Effectuer les tâches d'administration du système

Cette rubrique contient les sections suivantes :

Survol de l'administration du système

L'appliance série S offre divers outils pour la gestion du système. Les fonctionnalités de l'onglet System Administration (Administration système) vous aident à gérer les tâches suivantes :

- Configuration des appliances
- Clés de fonctionnalité
- Ajout, modification et suppression de comptes d'utilisateur
- Mises à jour et mises à niveau du logiciel AsyncOS
- Heure système

Enregistrement, chargement et réinitialisation de la configuration de l'appliance

Tous les paramètres de configuration dans Secure Web Appliance sont gérés à l'aide d'un fichier de configuration XML unique.

Affichage et impression de la configuration de l'appliance

Étape 1 Choisissez **System Administration > Configuration Summary** (Administration système > Résumé de la configuration).

Étape 2 Affichez ou imprimer la page du sommaire de la configuration, le cas échéant.

Enregistrement du fichier de configuration de l'appliance

Étape 1 Choisissez **System Administration > Configuration File** (Administration système > Fichier de configuration).

Étape 2 Remplissez les options du fichier de configuration .

Option	Description
Indiquer une option de gestion de fichiers	Choisissez le mode de traitement du fichier de configuration généré : • Téléchargez le fichier sur l'ordinateur local pour l'afficher ou l'enregistrer. • **Enregistrez le fichier sur cette appliance** (wsa_exemple.com). • **Email file to** (Envoyer le fichier par courriel à) : indiquez une ou plusieurs adresses de courriel.
Indiquez une option de gestion de la phrase secrète	• **Masquer les phrases secrètes dans les fichiers de configuration** – Les phrases secrètes d'origine sont remplacées par « ***** » dans le fichier exporté ou enregistré. Veuillez noter que les fichiers de configuration avec des phrases secrètes masquées ne peuvent pas être chargés directement dans AsyncOS pour le Web. • **Chiffrer les phrases secrètes dans les fichiers de configuration** : si le mode FIPS est activé, cette option est disponible. Consultez Activation ou désactivation du mode FIPS , on page 51 pour obtenir des renseignements sur l'activation du mode FIPS.

Option	Description
Sélectionner une option de nom de fichier	Choisissez le nom du fichier de configuration : • **Utiliser le nom de fichier généré par le système** • **Utiliser un nom de fichier défini par l'utilisateur**

Étape 3 Cliquez sur **Submit** (Soumettre).

Chargement du fichier de configuration de l'appliance

Caution Le chargement de la configuration supprimera définitivement tous vos paramètres de configuration actuels. Il est fortement recommandé d'enregistrer votre configuration avant d'effectuer ces actions.

Nous vous déconseillons de charger des configurations d'une version précédente dans la dernière version. Vous pouvez conserver les paramètres de configuration en mettant à niveau les chemins.

Les fichiers de configuration chargés avec des modifications manuelles peuvent entraîner des problèmes de performances et fonctionnels.

Note Si un fichier de configuration compatible est basé sur une version de l'ensemble de catégories d'URL plus ancienne que la version actuellement installée sur l'appliance, les politiques et les identités du fichier de configuration peuvent être modifiées automatiquement.

Note Si vous rencontrez une erreur de validation de certificat lors du chargement du fichier de configuration, chargez l'autorité de certification racine du certificat dans le répertoire racine approuvé de Secure Web Appliance, puis chargez à nouveau le fichier de configuration. Pour savoir comment charger l'autorité de certification racine, consultez Certificate Management, on page 54.

Étape 1 Choisissez **System Administration > Configuration File** (Administration système > Fichier de configuration).

Étape 2 Choisissez les options Load Configuration (Charger la configuration) et un fichier à charger. Remarque :

Note
- Les fichiers dont la phrase secrète est masquée ne peuvent pas être chargés.
- Les fichiers doivent avoir l'en-tête suivant :

  `<?xml version="1.0" encoding="ISO-8859-1"?> <!DOCTYPE config SYSTEM "config.dtd">`

  et une section de configuration correctement mise en forme :

  `<config>` ... *vos informations de configuration dans un fichier XML valide* `</config>`

Étape 3 Cliquez sur **Load** (Charger).

Étape 4 Lisez l'avertissement qui s'affiche. Si vous comprenez les conséquences de cette procédure, cliquez sur **Continue** (Continuer).

Réinitialisation de la configuration de l'appliance aux valeurs par défaut

Vous pouvez choisir de conserver ou non les paramètres réseau existants lorsque vous réinitialisez la configuration de l'appliance.

Cette action ne nécessite pas de validation.

Before you begin

Enregistrez votre configuration à un emplacement hors de l'appliance.

Étape 1 Choisissez **System Administration > Configuration File** (Administration système > Fichier de configuration).

Étape 2 Faites défiler la liste vers le bas pour afficher la section **Reset Configuration** (Réinitialiser la configuration).

Étape 3 Lisez les informations sur la page et sélectionnez les options.

Étape 4 Cliquez sur **Reset** (Réinitialiser).

Enregistrement de la sauvegarde du fichier de configuration

La fonction de sauvegarde du fichier de configuration enregistre la configuration de l'appliance à chaque validation et envoie le fichier de configuration précédent avant l'actuel à un serveur de sauvegarde distant par FTP ou SCP.

Étape 1 Choisissez **System Administration > Configuration File** (Administration système > Fichier de configuration).

Étape 2 Cochez la case **Enable Config Backup** (Activer la sauvegarde de la configuration).

Étape 3 Choisissez **Yes** (Oui) pour inclure la phrase secrète dans le fichier de configuration. Vous pouvez également choisir **No** (Non) pour exclure la phrase secrète du fichier de configuration.

Étape 4 Choisissez la méthode de récupération. Les options disponibles sont les suivantes :

- FTP on Remote Server (FTP sur le serveur distant) : saisissez le nom d'hôte, le répertoire, le nom d'utilisateur et la phrase secrète du FTP.
- SCP on Remote Server (SCP sur le serveur distant) : saisissez le nom d'hôte, le numéro de port, le répertoire et le nom d'utilisateur SCP.
- Host Key Checking (Vérification de la clé de l'hôte) : le SSH gère et vérifie automatiquement une base de données des identifications pour tous les hôtes avec lesquels il a été utilisé. Les clés d'hôte sont stockées dans le répertoire de base de l'utilisateur, à savoir le répertoire */.ssh/known_hosts*.

  Si vous sélectionnez **SCP on Remote Server** (SCP sur le serveur distant), puis sélectionnez **Enable Host Key Checking** (Activer la vérification de la clé hôte), vous disposerez des options suivantes :

  - Automatic (Automatique) : la clé d'hôte sera définie automatiquement par Secure Web Appliance.
  - Manual (Manuel) : l'utilisateur peut saisir la clé d'hôte manuellement.

Une fois les modifications envoyées, l'appliance Cisco pour la sécurité du Web fournit une ou plusieurs clés SSH à ajouter au fichier de clés autorisées sur l'hôte distant, afin que les fichiers de configuration puissent être chargés de l'appliance Cisco pour la sécurité du Web vers l'hôte distant. Par conséquent, SSH gère et vérifie une base de données contenant les informations d'identification de tous les hôtes auxquels il s'est connecté. Les clés d'hôte sont stockées dans le répertoire de base de l'utilisateur, à savoir le répertoire */.ssh/known_hosts*.

Étape 5 Cliquez sur **Submit** (Soumettre).

Vous pouvez également activer la fonction de sauvegarde du fichier de configuration en utilisant la commande de l'interface de ligne de commande `configbackup`

Licenses Cisco Secure Web Appliance

Utilisation des clés de fonctionnalité

Les clés de fonctionnalité activent des fonctionnalités spécifiques sur votre système. Les clés sont spécifiques au numéro de série de votre appliance (vous ne pouvez pas réutiliser une clé d'un système sur un autre système).

Affichage et mise à jour des clés de fonctionnalité

Étape 1 Choisissez **System Administration > Feature Keys** (Administration système > Clés de fonctionnalité).

Étape 2 Pour actualiser la liste des clés en attente, cliquez sur **Check for New Keys** (Rechercher de nouvelles clés) afin d'actualiser la liste des clés en attente.

Étape 3 Pour ajouter une nouvelle clé de fonctionnalité manuellement, collez ou saisissez la clé dans le champ Feature Key (Clé de fonctionnalité) et cliquez sur **Submit Key** (Envoyer la clé). Si la clé de fonctionnalité est valide, elle est ajoutée à l'affichage.

Étape 4 Pour activer une nouvelle clé de fonctionnalité à partir de la liste Pending Activation (Activation en attente), cochez la case « Select » (Sélectionner) et cliquez sur **Activate Selected Keys** (Activer les clés sélectionnées).

Vous pouvez configurer votre appliance de manière à télécharger et installer automatiquement les nouvelles clés dès qu'elles sont émises. Dans ce cas, la liste Pending Activation (Activation en attente) sera toujours vide. Vous pouvez demander à AsyncOS de rechercher de nouvelles clés à tout moment en cliquant sur le bouton **Check for New Keys** (Rechercher les nouvelles clés), même si vous avez désactivé la vérification automatique dans la page Feature Key Settings (Paramètres des clés de fonctionnalité).

Modification des paramètres de mise à jour des clés de fonctionnalité

La page des paramètres des clés de fonctionnalité permet de contrôler si votre appliance vérifie et télécharge de nouvelles clés de fonctionnalité, et si ces clés sont activées automatiquement.

Étape 1 Choisissez **System Administration > Feature Key Settings** (Administration système > Paramètres des clés de fonctionnalité).

Étape 2 Cliquez sur **Edit Settings** (Modifier les paramètres).

Étape 3 Modifiez les paramètres des clés de fonctionnalité au besoin.

Option	Description
Transmission automatique des clés de fonctionnalité	Options permettant de vérifier et de télécharger automatiquement les clés de fonctionnalité et d'activer automatiquement les clés de fonctionnalité téléchargées. Les vérifications automatiques sont normalement effectuées une fois par mois, mais ce nombre passe à une fois par jour si une clé de fonctionnalité doit expirer dans moins de 10 jours et à une fois par jour après l'expiration de la clé, pendant un maximum d'un mois. Après un mois, la clé expirée n'est plus incluse dans la liste des clés sur le point d'expirer et qui ont expiré.

Étape 4 Envoyez et validez vos modifications.

Gestion des licences Smart Software

Survol

Les licences logicielles Smart vous permettent de gérer et de surveiller les licences Cisco Secure Web Appliance. Pour activer les licences logicielles Smart, vous devez enregistrer votre appliance auprès de Cisco Smart Software Manager (CSSM), la base de données centralisée contenant les détails de la licence pour tous

les produits Cisco que vous achetez et utilisez. Grâce aux licences Smart, vous pouvez vous inscrire avec un jeton unique plutôt que de les enregistrer individuellement sur le site Web à l'aide des clés d'autorisation de produit (PAK).

Une fois l'appliance enregistrée, vous pouvez suivre vos licences d'appliance et surveiller l'utilisation des licences sur le portail CSSM. L'agent Smart installé sur l'appliance connecte cette dernière au portail CSSM et transmet les informations d'utilisation des licences au portail CSSM pour le suivi de la consommation.

Consultez https://www.cisco.com/c/en/us/td/docs/wireless/technology/mesh/8-2/b_Smart_Licensing_Deployment_Guide.html pour en savoir plus sur Cisco Smart Software Manager.

Remarque AsyncOS version 15.0 est la dernière version à prendre en charge la licence classique. Les prochaines versions ne prendront en charge que les licences Smart.

Avant de commencer

- Assurez-vous que votre appliance est connectée à Internet.
- Communiquez avec l'équipe commerciale de Cisco pour créer un compte Smart dans le portail Cisco Smart Software Manager (https://software.cisco.com/#module/SmartLicensing) ou installez un satellite Cisco Smart Software Manager sur votre réseau.

  Consultez https://www.cisco.com/c/en/us/td/docs/wireless/technology/mesh/8-2/b_Smart_Licensing_Deployment_Guide.html pour en savoir plus sur la création de compte d'utilisateur ou l'installation d'un satellite Cisco Smart Software Manager.

  Pour les utilisateurs qui ne souhaitent pas envoyer directement les informations d'utilisation des licences sur Internet, le satellite Smart Software Manager peut être installé sur site et fournit un sous-ensemble de la fonctionnalité CSSM. Une fois que vous avez téléchargé et déployé l'application satellite, vous pouvez gérer les licences localement et en toute sécurité sans envoyer de données au CSSM sur Internet. Le satellite CSSM transmet périodiquement les informations au nuage.

Remarque Si vous souhaitez utiliser le satellite Smart Software Manager, utilisez Smart Software Manager Satellite Enhanced Edition 6.1.0.

- Les utilisateurs existants de licences classiques (traditionnelles) doivent migrer leurs licences classiques vers des licences Smart.

  Consultez https://video.cisco.com/detail/video/5841741892001/convert-classic-licenses-to-smart-licenses?autoStart=true&q=classic.
- L'horloge système de l'appliance doit être synchronisée avec celle du CSSM. Tout écart entre l'horloge système de l'appliance et celle du CSSM entraînera l'échec des opérations de licence Smart.

Remarque Si vous avez une connexion Internet et que vous souhaitez vous connecter au CSSM par l'intermédiaire d'un proxy, vous devez utiliser le même proxy que celui configuré pour l'appliance à l'aide du menu **System Administration-> Upgrade and Update Settings** (Administration système > Paramètres de mise à niveau et de mise à jour).

Remarque Pour les utilisateurs virtuels, chaque fois que vous recevez un nouveau fichier PAK (nouveau ou renouvelé), générez le fichier de licence et chargez-le sur l'appliance. Après avoir chargé le fichier, vous devez convertir la clé PAK en licence Smart. En mode de licence Smart, la section des clés de fonctionnalité dans le fichier de licence sera ignorée lors du chargement du fichier et seules les informations du certificat seront utilisées.

Remarque L'appliance basculera du mode de licence Smart au mode de licence classique lorsque vous reviendrez à une version antérieure d'AsyncOS. Vous devez activer les licences Smart manuellement et demander les licences requises.

Pour activer la licence logicielle Smart pour votre appliance, vous devez procéder de la manière suivante :

	Faire ceci	Plus d'informations
Étape 1	Activez les licences logicielles Smart	Activation des licences logicielles Smart , à la page 8
Étape 2	Enregistrez l'appliance auprès de Cisco Smart Software Manager	Enregistrement de l'appliance dans Cisco Smart Software Manager , à la page 9
Étape 3	Demandez les licences (clés de fonctionnalité)	Demande de licences, à la page 11

Activation des licences logicielles Smart

Étape 1 Choisissez **System Administration > Smart Software Licensing** (Administration système > Licence logicielle Smart).

Étape 2 Cliquez sur **Enable Smart Software Licensing** (Activer les licences logicielles Smart).

Pour en savoir plus sur les licences logicielles Smart, cliquez sur le lien **En savoir plus sur les licences logicielles Smart**.

Étape 3 Cliquez sur **OK** après avoir lu les informations sur les licences logicielles Smart.

Étape 4 Validez vos modifications.

Prochaine étape

Après avoir activé les licences logicielles Smart, toutes les fonctionnalités du mode d'octroi de licences classique seront automatiquement disponibles dans le mode d'octroi de licences Smart. Si vous êtes un utilisateur existant en mode de licence classique, vous avez une période d'évaluation de 90 jours pour utiliser la fonctionnalité de licence logicielle Smart sans enregistrer votre appliance auprès du CSSM.

Vous recevrez des notifications à des intervalles réguliers (90e, 60e, 30e, 15e, 5e et dernier jour) avant l'expiration et aussi à l'expiration de la période d'évaluation. Vous pouvez enregistrer votre appliance auprès du CSSM pendant ou après la période d'évaluation.

Remarque

- Les nouveaux utilisateurs d'appliance virtuelle sans licence active en mode de licence classique n'auront pas de période d'évaluation même s'ils activent la fonction d'octroi de licences logicielles Smart. Seuls les utilisateurs de l'appliance virtuelle existante avec des licences actives en mode de licence classique auront une période d'évaluation. Si de nouveaux utilisateurs d'appliance virtuelle souhaitent évaluer la fonctionnalité de licences Smart, communiquez avec l'équipe des ventes de Cisco pour ajouter la licence d'évaluation au compte Smart. Les licences d'évaluation sont utilisées à des fins d'évaluation après l'enregistrement.
- Après avoir activé la fonction de licences Smart sur votre appliance, vous ne pourrez pas revenir du mode de licences Smart au mode d'octroi de licences classique.
- Les fonctionnalités suivantes sont redémarrées lorsque vous activez la fonction d'octroi de licences Smart :
  - Secure Web Appliance Filtres de réputation Web
  - Secure Web Appliance Anti-Virus Sophos
  - Secure Web Appliance Anti-Virus Webroot
  - Secure Web Appliance Proxy Web et moteur DVS
- Dans AsyncOS version 15.0, les licences Smart peuvent être activées pour les nouveaux déploiements virtuels de Cisco Secure Web Appliance. Même si la licence classique n'est pas obligatoire. Pour en savoir plus, consultez les conditions préalables disponibles dans la section Survol.

Enregistrement de l'appliance dans Cisco Smart Software Manager

Vous devez activer la fonction d'octroi de licences logicielles Smart dans le menu System Administration (Administration système) afin d'enregistrer votre appliance auprès de Cisco Smart Software Manager.

Remarque Vous ne pouvez pas enregistrer plusieurs appliances dans une seule instance. Vous devez enregistrer les appliances une par une.

Étape 1 Choisissez **System Administration** > **Smart Software Licensing** (Administration système > Licences logicielles Smart).

Étape 2 Sélectionnez l'option **Smart License Registration** (Enregistrement de licence Smart).

Étape 3 Cliquez sur **Confirm (Confirmer)**.

Étape 4 Cliquez sur **Edit** (Modifier) si vous souhaitez modifier les paramètres de transport. Les options disponibles sont les suivantes :

- **Direct** : connecte l'appliance directement à Cisco Smart Software Manager par le biais du protocole HTTP. Cette option est sélectionnée par défaut.
- **Transport Gateway** (Passerelle de transport) : connecte l'appliance à Cisco Smart Software Manager par l'intermédiaire d'une passerelle de transport ou d'un satellite Smart Software Manager. Lorsque vous choisissez cette option, vous devez entrer l'URL de la passerelle de transport ou du satellite Smart Software Manager et

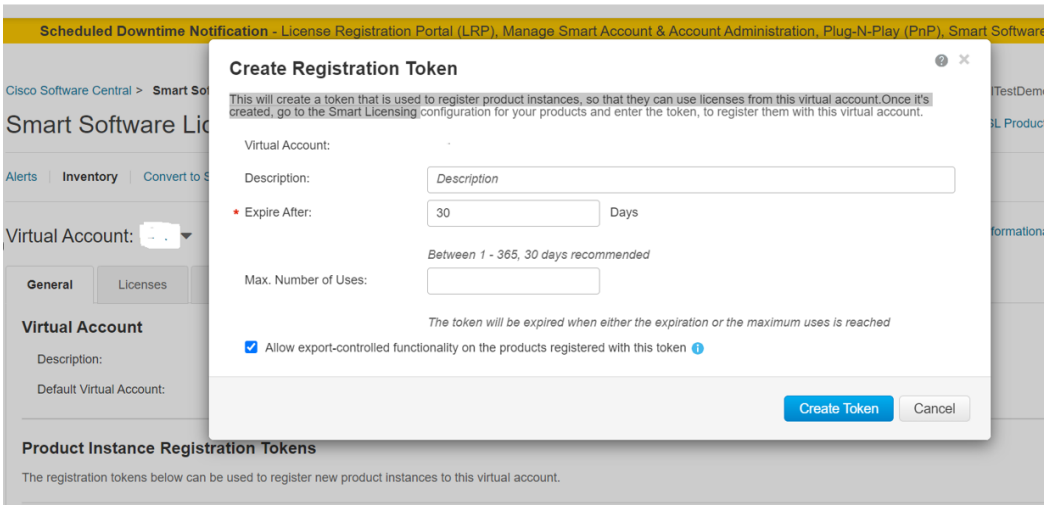
cliquer sur OK. Cette option prend en charge HTTP et HTTPS. En mode FIPS, la passerelle de transport prend en charge uniquement HTTPS.

Consultez le site https://www.cisco.com/c/en/us/td/docs/wireless/technology/mesh/8-2/b_Smart_Licensing_Deployment_Guide.html pour en savoir plus sur la passerelle de transport.

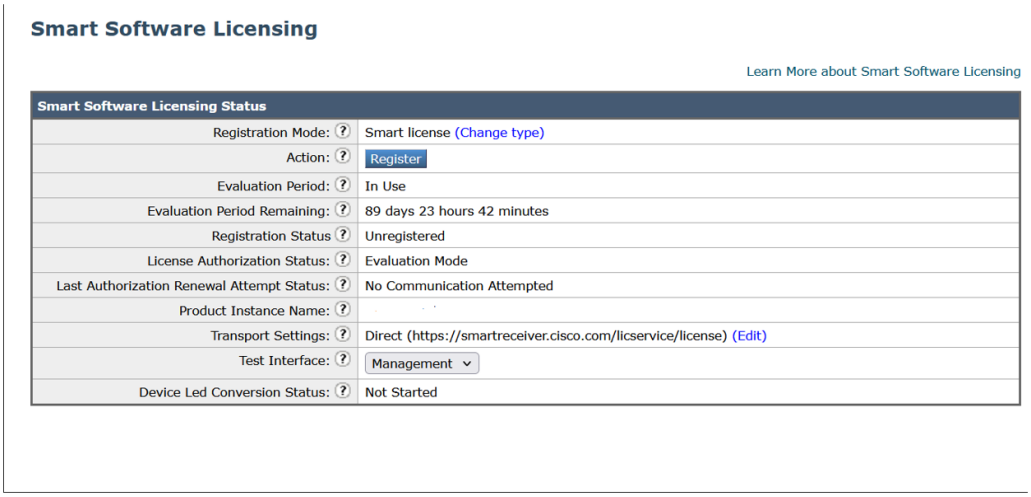
Étape 5 (Facultatif) **Tester l'interface** : choisissez l'interface de gestion ou de données lors de l'enregistrement de l'appliance pour la fonction de licence Smart. Cela s'applique uniquement lorsque vous activez le routage fractionné et que vous vous inscrivez pour obtenir une licence Smart.

Remarque Si le routage fractionné n'est pas activé, seule l'option d'interface de gestion est disponible dans la liste déroulante **Test Interface** (Tester l'interface).

Étape 6 Accédez au portail Cisco Smart Software Manager (https://software.cisco.com/#module/SmartLicensing) en utilisant vos coordonnées de connexion. Accédez à la page Virtual Account (Compte virtuel) du portail et accédez à l'onglet General (Général) pour générer un nouveau jeton. Copiez le jeton d'enregistrement d'instance de produit pour votre appliance. Consultez le site https://www.cisco.com/c/en/us/td/docs/wireless/technology/mesh/8-2/b_Smart_Licensing_Deployment_Guide.html pour en savoir plus sur la création des jetons d'enregistrement d'instance de produit.

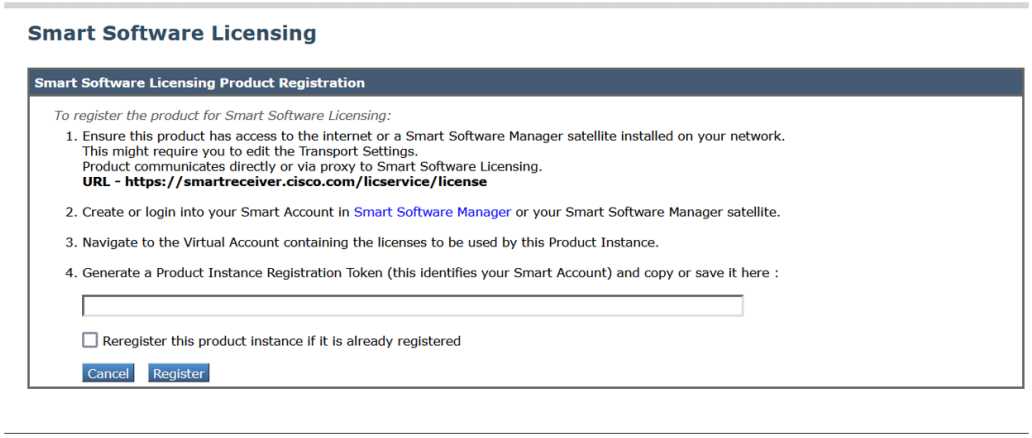


Étape 7 Revenez à votre appliance et cliquez sur **Register**(Enregistrer).



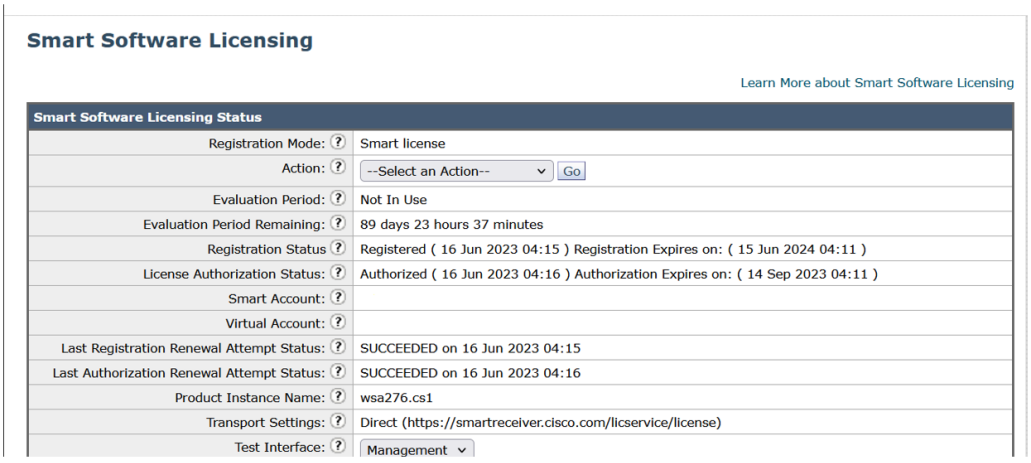
Étape 8 Collez le **jeton d'enregistrement d'instance de produit** dans la zone de texte.

Dans la page Smart Software Licensing (Licences logicielles Smart), vous pouvez cocher la case **Reregister this product instance if it is already registered** (Réenregistrer cette instance de produit si elle est déjà enregistrée) pour réenregistrer votre appliance.



Prochaine étape

Le processus d'enregistrement du produit prend quelques minutes et vous pouvez voir l'état de l'enregistrement dans la page des licences logicielles Smart.



Demande de licences

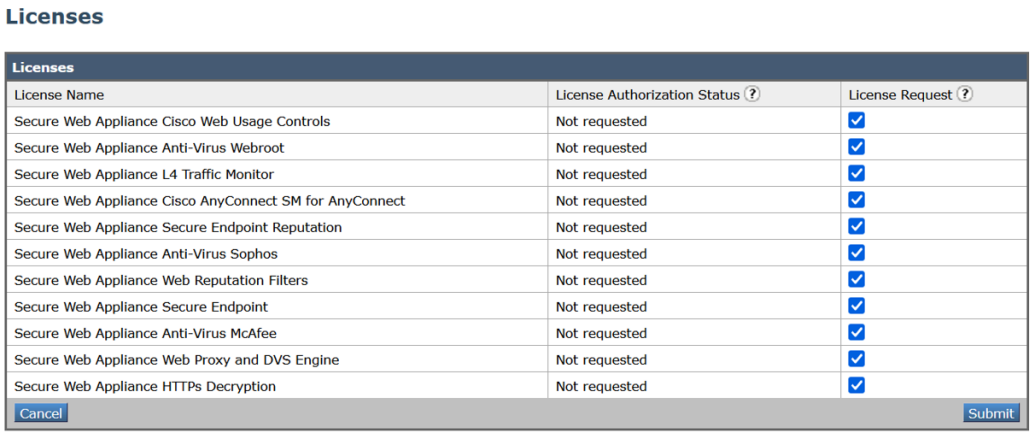
Une fois que vous avez terminé le processus d'enregistrement, vous devez demander des licences pour les fonctionnalités de l'appliance, au besoin.

Étape 1 Choisissez **System Administration > Licenses** (Administration système > Licences).

Étape 2 Cliquez sur **Edit Settings** (Modifier les paramètres).

Étape 3 Cochez les cases sous la colonne License Request/Release (Demande/émission de licence) correspondant aux licences que vous souhaitez demander.

Étape 4 Cliquez sur **Submit** (Soumettre).



Prochaine étape

Lorsque les licences sont utilisées excessivement ou expirent, elles passent en mode non conforme (OOC) et un délai de grâce de 30 jours est accordé pour chaque licence. Vous recevrez des notifications à des intervalles réguliers (le 30e, le 15e, le 5e et le dernier jour) avant l'expiration et à l'expiration du délai de grâce OOC.

Après l'expiration du délai de grâce OOC, vous ne pourrez plus utiliser les licences et les fonctionnalités ne seront pas disponibles. Pour accéder de nouveau aux fonctionnalités, vous devrez mettre à jour les licences sur le portail CSSM et renouveler l'autorisation.

Octroi de licences

Étape 1 Choisissez **System Administration > Licenses** (Administration système > Licences).

Étape 2 Cliquez sur **Edit Settings** (Modifier les paramètres).

Étape 3 Décochez les cases sous la colonne License Request (Demande de licence) correspondant aux licences que vous souhaitez émettre.

Étape 4 Cliquez sur **Submit** (Soumettre).

Annulation de l'enregistrement de l'appliance dans Cisco Smart Software Manager

Étape 1 Choisissez **System Administration > Smart Software Licensing** (Administration système > Licence logicielle Smart).

Étape 2 Dans la liste déroulante **Action**, choisissez **Deregister** (Annuler l'enregistrement) et cliquez sur **Go** (Aller).

Étape 3 Cliquez sur **Submit** (Soumettre).

Réenregistrement de l'appliance dans Cisco Smart Software Manager

Étape 1 Choisissez **System Administration > Smart Software Licensing** (Administration système > Licence logicielle Smart).

Étape 2 Dans la liste déroulante **Action**, choisissez **Reregister** (Réenregistrer), puis cliquez sur **Go** (Aller).

Prochaine étape

Consultez Enregistrement de l'appliance dans Cisco Smart Software Manager , à la page 9 pour en savoir plus sur le processus d'enregistrement.

Vous pouvez réenregistrer l'appliance après avoir réinitialisé les configurations de l'appliance dans des scénarios inévitables.

Modification des paramètres de transport

Vous pouvez modifier les paramètres de transport uniquement avant d'enregistrer l'appliance auprès du CSSM.

Remarque Vous pouvez modifier les paramètres de transport uniquement lorsque la fonction de licence Smart est activée. Si vous avez déjà enregistré votre appliance, vous devez annuler l'enregistrement de l'appliance pour modifier les paramètres de transport. Après avoir modifié les paramètres de transport, vous devez enregistrer à nouveau l'appliance.

Consultez Enregistrement de l'appliance dans Cisco Smart Software Manager , à la page 9 pour savoir comment modifier les paramètres de transport.

Renouvellement de l'autorisation et du certificat

Après avoir enregistré votre appliance auprès de Smart Cisco Software Manager, vous pouvez renouveler le certificat.

Remarque Vous ne pouvez renouveler l'autorisation qu'après l'enregistrement réussi de l'appliance.

Étape 1 Choisissez **System Administration > Smart Software Licensing** (Administration système > Licence logicielle Smart).

Étape 2 Dans la liste déroulante **Action**, choisissez l'option appropriée :

- **Renew Authorization Now** (Renouveler l'autorisation maintenant)
- **Renew Certificates Now** (Renouveler le certificat maintenant)

Étape 3 Cliquez sur **Go** (Aller).

Prochaine étape

Mise à jour de Smart Agent

Pour mettre à jour la version de Smart Agent installée sur votre appliance, procédez comme suit :

Étape 1 Choisissez **System Administration > Smart Software Licensing** (Administration système > Licence logicielle Smart).

Étape 2 Dans la section **Smart Agent Update Status** (État de mise à jour de Smart Agent), cliquez sur **Update Now** (Mettre à jour maintenant) et suivez la procédure.

Remarque Si vous essayez d'enregistrer des modifications de configuration à l'aide de la commande `saveconfig` de l'interface de ligne de commande ou à l'aide de l'interface Web, en sélectionnant **System Administration > Configuration Summary** (Administration système > Résumé de la configuration), la configuration liée aux licences Smart ne sera pas enregistrée.

Alerts (Alertes)

Vous recevrez des notifications dans les scénarios suivants :

- Licence logicielle Smart activée avec succès
- Échec de l'activation de l'octroi de licences logicielles Smart
- Début de la période d'évaluation
- Expiration de la période d'évaluation (à des intervalles réguliers pendant la période d'évaluation et à l'expiration)
- Enregistrement réussi
- Échec de l'enregistrement
- Autorisation réussie
- Échec de l'autorisation
- Désenregistrement réussi
- Échec du désenregistrement
- Certificat d'ID renouvelé avec succès
- Échec du renouvellement du certificat d'ID
- Expiration de l'autorisation
- Expiration du certificat d'ID
- Expiration du délai de grâce de non-conformité (à des intervalles réguliers pendant le délai de grâce et à l'expiration).
- Première instance de l'expiration d'une fonctionnalité

Interface de commande en ligne

license_smart

Description

Configurez la fonction d'octroi de licences logicielles intelligentes.

Utilisation

Commit (Valider) : cette commande nécessite une « validation ».

Batch Command (Commande par lot) : cette commande prend en charge le format par lot. Pour en savoir plus, consultez l'aide en ligne en saisissant la commande : `Help license_smart`.

Exemple : configuration du port pour le service Smart Agent

```
example.com> license_smart
Choose the operation you want to perform:
- ENABLE - Enables Smart Licensing on the product.
- SETAGENTPORT - Set port to run Smart Agent service.
[]> setagentport

Enter the port to run smart agent service.
[65501]>
```

Exemple : activation des licences Smart

```
example.com> license_smart
Choose the operation you want to perform:
- ENABLE - Enables Smart Licensing on the product.
 []> enable
After enabling Smart Licensing on your appliance, follow below steps to activate
the feature keys (licenses):
```

```
a) Register the product with Smart Software Manager using license_smart > register command
 in the CLI.
b) Activate the feature keys using license_smart > requestsmart_license command in the CLI.

Note: If you are using a virtual appliance, and have not enabled any of the
features in the classic licensing mode; you will not be able to activate the
licenses, after you switch to the smart licensing mode. You need to first register
your appliance, and then you can activate the licenses (features) in the smart licensing
mode.
Commit your changes to enable the Smart Licensing mode on your appliance.
All the features enabled in the Classic Licensing mode will be available in the Evaluation
 period.
Type "Y" if you want to continue, or type "N" if you want to use the classic licensing mode
 [Y/N] []> y

> commit

Please enter some comments describing your changes:
[]>
Do you want to save the current configuration for rollback? [Y]>
```

Exemple : enregistrement de l'appliance dans Smart Software Manager

```
example.com> license_smart
To start using the licenses, please register the product.
Choose the operation you want to perform:

- REGISTER - Register the product for Smart Licensing.
- URL - Set the Smart Transport URL.
- STATUS - Show overall Smart Licensing status.
- SUMMARY - Show Smart Licensing status summary.

[]> register
Reregister this product instance if it is already registered [N]> n

Enter token to register the product:
[]>
ODRlOTM5MjItOTQzOS00YjY0LWExZTUtZTdmMmY3OGNlNDZmLTE1MzM3Mzgw%0AMDEzNTR8WlpCQ1lMbGVMQWRx
OXhuenN4OWZDdktFckJLQzF5V3VIbzkyTFgx%0AQWcvaz0%3D%0A
Product Registration is in progress. Use license_smart > status command to check status of
 registration.
```

Exemple : état des licences Smart

```
example.com> license_smart
To start using the licenses, please register the product.
Choose the operation you want to perform:

- REQUESTSMART_LICENSE - Request licenses for the product.
- RELEASESMART_LICENSE - Release licenses of the product.
- REGISTER - Register the product for Smart Licensing.
- URL - Set the Smart Transport URL.
- STATUS - Show overall Smart Licensing status.
- SUMMARY - Show Smart Licensing status summary.

[]> status
Smart Licensing is: Enabled

Evaluation Period: In Use

Evaluation Period Remaining: 89 days 23 hours 53 minutes
Registration Status: Unregistered

License Authorization Status: Evaluation Mode
```

```
Last Authorization Renewal Attempt Status: No Communication Attempted

Product Instance Name: mail.example.com

Transport Settings: Direct (https://smartreceiver.cisco.com/licservice/license)
```

Exemple : résumé de l'état des licences Smart

```
example.com> license_smart
To start using the licenses, please register the product.
Choose the operation you want to perform:
- REGISTER - Register the product for Smart Licensing.
- URL - Set the Smart Transport URL.
- STATUS - Show overall Smart Licensing status.
- SUMMARY - Show Smart Licensing status summary.

[]> summary

FeatureName                                  LicenseAuthorizationStatus
Web Security Appliance Cisco                 Eval
Web Usage Controls
Web Security Appliance Anti-Virus Webroot    Eval
Web Security Appliance Anti-Virus Sophos     Eval
```

Exemple : Définition de l'URL de Smart Transport

```
example.com> license_smart

Choose the operation you want to perform:
- REQUESTSMART_LICENSE - Request licenses for the product.
- RELEASESMART_LICENSE - Release licenses of the product.
- REGISTER - Register the product for Smart Licensing.
- URL - Set the Smart Transport URL.
- STATUS - Show overall Smart Licensing status.
- SUMMARY - Show Smart Licensing status summary.

[]> url

1. DIRECT - Product communicates directly with the cisco license servers
2. TRANSPORT_GATEWAY - Product communicates via transport gateway or smart software manager
 satellite.

Choose from the following menu options:
[1]> 1
Note: The appliance uses the Direct URL
(https://smartreceiver.cisco.com/licservice/license) to communicate with Cisco
Smart Software Manager (CSSM) via the proxy server configured using the updateconfig command.
Transport settings will be updated after commit.
```

Exemple : demande de licences

Remarque Les utilisateurs d'appliances virtuelles doivent enregistrer leur appliance pour demander ou émettre les licences.

```
example.com> license_smart
Choose the operation you want to perform:

- REQUESTSMART_LICENSE - Request licenses for the product.
- RELEASESMART_LICENSE - Release licenses of the product.
- REGISTER - Register the product for Smart Licensing.
```

```
- URL - Set the Smart Transport URL.
- STATUS - Show overall Smart Licensing status.
- SUMMARY - Show Smart Licensing status summary.

[]> requestsmart_license

Feature Name                                    License Authorization Status
1. Web Security Appliance Anti-Virus Sophos      Not Requested
2. Web Security Appliance                        Not requested
   L4 Traffic Monitor

Enter the appropriate license number(s) for activation.
Separate multiple license with comma or enter range:
[]> 1
Activation is in progress for following features:
Web Security Appliance Anti-Virus Sophos
Use license_smart > summary command to check status of licenses.
```

Exemple : octroi de licences

```
example.com> license_smart
Choose the operation you want to perform:

- REQUESTSMART_LICENSE - Request licenses for the product.
- RELEASESMART_LICENSE - Release licenses of the product.
- REGISTER - Register the product for Smart Licensing.
- URL - Set the Smart Transport URL.
- STATUS - Show overall Smart Licensing status.
- SUMMARY - Show Smart Licensing status summary.

[]> releasesmart_license

Feature Name                                  License Authorization Status
1. Web Security Appliance Cisco               Eval
   Web Usage Controls
2. Web Security Appliance                     Eval
   Anti-Virus Webroot
3. Web Security Appliance                     Eval
   L4 Traffic Monitor
4. Web Security Appliance Cisco               Eval
   AnyConnect SM for AnyConnect
5. Web Security Appliance Advanced            Eval
   Malware Protection Reputation
6. Web Security Appliance                     Eval
   Anti-Virus Sophos
7. Web Security Appliance                     Eval
   Web Reputation Filters
8. Web Security Appliance Advanced            Eval
   Malware Protection
```

show_license

- Description, à la page 18
- Exemple : état des licences Smart, à la page 19
- Exemple : résumé de l'état des licences Smart, à la page 19

Description

Affichez l'état des licences Smart et un résumé de l'état.

Exemple : état des licences Smart

```
example.com> showlicense_smart
Choose the operation you want to perform:
- STATUS- Show overall Smart Licensing status.
- SUMMARY - Show Smart Licensing summary.
[]> status
Smart Licensing is: Enabled
Evaluation Period: In Use
Evaluation Period Remaining: 89 days 23 hours 53 minutes
Registration Status: Unregistered
License Authorization Status: Evaluation Mode
Last Authorization Renewal Attempt Status: No Communication Attempted
Product Instance Name: example.com
Transport Settings: Direct (https://smartreceiver.cisco.com/licservice/license)
```

Exemple : résumé de l'état des licences Smart

```
example.com> showlicense_smart
Choose the operation you want to perform:
- STATUS- Show overall Smart Licensing status.
- SUMMARY - Show Smart Licensing summary.

[]> summary

FeatureName                          LicenseAuthorizationStatus
Web Security Appliance Cisco         Eval
Web Usage Controls
Web Security Appliance               Eval
Anti-Virus Webroot
Web Security Appliance               Eval
Anti-Virus Sophos
```

cloudserviceconfig

Description

La commande **cloudserviceconfig** est utilisée pour :

- Activer le portail des services Cisco Cloud sur Secure Web Appliance.
- Désactiver le portail des services Cisco Cloud sur Secure Web Appliance.
- Enregistrer votre Secure Web Appliance sur le portail des services Cisco Cloud.
- Enregistrer automatiquement votre Secure Web Appliance sur le portail des services Cisco Cloud.
- Annuler l'enregistrement de votre Secure Web Appliance sur le portail des services Cisco Cloud.
- Choisissez le serveur Cisco Secure Cloud pour connecter Secure Web Appliance au portail des services Cisco Cloud.
- Téléchargez le certificat et la clé de services Cisco Cloud à partir du portail des services Cisco Talos Intelligence.
- Chargement du certificat client et de la clé

Remarque Cette commande est applicable uniquement en mode de licences Smart.

Utilisation

- **Commit** (Valider) : cette commande ne nécessite pas de « validation ».
- **Batch Command** (Commande par lot) : cette commande prend en charge le format par lot.

Exemple : activation des services Cisco Cloud sur Secure Web Appliance

Dans l'exemple suivant, vous pouvez utiliser la sous-commande `cloudserviceconfig > enable` pour activer les services Cisco Cloud sur Secure Web Appliance

```
example.com > cloudserviceconfig
Choose the operation you want to perform:
- ENABLE - The Cisco Cloud Service is currently disabled on your appliance.
[]> enable
The Cisco Cloud Service is currently enabled on your appliance.
Currently configured Cisco Secure Cloud Server is: api.apj.sse.itd.cisco.com
Available list of Cisco Secure Cloud Servers:
1. AMERICAS (api-sse.cisco.com)
2. APJC (api.apj.sse.itd.cisco.com)
3. EUROPE (api.eu.sse.itd.cisco.com)
Enter Cisco Secure Cloud Server to connect to the Cisco Cloud Service portal.:
[]> 1
Selected Cisco Secure Cloud Server is api-sse.cisco.com.
Make sure you run "commit" to make these changes active.
example.com > commit
Please enter some comments describing your changes:
[]> commit changes
Do you want to save the current configuration for rollback? [Y]>
Changes committed: Tue Dec 29 13:23:19 2020 GMTexample.com >
```

Exemple : désactivation des services Cisco Cloud sur Secure Web Appliance

Dans l'exemple suivant, vous pouvez utiliser la sous-commande `cloudserviceconfig > disable` pour désactiver les services Cisco Cloud sur Secure Web Appliance.

```
example.com > cloudserviceconfig
The appliance is not registered with the Cisco Cloud Service portal.
```

```
Currently configured Cisco Cloud Server is api-sse.cisco.com
Choose the operation you want to perform:
- DISABLE - The Cisco Cloud Service is currently enabled on your appliance.
- REGISTER - To register the appliance with the Cisco Cloud Service portal.
- SETTRS - Set the Cisco Secure Cloud Server to connect to the Cisco Cloud
Service portal.
[]> disable
The Cisco Cloud Service is currently disabled on your appliance.
example.com > commit
Please enter some comments describing your changes:
[]> commit changes
Do you want to save the current configuration for rollback? [Y]>
Changes committed: Tue Dec 29 13:01:07 2020 GMT
example.com >
```

Exemple : enregistrement de Secure Web Appliance sur le portail des services Cisco Cloud

Dans l'exemple suivant, vous pouvez utiliser la sous-commande `cloudserviceconfig > register` pour enregistrer Secure Web Appliance sur le portail des services Cisco Cloud.

Remarque Vous ne pouvez utiliser cette sous-commande que si l'octroi de licences logicielles Smart n'est pas activé et que Secure Web Appliance n'est pas enregistré dans Cisco Smart Software Manager

```
example.com > cloudserviceconfig

Registration/deregistration of the device with cloud service:

Choose the operation you want to perform:
- DISABLE - The Cisco Cloud Service is currently enabled on your appliance.
- REGISTER - To register the appliance with the Cisco Cloud Service portal.
- SETTRS - Set the Cisco Secure Cloud Server to connect to the Cisco Cloud Service portal.
- STATUS - Check the appliance registration status with the Cisco Cloud Service portal.
[]> register

Enter a registration token key to register your appliance
[]> c51fa32bd9a31227eaab50dea873062c

Registering
The Web Security appliance is successfully registered with the Cisco Cloud Service portal.
example.com >
```

Exemple : enregistrement automatique de Secure Web Appliance sur le portail des services Cisco Cloud

Dans l'exemple suivant, vous pouvez utiliser la commande `cloudserviceconfig > autoregister` pour enregistrer Secure Web Appliance auprès du portail des services Cisco Cloud.

```
example.com > cloudserviceconfig

Registration/deregistration of the device with cloud service:

Choose the operation you want to perform:
- AUTOREGISTER - register the appliance with the Cisco Cloud Service portal automatically
using SL Payload.
- SETTRS - Set the Cisco Secure Cloud Server to connect to the Cisco Cloud Service portal.
- STATUS - Check the appliance registration status with the Cisco Cloud Service portal.
[]> autoregister

The Web Security appliance successfully auto-registered with the Cisco Cloud Service portal.
```

Exemple : Désenregistrement de Secure Web Appliance du portail de services Cisco Cloud

Dans l'exemple suivant, vous pouvez utiliser la sous-commande `cloudserviceconfig > deregister` pour annuler l'enregistrement de Secure Web Appliance auprès du portail des services Cisco Cloud.

```
example.com > cloudserviceconfig

Registration/deregistration of the device with cloud service:

Choose the operation you want to perform:
- DISABLE - The Cisco Cloud Service is currently enabled on your appliance.
- DEREGISTER - To deregister the appliance from the Cisco Cloud Service portal.
- STATUS - Check the appliance registration status with the Cisco Cloud Service portal.
[]> deregister

Do you want to deregister your appliance from the Cisco Cloud Service portal.
If you deregister, you will not be able to access the Cloud Service features. [N]> y

The Web Security appliance successfully deregistered from the Cisco Cloud Service portal.
example.com >
```

Exemple : choix du serveur Cisco Secure Cloud pour connecter Secure Web Appliance au portail des services Cisco Cloud

Dans l'exemple suivant, vous pouvez utiliser la sous-commande `cloudserviceconfig > settrs` pour choisir le serveur Cisco Secure Cloud requis pour connecter Secure Web Appliance au portail des services Cisco Cloud.

```
example.com > cloudserviceconfig
The appliance is not registered with the Cisco Cloud Service portal.
Currently configured Cisco Cloud Server is api-sse.cisco.com
Choose the operation you want to perform:
- DISABLE - The Cisco Cloud Service is currently enabled on your appliance.
- REGISTER - To register the appliance with the Cisco Cloud Service portal.
- SETTRS - Set the Cisco Secure Cloud Server to connect to the Cisco Cloud
Service portal.
[]> settrs
Currently configured Cisco Secure Cloud Server is: api-sse.cisco.com
Available list of Cisco Secure Cloud Servers:
1. AMERICAS (api-sse.cisco.com)
2. APJC (api.apj.sse.itd.cisco.com)
3. EUROPE (api.eu.sse.itd.cisco.com)
Enter Cisco Secure Cloud Server to connect to the Cisco Cloud Service portal.:
[]> 3
Selected Cisco Secure Cloud Server is api.eu.sse.itd.cisco.com.
Make sure you run "commit" to make these changes active.
example.com > commit
Please enter some comments describing your changes:
[]> commit changes
Do you want to save the current configuration for rollback? [Y]>
Changes committed: Tue Dec 29 13:37:40 2020 GMT
```

Exemple : téléchargement du certificat et de la clé pour les services Cisco Cloud à partir du portail de services de renseignement Cisco Talos

Dans l'exemple suivant, vous pouvez utiliser la sous-commande `cloudserviceconfig > fetchcertificate` pour télécharger le certificat et la clé des services Cisco Cloud à partir du portail des services Cisco Talos Intelligence.

Remarque Vous ne pouvez utiliser cette sous-commande que lorsque le certificat des services Cisco Cloud existant a expiré et si vous avez enregistré Secure Web Appliance avec Cisco Smart Software Manager.

```
example.com > cloudserviceconfig

Registration/deregistration of the device with cloud service:


Choose the operation you want to perform:
- FETCHCERTIFICATE - Download the Cisco Talos certificate and key
- SETTRS - Set the Cisco Secure Cloud Server to connect to the Cisco Cloud Service portal.
- STATUS - Check the appliance registration status with the Cisco Cloud Service portal.
[]> fetchcertificate

Successfully downloaded the Cisco Talos certificate and key
example.com >
```

Exemple : certificat client (updateconfig)

Dans l'exemple suivant, vous pouvez utiliser la sous-commande `Updateconfig > clientcertificate` pour charger le certificat et la clé.

```
example.com > updateconfig

Service (images):                   Update URL:
-------------------------------------------------------------------------------
Web Reputation Filters              Cisco Servers
Support Request updates             Cisco Servers
Timezone rules                      Cisco Servers
How-Tos Updates                     Cisco Servers
HTTPS Proxy Certificate Lists       Cisco Servers
Cisco AsyncOS upgrades              Cisco Servers
Smart License Agent Updates         Cisco Servers

Service (list):                     Update URL:
-------------------------------------------------------------------------------
Web Reputation Filters              Cisco Servers
Support Request updates             Cisco Servers
Timezone rules                      Cisco Servers
How-Tos Updates                     Cisco Servers
HTTPS Proxy Certificate Lists       Cisco Servers
Cisco AsyncOS upgrades              Cisco Servers
Smart License Agent Updates         Cisco Servers

Update interval for Web Reputation and Categorization: 5m
Update interval for all other services: 5m
Proxy server: not enabled
HTTPS Proxy server: not enabled
Routing table for updates: Management
    The following services will use this routing table:
    - Web Reputation Filters
    - Support Request updates
    - Timezone rules
    - How-Tos Updates
    - HTTPS Proxy Certificate Lists
    - Cisco AsyncOS upgrades
    - Smart License Agent Updates

Upgrade notification: enabled

Choose the operation you want to perform:
- SETUP - Edit update configuration.
- CLIENTCERTIFICATE - Upload the client certificate and key.
- VALIDATE_CERTIFICATES - Validate update server certificates
- TRUSTED_CERTIFICATES - Manage trusted certificates for updates
[]> clientcertificate
```

```
Current Cisco certificate is valid for 179 days

Do you like to overwrite the existing certificate and key [Y|N] ? []> y

Paste the certificate.
Press CTRL-D on a blank line when done.
^D
```

Collez les détails de votre certificat et de votre clé privée. Le certificat et la clé sont stockés avec succès.

Smart Software Licensing Points pour AsyncOS 14.0 et versions ultérieures

- Lorsque l'octroi de licences logicielles Smart est activé et enregistré, le service Cisco Cloud est activé et enregistré automatiquement.
- Si le certificat des services Cisco Cloud a expiré, vous pouvez maintenant télécharger un nouveau certificat à partir du portail des services Cisco Talos Intelligence à l'aide de la sous-commande `cloudserviceconfig > fetchcertificate` de l'interface de ligne de commande.
- Vous ne pouvez pas effectuer l'enregistrement automatique auprès du service Cisco Cloud lorsque la licence Smart est en mode d'évaluation.

Licence pour appliance virtuelle

L'appliance virtuelle Cisco Web Security nécessite une licence supplémentaire pour l'exécuter sur un hôte.

Pour en savoir plus sur les licences d'appliances virtuelles, consultez le *Guide d'installation de Cisco Content Security Virtual Appliance*, disponible à l'adresse http://www.cisco.com/c/en/us/support/security/web-security-appliance/products-installation-guides-list.html.

Note Vous ne pouvez pas ouvrir un tunnel d'assistance technique avant d'installer la licence d'appliance virtuelle.

Après l'expiration de la licence, l'appliance continue de servir de proxy Web sans services de sécurité pendant 180 jours. Aucune mise à jour des services de sécurité n'est effectuée pendant cette période.

Vous pouvez configurer l'appliance de manière à recevoir des alertes concernant l'expiration de la licence.

Thèmes connexes

- Gestion des alertes, on page 36

Installation d'une licence d'appliance virtuelle

Voir le *Guide d'installation de Cisco Content Security Virtual Appliance*, disponible à l'adresse http://www.cisco.com/c/en/us/support/security/web-security-appliance/products-installation-guides-list.html

Activation du redémarrage à distance

Before you begin

- Câblez le port dédié au redémarrage à distance (RPC) directement à un réseau sécurisé. Pour plus d'informations, consultez le guide du matériel pour votre modèle d'appliance. Pour connaître l'emplacement de ce document, consultez Documentation.
- Vérifiez que l'appliance est accessible à distance; par exemple, ouvrez tous les ports nécessaires sur le pare-feu.
- Cette fonction nécessite une adresse IPv4 unique pour l'interface dédiée au redémarrage à distance. Cette interface ne peut être configurée qu'au moyen de la procédure décrite dans cette section; elle ne peut pas être configurée à l'aide de la commande ipconfig.
- Pour redémarrer l'appliance, vous aurez besoin d'un outil tiers capable de gérer les périphériques qui prennent en charge Intelligent Platform Management Interface (IPMI) version 2.0. Assurez-vous d'être prêt à utiliser un tel outil.
- Pour en savoir plus sur l'accès à l'interface de ligne de commande, consultez Interface de commande en ligne

Après avoir configuré la fonction RPC et validé les modifications, attendez 10 à 15 minutes avant d'envoyer les appels à RPC. Secure Web Appliance initialise les services RCP pendant ce temps d'attente.

La possibilité de réinitialiser l'alimentation à distance pour le châssis de l'appliance est disponible sur le matériel séries x80, x90 et x95.

Si vous souhaitez pouvoir redémarrer à distance l'appliance, vous devez activer et configurer cette fonctionnalité au préalable, en utilisant la procédure décrite dans cette section.

Étape 1 Utilisez SSH ou le port de console série pour accéder à l'interface de ligne de commande.

Étape 2 Connectez-vous en utilisant un compte avec accès administrateur.

Étape 3 Saisissez les commandes suivantes :

```
remotepower

Configurer
```

Étape 4 Suivez les invites pour définir les éléments suivants :

- Adresse IP dédiée à cette fonctionnalité, plus le masque réseau et la passerelle.
- Le nom d'utilisateur et la phrase secrète nécessaires pour exécuter la commande de redémarrage.

  Ces informations d'authentification sont indépendantes des autres informations d'authentification utilisées pour accéder à votre appliance.

Étape 5 Saisissez `commit` (valider) pour enregistrer vos modifications.

Étape 6 Testez votre configuration pour vous assurer que vous pouvez gérer l'alimentation de l'appliance à distance.

Étape 7 Assurez-vous que les identifiants que vous avez saisis seront disponibles indéfiniment. Par exemple, rangez ces informations en lieu sûr et assurez-vous que les administrateurs qui peuvent avoir besoin d'effectuer cette tâche ont accès aux informations d'authentification requises.

What to do next

Thèmes connexes

- Appliances matérielles : réinitialisation à distance de l'alimentation des appliances

Administration des comptes d'utilisateur

Les types d'utilisateurs suivants peuvent se connecter à l'appliance pour la gérer :

- **Utilisateurs locaux.** Vous pouvez définir les utilisateurs localement, sur l'appliance même.
- **Utilisateurs définis dans un système externe.** Vous pouvez configurer l'appliance de sorte qu'elle se connecte à un serveur LDAP ou RADIUS externe pour authentifier les utilisateurs qui se connectent à l'appliance.

Note Tout utilisateur que vous définissez peut se connecter à l'appliance par n'importe quelle méthode, par exemple par la connexion à l'interface Web ou par SSH.

Thèmes connexes

- Gestion des comptes d'utilisateur locaux, on page 26
- Authentification des utilisateurs RADIUS, on page 29
- Configuration de l'authentification extérieure par l'intermédiaire d'un serveur LDAP

Gestion des comptes d'utilisateur locaux

Vous pouvez définir n'importe quel nombre d'utilisateurs localement sur Secure Web Appliance.

Le compte d'administrateur système par défaut dispose de tous les privilèges d'administration. Vous pouvez modifier la phrase secrète du compte administrateur, mais vous ne pouvez pas modifier ou supprimer ce compte.

Note Si vous avez perdu la phrase secrète de l'utilisateur admin, communiquez avec votre fournisseur d'assistance Cisco. Pour en savoir plus, consultez Réinitialiser votre mot de passe administrateur et déverrouiller le compte utilisateur administrateur.

Ajout de comptes d'utilisateur locaux

Before you begin

Définissez les exigences relatives à la phrase secrète que tous les comptes d'utilisateur doivent respecter. Consultez Définition des exigences de phrase secrète pour les utilisateurs administratifs , on page 32.

Étape 1 Choisissez **System Administration > Users** (Administration système > Utilisateurs).

Étape 2 Cliquez sur **Add User** (Ajouter un utilisateur).

Étape 3 Saisissez un nom d'utilisateur en respectant les règles suivantes :

- Les noms d'utilisateur peuvent contenir des lettres minuscules, des chiffres et le tiret (-), mais ne peuvent pas commencer par un tiret.
- Les noms d'utilisateur ne peuvent pas dépasser 16 caractères.
- Les noms d'utilisateur ne peuvent pas être des noms spéciaux réservés par le système, comme « operator » ou « root ».
- Si vous utilisez également l'authentification extérieure, les noms d'utilisateurs ne doivent pas dupliquer des noms d'utilisateurs authentifiés en externe.

Étape 4 Saisissez le nom complet de l'utilisateur.

Étape 5 Sélectionnez un type d'utilisateur

Type d'utilisateur	Description
Administrateur	Autorise l'accès complet à tous les paramètres de configuration du système. Cependant, les commandes de l'interface de ligne de commande `upgradecheck` et `upgradeinstall` ne peuvent être exécutées qu'à partir du compte « admin » défini par le système.
Opérateur	Empêche les utilisateurs de créer, de modifier ou de supprimer des comptes d'utilisateur. Le groupe Opérateurs restreint également l'utilisation des commandes suivantes de l'interface de ligne de commande : • `resetconfig` • `upgradecheck` • `upgradeinstall` Le groupe des opérateurs restreint également l'utilisation de l'Assistant de configuration du système.

Type d'utilisateur	Description
Opérateur en lecture seule	Les comptes utilisateur possédant ce rôle : • Peuvent afficher les informations de configuration. • Peuvent effectuer et envoyer des modifications pour voir comment configurer une fonctionnalité, mais ne peuvent pas les valider. • Ne peuvent pas apporter d'autres modifications à l'appliance, comme effacer le cache ou enregistrer des fichiers. • Ne peuvent pas accéder au système de fichiers, au FTP ou au SCP.
Invité	Les utilisateurs du groupe des invités peuvent uniquement afficher les informations sur l'état du système, y compris les rapports et le suivi.

Étape 6 Saisissez ou générez une phrase secrète.

Étape 7 Envoyez et validez vos modifications.

Suppression de comptes d'utilisateur

Étape 1 Choisissez **System Administration > Users** (Administration système > Utilisateurs).

Étape 2 Cliquez sur l'icône de la corbeille correspondant au nom d'utilisateur indiqué et confirmez lorsque vous y êtes invité.

Étape 3 Envoyez et validez vos modifications.

Modifications de comptes d'utilisateur

Étape 1 Choisissez **System Administration > Users** (Administration système > Utilisateurs).

Étape 2 Cliquez sur le nom d'utilisateur.

Étape 3 Apportez les modifications nécessaires à l'utilisateur sur la page Edit User (Modifier l'utilisateur).

Étape 4 Envoyez et validez vos modifications.

Modification des phrases secrètes

Pour modifier la phrase secrète du compte actuellement connecté, sélectionnez **Options > Change Passphrase** (Options > Modifier la phrase secrète) dans le coin supérieur droit de la fenêtre.

Pour les autres comptes, modifiez le compte et la phrase secrète dans la page Local User Settings (Paramètres de l'utilisateur local).

Thèmes connexes

• Modifications de comptes d'utilisateur, on page 28

• Définition des exigences de phrase secrète pour les utilisateurs administratifs , on page 32

Configuration de paramètres restrictifs de comptes d'utilisateur et de phrases secrètes

Vous pouvez définir des restrictions de compte d'utilisateur et de phrase secrète pour appliquer les politiques de phrase secrète de l'entreprise. Les restrictions liées au compte d'utilisateur et à la phrase secrète s'appliquent aux utilisateurs locaux définis sur l'appliance Cisco. Vous pouvez configurer les paramètres suivants :

- **Verrouillage du compte d'utilisateur.** Vous pouvez définir le nombre de tentatives de connexion infructueuses entraînant le blocage de l'accès du compte à l'utilisateur. Vous pouvez définir le nombre de tentatives de connexion de l'utilisateur entre 1 et 60. La valeur par défaut est égale à 5.
- **Règles relatives à la durée de vie des phrases secrètes.** Vous pouvez définir la durée de vie d'une phrase secrète avant que l'utilisateur ne soit tenu de la modifier après s'être connecté.
- **Règles relatives aux phrases secrètes.** Vous pouvez définir les types de phrase secrète que les utilisateurs peuvent choisir, par exemple les caractères facultatifs ou obligatoires.

Remarque À partir de la version 14.0 d'AsyncOS, les règles de phrase secrète sont activées par défaut, à l'exception du **refus de 3 caractères répétitifs ou séquences supérieurs dans les phrases secrètes** et **de la liste de mots à interdire dans les règles de phrase secrète**.

- **Force des phrases secrètes.** Vous pouvez afficher un indicateur de force de phrase secrète lorsqu'un utilisateur administrateur saisit une nouvelle phrase secrète.

  Pour en savoir plus, consultez Définition des exigences de phrase secrète pour les utilisateurs administratifs .

Vous définissez les restrictions de compte d'utilisateur et de phrase secrète sur la page System Administration > Users (Administration système > Utilisateurs) dans la section Local User Account and Passphse Settings (Paramètres de compte d'utilisateur local et de phrase secrète).

Authentification des utilisateurs RADIUS

Secure Web Appliance peut utiliser un service d'annuaire RADIUS pour authentifier les utilisateurs qui se connectent à l'appliance à l'aide de HTTP, HTTPS, SSH et FTP. Vous pouvez configurer l'appliance pour contacter plusieurs serveurs externes aux fins d'authentification, en utilisant l'authentification PAP ou CHAP. Vous pouvez mapper des groupes d'utilisateurs externes sur différents types de rôles utilisateur Secure Web Appliance.

Séquence des événements pour l'authentification Radius

Lorsque l'authentification extérieure est activée et qu'un utilisateur se connecte à Secure Web Appliance, l'appliance :

1. Détermine si l'utilisateur est le compte « admin » défini par le système.
2. Sinon, vérifie le premier serveur externe configuré pour déterminer si l'utilisateur y est défini.
3. Si l'appliance ne peut pas se connecter au premier serveur externe, elle vérifie le serveur externe suivant dans la liste.

4. Si l'appliance ne peut pas se connecter à un serveur externe, elle tente d'authentifier l'utilisateur en tant qu'utilisateur local, défini sur la Secure Web Appliance.
5. Si l'utilisateur n'existe sur aucun serveur externe ou sur l'appliance, ou si l'utilisateur saisit la mauvaise phrase secrète, l'accès à l'appliance est refusé.

Activation de l'authentification extérieure à l'aide de RADIUS

Étape 1 Dans la page **System Administration > Users** (Administration système > Utilisateurs), cliquez sur **Enable External Authentication** (Activer l'authentification extérieure).

Étape 2 Choisissez **RADIUS** dans le champ Authentication Type (Type d'authentification).

Étape 3 Saisissez le nom d'hôte, le numéro de port et la phrase secrète du secret partagé pour le serveur RADIUS. Le port par défaut est `1812`.

Étape 4 Saisissez le nombre de secondes pendant lesquelles l'appliance doit attendre une réponse du serveur avant d'expirer.

Étape 5 Choisissez le protocole d'authentification utilisé par le serveur RADIUS.

Étape 6 (Facultatif) Cliquez sur **Add Row** (Ajouter une ligne) pour ajouter un autre serveur RADIUS. Répétez les **étapes 1 à 5** pour chaque serveur RADIUS.

Note Vous pouvez ajouter jusqu'à dix serveurs RADIUS.

Étape 7 Dans le champ **External Authentication Cache Timeout** (Délai d'expiration du cache d'authentification extérieure), saisissez le nombre de secondes pendant lesquelles AsyncOS stocke les informations d'authentification extérieure avant de recontacter le serveur RADIUS pour s'authentifier à nouveau. La valeur par défaut est zéro.

Note Si le serveur RADIUS utilise des phrases secrètes à usage unique, par exemple des phrase secrètes créées à partir d'un jeton, saisissez zéro (0). Lorsque la valeur est définie sur zéro, AsyncOS ne contacte pas à nouveau le serveur RADIUS pour s'authentifier pendant la session en cours.

Étape 8 Configure Group Mapping (Configuration du mappage de groupe) : sélectionnez s'il faut mapper tous les utilisateurs authentifiés en externe sur le rôle administrateur ou sur différents types de rôles utilisateur de l'appliance.

Paramètres	Description
Map externally authenticated users to multiple local roles (Mapper les utilisateurs authentifiés de l'extérieur sur plusieurs rôles locaux)	Saisissez un nom de groupe tel que défini dans l'attribut RADIUS CLASS et choisissez un type de rôle pour l'appliance. Vous pouvez ajouter d'autres mappages de rôles en cliquant sur Ajouter une ligne. AsyncOS affecte les utilisateurs RADIUS aux rôles dans l'appliance en fonction de l'attribut CLASS de RADIUS. Exigences de l'attribut CLASS : • au moins trois caractères • 253 caractères maximum • Pas de deux-points, de virgules ni de caractères de nouvelle ligne • Un ou plusieurs attributs CLASS mappés pour chaque utilisateur RADIUS (avec ce paramètre, AsyncOS refuse l'accès aux utilisateurs RADIUS sans attribut CLASS mappé.) Si les utilisateurs RADIUS ont plusieurs attributs CLASS, AsyncOS attribue le rôle le plus restrictif. Par exemple, si un utilisateur RADIUS a deux attributs CLASS, qui sont mappés sur les rôles Opérateur et Opérateur en lecture seule, AsyncOS affecte l'utilisateur RADIUS au rôle Opérateur en lecture seule, qui est plus restrictif que le rôle Opérateur. Voici les rôles de l'appliance, classés du plus restrictif au moins restrictif : • Administrateur • Opérateur • Opérateur en lecture seule • Invité
Map all externally authenticated users to the Administrator role (Mapper tous les utilisateurs authentifiés en externe sur le rôle administrateur).	AsyncOS affecte à tous les utilisateurs RADIUS le rôle administrateur.

Étape 9 Envoyez et validez vos modifications.

What to do next

Thèmes connexes

- Authentification extérieure
- Ajout de comptes d'utilisateur locaux, on page 27.

Définition des préférences des utilisateurs

Les paramètres de préférences, tels que les formats d'affichage des rapports, sont stockés pour chaque utilisateur et sont identiques, quel que soit l'ordinateur client à partir duquel l'utilisateur se connecte à l'appliance.

Étape 1 Choisissez **Options > Preferences** (Options > Préférences).

Étape 2 Dans la page User Preferences (Préférences de l'utilisateur), cliquez sur **Edit Preferences** (Modifier les préférences).

Étape 3 Configurez les paramètres de préférences selon vos besoins.

Paramètre de préférence	Description
Language Display (Langue d'affichage)	Langue utilisée par AsyncOS pour le Web dans l'interface Web et l'interface de ligne de commande.
Landing Page (Page de destination)	Page qui s'affiche lorsque l'utilisateur se connecte à l'appliance.
Reporting Time Range Displayed (Affichage de la plage de temps des rapports) (valeur par défaut)	La plage de temps par défaut qui s'affiche pour les rapports sous l'onglet Reporting (Rapports).
Number of Reporting Rows Displayed (Nombre de lignes de rapport affichées)	Le nombre de lignes de données affichées par défaut pour chaque rapport.

Étape 4 Envoyez et validez vos modifications.

Configuration des paramètres d'administrateur

Définition des exigences de phrase secrète pour les utilisateurs administratifs

Pour définir les exigences de phrase secrète pour les utilisateurs administratifs de l'appliance définis localement :

Étape 1 Sélectionnez **System Administration > Users** (Administration système > Utilisateurs).

Étape 2 Dans la section **Passphrase Settings** (Paramètres de la phrase secrète), cliquez sur **Edit Settings** (Modifier les paramètres).

Étape 3 Choisissez les options :

Option	Description
List of words to disallow in passphrases (Liste de mots à interdire dans les phrases secrètes)	Créez un fichier.txt avec chaque mot interdit sur une ligne distincte, puis sélectionnez le fichier pour le charger. Les téléchargements suivants remplacent les téléchargements précédents.

Option	Description
Passphrase Strength (Force des phrases secrètes)	Vous pouvez afficher un indicateur de force de phrase secrète lorsqu'un utilisateur administrateur saisit une nouvelle phrase secrète. Ce paramètre n'applique pas la création de phrase secrète sécurisée, il montre simplement à quel point il est facile de deviner la phrase secrète saisie. Sélectionnez les rôles pour lesquels vous souhaitez afficher l'indicateur. Pour chaque rôle sélectionné, entrez ensuite une valeur supérieure à zéro. Un nombre élevé signifie qu'une phrase secrète enregistrée comme forte est plus difficile à deviner. Ce paramètre n'a pas de valeur maximale, mais un nombre très élevé rend impossible la saisie d'une phrase secrète jugée « bonne ». Faites des essais pour voir quel nombre correspond le mieux à vos besoins. La force de la phrase secrète est mesurée sur une échelle logarithmique. L'évaluation est basée sur les règles d'entropie du National Institue of Standards and Technology des États-Unis, comme défini dans la norme NIST SP 800-63, section Troubleshooting. En général, les phrases secrètes sont plus strictes : • Elles sont longues. • Elles sont composées de majuscules, de minuscules, de chiffres et de caractères spéciaux. • Elles ne comprennent pas de mots figurant dans un dictionnaire, quelle que soit la langue. Pour appliquer des phrases secrètes ayant ces caractéristiques, utilisez les autres paramètres sur cette page.

Étape 4 Envoyez et validez vos modifications.

Paramètres de sécurité supplémentaires pour l'accès à l'appliance

Vous pouvez utiliser la commande `adminaccessconfig` de l'interface de ligne de commande pour configurer Secure Web Appliance afin d'avoir des exigences d'accès plus strictes pour les administrateurs qui se connectent à l'appliance.

Commande	Description
`adminaccessconfig > banner`	Configure l'appliance pour afficher le texte que vous spécifiez lorsqu'un administrateur tente de se connecter. La bannière de connexion personnalisée s'affiche lorsqu'un administrateur accède à l'appliance par une interface; par exemple, par l'interface utilisateur Web, l'interface de ligne de commande ou le FTP. Vous pouvez charger le texte personnalisé en le copiant dans l'invite de l'interface de ligne de commande ou en le copiant à partir d'un fichier texte situé sur Secure Web Appliance. Pour charger le texte à partir d'un fichier, vous devez d'abord transférer le fichier vers le répertoire de configuration de l'appliance à l'aide du protocole FTP.
`adminaccessconfig > welcome`	Il s'agit d'une bannière après la connexion, qui s'affiche après une connexion réussie de l'administrateur. Ce texte est ajouté à la configuration de l'appliance par les mêmes moyens que le texte de connexion `adminaccessconfig > banner`.
`adminaccessconfig > ipaccess`	Contrôle les adresses IP des administrateurs pour accéder à Secure Web Appliance. Les administrateurs peuvent accéder à l'appliance à partir de n'importe quelle ordinateur ou à partir d'ordinateurs dotés d'une adresse IP figurant dans une liste que vous définissez. Lorsque vous restreignez l'accès à une liste d'autorisation, vous pouvez spécifier des adresses IP, des sous-réseaux ou des adresses CIDR. Par défaut, lorsque vous répertoriez les adresses qui peuvent accéder à l'appliance, l'adresse IP de votre appliance actuelle est répertoriée comme première adresse dans la liste d'autorisation. Vous ne pouvez pas supprimer l'adresse IP de votre appliance actuelle de la liste d'autorisation. Ces informations peuvent également être fournies à l'aide de l'interface utilisateur Web; voir Accès au réseau de l'utilisateur, on page 35.
`adminaccessconfig - csrf`	Activez/désactivez la protection contre la falsification des demandes intersites de l'interface utilisateur Web, utilisée pour identifier et protéger contre les demandes malveillantes ou frauduleuses. Pour une sécurité optimale, il est recommandé d'activer la protection CSRF.
`adminaccessconfig > hostheader`	Configurez l'utilisation de l'en-tête host dans les demandes HTTP. Par défaut, l'interface utilisateur Web répond par l'en-tête d'hôte envoyé par le client Web dans une requête HTTP. Pour une sécurité accrue, vous pouvez configurer l'interface utilisateur Web de manière à répondre uniquement par le nom d'hôte propre à l'appliance, c'est-à-dire le nom configuré de l'appliance (par exemple, `wsa_04.local`).
`adminaccessconfig > timeout`	Indiquez un intervalle d'expiration de délai d'inactivité; c'est-à-dire le nombre de minutes pendant lesquelles les utilisateurs peuvent être inactifs avant d'être déconnectés. Cette valeur peut être comprise entre 5 et 1 440 minutes (24 heures). La valeur par défaut est de 30 minutes. Ces informations peuvent également être fournies à l'aide de l'interface utilisateur Web; voir Accès au réseau de l'utilisateur, on page 35.

Commande	Description
`adminaccessconfig > how-tos`	Activez des procédures pas à pas qui vous aident à accomplir des tâches de configuration spécifiques.
`adminaccessconfig > strictssl`	Configure l'appliance pour que les administrateurs se connectent à l'interface Web sur le port 8443 à l'aide de chiffrements SSL plus forts (chiffrement supérieur à 56 bits). Lorsque vous configurez l'appliance pour exiger des chiffrements SSL plus forts, la modification s'applique uniquement aux administrateurs accédant à l'appliance à l'aide du protocole HTTPS pour gérer l'appliance. Elle ne s'applique pas aux autres trafics réseau connectés au proxy Web à l'aide de HTTPS.
`adminaccessconfig > loginhistory`	Configurez le nombre de jours pendant lesquels l'historique de connexion est conservé.
`adminaccessconfig > maxsessions`	Configurez le nombre maximal de sessions de connexion simultanées (CLI et interface Web).

Accès au réseau de l'utilisateur

Vous pouvez spécifier combien de temps un utilisateur peut être connecté à l'appliance avant qu'AsyncOS ne déconnecte l'utilisateur pour cause d'inactivité. Vous pouvez également indiquer le type de connexions utilisateur autorisées.

L'expiration de la session s'applique à tous les utilisateurs, y compris les administrateurs, connectés à l'interface utilisateur Web ou à l'interface de ligne de commande. Si AsyncOS déconnecte un utilisateur, celui-ci est redirigé vers la page de connexion de l'appliance.

Remarque Vous pouvez également utiliser l'interface de ligne de commande `adminaccessconfig > timeout` pour définir cette valeur d'expiration.

Étape 1 Choisissez **System Administration** > **Network Access** (Administration système > Accès au réseau).

Étape 2 Cliquez sur **Edit Settings** (Modifier les paramètres).

Étape 3 Dans le champ **Session Inactivity Timeout** (Délai d'expiration pour inactivité de session), saisissez le nombre de minutes que les utilisateurs peuvent être inactifs avant d'être déconnectés.

Vous pouvez définir un intervalle d'expiration entre cinq et 1 440 minutes (24 heures); la valeur par défaut est 30 minutes.

Étape 4 Dans la section **User Access** (Accès de l'utilisateur), vous contrôlez l'accès au système des utilisateurs : choisissez **Allow Any Connection** (Autoriser toute connexion) ou **Only Allow Specific Connections** (Autoriser uniquement des connexions spécifiques).

Si vous choisissez **Only Allow Specific Connections** (Autoriser uniquement des connexions spécifiques), définissez les connexions spécifiques en tant qu'adresses IP, plages d'adresses IP ou plages d'adresse CIDR. Outre l'adresse IP du client, l'adresse IP de l'appliance est automatiquement ajoutée dans la section **User Access** (Accès de l'utilisateur).

Étape 5 Envoyez et validez vos modifications.

Réinitialisation de la phrase secrète de l'administrateur

Before you begin

- Si vous ne connaissez pas la phrase secrète du compte administrateur, communiquez avec votre agent d'assistance client pour réinitialiser la phrase secrète.
- Sachez que les modifications de la phrase secrète prennent effet immédiatement et vous n'êtes pas tenu de les valider.

Tout utilisateur de niveau administrateur peut modifier la phrase secrète de l'utilisateur « admin ».

Étape 1 Sélectionnez **Management Appliance** > **System Administration** > **Users** (Appliance de gestion > Administration système > Utilisateurs).

Étape 2 Cliquez sur le lien **admin** dans la liste Users (Utilisateurs).

Étape 3 Sélectionnez **Change the passphrase** (Modifier la phrase secrète).

Étape 4 Générez ou saisissez la nouvelle phrase secrète.

Configuration de l'adresse de retour pour les messages générés

Vous pouvez configurer l'adresse de retour des courriels générés par AsyncOS pour les rapports.

Étape 1 Choisissez **System Administration > Return Addresses** (Administration système > Adresses de retour).

Étape 2 Cliquez sur **Edit Settings** (Modifier les paramètres).

Étape 3 Saisissez le nom d'affichage, le nom d'utilisateur et le nom de domaine.

Étape 4 Envoyez et validez vos modifications.

Gestion des alertes

Les alertes sont des notifications par courriel contenant des renseignements sur les événements se produisant sur Secure Web Appliance. Ces événements peuvent être de différents niveaux d'importance (ou de gravité), de mineur (informatif) à majeur (critique) et concernent généralement un composant ou une fonctionnalité spécifique de l'appliance.

Note Pour recevoir des alertes et des notifications par courriel, vous devez configurer l'hôte de relais SMTP que l'appliance utilise pour envoyer les courriels.

Classifications et gravités des alertes

Les informations contenues dans une alerte sont déterminées par une classification d'alerte et un niveau de gravité. Vous pouvez préciser quelles classifications d'alertes et quel niveau de gravité sont envoyés à n'importe quel destinataire d'alerte.

Classifications des alertes

AsyncOS envoie les types d'alertes suivants :

- System (Système)
- Matériel
- Programme de mise à jour
- Proxy Web
- Protection contre les programmes malveillants
- AMP
- L4 Traffic Monitor (Supervision du trafic de la couche 4)
- Catégories d'URL externes
- Expiration de la politique

Alert Severities (Gravités des alertes)

Des alertes peuvent être envoyées pour les gravités suivantes :

- **Critical** (Critique) : nécessite une attention immédiate.
- **Warning** (Avertissement) : problème ou erreur nécessitant une supervision supplémentaire et une attention potentiellement immédiate.
- **Information** : informations générées dans le cadre du fonctionnement de routine de cet appareil.

Gestion des destinataires des alertes

Note Si vous avez activé AutoSupport (AutoAssistance) lors de la configuration du système, l'adresse de messagerie que vous avez spécifiée recevra des alertes pour toutes les gravités et toutes les classes par défaut. Vous pouvez modifier cette configuration à tout moment.

Ajout et modification de destinataires d'alertes

Étape 1 Choisissez **System Administration > Alerts** (Administration système > Alertes).

Étape 2 Cliquez sur un destinataire dans la liste des destinataires des alertes pour le modifier ou cliquez sur **Add Recipient** (Ajouter un destinataire) pour ajouter un nouveau destinataire.

Étape 3 Ajoutez ou modifiez l'adresse de messagerie du destinataire. Il est possible d'entrer des adresses multiples, séparées par des virgules.

Étape 4 Sélectionnez les gravités d'alerte à recevoir pour chaque type d'alerte.

Étape 5 Envoyez et validez vos modifications.

Suppression de destinataires d'alertes

Étape 1 Choisissez **System Administration > Alerts** (Administration système > Alertes).

Étape 2 Cliquez sur l'icône de la corbeille correspondant au destinataire de l'alerte dans la liste des destinataires des alertes, puis confirmez.

Étape 3 Validez vos modifications.

Configuration des paramètres d'alerte

Les paramètres d'alertes sont des paramètres globaux, ce qui signifie qu'ils affectent le comportement de toutes les alertes.

Étape 1 Choisissez **System Administration > Alerts** (Administration système > Alertes).

Étape 2 Cliquez sur **Edit Settings** (Modifier les paramètres).

Étape 3 Configurez les paramètres d'alerte selon les besoins.

Option	Description
Adresse de l'expéditeur à utiliser lors de l'envoi d'alertes	L'adresse « Header from: » conforme à RFC 2822 à utiliser pour l'envoi d'alertes. Une option est fournie pour générer automatiquement une adresse en fonction du nom d'hôte du système (« alert@<hostname> »)

Option	Description
Attendez avant d'envoyer une alerte en double	Indique l'intervalle de temps pour les alertes en double. Il existe deux paramètres : **Initial Number of Seconds to Wait Before Sending a Duplicate Alert** (Nombre initial de secondes à attendre avant d'envoyer une alerte en double). Si vous réglez cette valeur sur 0, les résumés d'alertes en double ne sont pas envoyés mais toutes les alertes en double sont envoyées sans délai (une grande quantité de courriels peut être générée sur une courte période). Le nombre de secondes à attendre entre l'envoi d'alertes en double (intervalle d'alerte) augmente après l'envoi de chaque alerte. L'augmentation correspond au nombre de secondes d'attente plus deux fois le dernier intervalle. Ainsi, une attente de 5 secondes verrait les alertes envoyées à 5 secondes, 15, secondes, 35 secondes, 75 secondes, 155 secondes, 315 secondes, etc. **Maximum Number of Seconds to Wait Before Sending a Duplicate Alert** (Nombre maximal de secondes à attendre avant d'envoyer une alerte en double). Vous pouvez définir un nombre maximal de secondes d'attente entre les intervalles de la valeur du nombre maximal de secondes à attendre avant d'envoyer un champ d'alerte en double. Par exemple, si vous définissez la valeur initiale à 5 secondes et la valeur maximale à 60 secondes, des alertes seront envoyées après 5 secondes, 15 secondes, 35 secondes, 60 secondes, 120 secondes, etc.

Note À partir d'AsyncOS 12.0, l'option Cisco AutoSupport est supprimée des paramètres d'alerte. Vous pouvez uniquement activer ou désactiver la fonctionnalité AutoSupport en utilisant l'interface de ligne de commande **alertconfig**.

Étape 4 Envoyez et validez vos modifications.

Listes des alertes

Les sections suivantes répertorient les alertes par classification. Le tableau dans chaque section comprend le nom de l'alerte (descripteur utilisé en interne), le texte de l'alerte, la description, la gravité (critique, information ou avertissement) et les paramètres (le cas échéant) inclus dans le texte du message.

Alertes matérielles

Le tableau suivant contient une liste des différentes alertes matérielles qui peuvent être générées par AsyncOS, y compris une description de l'alerte et de sa gravité :

Message	Gravité de l'alerte	Paramètres
Un événement RAID est survenu : $error	Avertissement	**$error :** le texte de l'erreur RAID.

Alertes système

Le tableau suivant contient une liste des différentes alertes du système qui peuvent être générées par AsyncOS, y compris une description de l'alerte et de sa gravité :

Message	Gravité de l'alerte	Paramètres
Script de démarrage $name sorti avec l'erreur : $message	Critique.	**$name :** nom du script. **$message :** texte du message d'erreur.
Échec de l'arrêt du système : $exit_status : $output',	Critique.	**$exit_status :** code de sortie de la commande. **$output :** sortie de la commande.
Échec du redémarrage du système : $exit_status : $output	Critique.	**$exit_status :** code de sortie de la commande. **$output :** sortie de la commande.
Le processus $name a répertorié la $dependency comme dépendance, mais elle n'existe pas.	Critique.	**$name :** nom du processus. **$dependency :** nom de la dépendance répertoriée.
Le processus $name a répertorié la $dependency comme une dépendance, mais la $dependency n'est pas un processus allow_init.	Critique.	**$name :** nom du processus. **$dependency :** nom de la dépendance répertoriée.
Le processus $name s'est répertorié comme une dépendance.	Critique.	**$name :** nom du processus.
Le processus $name a répertorié la $dependency comme dépendance à plusieurs reprises.	Critique.	**$name :** nom du processus. **$dependency :** nom de la dépendance répertoriée.
Cycle de dépendance détecté : $cycle.	Critique.	**$cycle :** la liste des noms de processus impliqués dans le cycle.
Une erreur s'est produite lors de la tentative de partage de données statistiques à l'aide de la fonctionnalité de participation au réseau. Veuillez transmettre ces informations de suivi à votre fournisseur d'assistance : Erreur : $error.	Avertissement.	**$error :** message d'erreur associé à l'exception.
Il y a une erreur avec « $name ».	Critique.	**$name :** nom du processus qui a généré un fichier principal.
Une erreur d'application est survenue : « $error »	Critique.	**$error :** le texte de l'erreur, généralement un retour en arrière.

Message	Gravité de l'alerte	Paramètres
Appliance : $appliance, Utilisateur : $username, IP source : $ip, Événement : compte verrouillé en raison de X tentatives de connexion infructueuses. L'utilisateur $username a été verrouillé après X échecs de connexion consécutifs. La dernière tentative de connexion datait de $ip.	de l'autre partie.	**$appliance** : identifiant de l' Secure Web Appliance spécifique. **$username** : Identifiant du compte d'utilisateur spécifique. **$ip** : l'adresse IP à partir de laquelle la tentative de connexion a eu lieu.
Assistance technique : le tunnel de service a été activé, le port $port	de l'autre partie.	**$port :** numéro de port utilisé pour le tunnel de service.
Assistance technique : le tunnel de service a été désactivé.	de l'autre partie.	Sans objet.
• L'hôte $ip a été ajouté à la liste des personnes bloquées en raison d'une attaque SSH DOS. • L'hôte de $ip a été ajouté de façon permanente à la liste des autorisations SSH. • L'hôte à l'adresse $ip a été supprimé de la liste des hôtes bloqués.	Avertissement.	**$ip** : adresse IP à partir de laquelle une tentative de connexion a eu lieu. **Description :** Les adresses IP qui tentent de se connecter à l'appliance par SSH, mais qui ne fournissent pas d'informations d'authentification valides, sont ajoutées à la liste des utilisateurs bloqués SSH si plus de 10 tentatives se soldent par un échec en l'espace de deux minutes. Lorsqu'un utilisateur se connecte avec succès à partir de la même adresse IP, cette adresse IP est ajoutée à la liste des personnes autorisées. Les adresses figurant dans la liste des adresses autorisée sont autorisées à accéder même si elles figurent aussi dans la liste des adresses bloquées. Les entrées sont automatiquement supprimées de la liste des personnes bloquées après environ une journée.

Note Les alertes du système comprennent les alertes de clés de fonctionnalité, les alertes de journalisation et les alertes de rapports. Vous recevrez ces alertes après les avoir configurées dans les alertes du système.

Alertes liées aux clés de fonctionnalité

Le tableau suivant contient une liste des différentes alertes de clés de fonctionnalité qui peuvent être générées par AsyncOS, notamment la description de l'alerte et sa gravité :

Message	Gravité de l'alerte	Paramètres
Une clé « $feature » a été téléchargée à partir du serveur de clés et placée dans la zone en attente. Acceptation du CLUF requise.	de l'autre partie.	**$feature :** nom de la fonctionnalité.
Votre clé d'évaluation « $feature » a expiré. Veuillez communiquer avec votre représentant Cisco autorisé.	Avertissement.	**$feature :** nom de la fonctionnalité.
Votre clé d'évaluation « $feature » expirera dans moins de $days jour(s). Veuillez communiquer avec votre représentant Cisco autorisé.	Avertissement.	**$feature :** nom de la fonctionnalité. **$days :** le nombre de jours qui s'écoulent avant l'expiration de la clé de fonctionnalité.

Journalisation des alertes

Le tableau suivant contient une liste des différentes alertes de journalisation qui peuvent être générées par AsyncOS, notamment une description de l'alerte et sa gravité :

Message	Gravité de l'alerte	Paramètres
$error.	de l'autre partie.	**$error :** chaîne de recherche de la source de l'erreur.
Erreur de journal : Abonnement $name : La partition du journal est pleine.	Critique.	**$name :** Nom de l'abonnement au journal.
Erreur de journal : Erreur de transmission pour l'abonnement $name : La connexion à $ip a échoué : $reason.	Critique.	**$name :** Nom de l'abonnement au journal. **$ip :** Adresse IP de l'hôte distant. **$reason :** Texte décrivant l'erreur de connexion
Erreur de journal : Erreur de transmission pour l'abonnement $name : Une commande FTP a échoué sur $ip : $reason.	Critique.	**$name :** Nom de l'abonnement au journal. **$ip :** Adresse IP de l'hôte distant. **$reason :** Texte décrivant ce qui n'a pas fonctionné.

Message	Gravité de l'alerte	Paramètres
Erreur de journal : Erreur de transmission pour l'abonnement $name : SCP n'a pas pu être transféré vers $ip:$port : $reason.	Critique.	**$name :** Nom de l'abonnement au journal. **$ip :** Adresse IP de l'hôte distant. **$port :** Numéro de port sur l'hôte distant. **$reason :** Texte décrivant ce qui n'a pas fonctionné.
Erreur de journal : Abonnement $name : Échec de la connexion à $hostname ($ip) : $error.	Critique.	**$name :** Nom de l'abonnement au journal. **$hostname :** Nom d'hôte du serveur syslog. **$ip :** Adresse IP du serveur Syslog. **$error :** Texte du message d'erreur.
Erreur de journal : Abonnement $name : Erreur de réseau lors de l'envoi des données du journal au serveur syslog $hostname ($ip) : $error	Critique.	**$name :** Nom de l'abonnement au journal. **$hostname :** Nom d'hôte du serveur syslog. **$ip :** Adresse IP du serveur Syslog. **$error :** Texte du message d'erreur.
Abonnement $name : Expiré $timeout secondes après l'envoi de données au serveur syslog $hostname ($ip).	Critique.	**$name :** Nom de l'abonnement au journal. **$timeout :** Délai d'expiration (en secondes) **$hostname :** Nom d'hôte du serveur syslog. **$ip :** Adresse IP du serveur Syslog.
Abonnement $name : Le serveur Syslog $hostname ($ip) n'accepte pas les données assez rapidement.	Critique.	**$name :** Nom de l'abonnement au journal. **$hostname :** Nom d'hôte du serveur syslog. **$ip :** Adresse IP du serveur Syslog.

Message	Gravité de l'alerte	Paramètres
Abonnement $name : Le ou les fichiers de journaux les plus anciens ont été supprimés, car les fichiers journaux ont atteint le nombre maximal de $max_num_files. Les fichiers supprimés sont les suivants : $files_removed.	de l'autre partie.	**$name :** Nom de l'abonnement au journal. **$max_num_files :** Nombre maximal de fichiers autorisés par abonnement au journal. **$files_removed :** Liste des fichiers qui ont été supprimés.

Rapport d'alertes

Le tableau suivant contient la liste des différentes alertes de rapport qui peuvent être générées par AsyncOS, notamment une description de l'alerte et de la gravité de l'alerte :

Message	Gravité de l'alerte	Paramètres
Le système de rapports n'est pas en mesure de maintenir le débit des données générées. Toutes les nouvelles données générées seront perdues.	Critique.	Sans objet.
Le système de rapports est maintenant en mesure de gérer de nouvelles données.	de l'autre partie.	Sans objet.
Un échec s'est produit lors de la création du rapport périodique « $report_title ». Cet abonnement doit être examiné et supprimé si ses détails de configuration ne sont plus valides.	Critique.	**$report_title :** titre du rapport.
Un échec est survenu lors de l'envoi par courriel du rapport périodique « $report_title ». Cet abonnement a été supprimé du planificateur.	Critique.	**$report_title :** titre du rapport.
Le traitement des données de rapport recueillies a été désactivé en raison d'un manque d'espace disque de journalisation. L'utilisation du disque est supérieure au pourcentage du seuil $threshold. L'enregistrement des événements de rapport sera bientôt limité, et des données de rapport pourraient être perdues si de l'espace disque n'est pas libéré (en supprimant les anciens journaux, etc.). Une fois que l'utilisation du disque passe sous le pourcentage du seuil $threshold, le traitement complet des données de rapport sera redémarré automatiquement.	Avertissement.	**$threshold** : valeur de seuil.

Message	Gravité de l'alerte	Paramètres
RAPPORTS PÉRIODIQUES : lors de la création du rapport périodique « $report_title », le fichier de spécification de domaine attendu est introuvable dans « $file_name ». Aucun rapport n'a été envoyé.	Critique.	**$report_title :** titre du rapport. **$file_name** : nom du fichier.
Le groupe de compteurs « $counter_group » n'existe pas.	Critique.	**$counter_group** : nom de counter_group.
RAPPORTS PÉRIODIQUES : lors de la création du rapport périodique « $report_title », le fichier de spécification de domaine « $file_name » était vide. Aucun rapport n'a été envoyé.	Critique.	**$report_title :** titre du rapport. **$file_name** : nom du fichier.
RAPPORTS PÉRIODIQUES : des erreurs ont été rencontrées lors du traitement du fichier de spécification de domaine « $file_name » pour le rapport périodique « $report_title ». Toute ligne sur laquelle un problème a été signalé n'a fait l'objet d'aucun rapport envoyé. $error_text	Critique.	**$report_title :** titre du rapport. **$file_name** : nom du fichier. **$error_text** : liste des erreurs rencontrées.
Le traitement des données de rapport recueillies a été désactivé en raison d'un manque d'espace disque de journalisation. L'utilisation du disque est supérieure au pourcentage du seuil $threshold. L'enregistrement des événements de rapport sera bientôt limité, et des données de rapport pourraient être perdues si de l'espace disque n'est pas libéré (en supprimant les anciens journaux, etc.). Une fois que l'utilisation du disque passe sous le pourcentage du seuil $threshold, le traitement complet des données de rapport sera redémarré automatiquement.	Avertissement.	**$threshold** : valeur de seuil.
Le système de rapports a rencontré une erreur critique lors de l'ouverture de la base de données. Afin d'éviter d'interrompre d'autres services, les rapports ont été désactivés sur cette appliance. Veuillez contacter l'assistance client pour activer la création de rapports. Le message d'erreur est le suivant : $err_msg	Critique.	**$err_msg** : texte du message d'erreur.

Alertes du programme de mise à jour

Le tableau suivant contient une liste des différentes alertes du programme de mise à jour qui peuvent être générées par AsyncOS, notamment la description de l'alerte et la gravité de l'alerte :

Message	Gravité de l'alerte	Paramètres
L'application $app a essayé et échoué $attempts fois de terminer une mise à jour avec succès. Cela peut être dû à un problème de configuration réseau ou à une panne temporaire.	Avertissement.	**$app :** Secure Web Appliance nom du service de sécurité. **$attempts :** nombre de tentatives.
Le programme de mise à jour n'a pas pu communiquer avec le serveur de mise à jour depuis au moins $threshold.	Avertissement.	**$threshold :** durée de la valeur de seuil.
Erreur inconnue survenue : $traceback.	Critique.	**$traceback :** informations de recherche de la source.
Révoquer de certificat : échec de validation OCSP du certificat de serveur de mise à jour ($host:$port). Assurez-vous que le certificat est valide.	Éléments essentiels	**$host:** nom d'hôte du serveur de mise à jour. **$port :** port du serveur de mise à jour.

Alertes de protection contre les programmes malveillants

Pour plus d'informations sur les alertes relatives à Cisco Secure Endpoint, consultez Veiller à recevoir des alertes sur les problèmes Cisco Secure Endpoint.

Alertes AMP

Le tableau suivant contient une liste des différentes alertes AMP qui peuvent être générées par AsyncOS, y compris la description des alertes et leur gravité :

Message	Gravité de l'alerte	Paramètres
Échec de l'enregistrement de l'appliance auprès de la console AMP for Endpoints. $error	Avertissement	**$error :**message d'erreur.
Échec du désenregistrement de l'appliance ($devname) de la console AMP for Endpoints $error	Avertissement	**$devname:**nom du périphérique. **$error :**message d'erreur.

Alertes du proxy Web

Le tableau suivant contient la liste des différentes alertes de proxy Web qui peuvent être générées par AsyncOS, y compris la description de l'alerte et de sa gravité :

Message	Gravité de l'alerte	Paramètres
Une erreur s'est produite lors de l'opération de lecture/écriture sur le disque. $error	Information	**$info :**informations supplémentaires telles que l'objet et la taille de l'objet en cours d'écriture.
Le proxy Web a détecté que le contenu de la partition de mise en cache n'est pas valide. La purge du cache pourrait résoudre le problème : $errorstring	Information	**$errorstring :** informations supplémentaires sur le motif de l'invalidité du contenu du cache.
Erreurs des paramètres de configuration. $errorstring	Avertissement	**$errorstring :** description détaillée des erreurs de valeur de paramètre, notamment du paramètre et de sa valeur.
Le total des connexions côté client a dépassé le seuil défini. Les connexions persistantes sont temporairement désactivées. $info	Avertissement	**$info :** informations supplémentaires.
Le routeur WCCPv2 configuré ne répond pas ou est inaccessible. $info	Avertissement	**$info :** informations supplémentaires.
Le proxy de transmission en amont configuré ne répond pas ou est inaccessible. $info	Avertissement	**$info :** informations supplémentaires.
Le processus du proxy Web n'a pas de mémoire et a redémarré. $info	Avertissement	**$info :** informations supplémentaires.
Une erreur s'est produite dans la bibliothèque snmp. $info	Avertissement	**$info :** informations supplémentaires telles que la demande snmp en question.
Diverses erreurs ont entraîné la fermeture du proxy Web. $info	Avertissement	**$info :** informations supplémentaires, le cas échéant.
Le processus DNS s'est arrêté. $info	Avertissement	**$info :** informations supplémentaires, le cas échéant.
Le processus d'authentification s'est arrêté. $info	Avertissement	**$info :** informations supplémentaires, le cas échéant.

Message	Gravité de l'alerte	Paramètres
Le proxy Web n'a pas pu réserver de mémoire pour les principales structures de données internes lors du démarrage du processus. $info	Éléments essentiels	**$info :**informations supplémentaires telles que la taille de diverses structures de données internes principales.
Une erreur s'est produite lors de l'opération de lecture/écriture sur le disque. $info	Éléments essentiels	**$info :**informations supplémentaires telles que l'objet et la taille de l'objet en cours d'écriture.

Alertes de catégories d'URL externes

Le tableau suivant contient une liste des diverses alertes de catégories d'URL externes qui peuvent être générées par AsyncOS, notamment une description de l'alerte et la gravité de l'alerte :

Message	Gravité de l'alerte	Paramètres
$errmsg	Avertissement	**$errmsg** : message d'erreur.
$errmsg	Information	**$errmsg** : message d'erreur.
$errmsg	Éléments essentiels	**$errmsg** : message d'erreur.

L4 Traffic Monitor Alerts (Alertes de la supervision du trafic de la couche 4)

Le tableau suivant contient une liste des différentes alertes de la supervision du trafic de la couche 4 qui peuvent être générées par AsyncOS, notamment une description de l'alerte et de la gravité de l'alerte :

Message	Gravité de l'alerte	Paramètres
$errmsg	Avertissement	**$errmsg** : message d'erreur.
$errmsg	Information	**$errmsg** : message d'erreur.
$errmsg	Éléments essentiels	**$errmsg** : message d'erreur.

Alertes d'expiration des politiques

Le tableau suivant contient une liste des diverses alertes d'expiration de politique qui peuvent être générées par AsyncOS, y compris une description de l'alerte et de sa gravité :

Message	Gravité de l'alerte	Paramètres
« $PolicyType » : « $GroupName » a été désactivé en raison d'une configuration d'expiration.	Information	**$PolicyType :** politique d'accès/politique de déchiffrement en fonction du type de politique Web. **$GroupName :**nom du groupe de politiques.
'$PolicyType' : '$GroupName' expirera dans jours : 3.	Information	**$PolicyType :** politique d'accès/politique de déchiffrement en fonction du type de politique Web. **$GroupName :**nom du groupe de politiques.

Conformité à la norme FIPS

Les normes Federal Information Processing Standards (FIPS) précisent les exigences relatives aux modules cryptographiques utilisés par tous les organismes gouvernementaux pour protéger les informations sensibles, mais non classifiées. Les normes FIPS aident à assurer la conformité aux exigences fédérales en matière de sécurité et de confidentialité des données. Les normes FIPS, mises au point par le National Institue for Standards and Technology (NIST), sont destinées à être utilisées lorsqu'aucune norme volontaire n'existe pour répondre aux exigences fédérales.

Secure Web Appliance est conforme à la norme FIPS 140-2 en mode FIPS grâce au module cryptographique commun de Cisco (C3M). Le mode FIPS est désactivé par défaut.

Note **À partir de la version AsyncOS 15.0, le mode des normes fédérales de traitement de l'information (FIPS) n'est pas pris en charge.**

Thèmes connexes

- Problèmes du mode FIPS

Exigences du certificat FIPS

Le mode FIPS exige que tous les services de chiffrement activés sur le Secure Web Appliance utilisent un certificat conforme aux normes FIPS. Cela s'applique aux services de chiffrement suivants :

- Proxy HTTPS
- Authentification
- Fournisseur d'identité pour SaaS
- Service HTTPS de gestion d'appliances

- Configuration de la DLP externe pour ICAP sécurisé
- Identity Service Engine (ISE)
- Configuration SSL
- Configuration SSH

Note Le service HTTPS de gestion d'appliances doit être configuré avec un certificat de plainte FIPS pour que le mode FIPS puisse être activé. Il n'est pas nécessaire d'activer les autres services de chiffrement.

Un certificat conforme aux normes FIPS doit satisfaire aux exigences suivantes :

Certificate (certificat)	Algorithme	Signature Algorithm (algorithme de signature)	Notes
X509	RSA	sha1WithRSAEncryption sha256WithRSAEncryption	Cisco recommande une clé de 1024 bits pour des performances de déchiffrement optimales et une sécurité suffisante. Une taille en bits plus grande augmentera la sécurité, mais aura une incidence sur les performances de déchiffrement.

FIPS Certificate Validation (Validation du certificat FIPS)

Lorsque vous activez le mode FIPS, l'appliance effectue les vérifications de certificat suivantes :

- Tous les certificats chargés dans Secure Web Appliance, que ce soit au moyen de l'interface utilisateur ou de la commande de l'interface de ligne de commande `certconfig`, sont validés strictement conformes aux normes CC. Aucun certificat sans chemin approuvé approprié dans le magasin des certificats approuvés de Secure Web Appliance ne peut être chargé.
- Signature de certificat avec une validation de chemin approuvé; altération de certificats ou de clés publiques avec ensemble `basicConstrains` et `CAFlag` validé pour tous les certificats du signataire.
- La validation OCSP est disponible pour valider un certificat par rapport à une liste de révocation. Ce paramètre peut être configuré à l'aide de la commande de l'interface de ligne de commande `certconfig`.

Remarque Une nouvelle sous-commande `OCSPVALIDATION_FOR_SERVER_CERT` est ajoutée à la commande `certconfig` de l'interface de ligne de commande principale. La nouvelle sous-commande vous permet d'activer la validation OCSP pour les certificats de serveur LDAP et de mise à jour. Si la validation des certificats est activée, vous recevrez une alerte si les certificats impliqués dans la communication sont révoqués.

Voir aussi Validation stricte du certificat, à la page 54.

Activation ou désactivation du mode FIPS

Before you begin

- Effectuez une copie de sauvegarde de la configuration de l'appliance; voir Enregistrement du fichier de configuration de l'appliance, on page 2
- Assurez-vous que les certificats à utiliser en mode FIPS utilisent des algorithmes de clé publique approuvés par FIPS 140-2 (voir Exigences du certificat FIPS, on page 49).

Note

- La modification du mode FIPS déclenche un redémarrage de l'appliance.
- Lorsque vous désactivez le mode FIPS, les paramètres SSL et SSH, qui sont automatiquement devenus conformes aux normes FIPS lorsque le mode FIPS a été activé, ne sont pas réinitialisés à leurs valeurs par défaut. Vous devez explicitement modifier ces paramètres si vous souhaitez permettre à un client utilisant des paramètres SSH/SSL plus faibles de se connecter. Voir Configuration SSL , on page 52 pour de plus amples informations.

Étape 1 Choisissez **System Administration > FIPS Mode** (Administration système > Modèle FIPS).

Étape 2 Cliquez sur **Edit Settings** (Modifier les paramètres).

Étape 3 Cochez la case **Enable FIPS Compliance** (Activer la conformité FIPS) pour activer la conformité FIPS.

Lorsque vous cochez la case Enable FIPS Compliance (Activer la conformité FIPS), la case **Enable encryption of Critical Senstive Settings (CSP)** (Activer le chiffrement des paramètres critiques sensibles (CSP) est activée.

Étape 4 Cochez la case **Enable encryption of Critical Senstive Settings (CSP)** (Activer le chiffrement des paramètres critiques sensibles (CSP) pour activer le chiffrement des données de configuration comme les mots de passe, les informations d'authentification, les certificats, les clés partagées, etc.

Étape 5 Cliquez sur **Submit** (Soumettre).

Étape 6 Cliquez sur **Continue** (Continuer) pour permettre à l'appliance de redémarrer.

Gestion de la date et de l'heure du système

Définition du fuseau horaire

Étape 1 Choisissez **System Administration > Time Zone** (Administration système > Fuseau horaire).

Étape 2 Cliquez sur **Edit Settings** (Modifier les paramètres).

Étape 3 Sélectionnez votre région, votre pays et votre fuseau horaire ou sélectionnez le décalage GMT.

Étape 4 Envoyez et validez les modifications.

Synchronisation de l'horloge système avec un serveur NTP

Cisco vous recommande de configurer votre Secure Web Appliance pour suivre la date et l'heure actuelles en interrogeant un serveur NTP (Network Time Protocol), et non en réglant manuellement l'heure sur l'appliance. Cela est particulièrement vrai si votre appliance s'intègre à d'autres périphériques. Tous les périphériques intégrés doivent utiliser le même serveur NTP.

Étape 1 Choisissez **System Administration > Time Settings** (Administration système > Paramètres de temps).

Étape 2 Cliquez sur **Edit Settings** (Modifier les paramètres).

Étape 3 Sélectionnez **Use Network Time Protocol** (Utiliser Network Time Protocol) comme méthode de maintien de l'heure.

Étape 4 Entrez le nom d'hôte complet ou l'adresse IP du serveur NTP, en cliquant sur **Add Row** (Ajouter une ligne) si nécessaire pour ajouter des serveurs.

Étape 5 (Facultatif) Choisissez la table de routage associée à un type d'interface réseau de dispositif, Gestion ou Données, à utiliser pour les requêtes NTP. Il s'agit de l'adresse IP à partir de laquelle les requêtes NTP doivent provenir.

Note Cette option n'est modifiable que si l'appliance utilise le routage fractionné pour le trafic de données et de gestion.

Étape 6 Envoyez et validez vos modifications.

Configuration SSL

Pour une sécurité améliorée, vous pouvez activer et désactiver SSL v3 et diverses versions de TLS pour plusieurs services. Pour une sécurité optimale, il est recommandé de désactiver SSL v3 pour tous les services. Par défaut, toutes les versions de TLS sont activées et SSL est désactivé.

Note Vous pouvez également utiliser la commande de l'interface de ligne de commande `sslconfig` pour activer ou désactiver ces fonctionnalités. Consultez Commandes de l'interface de ligne de commande Secure Web Appliance.

Note Redémarrez l'application lorsque vous modifiez la configuration SSL et que cela entraîne la désactivation des chiffrements TLS.

Étape 1 Choisissez **System Administration > SSL Configuration** (Administration système > Configuration SSL).

Étape 2 Cliquez sur **Edit Settings** (Modifier les paramètres).

Étape 3 Cochez les cases correspondantes pour activer SSL v3 et TLS v1.x pour ces services :

- **Appliance Management Web User Interface** (Interface utilisateur Web de gestion d'appliance) : la modification de ce paramètre déconnectera toutes les connexions utilisateur actives.
- **Services de proxy** : inclut le proxy HTTPS et le chiffrement des informations d'authentification pour Secure Client. Cette section comprend également :
  - **Chiffrement à utiliser** : vous pouvez saisir des suites de chiffrement supplémentaires à utiliser avec les communications des services proxy. Utilisez les deux-points (:) pour séparer les suites. Pour empêcher l'utilisation d'un chiffrement particulier, ajoutez un point d'exclamation (!) devant cette chaîne. Par exemple, `!EXP-DHE-RSA-DES-CBC-SHA .`

    Assurez-vous de saisir uniquement des suites appropriées pour les versions TLS/SSL que vous avez vérifiées. Reportez-vous à https://www.openssl.org/docs/manmaster/man1/ciphers.html pour plus d'informations et pour en savoir plus sur les listes de chiffrement.

    L'appliance prend en charge la version TLSv1.3. Le chiffrement `TLS_AES_256_GCM_SHA384` est ajouté à la liste de chiffrement par défaut. Par défaut, TLSv1.3 est activé sur l'appliance.

    Dans AsyncOS version 14.0, les chiffrements `TLS_AES_128_GCM_SHA256` et `TLS_CHACHA20_POLY1305_SHA256` sont ajoutés à la liste de chiffrements par défaut.

    Le chiffrement par défaut pour AsyncOS versions 9.0 et antérieures est `Default:+kEDH`.

    Le chiffrement par défaut pour les versions 9.1 à 11.8 d'AsyncOS est le suivant :

    ```
    EECDH:DSS:RSA:!NULL:!eNULL:!EXPORT:!3DES:!RC4:!RC2:!DES:!SEED:!CAMELLIA
    :!SRP:!IDEA:!ECDHE-ECDSA-AES256-SHA:!ECDHE-RSA-AES256-SHA:!DHE-DSS-AES256-SHA:
    !AES256-SHA:DHE-RSA-AES128-SHA
    ```

    Dans ce cas, le chiffrement par défaut peut changer en fonction de vos sélections de chiffrement ECDHE.

    Le chiffrement par défaut pour AsyncOS versions 12.0 et ultérieures est :

    ```
    EECDH:DSS:RSA:!NULL:!eNULL:!aNULL:!EXPORT:!3DES:!SEED:!CAMELLIA
    :!SRP:!IDEA:!DHE-DSS-AES256-SHA:!AES256-SHA:DHE-RSA-AES128-SHA:
    TLS_AES_256_GCM_SHA384
    ```

    ```
    EECDH:DSS:RSA:!NULL:!eNULL:!aNULL:!EXPORT:!3DES:!SEED:!CAMELLIA
    :!SRP:!IDEA:!DHE-DSS-AES256-SHA:!AES256-SHA:DHE-RSA-AES128-SHA:
    TLS_AES_256_GCM_SHA384:TLS_AES_128_GCM_SHA256: TLS_CHACHA20_POLY1305_SHA256
    ```

    Note Mettez à jour la suite de chiffrement par défaut lors de la mise à niveau vers une version plus récente d'AsyncOS. Les suites de chiffrements ne sont pas automatiquement mises à jour. Lorsque vous effectuez une mise à niveau d'une version antérieure vers AsyncOS 12.0 ou une version ultérieure, Cisco recommande de mettre à jour la suite de chiffrement pour :

    ```
    EECDH:DSS:RSA:!NULL:!eNULL:!aNULL:!EXPORT:!3DES:!SEED:!CAMELLIA
    :!SRP:!IDEA:!DHE-DSS-AES256-SHA:!AES256-SHA:DHE-RSA-AES128-SHA:
    TLS_AES_256_GCM_SHA384
    ```

    ```
    EECDH:DSS:RSA:!NULL:!eNULL:!aNULL:!EXPORT:!3DES:!SEED:!CAMELLIA
    :!SRP:!IDEA:!DHE-DSS-AES256-SHA:!AES256-SHA:DHE-RSA-AES128-SHA:
    TLS_AES_256_GCM_SHA384:TLS_AES_128_GCM_SHA256: TLS_CHACHA20_POLY1305_SHA256
    ```

  - **Désactiver la compression TLS (recommandé)** – Vous pouvez cocher cette case pour désactiver la compression TLS. Cela est recommandé pour une sécurité optimale.
- **Services LDAP sécurisés** : incluent l'authentification, l'authentification extérieure et Secure Mobility.
- **Services ICAP sécurisés (DLP externe)** : sélectionnez le ou les protocoles utilisés pour sécuriser les communications ICAP entre l'appliance et les serveurs DLP (Data Loss Prevention) externes. Consultez Configuration des serveurs DLP externes pour obtenir de plus amples renseignements.

- **Service de mise à jour** : sélectionnez le ou les protocoles utilisés pour les communications entre l'appliance et les serveurs de mise à jour disponibles. Consultez Mises à niveau et mises à jour d'AsyncOS pour le Web, on page 59 pour en savoir plus sur les services de mise à jour.

Note Les serveurs de mise à jour de Cisco ne prennent pas en charge SSL v3, par conséquent, TLS 1.0 ou une version ultérieure doit être activé pour le service de mise à jour de Cisco. Cependant, SSL v3 peut toujours être utilisé avec un serveur de mise à jour local, s'il est configuré ainsi, vous devez déterminer quelles versions de SSL/TLS sont prises en charge sur ce serveur.

Étape 4 Cliquez sur **Submit** (Soumettre).

Certificate Management

L'appliance utilise des certificats numériques pour établir, confirmer et sécuriser diverses connexions. La page Certificate Management (Gestion des certificats) vous permet d'afficher et de mettre à jour les listes de certificats actuelles, de gérer les certificats racine approuvés et d'afficher les certificats bloqués.

Note La page Certificate Management (Gestion des certificats) prend du temps à se charger et entraîne une erreur d'expiration de délai lorsque l'appliance n'est pas connectée à Internet. En outre, l'erreur de réseau « Failed to fetch manifest » (Échec de la récupération du manifeste) s'affiche dans la liste des mises à jour de certificat après le chargement du certificat.

Thèmes connexes

- À propos des certificats et des clés, on page 55
- Mises à jour des certificats, on page 56
- Gestion des certificats racine approuvés, on page 55
- Affichage des certificats bloqués, on page 56

Validation stricte du certificat

Avec la sortie des mises à jour du mode FIPS dans AsyncOS 10.5, tous les certificats présentés sont validés strictement pour se conformer aux normes Common Criteria (CC) avant le téléchargement, et la validation OCSP est disponible pour valider les certificats par rapport à une liste de révocation.

Vous devez vous assurer que des certificats valides appropriés sont chargés dans Secure Web Appliance et que des certificats sécurisés valides sont configurés sur tous les serveurs associés pour faciliter des liaisons SSL sans interruption avec ces serveurs.

Une validation de certificat stricte est appliquée pour les chargements de certificat suivants :

- Proxy HTTPS [Security Services > HTTPS Proxy (Services de sécurité > Proxy HTTPS)]
- Serveur d'analyse des fichiers [Security Services > Anti-Malware and Reputation > Advanced Settings for File Analysis > File Analysis Server: Private Cloud & Certificate Authority: Use Uploaded Certificate Authority (Services de sécurité > Protection contre les programmes malveillants et réputation > Paramètres avancés pour l'analyse des fichiers > Serveur d'analyse des fichiers : Cloud privé et Autorité de certification)]

- Certificats racine approuvés [Network > Certificate Management (Réseau > Gestion des certificats)]
- Paramètres d'authentification globaux [Network > Authentication > Global Authentication Settings (Réseau > Authentification > Paramètres d'authentification globaux)]
- Fournisseur d'identité pour SaaS [Network > Identity Provider for SaaS (Réseau > Fournisseur d'identité pour SaaS)]
- Moteur du service d'identité [Network > Identity Services Engine (Réseau > Moteur du service d'identité)]
- Serveurs DLP externes [Network > External DLP Servers (Réseau > Serveurs DLP externes)]
- LDAP et LDAP sécurisé [Network > Authentication > Realm (Réseau > Authentification > Domaine)]

Voir aussi Conformité à la norme FIPS, à la page 49.

À propos des certificats et des clés

Lorsqu'un navigateur invite son utilisateur à s'authentifier, le navigateur envoie les informations d'authentification au proxy Web à l'aide d'une connexion sécurisée HTTPS. Par défaut, le Secure Web Appliance utilise le « certificat de démonstration de l'appliance Cisco pour la sécurité du Web » fourni avec pour créer une connexion HTTPS avec le client. La plupart des navigateurs avertissent les utilisateurs que le certificat n'est pas valide. Pour empêcher les utilisateurs de voir le message de certificat non valide, vous pouvez télécharger un certificat et une paire de clés que vos applications reconnaissent automatiquement.

Thèmes connexes

- Chargement ou génération d'un certificat et d'une clé, on page 56
- Requêtes de signature de certificat, on page 57
- Certificats intermédiaires, on page 58

Gestion des certificats racine approuvés

Le Secure Web Appliance est livré avec et gère une liste de certificats racine approuvés. Les sites Web dotés de certificats approuvés n'ont pas besoin de déchiffrement.

Vous pouvez gérer la liste des certificats approuvés, en y ajoutant et en en supprimant fonctionnellement des certificats. Bien que Secure Web Appliance ne supprime pas les certificats de la liste principale, il vous permet de remplacer la confiance dans un certificat, ce qui supprime fonctionnellement le certificat de la liste approuvée.

Pour ajouter, remplacer ou télécharger un certificat racine approuvé :

Étape 1 Choisissez **Network** > **Certificate Management** (Réseau > Gestion des certificats).

Étape 2 Cliquez sur **Manage Trusted root Certificates** (Gestion des certificats racine approuvés) sur la page Certificate Management (Gestion des certificats).

Étape 3 Pour ajouter un certificat racine approuvé personnalisé avec une autorité de signature ne figurant pas dans la liste des autorités reconnues par Cisco :

Cliquez sur **Import** (Importer), puis recherchez, sélectionnez et **envoyez** le fichier de certificat.

Étape 4 Pour remplacer la fiabilité d'un ou de plusieurs certificats reconnus par Cisco :

a) Cochez la case **Override Trust** (Remplacer la fiabilité) pour chaque entrée que vous souhaitez remplacer.
b) Cliquez sur **Submit** (Soumettre).

Étape 5 Pour télécharger une copie d'un certificat en particulier :

a) Cliquez sur le nom du certificat dans la liste des certificats racine approuvés de Cisco pour développer cette entrée.
b) Cliquez sur **Download Certificate** (Télécharger le certificat).

Mises à jour des certificats

La section Updates (Mises à jour) répertorie la version et les dernières informations mises à jour pour les ensembles de certificats racine approuvés et de listes bloquées de Cisco sur l'appliance. Ces ensembles sont régulièrement mis à jour.

Cliquez sur **Update Now** (Mettre à jour maintenant) dans la page Certificate Management (Gestion des certificats) pour mettre à jour tous les ensembles pour lesquels des mises à jour sont disponibles.

Affichage des certificats bloqués

Pour afficher une liste des certificats que Cisco a déterminés comme non valides et qu'il a bloqués :

Cliquez sur **View Blocked Certificates** (Afficher les certificats bloqués).

Chargement ou génération d'un certificat et d'une clé

Certaines fonctionnalités d'AsyncOS nécessitent un certificat et une clé pour établir, confirmer ou sécuriser une connexion, le moteur de services d'identité et. Vous pouvez soit charger un certificat et une clé existants, soit en générer un lorsque vous configurez la fonctionnalité.

Chargement d'un certificat et d'une clé

Un certificat que vous chargez sur l'appliance doit satisfaire aux exigences suivantes :

- Il doit utiliser la norme X.509.
- Il doit inclure une clé privée correspondante au format PEM. Format DER non pris en charge.

Étape 1 Sélectionnez **Use Uploaded Certificate and Key** (Utiliser le certificat et la clé téléchargés).

Étape 2 Dans le champ **Certificate** (Certificat), cliquez sur Browse (Parcourir); localisez le fichier à télécharger.

Note Le proxy Web utilise le premier certificat ou la première clé du fichier. Le fichier de certificat doit être au format PEM. Format DER non pris en charge.

Étape 3 Dans le champ **Key** (Clé), cliquez sur Browse (Parcourir); localisez le fichier à télécharger.

Note La longueur de la clé doit être de 512, 1024 ou 2048 bits. Le fichier de clé privée doit être au format PEM. Format DER non pris en charge.

Étape 4 Si la clé est chiffrée, sélectionnez **Key is Encrypted** (La clé est chiffrée).

Étape 5 Cliquez sur **Upload Files** (Charger des fichiers).

Génération d'un certificat et d'une clé

Étape 1 Sélectionnez **Use Generate Certificate and Key** (Utiliser le certificat et la clé générés).

Étape 2 Cliquez sur **Generate New Certificate and Key** (Générer un nouveau certificat et une nouvelle clé).

a) Dans la boîte de dialogue Generate Certificate and Key (Générer un certificat et une clé), saisissez les renseignements nécessaires à la génération.

Note Vous pouvez saisir n'importe quel caractère ASCII, à l'exception de la barre oblique (/) dans le champ Common Name (Nom commun).

b) Cliquez sur **Generate** (Générer) dans la boîte de dialogue Generate Certificate and Key (Générer un certificat et une clé).

Une fois la génération terminée, les informations sur le certificat s'affichent dans la section Certificate (Certificat) ainsi que deux liens : **Download Certificate** (Télécharger le certificat) et **Download Certificate Signing Request** (Télécharger la demande de signature de certificat). En outre, il existe une option de certificat signé qui est utilisée pour télécharger le certificat signé lorsque vous le recevez de l'autorité de certification (CA).

Étape 3 Cliquez sur **Download Certificate** (Télécharger le certificat) pour télécharger le nouveau certificat et le charger sur l'appliance.

Étape 4 Cliquez sur **Download Certificate Signing Request** (Télécharger la demande de signature de certificat) pour télécharger le nouveau fichier de certificat et le transmettre à une autorité de certification (AC) pour signature. Consultez Requêtes de signature de certificat, on page 57 pour en savoir plus sur ce processus.

a) Lorsque l'autorité de certification renvoie le certificat signé, cliquez sur Browse (Parcourir) dans la partie Signed Certificate (Certificat signé) du champ Certificate (Certificat) pour identifier le fichier de certificat signé, puis cliquez sur Upload File (Charger le fichier) pour le charger sur l'appliance.

b) Assurez-vous que le certificat racine de l'autorité de certification est présent dans la liste des certificats racine approuvés de l'appliance. Si ce n'est pas le cas, ajoutez-le. Consultez la Gestion des certificats racine approuvés, on page 55 pour de plus amples renseignements.

Requêtes de signature de certificat

Secure Web Appliance ne peut pas générer de demandes de signature de certificat (CSR) pour les certificats téléchargés sur l'appliance. Par conséquent, pour qu'un certificat soit créé pour l'appliance, vous devez émettre la demande de signature à partir d'un autre système. Enregistrez la clé au format PEM à partir de ce système, car vous devrez l'installer sur l'appliance plus tard.

Vous pouvez utiliser n'importe quel ordinateur UNIX sur lequel une version récente d'OpenSSL est installée. Veillez à indiquer le nom d'hôte de l'appliance dans la demande de signature de certificat (CSR). Suivez les directives à l'emplacement suivant pour obtenir des renseignements sur la génération d'une requête de signature de certificat (CSR) à l'aide d'OpenSSL :

`http://www.modssl.org/docs/2.8/ssl_faq.html#ToC28`

Une fois la demande de signature de certificat (CSR) générée, envoyez-la à une autorité de certification (AC). L'autorité de certification renverra le certificat au format PEM.

Si vous obtenez un certificat pour la première fois, recherchez sur Internet « certificats de serveur de services d'autorité de certification SSL » et choisissez le service qui répond le mieux aux besoins de votre entreprise. Suivez les instructions du service pour obtenir un certificat SSL.

Note Vous pouvez également générer et signer votre propre certificat. Les outils nécessaires sont inclus avec OpenSSL, le logiciel gratuit disponible à l'adresse `http://www.openssl.org` .

Certificats intermédiaires

Outre la vérification du certificat de l'autorité de certification racine, AsyncOS prend en charge la vérification des certificats intermédiaires. Les certificats intermédiaires sont des certificats émis par une autorité de certification racine approuvée qui sont ensuite utilisés pour créer des certificats supplémentaires. Cela crée une ligne de confiance en chaîne. Par exemple, un certificat peut être émis par le site exemple.com qui, à son tour, se voit accorder les droits d'émettre des certificats par une autorité de certification racine approuvée. Le certificat émis par le site exemple.com doit être validé par rapport à la clé privée du site exemple.com ainsi que par rapport à la clé privée de l'autorité de certification racine approuvée.

Les serveurs envoient une « chaîne de certificats » dans une liaison SSL pour que les clients (par exemple, les navigateurs et, dans ce cas, le Secure Web Appliance, qui est un proxy HTTPS) authentifient le serveur. Normalement, le certificat du serveur est signé par un certificat intermédiaire qui, à son tour, est signé par un certificat racine approuvé et, pendant la liaison, le certificat du serveur et la chaîne complète de certificats sont présentés au client. Comme le certificat racine est généralement présent dans le magasin de certificats approuvés de Secure Web Appliance, la chaîne de certificats est vérifiée avec succès.

Cependant, il peut parfois arriver, lorsque le certificat de l'entité terminale est modifié sur le serveur, que les mises à jour nécessaires pour la nouvelle chaîne ne soient pas effectuées. Par conséquent, à partir de maintenant, le serveur présente uniquement le certificat de serveur lors de l'établissement de la liaison SSL et le proxy Secure Web Appliance ne peut pas vérifier la chaîne de certificats, car le certificat intermédiaire est manquant.

Auparavant, la solution consistait en l'intervention manuelle de l'administrateur Secure Web Appliance, qui téléchargeait le certificat intermédiaire nécessaire dans le magasin de certificats approuvés. Vous pouvez désormais utiliser la commande d'interface de ligne de commande `advancedproxyconfig > HTTPS > Do you want to enable automatic discovery and download of missing Intermediate Certificates?` (advancedproxyconfig > HTTPS > Voulez-vous activer la découverte et le téléchargement automatiques des certificats intermédiaires manquants?) pour activer la « découverte de certificats intermédiaires », un processus que Secure Web Appliance utilise afin d'éliminer l'étape manuelle dans ces situations.

La découverte de certificats intermédiaires utilise une méthode appelée « analyse AIA » : lorsqu'un certificat non fiable se présente, l'appliance Secure Web Appliance l'examine pour détecter une extension nommée « Authority Information Access ». Cette extension comprend un champ facultatif URI pour les émetteurs de l'autorité de certification, qui peuvent être interrogés pour le certificat de l'émetteur utilisé pour signer le certificat du serveur en question. Si le certificat de l'émetteur est disponible, Secure Web Appliance le récupère de manière récursive jusqu'à ce que le certificat de l'autorité de certification racine soit obtenu, puis tente à nouveau de vérifier la chaîne.

Mises à niveau et mises à jour d'AsyncOS pour le Web

Cisco publie régulièrement des mises à niveau (nouvelles versions de logiciels) et des mises à jour (modifications des versions logicielles actuelles) pour AsyncOS pour le Web et ses composants.

Meilleures pratiques pour la mise à niveau d'AsyncOS pour le Web

- Avant de lancer la mise à niveau, enregistrez le fichier de configuration XML à partir de Secure Web Appliance, de la page **System Administration > Configuration File** (Administration système > Fichier de configuration) ou en utilisant la commande saveconfig.
- Enregistrez d'autres fichiers stockés sur l'appliance, tels que les fichiers PAC ou les pages de notification personnalisée à l'utilisateur final.
- Lors de la mise à niveau, ne faites pas de pause pendant de longues périodes aux différentes invites. Si la session TCP expire pendant le téléchargement, la mise à niveau pourrait échouer.
- Une fois la mise à niveau terminée, enregistrez les informations de configuration dans un fichier XML.

Thèmes connexes

- Enregistrement, chargement et réinitialisation de la configuration de l'appliance, on page 2

Mise à niveau et mise à jour d'AsyncOS et des composants du service Security

Téléchargement et installation d'une mise à niveau

Avant de commencer

Enregistrez le fichier de configuration de l'appliance (voir Enregistrement, chargement et réinitialisation de la configuration de l'appliance, à la page 2).

Remarque Lors du téléchargement et de la mise à niveau d'AsyncOS en une seule opération à partir d'un serveur local plutôt que d'un serveur Cisco, la mise à niveau est installée immédiatement lors du téléchargement. Une bannière s'affiche pendant 10 secondes au début du processus de mise à niveau. Pendant que cette bannière est affichée, vous pouvez taper Ctrl-C pour quitter le processus de mise à niveau avant le début du téléchargement.

Remarque Lors d'une mise à niveau, si le certificat d'authentification sécurisée n'est pas conforme aux normes FIP, il sera remplacé par le certificat par défaut du dernier chemin vers lequel votre appliance est mise à niveau. Cela se produit uniquement lorsque le client a utilisé le certificat par défaut avant la mise à niveau.

Vous pouvez télécharger et installer en une seule opération, ou télécharger en arrière-plan et installer plus tard.

La mise à niveau échoue si une valeur de configuration stockée dans les fichiers varstore comporte des caractères non ASCII.

Étape 1 Choisissez **System Administration** > **System Upgrade** (Administration système > Mise à niveau du système).

Étape 2 Cliquez sur **Upgrade Options** (Options de mise à niveau).

Sélectionnez les options de mise à niveau et une image de mise à niveau :

Paramètres	Description
Choisir une option de mise à niveau	• **Download and install** (Télécharger et installer) : téléchargez et installez la mise à niveau en une seule opération. Si vous avez déjà téléchargé un programme d'installation, vous serez invité à remplacer le téléchargement existant. • **Download only** (Télécharger seulement) : téléchargez un programme d'installation de mise à niveau, mais ne l'installez pas. Si vous avez déjà téléchargé un programme d'installation, vous serez invité à remplacer le téléchargement existant. Le programme d'installation se télécharge en arrière-plan sans interrompre le service. Un bouton **Install** (Installer) s'affiche lorsque le téléchargement est terminé; cliquez pour installer une mise à niveau déjà téléchargée.
	Sélectionnez une image de mise à niveau à télécharger, ou à télécharger et installer, dans le champ **List of available upgrade images files at upgrade server** (Liste des fichiers image de mise à niveau disponibles sur le serveur de mise à niveau).
Préparation de la mise à niveau	• Pour enregistrer une copie de sauvegarde de la configuration actuelle dans le répertoire **`configuration`** de l'appliance, cochez l'option **Save the current configuration to the configuration directory before upgrading** (Enregistrer la configuration actuelle dans le répertoire de configuration avant la mise à niveau). • Si l'option **Save current configuration** (Enregistrer la configuration actuelle) est cochée, vous pouvez cocher **Mask passwords in the configuration file** (Masquer les mots de passe dans le fichier de configuration) afin de masquer tous les mots de passe de la configuration actuelle dans la copie de sauvegarde. Cependant, vous ne pouvez pas charger un fichier de configuration avec des mots de passe masqués à l'aide de la commande **Load Configuration** (Charger la configuration) ni de la commande **`loadconfig`** de l'interface de ligne de commande. Si le mode FIPS est activé, vous pouvez sélectionner **Encrypt passphrases in the Configuration Files** (Chiffrer les phrases secrètes dans les fichiers de configuration). Ces fichiers peuvent être rechargés. • Si l'option **Save current configuration** (Enregistrer la configuration actuelle) est cochée, vous pouvez entrer une ou plusieurs adresses de messagerie dans le champ **Email file to** (Envoyer le fichier à); une copie du fichier de configuration de sauvegarde est envoyée à chaque adresse. Séparez les valeurs multiples par des virgules.

Étape 3 Cliquez sur **Procéder**.

Si vous installez :

a) Soyez prêt à répondre aux invites pendant le processus.
b) À l'invite de fin, cliquez sur **Reboot Now** (Redémarrer maintenant).
c) Après environ 10 minutes, accédez à nouveau à l'appliance et connectez-vous.

Si vous pensez devoir redémarrer l'appliance pour résoudre un problème de mise à niveau, ne le faites pas avant qu'au moins 20 minutes se soient écoulées depuis le redémarrage.

Affichage de l'état, annulation ou suppression d'un téléchargement en arrière-plan

Étape 1 Choisissez **System Administration** > **System Upgrade** (Administration système > Mise à niveau du système).

Étape 2 Cliquez sur **Upgrade Options** (Options de mise à niveau).

Étape 3 Choisissez une option :

Destinataire	Faire ceci
Afficher l'état du téléchargement	Regardez au milieu de la page. Si aucun téléchargement n'est en cours et s'il n'y a aucun téléchargement terminé en attente d'installation, vous ne verrez aucune information sur l'état du téléchargement.
Annuler un téléchargement	Cliquez sur le bouton **Cancel Download** (Annuler le téléchargement) au milieu de la page. Cette option ne s'affiche que lorsqu'un téléchargement est en cours.
Supprimer un programme d'installation téléchargé	Cliquez sur le bouton **Delete File** (Supprimer le fichier) au milieu de la page. Cette option ne s'affiche que si un programme d'installation a été téléchargé.

Étape 4 (Facultatif) Affichez les journaux de mise à niveau.

Prochaine étape

Thèmes connexes

- Serveurs de mise à jour locaux et distants, à la page 63

Requêtes automatiques et manuelles de mise à jour et de mise à niveau

AsyncOS interroge périodiquement les serveurs de mise à jour pour connaître les nouvelles mises à jour pour tous les composants du service de sécurité, mais pas pour les nouvelles mises à niveau d'AsyncOS. Pour mettre à niveau AsyncOS, vous devez inviter manuellement AsyncOS à rechercher les mises à niveau disponibles. Vous pouvez également inviter manuellement AsyncOS à rechercher les mises à jour disponibles des services de sécurité. Pour en savoir plus, consultez Retour à une version antérieure d'AsyncOS pour le Web, on page 67.

Quand AsyncOS interroge un serveur de mise à jour pour une mise à jour ou une mise à niveau, il effectue les étapes suivantes :

1. Contacte le serveur de mise à jour.

   Cisco autorise les sources suivantes pour les serveurs de mise à jour :

   - **Serveurs de mise à jour Cisco.** Pour en savoir plus, consultez Mise à jour et mise à niveau à partir des serveurs de mise à jour Cisco, on page 63.
   - **Serveur local.** Pour en savoir plus, consultez Mise à niveau à partir d'un serveur local, on page 63.

2. Reçoit un fichier XML qui répertorie les mises à jour disponibles ou les versions de mise à niveau d'AsyncOS. Ce fichier XML est connu sous le nom de « fichier manifeste ».
3. Télécharge les fichiers image de mise à jour ou de mise à niveau.

Mise à jour manuelle des composants du service Security

Par défaut, chaque composant des services de sécurité reçoit régulièrement des mises à jour de ses tableaux de bases de données des serveurs de mises à jour de Cisco. Cependant, vous pouvez mettre à jour manuellement les tableaux de la base de données.

Note Certaines mises à jour sont disponibles sur demande à partir des pages de l'interface graphique utilisateur associées à la fonctionnalité.

Tip Affichez un enregistrement de l'activité de mise à jour dans le fichier journal du programme de mise à jour. Abonnez-vous au fichier journal du programme de mise à jour sur la page **System Administration > Log Subscriptions** (Administration système > Abonnements aux journaux).

Note Les mises à jour en cours ne peuvent pas être interrompues. Toutes les mises à jour en cours doivent être terminées avant que de nouvelles modifications puissent être appliquées.

Étape 1 Choisissez **System Administration > Upgrade and Update Settings** (Administration système > Paramètres de mise à niveau et de mise à jour).

Étape 2 Cliquez sur **Edit Update Settings** (Modifier les paramètres de mise à jour).

Étape 3 Précisez l'emplacement des fichiers de mise à jour.

Étape 4 Lancez la mise à jour à l'aide de la touche de fonction Update Now (Mettre à jour maintenant) sur la page du composant située dans l'onglet Security Services (Services de sécurité). Par exemple, page Security Services > Web Reputation Filters (Services de sécurité > Filtres de réputation Web).

L'interface de commande en ligne et l'interface de l'application Web peuvent être lentes ou indisponibles pendant le processus de mise à jour.

Serveurs de mise à jour locaux et distants

Par défaut, AsyncOS contacte les serveurs de mise à jour Cisco pour obtenir les images de mise à jour et de mise à niveau et le fichier manifeste XML. Cependant, vous pouvez choisir de l'emplacement de téléchargement des images de mise à niveau et de mise à jour et du fichier manifeste. utilisation d'un serveur de mise à jour local pour les images ou le fichier manifeste pour l'une des raisons suivantes :

- **Vous avez plusieurs appliances à mettre à niveau simultanément.** Vous pouvez télécharger l'image de mise à niveau sur un serveur Web au sein de votre réseau et la diffuser sur toutes les appliances de votre réseau.
- **Les paramètres de votre pare-feu exigent des adresses IP statiques pour les serveurs de mise à jour Cisco.** Les serveurs de mise à jour Cisco utilisent des adresses IP dynamiques. Si vous avez des politiques de pare-feu strictes, vous devrez peut-être configurer un emplacement statique pour les mises à jour et les mises à niveau d'AsyncOS. Pour en savoir plus, consultez Configuration d'une adresse statique pour les serveurs de mise à jour Cisco, on page 63.

Note Les serveurs de mise à jour locaux ne reçoivent pas automatiquement les mises à jour du service de sécurité, mais uniquement les mises à niveau d'AsyncOS. Après avoir utilisé un serveur de mise à jour local pour la mise à niveau d'AsyncOS, modifiez les paramètres de mise à jour et de mise à niveau pour utiliser les serveurs de mise à jour Cisco afin que les services de sécurité se mettent à jour automatiquement.

Mise à jour et mise à niveau à partir des serveurs de mise à jour Cisco

Secure Web Appliance peut se connecter directement aux serveurs de mises à jour Cisco et télécharger les images de mise à niveau et les mises à jour des services de sécurité. Chaque appliance télécharge les mises à jour et les images de mise à niveau séparément.

Configuration d'une adresse statique pour les serveurs de mise à jour Cisco

Les serveurs de mise à jour Cisco utilisent des adresses IP dynamiques. Si vous avez des politiques de pare-feu strictes, vous devrez peut-être configurer un emplacement statique pour les mises à jour et les mises à niveau d'AsyncOS.

Étape 1 Communiquez avec l'assistance client de Cisco pour obtenir l'adresse URL statique.

Étape 2 Accédez à la page **System Administration** > **Upgrade and Update Settings** (Administration système > Paramètres de mise à niveau et de mise à jour), puis cliquez sur **Edit Update Settings** (Modifier les paramètres de mise à jour).

Étape 3 (Modifier les paramètres de mise à jour), dans la section « Update Servers (images) » [Serveurs de mise à jour (images)], choisissez **Local Update Servers** (Serveurs de mise à jour locaux) et entrez l'adresse URL statique reçue à l'étape 1.

Étape 4 Vérifiez que l'option Cisco Update Servers (Serveurs de mise à jour Cisco) est sélectionnée dans la section « Update Servers (list) » [Serveurs de mise à jour (liste)].

Étape 5 Envoyez et validez vos modifications.

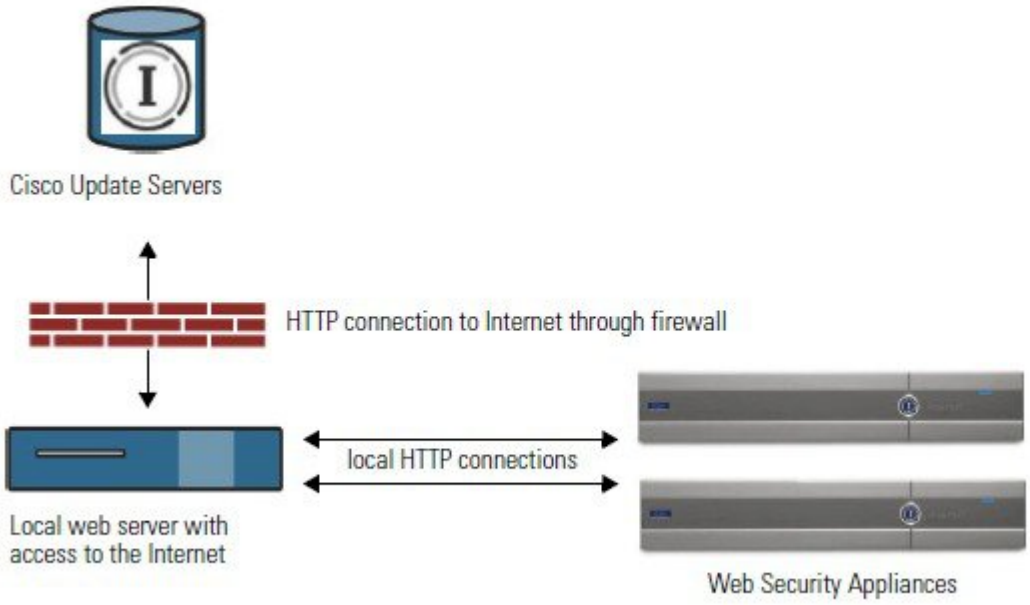
Mise à niveau à partir d'un serveur local

Secure Web Appliance peut télécharger les mises à niveau d'AsyncOS à partir d'un serveur de votre réseau au lieu d'obtenir des mises à niveau directement des serveurs de mise à jour Cisco. Cette fonctionnalité permet

de télécharger l'image de mise à niveau à partir de Cisco une seule fois, puis de la transmettre à tous les Secure Web Appliance de votre réseau.

La figure suivante montre comment les Secure Web Appliance télécharge les images de mise à niveau à partir de serveurs locaux.

Figure 1: Mise à niveau à partir d'un serveur local



Configuration matérielle et logicielle requise pour les serveurs locaux de mise à niveau

Pour *télécharger* les fichiers de mise à niveau AsyncOS, vous devez avoir un système dans votre réseau interne qui dispose d'un navigateur Web et d'un accès Internet aux serveurs de mise à jour Cisco.

Note Si vous devez configurer un paramètre de pare-feu pour autoriser l'accès HTTP à cette adresse, vous devez le faire en utilisant le nom DNS et non une adresse IP spécifique.

Pour *héberger* des fichiers de mise à niveau AsyncOS, un serveur du réseau interne doit avoir un serveur Web, comme Microsoft IIS (Internet Information Services) ou le serveur ouvert (Open Source) Apache, qui présente les caractéristiques suivantes :

- Prise en charge de l'affichage des noms de répertoires ou de fichiers dépassant 24 caractères.
- Navigation dans les répertoires activée.
- Configuré pour l'authentification anonyme (sans authentification) ou l'authentification de base (« simple »).
- Contient au moins 350 Mo d'espace disque libre pour chaque image de mise à niveau AsyncOS.

Configuration des mises à niveau à partir d'un serveur local

Note Cisco recommande de modifier les paramètres de mise à jour et de mise à niveau pour utiliser les serveurs de mise à jour Cisco (en utilisant des adresses dynamiques ou statiques) une fois la mise à niveau terminée pour garantir que les composants des services de sécurité continuent de se mettre à jour automatiquement.

Étape 1 Configurez un serveur local pour récupérer et distribuer servir les fichiers de mise à niveau.

Étape 2 Téléchargez le fichier de mise à niveau compressé.

À l'aide d'un navigateur sur le serveur local, accédez à la page http://updates.ironport.com/fetch_manifest.html pour télécharger un fichier compressé d'une image de mise à niveau. Pour télécharger l'image, entrez votre numéro de série (pour une appliance physique) ou VLN (pour une appliance virtuelle) et le numéro de version de l'appliance. Une liste des mises à niveau disponibles s'affichera ensuite. Cliquez sur la version de mise à niveau que vous souhaitez télécharger.

Étape 3 Décompressez le fichier compressé dans le répertoire racine sur le serveur local tout en préservant la structure de répertoires.

Étape 4 Configurez l'appliance pour utiliser le serveur local à l'aide de la page **System Administration > Upgrade and Update Settings** (Administration système > Paramètres de mise à niveau et de mise à jour) ou de la commande updateconfig.

Étape 5 Dans la page **System Administration > System Upgrade** (Administration système > Mise à niveau du système), cliquez sur **Availability Upgrades** (Mises à niveau disponibles) ou exécutez la commande upgrade.

Différences entre les méthodes de mise à niveau locale et à distance

Les différences suivantes s'appliquent lors de la mise à niveau d'AsyncOS à partir d'un serveur local plutôt que d'un serveur de mise à jour Cisco :

- La mise à niveau s'installe immédiatement *lors du téléchargement*.
- Une bannière s'affiche pendant 10 secondes au début du processus de mise à niveau. Pendant que cette bannière est affichée, vous avez la possibilité de taper Ctrl+C pour quitter le processus de mise à niveau avant le début du téléchargement.

Configuration des paramètres de mise à niveau et de mise à jour de services

Vous pouvez configurer la façon dont Secure Web Appliance télécharge les mises à jour des services de sécurité et les mises à niveau d'AsyncOS pour le Web. Par exemple, vous pouvez choisir l'interface réseau à utiliser lors du téléchargement des fichiers, configurer l'intervalle de mise à jour ou désactiver les mises à jour automatiques.

Étape 1 Choisissez **System Administration > Upgrade and Update Settings** (Administration système > Paramètres de mise à niveau et de mise à jour).

Étape 2 Cliquez sur **Edit Update Settings** (Modifier les paramètres de mise à jour).

Étape 3 Configurez les paramètres en vous référant aux informations suivantes :

Paramètres	Description
Automatic Updates (Mises à jour automatiques)	Choisissez si vous souhaitez activer les mises à jour automatiques des composants de sécurité. Si vous choisissez les mises à jour automatiques, saisissez l'intervalle de temps. La valeur par défaut est activée et l'intervalle de mise à jour est de 5 minutes.
Upgrade Notifications (Notifications de mise à niveau)	Choisissez si vous souhaitez afficher une notification en haut de l'interface Web quand une nouvelle mise à niveau vers AsyncOS est disponible. L'appliance affiche cette notification uniquement pour les administrateurs. Pour en savoir plus, consultez Mises à niveau et mises à jour d'AsyncOS pour le Web, on page 59.
Update Servers (list) [Mettre à jour les serveurs (liste)]	Permet de télécharger la liste des mises à niveau et mises à jour disponibles (fichier manifeste XML) à partir des serveurs de mises à jour Cisco ou d'un serveur Web local. Lorsque vous choisissez un serveur de mise à jour local, entrez le chemin d'accès complet au fichier manifeste XML pour obtenir la liste contenant le nom de fichier et le numéro de port du serveur. Si vous laissez le champ du port vide, AsyncOS utilise le port 80. Si le serveur exige une authentification, vous pouvez également saisir un nom d'utilisateur et une phrase secrète valides. • Pour obtenir le manifeste des appliances matérielles, tapez l'URL suivante : https://update-manifests.ironport.com • Pour obtenir le manifeste des appliances virtuelles, tapez l'URL suivante : https://update-manifests.sco.cisco.com
Update Servers (images) [Mettre à jour les serveurs (images)]	Permet de télécharger les images de mise à niveau et de mise à jour à partir des serveurs de mise à jour Cisco ou d'un serveur Web local. Lorsque vous choisissez un serveur de mise à jour local, entrez l'URL de base et le numéro de port du serveur. Si vous laissez le champ du port vide, AsyncOS utilise le port 80. Si le serveur exige une authentification, vous pouvez également saisir un nom d'utilisateur et une phrase secrète valides.
Routing Table (Tableau de routage)	Choisissez la table de routage de l'interface réseau à utiliser lorsque vous communiquez avec les serveurs de mise à jour.
Proxy Server (optional) [Serveur proxy (facultatif)]	S'il existe un serveur proxy en amont, qui exige une authentification, entrez les informations du serveur, le nom d'utilisateur et la phrase secrète ici.

Étape 4 Envoyez et validez vos modifications.

What to do next

Thèmes connexes

- Serveurs de mise à jour locaux et distants, on page 63
- Requêtes automatiques et manuelles de mise à jour et de mise à niveau, on page 61
- Mise à niveau et mise à jour d'AsyncOS et des composants du service Security, on page 59

Retour à une version antérieure d'AsyncOS pour le Web

AsyncOS pour le Web prend en charge la possibilité de rétablir une version précédente du système d'exploitation AsyncOS pour le Web pour les utilisations d'urgence.

Note Vous ne pouvez pas revenir à une version d'AsyncOS pour le Web antérieure à la version 7.5.

Le retour à une version antérieure d'AsyncOS sur les appliances virtuelles a une incidence sur la licence

Si vous revenez à AsyncOS 8.0, il n'y a pas de délai de grâce de 180 jours pendant lequel l'appliance traite les transactions Web sans fonctionnalités de sécurité. Les dates d'expiration des licences ne sont pas affectées.

Utilisation du fichier de configuration dans le processus de retour à une version antérieure

À partir de la version 7.5, lorsque vous mettez à niveau vers une version ultérieure, le processus de mise à niveau enregistre automatiquement la configuration actuelle du système dans un fichier sur Secure Web Appliance. (Cependant, Cisco recommande d'enregistrer manuellement le fichier de configuration sur un ordinateur local en tant que sauvegarde.) Cela permet à AsyncOS pour le Web de charger le fichier de configuration associé à la version antérieure après être revenu à la version antérieure. Cependant, lorsqu'il effectue une inversion, il utilise les paramètres réseau actuels pour l'interface de gestion.

Rétablissement de la version antérieure d'AsyncOS pour une appliance gérée par SMA

Vous pouvez rétablir AsyncOS pour le Web à partir de Secure Web Appliance. Toutefois, si Secure Web Appliance est géré par une appliance de gestion de la sécurité, tenez compte des règles et instructions suivantes :

- Lorsque les rapports centralisés sont activés sur Secure Web Appliance, AsyncOS pour le Web termine de transférer les données de rapport vers l'appliance de gestion de la sécurité avant de lancer le rétablissement de la version antérieure. Si le transfert des fichiers vers l'appliance de gestion de la sécurité est supérieur à 40 secondes, AsyncOS pour le Web vous invite à continuer à attendre pour transférer les fichiers, ou à poursuivre la restauration sans transférer tous les fichiers.
- Vous devez associer Secure Web Appliance à la configuration principale appropriée après le rétablissement. Sinon, le transfert d'une configuration de l'appliance de gestion de la sécurité vers Secure Web Appliance pourrait échouer.

Rétablissement d'une version antérieure d'AsyncOS pour le Web

Caution Rétablir le système d'exploitation sur un Secure Web Appliance est une action très destructrice, qui détruit tous les journaux de configuration et toutes les bases de données. Le rétablissement d'une version antérieure perturbe également le traitement du trafic Web jusqu'à ce que l'appliance soit reconfigurée. Selon la configuration initiale de Secure Web Appliance, cette action peut détruire la configuration réseau. Dans ce cas, vous aurez besoin d'un accès physique local à l'appliance après avoir effectué le rétablissement d'une version antérieure.

Caution La configuration des licences Smart ne peut pas être conservée si le système d'exploitation d'une appliance Cisco Secure Web Appliance est rétabli à la version antérieure avec les licences Smart activées. Lorsque vous êtes revenu à la version précédente d'AsyncOS, vous devez activer l'octroi de licences Smart et l'enregistrer sur le portail CSSM. Si l'option **Specific/Permanent License Reservation** (Réservation de licence permanente/spécifique) a été sélectionnée lors de l'activation de la licence logicielle Smart, il est recommandé de libérer les licences utilisées par l'appliance avant d'annuler l'opération et d'annuler l'enregistrement de l'appliance sur le portail CSSM. Vous pouvez contacter l'assistance de Cisco pour obtenir de l'aide, si les licences n'ont pas été publiées ou si l'enregistrement de l'appliance n'a pas été annulé avant l'opération de rétablissement d'une version antérieure.

Note Si des mises à jour de l'ensemble de catégories d'URL sont disponibles, elles seront appliquées après la restauration de la version antérieure d'AsyncOS.

Before you begin

- Communiquez avec le service d'assurance qualité de Cisco pour confirmer que vous pouvez effectuer le rétablissement d'une version antérieure prévu. (BS : il s'agit d'un résumé de la section Versions disponibles dans la rubrique d'origine. Ai demandé si cela est correct.)
- Sauvegardez les informations suivantes de Secure Web Appliance sur une machine distincte :
  - Fichier de configuration du système (avec phrase secrète non masquée)
  - Fichiers journaux que vous souhaitez conserver.
  - Rapports que vous souhaitez conserver.
  - Pages de notification personnalisées de l'utilisateur final stockées sur l'appliance.
  - Fichiers PAC stockés sur l'appliance.

Étape 1 Connectez-vous à l'interface de ligne de commande de l'appliance dont vous voulez rétablir une version antérieure.

Note Lorsque vous exécutez la commande `revert` à l'étape suivante, plusieurs invites d'avertissement sont émises. Une fois ces avertissements acceptés, le rétablissement de la version antérieure est exécuté immédiatement. Par conséquent, ne commencez pas le processus de restauration avant d'avoir terminé les étapes préalables au rétablissement de la version antérieure.

Étape 2 Saisissez la commande `revert`.

Étape 3 Confirmez deux fois que vous souhaitez poursuivre le rétablissement de la version antérieure.

Étape 4 Choisissez l'une des versions disponibles auquel revenir.

L'appliance redémarre deux fois.

Note Le processus de rétablissement d'une version antérieure prend du temps. Cela peut prendre de quinze à vingt minutes avant que la restauration ne soit terminée et que l'accès à l'appliance par la console soit à nouveau disponible.

L'appliance devrait maintenant fonctionner avec la version sélectionnée d'AsyncOS pour le Web. Vous pouvez accéder à l'interface Web à partir d'un navigateur Web.

Supervision de l'intégrité et de l'état du système à l'aide de SNMP

Le système d'exploitation AsyncOS prend en charge la supervision de l'état du système par le biais de SNMP (Simple Network Management Protocol). (Pour en savoir plus sur SNMP, consultez les RFC 1065, 1066 et 1067.)

Prenez note :

- SNMP est **désactivé** par défaut.
- Les opérations SET de SNMP (configuration) ne sont pas mises en œuvre.
- AsyncOS prend en charge SNMPv1, v2 et v3. Pour en savoir plus sur SNMPv3, consultez les RFC 2571-2575.
- L'authentification et le chiffrement des messages sont obligatoires lors de l'activation de SNMPv3. Les phrases secrètes pour l'authentification et le chiffrement doivent être différentes. L'algorithme de chiffrement peut être AES (recommandé) ou DES. L'algorithme d'authentification peut être SHA-1 (recommandé) ou MD5. La commande snmpconfig « se souviendra » de vos phrases secrètes la prochaine fois que vous l'exécuterez.
- Le nom d'utilisateur SNMPv3 est : v3get.

```
> snmpwalk -v 3 -l AuthNoPriv -u v3get -a MD5 serv.example.com
```

- Si vous utilisez uniquement SNMPv1 ou SNMPv2, vous devez définir un identifiant de communauté. L'identifiant de communauté ne prend pas la valeur `public` par défaut.
- Pour SNMPv1 et SNMPv2, vous devez spécifier un réseau à partir duquel les demandes SNMP GET sont acceptées.
- Pour utiliser des interruptions, un gestionnaire SNMP (non inclus dans AsyncOS) doit être en cours d'exécution et son adresse IP doit être saisie comme cible d'interruption. (Vous pouvez utiliser un nom d'hôte, mais si vous le faites, les interruptions ne fonctionneront que si le DNS est opérationnel.)

Fichiers MIB

Les fichiers MIB sont disponibles à l'adresse suivante http://www.cisco.com/c/en/us/support/security/web-security-appliance/tsd-products-support-series-home.html

Utilisez la dernière version de chaque fichier MIB.

Il existe plusieurs fichiers MIB :

- asyncoswebsecurityappliance-mib.txt : description compatible avec SNMPv2 de la MIB d'entreprise pour les Secure Web Appliance.
- ASYNCOS-MAIL-MIB.txt : description compatible avec SNMPv2 de la MIB d'entreprise pour les appliances de sécurité de la messagerie.
- IRONPORT-SMI.txt : ce fichier de « structure des informations de gestion » définit le rôle d'asyncoswebsecurityappliance-mib.

Cette version met en œuvre un sous-ensemble en lecture seule de MIB-II, comme défini dans les RFC 1213 et 1907.

Consultez https://www.cisco.com/c/en/us/support/docs/security/web-security-appliance/118415-technote-wsa-00.html pour en savoir plus sur la supervision de l'utilisation du processeur sur l'appliance à l'aide de SNMP.

Activation et configuration de la supervision SNMP

Pour configurer SNMP afin de recueillir des informations sur l'état du système pour l'appliance, utilisez la commande snmpconfig dans l'interface de ligne de commande (CLI). Une fois que vous avez choisi et configuré les valeurs d'une interface, l'appliance répond aux demandes SNMPv3 GET.

Lorsque vous utilisez la supervision SNMP, gardez les points suivants à l'esprit :

- Ces demandes de version 3 doivent inclure une phrase secrète correspondante.
- Par défaut, les demandes des versions 1 et 2 sont rejetées.
- Si elle est activée, les demandes des versions 1 et 2 doivent avoir un identifiant de communauté correspondant.

Objets matériels

Des capteurs matériels conformes à la spécification IPMI (Intellect Platform Management Interface Precision) transmettent des renseignements comme la température, la vitesse du ventilateur et l'état du bloc d'alimentation.

Pour déterminer les objets matériels disponibles pour la supervision (par exemple, le nombre de ventilateurs ou la plage de températures de fonctionnement), consultez le guide du matériel pour votre modèle d'appliance.

Thèmes connexes

- Documentation

Interruptions SNMP

SNMP permet d'envoyer des interruptions, ou des notifications, pour informer une application d'administration qu'une ou plusieurs conditions sont satisfaites. Les interruptions sont des paquets réseau qui contiennent des

données relatives à un composant du système qui envoie l'interruption. Les interruptions sont générées quand une condition est remplie sur l'agent SNMP (dans ce cas, Cisco Secure Web Appliance). Une fois la condition remplie, l'agent SNMP forme un paquet SNMP et l'envoie à l'hôte qui exécute le logiciel de la console de gestion SNMP.

Vous pouvez configurer les interruptions SNMP (activer ou désactiver des interruptions particulières) lorsque vous activez SNMP pour une interface.

Pour spécifier plusieurs cibles d'interruption : lorsque vous êtes invité à saisir la cible d'interruption, vous pouvez entrer jusqu'à 10 adresses IP séparées par des virgules.

Thèmes connexes

- À propos de l'interruption SNMP connectivityFailure , on page 71

À propos de l'interruption SNMP connectivityFailure

L'interruption connectivityFailure est destinée à surveiller la connexion de votre appliance à Internet. Pour ce faire, il tente de se connecter et envoie une requête HTTP GET à un seul serveur externe toutes les 5 à 7 secondes. Par défaut, l'URL surveillée est `downloads.ironport.com` sur le port 80.

Pour modifier l'URL ou le port surveillés, exécutez la commande `snmpconfig` et activez l'interruption connecivityFailure, même si elle est déjà activée. Vous verrez une invite pour modifier l'URL.

Tip Pour simuler des interruptions connectivityFailure, vous pouvez utiliser la commande d'interface de ligne de commande `dnsconfig` pour saisir un serveur DNS qui ne fonctionne pas. Les recherches pour downloads.ironport.com vont échouer, et des interruptions seront envoyées toutes les 5 à 7 secondes. Assurez-vous de remplacer le serveur DNS par un serveur qui fonctionne après avoir terminé votre test.

Exemple d'interface de ligne de commande : snmpconfig

```
wsa.example.com> snmpconfig

Current SNMP settings:
SNMP Disabled.

Choose the operation you want to perform:
- SETUP - Configure SNMP.
[]> SETUP

Do you want to enable SNMP?
[Y]>

Please choose an IP interface for SNMP requests.
1. Management (198.51.100.1: wsa.example.com)
[1]>

Which port shall the SNMP daemon listen on interface "Management"?
[161]>

Please select SNMPv3 authentication type:
1. MD5
2. SHA
[1]> 2
```

```
Please select SNMPv3 privacy protocol:
1. DES
2. AES
[1]> 2

Enter the SNMPv3 authentication passphrase.
[]>

Please enter the SNMPv3 authentication passphrase again to confirm.
[]>

Enter the SNMPv3 privacy passphrase.
[]>

Please enter the SNMPv3 privacy passphrase again to confirm.
[]>

Service SNMP V1/V2c requests?
[N]> Y

Enter the SNMP V1/V2c community string.
[ironport]> public

Shall SNMP V2c requests be serviced from IPv4 addresses?
[Y]>

From which IPv4 networks shall SNMP V1/V2c requests be allowed? Separate
multiple networks with commas.
[127.0.0.1/32]>

Enter the Trap target as a host name, IP address or list of IP
addresses separated by commas (IP address preferred). Enter "None" to disable traps.
[127.0.0.1]> 203.0.113.1

Enter the Trap Community string.
[ironport]> tcomm

Enterprise Trap Status
1. CPUUtilizationExceeded       Disabled
2. FIPSModeDisableFailure       Enabled
3. FIPSModeEnableFailure        Enabled
4. FailoverHealthy              Enabled
5. FailoverUnhealthy            Enabled
6. RAIDStatusChange             Enabled
7. connectivityFailure          Disabled
8. fanFailure                   Enabled
9. highTemperature              Enabled
10. keyExpiration               Enabled
11. linkUpDown                  Enabled
12. memoryUtilizationExceeded   Disabled
13. powerSupplyStatusChange     Enabled
14. resourceConservationMode    Enabled
15. updateFailure               Enabled
Do you want to change any of these settings?
[N]> Y

Do you want to disable any of these traps?
[Y]> n

Do you want to enable any of these traps?
[Y]> y

Enter number or numbers of traps to enable.  Separate multiple numbers with
```

```
commas.
[]> 1,7,12

What threshold would you like to set for CPU utilization?
[95]>

What URL would you like to check for connectivity failure?
[http://downloads.ironport.com]>

What threshold would you like to set for memory utilization?
[95]>

Enter the System Location string.
[Unknown: Not Yet Configured]> Network Operations Center - west; rack #30, position 3

Enter the System Contact string.
[snmp@localhost]> wsa-admin@example.com

Current SNMP settings:
Listening on interface "Management" 198.51.100.1  port 161.
SNMP v3: Enabled.
SNMP v1/v2: Enabled, accepting requests from subnet 127.0.0.1/32 .
SNMP v1/v2 Community String: public
Trap target: 203.0.113.1
Location: Network Operations Center - west; rack #30, position 3
System Contact: wsa-admin@example.com

Choose the operation you want to perform:
- SETUP - Configure SNMP.
[]>

wsa.example.com> commit

Please enter some comments describing your changes:
[]> Enable and configure SNMP

Changes committed: Fri Nov 06 18:13:16 2015 GMT
wsa.example.com>
```

Dérivation du trafic Web

Avant de commencer : l'activation de la fonction Web Traffic Tap (Dérivation du trafic Web) réduira la capacité de traitement des transactions (demandes par seconde) de l'appliance, car cette dernière aura besoin de cycles de processeur et de mémoire supplémentaires pour copier les messages dans l'interface de dérivation.

Remarque Pour réduire l'impact sur les performances de la fonctionnalité Web Traffic Tap (Dérivation du trafic Web), réduisez le volume de trafic dérivé en définissant des politiques de dérivation du trafic Web appropriées.

Cette fonctionnalité n'est pas prise en charge sur Amazon Web Services (AWS)

La fonctionnalité Web Traffic Tap (Dérivation du trafic Web) vous permet de dériver le trafic Web HTTP et HTTPS qui traverse l'appliance et de le copier dans une interface Secure Web Appliance en ligne avec le trafic de données en temps réel. Vous pouvez sélectionner l'interface Secure Web Appliance à laquelle les données de trafic dérivées sont envoyées. Si le trafic dérivé inclut des données HTTPS, l'appliance les déchiffre en fonction des politiques de déchiffrement avant de les envoyer à l'interface de dérivation. Consultez Politiques de déchiffrement.

L'interface de dérivation sélectionnée doit être directement connectée à un périphérique de sécurité externe à des fins d'analyse, d'investigation et d'archivage. Sinon, elle peut être connectée à un commutateur L2 sur un VLAN dédié.

Remarque Le trafic reflété sur l'interface de dérivation est diffusé sur la couche Ethernet et n'est pas routable sur IP. Par conséquent, un VLAN dédié est requis s'il est connecté à un commutateur de couche 2.

Cette fonctionnalité vous permet également de définir des politiques de dérivation du trafic Web. En fonction de ces filtres de politique définis par le client, l'appliance reflète le trafic Web disponible pour le périphérique de sécurité externe. La fonctionnalité Web Traffic Tap (Dérivation du trafic Web) offre une visibilité sur le trafic HTTPS.

Le terme « dérivation » fait référence à la reconstitution de flux TCP (Transmission Control Protocol) complets comme s'ils se produisaient entre un client et un serveur directement connectés.

Les Secure Web Appliance virtuels prennent en charge la fonctionnalité Web Traffic Tap (Dérivation du trafic Web).

Remarque L'inspection du trafic SSL peut être soumise aux politiques de l'entreprise et/ou à la législation nationale. Cisco n'est responsable d'aucune obligation légale et il est de votre seule responsabilité de vous assurer que votre utilisation de la fonctionnalité Web Traffic Tap (Dérivation du trafic Web) sur Secure Web Appliance est conforme à ces exigences légales ou à ces politiques.

Vous devez effectuer les procédures suivantes pour dériver le trafic Web à l'aide de l'appliance :

1. Activer la fonctionnalité Web Traffic Tap (Dérivation du trafic Web)
2. Configurer les politiques de dérivation du trafic Web

Thèmes connexes

- Activation de la dérivation du trafic Web, à la page 74
- Configuration des politiques de dérivation du trafic Web, à la page 75

Activation de la dérivation du trafic Web

Avant de commencer

La fonctionnalité Web Traffic Tap (Dérivation du trafic Web) est désactivée par défaut. Vous devez activer cette fonctionnalité avant de définir les politiques de dérivation du trafic Web en sélectionnant **Web Security Manager** > **Web Traffic Tap Policies** (Politiques de dérivation du trafic Web).

Remarque Des politiques de déchiffrement doivent être définies afin de dériver les transactions HTTPS. Consultez Politiques de déchiffrement.

Étape 1 Choisissez **Network** > **Web Traffic Tap** (Réseau > Dérivation du trafic Web).

Étape 2 Cliquez sur **Edit Settings** (Modifier les paramètres).

Étape 3 Dans la page Edit Web Traffic Tap (Modifier la dérivation du trafic Web), cochez la case **Enable** (Activer) pour activer la fonction Web Traffic Tap (Dérivation du trafic Web).

Remarque Pour désactiver la fonctionnalité Web Traffic Tap feature, (Dérivation du trafic Web), décochez la case **Enable** (Activer). Si vous désactivez la fonctionnalité Web Traffic Tap (Dérivation du trafic Web), vous ne pourrez pas afficher ni modifier les politiques relatives à la dérivation du trafic Web. Vous devez réactiver cette fonction pour afficher et modifier les politiques.

Étape 4 Dans la liste déroulante Tap Interface (Interface de dérivation), choisissez l'interface Secure Web Appliance vers laquelle les données du trafic déviées sont envoyées. Les options d'interface sont P1, P2, T1 et T2. Consultez Connecter l'appliance pour en savoir plus sur les interfaces.

Remarque L'interface de dérivation sélectionnée doit être directement connectée à un périphérique de sécurité externe à des fins d'analyse, d'investigation et d'archivage. Sinon, elle peut être connectée à un commutateur L2 sur un VLAN dédié. L'interface de dérivation choisie doit être connectée et son état doit être actif; sinon, la mise en miroir du trafic dévié échouera.

Étape 5 Cliquez sur **Submit** (Envoyer) et validez vos modifications.

Configuration des politiques de dérivation du trafic Web

Étape 1 Choisissez **Web Security Manager** > **Web Traffic Tap Policies** (Politiques de dérivation du trafic Web).

Étape 2 Cliquez sur **Add Policy** (Ajouter une politique).

Suivez les instructions à la section Création d'une politique pour ajouter une nouvelle politique de dérivation du trafic Web.

Remarque Une politique de dérivation du trafic globale sans dérivation définie est disponible par défaut dans la page Web Traffic Tap Policies (Politiques de dérivation du trafic Web) [**Web Security Manager** > **Web Traffic Tap Policies** (Web Security Manager > Politiques de dérivation du trafic Web)].

Étape 3 Développez la section avancée de la zone de définition de membre de politique pour ajouter les critères d'appartenance au groupe supplémentaires suivants pour la dérivation du trafic Web.

- Protocols (Protocoles) : choisissez les protocoles HTTP, HTTPS ou les deux pour créer une politique de déviation du trafic Web.

  Remarque Vous devez définir la politique de déchiffrement correspondante [**Web Security Manager** > **Decryption Policies** (Web Security Manager > Politiques de déchiffrement)] afin de dériver le trafic HTTPS.

  Les politiques de dérivation du trafic Web ne prennent pas en charge les protocoles natifs FTP et SOCKS.

- Subnets (Sous-réseaux)

- URL Categories (Catégories d'URL) : définissez les catégories de filtrage d'URL sur **Tap** (Dérivation) **No Tap** (Sans dérivation), selon vos besoins. Pour définir le dérivateur de trafic pour les URL non classées, choisissez **Tap** (Dérivation) dans la liste déroulante des URL non classées et cliquez sur **Submit** (Envoyer).
- User Agents (Agents utilisateur)

Consultez Création d'une politique pour en savoir plus sur la définition de critères d'appartenance à un groupe supplémentaires.

Remarque Le trafic que vous souhaitez dériver doit satisfaire à toutes les conditions de filtre que vous avez définies pour la politique de dérivation du trafic Web.

Vous pouvez également ajouter des catégories d'URL à partir du tableau de filtrage d'URL en sélectionnant **Web Security Manager** > **Web Traffic Tap Policies** (Web Security Manager > Politiques de dérivation du trafic Web).

Remarque Si vous avez déjà ajouté les catégories d'URL dans la section Advanced (Avancé), vous ne verrez que les catégories d'URL répertoriées dans le tableau de filtrage d'URL [**Web Security Manager** > **Web Traffic Tap Policies** (Web Security Manager > Politiques de dérivation du trafic Web)].

Consultez Ordre des politiques pour connaître l'ordre des politiques de dérivation du trafic Web.

Configuration du protocole HTTP 2.0

La version 14.0 de Cisco AsyncOS prend en charge HTTP 2.0 pour les demandes et les réponses Web sur TLS.

HTTP 2.0 pour les requêtes et réponses Web sur TLS. La prise en charge de HTTP 2.0 nécessite une négociation basée sur TLS ALPN, disponible uniquement à partir de la version TLS 1.2.

Dans cette version, HTTPS 2.0 n'est pas pris en charge pour les fonctionnalités suivantes :

- Dérivation du trafic Web
- DLP externe
- Bande passante globale et bande passante de l'application

Remarque Par défaut, la fonctionnalité HTTP 2.0 est désactivée et utilisez la commande de l'interface de ligne de commande HTTP 2 pour l'activer.

La fonctionnalité HTTP 2.0 prend en charge :

- Un maximum de 4096 sessions simultanées et 128 flux simultanés
- Tous les protocoles HTTP dans l'ALPN et un maximum de sept protocoles dans l'ALPN annoncé.
- Une taille d'en-tête maximale de 16 Ko.

Remarque CONNECT pour le proxy explicite dans la version 2.0 commence également par HTTP 1.1.

Une nouvelle commande de l'interface de ligne de commande `HTTP2` est introduite pour activer ou désactiver les configurations HTTP 2.0. Voir les commandes d'interface de ligne de commande Secure Web Appliance.

Vous ne pouvez pas activer ou désactiver HTTP 2.0 et restreindre le domaine pour HTTP 2.0 à l'aide de l'interface utilisateur Web de l'appliance. La configuration de HTTP 2.0 n'est pas prise en charge par Cisco Secure Email and Web Manager (appliances de gestion de la sécurité du contenu Cisco).

- Lorsque l'URL échoue à la fois dans les listes d'exceptions HTTP 2 et dans les catégories d'URL d'intercommunication, HTTP 2 prévaut sur l'intercommunication.
- La journalisation ALPN n'est pas cohérente pour les catégories d'URL de liaison.

À propos de la traduction

Cisco peut fournir des traductions du présent contenu dans la langue locale pour certains endroits. Veuillez noter que des traductions sont fournies à titre informatif seulement et, en cas d’incohérence, la version anglaise du présent contenu prévaudra.