# Comprenez comment la caractéristique automatique de mise à jour de signature de Cisco IPS fonctionne

## Contenu


Introduction
Conditions préalables
Conditions requises
Composants utilisés
Conventions
Informations générales
Spécifications du réseau
Mises en garde de contournement
Processus automatique de mise à jour de signature
Configurez
Configuration de base d'Automatique-mise à jour de signature
Améliorations automatiques de mise à jour de signature
La mise à jour comportent maintenant
Mise à jour automatique par l'intermédiaire de proxy d'Internet
Validez les certificats racine de confiance
Visualisez la mémoire locale de certificat de confiance
Validation stricte de certificat de serveur de TLS d'enable
Certificats racine d'Add/Update à la mémoire locale de certificat de confiance
Vérifiez
Dépannez


## Introduction

Ce document fournit un aperçu de la caractéristique automatique de mise à jour du Système de protection contre les intrusions Cisco (IPS) et de son exécution.

La caractéristique automatique de mise à jour IPS a été introduite dans la version 6.1 IPS et fournit à des administrateurs une méthode facile de mettre à jour des signatures IPS sur un intervalle régulièrement programmé.

## Conditions préalables

### Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Les mises à jour de signature exigent un abonnement et une clé de licence valides de Services Cisco pour IPS. Allez à http://www.cisco.com/go/license et cliquez sur l'**abonnement de signature IPS** afin de s'appliquer pour une clé de licence.
- Un compte utilisateur de Cisco.com (CCO) qui est associé avec un abonnement actif de Services Cisco pour IPS.
- Privilèges de télécharger le logiciel cryptographique. Allez à : http://tools.cisco.com/legal/k9/controller/do/k9Check.x?eind=Y afin de vérifier si vous avez accès.

## Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Versions 6.1 et ultérieures de Cisco IPS
- Caractéristiques spécifiques pour des versions 7.2(1) de Cisco IPS, 7.3(1), et plus tard

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

### Conventions

Pour plus d'informations sur les conventions utilisées dans ce document, reportez-vous à Conventions relatives aux conseils techniques Cisco.

# Informations générales

### Spécifications du réseau

1. L'interface de commandement et de contrôle de l'IPS exige l'accès direct à l'Internet utilisant HTTPS (TCP 443) et HTTP (TCP 80).
2. Le Traduction d'adresses de réseau (NAT) et le Listes de contrôle d'accès (ACL) sur des périphériques de périphérie tels que des Routeurs et des Pare-feu doivent être configurés afin de permettre la Connectivité IPS à l'Internet.
3. Excluez l'adresse IP d'interface de commandement et de contrôle de tous les filtres de contenu et modélisateurs du trafic réseau.
4. Les serveurs proxys automatiques de prises en charge de fonctionnalité de mise à jour dans

7.2(1) la release certifiée par FIPS/CC. Toutes autres versions logicielles 6.x et 7.x ne prennent en charge pas la mise à jour automatique par un serveur proxy à ce moment. 7.2(1) La release inclut un certain nombre de modifications au Protocole Secure Shell (SSH) par défaut et aux configurations HTTPS. Référez-vous aux notes de mise à jour pour le Système de protection contre les intrusions Cisco 7.2(1)E4 avant que vous amélioriez à 7.2(1).

**Avertissement** : Dans la version 7.0(8)E4 de Cisco IPS, la valeur par défaut pour l'IP address de serveur Cisco est changée de 198.133.219.25 à 72.163.4.161 dans la configuration automatique URL de mise à jour. Si votre capteur est configuré pour les mises à jour automatiques, vous pourriez devoir mettre à jour les règles de Pare-feu afin de permettre au capteur pour se connecter à la nouvelle adresse IP. Pour des versions 7.2 et ultérieures de Cisco IPS, l'adresse IP du serveur automatique codée en dur de mise à jour est remplacée par une consultation Désignée de Fully-qualified-domain-name (FQDN) et de Système de noms de domaine (DNS). Référez-vous à la section de configuration de ce document pour information les informations complémentaires.

## Mises en garde de contournement

Quelques mises à jour de signature exigent des tables d'expression régulière d'être recompilées et pendant ce temps l'IPS peut entrer dans le mode bypass de logiciel. Pour les capteurs intégrés avec le mode bypass réglé à l'automatique, l'engine d'analyse est sautée permettant au trafic pour traverser les interfaces intégrées et les paires intégrées VLAN sans inspection.  Si le mode bypass est placé à hors fonction, le capteur intégré cesse le dépassement du trafic tandis que la mise à jour est appliquée.

## Processus automatique de mise à jour de signature

1. L'IPS authentifie au serveur automatique de mise à jour chez 72.163.4.161 utilisant HTTPS (TCP 443).

2. L'IPS envoie un client manifeste au serveur automatique de mise à jour, qui inclut l'ID de plate-forme et un secret partagé chiffré que le serveur l'utilise pour vérifier l'authenticité du capteur de Cisco IPS.

3. Une fois qu'authentifié, le serveur de mise à jour répond avec un serveur manifeste qui contient une liste d'options de fichier téléchargé associées avec l'ID de plate-forme. Les données contenues ici incluent relatif à l'information pour mettre à jour la version, le site de téléchargement, et les protocoles de transfert de fichiers pris en charge. Basé sur ces données, la logique automatique de mise à jour IPS détermine si les options l'unes des de téléchargement sont valides et puis sélectionne le meilleur module de mise à jour pour le téléchargement. En vue du téléchargement, le serveur fournit à l'IPS un ensemble de clés à utiliser pour déchiffrer le fichier de mise à jour.

4. L'IPS établit une nouvelle connexion au serveur de téléchargement identifié dans le serveur manifeste. L'adresse IP du serveur de téléchargement varie, qui dépend de l'emplacement.

L'IPS utilise le protocole de transfert de fichiers défini dans l'URL de données de téléchargement de fichier appris dans le serveur manifeste (actuellement HTTP d'utilisations (TCP 80)).

5. L'IPS emploie les clés précédemment téléchargées pour déchiffrer le module de mise à jour et puis applique les fichiers de signatures au capteur.

# Configurez

## Configuration de base d'Automatique-mise à jour de signature

La caractéristique automatique de mise à jour peut être configurée du gestionnaire de périphériques IPS (IDM) ou du Manager Express IPS (IME). Procédez comme suit :

1. D'IDM/IME, choisissez la **mise à jour de configuration > de Gestion > d'automatique de capteur/Cisco.com.**

2. Choisissez les **mises à jour de signature et d'engine d'enable de la** case de **Cisco.com** sur le volet droit, et cliquez sur en fonction le titre bleu de **configurations de serveur de Cisco.com** afin de relâcher vers le bas le volet de configuration.

3. Écrivez le nom d'utilisateur et mot de passe CCO.

   Voici un URL d'exemple pour des versions 7.0(8) et 7.1(6) de Cisco IPS :

   **https://72.163.4.161//cgi-bin/front.x/ida/locator/locator.pl**

   Voici un URL d'exemple pour des versions 7.2(1) de Cisco IPS, 7.3(1), et plus tard :

   **https://www.cisco.com//cgi-bin/front.x/ida/locator/locator.pl**

   **Note**: Ne changez pas l'URL de Cisco.com. Il ne devrait pas devoir être changé de sa valeur par défaut. //est intentionnel et pas une erreur typographique. Dans des versions 7.2(1) de Cisco IPS, 7.3(1), et plus tard, le capteur questionne le serveur DNS qui est défini en configuration réseau de capteur afin de résoudre l'URL de www.cisco.com à un IP address routable d'Internet.

4. Configurez une heure de début et une fréquence afin de programmer la mise à jour de signature. Il est recommandé pour placer l'heure de début à une période aléatoire qui n'est pas sur le dessus de l'heure.  Dans cet exemple, l'heure est placée à 23:15:00.  La fréquence peut être configurée pour la prendre en charge d'heure en heure ou des tentatives quotidiennes de mise à jour. Cliquez sur Apply afin d'appliquer des modifications de configuration.

# Améliorations automatiques de mise à jour de signature

Beaucoup d'améliorations à la caractéristique automatique de mise à jour sont incluses dans des versions 7.2(1) et ultérieures de Cisco IPS. Des améliorations de la sécurité supplémentaires sont également ajoutées aux versions 7.3(2) et ultérieures de Cisco IPS.  Référez-vous aux options de configuration décrites dans cette section pour information les informations complémentaires.

## La mise à jour comportent maintenant

La version 7.2(1) de Cisco IPS a introduit une nouvelle capacité au biais IPS et au CLI qui permet à des administrateurs pour initier une mise à jour automatique de signature immédiatement, qui saute la nécessité d'attendre le moment programmé de se produire.

Afin de sauter le programme de mise à jour et la mise à jour automatiques immédiatement, naviguez vers l'IDM/IME et choisissez la **mise à jour de configuration > de Gestion > d'automatique de capteur/Cisco.com. Tant que** la mise à jour automatique est correctement configurée et appliquée, vous pouvez cliquer sur le **bouton d'**UpdateNow dans le coin supérieur droit de l'écran afin de déclencher une tentative de mise à jour.

Vous pouvez également sélectionner la commande d'**autoupdatenow** dans le capteur CLI afin de déclencher une tentative de mise à jour. Voici un exemple :

```
SSP-60# autoupdatenow
Warning: Executing this command will perform an auto-upgrade on the sensor immediately.
Before executing this command, you must have a valid license to apply the Signature
AutoUpdates and auto-upgrade settings configured.After executing this command please
disable user-server/cisco-server inside 'auto-upgrade' settings, if you don't want
scheduled auto-updates
Continue? []: yes
Automatic Update for the sensor has been executed.Use 'show statistics host' command
to check the result of auto-update.Please disable user-server/cisco-server in
auto-upgrade settings, if you don't want scheduled auto-updates
```

## Mise à jour automatique par l'intermédiaire de proxy d'Internet

Afin de déclencher une mise à jour automatique par l'intermédiaire du proxy d'Internet, naviguez vers l'IDM/IME et choisissez la **configuration > le capteur installés > réseau**. Écrivez les DN et (sur option) l'adresse IP de serveur proxy de HTTP et mettez en communication :

## Validez les certificats racine de confiance

La version 7.3(2) de Cisco IPS a introduit la capacité l'IPS de valider la chaîne de certificat racine du serveur d'updater quand des mises à jour sont téléchargées. Avec cette fonction activée, l'IPS valide si le certificat racine dans la chaîne de certificat est signé par une racine de confiance CA par exemple, les certificats racine de TLS qui sont obtenus dans le processus de mise à jour de signature du serveur Cisco et le serveur global de corrélation sont validés. Cette caractéristique

est actuellement désactivée par défaut dans la version 7.3(2) de Cisco IPS ; cependant, il pourrait être activé par défaut dans une version future.  Référez-vous à l'IPS *me lisent* pour en savoir plus de fichier.

### Visualisez la mémoire locale de certificat de confiance

Afin de visualiser la liste en cours de certificats racine de confiance installés dans des versions 7.3(2) et ultérieures IPS, naviguez vers la **configuration > la Gestion > les Certificats de capteur > les certificats racine de confiance** :

### Validation stricte de certificat de serveur de TLS d'enable

Terminez-vous ces étapes afin d'activer la caractéristique stricte de validation de serveur de TLS :

1. Naviguez vers la **configuration > le capteur installés > réseau**.
2. Développez le **HTTP, FTP, telnet, SSH, CLI et d'autres options** relâchent vers le bas le menu.
3. Cochez la case **stricte de validation de serveur de TLS d'enable**.
4. Cliquez sur Apply afin d'appliquer la configuration au capteur.

### Certificats racine d'Add/Update à la mémoire locale de certificat de confiance

Pendant que les Certificats expirent sur les serveurs d'updater, Cisco se réserve le droit d'utiliser une chaîne de certificat racine autre que GeoTrust et Thawte. Si le certificat mis à jour n'existe pas dans l'image logicielle IPS de courant, alors la chaîne de certificat racine mise à jour peut être manuellement installée dans le stock local de certificat de confiance du capteur. Les Certificats DER-encodés peuvent être placés sur un serveur de fichiers et être récupérés par le capteur par l'intermédiaire du SCP ou du HTTPS. L'exemple suivant emploie le SCP afin d'expliquer l'installation de certificat/processus de mise à jour.

1. De l'IDM/IME, naviguez vers la **configuration > la Gestion > le SSH de capteur > les clés RSA connues d'hôte**.
2. Cliquez sur Add et écrivez l'adresse IP du serveur SCP.
3. Le clic **récupèrent la clé de hôte** afin de faire récupérer le capteur automatiquement la clé publique du serveur.
4. Cliquez sur OK deux fois et **appliquez** alors afin d'appliquer la configuration au capteur. **Note**: Un avertissement apparaît si la taille de clé présentée par le serveur SCP est plus petite que 2,048 bits.
5. Le clic **oui** afin d'ajouter la clé aux hôtes connus ajournent ou **aucun** afin de retourner à l'écran de **clé RSA d'hôte connu par ajouter**.

6. Naviguez vers la **Gestion de configuration > de capteur > les certificats racine de confiance**.

7. Cliquez sur Add**/mise à jour** afin d'ajouter un nouveau fichier du certificat DER-encodé du serveur SCP. Assurez-vous que le fichier du certificat est mis en place préalablement sur le serveur et disponible pour la récupération distante par l'intermédiaire du SSH.

8. **Le SCP** choisi comme protocole et entrent l'URL, le nom d'utilisateur, et le mot de passe.

9. Cliquez sur OK afin de commencer le transfert de fichiers et l'installation de certificat.

10. Le clic **oui** afin d'ajouter le certificat aux gens du pays IPS a fait confiance à la mémoire de racine et alors **OK** afin de quitter.

# Vérifiez

De l'IDM/IME, choisissez la **mise à jour de configuration > de Gestion > d'automatique de capteur/Cisco.com. Développez la section Informations d'**AutoUpdate afin de passer en revue le statut de la dernière tentative de téléchargement. **Cliquez sur la** commande de Refreshin pour régénérer les **données de l'information d'**AutoUpdate.

Afin de vérifier le statut du processus automatique de mise à jour par l'intermédiaire du CLI, sélectionnez la commande d'**hôte de statistiques d'exposition** :

```
IPS# show statistics host
<Output truncated>
Auto Update Statistics
lastDirectoryReadAttempt = 16:55:03 GMT-06:00 Wed Jun 27 2012
= Read directory: http://CCOUser@72.163.7.55//swc/esd/06/273556262/guest/
= Success
lastDownloadAttempt = 16:55:03 GMT-06:00 Wed Jun 27 2012
= Download: http://CCOUser@72.163.7.55//swc/esd/06/273556262/guest/
IPS-sig-S654-req-E4.pkg
= Success
nextAttempt = 17:55:00 GMT-06:00 Wed Jun 27 2012
lastInstallAttempt = 16:55:46 GMT-06:00 Wed Jun 27 2012
= Success
<Output truncated>
```

De l'IDM/IME, référez-vous à l'instrument d'autorisation sur le tableau de bord à la maison afin de visualiser l'état de permis et la version actuellement installée de signature. Les mêmes informations peuvent être obtenues par l'intermédiaire du CLI avec la commande de **show version**.

```
SSP-60# show version
Application Partition:

Cisco Intrusion Prevention System, Version 7.3(2)E4
```

```
Host:
Realm Keys key1.0
Signature Definition:
Signature Update S805.0 2014-06-03
Threat Profile Version 7
OS Version: 2.6.29.1
Platform: ASA5585-SSP-IPS60
Serial Number: JAF1527CPNK
Licensed, expires: 21-Jun-2014 UTC
Sensor up-time is 39 days.
Using 46548M out of 48259M bytes of available memory (96% usage)
system is using 32.4M out of 160.0M bytes of available disk space (20% usage)
application-data is using 86.6M out of 377.5M bytes of available disk space (24% usage)
boot is using 63.4M out of 70.5M bytes of available disk space (95% usage)
application-log is using 494.0M out of 513.0M bytes of available disk space (96% usage)

MainApp C-2014_04_14_22_11_7_3_1_48 (Release) 2014-04-14T22:15:32-0500
Running
AnalysisEngine C-2014_04_14_22_11_7_3_1_48 (Release) 2014-04-14T22:15:32-0500
Running
CollaborationApp C-2014_04_14_22_11_7_3_1_48 (Release) 2014-04-14T22:15:32-0500
Running
CLI C-2014_04_14_22_11_7_3_1_48 (Release) 2014-04-14T22:15:32-0500

Upgrade History:

* IPS-sig-S802-req-E4 16:07:23 UTC Thu May 29 2014
IPS-sig-S805-req-E4.pkg 16:18:51 UTC Mon Jun 09 2014

Recovery Partition Version 1.1 - 7.3(2)E4

Host Certificate Valid from: 15-Jul-2013 to 16-Jul-2015
```

# Dépannez

Après configuration correcte de mise à jour automatique de signature, terminez-vous ces étapes afin d'isoler et corriger les questions généralement produites :

1. Pour tous les appliances IPS et modules excepté AIM et l'IDSM, assurez-vous que l'interface de commandement et de contrôle est connectée au réseau local, assigné un adresse IP/masque de sous-réseau valide/passerelle, et a l'accessibilité par IP à l'Internet. Pour les modules d'AIM et IDSM, la commande et l'interface de contrôle virtuelles ser de définies dans la configuration. Afin de confirmer le statut opérationnel de l'interface du CLI, sélectionnez cette commande show :

   ```
   IPS# show interfaces
   <Output truncated>
   MAC statistics from interface Management0/0
   Interface function = Command-control interface
   Description = Media Type = TX
   Default Vlan = 0
   Link Status = Up <---
   <Output truncated>
   ```

2. Afin de valider si le compte d'utilisateur CCO a des privilèges nécessaires de télécharger des

modules de mise à jour de signature, ouvrez un navigateur Web et une procédure de connexion à Cisco.com avec ce même compte CCO. Une fois qu'authentifié, téléchargez manuellement le dernier module de signature IPS. L'incapacité de télécharger manuellement le module est vraisemblablement due au manque d'association du compte utilisateur d'un abonnement valide de Services Cisco pour IPS. En outre, l'accès au logiciel de sécurité sur CCO est limité aux utilisateurs autorisés qui ont reçu l'accord annuel de cryptage/exportation. Le manque d'approuver cet accord a été connu d'empêcher des téléchargements de signature d'IDM/IME/CSM. Afin de vérifier si cet accord a été reçu, ouvrez un navigateur et une procédure de connexion à Cisco.com avec le même compte CCO. Une fois qu'authentifié, tentative de télécharger manuellement le Cisco IOS ? progiciel avec l'ensemble de caractéristiques K9.

3. Vérifiez s'il y a un proxy en place pour le trafic attaché d'Internet (tous les versions excepté 7.2(1) et plus tard). Si le trafic du port de commandement et de contrôle passe par ce proxy, la caractéristique automatique de mise à jour ne fonctionne pas. Modifiez le réseau de sorte que le trafic portuaire de commandement et de contrôle ne soit pas filtré à l'aide d'un proxy et testez de nouveau.

4. Pour les capteurs qui exécutent le logiciel de versions 7.2 ou 7.3, assurez-vous qu'un ou plusieurs serveurs DNS sont configurés. Ceci est exigé de sorte que le capteur puisse résoudre le FQDN d'updater de www.cisco.com à une adresse IP d'Internet-routable.

5. Vérifiez s'il y a n'importe quel filtrage selon le contenu ou trafiquez en formant des applications ou des appliances dans le chemin à l'Internet. Si le présent, configurent une exclusion afin de permettre l'adresse IP de l'interface de commandement et de contrôle d'accéder à l'Internet sans restriction.

6. Si on permet le trafic d'ICMP vers l'Internet, ouvrez le CLI du capteur et de l'essai IPS pour cingler une adresse IP publique.

   Ce test peut être utilisé pour vérifier si le routage et les règles NAT nécessaires (si utilisé) sont configurés correctement. Si le test d'ICMP réussit pourtant les mises à jour automatiques continuent à échouer, assurez-vous que les périphériques de réseau tels que des Routeurs et des Pare-feu le long du chemin permettent les sessions HTTPS et de HTTP de l'IP d'interface de commandement et de contrôle IPS. Par exemple, si l'adresse IP de commandement et de contrôle est 10.1.1.1, un rubrique de liste ACL simple sur un Pare-feu ASA peut ressembler à cet exemple :

```
IPS# show interfaces
<Output truncated>
MAC statistics from interface Management0/0
Interface function = Command-control interface
Description = Media Type = TX
Default Vlan = 0
Link Status = Up <---
<Output truncated>
```

7. Le nom d'utilisateur CCO ne devrait contenir aucun caractères particuliers, par exemple,

@. Référez-vous au pour en savoir plus de l'ID de bogue Cisco CSCsq30139.

8. Quand les pannes d'automatique-mise à jour de signature se produisent, employez la prochaine table afin d'apparier codes d'erreur associés de HTTP.

```
IPS# show statistics host
Auto Update Statistics
lastDirectoryReadAttempt = 19:31:09 CST Thu Nov 18 2010
= Read directory: https://72.163.4.161//cgi-bin/front.x/ida/locator/locator.pl
= Error: AutoUpdate exception: HTTP connection failed [1,110] <--
lastDownloadAttempt = 19:08:10 CST Thu Nov 18 2010
lastInstallAttempt = 19:08:44 CST Thu Nov 18 2010
nextAttempt = 19:35:00 CST Thu Nov 18 2010
```

| Message | Signification |
|---|---|
| Erreur : Exception d'AutoUpdate : La connexion HTTP a manqué [1,110] | Échec de l'authentification. Vérifiez le nom d'utilisateur et mot de passe. |
| exception d'AutoUpdate de status=false : Recevez la réponse de HTTP a manqué [3,212] | La demande au serveur automatique de mise à jour chronométré. |
| Erreur : réponse d'erreur de HTTP : 400 | Assurez-vous que la configuration Cisco-URL est transférée. Si l'ID CCO est plus grand c caractères de longueur, essayez un ID CCO différent. Ceci peut être une limite sur le serv téléchargement de Cisco. |
| Erreur : Exception d'AutoUpdate : La connexion HTTP a manqué [1,0] | Le problème de réseau a empêché le téléchargement ou il y a un éventuel problème avec serveurs de téléchargement. |