# CSM 3.x - Ajout de capteurs et de modules IDS à l'inventaire

## Table des matières



## Introduction

Ce document fournit des informations sur la façon d'ajouter des capteurs et des modules IDS (Intrusion Detection System) (y compris IDSM sur les commutateurs Catalyst 6500, NM-CIDS sur les routeurs et AIP-SSM sur ASA) dans Cisco Security Manager (CSM).

Remarque : CSM 3.2 ne prend pas en charge IPS 6.2. Il est pris en charge dans CSM 3.3.

## Conditions préalables

### Exigences

Ce document suppose que les périphériques CSM et IDS sont installés et fonctionnent correctement.

### Composants utilisés

Les informations de ce document sont basées sur CSM 3.0.1.

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.

# Ajouter des périphériques à l'inventaire de Security Manager

Lorsque vous ajoutez un périphérique à Security Manager, vous apportez une plage d'informations d'identification pour le périphérique, telles que son nom DNS et son adresse IP. Une fois le périphérique ajouté, il apparaît dans l'inventaire des périphériques de Security Manager. Vous ne pouvez gérer un périphérique dans Security Manager qu'après l'avoir ajouté à l'inventaire.

Vous pouvez ajouter des périphériques à l'inventaire du Gestionnaire de sécurité avec les méthodes suivantes :

- Ajoutez un périphérique à partir du réseau.
- Ajouter un nouveau périphérique qui n'est pas encore sur le réseau
- Ajoutez un ou plusieurs périphériques à partir du référentiel de périphériques et d'informations d'identification (DCR).
- Ajoutez un ou plusieurs périphériques à partir d'un fichier de configuration.

Remarque : ce document se concentre sur la méthode : Ajouter un nouveau périphérique qui n'est pas encore sur le réseau.

## Étapes d'ajout du capteur et des modules IDS

Utilisez l'option Add New Device afin d'ajouter un seul périphérique à l'inventaire de Security Manager. Vous pouvez utiliser cette option pour le pré-provisionnement. Vous pouvez créer le périphérique dans le système, lui attribuer des stratégies et générer des fichiers de configuration avant de recevoir le matériel du périphérique.

Lorsque vous recevez le matériel du périphérique, vous devez préparer les périphériques à être gérés par Security Manager. Référez-vous à Préparation des périphériques à gérer par Security Manager pour plus d'informations.

Cette procédure montre comment ajouter un nouveau capteur IDS et des modules :

1. Cliquez sur le bouton Device View dans la barre d'outils.

   La page Périphériques s'affiche.

2. Cliquez sur le bouton Add dans le sélecteur Device.

   La page New Device - Choose Method s'affiche avec quatre options.

3. Choisissez Add New Device, puis cliquez sur Next.

La page New Device - Device Information s'affiche.

4. Saisissez les informations relatives au périphérique dans les champs appropriés.

   Pour plus d'informations, reportez-vous à la section Fourniture d'informations sur le périphérique - Nouveau périphérique.

5. Cliquez sur Finish (Terminer).

   Le système effectue les tâches de validation des périphériques :

   - Si les données sont incorrectes, le système génère des messages d'erreur et affiche la page sur laquelle l'erreur se produit avec une icône d'erreur rouge qui lui correspond.
   - Si les données sont correctes, le périphérique est ajouté à l'inventaire et apparaît dans le sélecteur de périphérique.

## Fournir des informations sur le nouveau périphérique

Procédez comme suit :

1. Sélectionnez le type de périphérique du nouveau périphérique :

   a. Sélectionnez le dossier de type de périphérique de niveau supérieur afin d'afficher les familles de périphériques prises en charge.

   b. Sélectionnez le dossier de la famille de périphériques pour afficher les types de périphériques pris en charge.

      a. Sélectionnez Cisco Interfaces and Modules > Cisco Network Modules afin d'ajouter le Cisco IDS Access Router Network Module. De même, sélectionnez Cisco Interfaces and Modules > Cisco Services Modules afin d'ajouter les modules AIP-SSM et IDSM indiqués.

      b. Sélectionnez Security and VPN > Cisco IPS 4200 Series Sensors afin d'ajouter le Cisco IDS 4210 Sensor à l'inventaire CSM.

   c. Sélectionnez le type de périphérique.

      Remarque : une fois que vous avez ajouté un périphérique, vous ne pouvez pas modifier son type.

      Les ID d'objet système de ce type de périphérique sont affichés dans le champ SysObjectId. Le premier ID objet système est sélectionné par défaut. Vous pouvez en sélectionner un autre si nécessaire.

2. Saisissez les informations d'identité du périphérique, telles que le type d'adresse IP (statique ou dynamique), le nom d'hôte, le nom de domaine, l'adresse IP et le nom d'affichage.

3. Saisissez les informations du système d'exploitation du périphérique, telles que le type de

système d'exploitation, le nom de l'image, la version du système d'exploitation cible, les contextes et le mode opérationnel.

4. Le champ Auto Update ou CNS-Configuration Engine s'affiche, en fonction du type de périphérique sélectionné :

   - Auto Update : s'affiche pour les périphériques PIX Firewall et ASA.
   - CNS-Configuration Engine : affiché pour les routeurs Cisco IOS®.

   Remarque : ce champ n'est pas actif pour les périphériques Catalyst 6500/7600 et FWSM.

5. Procédez comme suit :

   - Auto Update : cliquez sur la flèche pour afficher la liste des serveurs. Sélectionnez le serveur qui gère le périphérique. Si le serveur n'apparaît pas dans la liste, procédez comme suit :

     a. Cliquez sur la flèche, puis sélectionnez + Ajouter un serveur... La boîte de dialogue Propriétés du serveur s'affiche.

     b. Saisissez les informations dans les champs obligatoires.

     c. Click OK. Le nouveau serveur est ajouté à la liste des serveurs disponibles.

   - CNS-Configuration Engine : différentes informations s'affichent, selon que vous sélectionnez le type d'IP statique ou dynamique :

     Statique : cliquez sur la flèche pour afficher la liste des moteurs de configuration. Sélectionnez le moteur de configuration qui gère le périphérique. Si le moteur de configuration n'apparaît pas dans la liste, procédez comme suit :

     a. Cliquez sur la flèche, puis sélectionnez + Ajouter un moteur de configuration... La boîte de dialogue Propriétés du moteur de configuration apparaît.

     b. Saisissez les informations dans les champs obligatoires.

     c. Click OK. Le nouveau moteur de configuration est ajouté à la liste des moteurs de configuration disponibles.

   - Dynamique : cliquez sur la flèche pour afficher la liste des serveurs. Sélectionnez le serveur qui gère le périphérique. Si le serveur n'apparaît pas dans la liste, procédez comme suit :

     a. Cliquez sur la flèche, puis sélectionnez + Ajouter un serveur... La boîte de dialogue Propriétés du serveur s'affiche.

     b. Saisissez les informations dans le champ requis.

     c. Click OK. Le nouveau serveur est ajouté à la liste des serveurs disponibles.

6. Procédez comme suit :

    - Afin de gérer le périphérique dans Security Manager, cochez la case Manage in Cisco Security Manager. Il s'agit de la configuration par défaut.
    - Si la seule fonction du périphérique que vous ajoutez est de servir de point d'extrémité VPN, décochez la case Manage in Cisco Security Manager.

      Security Manager ne gère pas les configurations, ni ne télécharge ni ne télécharge les configurations sur ce périphérique.

7. Cochez la case Security Context of Unmanaged Device afin de gérer un contexte de sécurité dont le périphérique parent (PIX Firewall, ASA ou FWSM) n'est pas géré par Security Manager.

   Vous pouvez partitionner un pare-feu PIX, ASA ou FWSM en plusieurs pare-feu de sécurité, également appelés contextes de sécurité. Chaque contexte est un système indépendant, avec sa propre configuration et ses propres politiques. Vous pouvez gérer ces contextes autonomes dans Security Manager, même si le parent (PIX Firewall, ASA ou FWSM) n'est pas géré par Security Manager.

   Remarque : ce champ n'est actif que si le périphérique sélectionné dans le sélecteur de périphérique est un périphérique pare-feu, tel que PIX Firewall, ASA ou FWSM, qui prend en charge le contexte de sécurité.

8. Cochez la case Manage in IPS Manager afin de gérer un routeur Cisco IOS dans IPS Manager.

   Ce champ n'est actif que si vous avez sélectionné un routeur Cisco IOS dans le sélecteur de périphérique.

   Remarque : IPS Manager ne peut gérer les fonctionnalités IPS que sur un routeur Cisco IOS doté de fonctionnalités IPS. Pour plus d'informations, reportez-vous à la documentation IPS.

   Si vous cochez la case Gérer dans IPS Manager, vous devez également cocher la case Gérer dans Cisco Security Manager.

   Si le périphérique sélectionné est IDS, ce champ n'est pas actif. Toutefois, cette case est cochée car IPS Manager gère les capteurs IDS.

   Si le périphérique sélectionné est PIX Firewall, ASA ou FWSM, ce champ n'est pas actif car IPS Manager ne gère pas ces types de périphériques.

9. Cliquez sur Finish (Terminer).

   Le système effectue les tâches de validation des périphériques :

    - Si les données que vous avez entrées sont incorrectes, le système génère des messages d'erreur et affiche la page où l'erreur se produit.

- Si les données que vous avez entrées sont correctes, le périphérique est ajouté à l'inventaire et apparaît dans le sélecteur de périphérique.

# Dépannage

Utilisez cette section pour dépanner votre configuration.

## Messages d'erreur

Lorsque vous ajoutez IPS à CSM, le message d'erreur `Invalid device : Could not deduce the SysObjId for the platform type` apparaît.

Solution

Procédez comme suit pour résoudre ce message d'erreur .

1. Arrêtez le service Démon CSM sous Windows, puis choisissez Program Files > CSCOpx > MDC > athena > config > Directory, où vous pouvez trouver `VMS-SysObjID.xml`.
2. Sur le système CSM, remplacez le fichier VMS-SysObjID.xml d'origine situé par défaut dans `C:\Program Files\CSCOpx\MDC\athena\config\directory` par le fichier `VMS-SysObjID.xml` le plus récent.
3. Redémarrez le service CSM Daemon Manager (CRMDmgtd) et réessayez d'ajouter ou de détecter le ou les périphériques affectés.

# Informations connexes

- Page d'assistance Cisco Security Manager
- Page d'assistance de Cisco Intrusion Detection System
- Assistance et documentation techniques - Cisco Systems

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.