BeyondTrust

Privileged Remote Access
Interface de serveur 5.x (/appliance)

TC:9/25/2020

Table des matières

Interface Web du Secure Remote Access Appliance BeyondTrust

Ce guide a pour but de vous permettre de configurer et de gérer le Secure Remote Access Appliance à travers son interface Web **/appliance**. Le serveur sert de point d'administration et de gestion central de vos sites BeyondTrust.

Utilisez ce guide uniquement après que l'administrateur a procédé à l'installation et à la configuration initiales du Secure Remote Access Appliance, comme l'explique le Guide d'installation matérielle du Secure Remote Access Appliance à l'adresse www.beyondtrust.com/docs/privileged-remote-access/getting-started/deployment/hardware/. Une fois BeyondTrust correctement installé, vous pouvez commencer immédiatement à accéder à vos points de terminaison. Si vous avez besoin d'aide, contactez l'Assistance technique BeyondTrust à l'adresse www.beyondtrust.com/support.

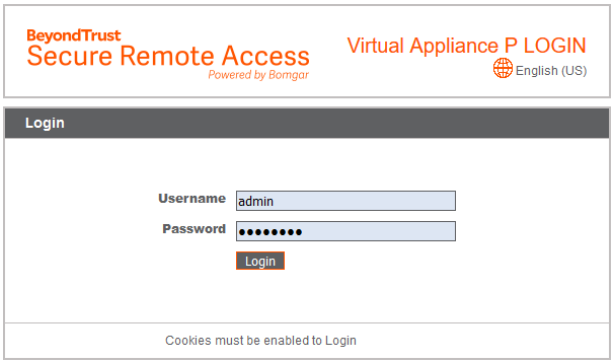
Connexion à l'interface d'administration du Secure Remote Access Appliance

Une fois le serveur installé, connectez-vous à l'interface d'administration du Secure Remote Access Appliance en allant à l'URL publique de votre serveur, suivie de **/appliance** (par exemple : http://access.example.com/appliance).

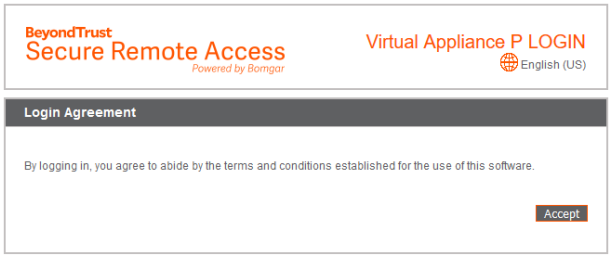
Nom d'utilisateur par défaut : **admin**

Mot de passe par défaut : **password**

Il vous sera demandé de changer le mot de passe d'administration à votre première connexion.[1]



Vous pouvez restreindre l'accès à l'écran de connexion en activant un accord de connexion devant être validé pour pouvoir continuer.



Si vous souhaitez activer l'accord de connexion, consultez « Administration du serveur : Définissez des restrictions liés aux comptes, aux réseaux et aux ports, activez un serveur STUN, installez un protocole Syslog, activez un accord de connexion, réinitialisez un compte d'administrateur », page 24.

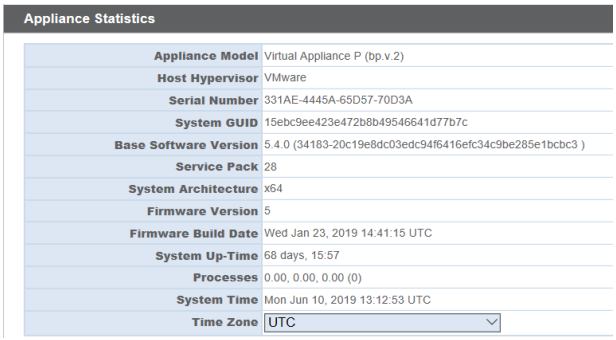
Remarque : *Pour des raisons de sécurité, le nom d'utilisateur et le mot de passe d'administration utilisés pour l'interface* ***/appliance*** *sont différents de ceux utilisés pour l'interface* ***/login*** *et doivent être gérés séparément.*

[1]Les mots de passe doivent comporter au moins huit caractères et inclure chacun des éléments suivants : une lettre majuscule, une lettre minuscule, un chiffre et un caractère spécial.

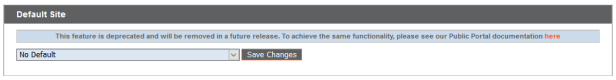
État

Bases : Consulter les informations du serveur

La page **Bases** affiche des informations sur votre Secure Remote Access Appliance et vous permet de contrôler votre système. Vous pouvez également y indiquer l'heure locale de votre système en concordance avec n'importe quel fuseau horaire. L'heure du système est affichée par défaut par rapport à l'échelle UTC.

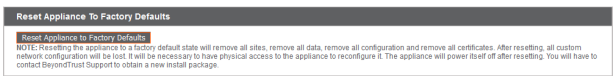


Dans la plupart des cas, il n'est pas nécesaire de changer ce paramètre. BeyondTrust déconseille l'utilisation de plusieurs sites sur un seul serveur. Toutefois, si votre installation nécessite plusieurs sites répondant à une adresse IP, sélectionnez un site de réponse par défaut dans le cas où l'on utiliserait directement une adresse IP au lieu du nom de domaine. Lorsque plusieurs DNS pointent vers cette adresse IP et que vous sélectionnez **Aucun paramètre par défaut**, un message d'erreur apparaît lorsqu'on tente d'accéder à votre site en utilisant une adresse IP.



À partir de cette page, vous pouvez aussi redémarrer ou éteindre votre Secure Remote Access Appliance. Bien qu'il ne soit pas nécessaire de redémarrer votre serveur, il peut être utile d'effectuer un redémarrage mensuel dans le cadre d'une maintenance régulière. Vous n'avez pas besoin d'avoir un accès physique au serveur pour réaliser le redémarrage.

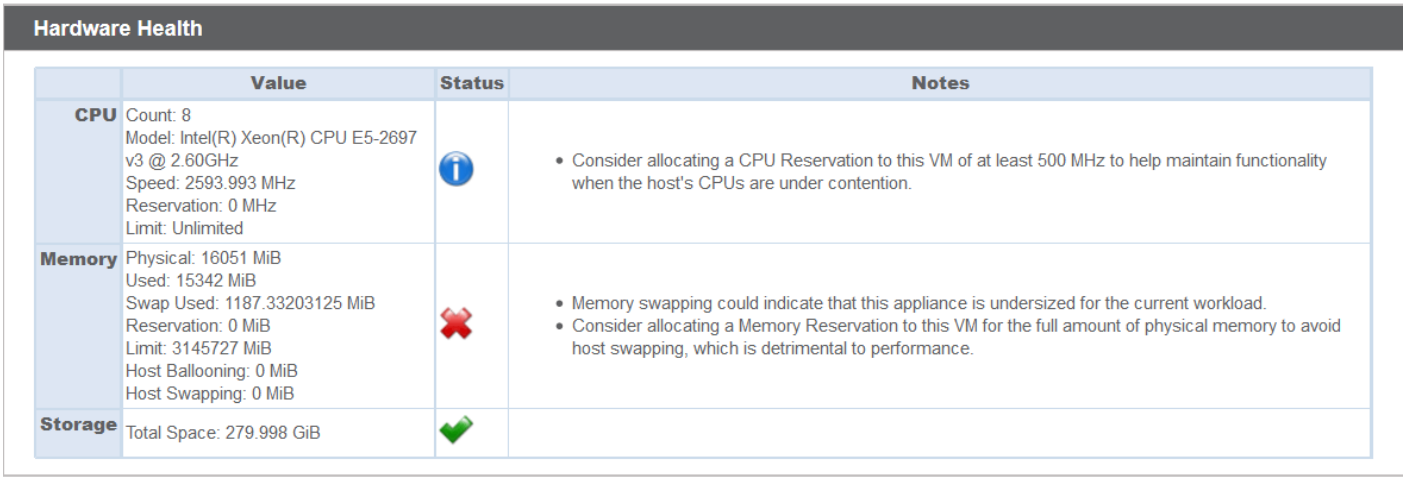
Veuillez ne pas effectuer les opérations suivantes sans que cela vous ait été demandé par l'Assistance technique BeyondTrust : Si vous cliquez sur le bouton **Rétablir la version par défaut du serveur**, le Secure Remote Access Appliance revient à la version d'usine. Cette option supprime l'ensemble des données, des paramètres de configuration et des certificats de votre serveur. Après sa réinitialisation, le serveur s'éteint.



Santé : Consultez la santé du PRA Virtual Appliance

> ***Remarque :*** *L'onglet **Santé** n'est visible que pour les sites pris en charge par le PRA Virtual Appliance ou le serveur cloud.*

La page **Santé** sert à contrôler l'état du serveur virtuel ou cloud. Elle affiche des informations par rapport au nombre de processeurs utilisés et à la quantité de mémoire et de stockage employée. Consultez les colonnes **État** et **Notes** pour obtenir des conseils liés à l'amélioration de la santé de votre serveur.



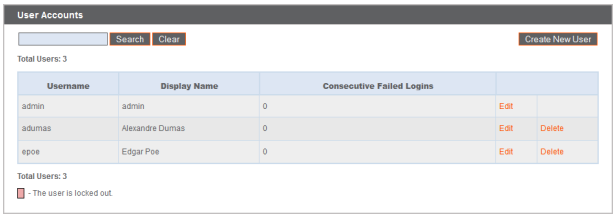
Hardware Health

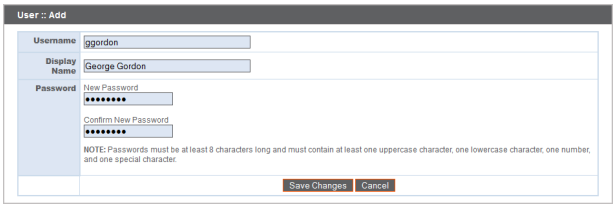
	Value	Status	Notes
CPU	Count: 8 Model: Intel(R) Xeon(R) CPU E5-2697 v3 @ 2.60GHz Speed: 2593.993 MHz Reservation: 0 MHz Limit: Unlimited		• Consider allocating a CPU Reservation to this VM of at least 500 MHz to help maintain functionality when the host's CPUs are under contention.
Memory	Physical: 16051 MiB Used: 15342 MiB Swap Used: 1187.33203125 MiB Reservation: 0 MiB Limit: 3145727 MiB Host Ballooning: 0 MiB Host Swapping: 0 MiB		• Memory swapping could indicate that this appliance is undersized for the current workload. • Consider allocating a Memory Reservation to this VM for the full amount of physical memory to avoid host swapping, which is detrimental to performance.
Storage	Total Space: 279.998 GiB		

Utilisateurs

Modifier le mot de passe et le nom d'utilisateur, ajouter un utilisateur, supprimer un utilisateur

Sur la page **Utilisateurs**, vous pouvez ajouter, modifier ou supprimer les utilisateurs administratifs pour l'interface /appliance. Vous pouvez aussi changer le nom d'utilisateur, le nom affiché ou le mot de passe d'un administrateur. BeyondTrust vous recommande de changer régulièrement votre mot de passe pour vous prémunir d'un accès non autorisé.





Pour définir les règles de restriction de compte, relatives notamment à l'historique et à l'expiration des mots de passe, veuillez consulter « Administration du serveur : Définissez des restrictions liés aux comptes, aux réseaux et aux ports, activez un serveur STUN, installez un protocole Syslog, activez un accord de connexion, réinitialisez un compte d'administrateur », page 24

Remarque : *il faut qu'au moins un compte d'utilisateur soit défini. Le Secure Remote Access Appliance dispose d'un compte prédéfini, qui correspond au compte de l'administrateur. Vous pouvez conserver le compte de l'administrateur, créer des comptes supplémentaires ou remplacer le compte d'administrateur.*

Réseau

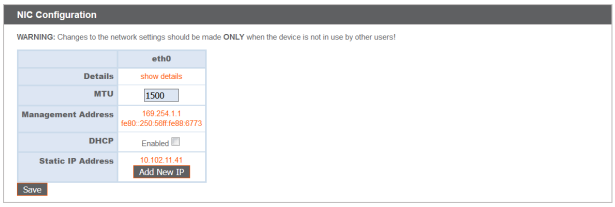
Configuration de l'IP : configuration de l'adresse IP et des paramètres du réseau

Les entreprises dotées de configurations de réseau poussées peuvent configurer plusieurs adresses IP sur les ports Ethernet du serveur. L'utilisation de plusieurs ports peut augmenter la sécurité ou activer des connexions sur des réseaux particuliers. Par exemple, si vos employés n'ont pas le droit d'utiliser internet, mais qu'ils doivent travailler hors ligne, il est possible, avec l'utilisation d'un port pour votre réseau interne privé et l'utilisation d'un second port pour l'internet public, de permettre aux utilisateurs du monde entier d'accéder aux systèmes sans enfreindre votre politique de sécurité liée au réseau.

Le couplage NIC regroupe les cartes d'interface réseau physiques de votre système en une seule interface logique. Le couplage NIC fonctionne en mode actif-sauvegarde. L'un des NIC est utilisé pour acheminer tout le trafic du réseau. Si le lien de cette carte est perdu pour une raison quelconque, l'autre carte devient active. Avant d'activer le couplage NIC, assurez-vous que les deux cartes NIC sont connectées au même segment de réseau (sous-réseau) et que vos adresses IP sont uniquement configurées sur l'une des NIC existantes.

> ***Remarque :*** *si vous utilisez un environnement de serveur virtuel ou dans le cloud, l'option* ***Activer le couplage NIC*** *n'est pas disponible.*

Bien que plusieurs adresses IP peuvent être attribuées à chaque contrôleur d'interface réseau (NIC), ne configurez pas un NIC de sorte qu'il est une adresse IP se trouvant sur le même sous-réseau en tant qu'adresse IP de l'autre carte NIC. Dans ce cas, des paquets de données sont perdus pour les paquets provenant de l'IP de la NIC qui n'a pas la passerelle par défaut. Veuillez prendre en considération l'exemple de configuration suivant :



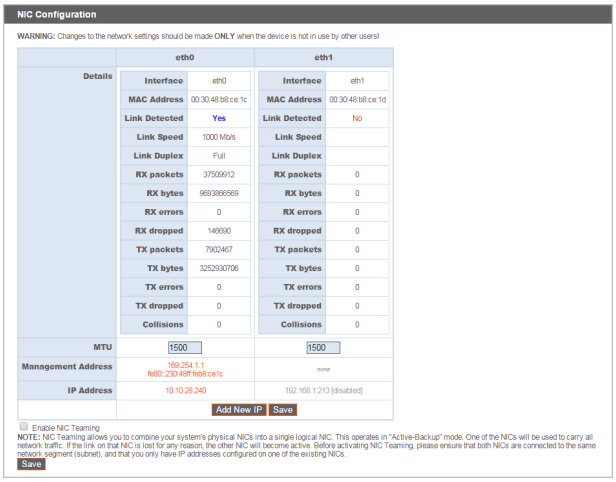
- eth0 est configuré avec la passerelle par défaut 192.168.1.1
- eth0 est associé à 192.168.1.5
- eth1 est associé à 192.168.1.10
- eth0 et eth1 sont connectés au même commutateur de sous-réseau

Avec cette configuration, le trafic des deux cartes NIC est envoyé vers la passerelle par défaut (192.168.1.1), quelle que soit la carte NIC ayant reçu le trafic. Les commutateurs configurés à l'aide de protocoles de résolution d'adresse dynamiques (ARP) envoient des paquets aléatoirement à eth0 (192.168.1.5) ou à eth1 (192.168.1.10), pas aux deux cartes. Lorsque eth0 reçoit ces paquets du commutateur destiné à eth1, eth0 abandonne les paquets. Certains commutateurs sont configurés avec un protocole ARP statique. Ces commutateurs abandonnent tous les paquets reçus par eth1, puisque cette carte NIC n'a pas de passerelle par défaut et ne se trouve pas dans le tableau ARP statique de la passerelle. Si vous souhaitez configurer des cartes NIC redondantes sur le même sous-réseau, utilisez le couplage NIC.

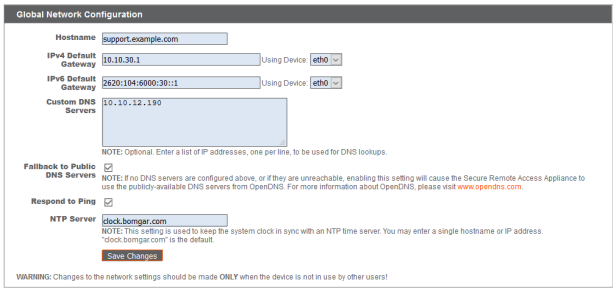
Par défaut, Dynamic Host Configuration Protocol (DHCP) est activé pour votre serveur. Le DHCP est un protocole de réseau qui utilise le serveur DHCP pour contrôler la distribution des paramètres de réseau, notamment les adresses IP, ce qui permet aux systèmes de demander ces paramètres automatiquement. Ainsi, la configuration manuelle des paramètres est réduite. Dans ce cas, lorsqu'on coche cette option, l'adresse IP est obtenue à partir du serveur DHCP et elle est retirée du groupe d'adresses IP disponibles.

Pour en savoir plus sur DHCP, consultez Qu'est-ce que DHCP ? à l'adresse docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/dd145320(v=ws.10).

Cliquez sur **Afficher les informations** pour consulter et vérifier les statistiques de transmission et de réception pour chaque port Ethernet sur le serveur.



Dans la section **Configuration globale du réseau**, configurez le nom d'hôte pour votre Secure Remote Access Appliance.

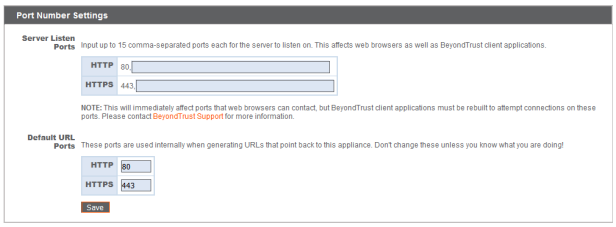


Remarque : *le champ Nom de l'hôte ne doit satisfaire aucune exigence technique. Cela n'affecte pas la connexion du nom d'hôte du logiciel client ou des utilisateurs distants. Si le nom d'hôte tenté par un logiciel client doit changer, prévenez l'Assistance technique BeyondTrust des changements requis afin qu'elle puisse créer une mise à jour logicielle. Le champ Nom d'hôte sert principalement à effectuer une différenciation quand il y a plus d'un Secure Remote Access Appliance. Ce champ est également utilisé en tant qu'identificateur de serveur local lorsqu'on établit des connexions SMTP pour envoyer des alertes par e-mail. Cette option est utile lorsque le* ***Serveur relais SMTP*** *défini dans* ***/appliance > Sécurité > Configuration e-mail*** *est verrouillé. Dans ce cas, le nom d'hôte configuré doit parfois correspondre à la résolution DNS inverse de l'adresse IP du serveur.*

Assignez une passerelle par défaut, en sélectionnant le port Ethernet à utiliser. Indiquez une adresse IP pour un ou plusieurs serveur DNS. Si le protocole DHCP est activé, le bail DHCP offre une passerelle par défaut, ainsi qu'une liste de serveurs DNS par ordre de préférence. Les serveurs DNS configurés de façon statique répertoriés dans les **serveurs DNS personnalisés** sont prioritaires lors des tentatives de connexion, suivis des serveur DNS provenant du DHCP. Si ces serveurs DNS locaux ne sont pas disponibles, l'option **Utilisation des serveurs DNS publics** permet au Secure Remote Access Appliance d'utiliser des serveurs DNS publics disponibles sur OpenDNS.

Pour plus d'informations sur OpenDNS, veuillez consulter www.opendns.com.

Autorisez votre serveur à répondre aux pings si vous souhaitez que la fonction teste si l'hôte fonctionne. Configurez le nom d'hôte ou l'adresse IP par rapport à un serveur NTP (protocole d'heure réseau) avec lequel vous souhaitez synchroniser votre Secure Remote Access Appliance.

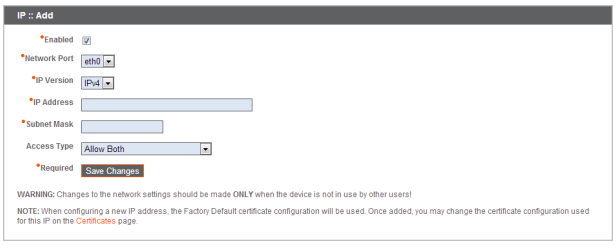


Deux options sont disponibles dans la **Configuration du numéro de port** : **Ports détectés par le serveur** et **Ports URL par défaut**. Lors de la configuration, n'oubliez pas que les connexions à des ports valables sont susceptibles d'être rejetées en raison des restrictions liées au réseau définies dans **/appliance > Sécurité > Administration du serveur** et dans **/login > Gestion > Sécurité**. L'inverse est tout aussi vrai : les connexions à des ports non valables sont rejetées, même si elles satisfont aux restrictions du réseau.

La section **Ports détectés par le serveur** permet de définir les ports détectables par le serveur. Vous pouvez utiliser jusqu'à 15 ports séparés par la virgule pour le protocole HTTP et 15 ports séparés par la virgule pour le protocole HTTPS. Un port ne doit apparaître qu'une seule fois dans un champ, et il doit apparaître dans un seul champ, pas dans les deux champs. Le serveur répond aux connexions HTTP associées aux ports répertoriés dans le champ HTTP, et le serveur répond aux connexions HTTPS associées aux ports du champ HTTPS. Il est impossible de modifier les ports d'écoute intégrés (80 et 443), à moins de contacter l'assistance technique BeyondTrust et de mettre à jour le serveur.

Pour accéder au serveur sur un port donné, utilisez un navigateur qui vous oblige à indiquer le port dans l'URL du navigateur (ex. : support.example.com:8200). Les clients téléchargés depuis le serveur tentent de se connecter aux ports répertoriés sur la page **/login > État > Information** dans **Ce logiciel client est paramétré pour se connecter à**. Ces ports ne sont pas configurables depuis /login ou /appliance. Pour les changer, vous devez contacter l'assistance technique BeyondTrust pour qu'elle vous fournisse une nouvelle mise à jour pour votre serveur. Une fois installée, la mise à jour définit les ports de **Tentative** tels que définis par l'assistance technique BeyondTrust dans les paramètres de la mise à jour.

L'option **Ports URL par défaut** est utilisée lors de la création d'URL pointant vers le serveur, comme une clé de session générée par la console d'accès. Lorsque les ports par défaut sont bloqués sur le réseau (ou qu'ils sont susceptibles de ne pas fonctionner pour toute autre raison), il est possible de changer les ports URL par défaut pour obtenir des URL générées par les ports que l'on souhaite. Les ports indiqués doivent aussi être répertoriés dans les **Ports détectés par le serveur** ; dans le cas contraire, les ports par défaut ne se connectent pas. Ainsi, si vous saisissez **8080** dans le champ **Ports URL par défaut**, vérifiez que **8080** se trouve également dans le champ **Ports détectés HTTP** ou dans le champ **Ports détectés HTTPS**. Contrairement aux champs Ports détectés, il est impossible d'indiquer plus d'un port dans les deux champs Ports URL. Vous ne pouvez pas indiquer le même port dans les deux champs.



Lors de l'ajout ou de la modification d'une adresse IP, vous pouvez choisir d'activer ou de désactiver cette IP. Sélectionnez le port réseau pour lequel cette IP doit fonctionner. Le champ **Adresse IP** configure l'adresse à laquelle votre serveur peut répondre, et le champ **Masque de sous-réseau** permet à BeyondTrust de communiquer avec d'autres appareils.

Lorsque vous modifiez une adresse IP se trouvant sur le même sous-réseau qu'une autre adresse IP pour ce serveur, vous pouvez la définir en tant qu'adresse **Principale**. Lorsque cette case est cochée, le serveur la considère comme adresse IP principale ou comme adresse IP de départ pour le sous-réseau. Cette option permet, par exemple, de s'assurer que tout trafic réseau provenant du serveur sur le sous-réseau respecte un ensemble de règles définies liées au pare-feu.

Depuis **Type d'accès**, vous pouvez limiter l'accès à cette IP au site public ou au client d'utilisateur. Utilisez **Autoriser les deux** pour permettre l'accès au site public et au client d'utilisateur.

> ***Remarque :*** *pour limiter l'accès à l'interface* ***/login****, définissez les restrictions de réseau dans* ***/login > Gestion > Sécurité****. Pour limiter l'accès à l'interface* ***/appliance****, définissez les restrictions de réseau dans* ***/appliance > Sécurité > Administration du serveur****.*

Lorsque vous consultez l'adresse IP de gestion[1], le menu déroulant du **Serveur Telnet** propose trois options : **Complet**, **Simplifié** et **Désactivé** (voir explications ci-dessous). Ces paramètres servent à changer les options du menu du serveur Telnet disponibles uniquement sur cette IP privée. Cette fonctionnalité peut se révéler utile dans les situations de récupération d'urgence. Dans la mesure où la fonction Telnet est liée à l'IP privée intégrée, elle n'apparaît dans aucune autre adresse IP configurée.

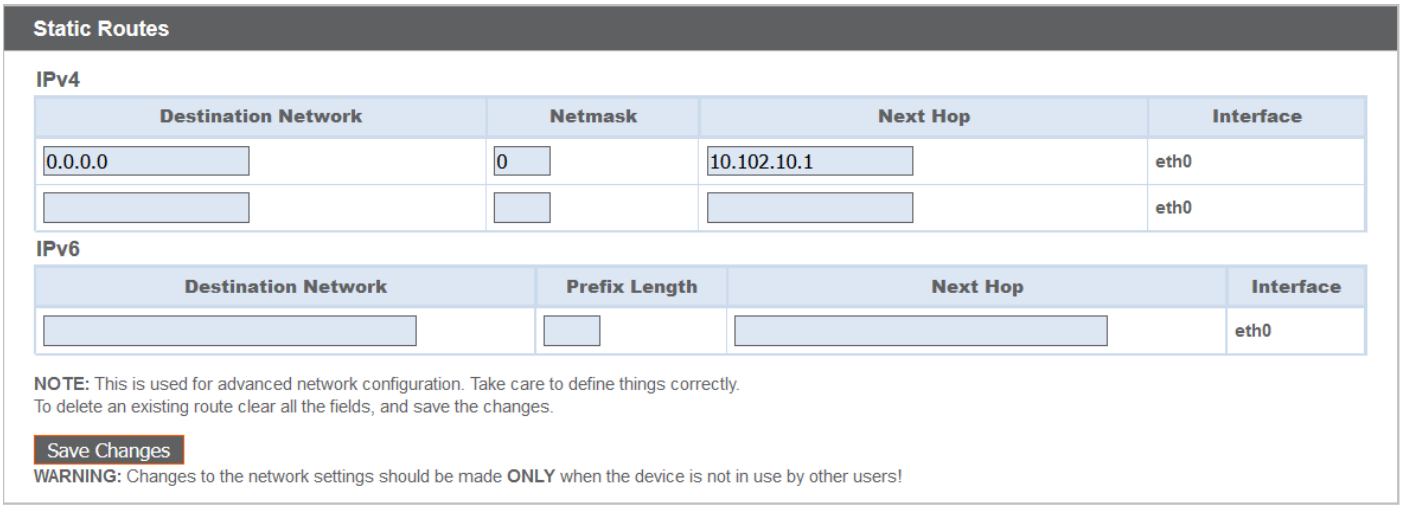
Paramètre	Fonction
Complet	Permet au serveur Telnet d'utiliser l'ensemble de ses fonctionnalités
Simplifié	Offre quatre options différentes : **Voir l'erreur du FIPS**, **Revenir aux paramètres d'usine par défaut**, **Éteindre** et **Redémarrer**
Désactivé (e)	Désactive complètement le serveur Telnet

[1]Ne pas supprimer ou modifier l'adresse IP de gestion.

Routes statiques : définissez des routes statiques pour établir une communication entre réseaux

Lorsque deux réseaux sont incapables de communiquer entre eux, la configuration d'une route statique permet à un administrateur doté d'un ordinateur sur l'un des réseaux de se connecter, par le biais du Secure Remote Access Appliance, à un ordinateur sur l'autre réseau, pour peu que le serveur se trouve à un endroit où les deux réseaux sont en mesure de communiquer individuellement avec ce dernier.

L'installation de routes statiques devrait être réservée aux administrateurs avancés.



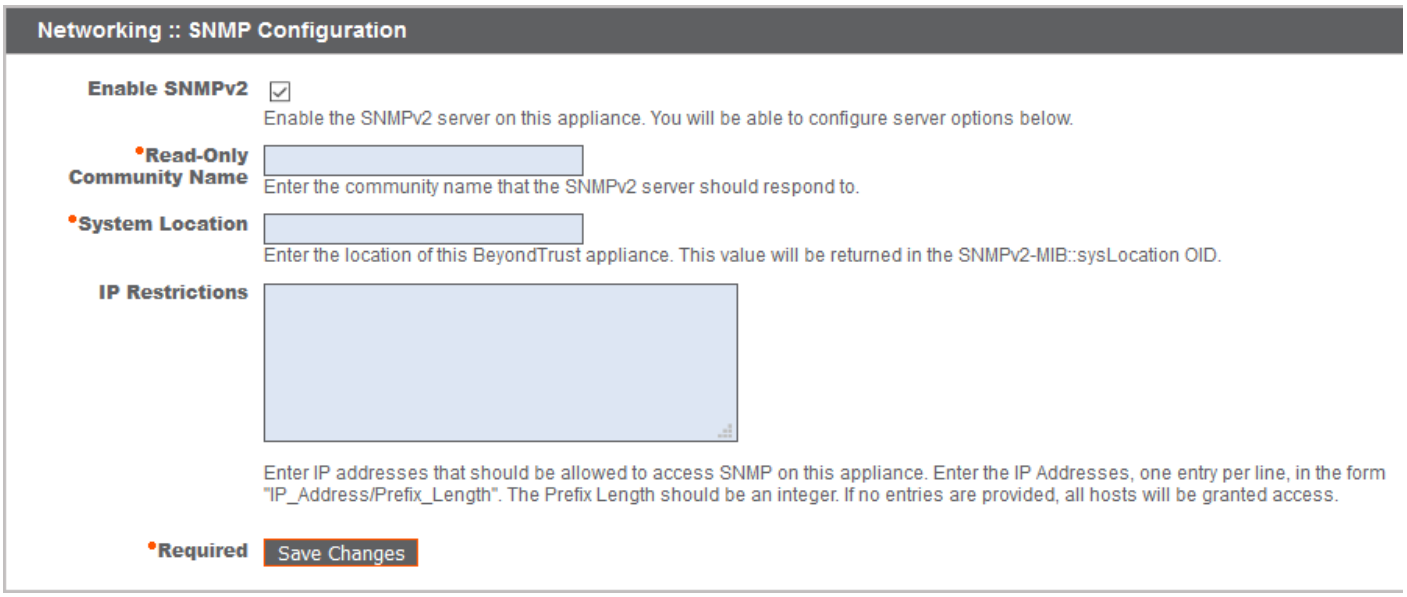
SNMP : activez le protocole simple de gestion réseau

Le Secure Remote Access Appliance prend en charge le protocole simple de gestion réseau (SNMP). Le SNMP est un protocole Internet standard servant au contrôle et à la surveillance des équipements en réseau.

> Pour plus d'informations sur le SNMP, veuillez consulter Protocole simple de gestion réseau à l'adresse wikipedia.org/wiki/Simple_Network_Management_Protocol.

Grâce à cette option, les outils chargés de recueillir les données relatives à la disponibilité et d'autres statistiques par le biais du protocole SNMP peuvent interroger le Secure Remote Access Appliance à des fins de contrôle.

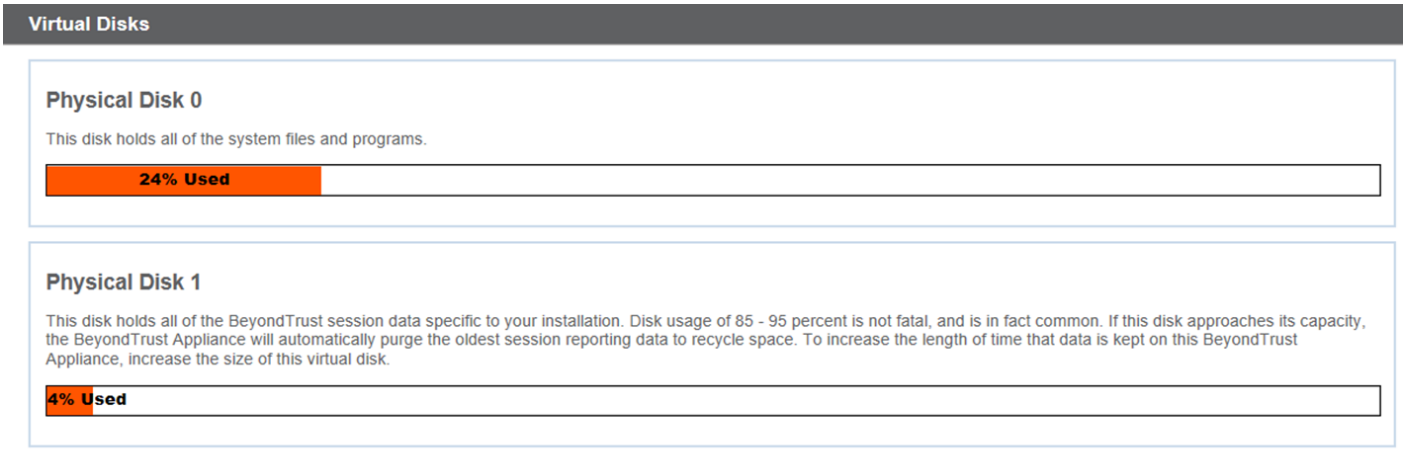
Pour activer le SNMP pour ce serveur, cochez **Activer SNMPv2**. Ce paramètre permet au serveur SNMPv2 de répondre aux demandes du SNMP. Saisissez une valeur pour le **Nom de communauté en lecture seule**, l'**Emplacement du système** et les **Restrictions d'IP** (adresses IP autorisées à interroger ce serveur à l'aide du SNMP). Si aucune adresse IP n'est indiquée, tous les hôtes ont un droit d'accès.



Stockage

État : Espace disque et état des disques durs

La page **État** affiche le pourcentage de l'espace sur le disque dur utilisé de votre Secure Remote Access Appliance.



Si vous autorisez les fonctions d'enregistrement sur votre site (session, tunnel par protocole et enregistrements de Shell distants) ou si le nombre de vos sessions est élevé, il est probable que l'utilisation de votre disque soit importante. Une utilisation de disque de 85 % à 95 % n'a rien d'inquiétant. Si le disque dur n'a pas beaucoup d'espace disque, le serveur est configuré pour purger automatiquement les données de l'ancienne session et recycler l'espace disque pour les nouvelles données de session.

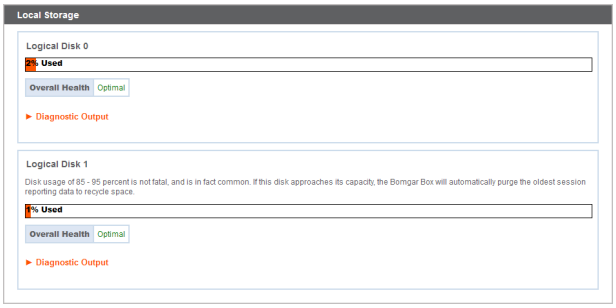
Spécifique au serveur BeyondTrust B300P

Le B300P utilise un ensemble redondant de disques indépendants pour sauvegarder vos données. RAID 6 permet au serveur de perdre 2 disques sur 4 sans perte de données. En cas de défaillance, retirez le disque corrompu et contactez BeyondTrust pour profiter de la procédure de retour d'article défectueux et de réparation ou de remplacement du disque. Lors du remplacement du disque endommagé, le serveur recrée automatiquement le RAID à l'aide du nouveau disque. Il n'est pas nécessaire d'éteindre le serveur lors du remplacement d'un disque.

Spécifique au serveur BeyondTrust B400P

Le B400P possède deux groupes de disques logiques de type RAID. La configuration RAID comprend huit disques physiques configurés dans deux disques RAID logiques : Une configuration RAID 1 qui correspond à un disque logique 0, et une configuration RAID 6 qui correspond à un disque logique 1.

Le dysfonctionnement de l'un des disques physiques RAID 1 ou RAID 6 n'entraîne pas de pertes de données et n'affecte pas les performances. Toutefois, le dysfonctionnement du second disque dans la configuration RAID 6 a un effet sur les performances, mais ne se traduit pas par une perte de données.



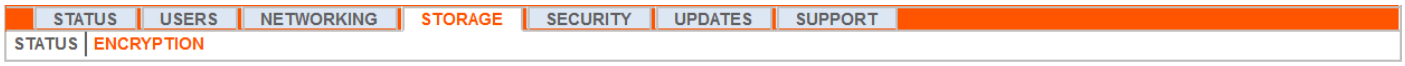
Notification de dysfonctionnement du matériel (B300P et B400P uniquement)

Les témoins LED de votre serveur renseignent également sur l'état de vos disques durs. Normalement, les témoins LED clignotent pour signaler l'activité du disque. Lorsque le disque dur ne fonctionne pas correctement, le témoin DEL passe au rouge et une alarme vous indique un dysfonctionnement. Pour désactiver l'alarme avant que le système ne soit rétabli, cliquez sur le bouton **Arrêter l'alarme** sur l'interface Web.

Remarque : *le bouton* ***Arrêter l'alarme*** *est disponible, même si aucune alarme n'est en train de retentir. Le bouton ne peut utilisé comme un indicateur pour savoir si une alarme est active à un moment donné.*

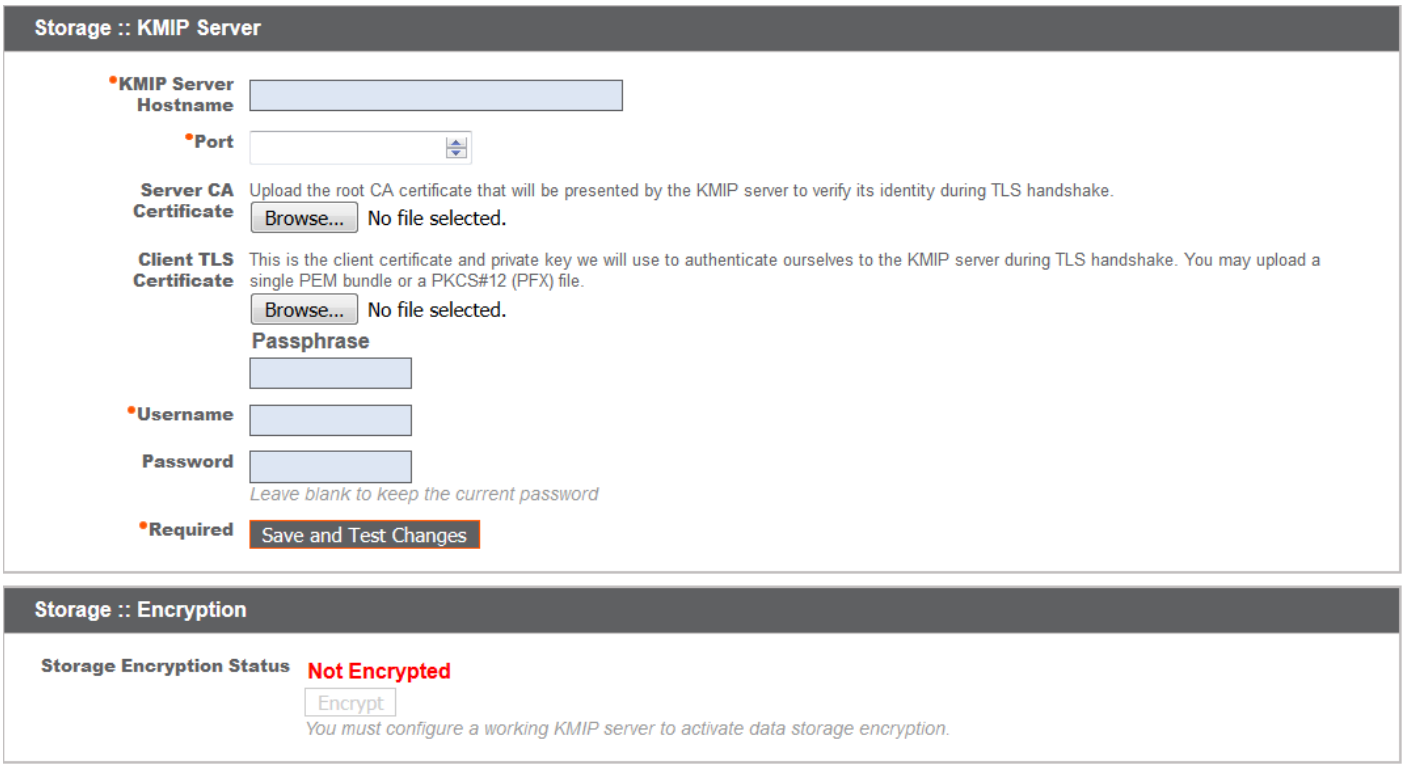
Remarque : *pour vérifier si une alarme sonne, consultez l'option* ***État de santé*** *située juste au-dessus du bouton* ***Arrêter l'alarme****. Si une alarme sonne dans la pièce où se trouve le Secure Remote Access Appliance et que vous souhaitez éliminer le serveur comme source, cliquez sur le bouton* ***Arrêter l'alarme*** *plusieurs fois pour annuler les alarmes susceptibles d'être actives.*

Chiffrement : Configurez le serveur KMIP et chiffrez les données de session



La section **Chiffrement** vous permet de chiffrer les données de session stockées dans votre Secure Remote Access Appliance. Avant d'utiliser la fonctionnalité de chiffrement des données stockées pour chiffrer vos données de session, il faut disposer d'un serveur KMIP (protocole d'interopérabilité et de gestion des clés) dans votre environnement pour stocker les clés de chiffrement pour chiffrer et déchiffrer les disques sur votre Secure Remote Access Appliance. Lorsque vous chiffrez vos données pour la première fois, la quantité maximale de données à utiliser est de 4 Go. Après le premier chiffrement, la limite de 4 Go ne s'applique plus.

> ***Remarque :*** *Si vous souhaitez chiffrer au-delà de 4 Go dans un premier temps, contactez Assistance technique BeyondTrust à l'adresse www.beyondtrust.com/support.*



Dans la section **Stockage :: Serveur KMIP**, saisissez le nom d'hôte pour votre serveur KMIP externe et le port à utiliser pour accéder au serveur. Mettez en ligne un certificat valable signé par une autorité de certification, qui sera soumis au serveur KMIP pour que son identité soit vérifiée auprès du Secure Remote Access Appliance, ainsi qu'une clé privée de certificat client, utilisée pour authentifier le Secure Remote Access Appliance auprès du serveur KMIP.

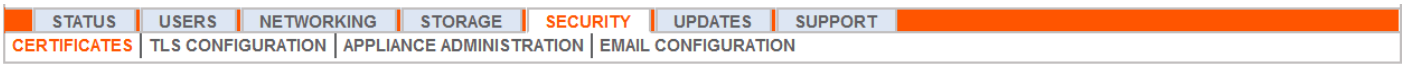
Saisissez une phrase secrète, un nom d'utilisateur et un mot de passe pour permettre l'authentification auprès du serveur KMIP. Cliquez sur **Enregistrer et tester les changements** pour enregistrer et tester la connexion entre le Secure Remote Access Appliance et le serveur KMIP.

Lorsqu'une connexion est établie entre le serveur KMIP et le serveur, le bouton **Chiffrer** apparaît dans la section **Stockage :: Chiffrement**. Si le serveur KMIP n'est pas bien configuré ou si les données n'ont pas encore été chiffrées, l'option **Chiffrer** n'est pas disponible et affiche **Non chiffré**.

Lorsqu'on clique sur le bouton **Chiffrer**, le serveur lance le processus de sauvegarde des données de session et la création d'une clé de chiffrement à stocker sur le serveur KMIP. Une fois que la clé de chiffrement est stockée, les données sont chiffrées et une sauvegarde est rétablie.

Sécurité

Certificats : Créer et gérer les certificats TLS



Gérez les certificats TLS, créez des certificats auto-signés et des demandes de certificat, et importez des certificats signés par une autorité de certification.

Installation de certificat

Le Secure Remote Access Appliance dispose d'un certificat auto-signé préinstallé. Toutefois, pour utiliser efficacement votre Secure Remote Access Appliance, il est nécessaire de créer au moins un certificat auto-signé, en privilégiant les demandes et les mises en ligne de certificat signé par une autorité de certification. 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.

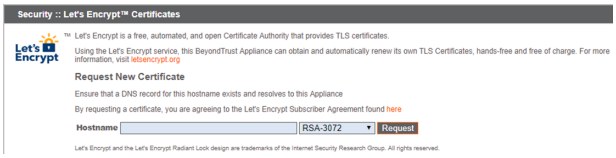
Let's Encrypt

Let's Encrypt remet des certificats signés d'une validité de 90 jours qui peuvent se renouveler automatiquement et indéfiniment. Pour demander un certificat Let's Encrypt ou en renouveler un à l'avenir, vous devez satisfaire aux exigences suivantes :

- Le DNS pour le nom d'hôte que vous demandez doit pointer vers le serveur.
- Le serveur doit pouvoir contacter Let's Encrypt sur le port TCP 443.
- Let's Encrypt doit pouvoir contacter le serveur sur le port TCP 80.

Pour plus d'informations, veuillez visiter letsencrypt.org.

Pour implémenter un certificat Let's Encrypt, allez dans la section **Sécurité :: Certificats Let's Encrypt™** et :



- Saisissez le nom de domaine complet (FQDN) du serveur dans le champ **Nom d'hôte**.
- Utilisez le menu déroulant pour choisir le type de clé de certificat.
- Cliquez sur **Demande**.

Tant que les conditions ci-dessus sont remplies, le certificat se renouvellera automatiquement tous les 90 jours une fois le contrôle de validité avec Let's Encrypt effectué.

Remarque : *Le serveur lance le processus de renouvellement du certificat 30 jours avant l'expiration du certificat et nécessite le même processus que la requête d'origine. Si celui-ci n'a pas abouti 25 jours avant l'expiration, le serveur enverra des alertes quotidiennes par e-mail à l'administrateur (si les notifications par e-mail sont activées). Le statut affichera le certificat dans un statut d'erreur.*

IMPORTANT !

Étant donné que le DNS ne peut s'appliquer qu'à un serveur à la fois, et comme un serveur doit se voir attribuer le nom d'hôte de DNS pour lequel il fait une demande de certificat ou une demande de renouvellement, nous vous recommandons d'éviter d'utiliser des certificats Let's Encrypt pour les paires de serveurs en reprise en séquence.

***Remarque :** si le certificat demandé est un remplacement, il est nécessaire de sélectionner la clé existante du certificat à remplacer.*

*Si le certificat demandé est un renouvellement de clé, sélectionnez **Nouvelle clé** pour le certificat.*

*Lors d'un renouvellement de clé, les informations de la section **Sécurité :: Certificats :: Nouveau certificat** doivent correspondre à celles du certificat pour lequel le renouvellement de clé est demandé. Il est possible d'utiliser un nouveau nom de certificat reconnaissable pour identifier facilement le certificat dans la section **Sécurité :: Certificats**.*

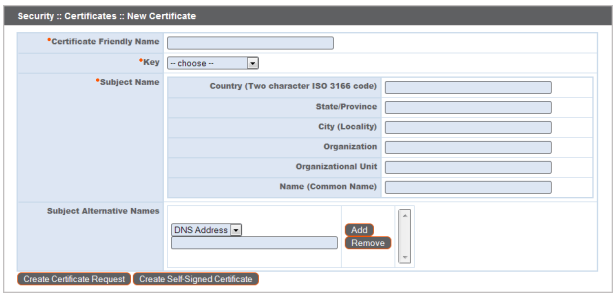
*Les informations à fournir pour un renouvellement de clé peuvent être obtenues en cliquant sur l'ancien certificat répertorié dans la section **Sécurité :: Certificats**.*

Pour obtenir un certificat de nouvelle clé ou de renouvellement de clé, la marche à suivre pour l'importation est identique.

Autres certificats remis par des AC

Pour créer une demande de certificat :

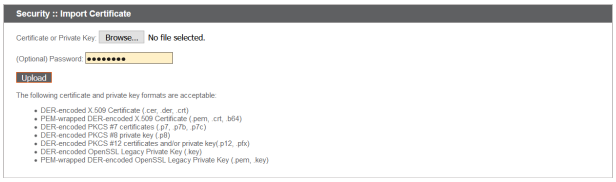
- Allez dans la section **Sécurité :: Autres certificats** et cliquez sur **Créer**.
- Dans le champ **Nom du certificat**, saisissez un nom que vous utiliserez pour identifier ce certificat.
- Dans le menu déroulant **Clé**, trouvez la **Clé existante** de votre certificat *.beyondtrustcloud.com.
- Indiquez le reste des informations relatives à votre organisation.
- Dans le champ **Nom (nom courant)**, saisissez un titre descriptif pour votre site BeyondTrust.
- Dans la section **Noms du sujet alternatifs**, indiquez le nom d'hôte de votre site BeyondTrust, puis cliquez sur **Ajouter**.
  Ajoutez un certificat SAN pour chaque nom DNS ou adresse IP à protéger par ce certificat SSL.



***Remarque :** Les adresses DNS peuvent être saisies comme des noms de domaine complets, comme access.example.com, ou comme des noms de domaine à caractère générique, comme *.example.com. Un nom de domaine à caractère générique englobe plusieurs sous-domaines, comme access.example.com, remote.example.com et ainsi de suite.*

Cliquez sur **Créer une demande de certificat**.

Pour utiliser un certificat signé par une AC, contactez l'autorité de certificat de votre choix et achetez-lui un nouveau certificat à l'aide d'une DSC que vous avez créée dans BeyondTrust. Une fois l'achat effectué, l'AC vous envoie un ou plusieurs fichiers de certificat à installer sur le Secure Remote Access Appliance.



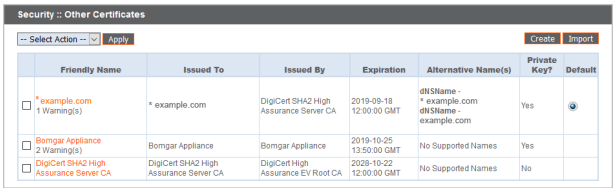
Pour mettre en ligne vos nouveaux fichiers de certificat, cliquez sur **Importer**. Accédez au premier fichier et mettez-le en ligne. Répétez cette opération pour chaque certificat envoyé par votre AC. Bien souvent, l'AC n'envoie pas le certificat racine, celui-ci devant être installé sur votre Secure Remote Access Appliance. En l'absence d'un certificat racine, un avertissement est visible sous le nouveau certificat : « Il manque une ou plusieurs autorités de certification à la chaîne de certificats. La chaîne ne se termine pas par un certificat auto-signé. »

Pour télécharger un certificat racine pour le certificat de votre serveur, consultez les informations envoyées par votre AC pour obtenir un lien vers le certificat racine adéquat. Si aucun n'est accessible, contactez l'AC pour en obtenir un. Si cette démarche se révèle peu pratique, recherchez dans son site Web pour accéder à son magasin de certificats racine. Vous y trouverez l'ensemble des certificats racine de l'AC. Les principales AC proposent leurs certificats racine en ligne.

En général, la façon la plus simple de trouver la racine adaptée à votre certificat est d'ouvrir le fichier de certificat de votre machine locale et d'analyser son **Chemin d'accès de certification** ou sa **Hiérarchie de certification**. La racine de la hiérarchie ou du chemin se trouve en principe au sommet de l'arbre. Repérez le certificat racine. Téléchargez-le ensuite dans le magasin de certificats racine de l'AC et importez-le dans votre Secure Remote Access Appliance, comme indiqué ci-dessus.

Certificats

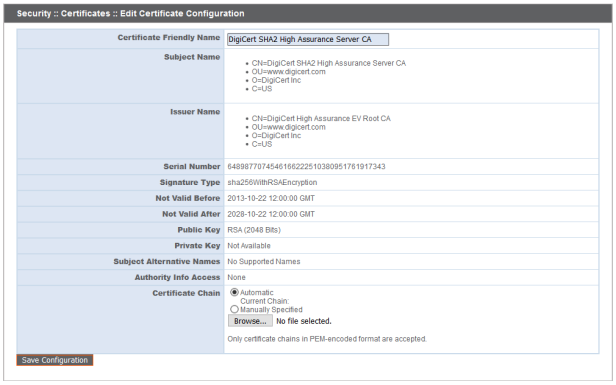
Consultez un tableau de certificats SSL disponibles sur votre serveur.



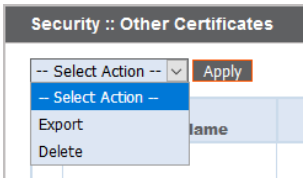
Pour les connexions incompatibles avec l'indication du nom de serveur (SNI) ou pour celles qui ne fournissent pas le bon SNI, sélectionnez un certificat SSL par défaut dans la liste pour prendre en charge ces connexions en cliquant sur le bouton sous la colonne **Défaut**. Le certificat SSL par défaut ne peut pas être un certificat auto-signé ni être le certificat du Secure Remote Access Appliance fourni lors de l'installation initiale.

> Pour en savoir plus sur les SNI, consultez Indication du nom de serveur à l'adresse https://cio.gov/sni/.

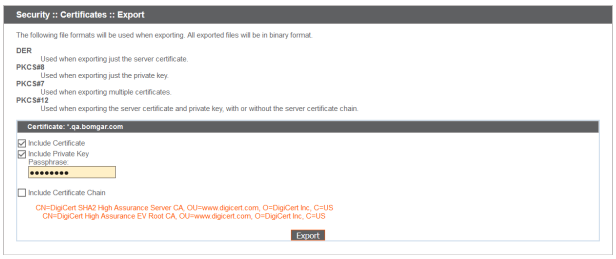
Cliquez sur un nom de certificat pour consulter ses détails et gérer sa chaîne de certificats.



Pour exporter un ou plusieurs certificats, cochez la case du certificat à exporter, sélectionnez **Exporter** dans le menu déroulant en haut du tableau et cliquez sur **Appliquer**.

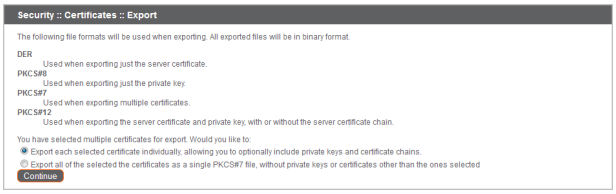


Si vous n'exportez qu'un seul certificat, vous pouvez immédiatement indiquer le certificat ou la chaîne de certificats si disponibles. Cliquez sur **Exporter** pour lancer le téléchargement.

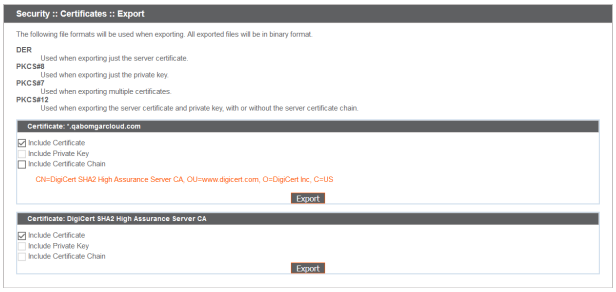


Si vous exportez plusieurs certificats, vous disposez d'une option pour exporter chaque certificat individuellement ou dans un seul fichier PKCS#7.

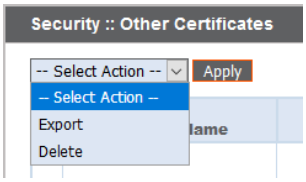
Si vous choisissez d'exporter plusieurs certificats dans un seul fichier, cliquez sur **Continuer** pour lancer le téléchargement. Avec cette option, seuls les fichiers du certificat actuel sont exportés, sans les chaînes de certificat.



Pour prendre en compte les chaînes de certificat lors de l'exportation, choisissez l'exportation individuelle et cliquez sur **Continuer** pour voir les certificats sélectionnés. Pour chaque liste, vous pouvez indiquer le certificat ou la chaîne de certificats si disponibles. Cliquez sur **Exporter** pour lancer le téléchargement.



Pour supprimer un ou plusieurs certificats, cochez la case de chaque certificat à supprimer, sélectionnez **Supprimer** dans le menu déroulant en haut du tableau et cliquez sur **Appliquer**.

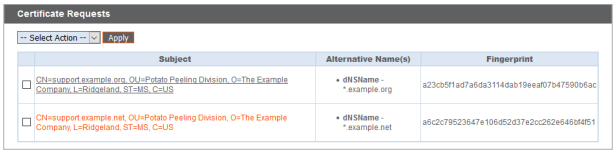


> ***Remarque :*** *en principe, un certificat ne doit jamais être supprimé à moins qu'il n'ait été remplacé par un remplaçant fonctionnel.*

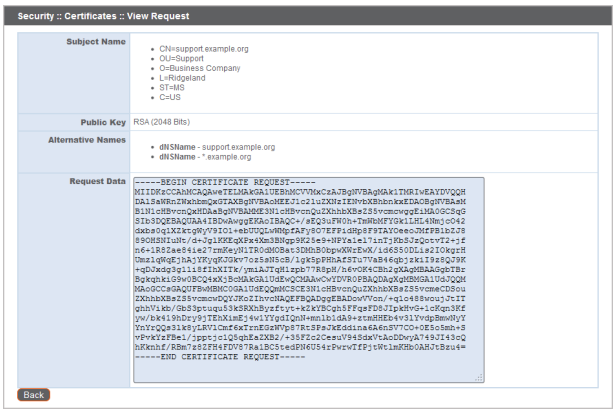
Pour confirmer la précision de votre sélection, consultez les certificats à supprimer, puis cliquez sur **Supprimer.**

Demandes de certificat

Consultez un tableau des demandes en attente pour les certificats signés par une tierce partie. Cliquez sur un nom de demande de certificat pour consulter les informations.

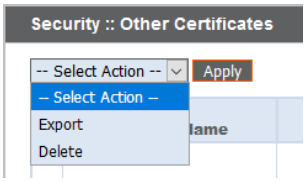


La demande d'informations affiche aussi les données de demande que vous avez indiquées à l'autorité de certification de votre choix lors de la demande d'un certificat signé.

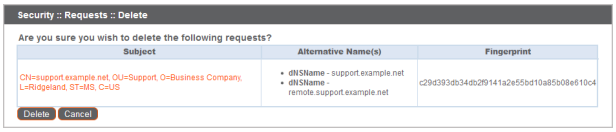


> ***Remarque :*** *si vous renouvelez un certificat, utilisez le même certificat Demande de données utilisé pour le certificat d'origine.*

Pour supprimer une ou plusieurs demandes de certificat, cochez la case de chaque demande à supprimer, sélectionnez **Supprimer** dans le menu déroulant en haut du tableau et cliquez sur **Appliquer**.

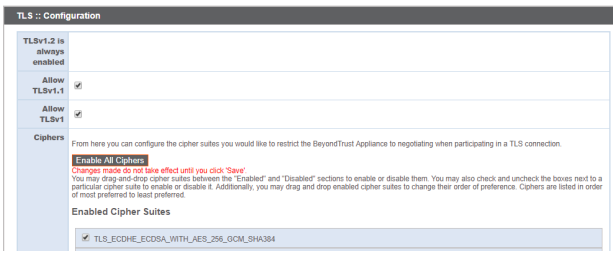


Pour confirmer la précision de votre sélection, consultez les demandes de certificat à supprimer, puis cliquez sur **Supprimer**.



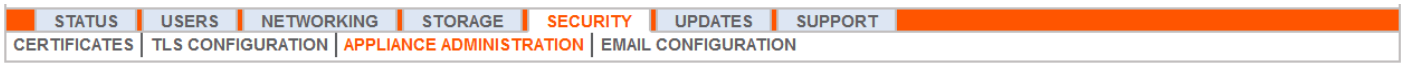
Configuration TLS : choisir les suites cryptographiques et les versions TLS

Il est à noter que certains navigateurs anciens ne prennent pas en charge TLSv1.2. Si vous désactivez une ou plusieurs versions anciennes de protocoles de sécurité et que vous tentez d'accéder à votre interface d'administration depuis un navigateur ancien incompatible avec les protocoles de sécurité activés, BeyondTrust ne vous autorise pas à vous connecter.
Ce paramètre affecte principalement les connexions à l'interface Web de votre Secure Remote Access Appliance. Le tunnel d'assistance entre votre ordinateur et votre ordinateur client utilise par défaut TLSv1.2, même si vous avez activé d'autres protocoles de sécurité.

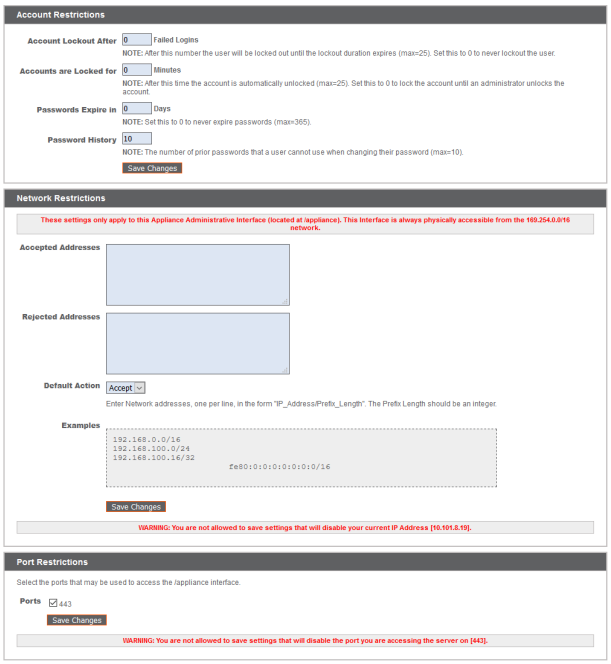


Sélectionnez les suites cryptographiques à activer ou à désactiver sur votre serveur. Faites glisser et déplacez les suites cryptographiques pour changer l'ordre de préférence. Les changements apportés aux suites cryptographiques ne prennent effet que lorsqu'on clique sur le bouton **Enregistrer**.

Administration du serveur : Définissez des restrictions liés aux comptes, aux réseaux et aux ports, activez un serveur STUN, installez un protocole Syslog, activez un accord de connexion, réinitialisez un compte d'administrateur



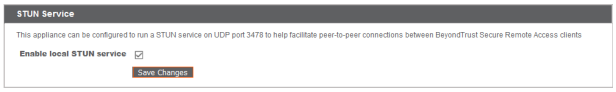
Gérez l'accès aux comptes d'interface d'administration /appliance en définissant le nombre d'échecs de connexion autorisé. Configurez la durée de blocage d'un compte lorsque la limite d'échecs de connexion est dépassée. Paramétrez aussi le nombre de jours de validité d'un mot de passe avant son expiration, et limitez la réutilisation d'anciens mots de passe.



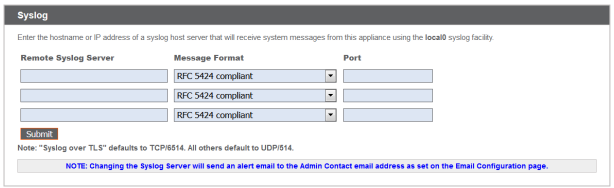
Vous pouvez limiter l'accès à l'interface d'administration de votre serveur en définissant des adresses de réseau autorisées ou non. Il est également possible de sélectionner les ports pour lesquels cette interface est accessible.

Dans le champ **Adresses autorisées**, définissez les adresses IP ou les réseaux qui sont toujours autorisés à accéder à /appliance. Dans le champ **Adresses interdites**, définissez les adresses IP ou les réseaux qui ne sont jamais autorisés à accéder à /appliance. Utilisez le menu déroulant d'**Action par défaut** pour autoriser ou interdire les adresses IP et les réseaux ne figurant pas dans les champs ci-dessus. Dans les cas de chevauchement, la correspondance la plus spécifique est privilégiée.

Ainsi, si vous souhaitez autoriser l'accès à 10.10.0.0/16, mais que vous interdisez l'accès à 10.10.16.0/24 et à toute autre adresse, il convient d'indiquer **10.10.0.0/16** dans le champ **Adresses autorisées**, d'indiquer **10.10.16.0/24** dans le champ **Adresses interdites**, et de régler l'**Action par défaut** sur **Interdire**.



Le Secure Remote Access Appliance peut être configuré pour exécuter un service STUN sur le port UDP 3478 pour faciliter les connexions pair-à-pair entre les clients BeyondTrust. Cochez la case **Activer le service STUN local** pour utiliser cette fonctionnalité.



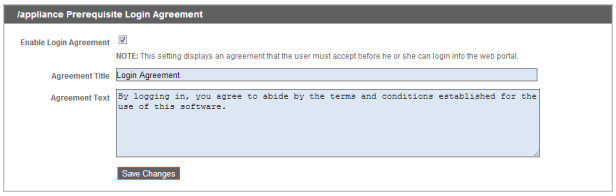
Vous pouvez configurer votre serveur pour envoyer des messages de connexion à trois serveurs syslog au maximum. Saisissez le nom d'hôte ou l'adresse IP du serveur syslog hôte recevant les messages de ce serveur dans le champ **Serveur Syslog distant**. Sélectionnez le format de date pour les messages de notification d'événement. Choisissez parmi les normes **RFC 5424**, l'un des formats **BSD existants** ou le format **Syslog via le protocole TLS**. Le syslog sur TLS utilise par défaut le port TCP 6514. Tous les autres formats utilisent par défaut UDP 514. Cependant, les valeurs par défaut peuvent être modifiées. Les connexions au Secure Remote Access Appliance sont envoyées à l'aide de la fonction **local0**.

Pour des paramètres spécifiques au cloud, veuillez consulter la section Administration du serveur : Syslog sur configuration TLS à l'adresse https://www.beyondtrust.com/docs/privileged-remote-access/getting-started/deployment/cloud/syslog-over-tls.htm.

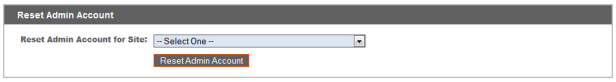
Remarque : *lorsqu'un serveur syslog est ajouté ou modifié, une alerte est envoyée par e-mail à l'administrateur. Les informations de l'administrateur sont configurées dans la section* ***Sécurité > Configuration e-mail > Sécurité :: Contact administrateur****.*

Pour en savoir plus sur les messages Syslog, consultez la section Guide pour les messages Syslog à l'adresse www.beyondtrust.com/docs/privileged-remote-access/how-to/integrations/syslog/.

Vous pouvez activer un accord de connexion que les utilisateurs devront accepter pour pouvoir accéder à l'interface d'administration /appliance. Cet accord configurable permet de spécifier des restrictions et des règles de politique interne relatives aux connexions utilisateur.



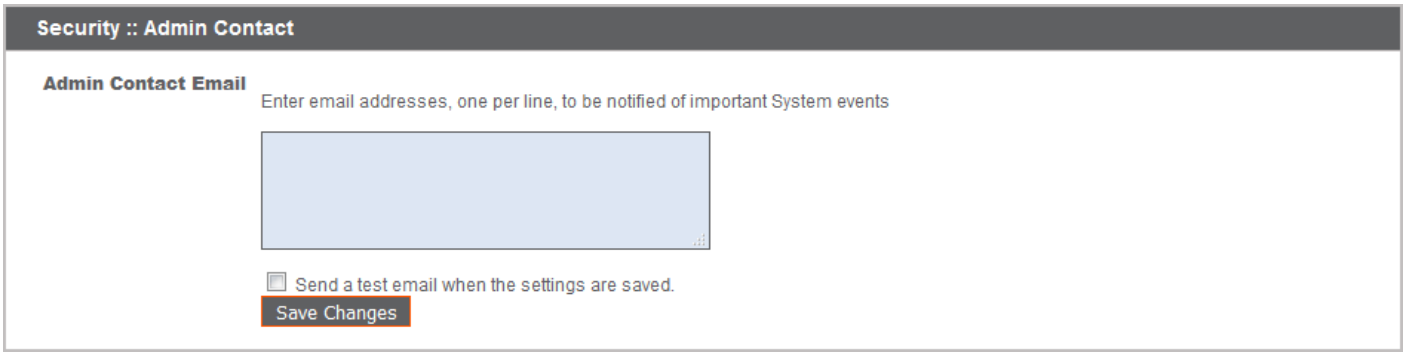
Vous pouvez sélectionner un site et cliquer sur **Réinitialiser le compte de l'administrateur** pour attribuer la valeur par défaut au nom d'utilisateur et au mot de passe de l'administrateur d'un site lorsqu'il est nécessaire d'oublier ou de remplacer l'identifiant de connexion.



Configuration e-mail : Configurer le serveur pour envoyer une alerte par e-mail

Configurez votre serveur relais SMTP et définissez un ou plusieurs administrateurs à contacter pour autoriser votre Secure Remote Access Appliance à vous envoyer des notifications automatiques par e-mail.

Après avoir indiqué les adresses e-mail pour les contacts de l'administrateur, enregistrez vos paramètres et envoyez un e-mail de test pour vous assurer que tout fonctionne convenablement.



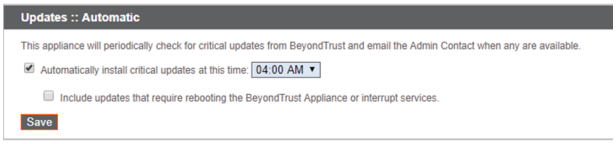
Un e-mail est envoyé dans les cas suivants :

- **Le serveur Syslog a été modifié** : un utilisateur sur /appliance a modifié le paramètre du serveur Syslog.
- **Problème de RAID** : un ou plusieurs disques logiques RAID ne se trouvent pas dans un état optimal (dégradé ou partiellement dégradé).
- **Notification d'expiration du certificat SSL** : un certificat SSL en cours d'utilisation (certificats d'entité de fin ou certificat AC dans la chaîne) expire dans 90 jours ou moins.

Mises à jour

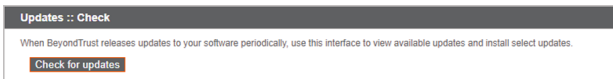
Rechercher les mises à jour disponibles et installer le logiciel

Le serveur recherche régulièrement les mises à jour critiques et envoie un e-mail à l'administrateur à contacter lorsque les mises à jour sont disponibles. Vous pouvez choisir d'installer automatiquement les mises à jour et utiliser le menu déroulant pour sélectionner une heure d'installation.



Les mises à jour nécessitant un redémarrage de serveur ou l'interruption de services sont exclues du processus de mise à jour automatique, sauf si vous cochez la case pour les prendre en compte.

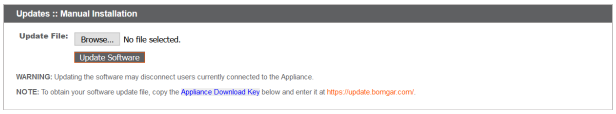
BeyondTrust continue à informerdes dernières versions dès qu'elles sont disponibles . Lorsqu'on vous informe de la disponibilité de nouvelles mises à jour pour votre serveur, cliquez sur le bouton **Rechercher les mises à jour** pour trouver les packages de mises à jour et pouvoir les installer.

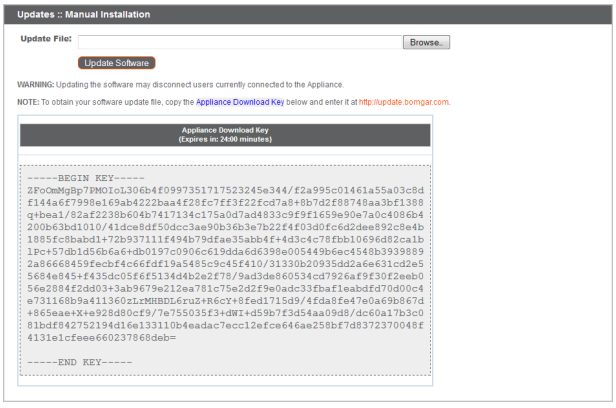


Si plusieurs packages logiciels ont été créés pour votre serveur, chacun d'entre eux est répertorié séparément dans la liste des mises à jour disponibles. Votre nouveau logiciel est automatiquement téléchargé et installé lorsque vous cliquez sur le bouton **Installer cette mise à jour**.

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.

Il n'est pas obligatoire d'utiliser la fonction **Rechercher les mises à jour**. Lorsque la règle de sécurité de votre organisation n'autorise pas les mises à jour automatiques, il est possible de rechercher les mises à jour manuellement. Cliquez sur le lien de la **Clé de téléchargement du serveur** pour générer une clé de serveur unique, puis, à partir d'un système non restreint, envoyez cette clé au serveur de mise à jour BeyondTrust à l'adresse https://btupdate.com. Téléchargez toutes les mises à jour disponibles sur un périphérique de stockage amovible, puis transférez-les sur un système à partir duquel vous pouvez gérer votre serveur.





Après avoir téléchargé un package logiciel, accédez au fichier à partir de la section **Installation manuelle**, puis cliquez sur le bouton **Mettre à jour le logiciel** pour terminer l'installation.

IMPORTANT !

Préparez-vous à installer les mises à jour du logiciel directement après le téléchargement. Une fois qu'une mise à jour a été téléchargée, elle n'apparaît plus sur votre liste de mises à jour disponibles. Si vous avez besoin de télécharger de nouveau une mise à jour logicielle, contactez l'Assistance technique BeyondTrust.

Lorsque l'écran du contrat de licence utilisateur final (CLUF) BeyondTrust apparaît, indiquez les informations de contact nécessaires et cliquez sur le bouton **Accepter-Lancer le téléchargement** pour accepter le CLUF et poursuivre l'installation.

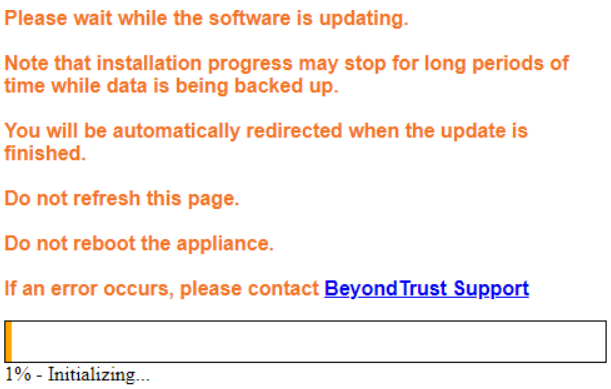
Si vous refusez le CLUF, un message d'erreur apparaît et il est impossible de mettre à jour votre logiciel BeyondTrust.

Si vous rencontrez le moindre problème pour mettre à jour le logiciel après avoir accepté le CLUF, contactez l'Assistance technique BeyondTrust à l'adresse www.beyondtrust.com/support.

Durant le processus d'installation, la page **Mises à jour** affiche une barre de progression vous informant du déroulement global de l'installation. Les mises à jour effectuées ici mettent automatiquement à jour l'ensemble des sites et des licences sur votre Secure Remote Access Appliance.

Si vous installez une mise à jour du logiciel, les utilisateurs connectés perdent momentanément la connexion à toute session d'accès et à la console d'accès. Il convient donc de lancer les mises à jour pendant les périodes calmes. Toutefois, lorsque le package de mise à jour contient uniquement des licences supplémentaires, il est possible d'installer la mise à jour sans interrompre la connexion des utilisateurs.

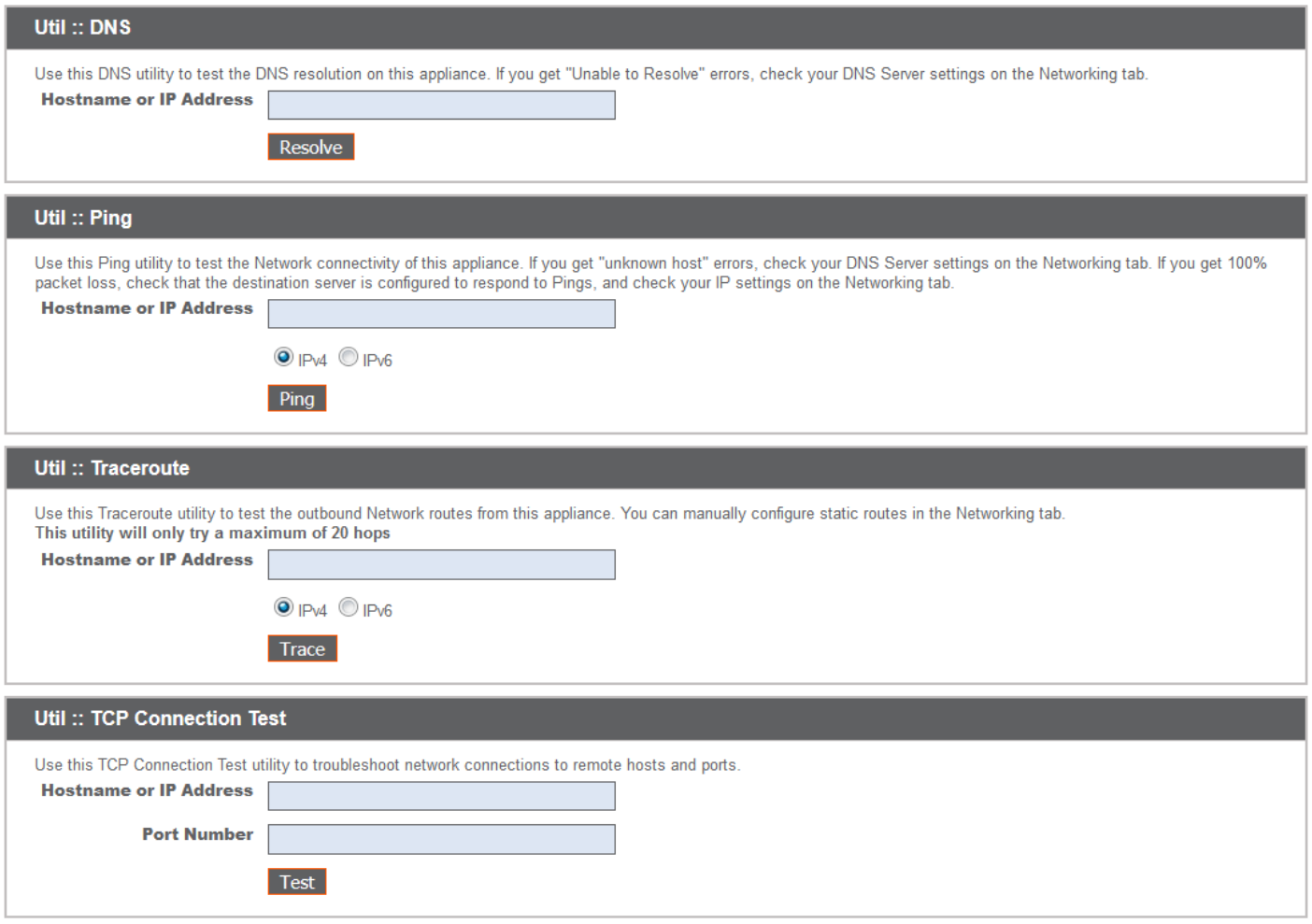
Pour obtenir les informations relatives aux dernières mises à jour BeyondTrust, consultez www.beyondtrust.com/support/changelog.



Assistance technique

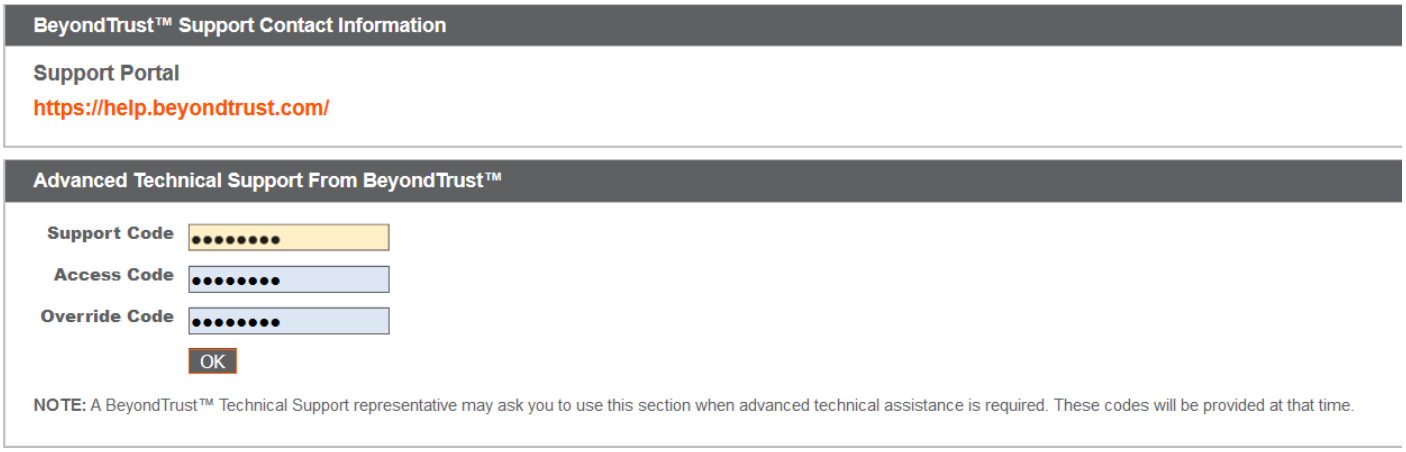
Outils : Corriger les problèmes réseau

La section **Outils** peut être utilisée pour corriger les problèmes de réseau. Lorsqu'il est impossible d'établir une connexion, ces outils peuvent vous permettre d'en comprendre la raison. Testez le serveur DNS pour vérifier que le nom d'hôte ou l'adresse IP interprète correctement. Effectuez un ping vers votre Secure Remote Access Appliance pour tester sa connectivité de réseau. Utilisez traceroute pour voir le chemin emprunté par les paquets depuis le serveur vers le système externe. Vous pouvez aussi utiliser le test de connexion TCP pour vérifier la connectivité d'un port spécifique sur une adresse IP ou un nom d'hôte cible.



Assistance technique avancée : Contacter l'Assistance technique BeyondTrust

La section **Assistance technique avancée** vous fournit des informations de contact pour votre équipe d'Assistance technique BeyondTrust et permet la création d'un tunnel d'assistance technique lancé par le serveur vers l'Assistance technique BeyondTrust afin de résoudre rapidement des problèmes complexes.



Si la section **Une session d'assistance technique avec BeyondTrust Corporation en cours** est visible, l'Assistance technique BeyondTrust dispose d'une session active dans votre Secure Remote Access Appliance. La colonne **Durée** indique la durée de la session d'Assistance technique BeyondTrust sur votre serveur. Pour mettre fin à la session, cliquez sur **Terminer**, et le tunnel entre votre serveur et l'Assistance technique BeyondTrust sera fermé.