Exemple de configuration de CiscoWorks Management Center IPS dans IPS Cisco IOS

Contenu

Introduction

CiscoWorks Management Center for IPS Sensors (IPS MC) est la console de gestion des périphériques Cisco IPS. IPS MC version 2.2 prend en charge le provisionnement de la fonctionnalité IPS (Intrusion Prevention System) sur les routeurs du logiciel Cisco IOS®. Ce document décrit comment utiliser IPS MC 2.2 pour configurer Cisco IOS IPS.

Pour plus d'informations sur l'utilisation d'IPS MC (qui inclut comment l'utiliser pour configurer des périphériques qui ne sont pas basés sur le logiciel Cisco IOS), consultez la documentation de CiscoWorks Management Center for IPS Sensors à l'adresse suivante :

http://www.cisco.com/en/US/products/sw/cscowork/ps3990/index.html

Conditions préalables

Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

Components Used

Les informations de ce document sont basées sur la version 2.2 de CiscoWorks Management Center for IPS Sensors (IPS MC).

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

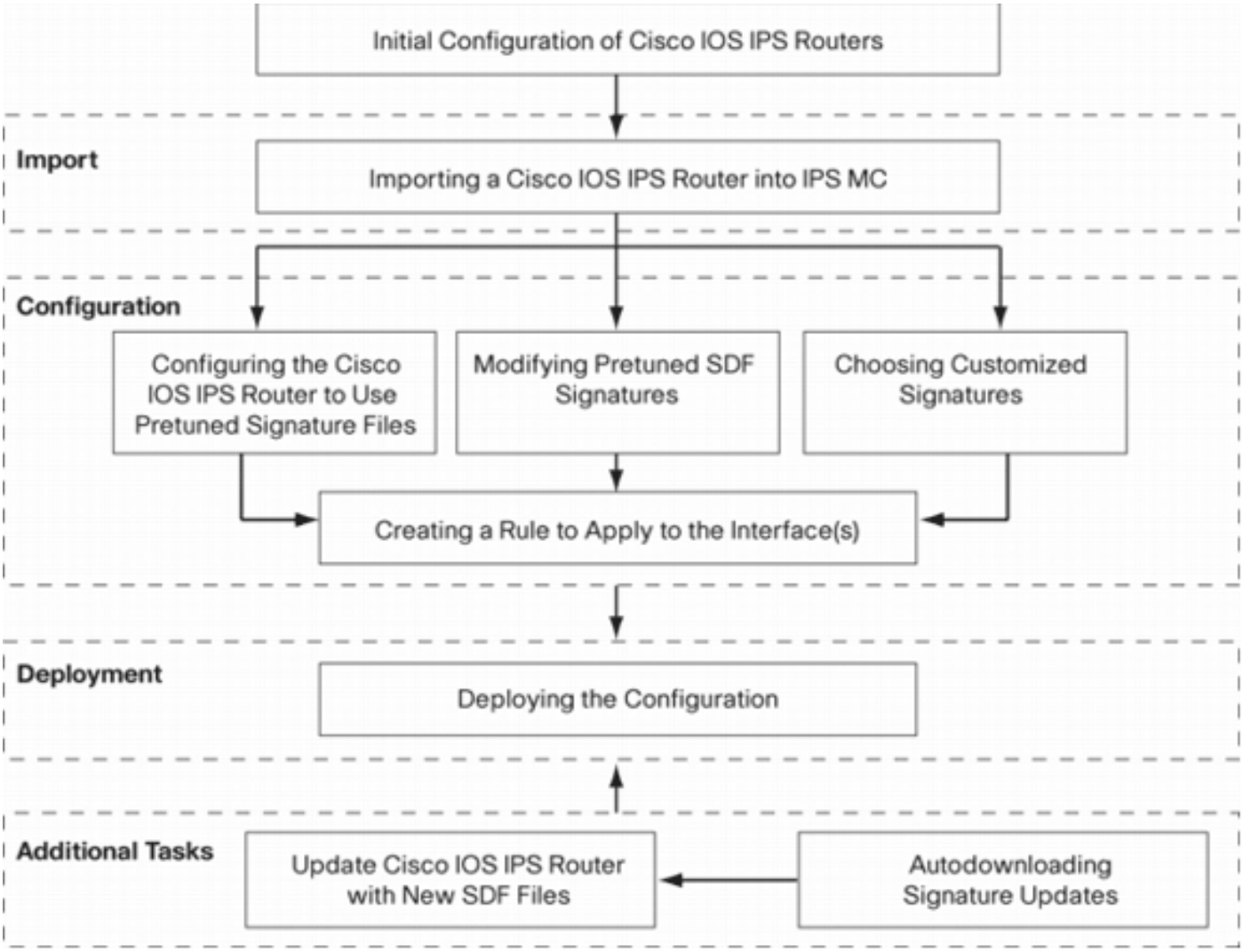
Conventions

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

Configuration

Compréhension de base des tâches de configuration

IPS MC est utilisé pour gérer la configuration d'un groupe de routeurs IPS Cisco IOS. Notez que IPS MC ne gère pas les alertes des routeurs qui exécutent IPS. Cisco recommande Cisco Security Monitoring, Analysis and Response System (Cisco Security MARS) pour la surveillance IPS. La gestion de la configuration consiste en une série de tâches décrites dans ce document. Ces tâches peuvent être divisées en trois phases : importez, configurez et déployez comme indiqué dans cette image.



Chaque phase a son propre ensemble de responsabilités et de fonctions :

- *Import* : importez un routeur dans IPS MC. Vous devez importer un routeur dans IPS MC avant de pouvoir utiliser IPS MC pour le configurer. Un routeur ne peut pas être importé sauf s'il existe une configuration IPS initiale sur le routeur (les détails sont donnés plus loin dans ce document).
- *Configuration* : configurez le périphérique. Par exemple, vous pouvez configurer un routeur IPS Cisco IOS pour utiliser l'un des fichiers de signature préconfigurés recommandés par Cisco. Les modifications de configuration sont stockées dans IPS MC, mais ne sont pas envoyées au routeur dans cette phase.
- *Déploiement* : permet de modifier la configuration du périphérique réel. Au cours de cette phase, vous validez les modifications apportées aux tâches de configuration aux routeurs.
- *Tâches supplémentaires* - IPS MC fournit une fonction de téléchargement automatique pour télécharger automatiquement les mises à jour de signature à partir de Cisco.com.

Vous devez comprendre cette approche progressive afin d'utiliser efficacement IPS MC. Il est différent des interfaces utilisateur graphiques de gestion basées sur les périphériques, telles que Cisco Router and Security Device Manager (SDM). Les interfaces utilisateur graphiques basées sur les périphériques agissent directement sur un seul routeur, tandis que IPS MC est conçu pour fonctionner sur des groupes de routeurs (et d'autres périphériques IPS tels que les capteurs de la gamme Cisco IPS 4200) à l'échelle du réseau.

Ce document fournit des informations sur chacune des tâches du schéma pour vous aider à utiliser IPS MC pour gérer les routeurs IPS Cisco IOS.

Configuration initiale des routeurs IPS Cisco IOS

Pour importer ou ajouter un routeur IPS Cisco IOS à IPS MC, vous devez effectuer certaines étapes de configuration initiale sur les routeurs IPS Cisco IOS. Cette section décrit ces étapes.

Vous devez activer le protocole SSH (Secure Shell) dans un routeur IPS Cisco IOS pour la configuration, l'importation et le déploiement via Cisco IPS MC. En outre, le protocole SDEE (Security Device Event Exchange) doit être activé à des fins de rapport d'événements (bien que ces alertes ne soient pas envoyées à IPS MC car IPS MC est utilisé uniquement pour le provisionnement et non pour la création de rapports). Enfin, vous devez vous assurer que le paramètre d'horloge sur le routeur IPS est synchronisé avec la console de gestion IPS.

Complétez ces étapes afin de configurer vos routeurs IPS IOS :

1. Créez un nom d'utilisateur et un mot de passe locaux pour le routeur.
   ```
   Router#config terminal
   Router(config)#username <username> password <password>
   ```

2. Activez la connexion locale sur l'interface des lignes vty.
   ```
   Router#config terminal
   Router(config)#line vty 0 15
   Router(config-line)#login local
   Router(config-line)#exit
   ```

   Si l'interface de ligne de commande (CLI) transport input ou transport output est configurée sous la configuration de ligne vty, assurez-vous que SSH est activé. Exemple :
   ```
   Router#conf terminal
   Router(config)#line vty 0 15
   Router(config-line)#transport input ssh telnet
   Router(config-line)#exit
   ```

3. Générez une clé RSA 1 024 bits (si aucune clé n'existe déjà).SSH est automatiquement activé après la génération de la clé de chiffrement.
   ```
   Router#conf terminal
   Enter configuration commands, one per line. End with CNTL/Z.
   Router(config)#crypto key generate rsa
   The name for the keys will be: Router.cisco.com
   Choose the size of the key modulus in the range of 360 to 2048 for your General Purpose
   Keys.
       Choosing a key modulus greater than 512 may take a few minutes.
   How many bits in the modulus [512]: 1024
   % Generating 1024 bit RSA keys, keys will be non-exportable...[OK]
   Router(config)#
   *Jan 23 00:44:40.952: %SSH-5-ENABLED: SSH 1.99 has been enabled
   Router config)#
   ```
4. Activez SDEE sur le routeur.
   ```
   Router(config)#ip ips notify sdee
   ```

5. Activez HTTPS.HTTP ou HTTPS est requis pour qu'IPS MC communique avec le routeur avec SDEE afin de recueillir des informations sur les événements.
   ```
   Router(config)#ip http authentication local
   Router(config)#ip http secure-server
   ```

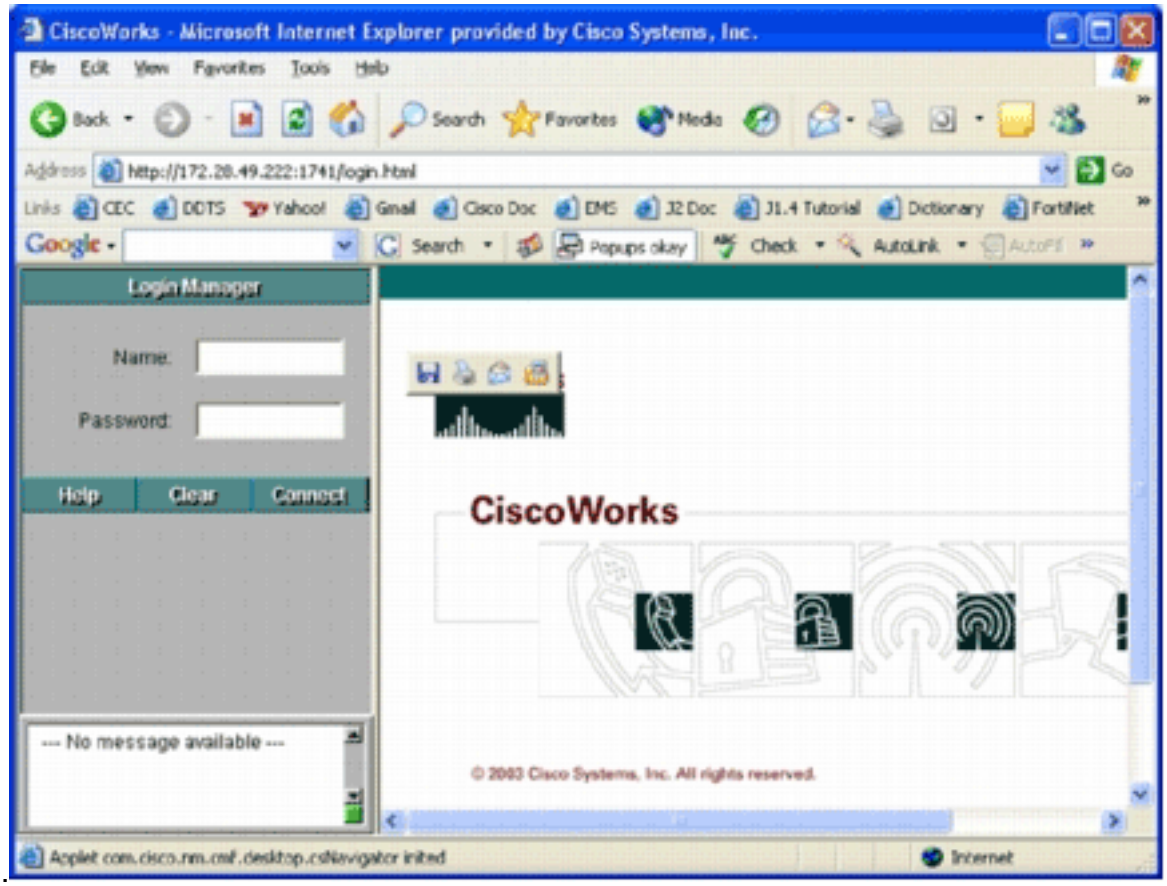
6. Utilisez la commande NTP (Network Time Protocol) ou clock externe afin de configurer le paramètre d'horloge sur le routeur IPS.

```
Router(config)#clock set hh:mm:ss day month year
```

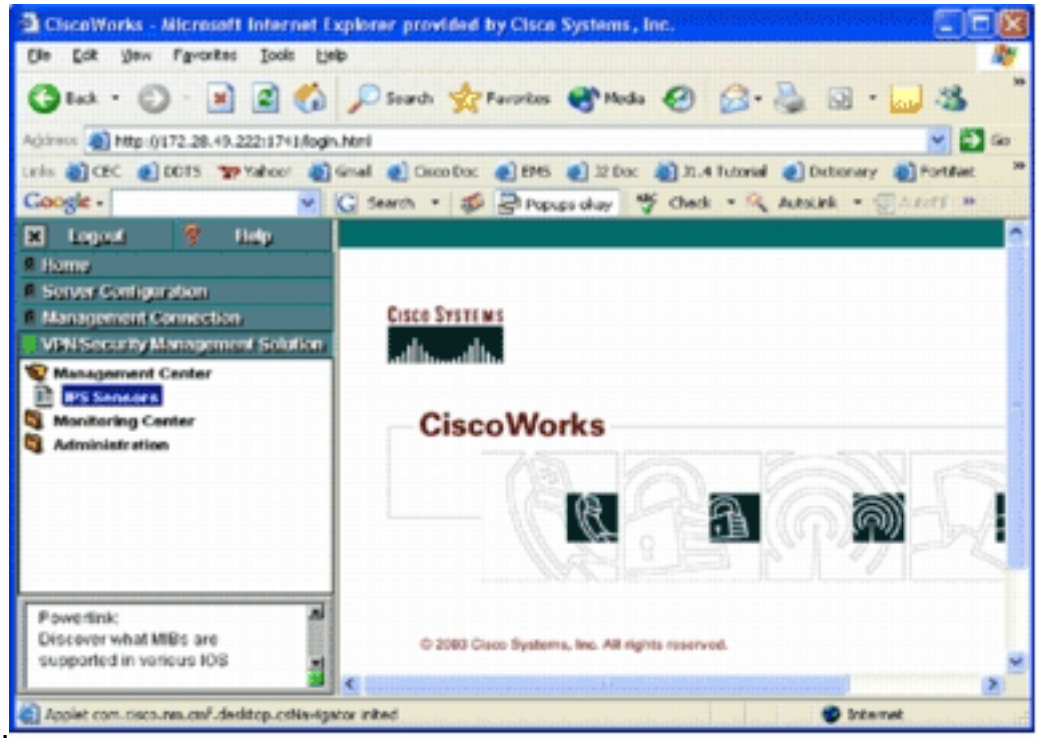
Désormais, le routeur IPS Cisco IOS est prêt et peut être importé dans IPS MC pour une configuration et une gestion supplémentaires.

Importer un routeur IPS Cisco IOS dans IPS MC

Une fois la configuration initiale terminée sur le routeur, vous pouvez l'ajouter (ou l'importer) dans IPS MC.

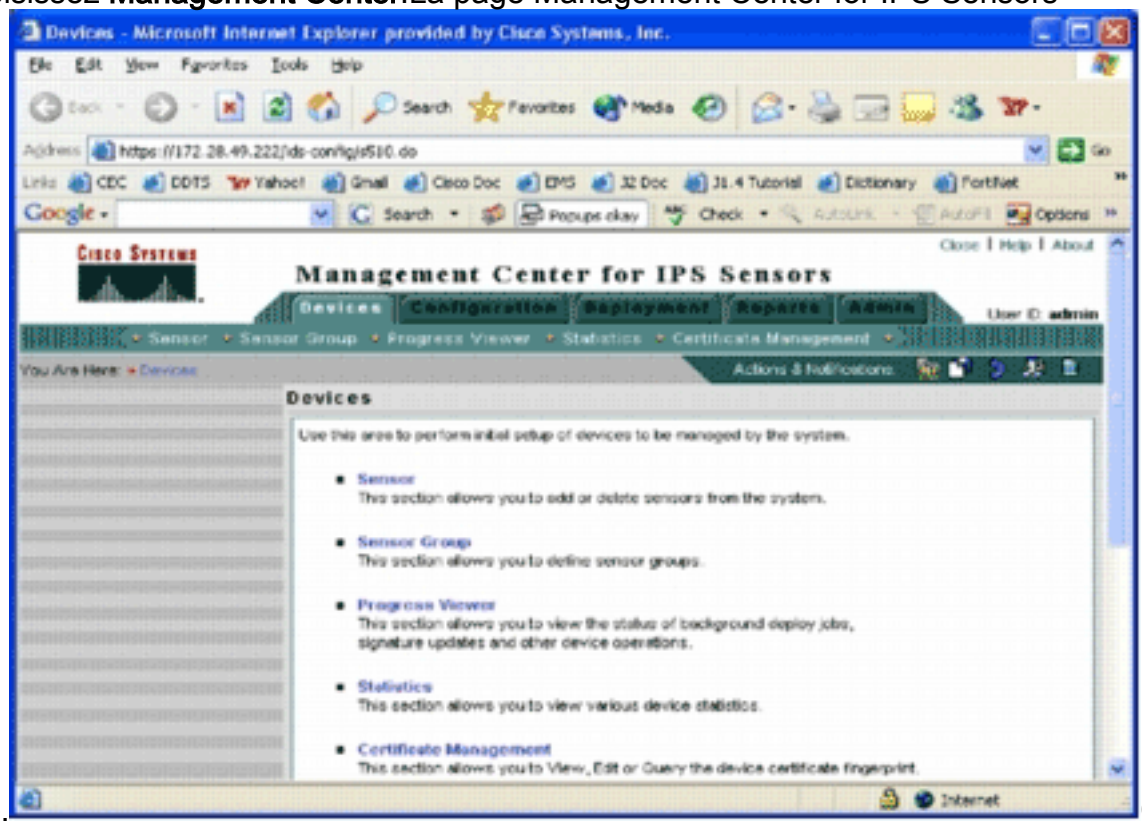
1. Démarrez votre navigateur Web et pointez sur le serveur CiscoWorks.Le Gestionnaire de connexion CiscoWorks s'affiche. 

R
emarque : le numéro de port par défaut du serveur Web est 1741 ; par conséquent, vous devez utiliser une URL similaire à http://<*adresse ip du serveur*>:1741/.
2. Entrez votre nom d'utilisateur et votre mot de passe afin de vous connecter.La page principale de CiscoWorks



s'affiche.

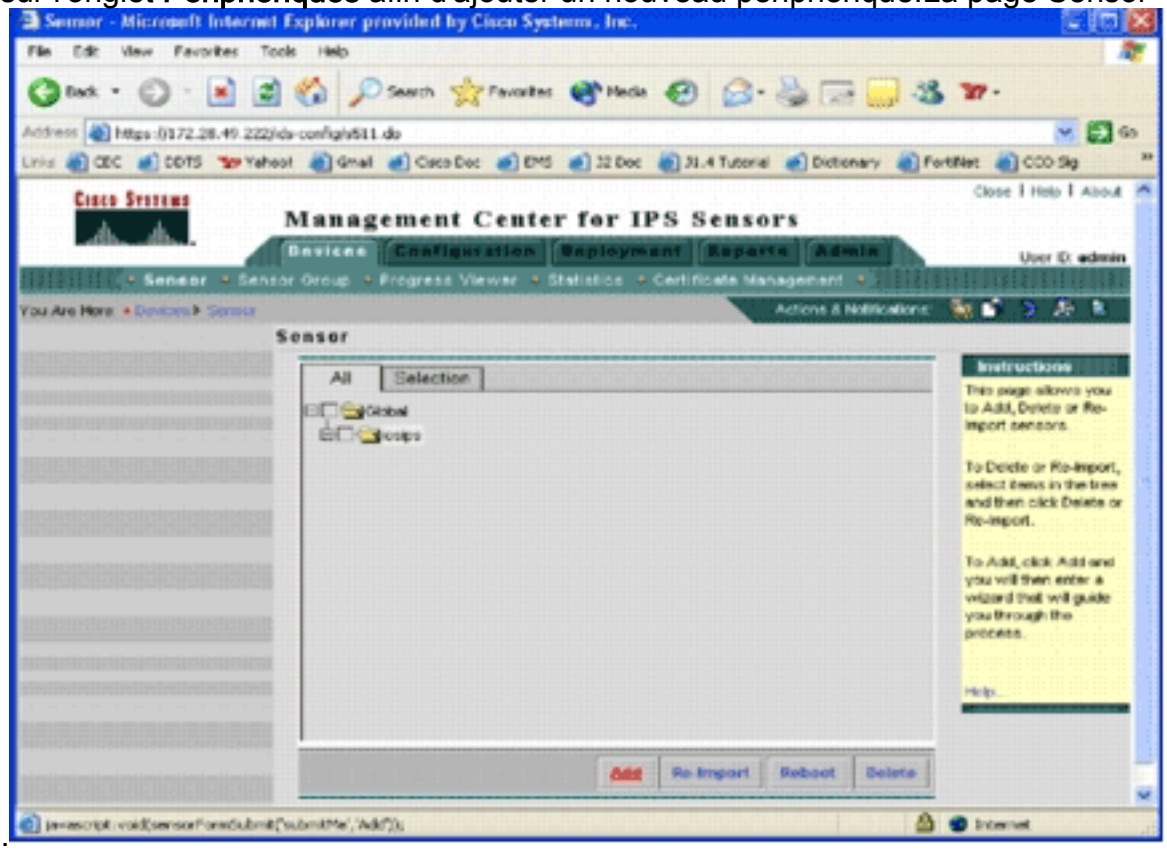
3. Dans le volet de navigation de gauche, sélectionnez **VPN/Security Management Solution**, puis choisissez **Management Center**.La page Management Center for IPS Sensors



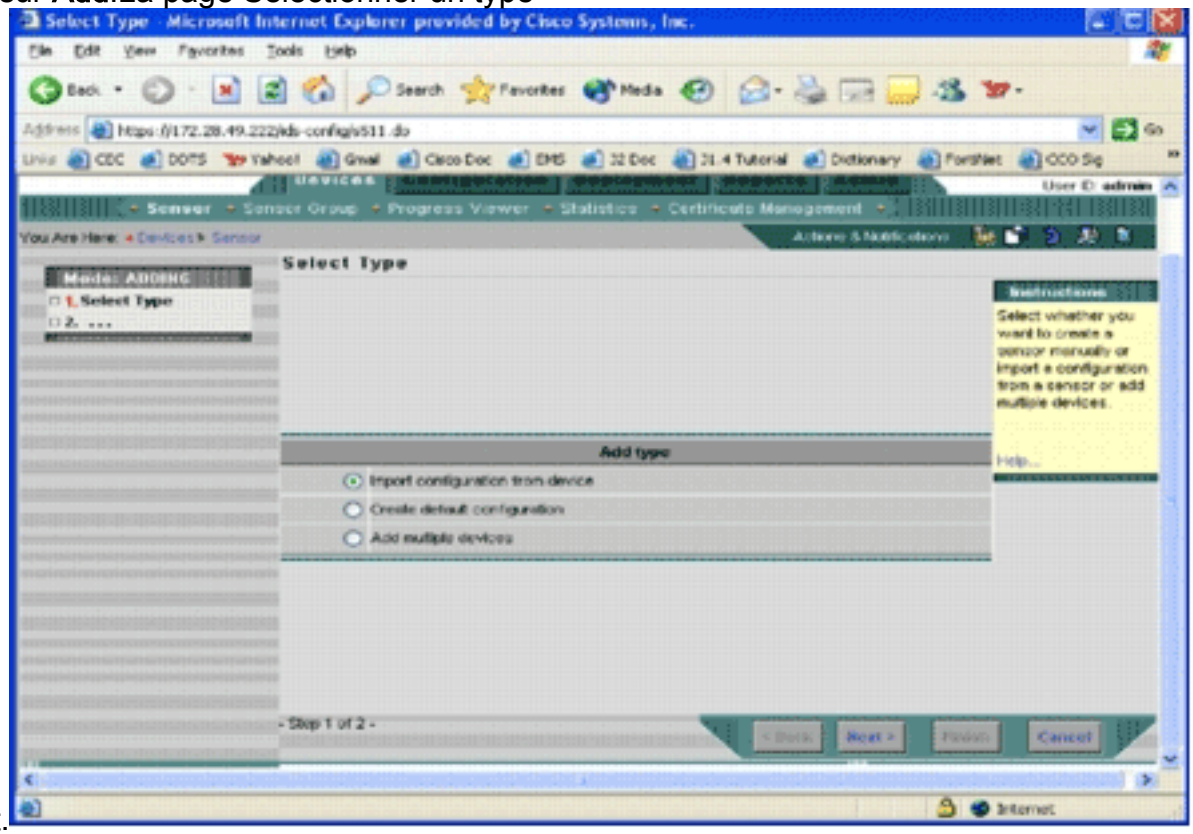
s'affiche.Cett e page affiche les cinq onglets suivants :*Périphériques* : dans l'onglet Périphériques, vous pouvez effectuer la configuration initiale et gérer tous les périphériques du système.*Configuration* - Dans l'onglet Configuration, vous pouvez effectuer des fonctions de provisionnement. Vous pouvez configurer des périphériques au niveau de chaque périphérique ou au niveau du groupe. Un groupe de périphériques peut contenir plusieurs périphériques. Toutes les modifications apportées par le biais des tâches de configuration doivent être enregistrées. La fonction de configuration ne modifie pas immédiatement les périphériques. Vous devez utiliser la fonction de déploiement pour déployer vos modifications.*Déploiement* : dans l'onglet Déploiement, vous pouvez déployer vos

modifications de configuration sur des périphériques. La fonctionnalité de planification permet de contrôler avec souplesse le moment où les modifications de configuration doivent prendre effet.*Rapports* : dans l'onglet Rapports, vous pouvez générer différents rapports d'opérations système.*Admin* - Dans l'onglet Admin, vous pouvez effectuer des tâches d'administration système, telles que la gestion de base de données, la configuration du système et la gestion des licences.

4. Cliquez sur l'onglet **Périphériques** afin d'ajouter un nouveau périphérique.La page Sensor s'affiche.

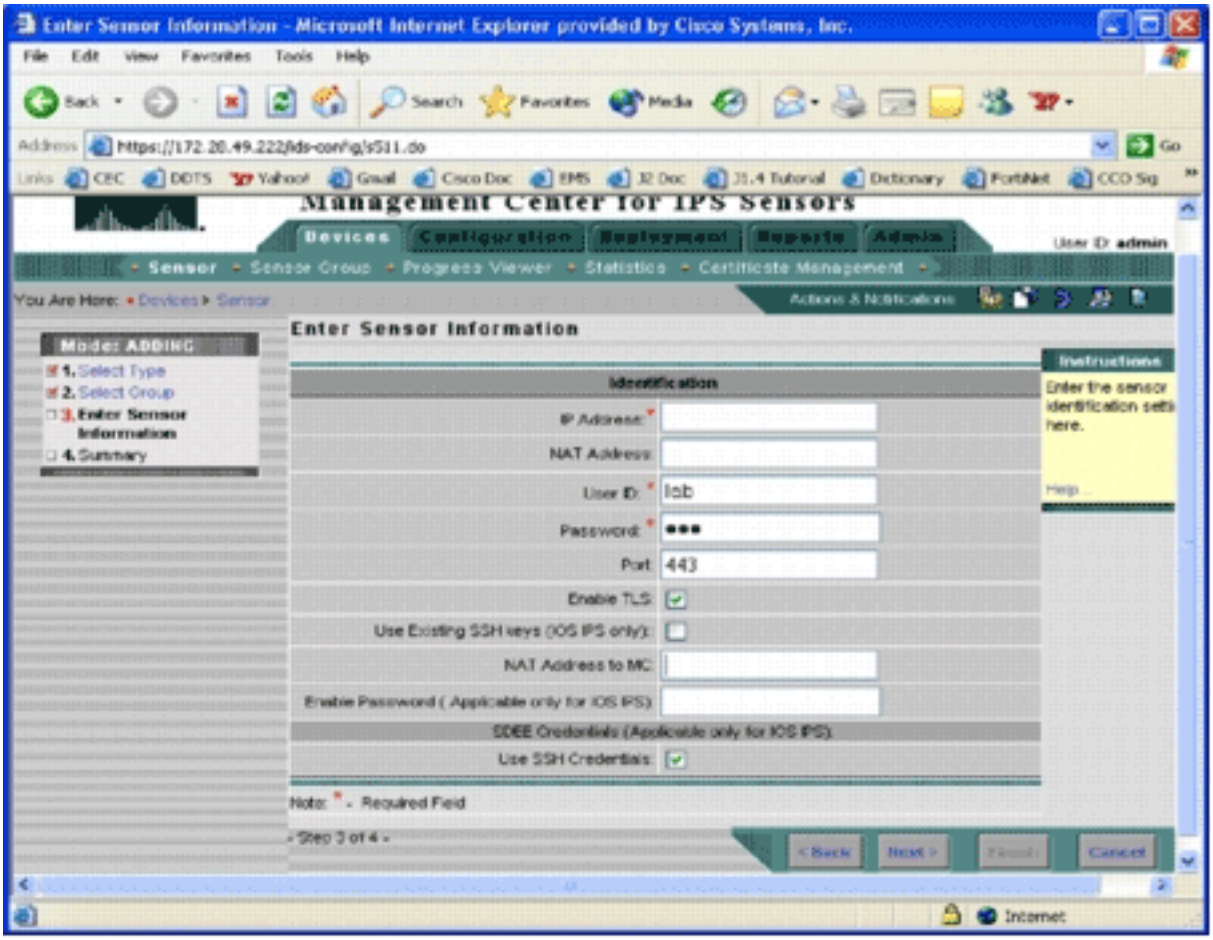


5. Cliquez sur **Add**.La page Sélectionner un type apparaît.



Vous devez indiquer à IPS MC le type de fonction d'ajout que vous voulez exécuter. Cette liste décrit chaque option :*Import configuration from device* : utilisez cette option pour ajouter aux périphériques IPS MC qui s'exécutent actuellement sur le réseau.*Créer une configuration par défaut* : utilisez cette option pour ajouter des périphériques qui ne s'exécutent pas encore sur le réseau.*Ajouter plusieurs périphériques* : utilisez cette option pour ajouter plusieurs périphériques. Vous pouvez créer un fichier .csv ou .xml qui contient toutes les informations de périphérique, puis l'importer dans IPS MC afin d'ajouter les périphériques à la fois.**Conseil :** Les exemples de fichiers au format .csv et .xml se trouvent dans : InstallDirectory\MDC\etc\ids\ and are named MultipleAddDevices-format.csv et MultipleAddDevices-format.xml, respectivement.

6. Choisissez l'option Ajouter le type approprié, puis cliquez sur **Suivant**.
7. Sélectionnez le groupe auquel vous voulez ajouter le routeur IPS Cisco IOS ou utilisez le groupe global par défaut, puis cliquez sur **Suivant**.La page Enter Sensor Information s'affiche.



8. Dans la page Identification, saisissez les informations d'identification du périphérique.**Remarque :** si l'utilisateur ne dispose pas de droits d'accès de niveau de privilège 15, vous devez fournir le mot de passe enable. Dans la dernière ligne de la page Identification, cochez la case **Utiliser les informations d'identification SSH**.
9. Cliquez sur **Next** (Suivant).Le résumé Add Sensor s'affiche.
10. **Cliquez sur Finish.**Le périphérique est correctement ajouté à IPS MC.**Remarque :** Si vous rencontrez des erreurs lors du processus d'importation, vérifiez les éléments suivants :*Configuration requise* - Ces configurations sont nécessaires pour qu'IPS MC puisse communiquer avec les routeurs IPS Cisco IOS.*Connectivité* - Assurez-vous qu'IPS MC peut atteindre les routeurs IPS Cisco IOS.*Clock* : vérifiez les heures sur le MC IPS et le routeur IPS Cisco IOS. Le temps est un composant essentiel du certificat https utilisé pour l'authentification. Les heures doivent être dans les 12 heures les unes des autres. (Les

meilleures pratiques ne durent que quelques heures.)*Certificat IPS Cisco IOS* - Parfois, le certificat IPS Cisco IOS stocké est incorrect. Pour supprimer un certificat de Cisco IOS IPS, vous devez supprimer le point de confiance du routeur IPS Cisco IOS.*Configuration supplémentaire* - Si **ip http timeout-policy** est configurée avec un nombre limité de requêtes maximales, telles que **ip http timeout-policy idle 600 life 86400 request 1**, vous devez augmenter le nombre maximal de requêtes. Exemple : **ip http timeout-policy idle 600 life 86400 requêtes 8400**

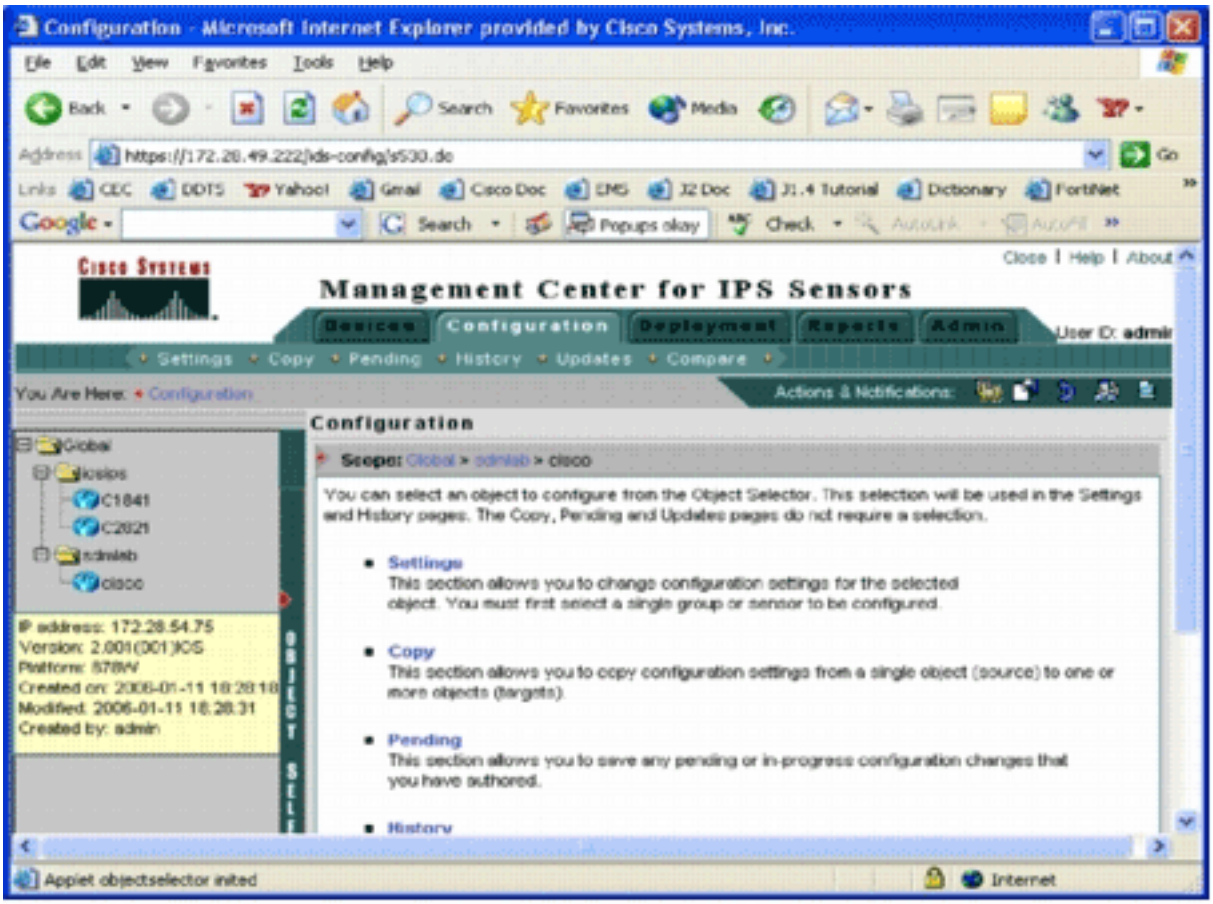
Configurer le routeur IPS Cisco IOS pour utiliser les fichiers de signature prédéfinis

Après avoir importé le routeur dans IPS MC, vous devez sélectionner le fichier de définition de signature (SDF) (fichier texte qui inclut les signatures de menace que le routeur IPS utilisera) et l'action à effectuer lorsque chaque signature est déclenchée (par exemple, abandonner, réinitialisation TCP, alarme).

Cisco Systems® vous recommande d'utiliser les fichiers SDF préconfigurés Cisco. Il existe actuellement trois fichiers de ce type : attentat-drop.sdf, 128 Mo.sdf et 256 Mo.sdf. IPS MC peut télécharger automatiquement ces fichiers depuis Cisco.com. Voir Mises à jour des signatures de téléchargement automatique pour plus d'informations.

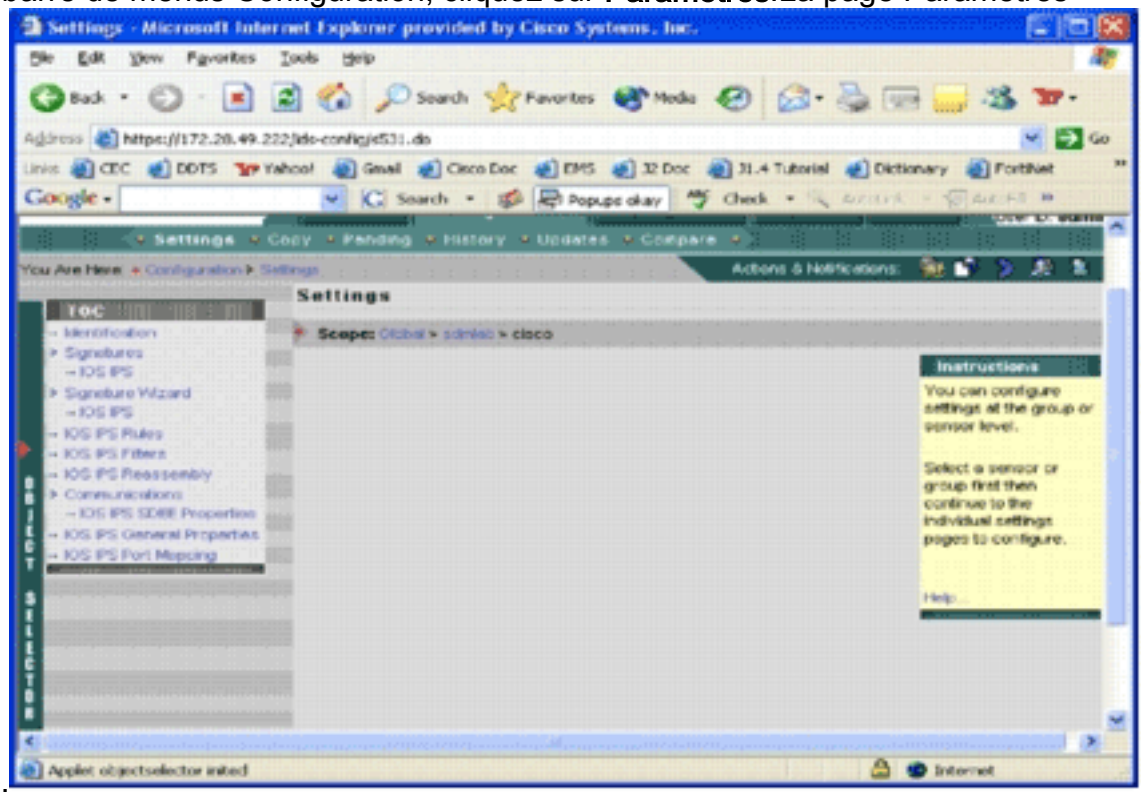
Cette procédure utilise un seul périphérique comme exemple et commence par un routeur sans configuration IPS. Vous pouvez également utiliser cette procédure pour plusieurs périphériques au niveau d'un groupe.

1. Cliquez sur l'onglet **Configuration**.La page Configuration s'affiche.

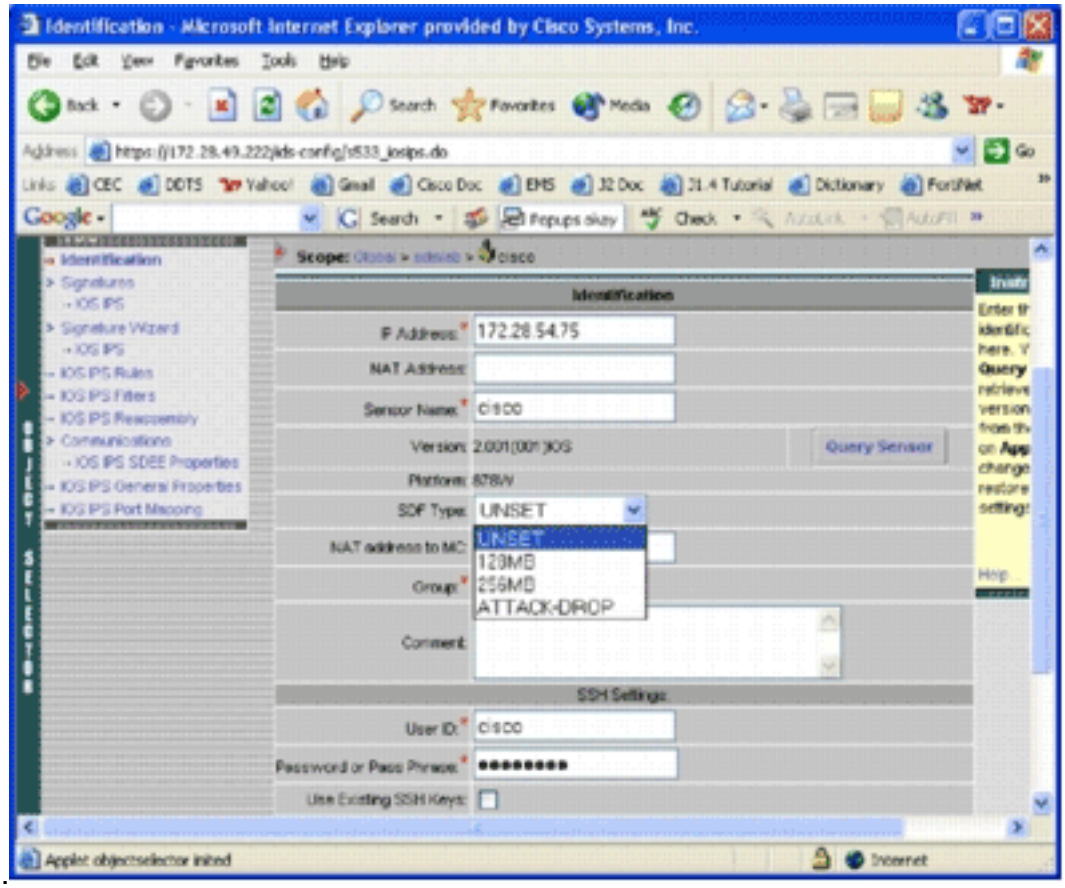


2. Dans le sélecteur d'objets situé sur le côté gauche de la page, sélectionnez le routeur IPS Cisco IOS à configurer.**Remarque :** La plupart des paramètres de configuration d'IPS MC 2.2

peuvent être configurés au niveau du groupe ainsi qu'au niveau de chaque périphérique. Par exemple, les groupes globaux, iosips et sdmlab sont tous des groupes d'objets configurables. Cet exemple utilise un périphérique individuel cisco du groupe sdmlab.Une fois que vous avez sélectionné le routeur à configurer, la barre de chemin située en haut de la page Configuration affiche la portée actuelle de la configuration. Par exemple, la portée de cet exemple est *Global > sdmlab > cisco*. *cisco* est l'objet de configuration actuel (c'est-à-dire le routeur sélectionné dans le sélecteur d'objets.

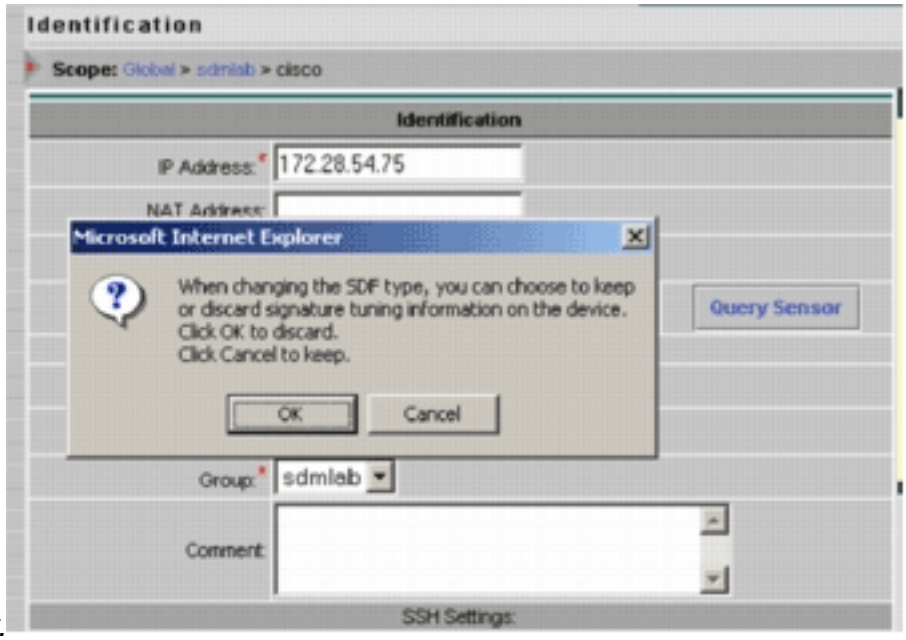
3. Dans la barre de menus Configuration, cliquez sur **Paramètres**.La page Paramètres s'affiche. 

Dans la page Paramètres, vous pouvez modifier les paramètres de configuration de l'objet sélectionné. Les paramètres de configuration spécifiques aux routeurs IPS Cisco IOS se trouvent dans la section TOC située sur le côté gauche de la page. Voici une liste des tâches disponibles dans la section Table des matières :*Identification* - informations de base du routeur IPS Cisco IOS ; vous pouvez spécifier un fichier SDF préréglé ici*Signature* - signatures du routeur IPS Cisco IOS*Assistant Signature* : assistant de signature permettant d'ajouter des signatures personnalisées*Règles IPS de Cisco IOS* - Pour configurer les règles IPS de Cisco IOS utilisées pour s'appliquer aux interfaces*Filtres IPS Cisco IOS* - Filtres IPS Cisco IOS*Réassemblage IPS de Cisco IOS* - Configuration du réassemblage virtuel IP d'interface*Propriétés SDEE de Cisco IOS IPS*—Pour la configuration des paramètres SDEE*Propriétés générales de Cisco IOS IPS* - Configurations supplémentaires liées à Cisco IOS IPS
4. Choisissez **Identification** afin de configurer les fichiers SDF préréglés.La page Identification

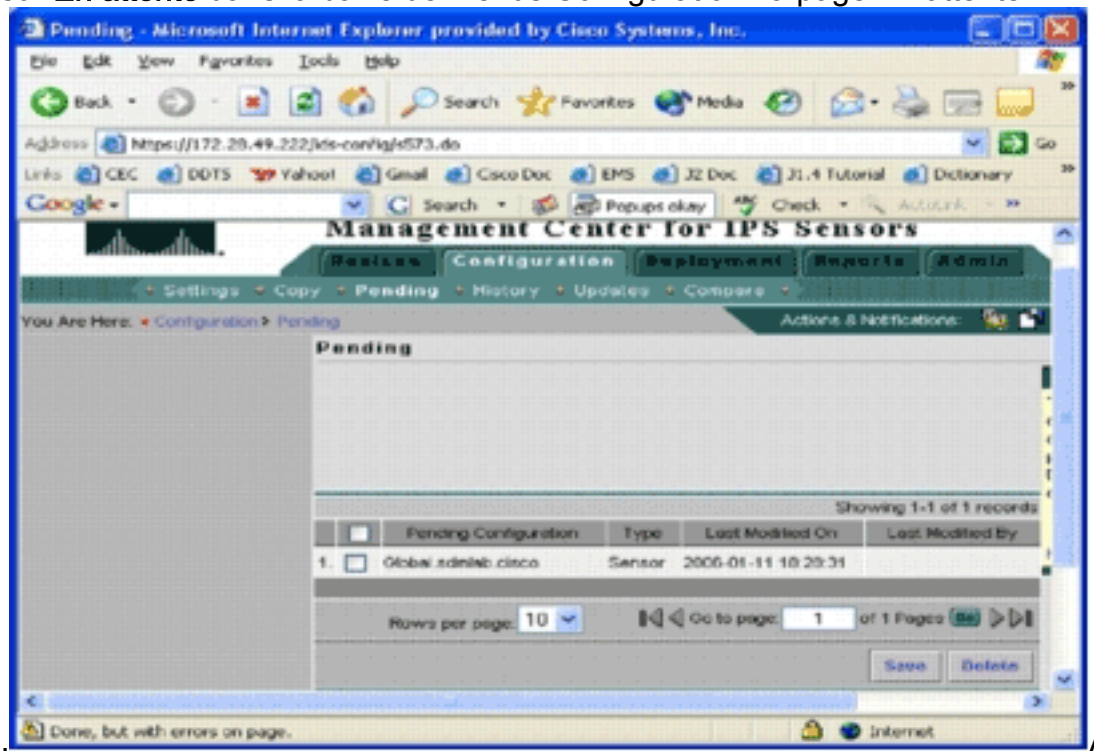


s'affiche.

5. Dans la liste déroulante SDF Type, sélectionnez le fichier SDF préconfiguré approprié, puis cliquez sur **Apply** afin d'appliquer les modifications.Cisco IOS IPS prend en charge plus de 1 600 signatures, ce qui dépasse la capacité mémoire des routeurs à accepter. Les SDF ont été développés comme un moyen pratique de sélectionner et de charger les signatures les plus vitales. Actuellement, vous pouvez choisir parmi trois SDF. Leur taille varie afin de vous permettre de sélectionner un fichier SDF en fonction de la capacité DRAM de vos routeurs. Les options disponibles sont décrites ici :UNSET : le type SDF n'est pas défini.ATTACK-DROP : ce SDF est destiné aux routeurs avec 64 Mo de DRAM.256 Mo : ce SDF est destiné aux routeurs avec 256 Mo de DRAM.128 Mo : ce SDF est destiné aux routeurs avec 128 Mo de DRAM.**Remarque :** Les SDF de 128 et 256 Mo nécessitent un moteur de 2.001 ou supérieur. Ces informations sont disponibles dans le champ **Paramètres > Interface utilisateur d'identification > Version**.**Avertissement :** IPS MC n'inclut pas de fonctions de gestion de la mémoire pour les routeurs IPS Cisco IOS. Soyez prudent lorsque vous sélectionnez des fichiers SDF pour votre routeur IPS Cisco IOS. Assurez-vous que le routeur IPS Cisco IOS dispose de suffisamment de mémoire pour exécuter le fichier SDF sélectionné.**Remarque :** lorsque vous modifiez le type SDF, vous pouvez recevoir ce message : *Lorsque vous modifiez le type SDF, vous pouvez conserver ou supprimer les informations de réglage de signature sur le périphérique. Cliquez sur OK pour annuler. Cliquez sur Annuler pour*



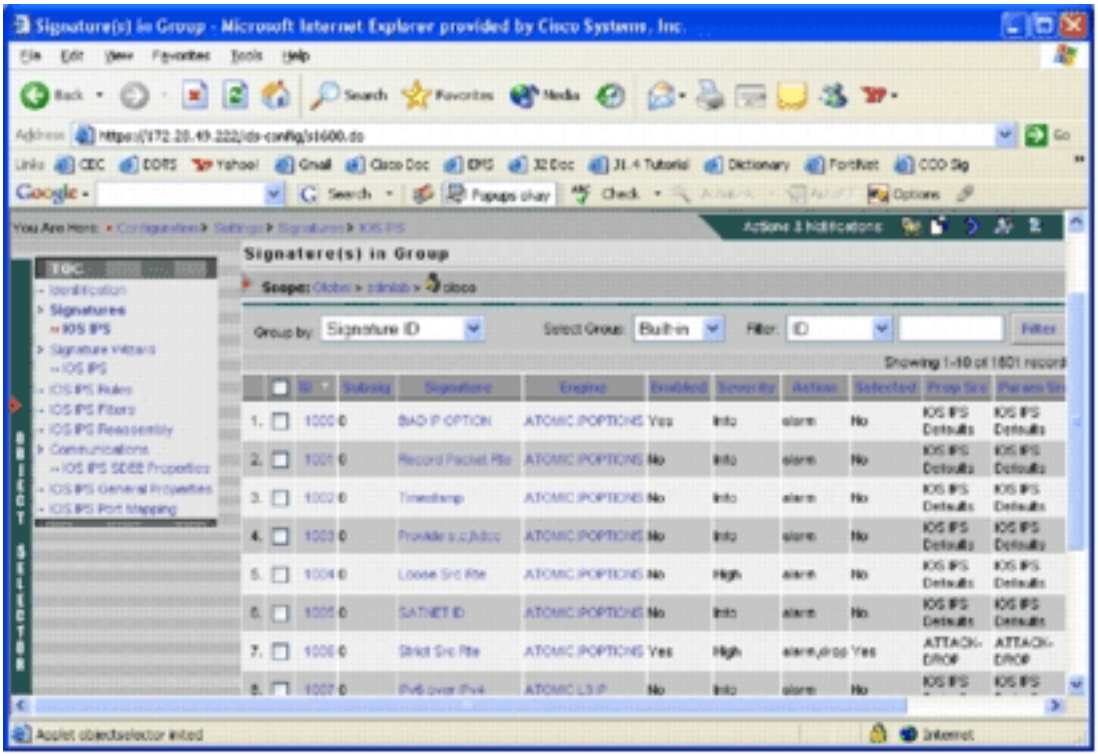
continuer.

6. Cliquez sur **Annuler** afin de conserver vos informations de réglage de signature.Maintenant que vous avez choisi avec succès un SDF préréglé pour le routeur cisco, vous pouvez effectuer des réglages de signature supplémentaires, comme ajouter ou modifier, ou même créer vos propres signatures, ou vous pouvez ignorer les tâches de réglage de signature et accéder directement à Créer une règle à appliquer aux interfaces.
7. Cliquez sur **En attente** dans la barre de menus Configuration.La page En attente s'affiche. 

Àce stade, la tâche de configuration est terminée. Cependant, vous devez terminer la tâche de déploiement afin de déployer vos modifications sur le périphérique cible.

Modifier les signatures SDF conservées

Après avoir sélectionné un fichier SDF préréglé pour un routeur, vous pouvez effectuer des tâches supplémentaires de réglage des signatures. Vous pouvez ajouter, modifier, supprimer et modifier des signatures selon vos besoins, ou créer vos propres signatures si nécessaire. Cet exemple utilise IPS MC afin d'ajouter des signatures supplémentaires et de modifier les actions. Cette image montre l'interface de configuration des signatures.



Vous pouvez utiliser la configuration des signatures afin d'activer ou désactiver, sélectionner ou désélectionner, ajouter une signature, supprimer une signature, modifier les actions de signature et modifier les paramètres de signature. Utilisez l'Assistant Signature à gauche pour créer des signatures personnalisées.

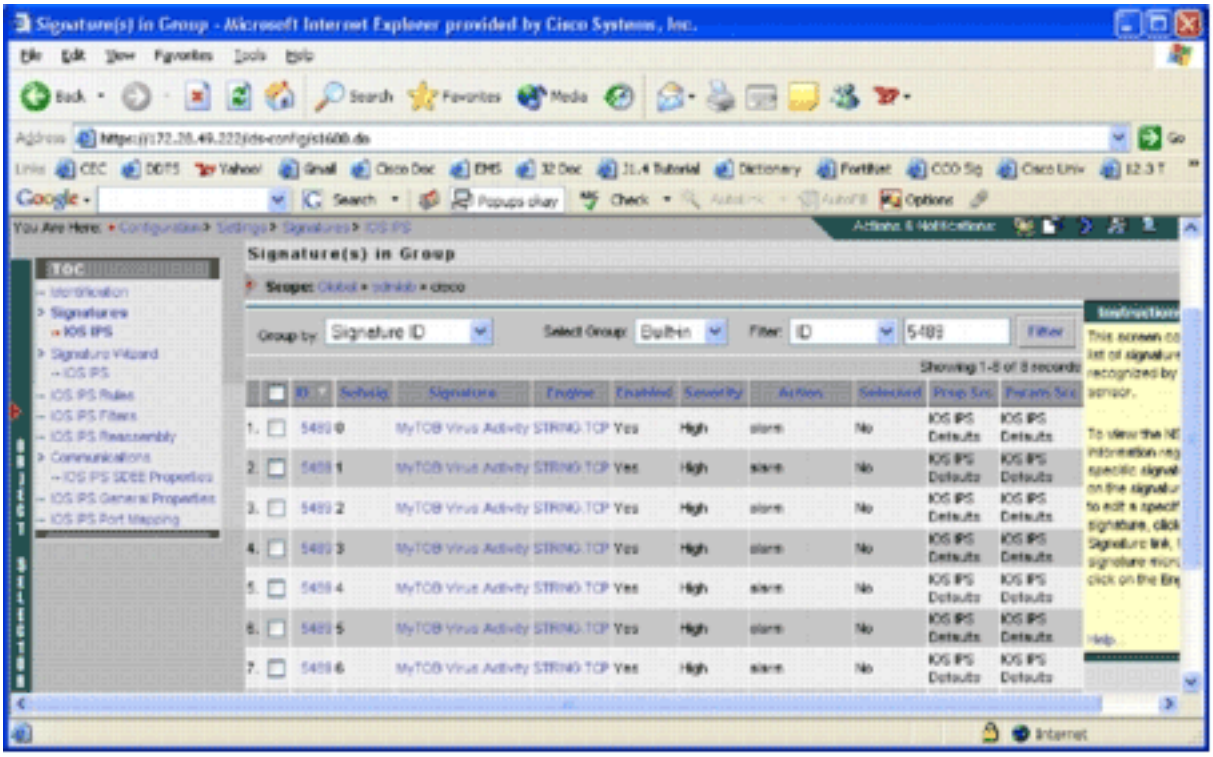
Dans l'interface utilisateur de configuration des signatures, certaines informations sont affichées par défaut. La sélection indique si la signature va être incluse dans le fichier SDF envoyé au routeur. Si aucune signature n'est sélectionnée, elle ne sera pas ajoutée. Activé s'applique uniquement si une signature est sélectionnée. Lorsqu'une signature est désactivée, les moteurs IPS n'envoient pas d'événements pour cette signature spécifique. Si une signature n'est pas sélectionnée, elle est également automatiquement désactivée.

Les deux dernières colonnes (Prop Src et Param Src) vous indiquent d'où viennent respectivement la signature et son paramètre. La signature aurait pu être prise à partir de fichiers SDF préréglés ou à partir de la valeur par défaut d'usine que vous pouvez trouver dans les mises à jour de fichiers IOS-Sxxx.zip (elle s'affiche sous la forme IOS IPS Defaults). Ces valeurs s'appliquent également à la colonne de paramètre.

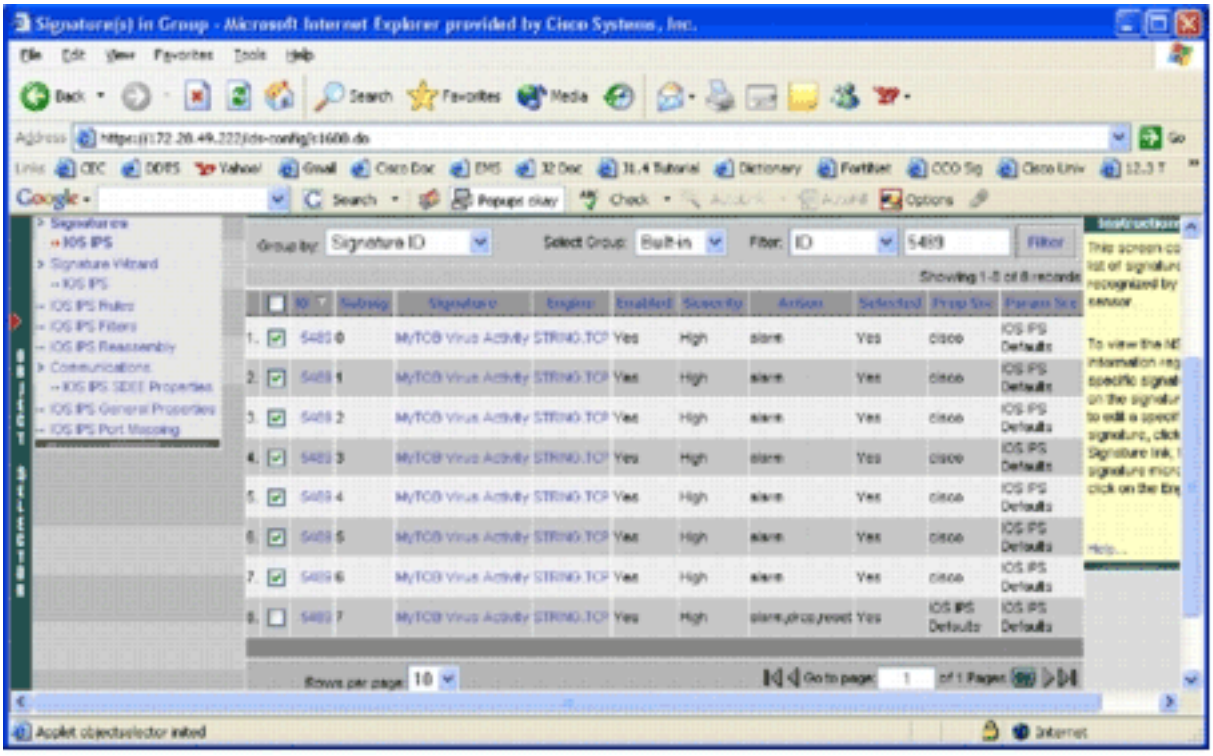
Lorsque vous ajoutez des signatures aux routeurs IPS Cisco IOS, vous devez tenir compte des considérations de mémoire. Si vous ajoutez plus de signatures que le routeur IPS Cisco IOS ne peut traiter, IPS MC ne pourra pas déployer les modifications de configuration sur les périphériques.

Complétez ces étapes afin d'ajouter des signatures 5489/x au routeur IPS Cisco IOS :

1. Sélectionnez **Configuration**, puis utilisez le sélecteur d'objets afin de sélectionner le routeur IPS Cisco IOS pour lequel vous voulez configurer les signatures IPS.
2. Choisissez **Configuration > Settings > Signatures > IOS IPS**.La page Signature(s) dans Groupe
   s'affiche.

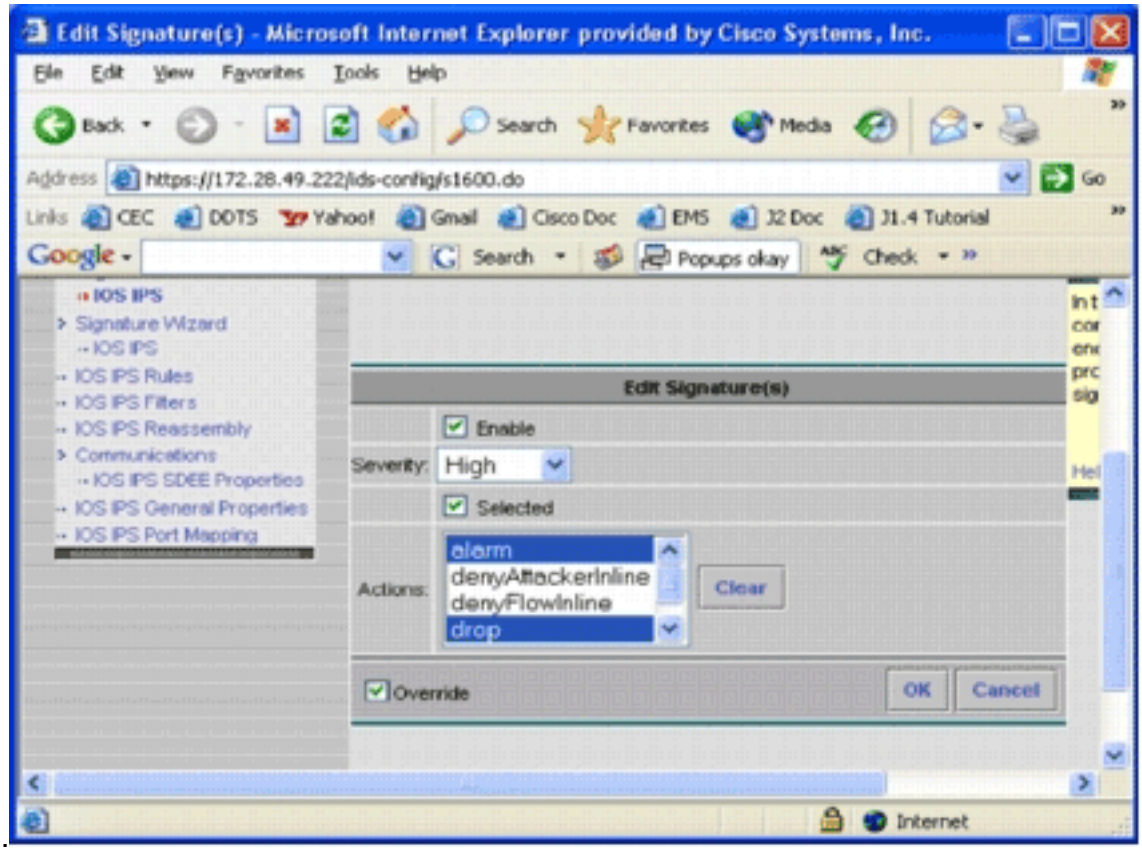


3. Dans la liste des signatures qui en résulte, sélectionnez Filtrer par ID et tapez ID de signature 5489.
4. Cliquez sur **Filtrer** afin de rechercher des signatures.Les résultats de la recherche s'affichent.



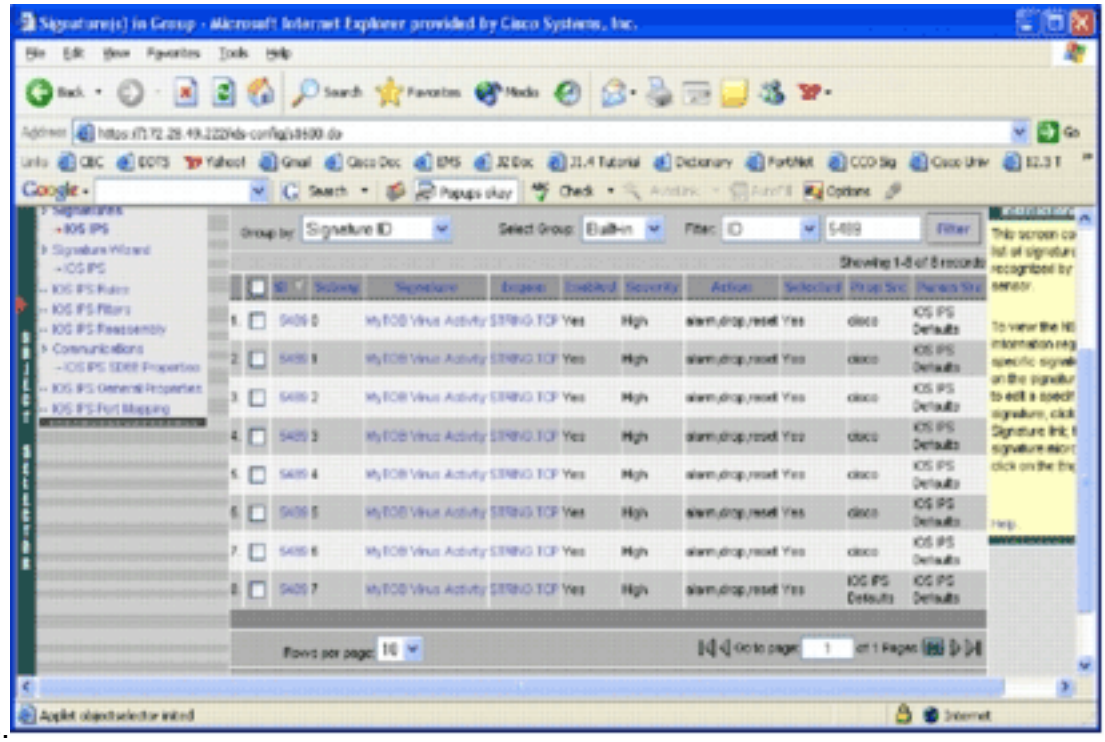
Remarque : IPS MC ne prend pas en charge la nouvelle catégorisation disponible dans Cisco SDM.

5. Cochez la case en regard des signatures qui n'ont pas été sélectionnées, puis cliquez sur **Sélectionner** dans la barre d'outils inférieure.
6. Cliquez sur **Modifier** afin de modifier les actions de signature.La page Modifier les signatures



s'affiche.

7. Cochez la case **Sélectionné**, puis sélectionnez **alarme**, **abandon** et **réinitialisation** dans la liste Actions.
8. Cochez la case **Remplacer**, puis cliquez sur **OK**.Toutes les signatures sont modifiées avec les actions



souhaitées.

9. Accédez à la tâche En attente et enregistrez toutes les modifications. La tâche de configuration est alors terminée.**Conseil :** prêtez une attention particulière à la colonne Prop Src. Après modification, la source est passée au périphérique *cisco*, ce qui signifie que toutes les informations de réglage sont enregistrées séparément des fichiers SDF préréglés par défaut. Ce mécanisme permet à IPS MC de conserver les modifications de signature personnalisées.

Dans la section précédente, lorsque vous avez modifié les types de fichiers SDF, l'IPS MC vous a demandé si vous vouliez conserver les informations de réglage des signatures. Il s'agit des informations de réglage de signature mentionnées.

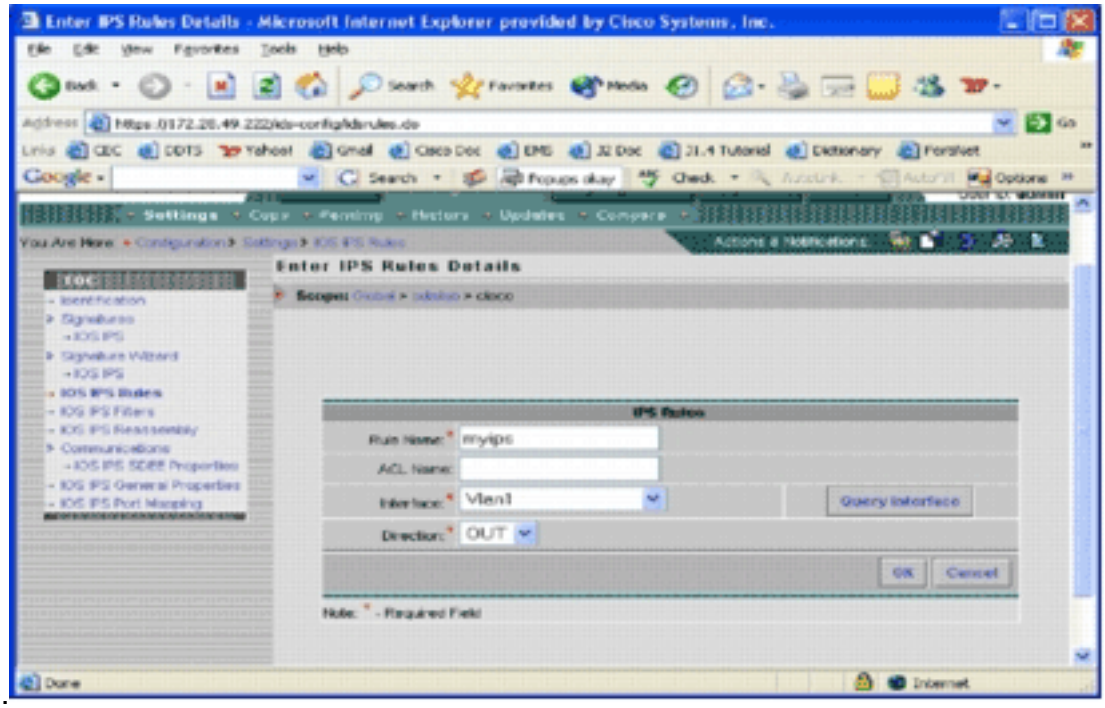
Choisir des signatures personnalisées

Si vous ne voulez pas utiliser les fichiers SDF préréglés par défaut, vous pouvez utiliser les étapes spécifiées dans la section Modifier les signatures SDF préréglées afin de sélectionner des signatures de réglage pour vos périphériques. Dans la page d'identification, vous devez vous assurer que le type SDF est UNSET. Reportez-vous à l'étape 3 de Configurer le routeur IPS Cisco IOS pour utiliser les fichiers de signature prédéfinis.

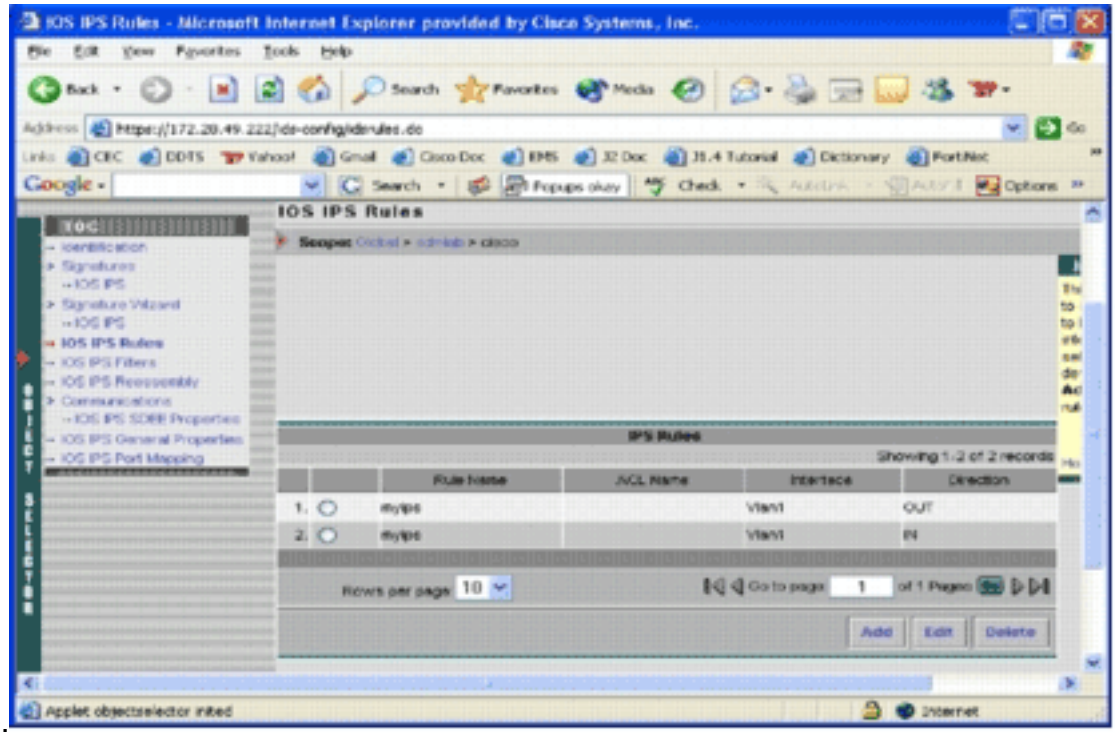
Créer une règle à appliquer aux interfaces

Après avoir réglé la signature, vous devez activer IPS sur les routeurs Cisco IOS. Pour activer IPS sur le routeur, vous devez créer une règle IPS et l'appliquer à au moins une interface.

1. Sélectionnez **Configuration**, puis utilisez le sélecteur d'objets afin de sélectionner le routeur IPS Cisco IOS que vous voulez configurer. Vérifiez dans la barre de chemin que votre étendue se situe au niveau du périphérique et non au niveau du groupe.
2. Sélectionnez **Configuration > Settings > IOS IPS Rules**, puis cliquez sur **Add**.La page Enter IPS Rules Details s'affiche.



3. Entrez les informations relatives au nom de la règle et à l'interface à laquelle vous souhaitez appliquer la règle et la direction.
4. Click OK.La page IOS IPS Rules



s'affiche. De même, vous pouvez créer des règles pour les deux directions pour une interface.

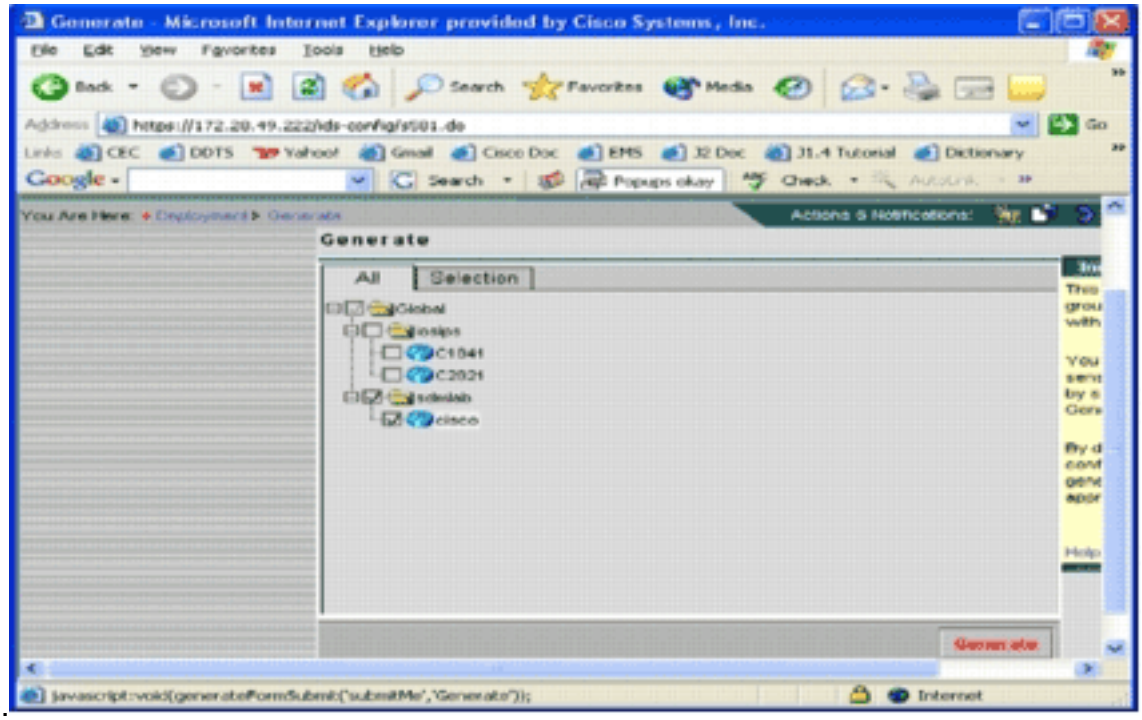
5. Vous devez enregistrer les modifications de configuration et passer par le processus de déploiement pour transmettre les modifications au périphérique ou au groupe de périphériques concernés.Vous pouvez également effectuer d'autres configurations IPS, mais toutes les autres tâches sont facultatives et ne sont pas obligatoires. Vous trouverez toutes les options à gauche de l'interface utilisateur de configuration. Ce document ne couvre pas les options de configuration facultatives.

Déployer la configuration

Après avoir effectué toutes les modifications de configuration, vous devez utiliser la tâche de déploiement afin de valider les modifications apportées aux périphériques. Toutes les configurations que vous avez effectuées jusqu'à présent sont enregistrées localement sur le serveur IPS MC.

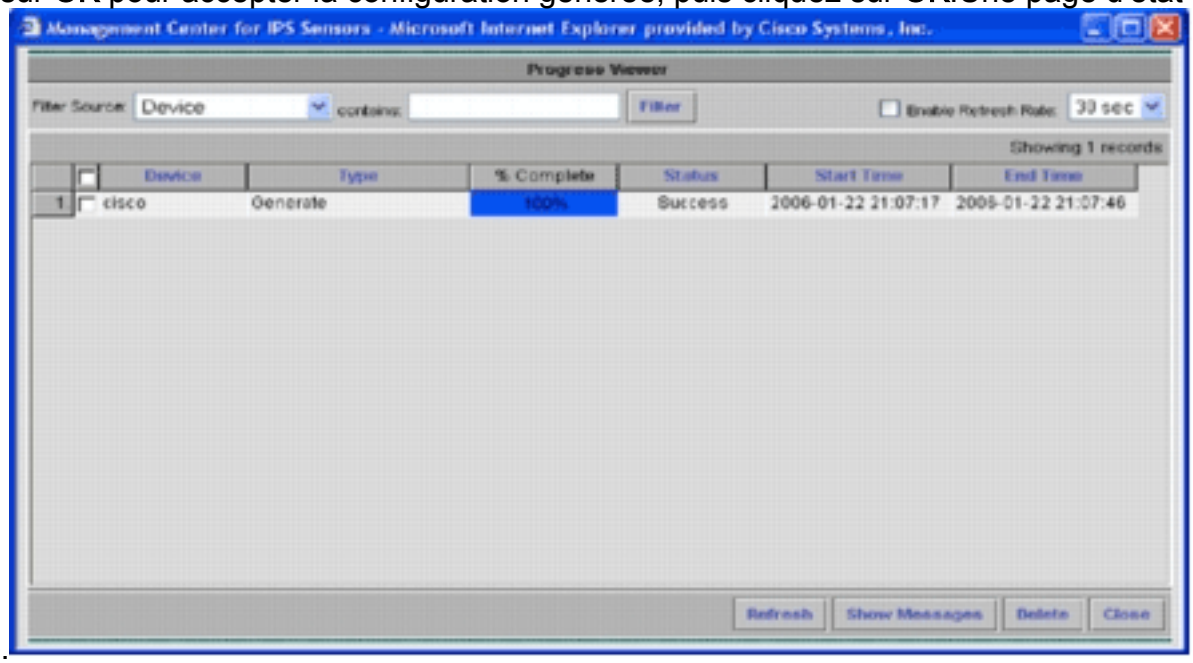
Afin de déployer les modifications de configuration, accédez à la page Déploiement et complétez ces étapes :

1. Cliquez sur l'onglet **Déploiement**, puis sélectionnez **Générer** afin de générer des modifications de configuration.La page Generate



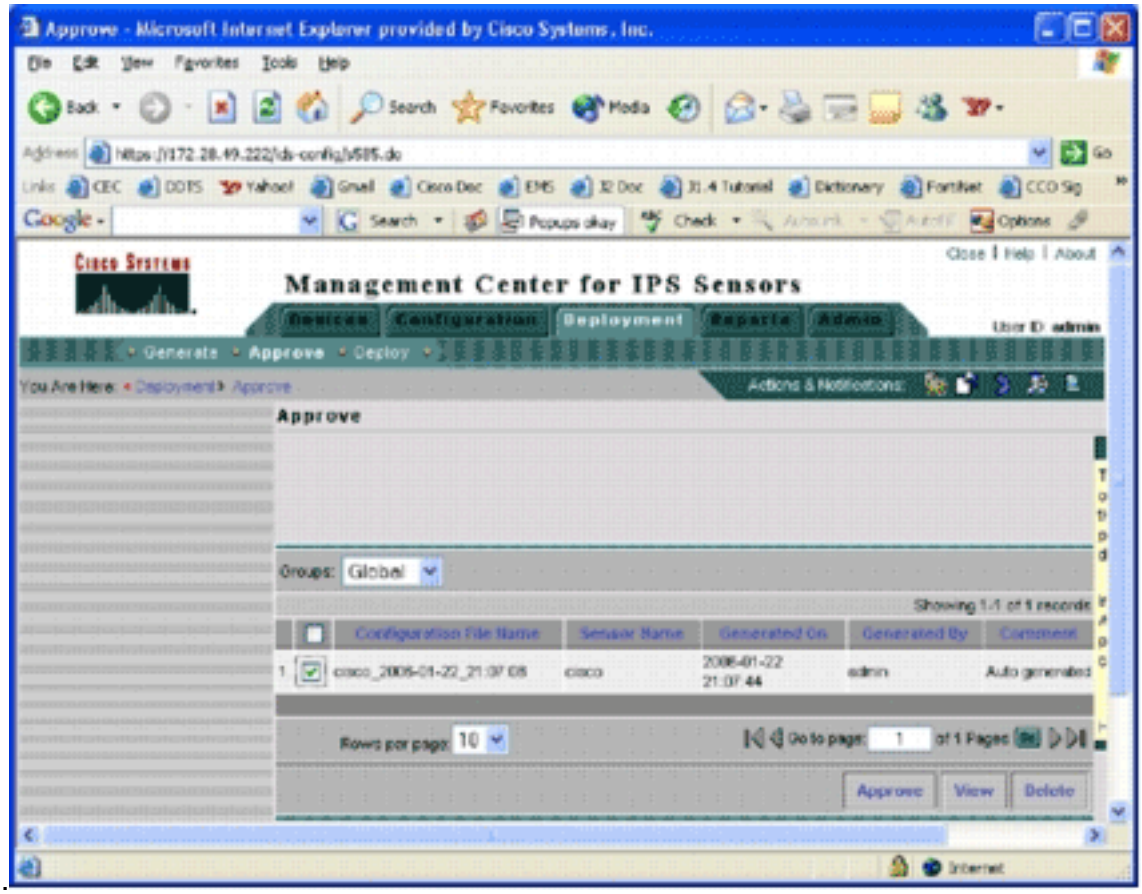
s'affiche.

2. Choisissez le périphérique *cisco* que vous venez de configurer, puis cliquez sur **Generate**.
3. Cliquez sur **OK** pour accepter la configuration générée, puis cliquez sur **OK**.Une page d'état



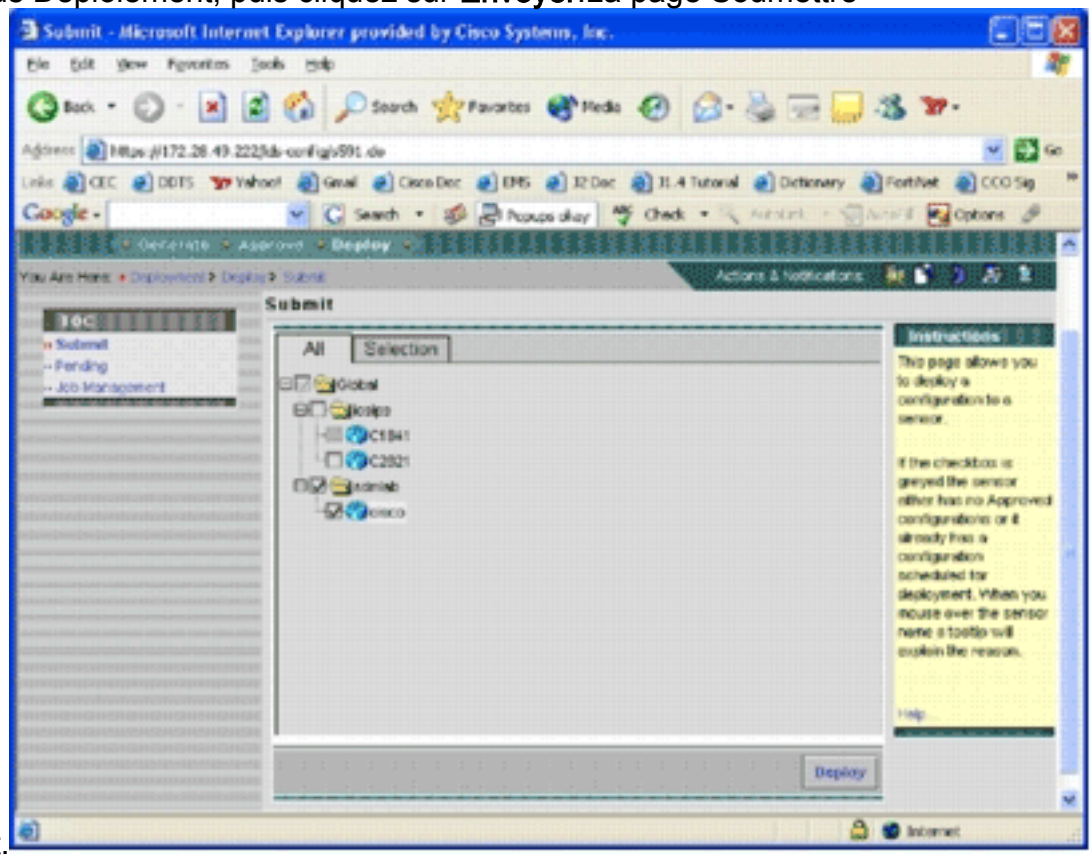
s'affiche.

4. Cliquez sur **Actualiser** jusqu'à ce que la tâche de génération se termine correctement.
5. Cliquez sur **Approuver** dans la barre de menus Déploiement et dans le groupe sdmlab afin d'afficher la liste des configurations nécessitant une approbation.La page Approuver



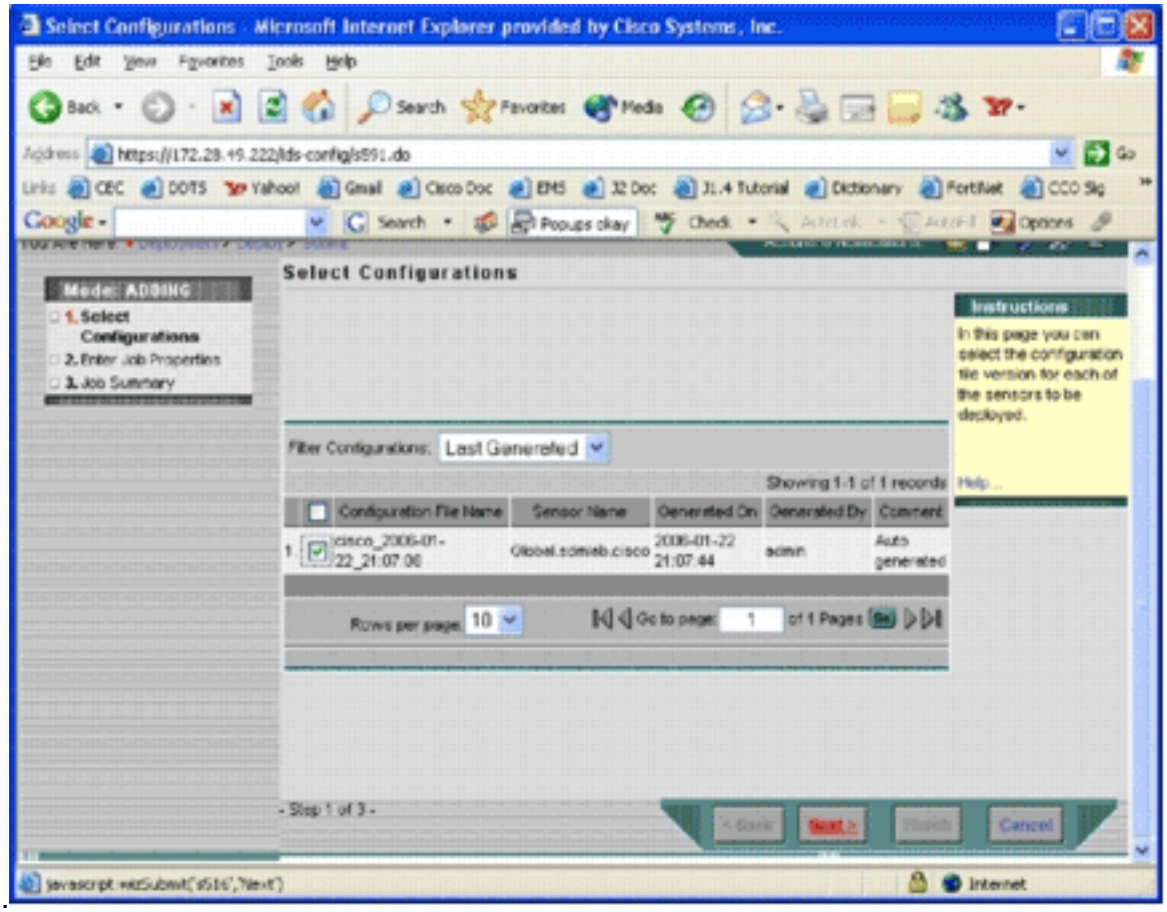
s'affiche.

6. Choisissez la ou les tâches, puis cliquez sur **Approuver**.Cliquez sur **Déployer** dans la barre de menus Déploiement, puis cliquez sur **Envoyer**.La page Soumettre



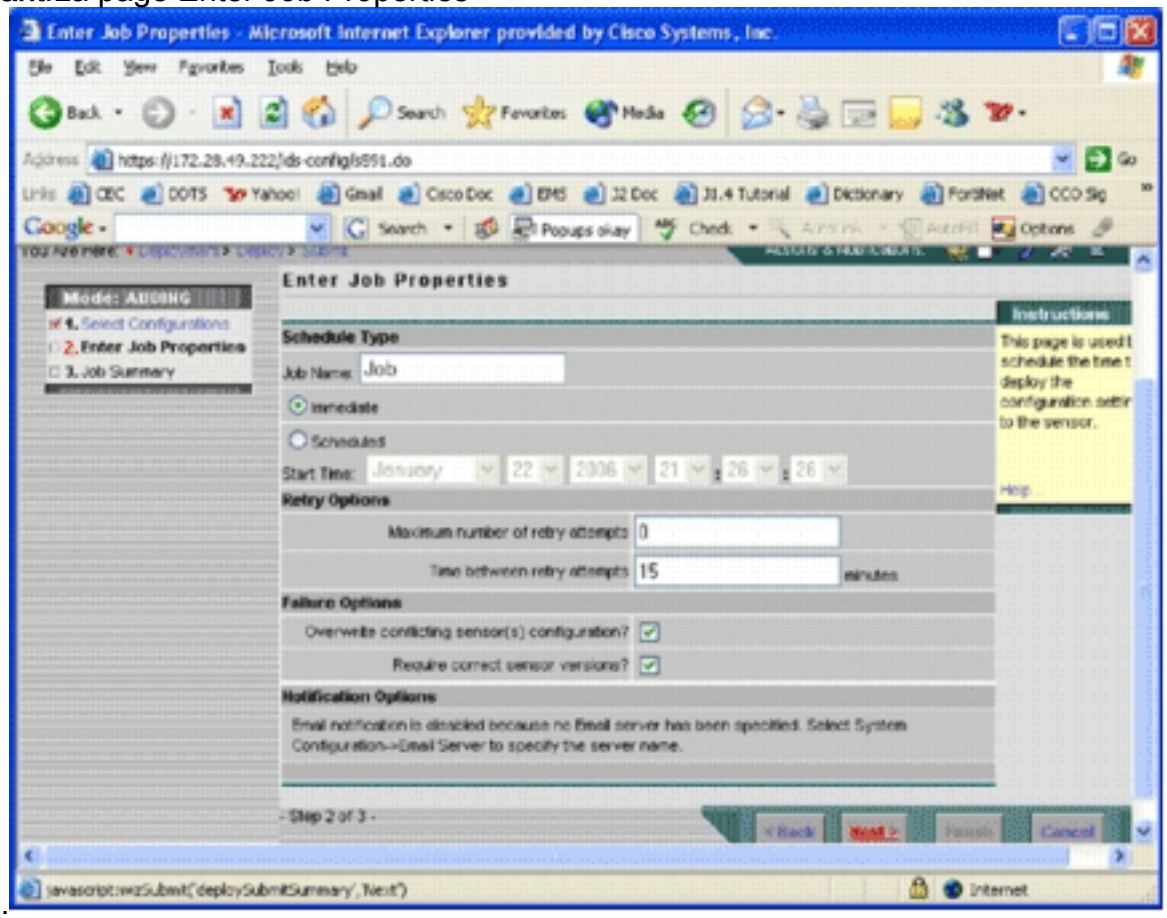
apparaît.

7. Choisissez les périphériques pour lesquels vous souhaitez soumettre la tâche de déploiement.
8. Sélectionnez le périphérique *cisco*, puis cliquez sur **Déployer**.La page Sélectionner les configurations



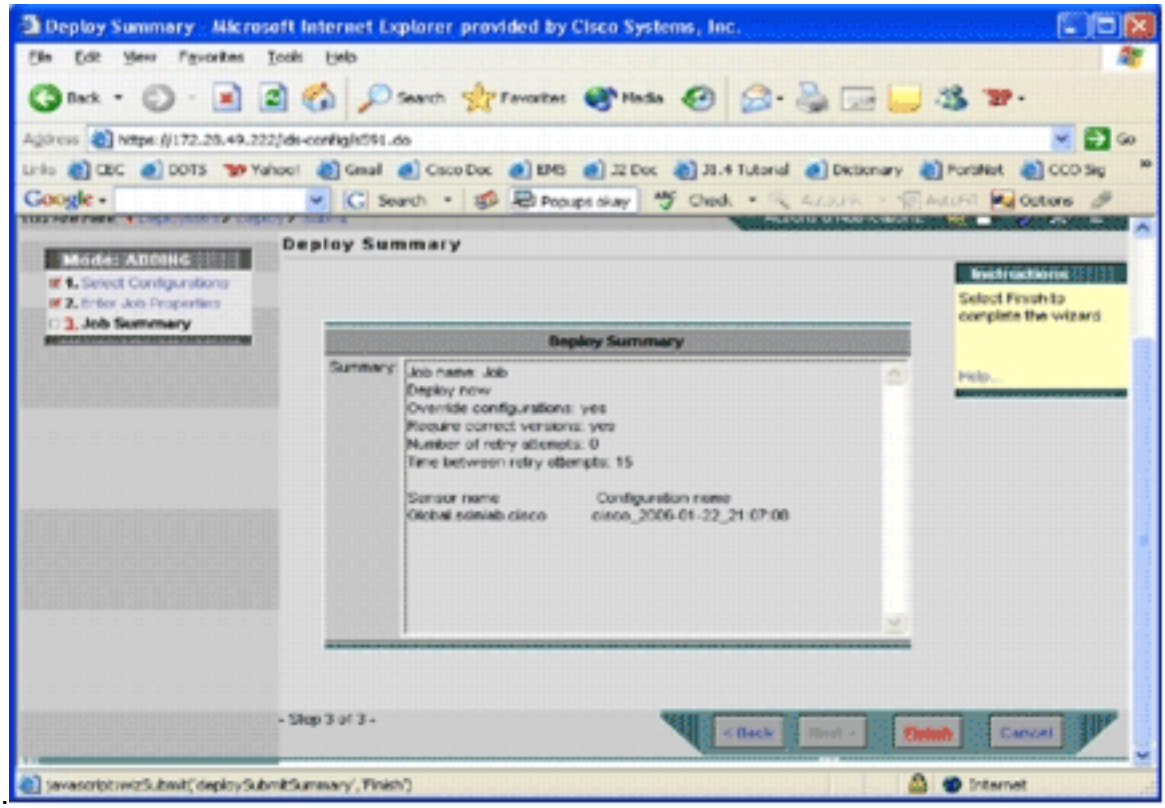
s'affiche.

9. Choisissez la configuration que vous venez d'effectuer sur le périphérique *cisco*, puis cliquez sur **Suivant**.La page Enter Job Properties



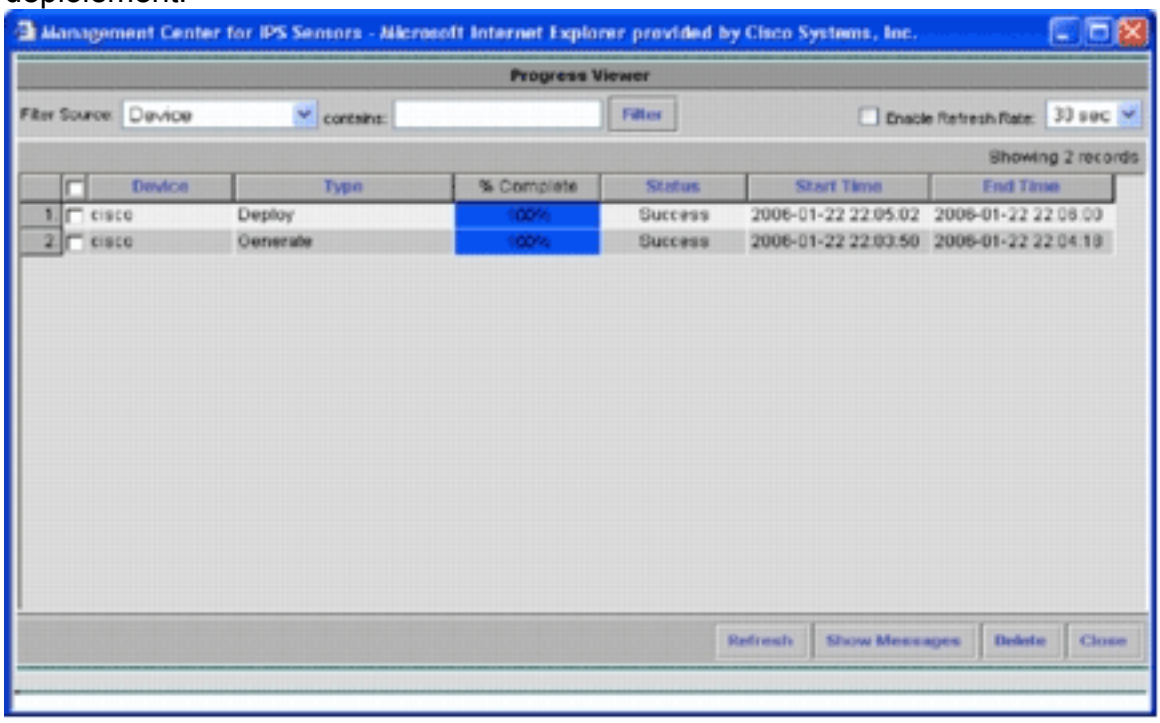
s'affiche.

10. Vous pouvez déployer immédiatement les modifications ou planifier une tâche pour le faire ultérieurement. Dans cet exemple, choisissez l'option **Immédiat**, puis cliquez sur **Suivant**.Un bref récapitulatif des tâches est affiché et prêt à être

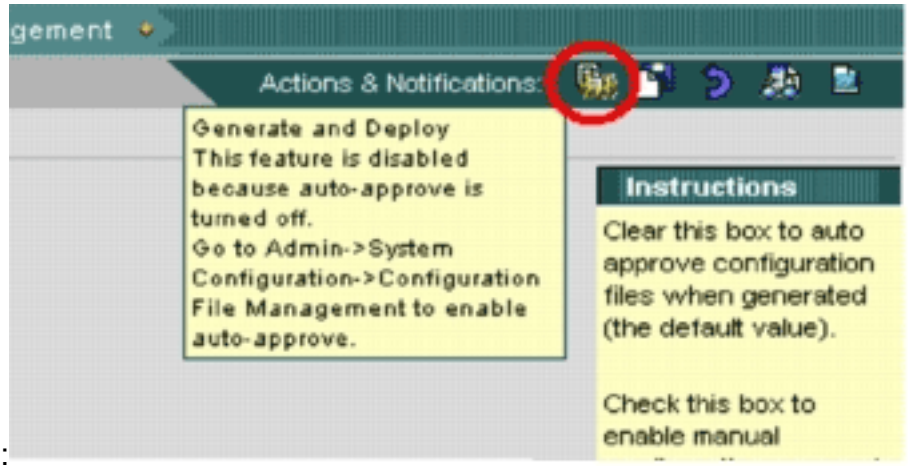


déployé.

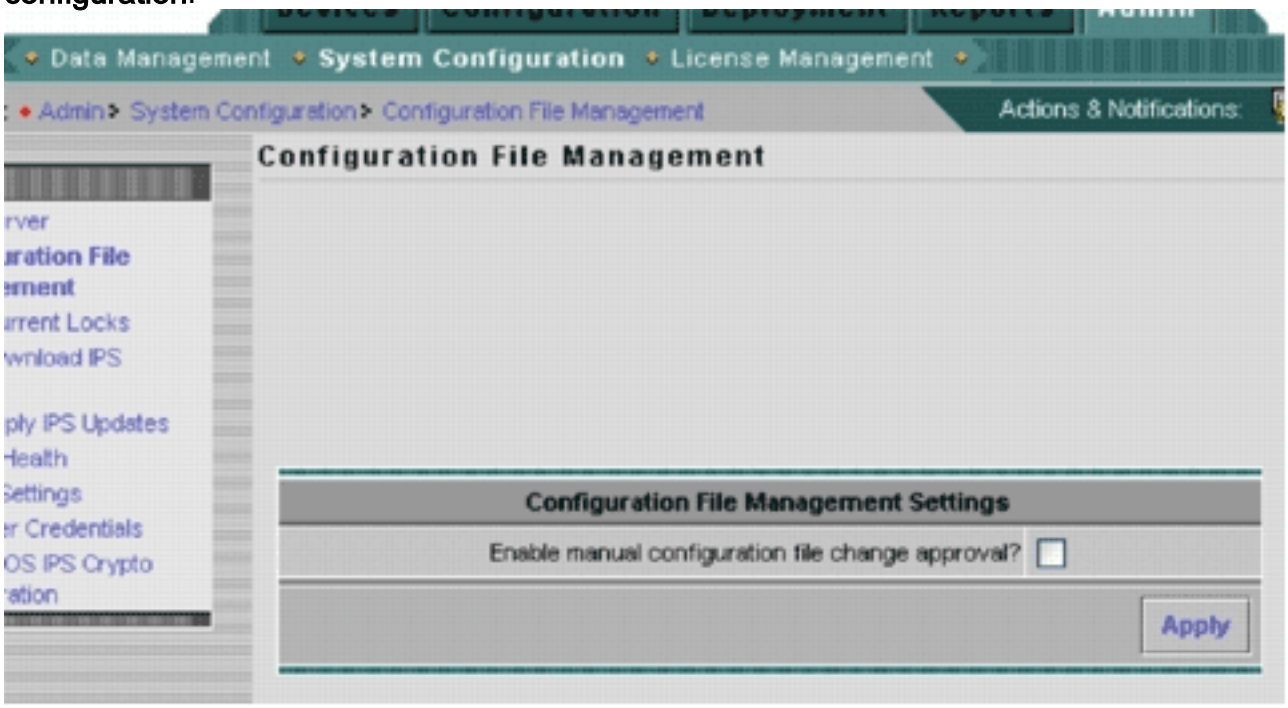
11. **Cliquez sur Finish.**À la fin du déploiement, une boîte de dialogue indique l'état du processus de
déploiement.

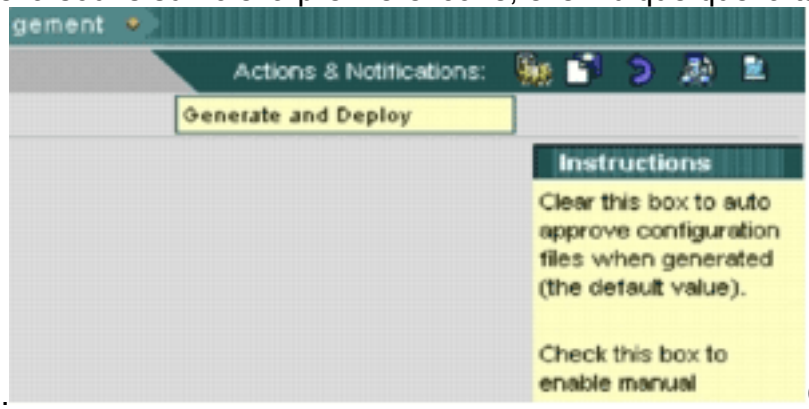


Vous avez correctement déployé les configurations IPS Cisco IOS sur le périphérique. Lorsque vous configurez plusieurs périphériques, vous pouvez modifier la configuration au niveau du groupe, puis appliquer les modifications à tous les routeurs IPS Cisco IOS appartenant au même groupe.**Conseil :** Ce processus est long, mais une fonctionnalité de livraison rapide est disponible. Lorsque vous utilisez cette fonction, vous n'avez pas besoin de passer par le processus **Générer > Approuver > Déployer**. Complétez ces étapes afin d'utiliser la fonction :En haut de l'interface utilisateur se trouve une ligne de petites icônes. Placez votre souris sur la première icône et affichez l'info-bulle affichée dans cette image



: Afin d'activer la tâche Générer et déployer, accédez à **Admin > Configuration du système > Gestion des fichiers de configuration**, puis décochez la case **Activer l'approbation manuelle des modifications de fichier de configuration**.



Lorsque la souris survole la première icône, elle indique que la tâche est activée. 

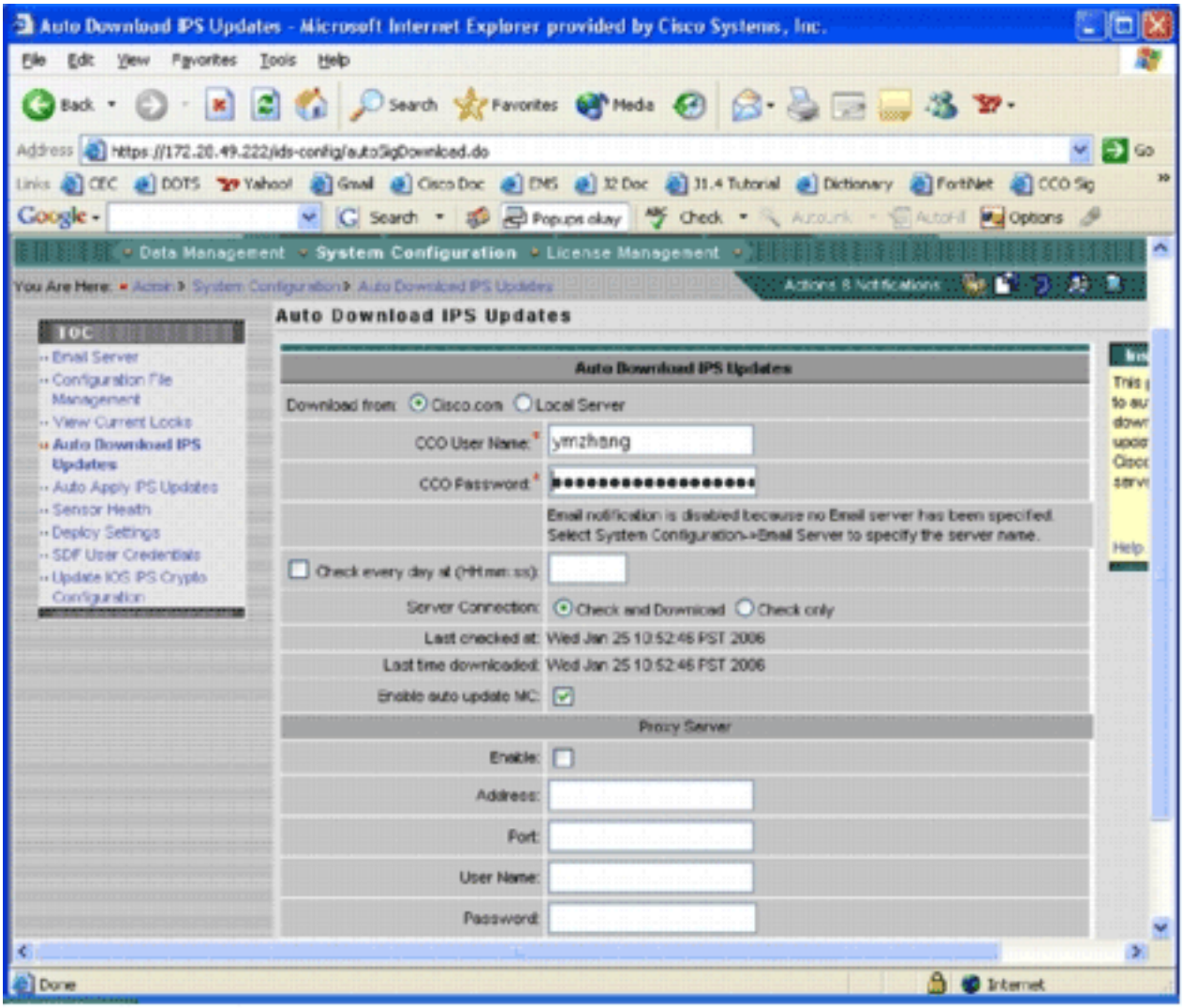
Cliquez sur cette icône.IPS MC génère automatiquement des modifications de configuration et les déploie sur les périphériques.

Mises à jour des signatures de téléchargement automatique

IPS MC prend en charge les mises à jour de signatures de téléchargement automatique depuis

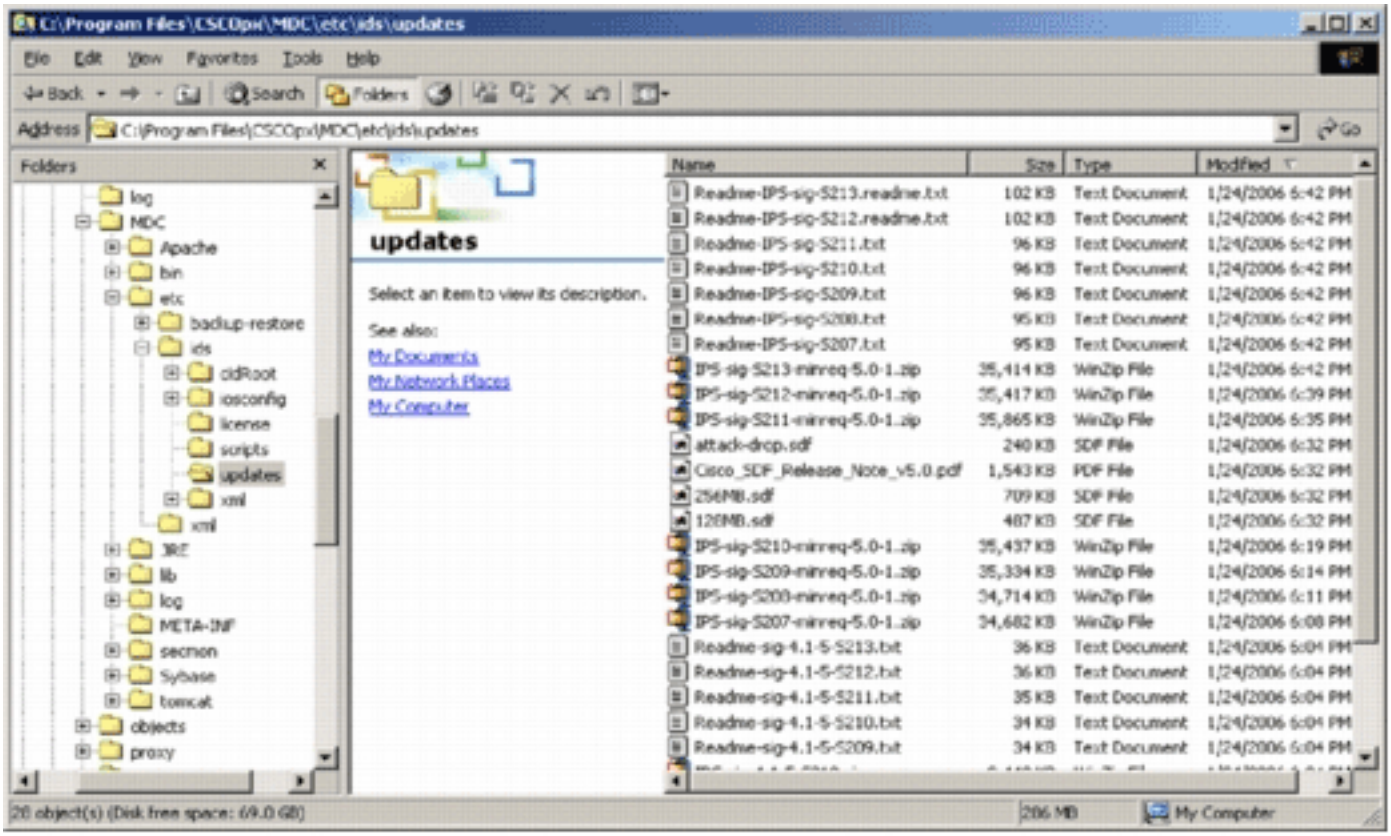
Cisco.com. Il peut télécharger des mises à jour de signatures pour les plates-formes de capteurs, ainsi que pour les plates-formes Cisco IOS IPS. Afin de configurer cette fonctionnalité, accédez à **Admin > System Configuration > Auto Download IPS Updates**.

La page Auto Download IPS Update s'affiche.



Vous devez disposer d'un compte Cisco.com valide pour télécharger cette mise à jour de signature. Afin de vérifier les fichiers téléchargés automatiquement, accédez au répertoire d'accueil de l'installation d'IPS MC. Par défaut, il s'agit de \program files\CSCOpx\MDC\etc\ids\updates.

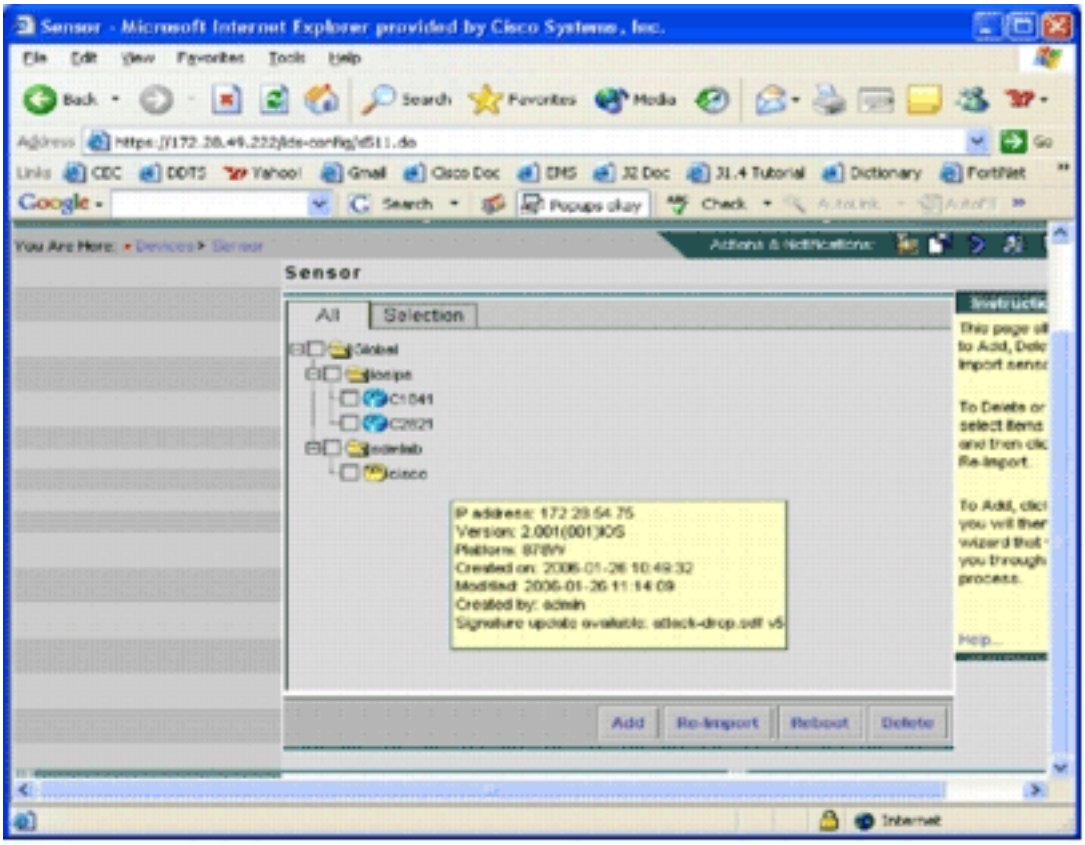
Cette image montre une image des fichiers téléchargés dans ce répertoire.



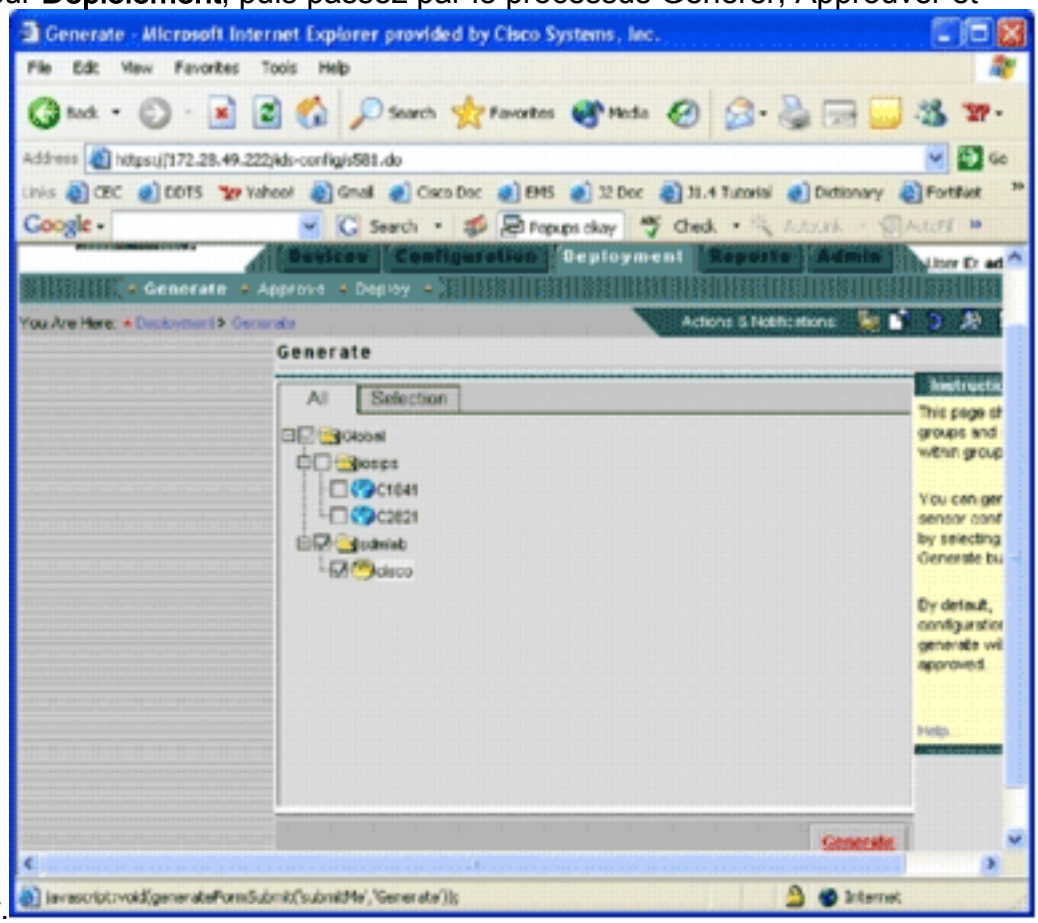
Vous pouvez voir ces fichiers de mise à jour de capteur. Le fichier de mise à jour du logiciel Cisco IOS et les fichiers SDF préconfigurés sont téléchargés.

Mettre à jour le routeur IPS Cisco IOS avec de nouveaux fichiers SDF

Pour les routeurs IPS Cisco IOS déployés avec des fichiers SDF préconfigurés, dès qu'une nouvelle version des fichiers SDF est disponible par téléchargement automatique ou copiée dans le répertoire des mises à jour, Cisco IPS MC reconnaît la nouvelle version. Après une actualisation de l'interface utilisateur, les icônes des périphériques applicables deviennent jaunes.



1. Cliquez sur **Déploiement**, puis passez par le processus Générer, Approuver et Déployer.



2. Après un déploiement réussi, le routeur IPS Cisco IOS utilise une nouvelle version des fichiers SDF.

Informations connexes

- Système de prévention des intrusions Cisco