

CSM 3.x: Hinzufügen von IDS-Sensoren und -Modulen zum Security Manager-Bestand

Inhalt

[Einführung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Konventionen](#)

[Hinzufügen von Geräten zum Security Manager-Bestand](#)

[Schritte zum Hinzufügen des IDS-Sensors und der IDS-Module](#)

[Bereitstellung von Geräteinformationen - neues Gerät](#)

[Fehlerbehebung](#)

[Fehlermeldungen](#)

[Zugehörige Informationen](#)

[Einführung](#)

Dieses Dokument enthält Informationen zum Hinzufügen von IDS-Sensoren und -Modulen (einschließlich IDS-M auf Catalyst 6500-Switches, NM-CIDS auf Routern und AIP-SSM auf ASA) zum Cisco Security Manager (CSM).

Hinweis: CSM 3.2 unterstützt IPS 6.2 nicht. Es wird in CSM 3.3 unterstützt.

[Voraussetzungen](#)

[Anforderungen](#)

In diesem Dokument wird davon ausgegangen, dass CSM- und IDS-Geräte installiert sind und ordnungsgemäß funktionieren.

[Verwendete Komponenten](#)

Die Informationen in diesem Dokument basieren auf CSM 3.0.1.

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

[Konventionen](#)

Weitere Informationen zu Dokumentkonventionen finden Sie unter [Cisco Technical Tips Conventions](#) (Technische Tipps zu Konventionen von Cisco).

Hinzufügen von Geräten zum Security Manager-Bestand

Wenn Sie ein Gerät zum Security Manager hinzufügen, geben Sie eine Reihe von Identifikationsdaten für das Gerät ein, z. B. den DNS-Namen und die IP-Adresse des Geräts. Nachdem Sie das Gerät hinzugefügt haben, wird es im Geräteinventar von Security Manager angezeigt. Sie können ein Gerät im Security Manager nur verwalten, nachdem Sie es dem Bestand hinzugefügt haben.

Sie können dem Security Manager-Bestand Geräte mit den folgenden Methoden hinzufügen:

- Hinzufügen eines Geräts aus dem Netzwerk
- Hinzufügen eines neuen Geräts, das sich noch nicht im Netzwerk befindet
- Fügen Sie ein oder mehrere Geräte aus dem DCR (Device and Credentials Repository) hinzu.
- Hinzufügen eines oder mehrerer Geräte aus einer Konfigurationsdatei

Hinweis: Im Mittelpunkt dieses Dokuments steht die Methode: Fügen Sie ein neues Gerät hinzu, das sich noch nicht im Netzwerk befindet.

Schritte zum Hinzufügen des IDS-Sensors und der IDS-Module

Verwenden Sie die Option Neues Gerät hinzufügen, um dem Inventar des Sicherheitsmanagers ein einzelnes Gerät hinzuzufügen. Sie können diese Option für die Vorabbereitstellung verwenden. Sie können das Gerät im System erstellen, dem Gerät Richtlinien zuweisen und Konfigurationsdateien generieren, bevor Sie die Geräte-Hardware erhalten.

Wenn Sie die Geräte-Hardware erhalten, müssen Sie die Geräte auf das Management durch Security Manager vorbereiten. Weitere Informationen finden Sie unter [Vorbereiten der Geräte für das Management von Security Manager](#).

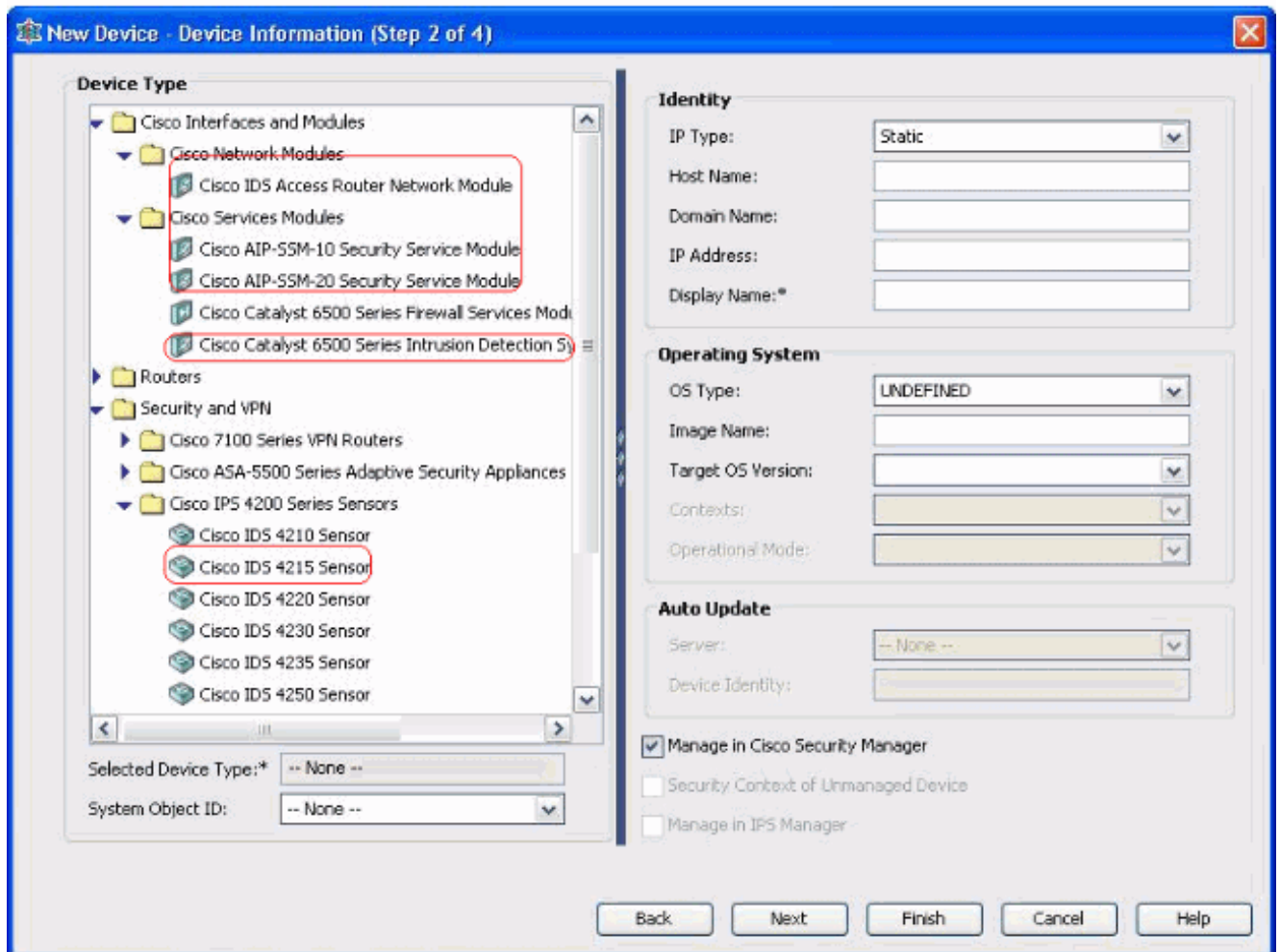
Dieses Verfahren zeigt, wie Sie einen neuen IDS-Sensor und neue Module hinzufügen:

1. Klicken Sie in der Symbolleiste auf die Schaltfläche **Geräteansicht**. Die Seite "Geräte" wird angezeigt.
2. Klicken Sie in der Geräteauswahl auf **Hinzufügen**. Die Seite Neues Gerät - Methode auswählen wird mit vier Optionen angezeigt.
3. Wählen Sie **Neues Gerät hinzufügen aus**, und klicken Sie dann auf **Weiter**. Die Seite Neue Geräte - Geräteinformationen wird angezeigt.
4. Geben Sie die Geräteinformationen in die entsprechenden Felder ein. Weitere Informationen finden Sie im Abschnitt [Providing Device Information - New Device](#) (Geräteinformationen bereitstellen - Neues Gerät).
5. Klicken Sie auf **Fertig stellen**. Das System führt Gerätevalidierungsaufgaben aus: Wenn die Daten falsch sind, generiert das System Fehlermeldungen und zeigt die Seite an, auf der der Fehler auftritt, sowie ein rotes Fehlersymbol entsprechend. Wenn die Daten korrekt sind, wird das Gerät dem Bestand hinzugefügt und in der Geräteauswahl angezeigt.

Bereitstellung von Geräteinformationen - neues Gerät

Gehen Sie wie folgt vor:

1. Wählen Sie den Gerätetyp für das neue Gerät aus: Wählen Sie den Ordner für Gerätetypen der obersten Ebene aus, um die unterstützten Gerätefamilien anzuzeigen. Wählen Sie den Ordner für die Gerätefamilie aus, um die unterstützten Gerätetypen anzuzeigen. Wählen Sie **Cisco-Schnittstellen und -Module > Cisco-Netzwerkmodule**, um das **Cisco IDS Access Router Network Module** hinzuzufügen. Wählen Sie ebenfalls **Cisco-Schnittstellen und -Module > Cisco Services-Module**, um die angezeigten AIP-SSM- und IDSM-Module hinzuzufügen. Wählen Sie **Security and VPN > Cisco IPS Sensoren der Serie 4200** aus, um den Cisco IDS 4210-Sensor dem CSM-Bestand hinzuzufügen.



Wählen Sie den Gerätetyp aus. **Hinweis:** Nachdem Sie ein Gerät hinzugefügt haben, können Sie den Gerätetyp nicht ändern. Systemobjekt-IDs für diesen Gerätetyp werden im Feld SysObjectId angezeigt. Die erste System-Objekt-ID wird standardmäßig ausgewählt. Sie können bei Bedarf ein anderes auswählen.

2. Geben Sie die Informationen zur Geräteidentität ein, z. B. den IP-Typ (statisch oder dynamisch), den Hostnamen, den Domännennamen, die IP-Adresse und den Anzeigenamen.
3. Geben Sie Informationen zum Betriebssystem des Geräts ein, z. B. Betriebssystem, Image-Name, Zielbetriebssystemversion, Kontexte und Betriebsmodus.
4. Das Feld Auto Update (Automatische Aktualisierung) oder CNS Configuration Engine (CNS-Konfigurationsmodul) wird angezeigt. Dies hängt vom ausgewählten Gerätetyp ab: Auto Update (Automatische Aktualisierung) - Wird für PIX-Firewall- und ASA-Geräte angezeigt. CNS-Configuration Engine - Wird für Cisco IOS®-Router angezeigt. **Hinweis:** Dieses Feld ist für Catalyst 6500/7600- und FWSM-Geräte nicht aktiv.

5. Gehen Sie wie folgt vor:Auto Update (Automatische Aktualisierung) - Klicken Sie auf den Pfeil, um eine Liste der Server anzuzeigen. Wählen Sie den Server aus, der das Gerät verwaltet. Wenn der Server nicht in der Liste angezeigt wird, gehen Sie wie folgt vor:Klicken Sie auf den Pfeil und wählen Sie **+ Server hinzufügen...** Das Dialogfeld Servereigenschaften wird angezeigt.Geben Sie die Informationen in die erforderlichen Felder ein.Klicken Sie auf **OK**. Der neue Server wird der Liste der verfügbaren Server hinzugefügt.CNS-Configuration Engine - Es werden unterschiedliche Informationen angezeigt, je nachdem, ob Sie einen statischen oder dynamischen IP-Typ auswählen:**Static (Statisch)**: Klicken Sie auf den Pfeil, um eine Liste der Konfigurationsmaschinen anzuzeigen. Wählen Sie die Configuration Engine aus, die das Gerät verwaltet. Wenn die Configuration Engine nicht in der Liste angezeigt wird, gehen Sie wie folgt vor:Klicken Sie auf den Pfeil, und wählen Sie **+ Konfigurationsmodul hinzufügen aus**. Das Dialogfeld Konfigurationsmoduleigenschaften wird angezeigt.Geben Sie die Informationen in die erforderlichen Felder ein.Klicken Sie auf **OK**. Die neue Configuration Engine wird der Liste der verfügbaren Configuration Engines hinzugefügt.**Dynamic (Dynamisch)** - Klicken Sie auf den Pfeil, um eine Liste der Server anzuzeigen. Wählen Sie den Server aus, der das Gerät verwaltet. Wenn der Server nicht in der Liste angezeigt wird, gehen Sie wie folgt vor:Klicken Sie auf den Pfeil und wählen Sie **+ Server hinzufügen...** Das Dialogfeld Servereigenschaften wird angezeigt.Geben Sie die Informationen in das gewünschte Feld ein.Klicken Sie auf **OK**. Der neue Server wird der Liste der verfügbaren Server hinzugefügt.
6. Gehen Sie wie folgt vor:Um das Gerät in Security Manager zu verwalten, aktivieren Sie das Kontrollkästchen **Manage in Cisco Security Manager (In Cisco Security Manager verwalten)**. Dies ist die Standardeinstellung.Wenn die einzige Funktion des Geräts, das Sie hinzufügen, darin besteht, als VPN-Endpunkt zu dienen, deaktivieren Sie das Kontrollkästchen **Verwalten in Cisco Security Manager**.Security Manager verwaltet keine Konfigurationen oder lädt keine Konfigurationen auf dieses Gerät hoch oder lädt diese herunter.
7. Aktivieren Sie das Kontrollkästchen Sicherheitskontext nicht verwalteter Geräte, um einen Sicherheitskontext zu verwalten, dessen übergeordnetes Gerät (PIX Firewall, ASA oder FWSM) nicht vom Security Manager verwaltet wird.Sie können eine PIX-Firewall, ASA oder FWSM in mehrere Sicherheits-Firewalls partitionieren, die auch als Sicherheitskontexte bezeichnet werden. Jeder Kontext ist ein unabhängiges System mit eigener Konfiguration und eigenen Richtlinien. Sie können diese Standalone-Kontexte in Security Manager verwalten, auch wenn die übergeordnete (PIX Firewall, ASA oder FWSM) nicht von Security Manager verwaltet wird.**Hinweis**: Dieses Feld ist nur dann aktiv, wenn es sich bei dem in der Geräteauswahl ausgewählten Gerät um ein Firewall-Gerät handelt, das Sicherheitskontext unterstützt, z. B. PIX Firewall, ASA oder FWSM.
8. Aktivieren Sie das Kontrollkästchen **Manage in IPS Manager (In IPS Manager verwalten)**, um einen Cisco IOS-Router in IPS Manager zu verwalten.Dieses Feld ist nur aktiv, wenn Sie einen Cisco IOS-Router aus dem Geräte-Selektor ausgewählt haben.**Hinweis**: IPS Manager kann die IPS-Funktionen nur auf einem Cisco IOS-Router verwalten, der über IPS-Funktionen verfügt. Weitere Informationen finden Sie in der IPS-Dokumentation.Wenn Sie das Kontrollkästchen In IPS Manager verwalten aktivieren, müssen Sie auch das Kontrollkästchen In Cisco Security Manager verwalten aktivieren.Wenn das ausgewählte Gerät IDS ist, ist dieses Feld nicht aktiv. Das Kontrollkästchen ist jedoch aktiviert, da IPS Manager IDS-Sensoren verwaltet.Wenn das ausgewählte Gerät PIX Firewall, ASA oder FWSM ist, ist dieses Feld nicht aktiv, da der IPS Manager diese Gerätetypen nicht verwaltet.
9. Klicken Sie auf **Fertig stellen**.Das System führt Gerätevalidierungsaufgaben aus:Wenn die eingegebenen Daten falsch sind, generiert das System Fehlermeldungen und zeigt die Seite

an, auf der der Fehler auftritt. Wenn die von Ihnen eingegebenen Daten korrekt sind, wird das Gerät dem Bestand hinzugefügt und in der Geräteauswahl angezeigt.

Fehlerbehebung

In diesem Abschnitt finden Sie eine Fehlerbehebung für Ihre Konfiguration.

Fehlermeldungen

Wenn Sie IPS zu CSM hinzufügen, ist das Gerät ungültig: Die SysObjId konnte nicht für die Fehlermeldung `Plattformtyp` angegeben werden.

Lösung

Führen Sie diese Schritte aus, um diese Fehlermeldung zu beheben.

1. Beenden Sie den CSM Daemon-Dienst in Windows, und wählen Sie dann **Programme > CSCOpX > MDC > athena > config > Directory**, wo Sie `VMS-SysObjID.xml` finden können.
2. Ersetzen Sie auf dem CSM-System die ursprüngliche `VMS-SysObjID.xml`-Datei, die sich standardmäßig in `C:\Program Files\CSCOpX\MDC\athena\config\directory` befindet, durch die neueste `VMS-SysObjID.xml`-Datei.
3. Starten Sie den Dienst CSM Daemon Manager (CRMDmgtd) neu, und versuchen Sie erneut, die betroffenen Geräte hinzuzufügen oder zu erkennen.

Zugehörige Informationen

- [Support-Seite für Cisco Security Manager](#)
- [Support-Seite für das Cisco Intrusion Detection System](#)
- [Technischer Support und Dokumentation - Cisco Systems](#)