Cisco IOS IPS中的CiscoWorks IPS MC配置示例

目錄

簡介

CiscoWorks Management Center for IPS Sensors(IPS MC)是Cisco IPS裝置的管理控制檯。IPS MC版本2.2支援Cisco IOS®軟體路由器上的入侵防禦系統(IPS)功能調配。本文檔介紹如何使用IPS MC 2.2配置Cisco IOS IPS。

有關如何使用IPS MC的詳細資訊（包括如何使用它來配置不基於Cisco IOS軟體的裝置），請參閱以下URL的CiscoWorks感測器管理中心文檔：

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

必要條件

需求

本文件沒有特定需求。

採用元件

本檔案中的資訊是根據CiscoWorks Management Center for IPS Sensors(IPS MC)版本2.2。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

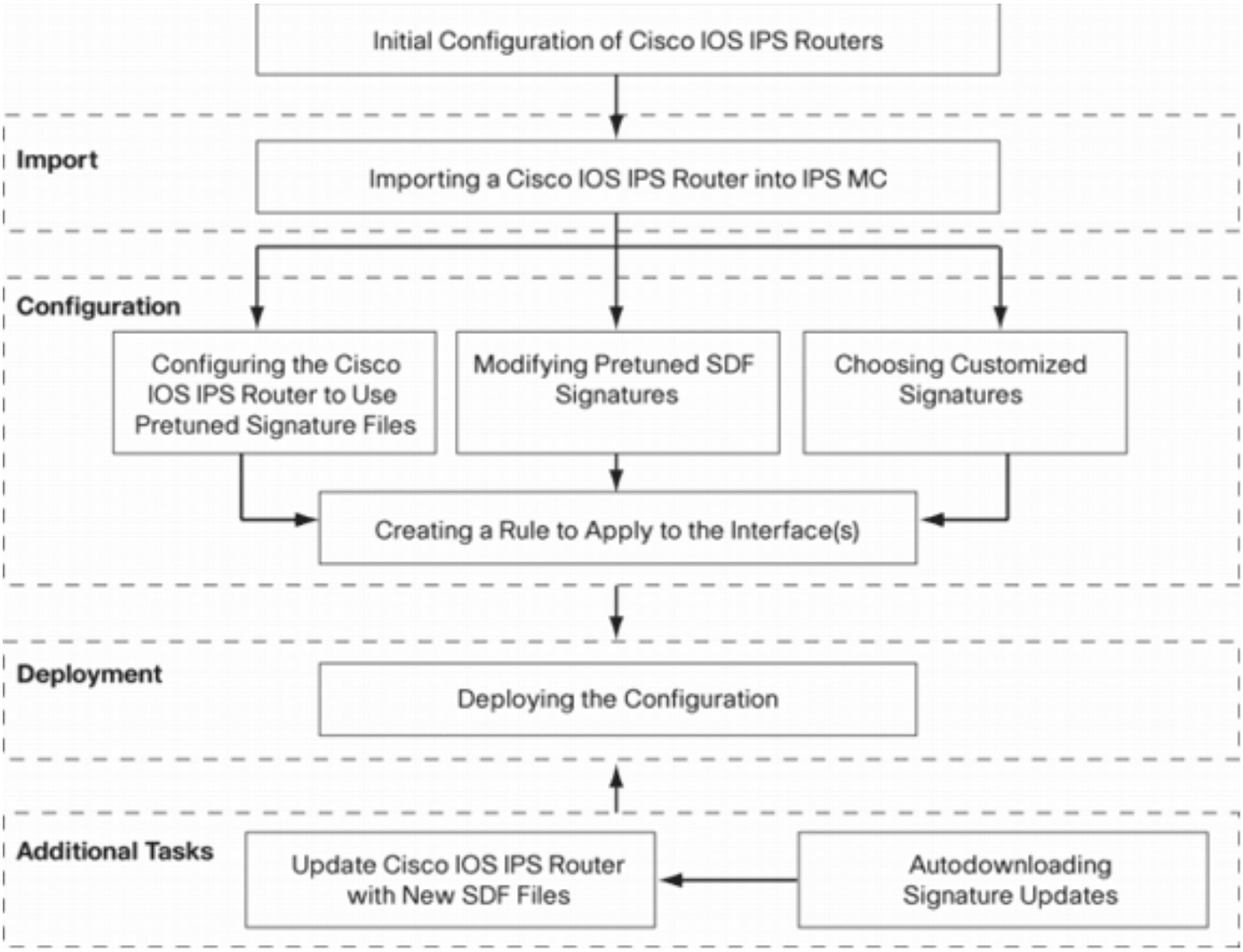
慣例

請參閱思科技術提示慣例以瞭解更多有關文件慣例的資訊。

設定

對配置任務的基本瞭解

IPS MC用於管理一組Cisco IOS IPS路由器的配置。請注意，IPS MC不管理運行IPS的路由器的警報。思科建議使用思科安全監控、分析和響應系統(Cisco Security MARS)進行IPS監控。配置管理包括本文檔中描述的一系列任務。這些任務可分為三個階段：匯入、組態和部署，如下圖所示。



每個階段都有自己的一套責任和職能：

- *Import* — 將路由器匯入IPS MC。必須先將路由器匯入IPS MC，然後才能使用IPS MC進行配置。除非路由器上存在初始IPS配置，否則無法匯入路由器（本文檔稍後將介紹詳細資訊）。
- *Configuration* — 配置裝置。例如，您可以將Cisco IOS IPS路由器配置為使用思科推薦的預調整簽名檔案之一。配置更改儲存在IPS MC中，但在此階段不會傳送到路由器。
- *部署* — 將配置更改傳送到實際裝置。在此階段，您將配置任務中的更改提交給路由器。

- *Additional Tasks* - IPS MC提供自動下載功能，可自動從Cisco.com下載特徵碼更新。

您必須瞭解這種分階段的方法，才能有效使用IPS MC。它不同於基於裝置的管理GUI，例如Cisco Router and Security Device Manager(SDM)。 基於裝置的GUI直接作用在單個路由器上，而IPS MC則設計用於網路範圍內的路由器（和其他IPS裝置，如Cisco IPS 4200系列感測器）組。

本文檔提供有關圖中的每項任務的資訊，幫助您使用IPS MC管理Cisco IOS IPS路由器。

Cisco IOS IPS路由器的初始配置

要成功將Cisco IOS IPS路由器匯入或新增到IPS MC，必須在Cisco IOS IPS路由器上執行某些初始配置步驟。本節介紹這些步驟。

您必須在Cisco IOS IPS路由器中啟用安全外殼(SSH)協定，以便通過Cisco IPS MC進行配置、匯入和部署。此外，出於事件報告的目的，必須啟用安全裝置事件交換(SDEE)協定（儘管這些警報不會傳送到IPS MC，因為IPS MC僅用於調配，而不用於報告）。 最後，您需要確保IPS路由器上的時鐘設定與IPS MC同步。

完成以下步驟以配置您的IOS IPS路由器：

1. 為路由器建立本地使用者名稱和密碼。
```
Router#config terminal
Router(config)#username <username> password <password>
```

2. 在vty線路介面上啟用本地登入。
```
Router#config terminal
Router(config)#line vty 0 15
Router(config-line)#login local
Router(config-line)#exit
```

   如果在vty線路配置下配置了transport input或transport output命令列介面(CLI)，請確保已啟用SSH。例如：
```
Router#conf terminal
Router(config)#line vty 0 15
Router(config-line)#transport input ssh telnet
Router(config-line)#exit
```

3. 生成1024位RSA金鑰（如果金鑰不存在）。生成加密金鑰後將自動啟用SSH。
```
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. 在路由器上啟用SDEE。
```
Router(config)#ip ips notify sdee
```

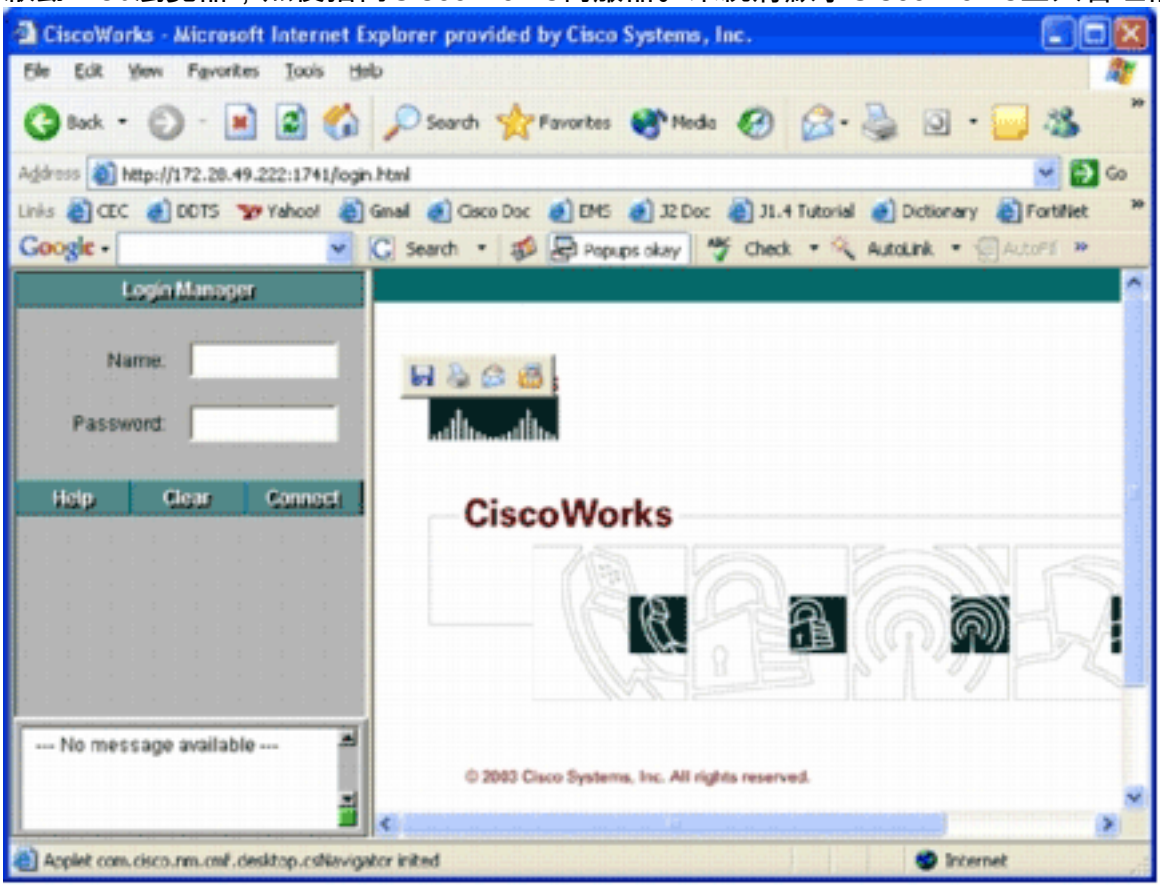
5. 啟用HTTPS。IPS MC需要使用HTTP或HTTPS與具有SDEE的路由器通訊以收集事件資訊。
```
Router(config)#ip http authentication local
Router(config)#ip http secure-server
```

6. 使用外部網路時間協定(NTP)伺服器或clock命令在IPS路由器上配置時鐘設定。
   ```
   Router(config)#clock set hh:mm:ss day month year
   ```

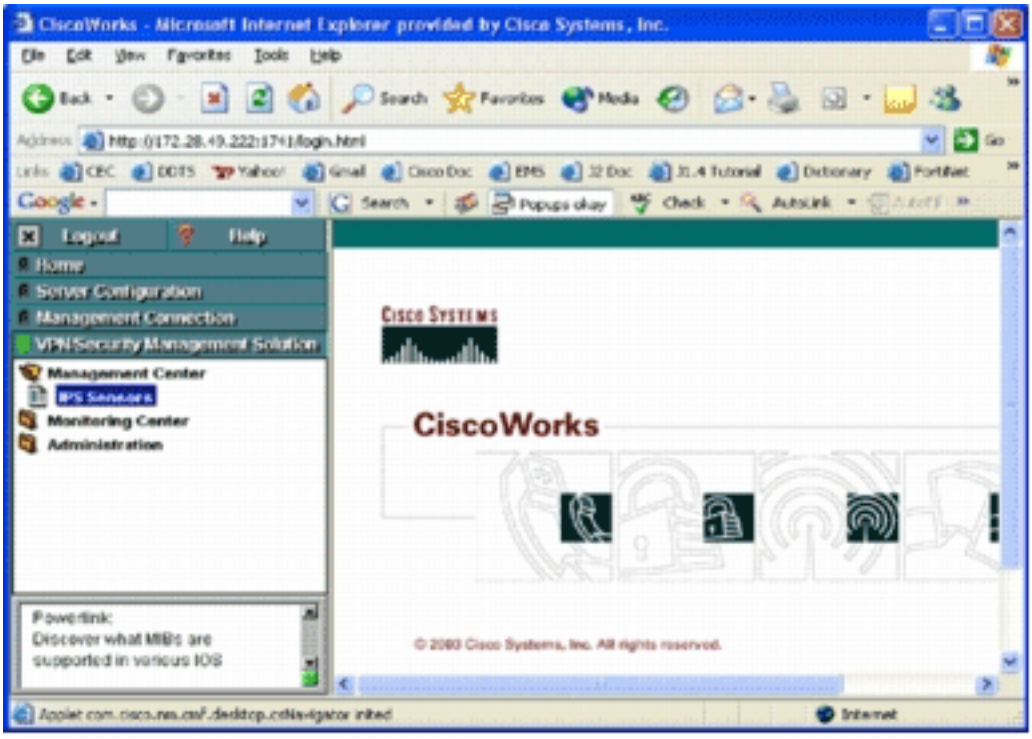
現在，Cisco IOS IPS路由器已準備就緒，可以匯入到IPS MC以進行進一步的配置和管理。

將Cisco IOS IPS路由器匯入IPS MC

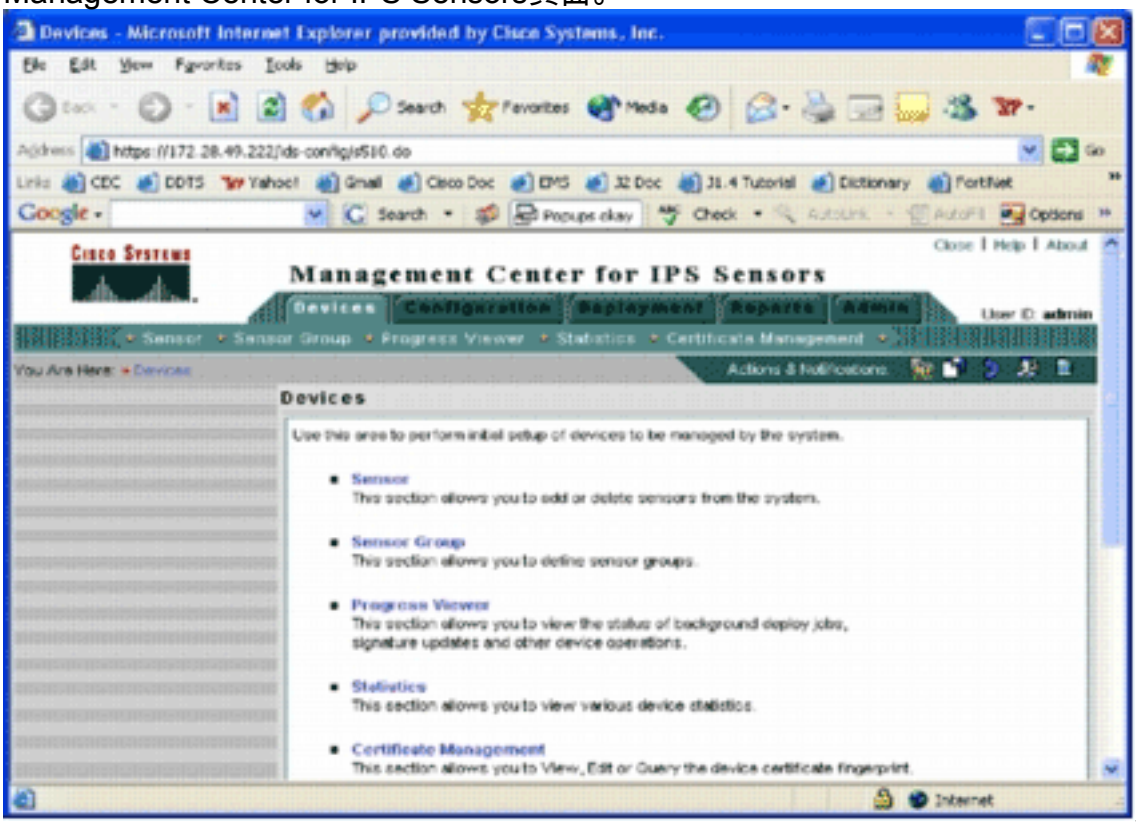
完成路由器上的初始配置後，可以將其新增（或匯入）到IPS MC中。

1. 啟動Web瀏覽器，然後指向CiscoWorks伺服器。系統將顯示CiscoWorks登入管理器。


註：Web伺服器的預設埠號為1741;因此，您應該使用類似於http://<*server ip address*>:1741/的URL。
2. 輸入您的使用者名稱和密碼以便登入。系統將顯示CiscoWorks首頁。

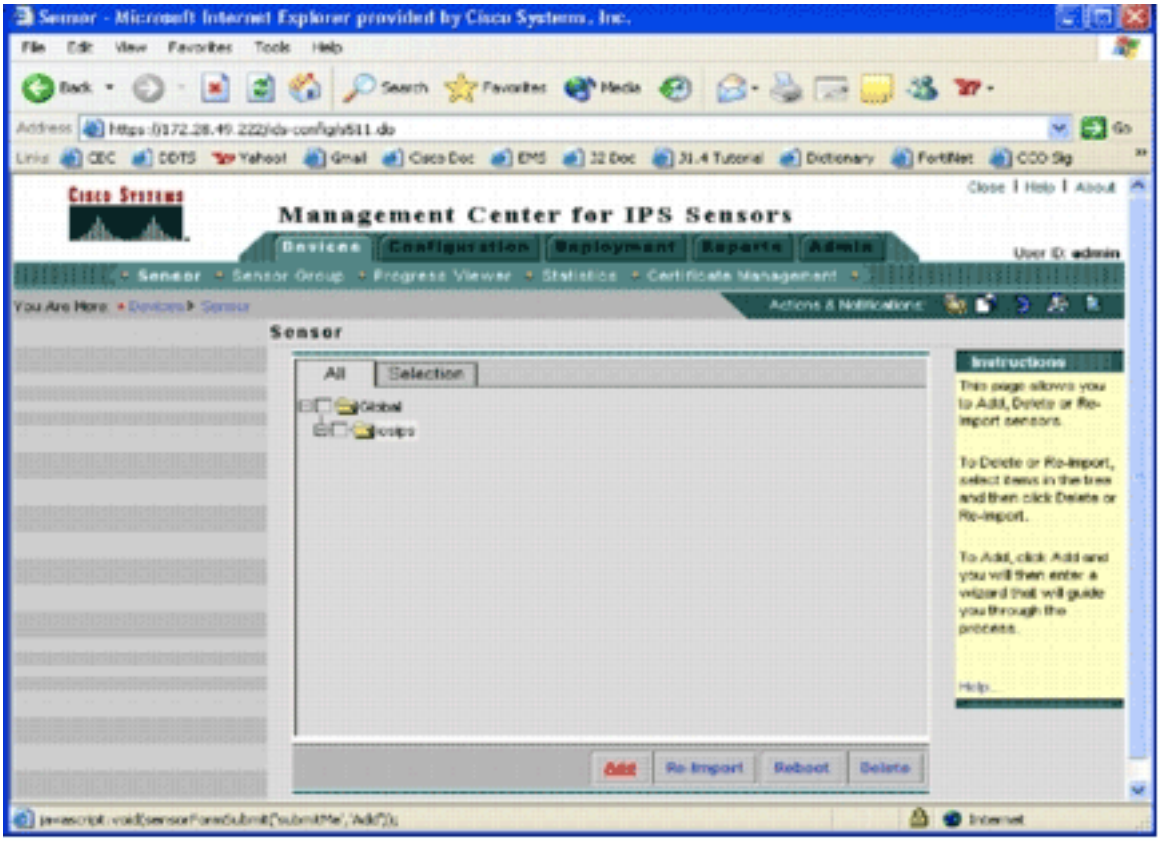


3. 在左側導航窗格中，選擇**VPN/安全管理解決方案**，然後選擇**管理中心**。系統將顯示Management Center for IPS Sensors頁面。

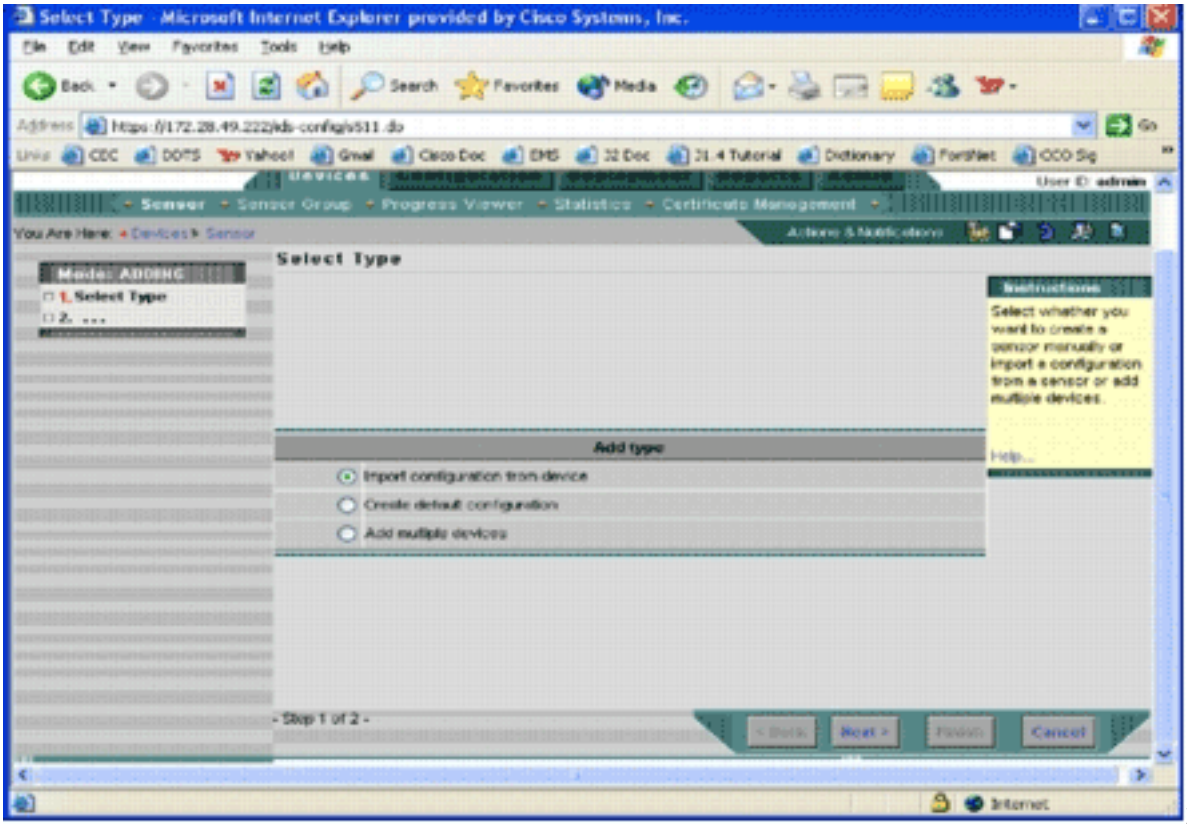


此頁顯示以下五個頁籤：*Devices* — 在Devices頁籤中，您可以執行系統上的所有裝置的初始設定並對其進行管理。*Configuration* — 在Configuration頁籤中，您可以執行調配功能。您可以在單個裝置級別或組級別配置裝置。一個裝置組可以包含多個裝置。必須儲存通過配置任務所做的所有更改。配置功能不會立即更改裝置。您必須使用部署功能才能部署更改。*部署* — 在「部署」頁籤中，您可以將配置更改部署到裝置。計畫功能可以靈活控制配置更改何時生效。*Reports* — 在Reports頁籤中，可以生成各種系統操作報告。*Admin* — 在Admin頁籤中，可以執行系統管理任務，如資料庫管理、系統配置和許可證管理。

4. 按一下**Devices**頁籤以新增新裝置。系統將顯示Sensor頁面。



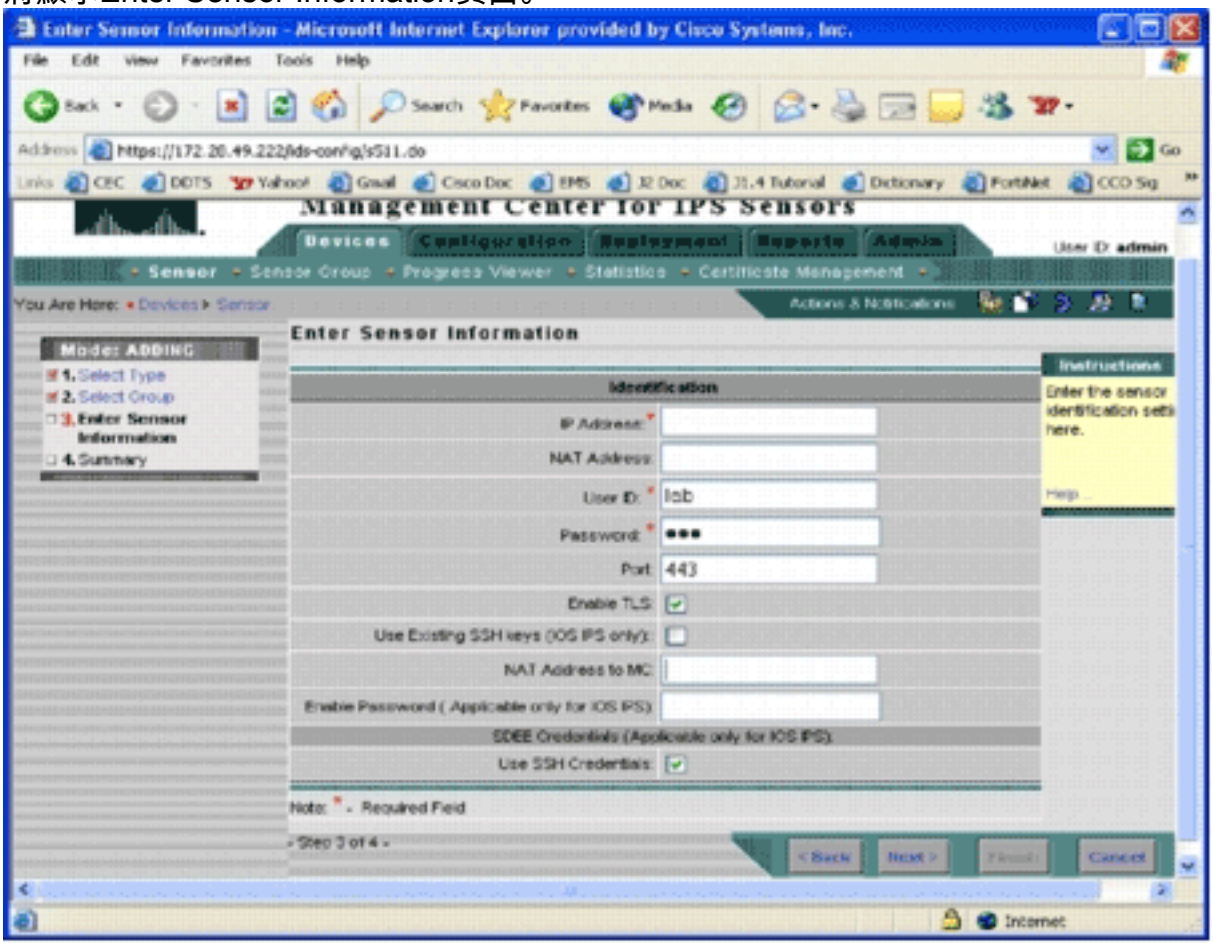
5. 按一下「**Add**」。此時會顯示「選擇型別」頁面。



您必須通知IPS MC要執行哪種型別的新增功能。此清單說明每個選項：*從裝置匯入配置* — 使用此選項可新增到當前在網路上運行的IPS MC裝置。*Create default configuration* — 使用此選項新增當前尚未在網路上運行的裝置。*新增多個設*備 — 使用此選項新增多個裝置。您可以建立包含所有裝置資訊的.csv或.xml檔案，然後將其匯入IPS MC以一次新增裝置。**提示：**示例.csv格式和.xml格式檔案位於：InstallDirectory\MDC\etc\ids\，分別命名為MultipleAddDevices-format.csv和MultipleAddDevices-format.xml。

6. 選擇適當的Add type選項，然後按一下**Next**。
7. 選擇要向其新增Cisco IOS IPS路由器的組，或使用預設全域性組，然後按一下**下一步**。系統

將顯示Enter Sensor Information頁面。



8. 在「標識」頁中，輸入裝置的標識資訊。**注意**：如果使用者沒有許可權級別15訪問許可權，則必須提供啟用密碼。在Identification頁的最後一行中，選中**Use SSH Credentials**覈取方塊。
9. 按「**Next**」（下一步）。出現「Add Sensor Summary（新增感測器摘要）」。
10. 按一下「**Finish**」（結束）。裝置已成功新增到IPS MC中。**注意**：如果在匯入過程中遇到錯誤，請確保選中以下項：*必備配置* - IPS MC與Cisco IOS IPS路由器通訊需要這些配置。*Connectivity* — 確保IPS MC可以到達Cisco IOS IPS路由器。*Clock* — 檢查IPS MC和Cisco IOS IPS路由器上的時間。時間是用於身份驗證的https證書的重要組成部分。時間必須在彼此的12小時內。（最佳實踐最多只有幾個小時。）*Cisco IOS IPS Certificate* — 有時所儲存的Cisco IOS IPS證書不正確。若要從Cisco IOS IPS刪除證書，您必須從Cisco IOS IPS路由器刪除信任點。*Additional Configuration* — 如果**ip http timeout-policy**配置的最大請求數較低，例如**ip http timeout-policy idle 600 life 86400 requests 1**，則必須增加最大請求數。例如：**ip http timeout-policy idle 600 life 86400 requests 8400**

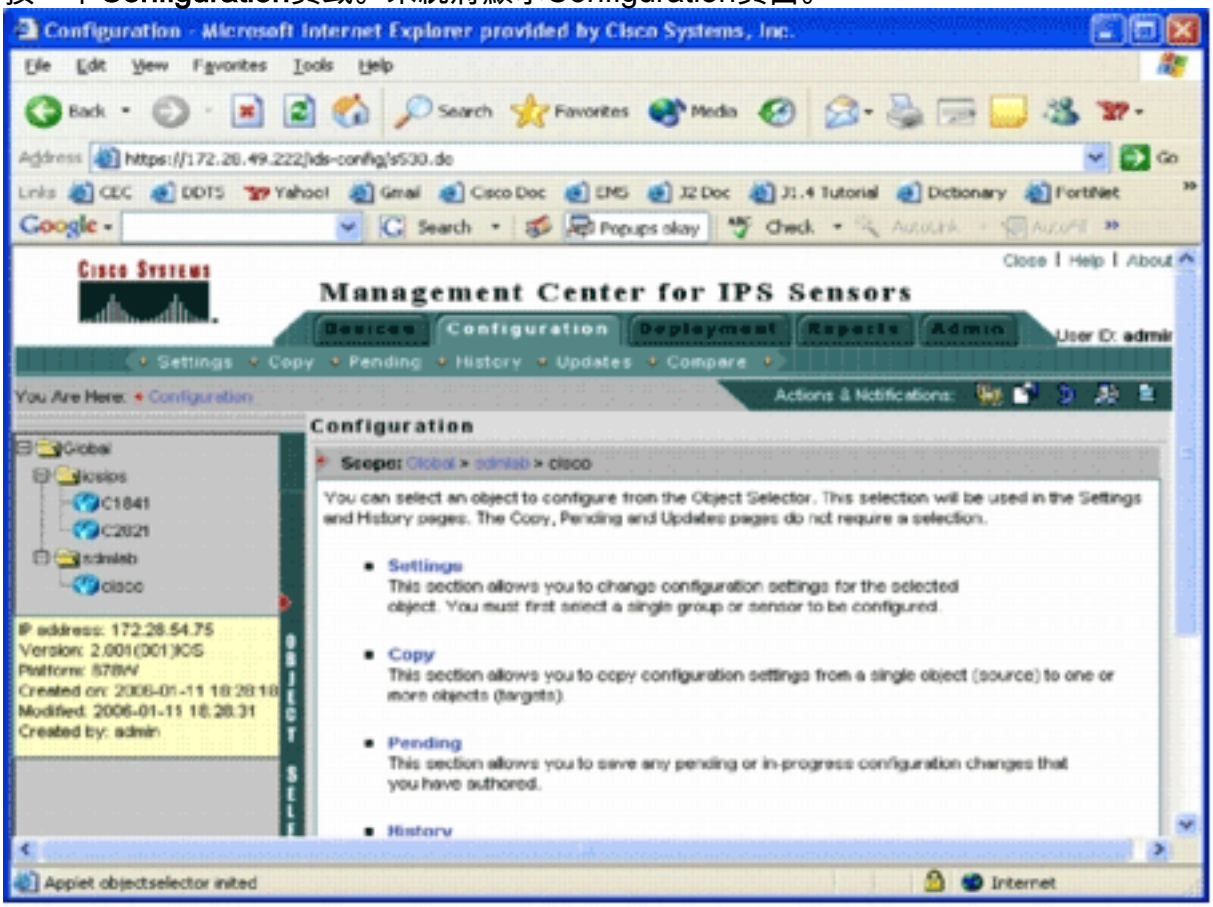
配置Cisco IOS IPS路由器以使用預最佳化的簽名檔案

將路由器匯入IPS MC後，必須選擇特徵碼定義檔案(SDF)（基於文本的檔案，包括IPS路由器將使用的威脅特徵碼）和觸發每個特徵碼時要採取的操作（例如，丟棄、TCP重置、警報）。

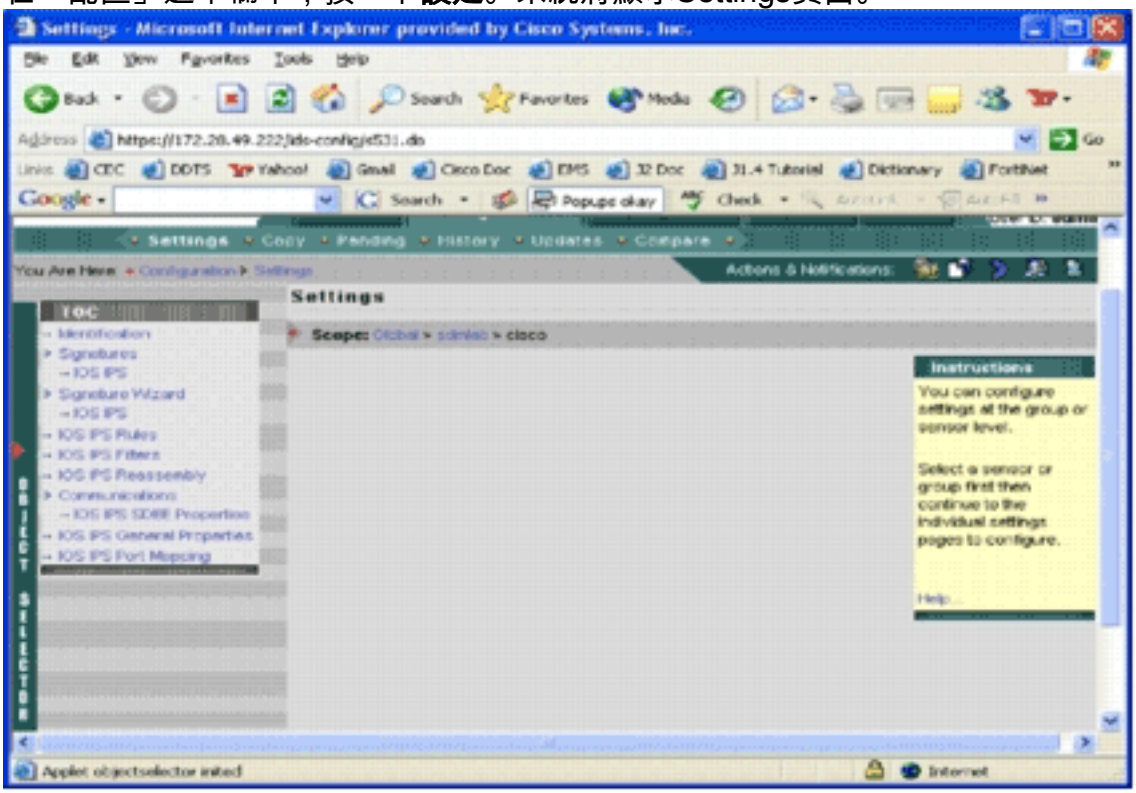
Cisco Systems®建議您使用思科預最佳化的SDF檔案。目前有三個此類檔案：attack-drop.sdf、128MB.sdf和256MB.sdf。IPS MC可以自動從Cisco.com下載這些檔案。有關詳細資訊，請參閱自動下載特徵碼更新。

此過程使用單個裝置作為示例，並以沒有IPS配置的路由器開頭。也可以將此過程用於組級別上的多個裝置。

1. 按一下**Configuration**頁籤。系統將顯示Configuration頁面。



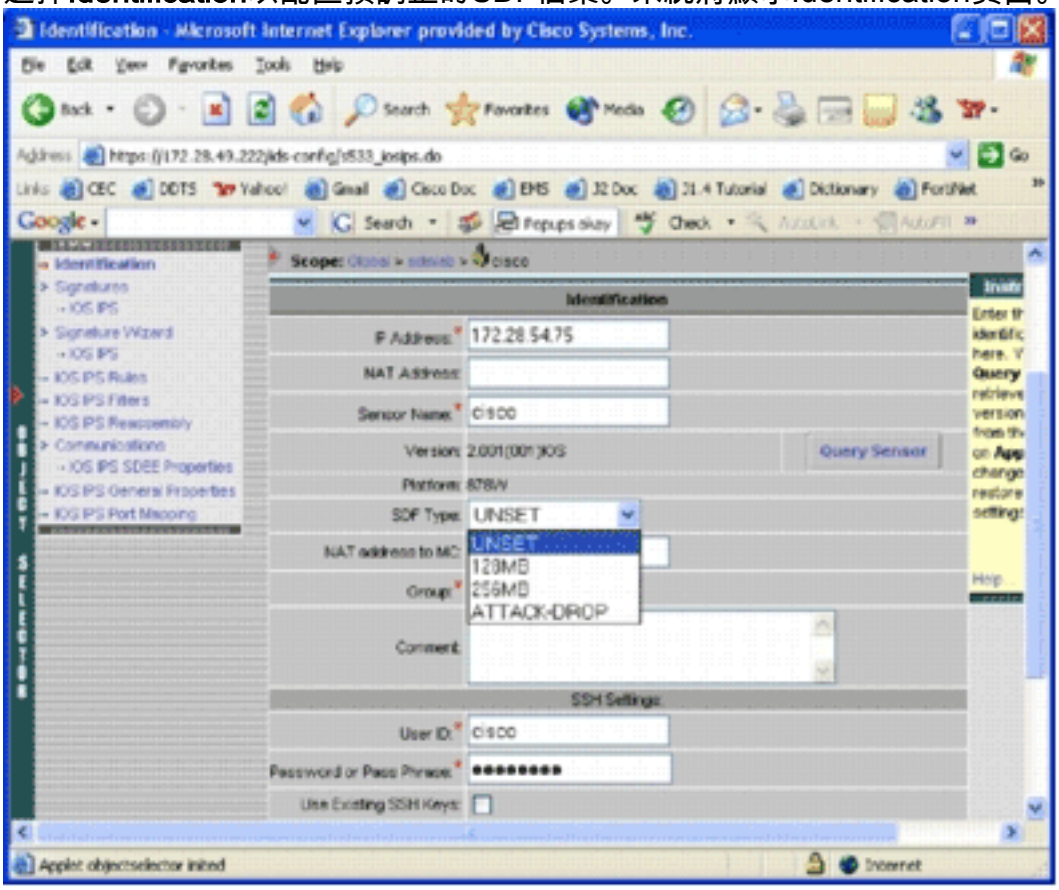
2. 從頁面左側的Object Selector中，選擇要配置的Cisco IOS IPS路由器。**注意：**IPS MC 2.2中的大多數配置設定可在組級別和單個裝置級別進行配置。例如，全域性、iosip和sdmlab組都是可配置的對象組。本示例使用sdmlab組的單個裝置cisco。選擇要配置的路由器後，位於Configuration頁面頂部的路徑欄會顯示當前配置範圍。例如，此示例的範圍是*Global > sdmlab > cisco*。*cisco*是目前的組態對象（即從物件選取器選取的路由器）。
3. 在「配置」選單欄中，按一下**設定**。系統將顯示Settings頁面。



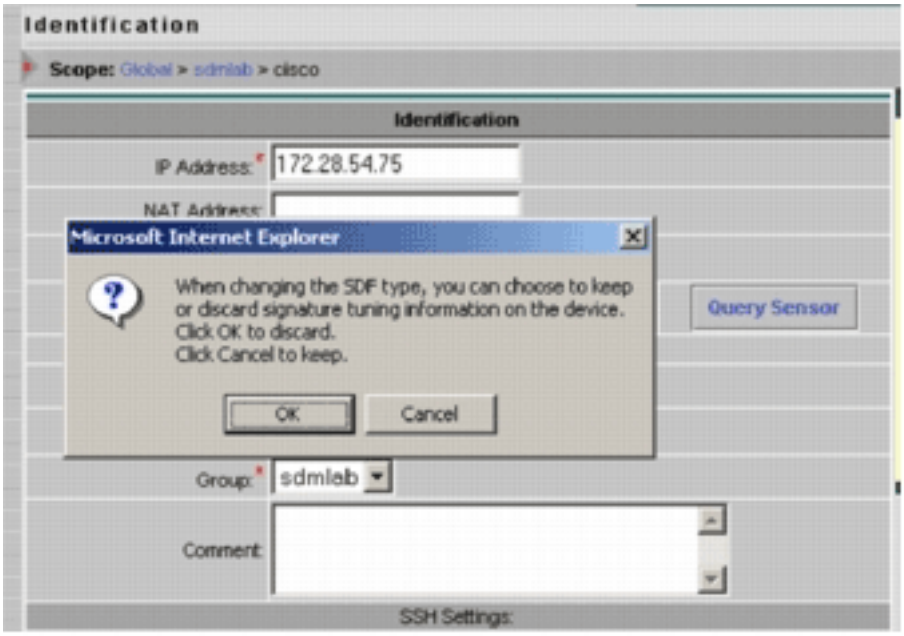
在「設定」頁中，可以更改所選對象的配置設定。Cisco IOS IPS路由器特定的配置設定位於頁面左側的

TOC部分。以下是「目錄」部分下可用的任務清單：*標識*- Cisco IOS IPS路由器基本資訊；您可以在此處指定預最佳化的SDF檔案*簽名*- Cisco IOS IPS路由器簽名*簽名向導* — 用於新增自定義簽名的簽名嚮導*Cisco IOS IPS規則* — 用於配置應用於介面的Cisco IOS IPS規則*Cisco IOS IPS過濾器*- Cisco IOS IPS過濾器*Cisco IOS IPS重組* — 介面IP虛擬重組組態*Cisco IOS IPS SDEE屬性* — 用於配置SDEE設定*Cisco IOS IPS常規屬性* — 其他Cisco IOS IPS相關配置

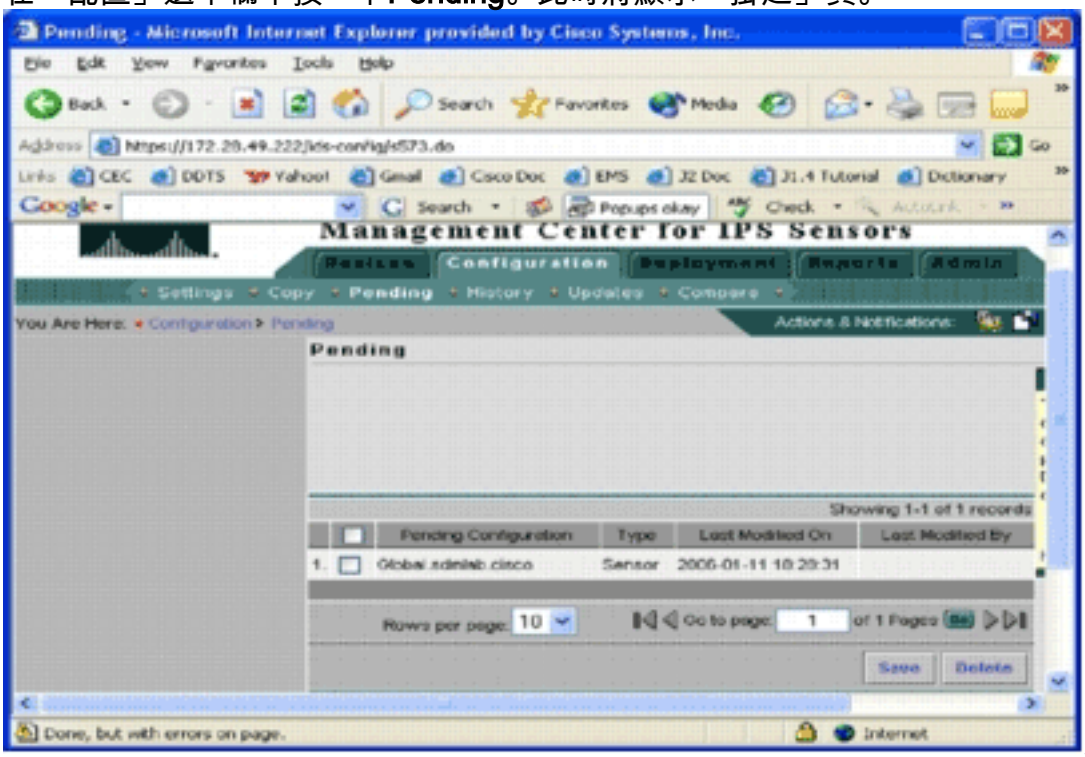
4. 選擇**Identification**以配置預調整的SDF檔案。系統將顯示Identification頁面。



5. 從SDF型別(SDF Type)下拉選單中，選擇相應的預最佳化的SDF，然後按一下**應用**以應用更改。Cisco IOS IPS支援超過1600個簽名，超出路由器所能接受的記憶體容量。SDF被開發為選擇和載入最重要的簽名的便利方法。目前，您可以從三個SDF中進行選擇。它們的大小不同，以便根據路由器的DRAM容量選擇SDF檔案。可用選項如下所述：UNSET — 未設定SDF型別。ATTACK-DROP — 此SDF用於具有64 MB DRAM的路由器。256MB — 此SDF用於具有256 MB DRAM的路由器。128MB — 此SDF用於具有128 MB DRAM的路由器。**註：**128和256 MB SDF需要2.001或更高版本的引擎。此資訊可在**Settings > Identification UI > Version**欄位中獲得。**警告：**IPS MC不包括Cisco IOS IPS路由器的記憶體管理功能。為Cisco IOS IPS路由器選擇SDF檔案時請小心。確保Cisco IOS IPS路由器有足夠的記憶體運行所選SDF檔案。**注意：**更改SDF型別時，可能會收到以下消息：*更改SDF型別時，可以選擇在裝置上保留或放棄簽名調整資訊。按一下「確定」以放棄。按一下「取消」保留。*



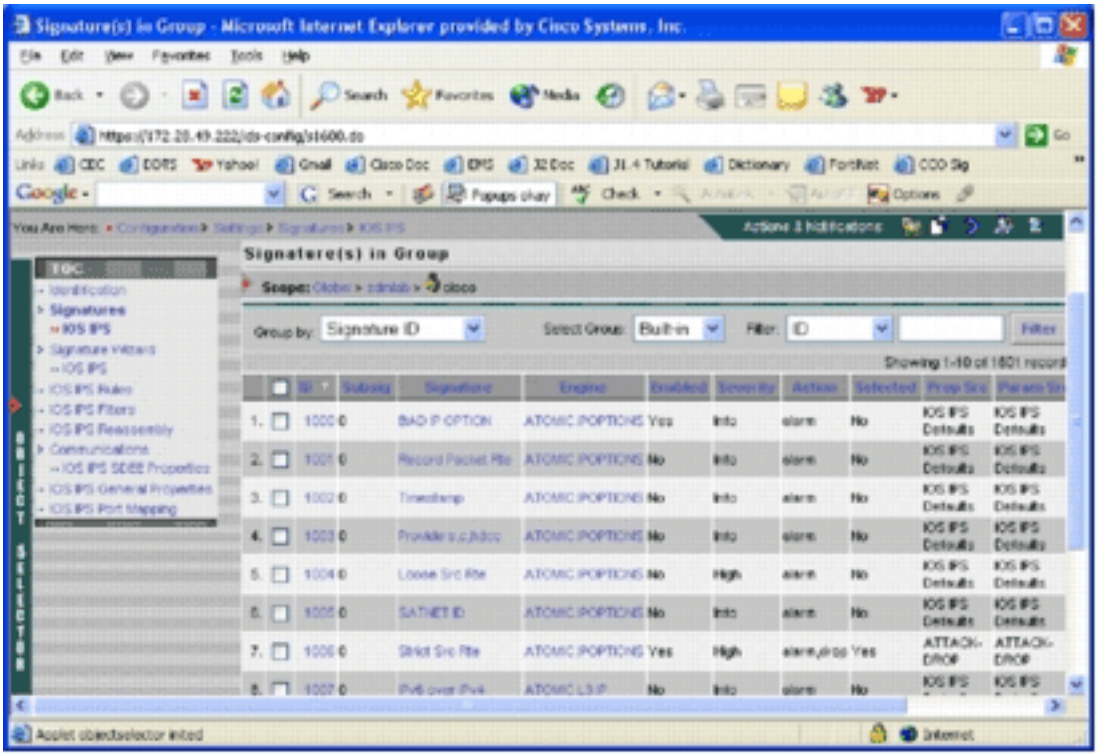
6. 按一下**取消**可保留您的簽名最佳化資訊。既然您已成功為路由器cisco選擇了預最佳化的SDF，那麼您可以執行額外的特徵碼調整，如新增或編輯，甚至建立您自己的特徵碼，也可以跳過特徵碼調整任務並直接轉至Create a Rule to Apply to the Interface(s)。
7. 在「配置」選單欄中按一下**Pending**。此時將顯示「掛起」頁。



此時，配置任務已完成。但是，您必須完成部署任務才能將更改部署到目標裝置。

修改預最佳化的SDF簽名

為路由器選擇預最佳化的SDF檔案後，可以執行其他簽名最佳化任務。您可以新增、編輯、刪除和修改簽名，使其最符合您的需要，也可以在必要時建立您自己的簽名。此示例使用IPS MC來新增其他簽名並修改操作。此圖顯示簽名配置介面。



您可以使用簽名配置來啟用或禁用、選擇或取消選擇、新增簽名、刪除簽名、更改簽名操作以及編輯簽名引數。使用左側的簽名嚮導建立自定義簽名。

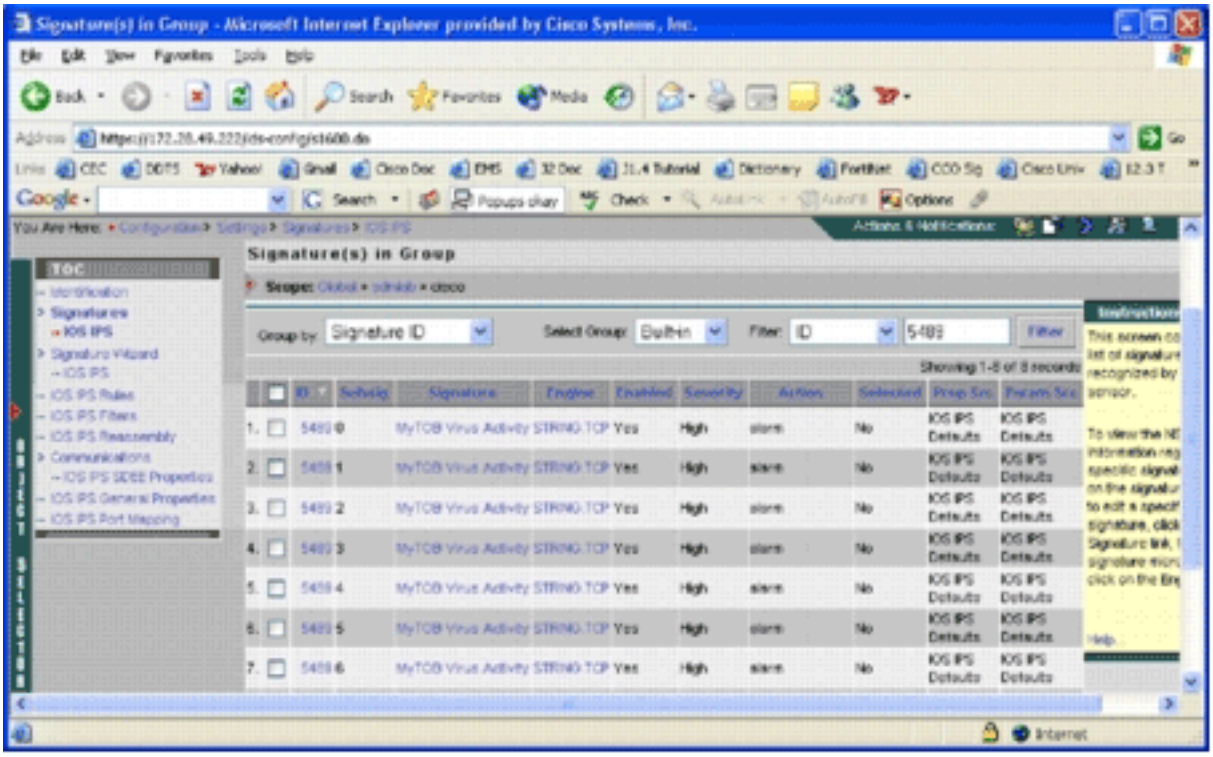
在簽名配置使用者介面中，預設情況下顯示一些資訊。Selected表示簽名是否將包括在傳送到路由器的SDF檔案中。如果未選擇簽名，將不會新增簽名。「啟用」僅在選擇簽名時適用。禁用特徵碼後，IPS引擎將不會傳送該特定特徵碼的事件。如果未選擇簽名，則也會自動禁用它。

最後兩列（Prop Src和Param Src）分別告訴您簽名及其引數來自何處。該簽名可能來自預最佳化的SDF檔案，也可能來自出廠預設設定，您可以在IOS-Sxxx.zip檔案更新中找到這些檔案（它顯示為IOS IPS預設值）。 這些值也適用於引數列。

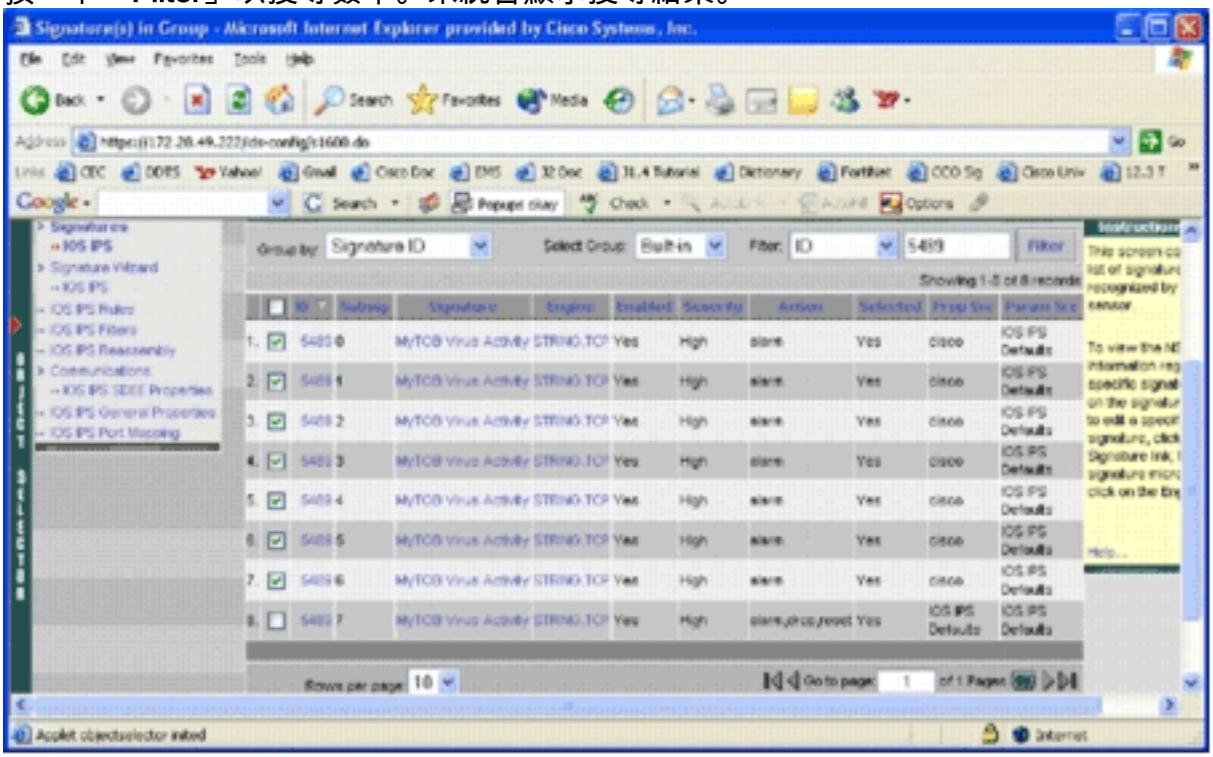
向Cisco IOS IPS路由器新增簽名時，必須考慮記憶體問題。如果新增的簽名數超過Cisco IOS IPS路由器可以處理的簽名數，IPS MC將無法將配置更改部署到裝置。

完成以下步驟，將簽名5489/x新增到Cisco IOS IPS路由器：

1. 選擇**Configuration**，然後使用對象選擇器選擇要為其配置IPS簽名的Cisco IOS IPS路由器。
2. 選擇**Configuration > Settings > Signatures > IOS IPS**。此時會顯示「組中的簽名」頁。

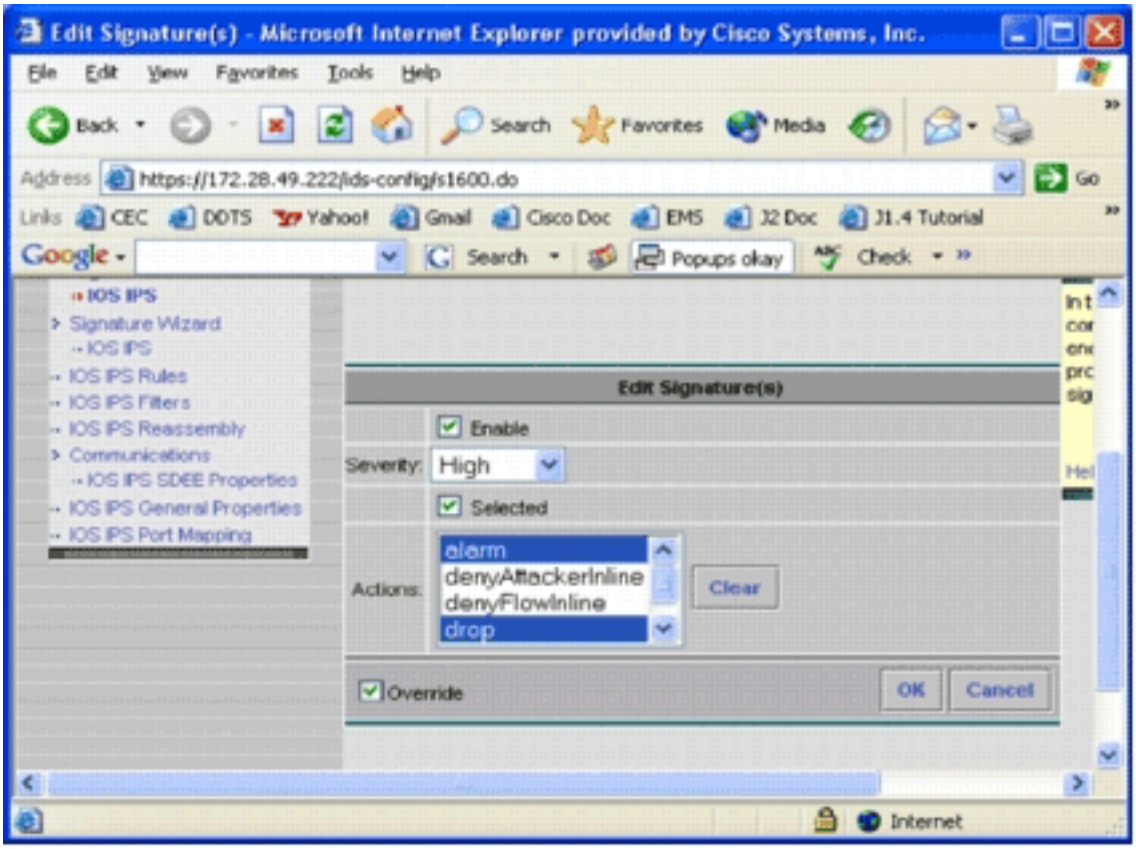


3. 在結果的簽名清單中，選擇按ID過濾，然後鍵入簽名ID 5489。
4. 按一下「**Filter**」以搜尋簽章。系統會顯示搜尋結果。

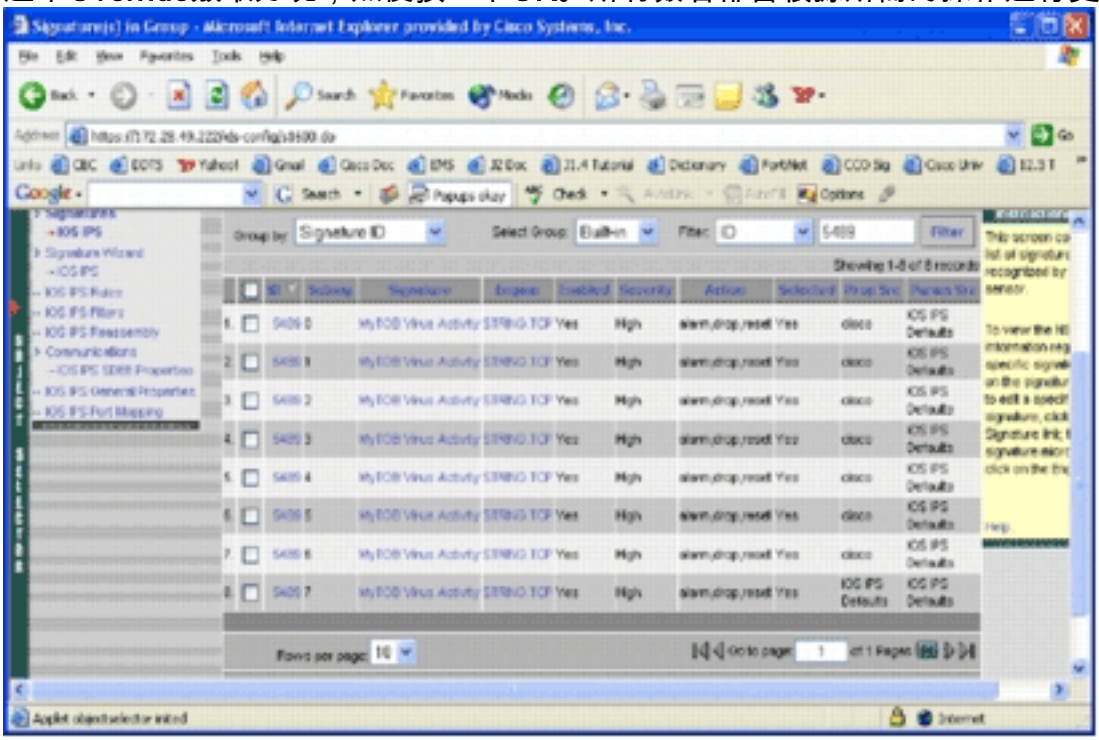


注意：IPS MC不支援Cisco SDM中可用的新分類。

5. 選中尚未選擇的簽名旁邊的覈取方塊，然後按一下底部工具欄上的**Select**。
6. 按一下**Edit**以更改簽名操作。系統將顯示Edit Signature(s)頁面。



7. 選中**Selected**覈取方塊，然後從「Actions」清單中選擇**alarm**、**drop**和**reset**。
8. 選中**Override**覈取方塊，然後按一下**OK**。所有簽名都會根據所需的操作進行更改。



9. 轉到「暫掛」任務並儲存所有更改。這樣即可完成配置任務。**提示**：密切注意「Prop Src」列。修改後，源裝置更改為名為*cisco*的裝置，這意味著所有調整資訊都與預設預調整的SDF檔案分開儲存。此機制使IPS MC能夠保留自定義簽名更改。

在前面的章節中，當您更改SDF檔案型別時，IPS MC會詢問您是否要保留特徵碼調整資訊。這是引用的簽名調整資訊。

選擇自定義簽名

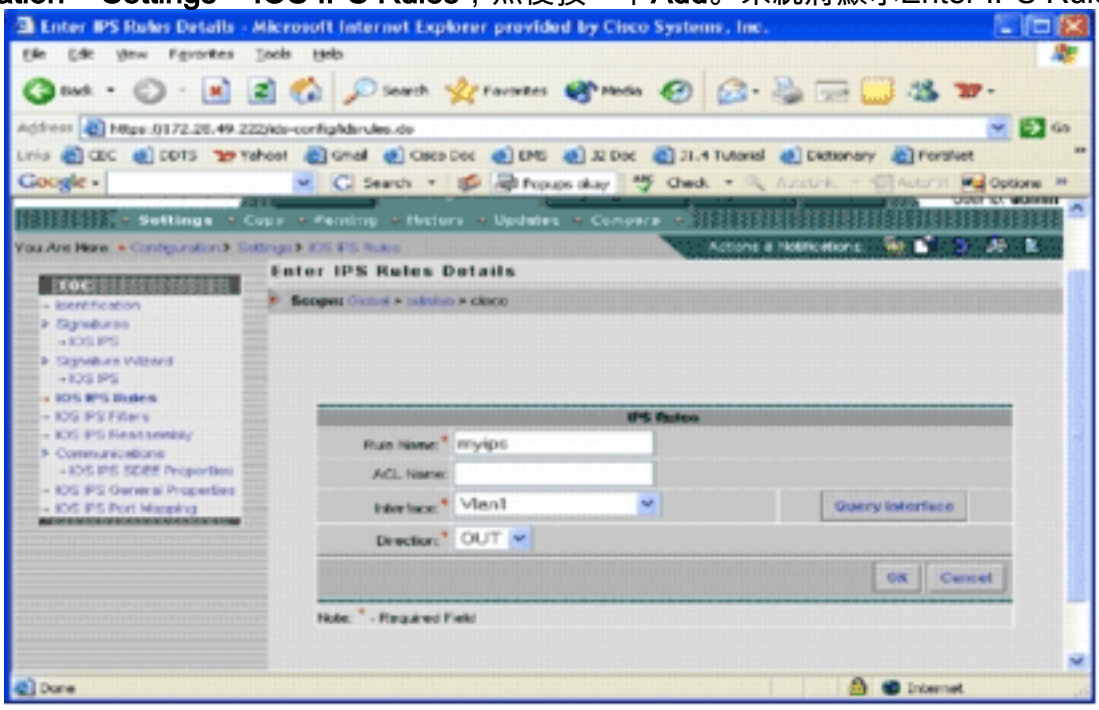
如果您不想使用預設預最佳化SDF檔案，則可以使用修改預最佳化SDF簽名部分中指定的步驟來選

擇裝置的最佳化簽名。在標識頁面中，需要確保SDF型別為UNSET。請參閱將Cisco IOS IPS路由器配置為使用預最佳化的簽名檔案中的步驟3。

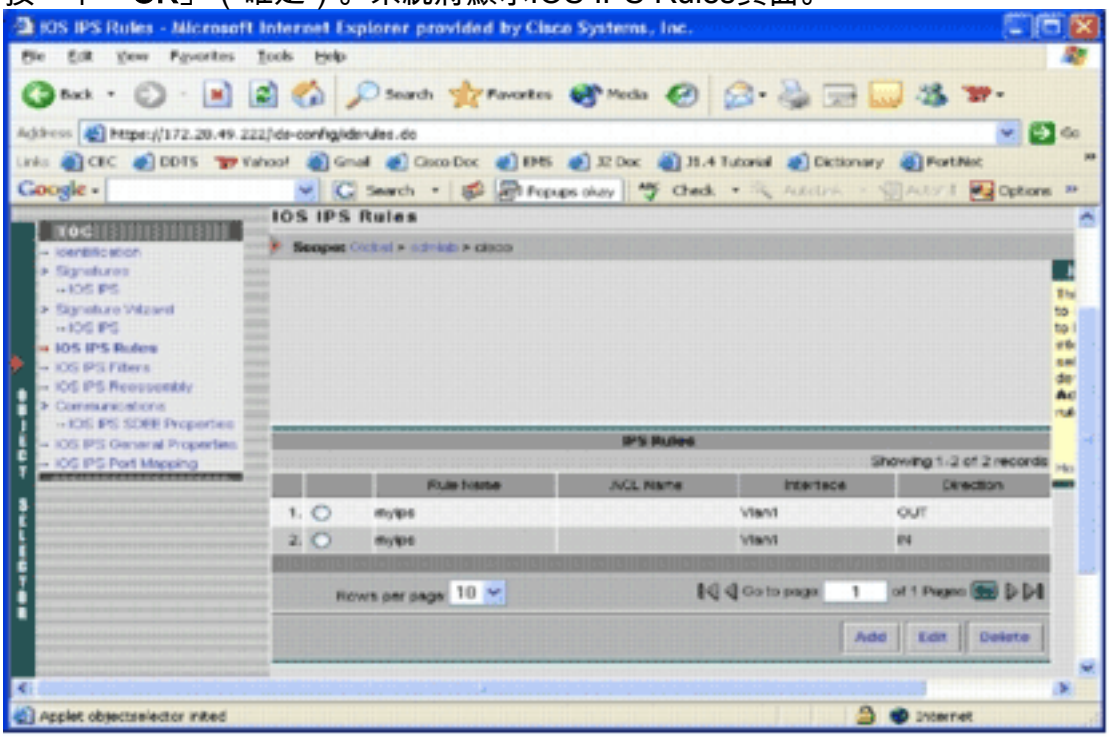
建立應用於介面的規則

調整簽名後，您需要在Cisco IOS路由器上啟用IPS。要在路由器上啟用IPS，必須建立一個IPS規則並將其應用於至少一個介面。

1. 選擇**Configuration**，然後使用對象選擇器選擇要配置的Cisco IOS IPS路由器。在路徑欄中驗證您的作用域位於裝置級別，而不是組級別。
2. 選擇**Configuration > Settings > IOS IPS Rules**，然後按一下**Add**。系統將顯示Enter IPS Rules Details頁面。



3. 輸入要應用規則和方向的規則名稱和介面的資訊。
4. 按一下「**OK**」（確定）。系統將顯示IOS IPS Rules頁面。



同樣，可以為介面的兩個方向建立規則。

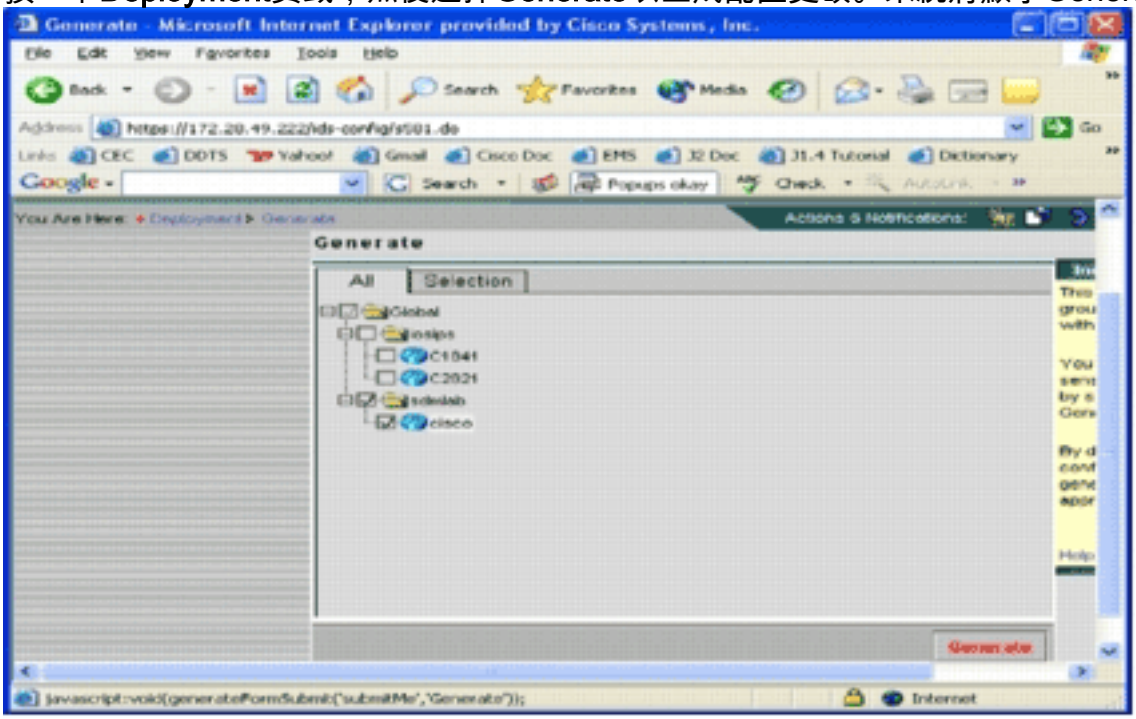
5. 您必須儲存配置更改並完成部署過程，以便將更改傳遞到受影響的裝置或裝置組。您也可以執行其他與IPS相關的配置，但所有其他任務都是可選的，不是必需的。您可以在配置使用者介面左側找到所有選項。本檔案沒有說明可選的組態選項。

部署配置

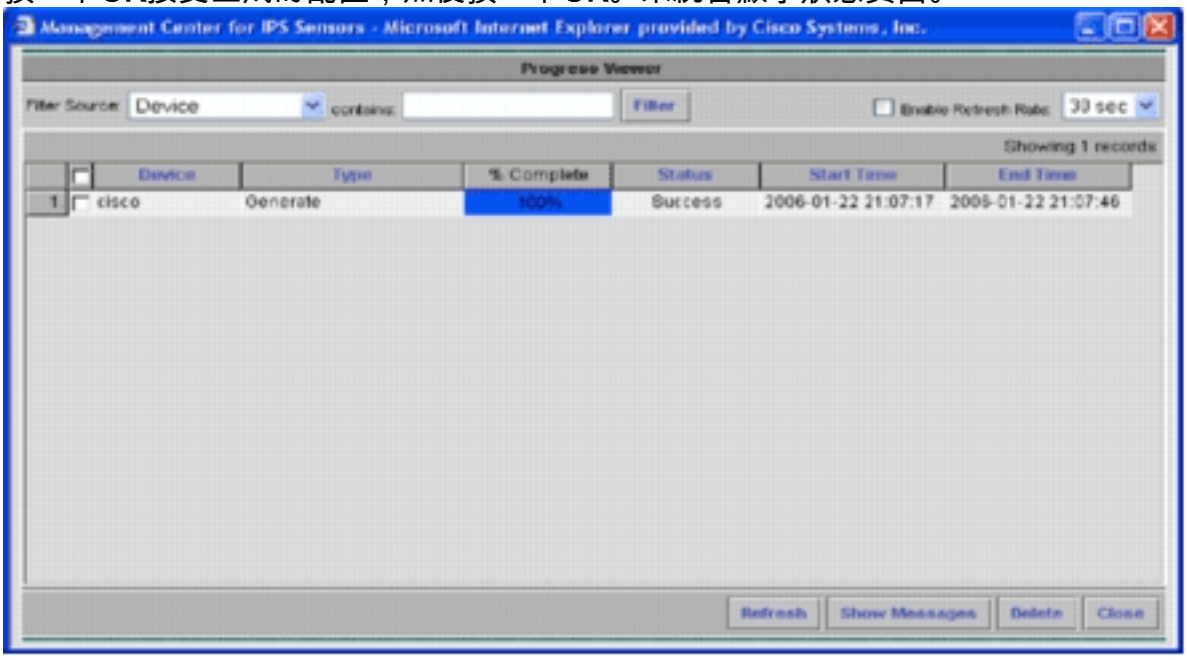
進行所有配置更改後，必須使用部署任務將更改提交到裝置。您到目前為止所做的所有配置都儲存在本地IPS MC伺服器上。

若要部署配置更改，請轉到「部署」頁，然後完成以下步驟：

1. 按一下**Deployment**頁籤，然後選擇**Generate**以生成配置更改。系統將顯示Generate頁面。

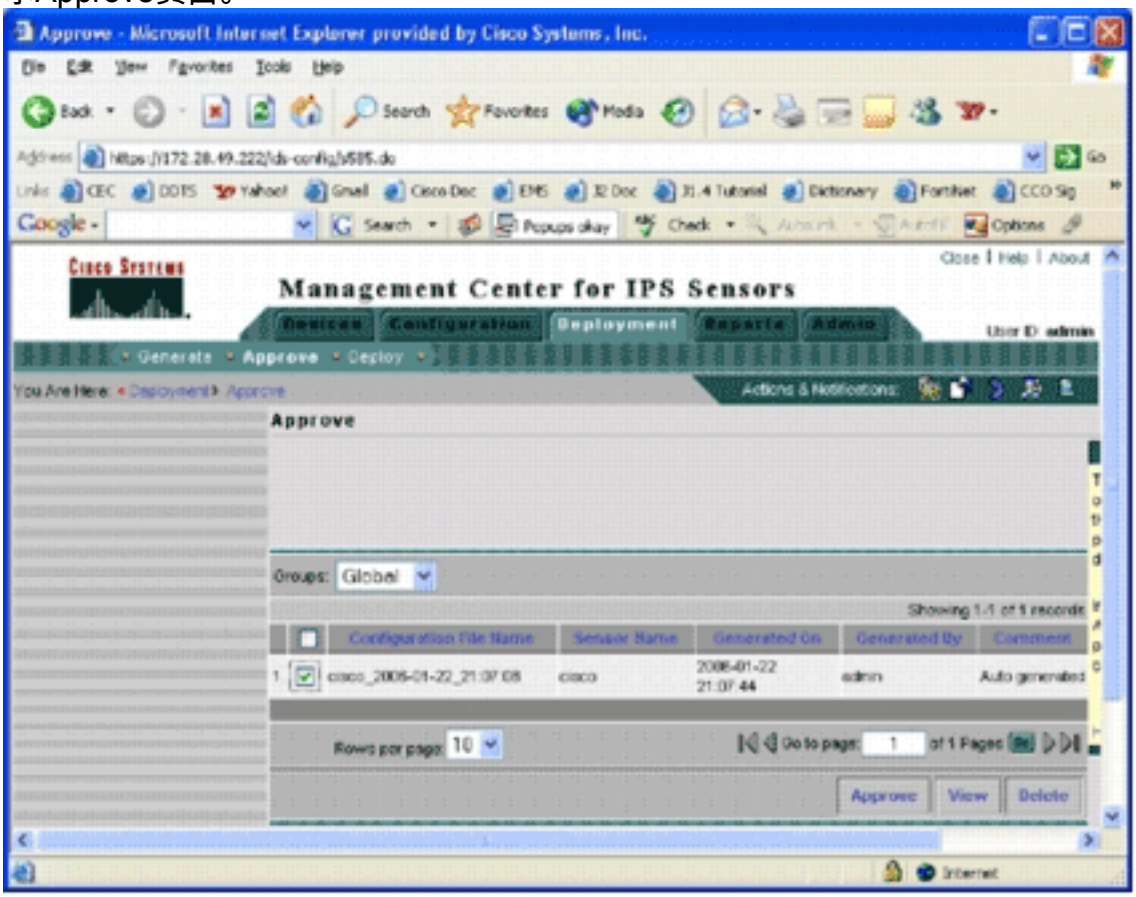


2. 選擇剛配置的*cisco*裝置，然後點選**Generate**。
3. 按一下**OK**接受生成的配置，然後按一下**OK**。系統會顯示狀態頁面。

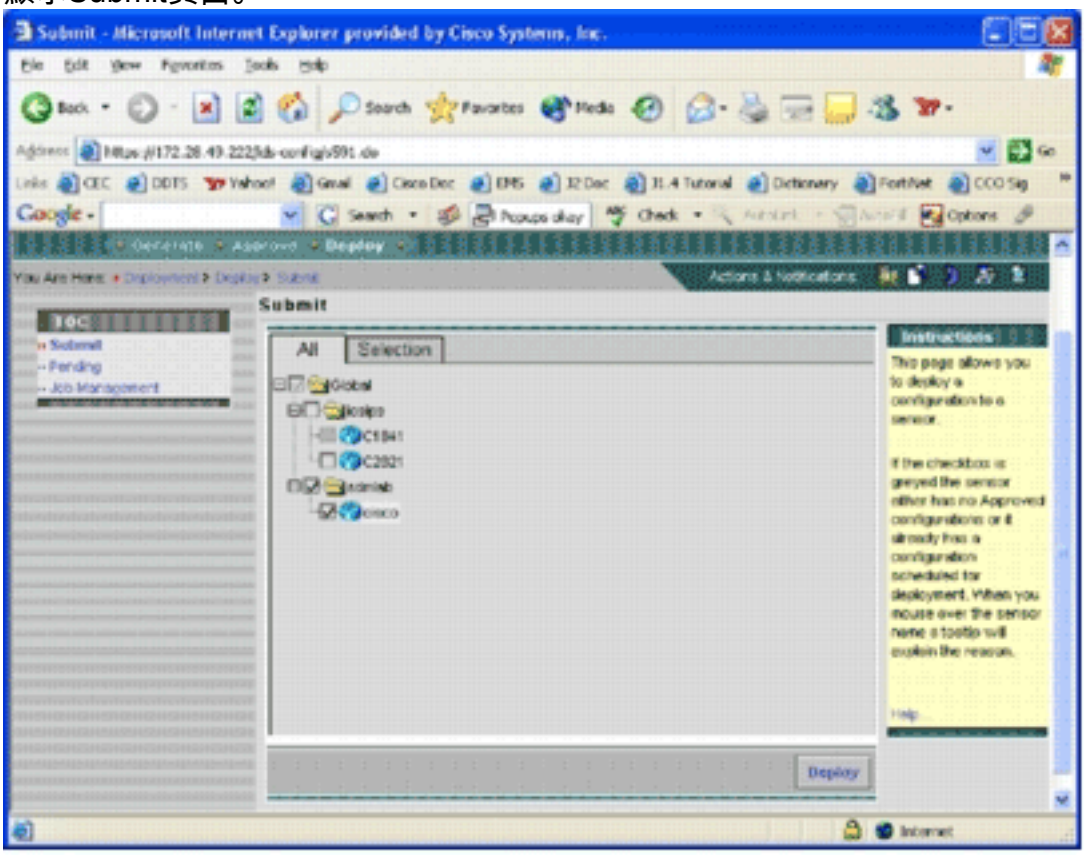


4. 按一下**刷新**，直到生成任務成功完成。
5. 按一下Deployment選單欄和sdmlab組中的**Approve**，以檢視需要審批的配置清單。系統將顯

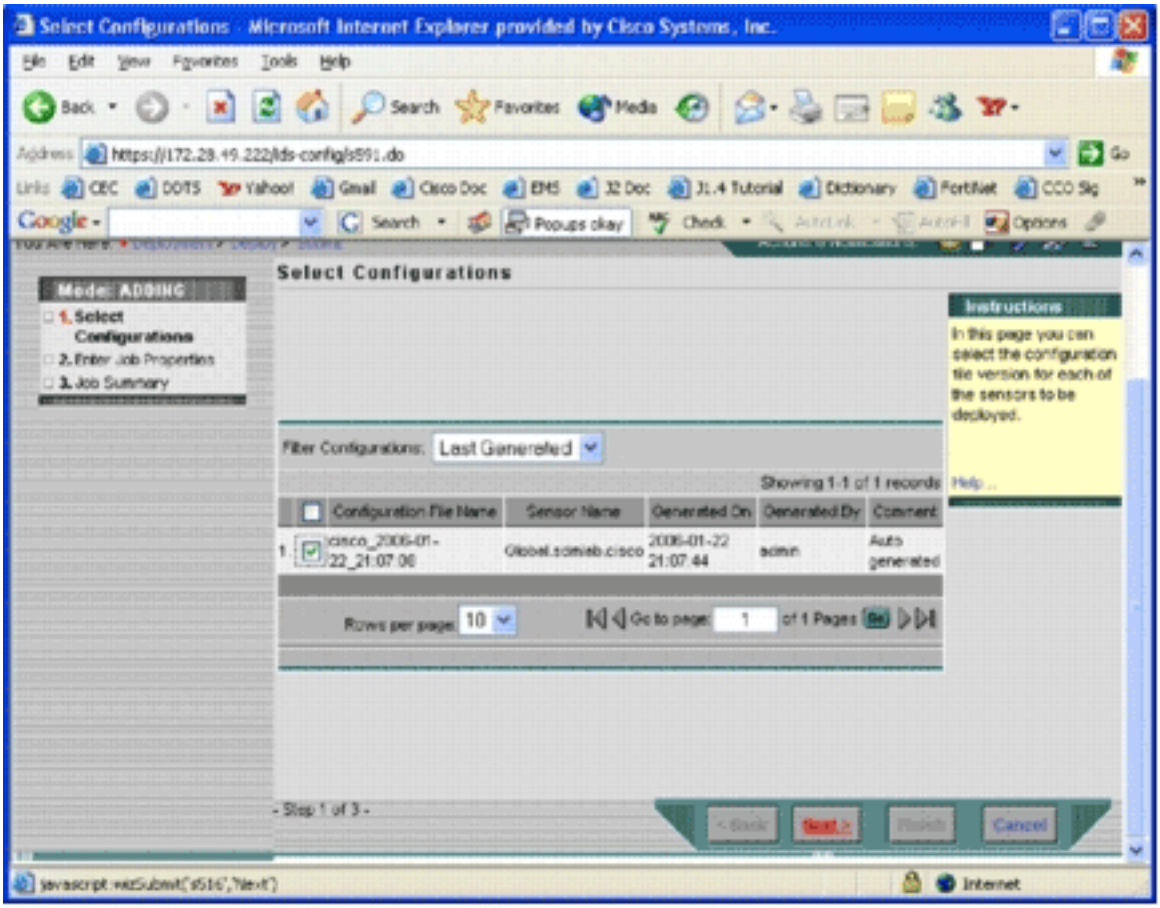
示Approve頁面。



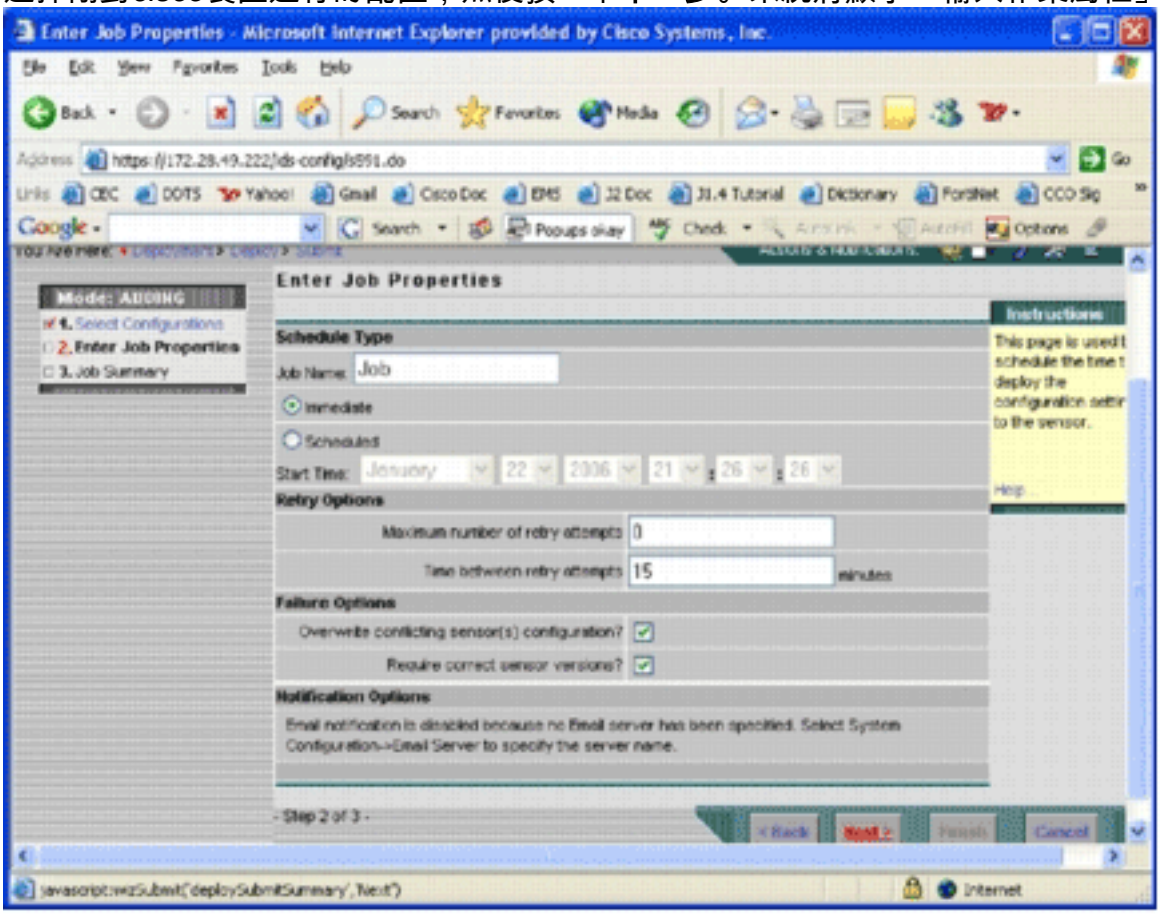
6. 選擇任務，然後按一下**批准**。按一下位於「部署」選單欄中的**部署**，然後按一下**提交**。系統將顯示Submit頁面。



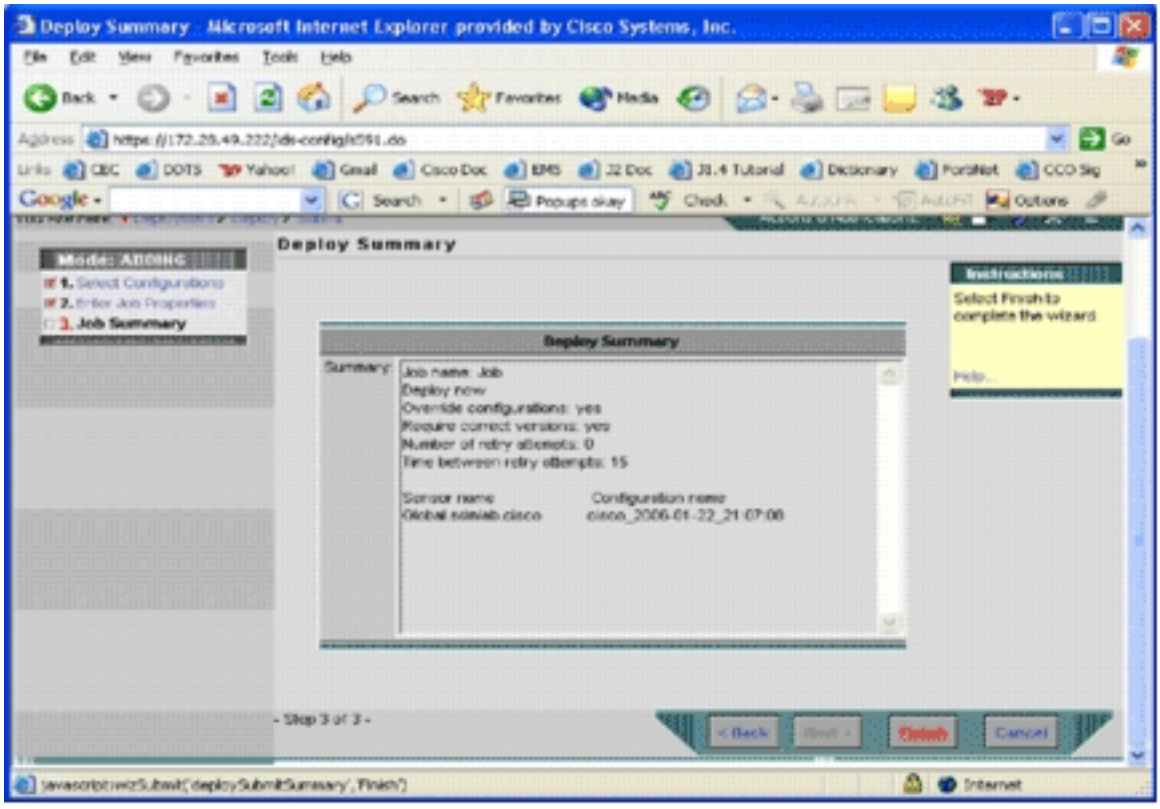
7. 選擇要為其提交部署任務的裝置。
8. 選擇*cisco*裝置，然後按一下**Deploy**。系統將顯示Select Configurations頁面。



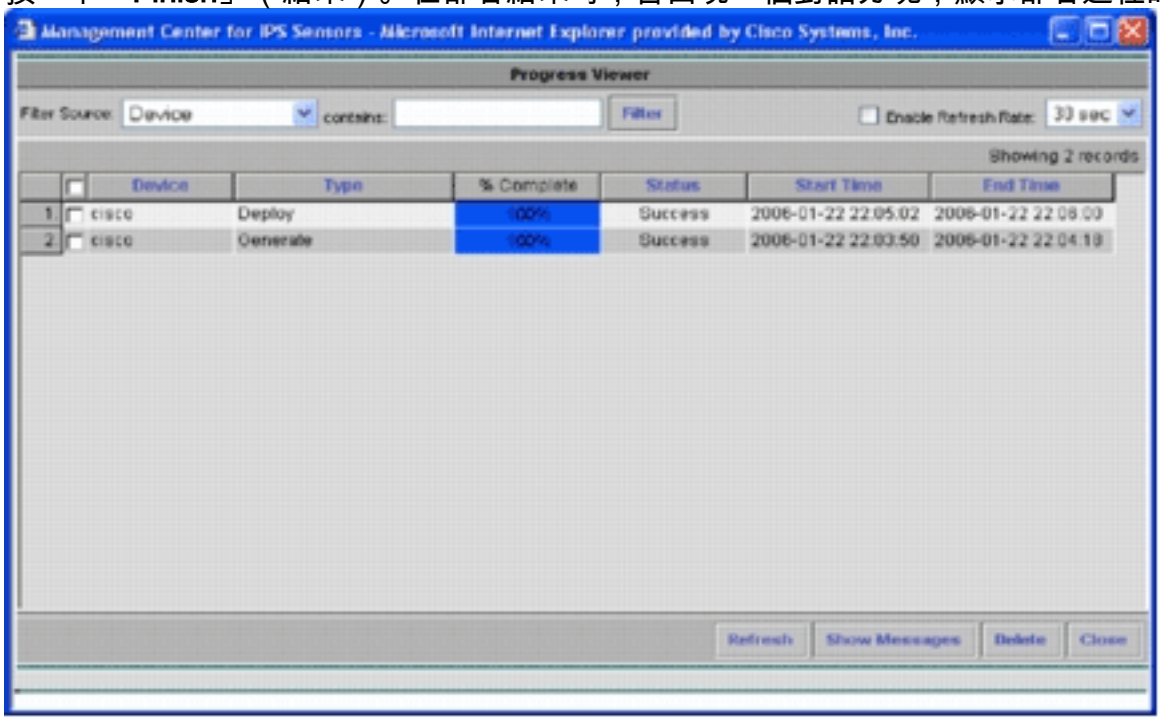
9. 選擇剛對*cisco*裝置進行的配置，然後按一下**下一步**。系統將顯示「輸入作業屬性」頁面。



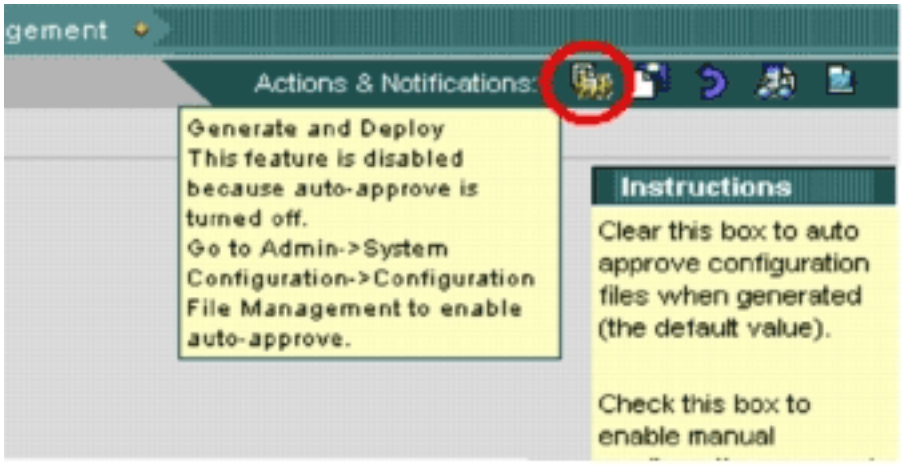
10. 您可以立即部署更改，也可以安排任務在稍後執行。在本例中，選擇**Immediate**選項，然後按一下**Next**。將顯示一個簡要的作業摘要，可供部署。



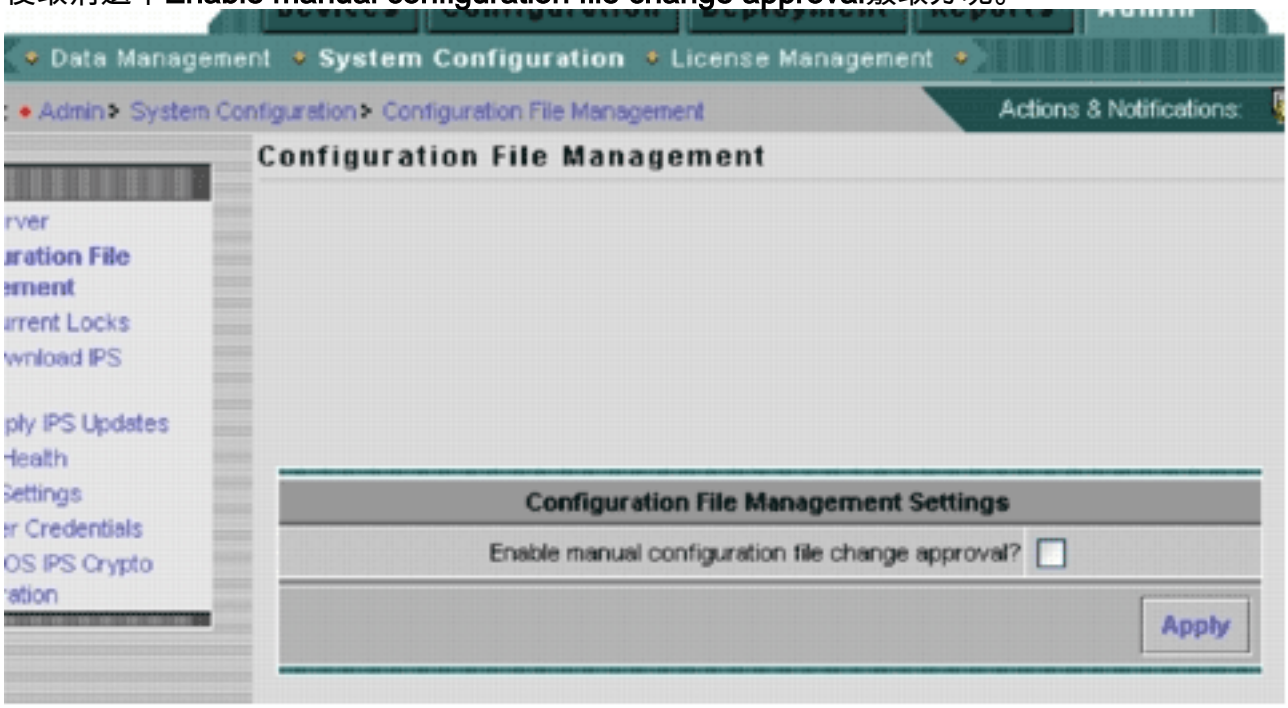
11. 按一下「**Finish**」（結束）。在部署結束時，會出現一個對話方塊，顯示部署進程的狀態。



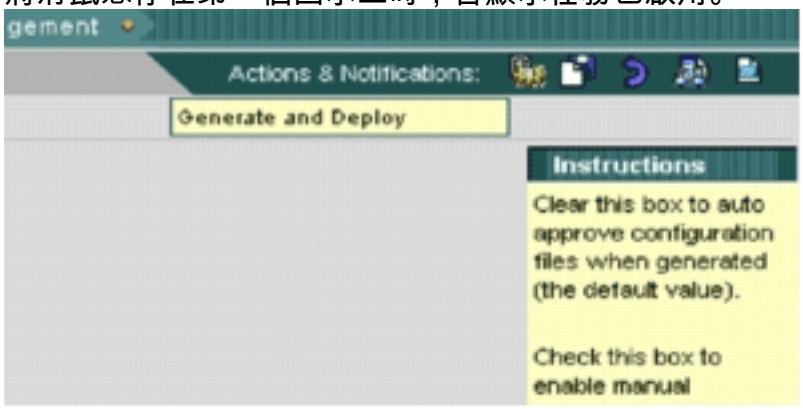
您已成功將Cisco IOS IPS配置部署到裝置。配置多個裝置時，可以在組級別進行配置更改，然後將更改應用到屬於同一組的所有Cisco IOS IPS路由器。**提示：**此過程很長，但提供快速交付功能。使用此功能時，您無需完成**生成>批准>部署**過程。完成以下步驟即可使用該功能：使用者介面頂部是一排小圖示。將滑鼠懸停在第一個圖示上，然後檢視如下圖所示的工具提示



：要啟用Generate and Deploy任務，請轉到**Admin > System Configuration > Configuration File Management**，然後取消選中**Enable manual configuration file change approval**覈取方塊。



將滑鼠懸停在第一個圖示上時，會顯示任務已啟用。

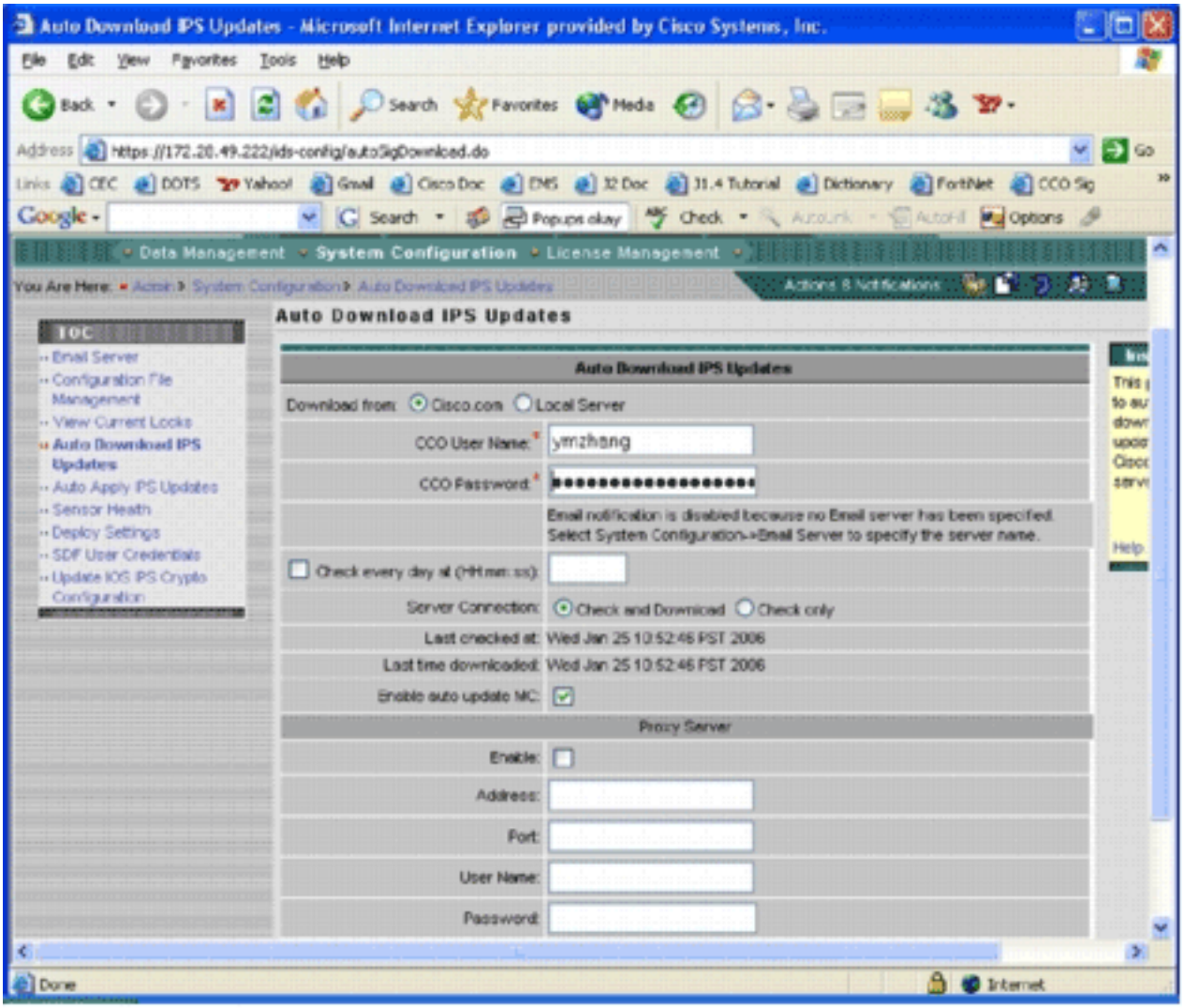


按一下此圖示。IPS MC會自動生成配置更改並將其部署到裝置。

自動下載特徵碼更新

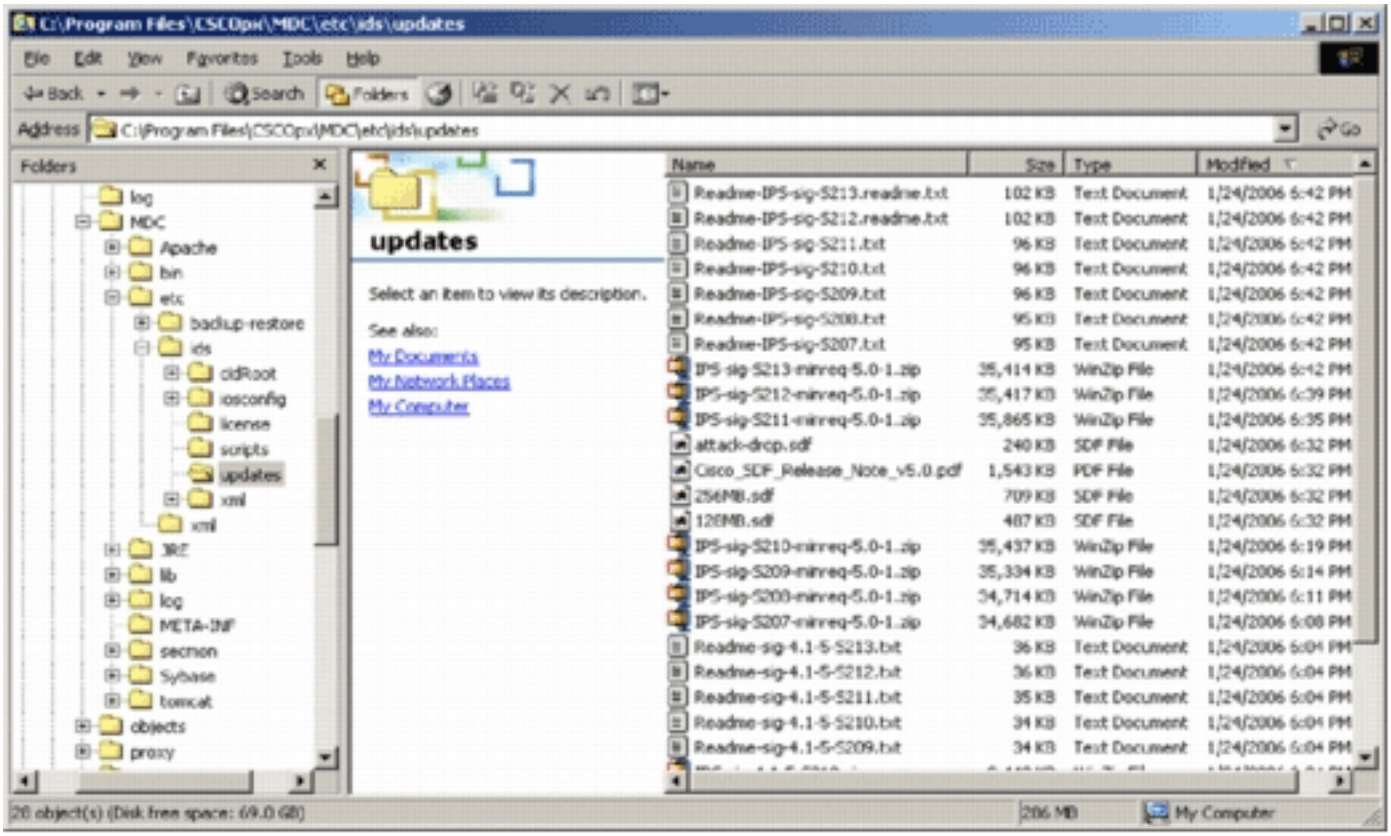
IPS MC支援從Cisco.com自動下載特徵碼更新。它可以下載感測器平台以及Cisco IOS IPS平台的特徵碼更新。要配置此功能，請轉到**Admin > System Configuration > Auto Download IPS Updates**。

系統將顯示Auto Download IPS Update頁面。



您必須擁有有效的Cisco.com帳戶才能下載此簽名更新。要檢查自動下載的檔案，請轉到IPS MC安裝主目錄。預設情況下為\program files\CSCOpx\MDC\etc\ids\updates。

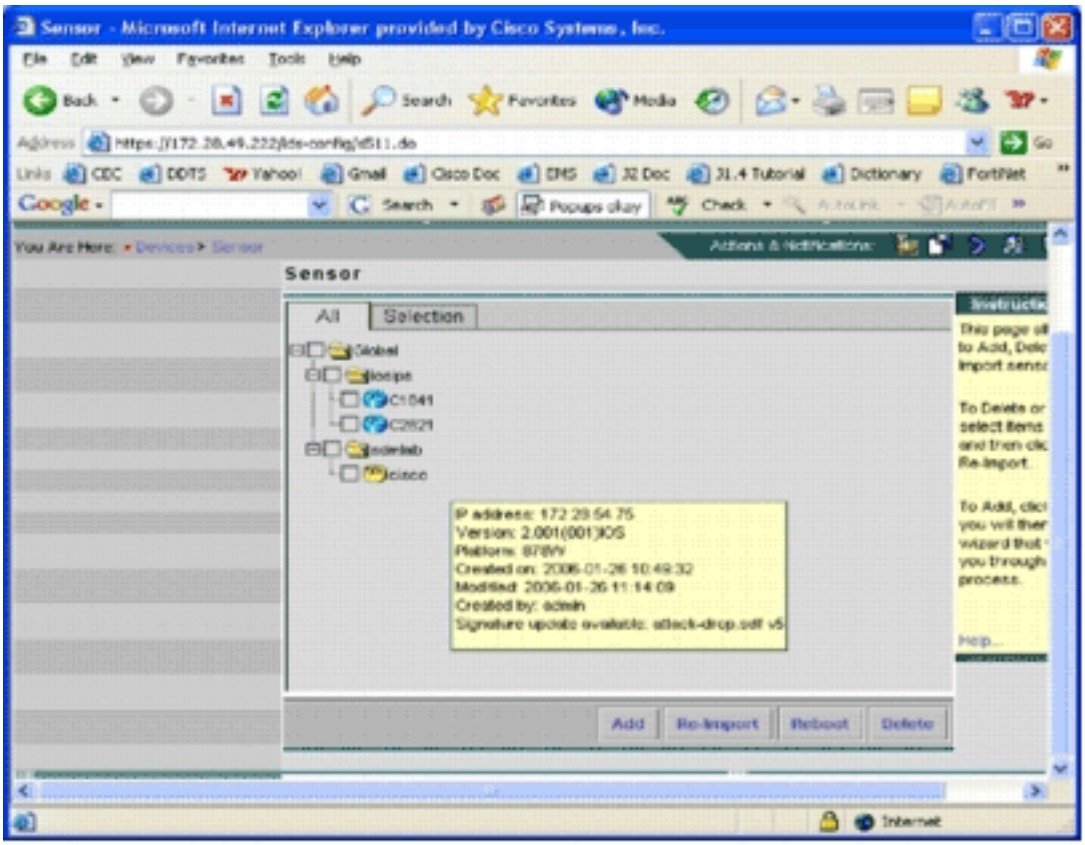
此圖顯示此目錄中下載的檔案的影象。



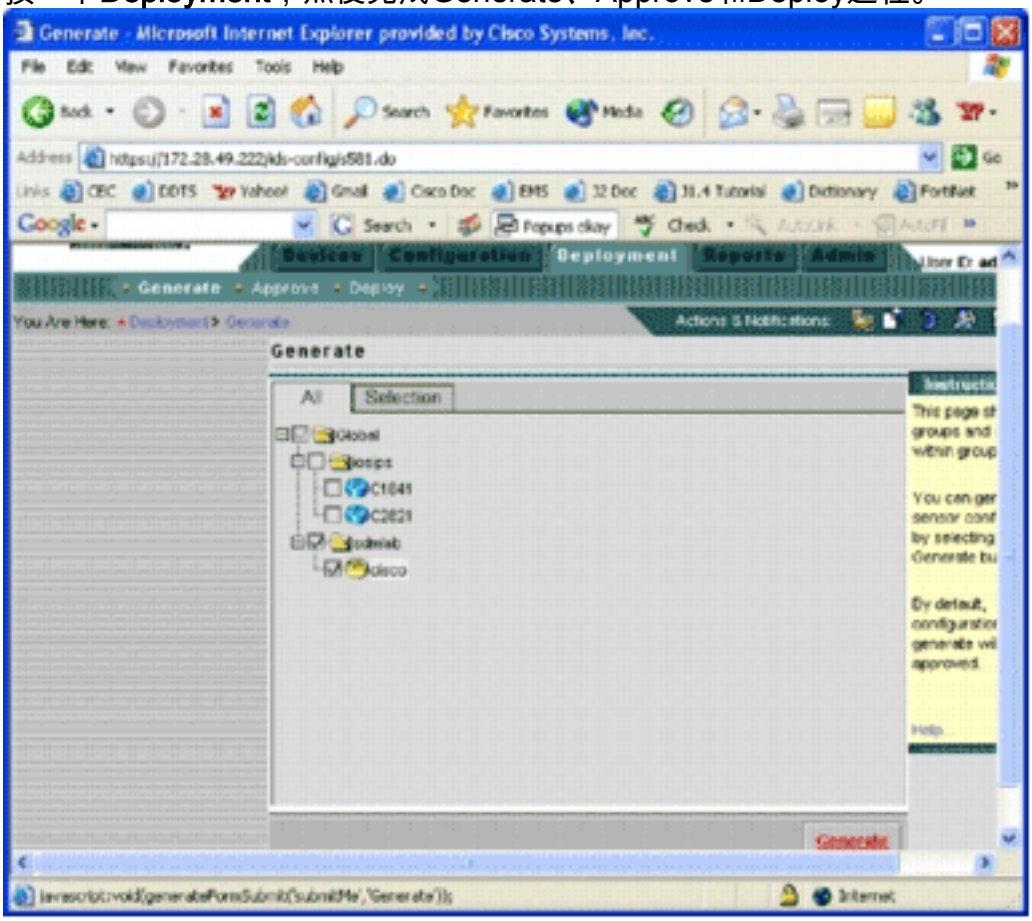
可以看到感測器更新檔案。會下載Cisco IOS軟體更新檔案和預調整的SDF檔案。

使用新的SDF檔案更新Cisco IOS IPS路由器

對於部署了預調SDF檔案的Cisco IOS IPS路由器，只要可以通過自動下載獲得新版本的SDF檔案或將其複製到更新目錄，Cisco IPS MC即可識別新版本。使用者介面刷新後，適用裝置的裝置圖示變為黃色。



1. 按一下**Deployment**，然後完成Generate、Approve和Deploy過程。



2. 成功部署後，Cisco IOS IPS路由器使用新版本的SDF檔案。

相關資訊

- 思科入侵防禦系統