Secure Remote Access
B Series Appliance Interface 6.2
(/appliance)

©2003-2022 BeyondTrust Corporation. 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.

TC:18/07/2022

Table of Contents

Vue d'ensemble du BeyondTrust Appliance B Series **4**
Anatomie du BeyondTrust Appliance B Series 5
Administration B Series Appliance 5
Administration utilisateurs 5
Utilisation de ce guide 6
Interface Web du BeyondTrust Appliance B Series **7**
Se connecter à l'interface d'administration de B Series Appliance **8**
État **9**
Bases : Afficher les détails de la B Series Appliance 9
Santé : Consulter la santé du serveur virtuel RS **10**
Utilisateurs **11**
Modifiez le mot de passe et l'utilisateur, ajoutez un utilisateur 11
SAML : Mettre en place une authentification via un fournisseur d'identité SAML **12**
Réseau **13**
Configuration de l'IP : Configuration de l'adresse IP et des paramètres du réseau 13
Routes statiques : Définir des routes statiques pour établir une communication entre réseaux **17**
SNMP : Activer le protocole simple de gestion réseau **18**
Stockage **20**
État : Espace disque et état des disques durs 20
Spécifique à la BeyondTrust B Series Appliance B300 20
Spécifique à la BeyondTrust B Series Appliance B400 20
Notification de panne matérielle (B300 et B400 uniquement) 20
Chiffrement : Chiffrer les données de session **22**
Sécurité **23**
Certificats : Création et gestion des certificats SSL 23
Installation de certificat 23
Certificats 25
Demandes de certificat 27
Configuration TLS : Choisir les suites cryptographiques et les versions TLS **29**
Administration du serveur : Restrictions relatives aux comptes, réseaux et ports, **30**

©2003-2022 BeyondTrust Corporation. 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.

configuration de Syslog, activation de l'accord de connexion, et réinitialisation des comptes administrateur .....

Configuration e-mail : Configurer la B Series Appliance pour envoyer des alertes par e-mail **32**

Configurer via SMTP 32

Configurer via OAuth2 pour Microsoft Azure AD 33

Configurer via OAuth2 pour Google 36

Magasin de secrets : Magasin et accès aux secrets **41**

Mises à jour : Rechercher les mises à jour disponibles et installer le logiciel **43**

Assistance technique **45**

Outils : Corriger les problèmes réseau 45

Assistance technique avancée : Contacter l'BeyondTrust Technical Support **47**

Comparaison entre BeyondTrust Appliance B Seriess **48**

©2003-2022 BeyondTrust Corporation. 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.

Vue d’ensemble du BeyondTrust Appliance B Series

BeyondTrust a été le premier à introduire une approche utilisant la B Series Appliance pour l’assistance technique à distance. Notre modèle de déploiement déposé, le BeyondTrust Appliance B Series, est une option très sûre pour la mise en place de services d’assistance technique à distance.

Le BeyondTrust Appliance B Series, qu’il soit physique ou virtuel, se trouve dans vos locaux ou votre data center, protégé par vos mesures de sécurité. Ce modèle de déploiement vous offre un meilleur contrôle de la sécurité et une méthode sûre d’intégration de l’assistance technique à distance avec la gestion des identités. L’export de données et de vidéos de reporting dans le cadre d’un test d’audit en vraie grandeur en est grandement facilité.

©2003-2022 BeyondTrust Corporation. 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.

Anatomie du BeyondTrust Appliance B Series

Le BeyondTrust Appliance B Series utilise deux interfaces Web d'administration, **/appliance** et **/login**, pour isoler l'administration matérielle de la gestion des utilisateurs.

Représenté : Le serveur B400 BeyondTrust B Series Appliance

Administration B Series Appliance

Interface Web **/appliance**
Applications :

- Installer et configurer le matériel
- Mise à niveau du logiciel BeyondTrust

Ressource
Le guide d'administration du B Series Appliance

Administration utilisateurs

L'interface Web **/login**
Applications :

- Gestion des utilisateurs et des flux
- Rapport d'activité d'assistance technique
- Création et utilisation d'intégrations

Ressource
Le guide d'administration BeyondTrust

©2003-2022 BeyondTrust Corporation. 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.

Utilisation de ce guide

Pour des raisons de sécurité, BeyondTrust a séparé l'administration du B Series Appliance de l'administration des utilisateurs.

Cette documentation s'intéresse exclusivement à l'administration du BeyondTrust Appliance B Series. Les informations concernant l'administration des utilisateurs (l'interface Web /login) se trouvent dans l'Interface d'administration BeyondTrust.

©2003-2022 BeyondTrust Corporation. 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.

Interface Web du BeyondTrust Appliance B Series

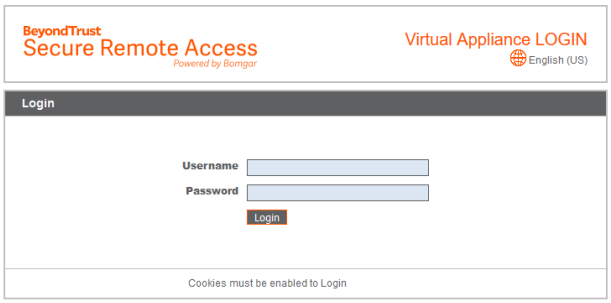
Ce guide vous aidera à administrer votre BeyondTrust Appliance B Series par l'intermédiaire de son interface Web **/appliance**. La B Series Appliance sert de point d'administration et de gestion central de vos sites BeyondTrust.

Utilisez ce guide uniquement après que l'administrateur a procédé à l'installation et à la configuration initiales de la B Series Appliance, qui sont expliquées dans le Guide d'installation matérielle de la BeyondTrust Appliance B Series 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 BeyondTrust à l'adresse www.beyondtrust.com/support.

©2003-2022 BeyondTrust Corporation. 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.

Se connecter à l'interface d'administration de B Series Appliance

Une fois l'B Series Appliance installée, connectez-vous à l'interface d'administration en allant à l'URL publique de votre B Series Appliance suivie de **/appliance** (par exemple : http://support.example.com/appliance).



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

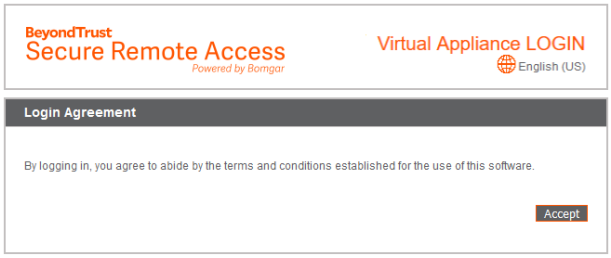
Mot de passe par défaut : **password**

Lors de votre première connexion, vous serez invité à modifier le mot de passe d'administration.[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 : Restrictions relatives aux comptes, réseaux et ports, configuration de Syslog, activation de l'accord de connexion, et réinitialisation des comptes administrateur », page 30.*

> ***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.*

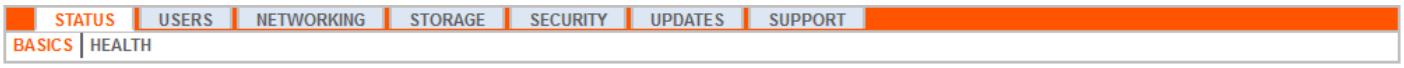


[1] Le mot de passe doit comporter huit caractères minimum et inclure au moins une lettre majuscule, une lettre minuscule, un chiffre et un caractère spécial.

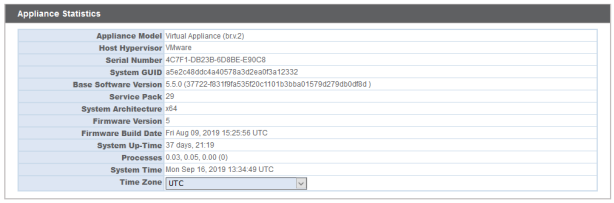
©2003-2022 BeyondTrust Corporation. Tous droits réservés. Les autres marques déposées identifiées sur cette page sont la propriété de leurs propriétaires respectifs. BeyondTrust n'est pas une banque à charte, une société de fiducie ou une institution de dépôt. Elle n'est pas autorisée à accepter des dépôts ou des comptes en fiducie et n'est ni sous licence ni gouvernée par une autorité bancaire nationale ou fédérale.

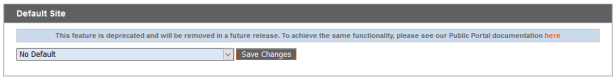
État

Bases : Afficher les détails de la B Series Appliance



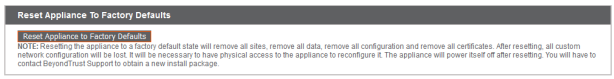
La page **Bases** affiche des informations sur votre BeyondTrust Appliance B Series et vous permet de contrôler votre système. Vous pouvez également y indiquer l'heure locale de votre système en concordance avec n'importe quel fuseau horaire. L'heure du système est affichée par défaut par rapport à l'échelle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





Dans la plupart des cas, il n'est pas nécessaire de changer ce paramètre. BeyondTrust déconseille l'utilisation de plusieurs sites sur une seule B Series Appliance. 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 BeyondTrust Appliance B Series. Bien qu'il ne soit pas nécessaire de redémarrer votre B Series Appliance, 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 à la B Series Appliance pour réaliser le redémarrage.



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

©2003-2022 BeyondTrust Corporation. 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.

Santé : Consulter la santé du serveur virtuel RS

STATUS | USERS | NETWORKING | STORAGE | SECURITY | UPDATES | SUPPORT
BASICS | HEALTH

> ***Remarque :*** *l'onglet **Santé** n'est visible que pour les sites pris en charge par un serveur virtuel RS ou la Cloud Appliance.*

La page **Santé** sert à contrôler l'état de votre Cloud Appliance ou virtuelle. 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 B Series Appliance.

Hardware Health

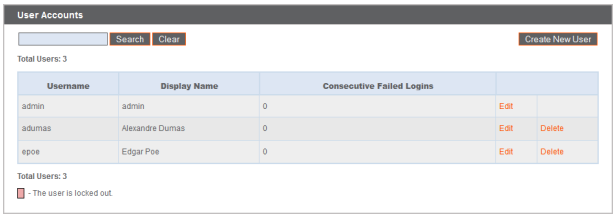
	Value	Status	Notes
CPU	Count: 8 Model: Intel(R) Xeon(R) CPU E5-2697 v3 @ 2.60GHz Speed: 2593.993 MHz Reservation: 0 MHz Limit: Unlimited		• Consider allocating a CPU Reservation to this VM of at least 500 MHz to help maintain functionality when the host's CPUs are under contention.
Memory	Physical: 16051 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		

©2003-2022 BeyondTrust Corporation. 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.

Utilisateurs

Modifiez le mot de passe et l'utilisateur, ajoutez un utilisateur

Vous pouvez ajouter, modifier ou supprimer des administrateurs 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.



> *Consultez « Administration du serveur : Restrictions relatives aux comptes, réseaux et ports, configuration de Syslog, activation de l'accord de connexion, et réinitialisation des comptes administrateur », page 30 pour définir les règles de restriction comme l'expiration et l'historique des mots de passe.*

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

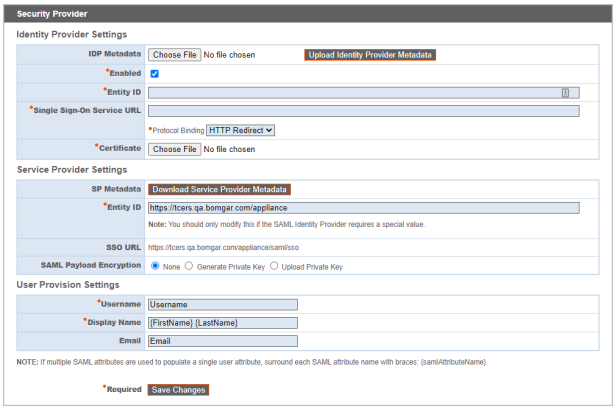
©2003-2022 BeyondTrust Corporation. Tous droits réservés. Les autres marques déposées identifiées sur cette page sont la propriété de leurs propriétaires respectifs. BeyondTrust n'est pas une banque à charte, une société de fiducie ou une institution de dépôt. Elle n'est pas autorisée à accepter des dépôts ou des comptes en fiducie et n'est ni sous licence ni gouvernée par une autorité bancaire nationale ou fédérale.

SAML : Mettre en place une authentification via un fournisseur d'identité SAML

STATUS | USERS | NETWORKING | STORAGE | SECURITY | UPDATES | SUPPORT
USERS | SAML

Configurez votre B Series Appliance pour permettre aux utilisateurs de s'authentifier via l'interface /appliance au moyen de SAML.

> ***Remarque :*** *pour utiliser l'authentification SAML, vous devez disposer d'un fournisseur d'identité tel que : Okta, OneLogin, Azure AD, or ADFS.*



Pour configurer la connexion, commencez par la section **Paramètres du fournisseur de service**. Si votre fournisseur d'identité (IDP) vous permet de transmettre des métadonnées depuis le fournisseur de service (SP), cliquez alors sur **Télécharger les métadonnées du fournisseur de service**. Cela vous donne un fichier XML que vous pouvez transmettre à votre IDP lors de la création de la demande. Vous pouvez aussi copier et coller l'**ID d'entité** et l'**URL du SSO** dans votre IDP.

> ***Astuce:*** *l'**ID d'entité** peut s'appeler **URI d'audience** dans votre fournisseur d'identité.*

Par défaut, le **Chiffrement de la charge utile SAML** est désactivé, mais vous pouvez générer ou transmettre une clé privée pour l'activer. Pour que la B Series Appliance génère une clé privée et un certificat, sélectionnez **Générer une clé privée** et cliquez sur **Enregistrer les modifications**. Puis cliquez sur **Télécharger le certificat du fournisseur de service (SP)** et transmettez le certificat généré à votre fournisseur d'identité. Pour fournir la clé privée et le certificat vous-même, sélectionnez **Transférer une clé privée**, choisissez le fichier de certificat et saisissez son mot de passe, si nécessaire. Vous devez transférer le même fichier de certificat à votre fournisseur d'identité.

Après avoir enregistré l'application dans votre fournisseur d'identité, vous pouvez avoir la possibilité de télécharger ses métadonnées. Si tel est le cas, transférez ce fichier sur votre B Series Appliance à l'aide du bouton **Transférer des métadonnées de fournisseur d'identité**. Vous pouvez aussi copier et coller l'**ID d'entité** et l'**URL de service d'authentification unique** dans votre B Series Appliance, dans la section **Paramètres du fournisseur d'identité**.

> ***Astuce:*** *l'**ID d'entité** peut s'appeler **Émetteur du fournisseur d'identité** ou **URL d'émetteur**, et l'**URL de service d'authentification unique** peut s'appeler **Point de terminaison SAML 2.0**.*

Liaison de protocole détermine si une requête HTTP POST a lieu ou si l'utilisateur est redirigé vers l'URL d'authentification unique. Gardez ce réglage sur **Redirection HTTP** sauf instruction contraire de votre fournisseur d'identité. Vous devez aussi fournir le **certificat** IDP que vous pouvez télécharger depuis l'IDP.

Sous **Paramètres d'approvisionnement de l'utilisateur**, mappez **Nom d'utilisateur**, **Nom affiché** et **E-mail** avec les attributs correspondants dans votre fournisseur d'identité.

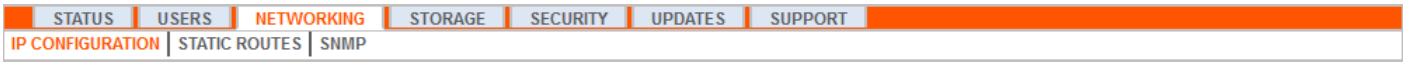
Cliquez sur **Enregistrer les modifications** pour enregistrer la configuration SAML.

Maintenant, sur la page de connexion /appliance, les utilisateurs verront un lien vers **Utiliser l'authentification SAML** sous le bouton **Connexion**. Les utilisateurs qui ont été affectés à l'application créée dans votre IDP peuvent cliquer sur ce lien pour se connecter. S'ils ne sont pas déjà connectés à l'IDP, ils seront redirigés vers l'IDP pour se connecter avant d'être redirigés vers /appliance.

©2003-2022 BeyondTrust Corporation. 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.

Réseau

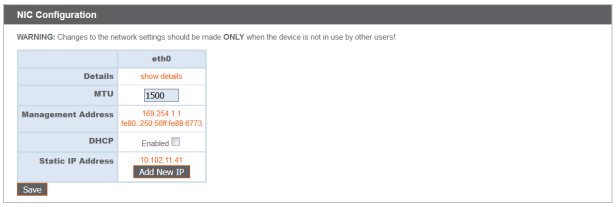
Configuration de l'IP : Configuration de l'adresse IP et des paramètres du réseau



Les entreprises dotées de configurations de réseau complexes peuvent configurer plusieurs adresses IP sur les ports Ethernet de la B Series Appliance. L'utilisation de plusieurs ports permet d'accroître la sécurité ou d'autoriser des connexions suivant des réseaux non-standards. 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.

L'association NIC regroupe les contrôleurs réseau physiques (NIC) de votre système dans une interface logique unique. L'association NIC fonctionne en mode « Sauvegarde active ». Une des cartes d'interface réseau sert à transporter 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 Cloud Appliance ou virtuel, l'option* ***Activer le couplage NIC*** *n'est pas disponible.*



Bien que plusieurs adresses IP peuvent être attribuées à chaque NIC, ne configurez aucun NIC de sorte qu'il ait une adresse IP se trouvant sur le même sous-réseau en tant qu'adresse IP de l'autre NIC. Dans ce cas, il y a un risque de perte de paquets lorsque les paquets provenant de l'IP du NIC sans 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

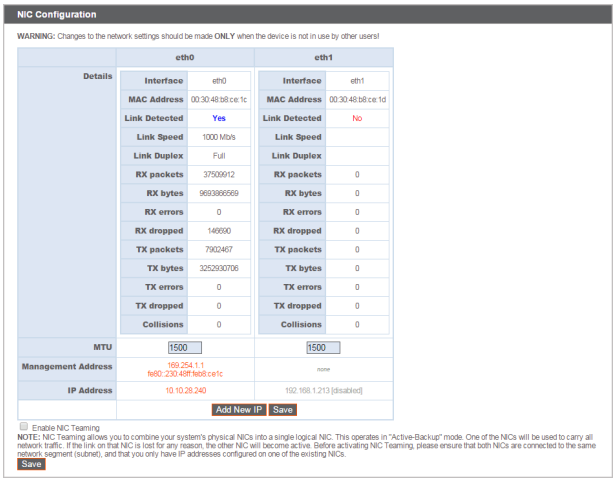
Avec cette configuration, le trafic des deux NIC est envoyé vers la passerelle par défaut (192.168.1.1), quelle que soit la NIC ayant reçu le trafic. Les commutateurs configurés avec des ARP dynamiques envoient des paquets aléatoirement à eth0 (192.168.1.5) ou à eth1 (192.168.1.10), mais pas aux deux. 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 B Series Appliance. 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.

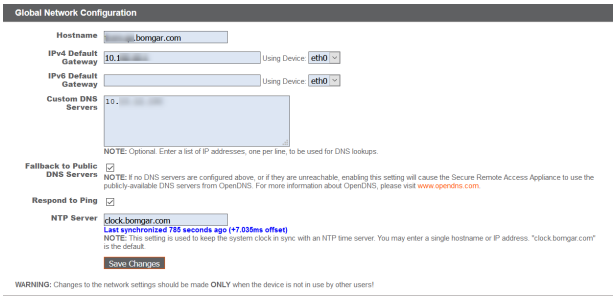
©2003-2022 BeyondTrust Corporation. Tous droits réservés. Les autres marques déposées identifiées sur cette page sont la propriété de leurs propriétaires respectifs. BeyondTrust n'est pas une banque à charte, une société de fiducie ou une institution de dépôt. Elle n'est pas autorisée à accepter des dépôts ou des comptes en fiducie et n'est ni sous licence ni gouvernée par une autorité bancaire nationale ou fédérale.

> ***Remarque :*** *pour en savoir plus sur DHCP, consultez Dynamic Host Configuration Protocol (DHCP) à l'adresse https://docs.microsoft.com/fr-fr/windows-server/networking/technologies/dhcp/dhcp-top.*

Cliquez sur **Afficher les informations** pour consulter et vérifier les statistiques de transmission et de réception pour chaque port Ethernet sur la B Series Appliance.



Dans la section **Configuration globale du réseau**, configurez le nom d'hôte pour votre BeyondTrust Appliance B Series.

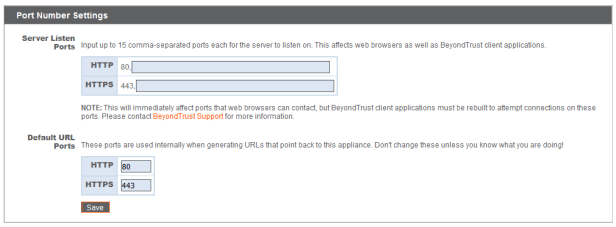


> ***Remarque :*** *le champ **Nom d'hôte** ne doit satisfaire aucune exigence technique. Cela n'affecte pas la connexion du nom d'hôte du logiciel client ou des utilisateurs distants. (Pour effectuer ces changements, consultez **/login > État > Informations > Logiciel client est paramétré pour tenter**. 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.) Le champ **Nom d'hôte** sert principalement à vous aider à faire la différence entre plusieurs B Series Appliances. 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 de la B Series Appliance.*

Assignez une passerelle par défaut, en sélectionnant le port Ethernet à utiliser. Saisissez une adresse IP pour un ou plusieurs serveurs 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 **Utiliser des serveurs OpenDNS de récupération** permet au B Series Appliance d'utiliser des serveurs DNS publics disponibles sur OpenDNS. Pour plus d'information à propos d'OpenDNS, rendez-vous sur www.opendns.com

©2003-2022 BeyondTrust Corporation. 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.

Autorisez votre B Series Appliance à répondre à des commandes ping afin de tester le fonctionnement de l'hôte. 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 B Series Appliance.

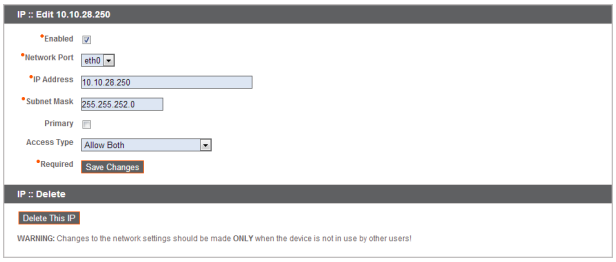


Deux options sont disponibles dans la **Configuration du numéro de port** : **Ports détectés par le serveur** et **Ports URL par défaut**. Lors de la configuration, n'oubliez pas que les connexions à des ports valables sont susceptibles d'être rejetées en raison des restrictions liées au réseau définies dans **/appliance > Sécurité > Administration de l'appliance** 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 la B Series Appliance. 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. La B Series Appliance répond aux connexions HTTP associées aux ports répertoriés dans le champ HTTP, et la B Series Appliance répond aux connexions HTTPS associées aux ports du champ HTTPS. Il est impossible de modifier les ports d'écoute intégrés (80 et 443).

Pour accéder à la B Series Appliance sur un port donné avec un navigateur, vous devez indiquer le port dans l'URL (par exemple : support.example.com:8200). Les clients téléchargés depuis la B Series Appliance 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 B Series Appliance. 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 la B Series Appliance, comme une clé de session générée par la console du technicien d'assistance. 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 que vous saisissez 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 B Series Appliance 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 cette B Series Appliance, vous pouvez la définir en tant qu'adresse **Principale**. Lorsque cette case est cochée, la B Series Appliance 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 de la B Series Appliance 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 de l'appliance****.*

©2003-2022 BeyondTrust Corporation. 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.

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

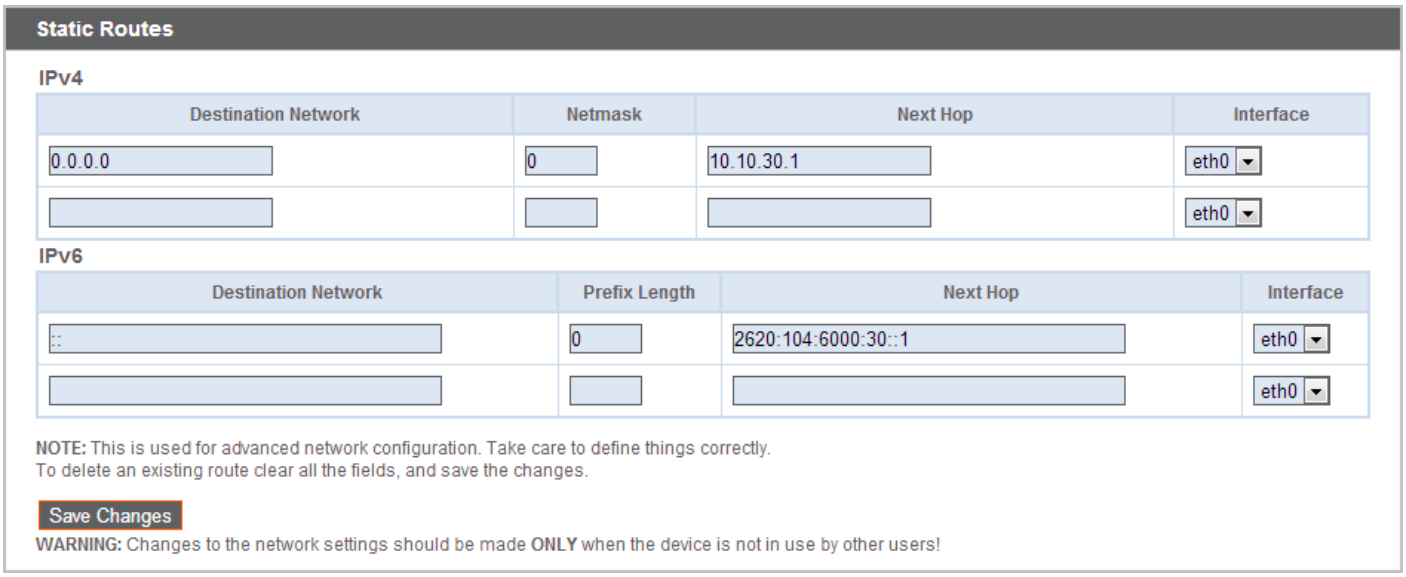
[1]Ne pas supprimer ou modifier l'adresse IP de gestion.

©2003-2022 BeyondTrust Corporation. 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.

Routes statiques : Définir 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 de la B Series Appliance, à un ordinateur sur l'autre réseau, pour peu que la B Series Appliance se trouve à un endroit où les deux réseaux sont en mesure de communiquer individuellement avec cette dernière.

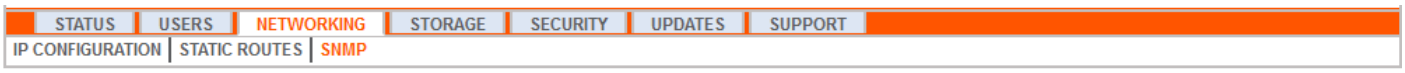
L'installation de routes statiques devrait être réservée aux administrateurs avancés.



Remarque : *des routes statiques peuvent également être créées dans la console. Pour plus d'informations, veuillez consulter Configuration de la console Secure Remote Access à l'adresse https://www.beyondtrust.com/docs/remote-support/getting-started/deployment/hardware-sra/console.htm.*

©2003-2022 BeyondTrust Corporation. 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.

SNMP : Activer le protocole simple de gestion réseau



Le BeyondTrust Appliance B Series prend en charge la surveillance SNMP[1] pour les statistiques relatives au réseau, aux disques durs, à la mémoire et au processeur. 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 la B Series Appliance à des fins de contrôle.

Pour activer le SNMP pour cette B Series Appliance, cochez **Activer SNMPv2** ou **Activer SNMPv3**. Cela permet à un serveur SNMPv2 ou v3 de répondre aux requêtes SNMP. Saisissez une valeur pour le **Nom de communauté en lecture seule**, l'**Emplacement du système** et les **Restrictions d'IP** (pour les adresses IP autorisées à interroger cette B Series Appliance à l'aide du SNMP). Si aucune adresse IP n'est indiquée, tous les hôtes ont un droit d'accès.

En cas de sélection de SNMPv3 :

1. Veuillez indiquer un **nom d'utilisateur** et un **mot de passe**.
2. Sélectionnez la **méthode d'authentification** de votre choix dans le menu déroulant.
3. Cochez **Activer la confidentialité SNMPv3** si vous souhaitez chiffrer les communications avec le client.
4. Saisissez un **mot de passe de confidentialité** et choisissez une **méthode de confidentialité**.

Cliquez sur **Enregistrer les modifications** pour terminer.

[1] Le protocole SNMP (Simple Network Management Protocol) est un protocole Internet standard utilisé pour la surveillance et la gestion des équipements en réseau (voir Simple Network Management Protocol).

©2003-2022 BeyondTrust Corporation. 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.

Networking :: SNMP Configuration

Enable SNMPv2 ☐
Enable the SNMPv2 server on this appliance.

***SNMPv2 Read-Only Community Name**

Enable SNMPv3 ☐
Enable the SNMPv3 server on this appliance.

***SNMPv3 Username**

***SNMPv3 Authentication Password**
NOTE: Leave blank to keep the current password.

***SNMPv3 Authentication Method** SHA-256

SNMPv3 Enable Privacy ☐
Enable SNMPv3 privacy, which encrpyts communication to the client.

***SNMPv3 Privacy Password**
NOTE: Leave blank to keep the current password.

***SNMPv3 Privacy Method** AES

***System Location** testlocation

IP Restrictions

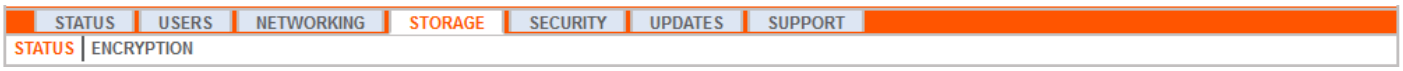
Enter IP addresses that should be allowed to access SNMP on this appliance. Enter the IP Addresses, one entry per line, in the form "IP_Address/Prefix_Length". The Prefix Length should be an integer. If no entries are provided, all hosts will be granted access.

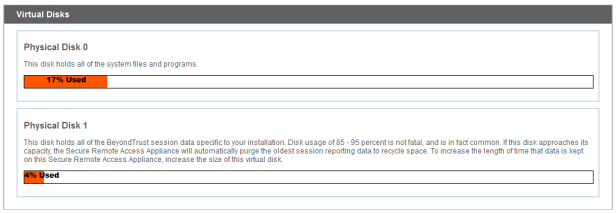
***Required** Save Changes

©2003-2022 BeyondTrust Corporation. 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.

Stockage

État : Espace disque et état des disques durs





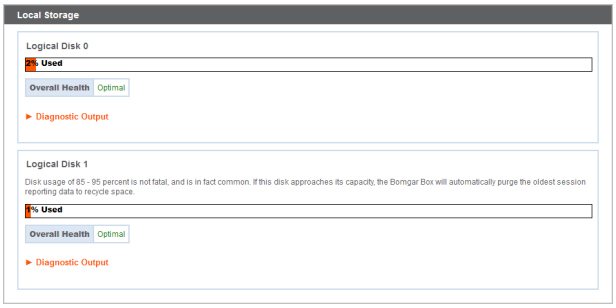
La page **État** affiche le pourcentage de l'espace sur le disque dur utilisé de votre B Series Appliance.

Si vous activez toutes les fonctions d'enregistrement sur vos sites d'accès (enregistrements de session et de l'interpréteur de commandes distant) ou si le nombre de vos sessions est important, il est normal de constater un taux d'utilisation élevé du disque dur. Notez bien qu'un taux d'utilisation de 85 à 95 % n'est PAS un motif d'inquiétude. Si le disque dur n'a pas beaucoup d'espace disque, la B Series Appliance est configurée pour purger automatiquement les données de l'ancienne session et recycler l'espace disque pour les nouvelles données de session.

Spécifique à la BeyondTrust B Series Appliance B300

Le B300 utilise une architecture RAID (structure redondante de disques indépendants) pour sauvegarder vos données. RAID 6 permet à la B Series Appliance 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, la B Series Appliance recrée automatiquement le RAID à l'aide du nouveau disque. Il n'est pas nécessaire d'éteindre la B Series Appliance lors du remplacement d'un disque.

Spécifique à la BeyondTrust B Series Appliance B400



Le B400 dispose de deux jeux de disques RAID (structure redondante de disques indépendants) logiques. 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 panne matérielle (B300 et B400 uniquement)

©2003-2022 BeyondTrust Corporation. 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.

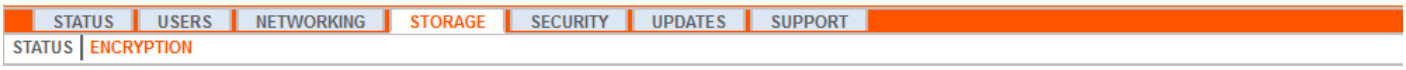
Les témoins LED de votre B Series Appliance renseignent également sur l'état de vos disques durs. Normalement, les LED clignotent lorsque les disques sont en activité. Si un lecteur tombe en panne, son affichage LED devient rouge et une alarme sonore vous avertit de la panne. Pour désactiver l'alarme avant que le système ne soit rétabli, cliquez sur le bouton **Arrêter l'alarme** sur l'interface Web.

Remarque : *le bouton* ***Éteindre l'alarme*** *sera disponible qu'une alarme soit en train de retentir ou pas. 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 la B Series Appliance et que vous souhaitez éliminer la B Series Appliance en tant que source, cliquez sur le bouton* ***Arrêter l'alarme*** *plusieurs fois pour annuler les alarmes susceptibles d'être actives.*

©2003-2022 BeyondTrust Corporation. 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.

Chiffrement : Chiffrer les données de session

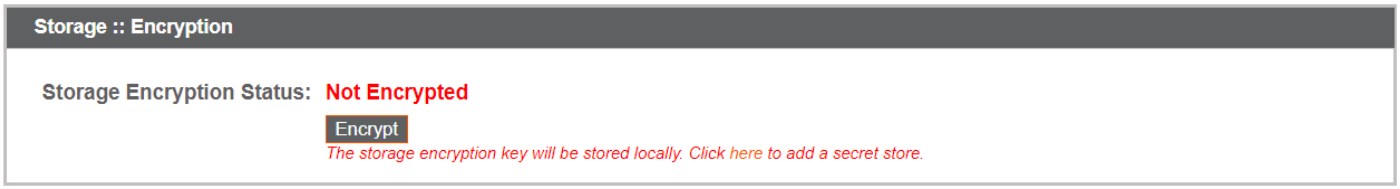


La section **Chiffrement** vous permet de chiffrer les données de session stockées dans votre BeyondTrust Appliance B Series. Lorsque vous chiffrez vos données pour la première fois, la quantité maximale de données à utiliser est de 4 Go. Après le premier chiffrement, la limite de 4 Go ne s'applique plus.

Si vous n'avez pas encore créé un magasin de secrets, allez dans **Sécurité > Magasin de secrets** pour en ajouter un.

Pour plus d'informations, veuillez visiter le magasin de secrets.

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



©2003-2022 BeyondTrust Corporation. 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.

Sécurité

Certificats : Création et gestion des certificats SSL

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

Installation de certificat

Le BeyondTrust Appliance B Series dispose d'un certificat auto-signé préinstallé. Cependant, pour utiliser efficacement votre BeyondTrust Appliance B Series, vous devrez aussi créer au minimum un certificat auto-signé, en demandant et en envoyant de préférence un certificat signé par une autorité de certificat.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.

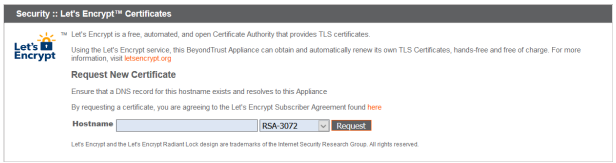
Let's Encrypt

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 la B Series Appliance.
- La B Series Appliance doit pouvoir contacter Let's Encrypt sur le port TCP 443.
- Let's Encrypt doit pouvoir contacter la B Series Appliance 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) de la B Series Appliance 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 :*** *La B Series Appliance 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, la B Series Appliance 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.*

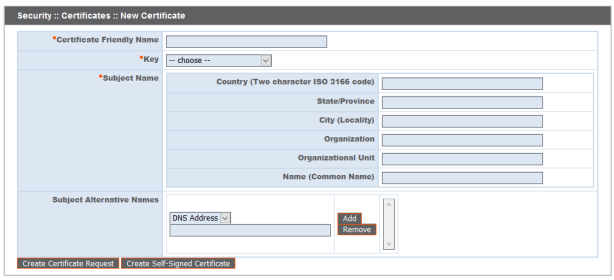
©2003-2022 BeyondTrust Corporation. Tous droits réservés. Les autres marques déposées identifiées sur cette page sont la propriété de leurs propriétaires respectifs. BeyondTrust n'est pas une banque à charte, une société de fiducie ou une institution de dépôt. Elle n'est pas autorisée à accepter des dépôts ou des comptes en fiducie et n'est ni sous licence ni gouvernée par une autorité bancaire nationale ou fédérale.

IMPORTANT !

Étant donné que le DNS ne peut s'appliquer qu'à une B Series Appliance à la fois, et comme une B Series Appliance 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 B Series Appliances en reprise en séquence.

Autres certificats remis par des AC

Pour créer un certificat auto-signé ou une demande de certificat auprès d'un autre émetteur, allez dans la section **Sécurité :: Autres certificats** et cliquez sur **Créer**. Dans **Nom convivial du certificat**, saisissez un nom pour identifier ce certificat. À partir du menu déroulant **Clé**, choisissez de créer une nouvelle clé ou sélectionnez une clé existante. Indiquez le reste des informations relatives à votre organisation.



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. Un nouveau nom convivial de certificat devrait être utilisé afin qu'il soit facile d'identifier 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****.*

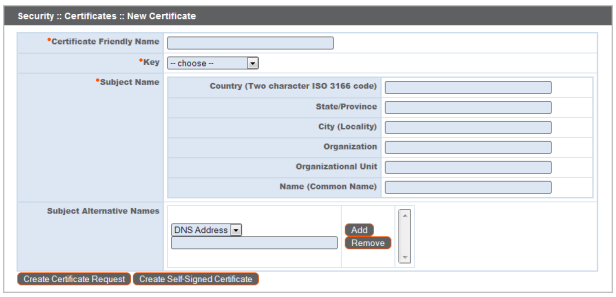
Pour obtenir un certificat de nouvelle clé ou de renouvellement de clé, la marche à suivre pour l'importation est identique.

Autres certificats remis par des AC

Pour créer une demande de certificat :

- Allez dans la section **Sécurité :: Autres certificats** et cliquez sur **Créer**.

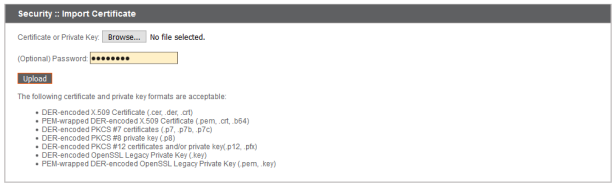
©2003-2022 BeyondTrust Corporation. Tous droits réservés. Les autres marques déposées identifiées sur cette page sont la propriété de leurs propriétaires respectifs. BeyondTrust n'est pas une banque à charte, une société de fiducie ou une institution de dépôt. Elle n'est pas autorisée à accepter des dépôts ou des comptes en fiducie et n'est ni sous licence ni gouvernée par une autorité bancaire nationale ou fédérale.



- 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, etc.*

Si vous comptez obtenir un certificat signé par une autorité de certificat, cliquez sur **Créer une demande de certificat** pour créer une demande de signature de certificat (DSC). Sinon, cliquez sur **Créer un certificat auto-signé**.



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 enverra un ou plusieurs fichiers de nouveau certificat à installer sur le B Series Appliance.

Pour envoyer des certificats ou des clés privées, cliquez sur **Importer**. Accédez au premier fichier et mettez-le en ligne. Répétez cette opération pour chaque certificat envoyé par votre AC. L'AC n'envoie souvent pas son certificat racine, qui doit être installé sur votre B Series 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 B Series Appliance, 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.

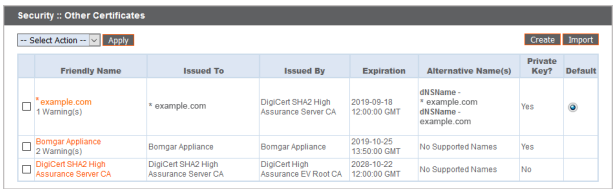
En général, la façon la plus simple de trouver le certificat racine adapté à votre certificat est d'ouvrir le fichier de certificat de votre machine locale et d'analyser son « Chemin de certification » ou sa « Hiérarchie de certification ». La racine de la hiérarchie ou du chemin se trouve en principe au sommet de l'arbre. Trouvez ce certificat racine dans le magasin de racines en ligne de votre AC. Téléchargez-le ensuite dans le magasin de certificats racine de l'AC et importez-le dans votre B Series Appliance, comme indiqué ci-dessus.

Si les certificats intermédiaires ou racines diffèrent de ceux en cours d'utilisation (ou si un certificat auto-signé était précédemment utilisé), veuillez demander une mise à jour à l'BeyondTrust Technical Support. L'BeyondTrust Technical Support vous demandera une copie du nouveau certificat, ainsi que de ses certificats intermédiaire et racine.

Certificats

©2003-2022 BeyondTrust Corporation. 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.

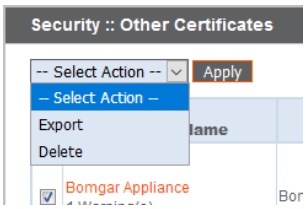
Consultez un tableau de certificats SSL disponibles sur votre B Series Appliance.



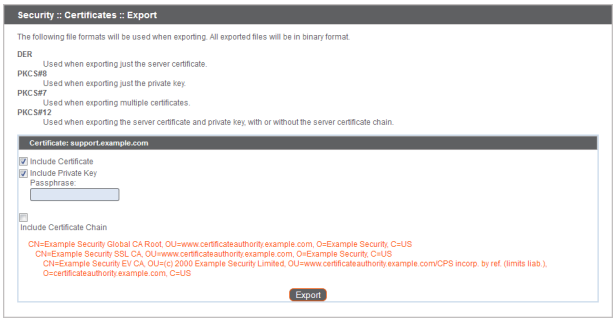
Pour les connexions incompatibles avec l'indication du nom de serveur (SNI) ou pour celles qui ne fournissent pas le bon SNI, sélectionnez un certificat SSL par défaut dans la liste pour prendre en charge ces connexions en cliquant sur le bouton sous la colonne **Défaut**. Le certificat SSL par défaut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

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

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**.

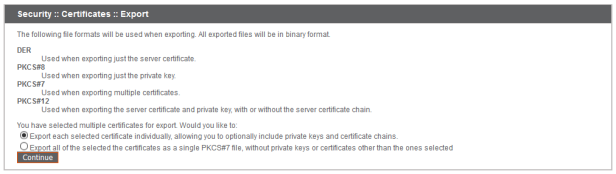


Si vous exportez uniquement un certificat, vous pouvez immédiatement choisir d'inclure le certificat, la clé privée (pouvant être sécurisée par une phrase secrète) et/ou la chaîne du certificat, selon la disponibilité de chaque élément. Cliquez sur **Exporter** pour lancer le téléchargement.



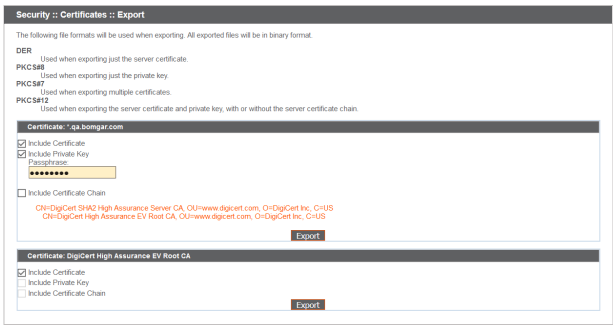
Si vous exportez plusieurs certificats, vous aurez le choix d'exporter chaque certificat individuellement ou un fichier PKCS#7 unique.

Si vous choisissez d'exporter plusieurs certificats dans un seul fichier, cliquez sur **Continuer** pour lancer le téléchargement. Grâce à cette option, seul le certificat réel sera exporté sans clé privée ou chaîne du certificat.



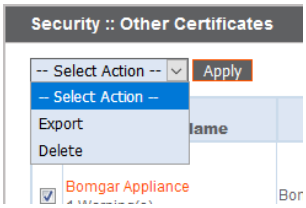
©2003-2022 BeyondTrust Corporation. Tous droits réservés. Les autres marques déposées identifiées sur cette page sont la propriété de leurs propriétaires respectifs. BeyondTrust n'est pas une banque à charte, une société de fiducie ou une institution de dépôt. Elle n'est pas autorisée à accepter des dépôts ou des comptes en fiducie et n'est ni sous licence ni gouvernée par une autorité bancaire nationale ou fédérale.

Pour inclure des clés privées et/ou des chaînes de certificats lors de l'exportation, sélectionnez l'exportation individuelle et cliquez sur **Continuer** pour consulter tous les certificats sélectionnés. Pour chaque liste, vous choisissez d'inclure le certificat, la clé privée (pouvant être sécurisée par une phrase secrète) et/ou la chaîne du certificat, selon la disponibilité de chaque élément. Cliquez sur **Exporter** pour lancer le téléchargement.



> ***Remarque :*** *une clé privée ne doit jamais, ou rarement, être exportée depuis une B Series Appliance. En cas de vol, une personne malveillante pourrait facilement compromettre le site BeyondTrust qui a généré la clé. Si vous devez tout de même exporter une clé, assurez-vous d'y associer un mot de passe fort.*

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**.

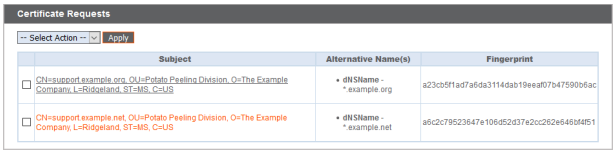


> ***Remarque :*** *en principe, un certificat ne doit jamais être supprimé à moins qu'il n'ait été remplacé par un remplaçant fonctionnel.*

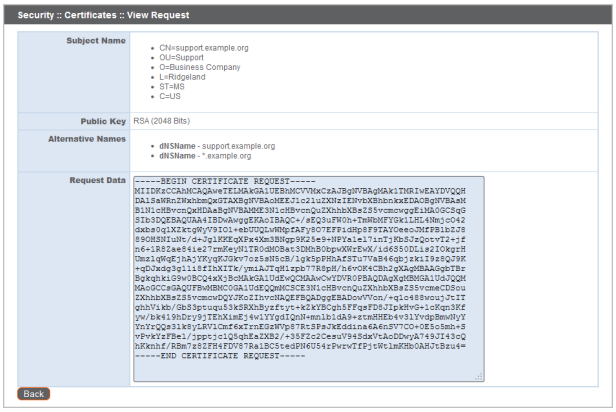
Pour confirmer l'exactitude, examinez les certificats que vous souhaitez supprimer, puis cliquez sur **Supprimer**.

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.



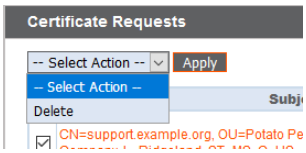
La consultation des détails vous fournit également les données sur la demande que vous transmettrez à votre autorité de certificat préférée lors de la demande de certificat signé.



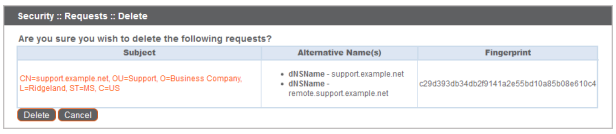
> ***Remarque :*** *si vous renouvelez un certificat, utilisez le même certificat Demande de données utilisé pour le certificat d'origine.*

©2003-2022 BeyondTrust Corporation. 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.

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**.



©2003-2022 BeyondTrust Corporation. 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.

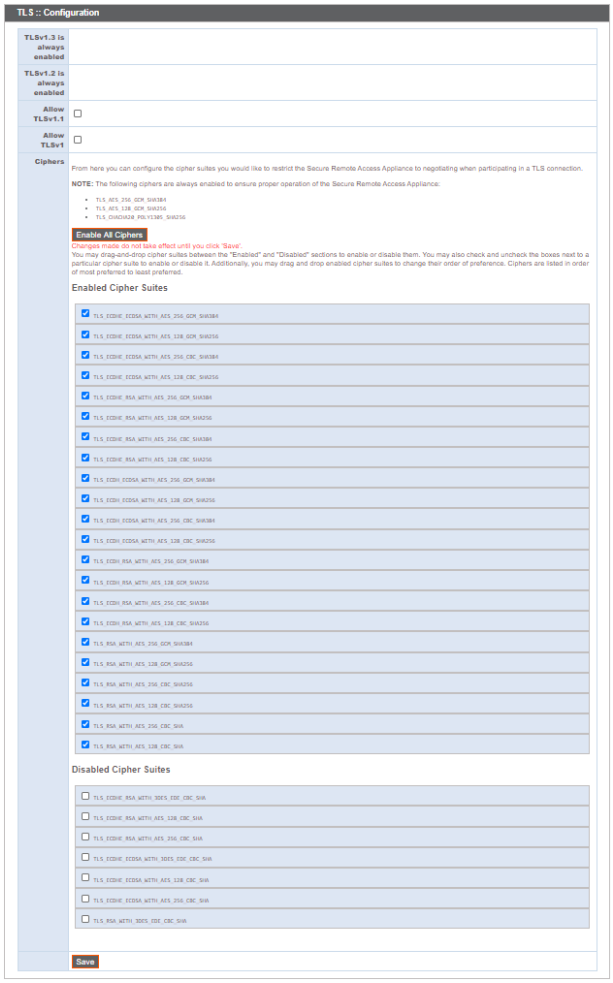
Configuration TLS : Choisir les suites cryptographiques et les versions TLS

Choisissez si TLSv1.3, TLSv1.1 TLSv1 et/ou SSLv3 doivent être activés ou désactivés. Pour une sécurité optimale, l'interface Web BeyondTrust est toujours définie par défaut sur TLSv1.2 avant de passer à TLSv1.1, TLS1.0 ou SSLv3.

Cependant, certains navigateurs plus anciens peuvent ne pas prendre en charge TLSv1.2. Si vous désactivez un ou plusieurs anciens protocoles de sécurité et que vous comptez accéder à votre interface d'administration depuis un navigateur ancien incompatible avec les protocoles de sécurité que vous avez activés, BeyondTrust ne vous autorisera pas à vous connecter. L'activation de TLSv1.1, TLSv1.0 et SSLv3 vous permet de vous connecter à votre interface Web depuis n'importe quel ordinateur, quelle que soit la version de navigateur utilisée.

Notez que ce réglage affecte principalement les connexions à l'interface Web de votre BeyondTrust Appliance B Series. 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.

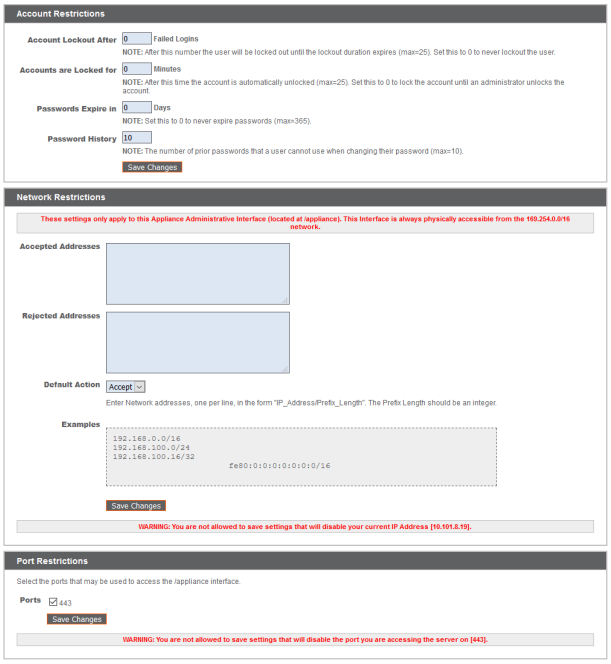
Sélectionnez quelles suites cryptographiques doivent être activées ou désactivées sur votre B Series Appliance. Déplacez les Suites cryptographiques pour modifier l'ordre de préférence. Notez que les changements apportés aux Suites cryptographiques ne prennent effet qu'en cliquant sur le bouton **Sauvegarder**.



©2003-2022 BeyondTrust Corporation. 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.

Administration du serveur : Restrictions relatives aux comptes, réseaux et ports, configuration de Syslog, activation de l'accord de connexion, et réinitialisation des comptes 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. ainsi que le nombre de jours pendant lequel un mot de passe peut être utilisé avant d'expirer, et limiter la réutilisation des anciens mots de passe.

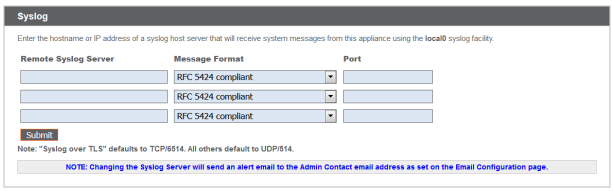


Vous pouvez restreindre l'accès à l'interface d'administration de votre B Series Appliance en indiquant les adresses réseau autorisées et en sélectionnant les ports par lesquels l'interface sera accessible.

Dans le champ **Adresses acceptées**, définissez les adresses IP ou les réseaux devant toujours avoir accès à /appliance. Dans le champ **Adresses refusées**, définissez les adresses IP et les réseaux ne devant en aucun cas avoir accès 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. En cas de conflit, c'est la correspondance la plus spécifique qui prévaut.

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 BeyondTrust Appliance B Series 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 B Series Appliance 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 cette B Series Appliance dans le champ **Serveur Syslog distant**. Sélectionnez le format de message 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. Les valeurs par défaut peuvent cependant être changées. Les journaux du BeyondTrust Appliance B Series sont envoyés au moyen du service **local0**.

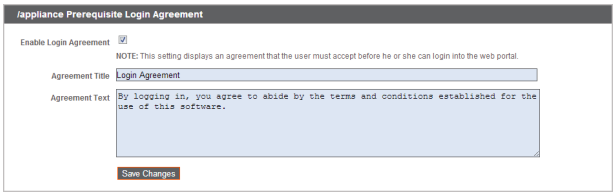
©2003-2022 BeyondTrust Corporation. Tous droits réservés. Les autres marques déposées identifiées sur cette page sont la propriété de leurs propriétaires respectifs. BeyondTrust n'est pas une banque à charte, une société de fiducie ou une institution de dépôt. Elle n'est pas autorisée à accepter des dépôts ou des comptes en fiducie et n'est ni sous licence ni gouvernée par une autorité bancaire nationale ou fédérale.

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

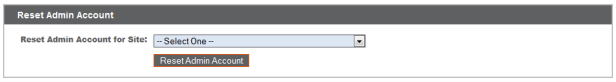
***Remarque :** lorsqu'un serveur syslog est ajouté ou modifié, une alerte est envoyée par e-mail à l'administrateur. Les informations de l'administrateur sont configurées dans la section **Sécurité > Configuration e-mail > Sécurité :: Contact administrateur**.*

Pour les références détaillées des messages syslog, consultez le Guide de référence sur les messages Syslog à l'adresse www.beyondtrust.com/docs/remote-support/how-to/integrations/syslog/index.

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 également utiliser l'option **Réinitialiser le compte administrateur**, afin de restaurer le nom d'utilisateur et le mot de passe administrateur d'un site en cas d'oubli ou de remplacement des informations d'authentification.



***Remarque :** Si vous réinitialisez le compte d'administrateur, toutes les autorisations de session existantes pour ce compte seront supprimées.*

©2003-2022 BeyondTrust Corporation. 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.

Configuration e-mail : Configurer la B Series Appliance pour envoyer des alertes par e-mail

STATUS | USERS | NETWORKING | STORAGE | SECURITY | UPDATES | SUPPORT
CERTIFICATES | TLS CONFIGURATION | APPLIANCE ADMINISTRATION | EMAIL CONFIGURATION | SECRET STORE

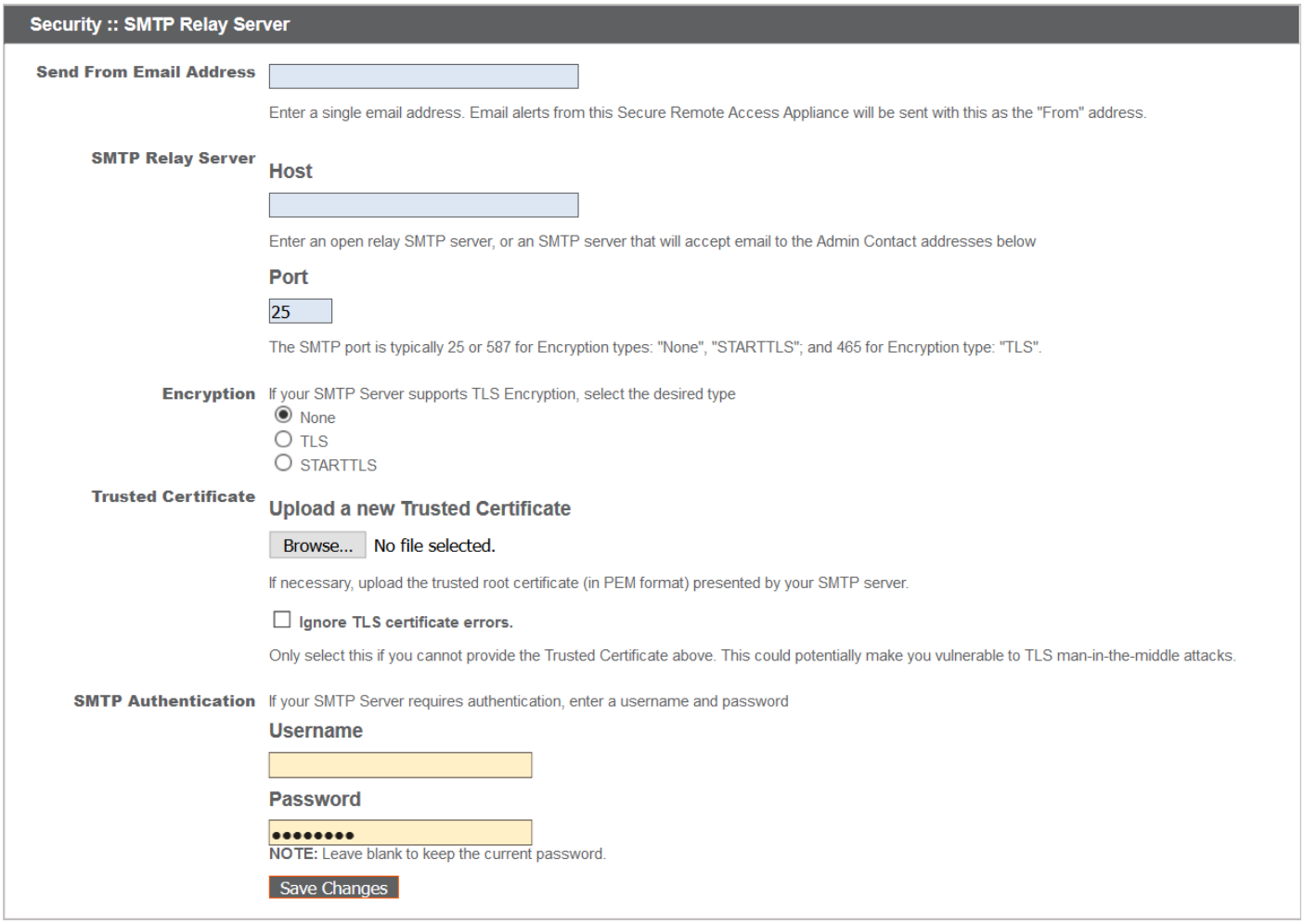
Votre B Series Appliance peut vous envoyer des notifications automatiques par e-mail. Un e-mail est envoyé dans les cas suivants :

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

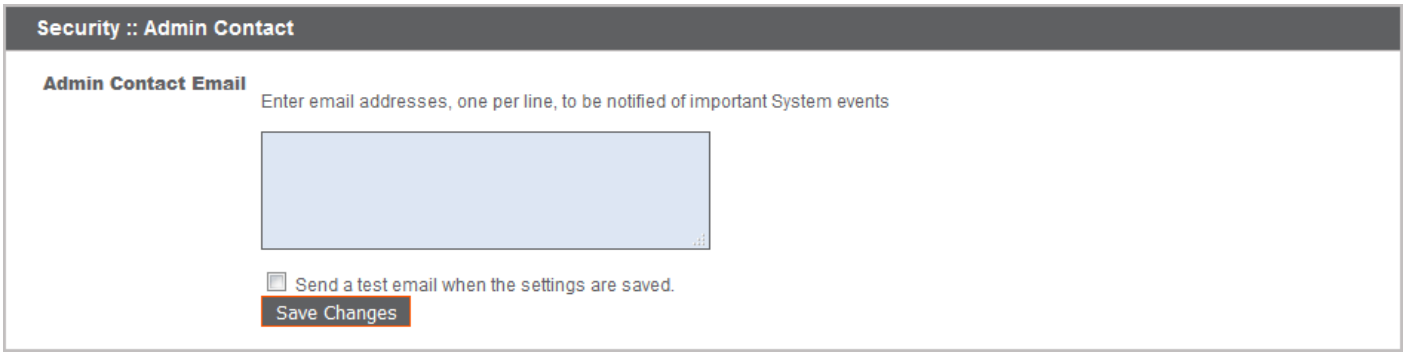
Configurer via SMTP

> ***Remarque :*** *cette méthode ne fonctionne pas pour certains services de messagerie. Veuillez vous reporter à* *« Configurer via OAuth2 pour Microsoft Azure AD », page 33* *ou* *« Configurer via OAuth2 pour Google », page 36* *afin d'avoir des configurations alternatives.*

©2003-2022 BeyondTrust Corporation. 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.



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.



Configurer via OAuth2 pour Microsoft Azure AD

La configuration nécessite la modification des paramètres de l'appliance BeyondTrust et de l'abonnement Microsoft 365 avec Azure AD.

©2003-2022 BeyondTrust Corporation. 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.

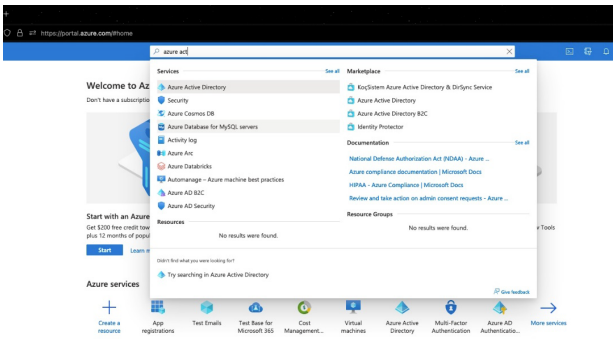
Commencez par modifier les paramètres de l'appliance BeyondTrust :

1. Allez dans **Appliance**, cliquez sur l'onglet **Sécurité** puis sur **Configuration e-mail**.
2. Basculez la **Méthode d'authentification** sur OAuth2.
3. Notez l'**URI de redirection d'autorisation**. Elle est requise plus tard.

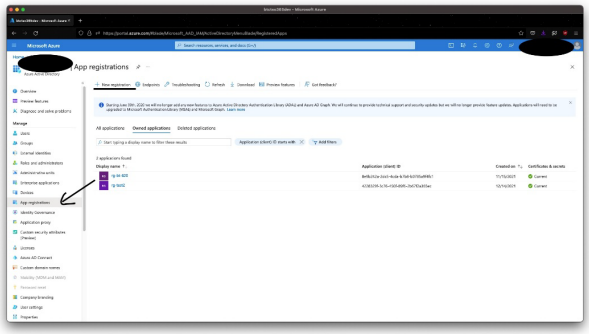
Avant de commencer la configuration sur Azure Active Directory, un administrateur Azure/Office 365 doit activer l'option « SMTP authentifié » pour chaque compte sur Exchange Online. Pour ce faire, allez sur le **Portail d'administration Office 365 (admin.microsoft.com) > Utilisateurs actifs > Courrier > Gérer les applications de courrier** et cochez **SMTP authentifié**.

Une fois que **SMTP authentifié** est activé, effectuez les étapes suivantes dans la console Azure :

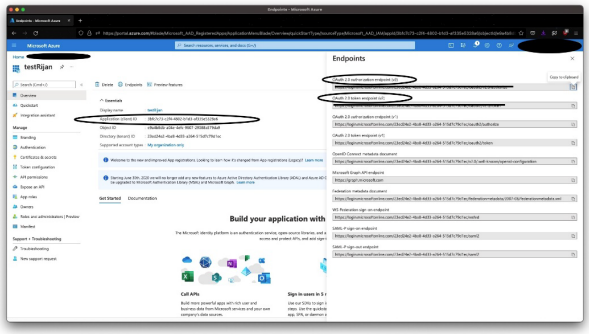
4. Connectez-vous à votre console Azure (portal.Azure.com).
5. Allez dans **Azure Active Directory**.



6. Allez dans **Inscriptions des applications** et sélectionnez **Nouvelle inscription**.
7. Saisissez un nom, tel qu'Appliance-OAuth2.
8. Sélectionnez les types de comptes de votre choix qui pourront se connecter à l'application via OAuth2. Sélectionnez **Client unique** pour interne uniquement.
9. Saisissez l'**URI de redirection**. C'est l'**URI de redirection d'autorisation** obtenue depuis l'appliance BeyondTrust au début de ce processus.
10. Cliquez sur **Inscription**.

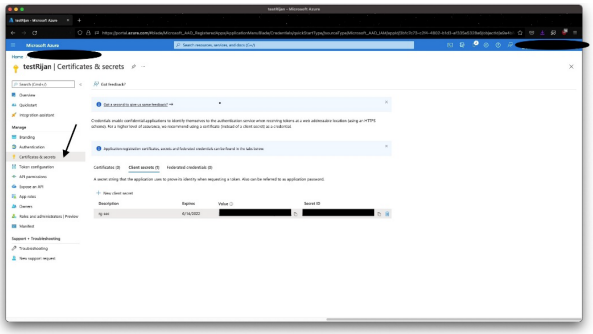


11. Sur la **page Vue d'ensemble** (sélectionnée depuis le menu de gauche), notez l'**ID d'application (client)**. Elle est requise plus tard.
12. Cliquez sur **Points de terminaison** (au-dessus de l'**ID d'application (client)**).
13. Notez l'URI du **point de terminaison d'autorisation OAuth 2.0 (v2)** et l'URI du **point de terminaison de jeton OAuth (v2)**. Elles seront requises plus tard.



©2003-2022 BeyondTrust Corporation. 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.

14. Sur la page **certificats et secrets** (sélectionnée depuis le menu de gauche), notez le **secret de client**. Elle est requise plus tard. Si vous n'avez pas un **secret de client**, cliquez sur **Nouveau secret de client** pour en créer un.



Les étapes restantes sont effectuées sur l'appliance BeyondTrust.

15. Allez dans **Appliance**, cliquez sur l'onglet **Sécurité** puis sur **Configuration e-mail**.
16. Saisissez les informations suivantes notées précédemment :
    - **Point de terminaison d'autorisation**
    - **Point de terminaison du jeton**
    - **ID client**
    - **Secret de client**
17. Saisissez l'adresse e-mail de ce service en tant que **Envoyer depuis l'adresse e-mail** et **E-mail d'utilisateur**.

> ***Remarque :*** *ces adresses doivent correspondre et être un compte valide pour Azure. Si l'option E-mail anonyme (Envoyer un e-mail en tant que n'importe qui) est activée pour le client Azure, vous pouvez ajouter n'importe quoi dans le champ d'envoi du message. À défaut, utilisez le nom d'utilisateur du propriétaire de l'application et les Utilisateurs autorisés.*

18. Saisissez les données pour les champs **Hôte**, **Chiffrement** et **Port**.
    - **Hôte** : smtp.office365.com
    - **Chiffrement** : STARTTLS
    - **Port** : 587

> ***Remarque :*** *les données par défaut pour Azure sont affichées, mais votre installation peut utiliser un autre hôte ou une autre méthode de chiffrement. Le port est applicable pour STARTTLS, mais d'autres méthodes de chiffrement peuvent utiliser un port différent.*

19. Saisissez votre certificat TLS si vous en avez un. Si ce n'est pas le cas, cochez **Ignorer les erreurs de certificat TLS**.
20. Saisissez ce qui suit pour **Scopes** : https://outlook.office.com/SMTP.Send offline_access
21. Cliquez sur **Enregistrer les modifications**.
22. Cliquez surk **Autoriser**. Sur la page de connexion qui s'affiche, acceptez la demande d'autorisation. La page de paramétrage du courrier se recharge et le bouton d'autorisation est remplacé par un message « autorisé ».
23. Pour tester la configuration :
    - Ajoutez une **Adresse e-mail du contact administrateur**.
    - Cochez **Envoyer un e-mail de test**.

©2003-2022 BeyondTrust Corporation. 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.

- Cliquez sur **Enregistrer les modifications**.

Configurer via OAuth2 pour Google

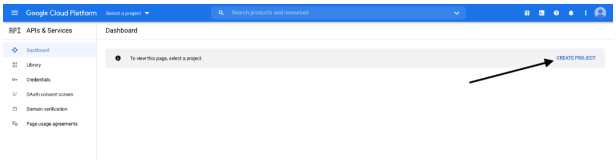
La configuration nécessite la modification des paramètres de l'appliance BeyondTrust et de la plateforme Google Cloud.

Commencez par modifier les paramètres de l'appliance BeyondTrust :

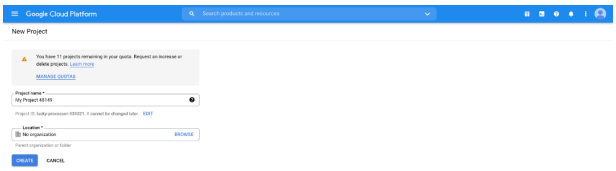
1. Allez dans **Appliance**, cliquez sur l'onglet **Sécurité** puis sur **Configuration e-mail**.
2. Basculez la **Méthode d'authentification** sur OAuth2.
3. Notez l'**URI de redirection d'autorisation**. Elle est requise plus tard.

Connectez-vous maintenant à votre console Google Cloud Platform (Google Dev Console) (console.cloud.google.com). Utilisez le compte Gmail pertinent, car seul le propriétaire du projet est en mesure de travailler dessus. Si vous n'avez pas encore de compte payant, vous pouvez choisir d'en acheter un en cliquant sur **Activer** dans la bannière supérieure. BeyondTrust ne peut pas fournir d'assistance pour l'achat d'un compte. Cliquez sur **En savoir plus** dans la bannière supérieure pour obtenir des informations sur les limitations des comptes gratuits.

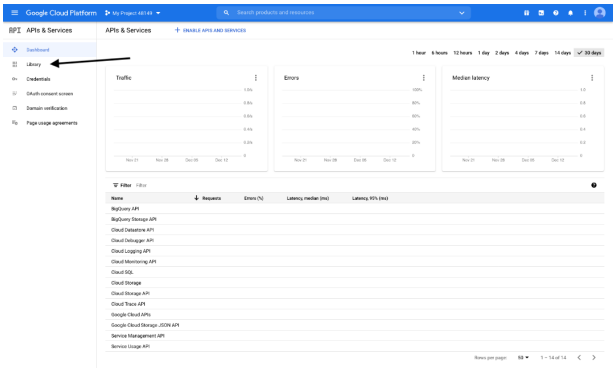
4. Cliquez sur **CRÉER UN PROJET**. Vous pouvez également utiliser un projet existant.



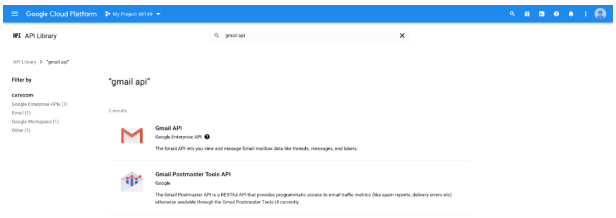
5. Acceptez le **Nom de projet** par défaut ou saisissez-en un.
6. Acceptez l'**Emplacement** par défaut ou sélectionnez un dossier parmi ceux disponibles pour votre organisation.
7. Cliquez sur **CRÉER**.



8. La page **API et services** apparaît. Cliquez sur **Bibliothèque** dans le menu de gauche.

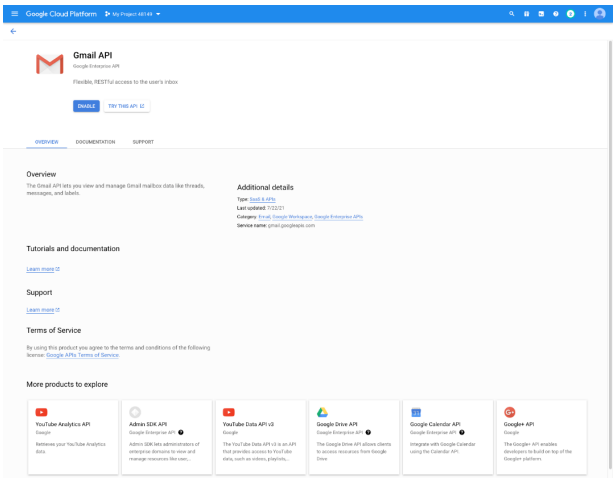


9. rcourez ou recherchez dans la bibliothèque pour trouver l'**API Gmail** et cliquez dessus.

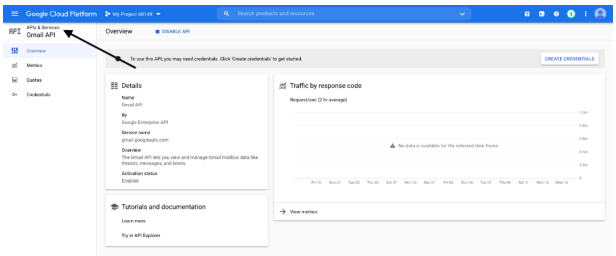


©2003-2022 BeyondTrust Corporation. Tous droits réservés. Les autres marques déposées identifiées sur cette page sont la propriété de leurs propriétaires respectifs. BeyondTrust n'est pas une banque à charte, une société de fiducie ou une institution de dépôt. Elle n'est pas autorisée à accepter des dépôts ou des comptes en fiducie et n'est ni sous licence ni gouvernée par une autorité bancaire nationale ou fédérale.

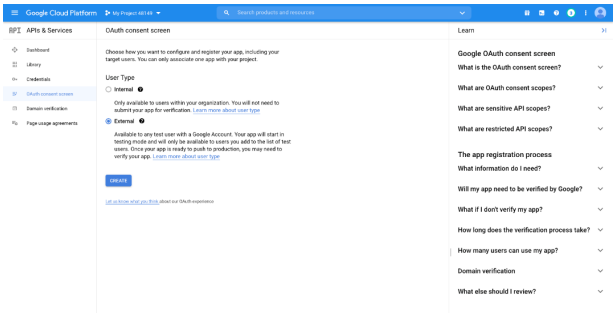
10. L'**API Gmail** apparaît sur sa propre page. Cliquez sur **ACTIVER**.



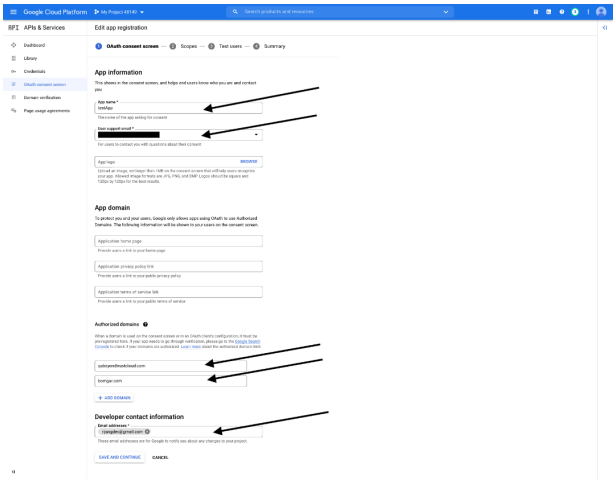
11. La **Présentation de l'API Gmail** s'affiche. Cliquez sur **API et services** en haut à gauche.
12. La page **API et services** apparaît à nouveau. Cliquez sur **Écran de consentement OAuth** dans le menu de gauche.



13. Sélectionnez le **type d'utilisateur**. « Interne » n'autorise que les utilisateurs de l'organisation, mais nécessite un compte Google Workspace.
14. Cliquez sur **CRÉER**.

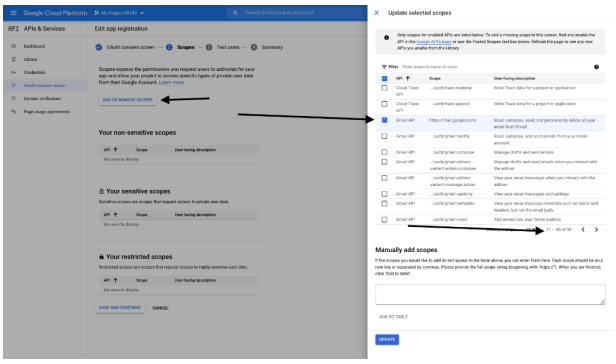


15. Saisissez le **nom de l'application**.
16. Saisissez une adresse **E-mail d'assistance aux utilisateurs**. Il peut s'agir par défaut de l'adresse que vous utilisez pour créer le projet.
17. Insérez un logo pour l'application, si vous le souhaitez. La section **Domaine de l'application** est également facultative.
18. Ajoutez les **Domaines autorisés**. Pour les appliances de test BeyondTrust, utilisez ceci :
    - qabeyondtrustcloud.com
    - bomgar.com
19. Saisissez les **Coordonnées du développeur**. Il s'agit de l'adresse e-mail que vous utilisez pour créer le projet.
20. Cliquez sur **ENREGISTRER ET CONTINUER**.



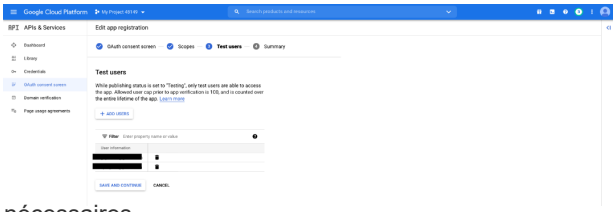
©2003-2022 BeyondTrust Corporation. Tous droits réservés. Les autres marques déposées identifiées sur cette page sont la propriété de leurs propriétaires respectifs. BeyondTrust n'est pas une banque à charte, une société de fiducie ou une institution de dépôt. Elle n'est pas autorisée à accepter des dépôts ou des comptes en fiducie et n'est ni sous licence ni gouvernée par une autorité bancaire nationale ou fédérale.

21. Sous l'onglet **Scopes**, cliquez sur **AJOUTER OU SUPPRIMER DES SCOPES**. Ceci ouvre la fenêtre **Mettre à jour les scopes sélectionnés**.
22. Localisez et cochez le scope **https://mail.google.com/** pour l'API Gmail.

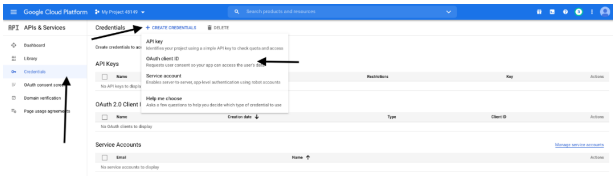


> ***Remarque :*** *l'API ne s'affiche pas si elle n'a pas été activée.*

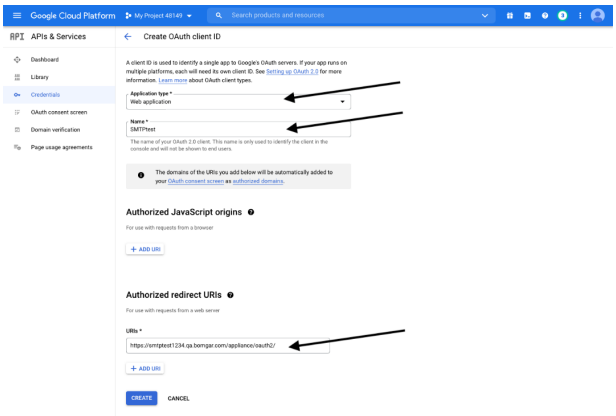
23. Cliquez sur **METTRE À JOUR**. La fenêtre **Mettre à jour les scopes sélectionnés** se ferme.
24. Cliquez sur **ENREGISTRER ET CONTINUER**.
25. Sous l'onglet **Utilisateurs test**, cliquez sur **AJOUTER DES UTILISATEURS**. Cela ouvre la fenêtre **Ajouter des utilisateurs**. Ajoutez les utilisateurs qui ont accès à l'application et cliquez sur **AJOUTER**. Notez les limites d'accès de l'utilisateur test et les restrictions associées.



26. Cliquez sur **ENREGISTRER ET CONTINUER**.
27. Passez en revue le résumé et apportez les modifications ou corrections nécessaires.
28. Cliquez sur **REVENIR AU TABLEAU DE BORD**.
29. Cliquez sur **Informations d'authentification** dans le menu de gauche.
30. Cliquez sur **CRÉER DES INFORMATIONS D'AUTHENTIFICATION** dans la bannière supérieure et sélectionnez **ID client OAuth**.

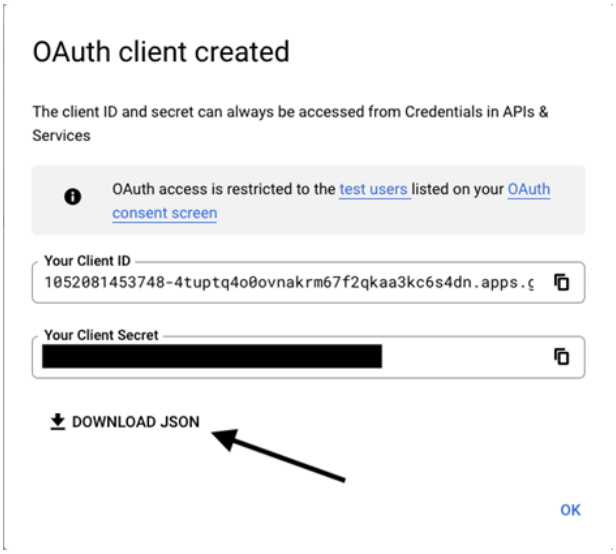


31. Sur la page de création d'informations d'authentification, sélectionnez **Application Web** pour le **Type d'application**. Des champs supplémentaires apparaissent lorsque cette option est sélectionnée.
32. Saisissez un nom pour l'application.
33. Faites défiles jusqu'à **URI de redirection autorisées** et cliquez sur **AJOUTER L'URI**.
34. Saisissez l'**URI de redirection d'autorisation** obtenue depuis l'appliance BeyondTrust au début de ce processus.
35. Cliquez sur **CRÉER**.



©2003-2022 BeyondTrust Corporation. 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.

36. Une fenêtre confirme la création du client OAuth et affiche l'**ID client** et le **secret de client**. Cliquez pour télécharger un fichier JSON. Le fichier contient des informations nécessaires aux étapes suivantes.
37. Cliquez sur **OK** pour revenir à la page API et services.



Les étapes restantes sont effectuées sur l'appliance BeyondTrust.

38. Allez dans **Appliance**, cliquez sur l'onglet **Sécurité** puis sur **Configuration e-mail**.
39. Saisissez les informations suivantes figurant dans le fichier JSON téléchargé :
    - **Point de terminaison d'autorisation**
    - **Point de terminaison du jeton**
    - **ID client**
    - **Secret de client**
40. Saisissez l'adresse e-mail de ce service en tant qu'**Envoyer depuis l'adresse e-mail**.
41. Saisissez l'**E-mail d'utilisateur**. Il doit s'agir d'une adresse e-mail saisie en tant qu'**Utilisateur test** ayant accès à l'application, lorsque vous avez rempli les écrans de consentement OAuth.
42. Saisissez les données pour les champs **Hôte**, **Chiffrement** et **Port**.
    - **Hôte** : smtp.gmail.com
    - **Chiffrement** : TLS
    - **Port** : 465

> ***Remarque :*** *les données par défaut pour Google sont affichées, mais votre installation peut utiliser un autre hôte ou une autre méthode de chiffrement. Le port est applicable pour TLS, mais d'autres méthodes de chiffrement peuvent utiliser un port différent.*

43. Saisissez votre certificat TLS si Google vous en a fourni un. Si ce n'est pas le cas, cochez **Ignorer les erreurs de certificat TLS**.
44. Saisissez ce qui suit pour **Scopes** : https://mail.google.com
45. Cliquez sur **Enregistrer les modifications**.
46. Cliquez surk **Autoriser**. Après la page de connexion qui s'affiche, l'avertissement **Google n'a pas vérifié ce message** peut s'afficher, si vous n'avez pas publié l'application. La page de consentement se recharge et le bouton d'autorisation est remplacé par un message « autorisé ».

©2003-2022 BeyondTrust Corporation. 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.

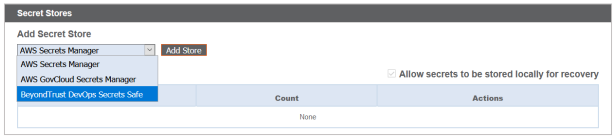
47. Pour tester la configuration :
    - Ajoutez une **Adresse e-mail du contact administrateur**.
    - Cochez **Envoyer un e-mail de test**.
    - Cliquez sur **Enregistrer les modifications**.

©2003-2022 BeyondTrust Corporation. 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.

Magasin de secrets : Magasin et accès aux secrets

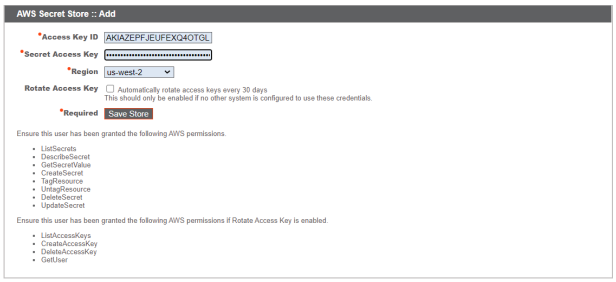
STATUS | USERS | NETWORKING | STORAGE | SECURITY | UPDATES | SUPPORT
CERTIFICATES | TLS CONFIGURATION | APPLIANCE ADMINISTRATION | EMAIL CONFIGURATION | SECRET STORE

Créez et gérez des clés secrètes stockées dans AWS et DevOps Secrets Safe (DSS) BeyondTrust pour stocker en toute sécurité les clés de chiffrement et les données de site. Pour ajouter un magasin de secrets, sélectionnez le magasin dans la liste déroulante puis cliquez sur **Enregistrer le magasin**. Fournissez et enregistrez les informations pour le magasin comme indiqué dans les étapes ci-dessous.



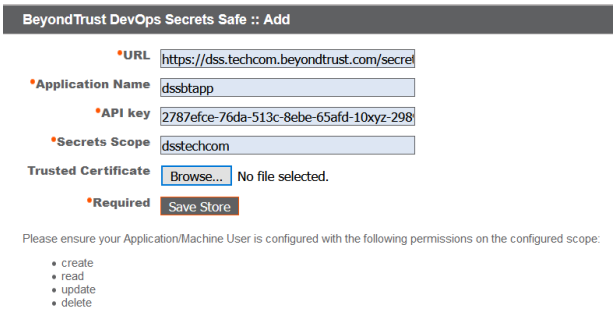
Ajouter un magasin de secrets AWS

1. Indiquez l'**ID de clé d'accès**, la **Clé d'accès secrète** et la **Région**.
2. Cochez la case **Provoquer la rotation de la clé d'accès** uniquement si vous n'utilisez pas les informations d'authentification dans un autre système.
3. Cliquez sur **Enregistrer le magasin**.



Ajouter un magasin BeyondTrust DevOps Secrets Safe

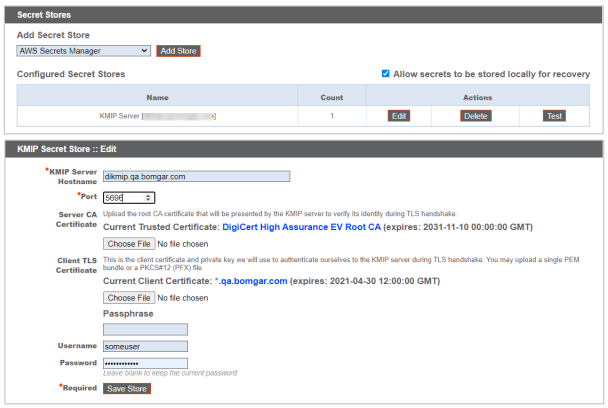
1. Saisissez l'**URL** pour votre instance DSS.
2. Indiquez le **Nom de l'application** que vous avez configuré dans DSS.
3. Indiquez la **Clé d'API** générée dans DSS pour l'application.
4. Saisissez le **Secrets Scope** que vous avez configuré avec des autorisations dans DSS.
5. Si vous utilisez un certificat auto-signé dans DSS, ajoutez le **Certificat approuvé**. Si vous utilisez un certificat d'un AC, vous n'avez pas besoin d'indiquer un certificat approuvé.
6. Cliquez sur **Enregistrer le magasin**.



Après l'ajout d'un magasin de secrets, cliquez sur **Tester** pour vérifier la connectivité au serveur du magasin de secrets et vous assurer que les autorisations appropriées sont en place pour les informations d'authentification permettent d'accéder audit serveur.

©2003-2022 BeyondTrust Corporation. 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.

Remarque : *la configuration d'un serveur KMIP pour un magasin de chiffrement n'est plus prise en charge dans la version 6.0 et les suivantes. Si vous avez un serveur KMIP configuré pour votre chiffrement avant la version 6.0, votre serveur KMIP sera migré vers la liste Magasin de secrets où vous pouvez le modifier, le supprimer et le tester.*



Remarque : *pour plus de sécurité, configurez votre règle AWS Identity and Access Management (IAM) pour limiter l'accès aux ressources correspondant à* ***BeyondTrust-**** *aux autorisations suivantes :*

- *DescribeSecret*
- *GetSecretValue*
- *TagResource*
- *UntagResource*
- *CreateSecret*
- *DeleteSecret*
- *UpdateSecret*

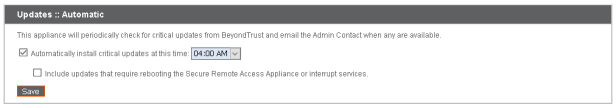
Pour plus d'informations sur la gestion des règles AWS IAM, veuillez consulter Gestion des règles IAM à l'adresse https://docs.aws.amazon.com/ IAM/latest/UserGuide/access_policies_manage.html.

Remarque : *si vous supprimez le dernier magasin distant, un message s'affiche indiquant que les secrets seront déplacés localement.*

©2003-2022 BeyondTrust Corporation. 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.

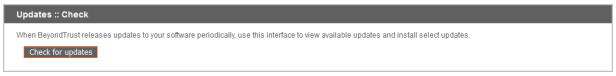
Mises à jour : Rechercher les mises à jour disponibles et installer le logiciel

La B Series Appliance vérifie régulièrement s'il y a des mises à jour critiques et envoie un e-mail à l'administrateur lorsqu'elles sont disponibles. Vous pouvez choisir d'installer automatiquement les mises à jour et utiliser le menu déroulant pour sélectionner une heure d'installation.

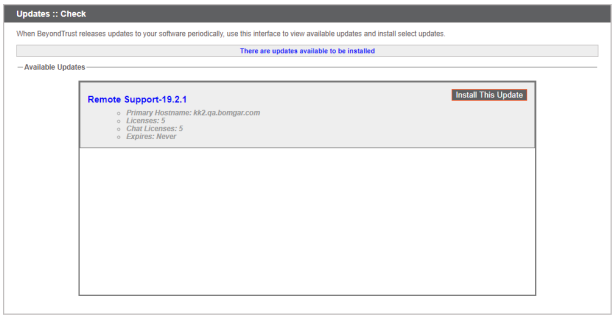


Les mises à jour nécessitant un redémarrage de la B Series Appliance ou l'interruption de services sont exclues du processus de mise à jour automatique, sauf si vous cochez la case pour le prendre en compte.

BeyondTrust vous informera toujours de la sortie des dernières versions dès qu'elles seront disponibles. Lorsque vous recevez une notification selon laquelle une mise à jour est disponible pour votre B Series Appliance, cliquez sur le bouton **Rechercher les mises à jour** pour localiser les paquets et les rendre disponibles à l'installation.



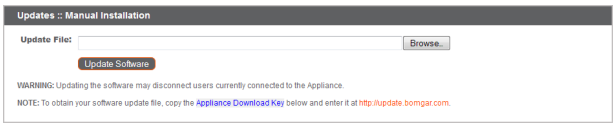
Si plusieurs paquets ont été compilés pour votre B Series Appliance, chacun d'eux sera indiqué séparément dans la liste des mises à jour disponibles. Votre nouveau logiciel est automatiquement téléchargé et installé lorsque vous cliquez sur le bouton **Installer cette mise à jour**.

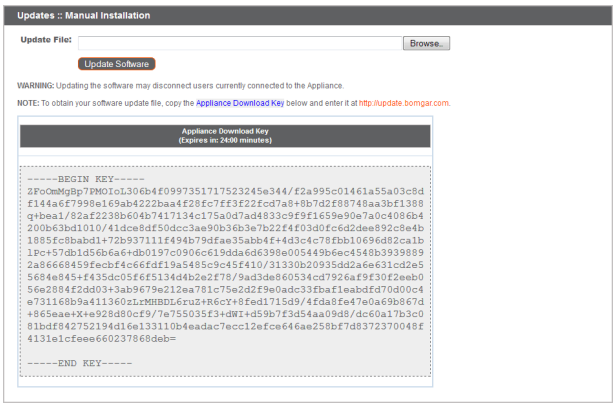


Si aucun package de mises à jour ni aucun correctif n'est disponible sur votre B Series Appliance, le message « Aucune mise à jour disponible » s'affichera. Si une mise à jour est disponible, mais qu'une erreur est survenue lors de la distribution de la mise à jour à votre B Series Appliance, un autre message s'affiche, comme : « Une erreur est survenue lors de la création de votre mise à jour. Pour plus d'informations, veuillez visiter www.beyondtrust.com/docs/index.htm#support."

©2003-2022 BeyondTrust Corporation. 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.

Il n'est pas obligatoire d'utiliser la fonction **Rechercher les mises à jour**. Si votre B Series Appliance n'a pas accès à Internet, ou si la politique de sécurité de votre entreprise n'autorise pas les mises à jour automatiques, vous pouvez les chercher manuellement. Cliquez sur le lien de la **Clé de téléchargement de l'appliance** pour générer une clé de la B Series Appliance 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 B Series Appliance.





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.

> ***Remarque :*** *Préparez-vous à installer les mises à jour du logiciel directement après le téléchargement. Une fois la mise à jour téléchargée, elle n'apparaîtra plus sur votre liste de mises à jour disponibles. Si vous avez besoin de télécharger de nouveau une mise à jour logicielle, contactez l'BeyondTrust Technical Support.*

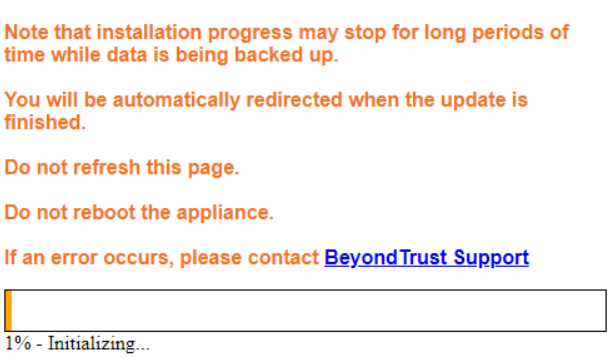
Lorsque l'écran du contrat de licence utilisateur final (CLUF) BeyondTrust apparaît, indiquez les informations de contact nécessaires et cliquez sur le bouton **Accepter-Lancer le téléchargement** pour accepter le CLUF et poursuivre l'installation. Si vous avez plusieurs B Series Appliances avec la même configuration de site (pour une reprise en séquence ou pour ATLAS), vous n'aurez à accepter le CLUF qu'une fois.

Remarque : si vous choisissez de refuser le CLUF, un message d'erreur s'affichera et vous ne pourrez pas 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'BeyondTrust Technical Support à l'adresse www.beyondtrust.com/support.

Pendant la procédure d'installation, la page **Mises à jour** affiche une barre de progression vous informant de la progression générale de la mise à jour. Les mises à jour effectuées ici mettent automatiquement à jour l'ensemble des sites et licences sur votre BeyondTrust Appliance B Series.

Si vous installez une mise à jour du logiciel, les techniciens d'assistance connectés perdent momentanément la connexion à toute session d'assistance technique et à la console du technicien d'assistance. Il convient donc de lancer les mises à jour pendant les périodes calmes. Cependant, si votre mise à jour ne contient que des licences supplémentaires, vous pouvez l'installer sans interrompre la connexion du technicien d'assistance.



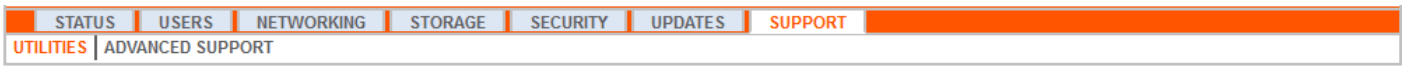
Vous trouverez les informations sur les dernières mises à jour BeyondTrust à l'adresse https://www.beyondtrust.com/docs/release-notes/remote-support/index.htm.

Pour afficher les correctifs installés, sélectionnez **Correctifs installés** dans l'onglet **Mises à jour**. Le tableau indique tous les correctifs de micrologiciel installés et leur date d'installation.

©2003-2022 BeyondTrust Corporation. 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.

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 la résolution **DNS** de votre B Series Appliance en effectuant une recherche d'un nom d'hôte ou une recherche inversée d'une adresse IP.
- Effectuez un **ping** sur un nom d'hôte ou une adresse IP pour tester la connectivité réseau de votre B Series Appliance.
- Utilisez **Traceroute** pour voir le chemin emprunté par les paquets depuis la B Series Appliance vers le système externe.
- Utilisez le **Test de connexion TCP** pour vérifier la connectivité d'un port spécifique sur une adresse IP ou un nom d'hôte cible.
- Utilisez le **Test de connexion SSL/TLS** pour vérifier la connectivité vers des serveurs distants HTTPS ou TLS.

©2003-2022 BeyondTrust Corporation. 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.

BeyondTrust
Secure Remote Access
Powered by Bomgar

Virtual Appliance ADMINISTRATION
English (US) | admin | LOGOUT

STATUS | USERS | NETWORKING | STORAGE | SECURITY | UPDATES | SUPPORT
UTILITIES | ADVANCED SUPPORT

Util :: DNS

Use this DNS utility to test the DNS resolution on this appliance. If you get "Unable to Resolve" errors, check your DNS Server settings on the Networking tab.

Hostname or IP Address

Resolve

Util :: Ping

Use this Ping utility to test the Network connectivity of this appliance. If you get "unknown host" errors, check your DNS Server settings on the Networking tab. If you get 100% packet loss, check that the destination server is configured to respond to Pings, and check your IP settings on the Networking tab.

Hostname or IP Address

IPv4 IPv6

Ping

Util :: Traceroute

Use this Traceroute utility to test the outbound Network routes from this appliance. You can manually configure static routes in the Networking tab.
This utility will only try a maximum of 20 hops

Hostname or IP Address

IPv4 IPv6

Trace

Util :: TCP Connection Test

Use this TCP Connection Test utility to troubleshoot network connections to remote hosts and ports.

Hostname or IP Address

Port Number

Test

Util :: SSL/TLS Connection Test

Use this to troubleshoot connections to remote HTTPS or any other TLS server.

Hostname or IP Address

Use of hostname here is encouraged instead of IP. Hostnames will be sent in the handshake in the Server Name Indication (SNI) field. Many TLS servers implement name-based virtual hosting and will send different certificates based on this SNI information, and are more likely to result in a successful connection.

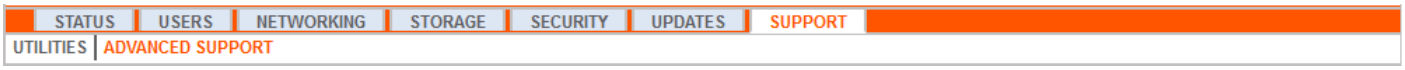
Port Number

Test

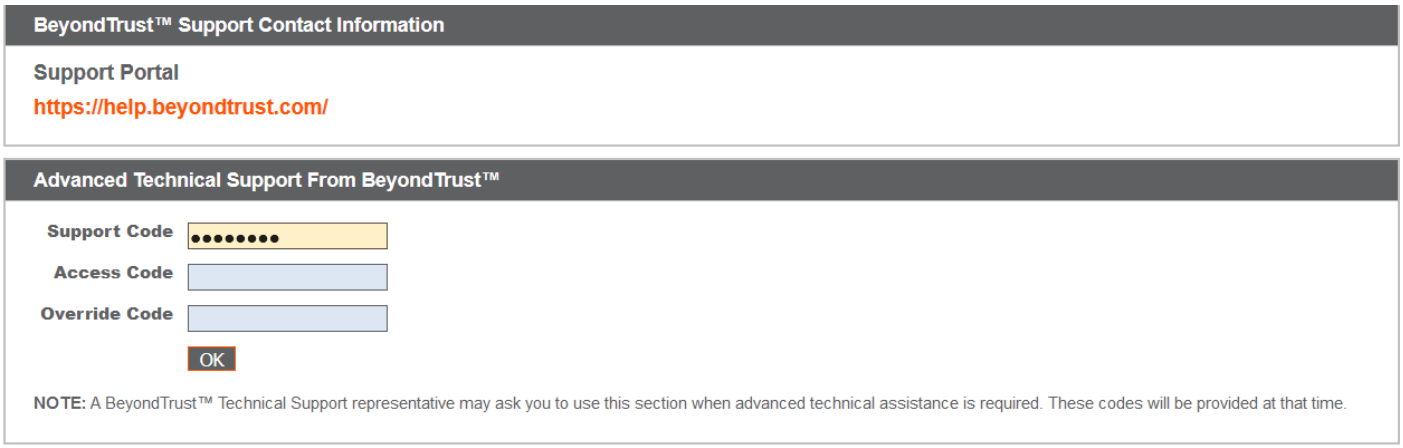
Copyright © 2002-2020 BeyondTrust Corporation. Redistribution Prohibited. All Rights Reserved. www.beyondtrust.com

©2003-2022 BeyondTrust Corporation. 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.

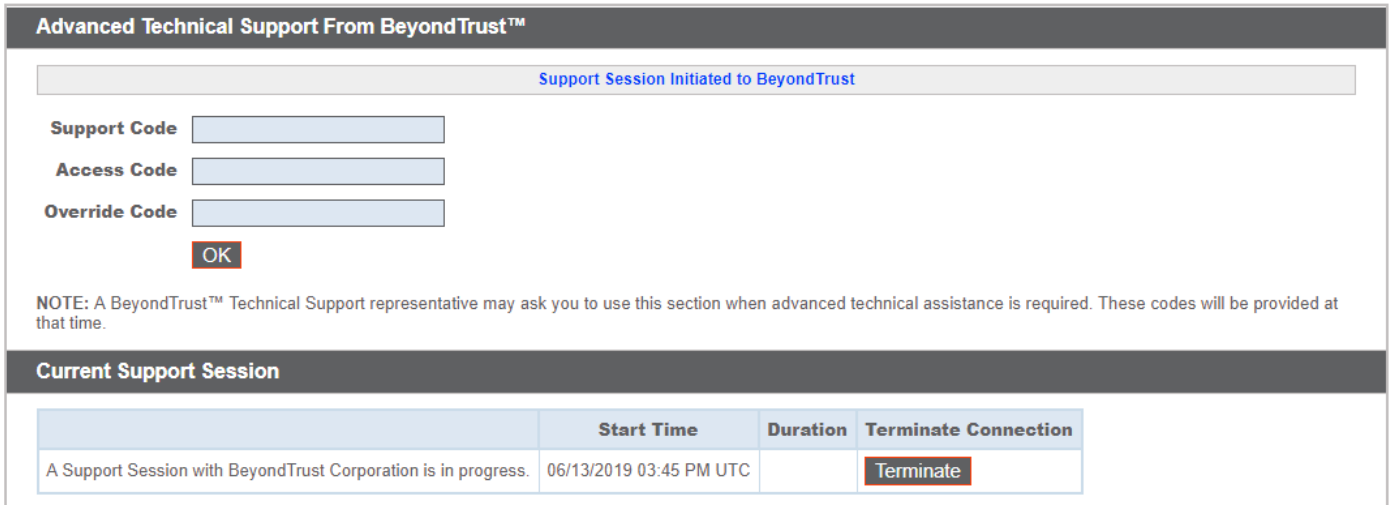
Assistance technique avancée : Contacter l'BeyondTrust Technical Support



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



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



©2003-2022 BeyondTrust Corporation. 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.

Comparaison entre BeyondTrust Appliance B Seriess

	B400	B300	B200
Capacité de technicien d'assistance	Jusqu'à 1 200 techniciens simultanés	Jusqu'à 300 techniciens simultanés	Jusqu'à 20 techniciens simultanés exécutant un maximum de 3 sessions chacun
Jump Technologie	Jusqu'à 25 000 Jump Clients actifs	Jusqu'à 10 000 Jump Clients actifs	Jusqu'à 1 000 Jump Clients actifs
Déploiement	Serveur montable sur rack 1U Compatible avec des déploiements Atlas	Serveur montable sur rack 1U Compatible avec des déploiements Atlas	Serveur montable sur rack 1U

©2003-2022 BeyondTrust Corporation. 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.