docs/privileged-remote-access/getting-started/admin) à l'adresse www.beyondtrust.com/docs/privileged-remote-access/getting-started/admin.

Configuration /appliance

- Une fois que vous vous êtes connecté à l'interface /appliance, vous verrez la page **État > Bases**. Cette page comprend des informations comme le numéro de série que l'Assistance technique BeyondTrust exige pour enregistrer le serveur auprès des serveurs de licence de BeyondTrust. Prenez une capture d'écran de cette page et envoyez-la à l'Assistance technique BeyondTrust pour qu'elle puisse enregistrer votre serveur.
- Allez ensuite sur **Réseau > Configuration IP**. Sous la section **Configuration NIC**, cliquez sur **Ajouter nouvelle IP**.



3. Saisissez l'adresse IP statique et le masque de sous-réseau pour votre Secure Remote Access Appliance. De manière générale, vous devriez laisser les valeurs par défaut pour ces deux champs. Vous pouvez choisir si cette adresse IP prend en charge le trafic de session, le trafic Internet, ou les deux. Cliquez ensuite sur **Enregistrer les modifications**.
4. Dans la section **Configuration globale du réseau**, configurez le nom de la passerelle par défaut. Saisissez la passerelle par défaut et l'adresse du serveur DNS. Après avoir saisi les informations requises, cliquez sur **Enregistrer les modifications**.


Remarque : des paramètres DNS valides sont nécessaires pour que la reprise en séquence et les mises à jour automatiques fonctionnent correctement.

Pour plus d'informations sur la configuration réseau, consultez [Le Secure Remote Access Appliance dans le réseau](http://www.beyondtrust.com/docs/privileged-remote-access/getting-started/deployment/dmz) à l'adresse www.beyondtrust.com/docs/privileged-remote-access/getting-started/deployment/dmz.

Exigence d'un certificat SSL pour le Secure Remote Access Appliance

Toutes les communications du logiciel BeyondTrust se font par des connexions sécurisées et cryptées. Elles reposent sur la technologie Secure Sockets Layer (SSL), une norme dans l'industrie, et l'adresse DNS du serveur. Le Secure Remote Access Appliance s'accompagne d'un certificat par défaut qui sécurise toutes les connexions sur toutes les adresses IP. Cependant, cela ne satisfera pas aux exigences du logiciel client BeyondTrust, qui effectue des contrôles de vérification plus rigoureux que les navigateurs internet standard. Ainsi, avant que BeyondTrust puisse vous fournir un package de licence logicielle complètement opérationnel, votre Secure Remote Access Appliance doit disposer d'un certificat SSL valide installé qui correspond à l'enregistrement DNS de type A que vous avez enregistré pour votre serveur.

Un certificat SSL valide peut être un certificat SSL signé par une autorité de certification (signé par une AC) ou un certificat SSL auto-signé. Les certificats signés par une AC sont nécessaires pour exploiter pleinement toutes les fonctions de BeyondTrust (comme la fonction cliquer-pour-messagerie instantanée et les clients mobiles), mais il faut alors qu'une demande de signature de certificat (DSC) soit soumise à l'AC. La DSC est une norme industrielle utilisée par tous les appareils et logiciels réseau qui utilisent le SSL. Si un certificat DSC/AC est utilisé à la place d'un certificat auto-signé, le certificat signé par une AC doit être téléchargé depuis le site de l'AC (ou l'e-mail de preuve d'achat) et importé dans le Secure Remote Access Appliance depuis l'interface /appliance. En plus de la fonction de demande de certificat d'AC, BeyondTrust inclut des fonctions permettant d'obtenir et de renouveler automatiquement ses propres certificats TLS auprès de l'autorité de certificat Let's Encrypt.

- i** Pour plus d'informations sur la création et la gestion de certificats SSL dans PRA BeyondTrust, veuillez consulter les articles suivants :
- [Créer un certificat SSL signé par une autorité de certificat pour votre Secure Remote Access Appliance](http://www.beyondtrust.com/docs/privileged-remote-access/how-to/sslcertificates/create-ca-signed.htm) à l'adresse www.beyondtrust.com/docs/privileged-remote-access/how-to/sslcertificates/create-ca-signed.htm
 - [Créer un certificat auto-signé pour votre Secure Remote Access Appliance](http://www.beyondtrust.com/docs/privileged-remote-access/how-to/sslcertificates/create-self-signed.htm) à l'adresse www.beyondtrust.com/docs/privileged-remote-access/how-to/sslcertificates/create-self-signed.htm
 - [Certificats : Créer et gérer les certificats SSL](http://www.beyondtrust.com/docs/privileged-remote-access/getting-started/deployment/web/security-certificates.htm) à l'adresse www.beyondtrust.com/docs/privileged-remote-access/getting-started/deployment/web/security-certificates.htm.

- i** Pour plus d'informations sur la façon dont BeyondTrust utilise les certificats SSL, et les étapes de configuration détaillées pour demander et installer des certificats dans BeyondTrust, consultez le [Guide des certificats SSL](http://www.beyondtrust.com/docs/privileged-remote-access/how-to/sslcertificates) à l'adresse www.beyondtrust.com/docs/privileged-remote-access/how-to/sslcertificates.

La section [Créer un certificat SSL](#) décrit en détail les étapes pour la configuration initiale. Une vue d'ensemble du processus est fournie ci-dessous.

1. Connectez-vous à l'interface /appliance BeyondTrust et créez une demande de signature de certificat (DSC) ou un certificat auto-signé.



Remarque : Si le Secure Remote Access Appliance devra utiliser une copie du certificat venant d'un autre Secure Remote Access Appliance ou d'un autre serveur, aucune DSC et aucun certificat auto-signé n'est nécessaire. Au lieu de cela, exportez le certificat et sa clé privée depuis le système sur lequel il se trouve et importez-le sur le Secure Remote Access Appliance. Pour des étapes détaillées, consultez la section [Répliquer le certificat SSL sur les serveurs de reprise en séquence et Atlas](#) dans le [Guide des certificats SSL](#).

2. Assignez le nouveau certificat à (aux) adresse(s) IP du Secure Remote Access Appliance.

3. Envoyez à l'Assistance technique BeyondTrust une copie du certificat racine SSL ou des adresses DNS du serveur.



Remarque : Si vous utilisez un certificat auto-signé, le certificat fait office de certificat racine ; ainsi, le certificat auto-signé doit être envoyé à l'Assistance technique BeyondTrust. Si un certificat signé par une AC est utilisé, contactez l'AC pour obtenir une copie de leur certificat racine. Si vous avez des difficultés à contacter l'AC, vous trouverez des articles pour vous aider à obtenir votre certificat racine à l'adresse beyondtrustcorp.service-now.com/csm. Quel que soit le cas, l'Assistance technique BeyondTrust devra connaître l'adresse DNS du serveur. Si votre adresse DNS est publique et que le certificat SSL est déjà installé, l'assistance technique peut récupérer une copie de la racine depuis l'adresse DNS publique ; dans ce cas, il n'est pas nécessaire d'envoyer manuellement le certificat racine.

Une fois ces étapes terminées, l'Assistance technique BeyondTrust encode le nom d'hôte DNS et le certificat racine SSL dans un nouveau package de licence logicielle, l'envoie aux serveurs de licences BeyondTrust pour qu'il soit construit, puis vous envoie des instructions sur l'installation du nouveau package une fois cela fait.

Envoyez des informations sur le Secure Remote Access Appliance à l'assistance technique BeyondTrust

Lors de la construction du package logiciel, l'Assistance technique BeyondTrust encode le nom d'hôte DNS et le certificat racine SSL de votre serveur dans le logiciel. Avant que l'Assistance technique BeyondTrust puisse construire votre logiciel, vous devez lui envoyer les éléments indiqués ci-dessous.

1. Nom d'hôte DNS (nom de domaine complet) du serveur (par ex. access.example.com).
2. Le certificat racine SSL ou le certificat SSL auto-signé. Vous pouvez obtenir cela sur la page **/appliance > Sécurité > Certificats**. Exportez la partie certificat avec les champs **Remis à** et **Émis par** correspondants.
3. Capture d'écran de la page **/appliance > État > Bases**.

Recherche de mises à jour pour installer des logiciels PRA BeyondTrust

Les mises à jour du Secure Remote Access Appliance sont installées depuis l'interface Web /appliance sur la page **Mises à jour**. Chaque mise à jour doit être créée par BeyondTrust et est liée au numéro de série du serveur pour lequel elle a été construite. Pour cette raison, le serveur doit être enregistré, afin de pouvoir rechercher des mises à jour.



1. Une fois que BeyondTrust a créé une mise à jour pour votre serveur, vous recevrez un e-mail de notification. Allez dans /appliance > Mises à jour. Récupérez la mise à jour en utilisant **Mises à jour :: Vérification > Rechercher les mises à jour** ou **Mises à jour :: Installation manuelle > Clé de téléchargement du serveur**.



Remarque : L'option **Rechercher les mises à jour** peut être utilisée seulement si le serveur dispose d'un accès sortant sur le port TCP 443 vers **btupdate.com**. L'installation manuelle ne nécessite pas cette connexion.

2. Une fois la vérification effectuée, toutes les mises à jour disponibles correspondant au numéro de série de votre serveur seront listées sur l'interface Web /appliance. Il existe deux types de mises à jour :
 - Les mises à jour pour les licences /login (toujours affichées selon le format **BeyondTrust-x.x.x**)
 - Les mises à jour pour le logiciel de base /appliance (toujours affichées selon le format **Base Software x.x.x**)

Si aucun package de mises à jour ni aucun correctif n'est disponible sur votre Secure Remote Access Appliance, le message « Aucune mise à jour disponible » s'affichera. Si une mise à jour est disponible mais qu'une erreur est survenue lors de la distribution de la mise à jour sur votre serveur, le message suivant s'affichera : « Une erreur est survenue lors de la création de votre mise à jour. Pour plus d'informations, veuillez visiter www.beyondtrust.com/support.



Le logiciel de base comprend les fonctions et les correctifs pour /appliance, ainsi que le code prérequis nécessaire avant l'installation de mises à jour de licence. Ainsi, les mises à jour de licence vous demandent en général d'installer d'abord une mise à jour du logiciel de base. Dans ce cas, l'interface de mise à jour de BeyondTrust notera l'ordre correct d'installation des mises à jour. Si vous n'êtes toujours pas sûr, prenez une capture d'écran des mises à jour disponibles et envoyez-la à l'Assistance technique BeyondTrust pour qu'elle vous aide.



IMPORTANT !

N'oubliez pas que vous devez envoyer les éléments suivants à l'Assistance technique BeyondTrust pour qu'elle puisse construire vos mises à jour de logiciel de base et/ou de licences :

1. *Nom d'hôte DNS (nom de domaine complet) du serveur*
 2. *Certificat SSL racine ou certificat SSL auto-signé*
 3. *Capture d'écran de la page /appliance > État > Bases*
3. Une fois que vous avez envoyé à l'Assistance technique BeyondTrust votre nom d'hôte, votre certificat SSL et une capture d'écran, elle construira les mises à jour nécessaires et vous enverra des instructions d'installation détaillées.
 4. Une fois l'installation terminée, le Secure Remote Access Appliance est prêt à être utilisé pour l'accès privilégié. Pour valider la disponibilité de votre serveur, connectez-vous à l'interface /login en allant sur l'URL de votre serveur, suivie de /login (par

ex. `access.example.com/login`).

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

Mot de passe par défaut : **password**

5. À la première connexion, vous serez invité à changer votre mot de passe.
6. Une fois la première connexion effectuée, vous pouvez valider votre configuration de licence logicielle sur la page **État > Informations**, ajouter des comptes utilisateur sur **Utilisateurs et sécurité > Utilisateurs** et télécharger des logiciels clients dans **Mon compte**. Étant donné que les licences de Privileged Remote Access BeyondTrust dépendent du nombre de points de terminaison autorisé, vous pouvez configurer autant de comptes que nécessaire, chacun ayant un nom d'utilisateur et un mot de passe uniques.

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. Les noms d'utilisateur et les mots de passe pour `/login` sont valides pour l'interface `/login` (où sont gérés les utilisateurs et la configuration) et pour toute console d'accès (où les sessions sont exécutées). Les options disponibles sur ces deux emplacements dépendent des autorisations assignées par l'administrateur de `/login` pour chaque compte utilisateur.

Pour obtenir de l'aide pour commencer à utiliser le logiciel client BeyondTrust, consultez la documentation à l'adresse www.beyondtrust.com/docs. Les guides du serveur et les guides d'administrateur de Privileged Remote Access vous présentent les différentes options administratives de vos interfaces Web `/appliance` et `/login`, et les guides d'utilisation vous expliquent comment utiliser le logiciel client BeyondTrust.

Mentions pour logiciels Open Source

Pour obtenir des informations sur les droits d'auteurs et les mentions des logiciels open source utilisés dans le matériel et les logiciels BeyondTrust, veuillez consulter l'[Index des attributions](#) à l'adresse www.beyondtrust.com/docs/privileged-remote-access/updates/attributions.