Esempio di configurazione di Cisco IOS IPS MC

Sommario

Introduzione

CiscoWorks Management Center for IPS Sensors (IPS MC) è la console di gestione per i dispositivi IPS Cisco. IPS MC versione 2.2 supporta il provisioning della funzionalità IPS (Intrusion Prevention System) sui router software Cisco IOS®. In questo documento viene descritto come utilizzare IPS MC 2.2 per configurare IPS Cisco IOS.

Per ulteriori informazioni su come utilizzare IPS MC (incluse le istruzioni per la configurazione di dispositivi non basati su software Cisco IOS), consultare la documentazione di CiscoWorks Management Center for IPS Sensors al seguente URL:

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

Prerequisiti

Requisiti

Nessun requisito specifico previsto per questo documento.

Componenti usati

Per la stesura del documento, è stato usato CiscoWorks Management Center for IPS Sensors (IPS MC) versione 2.2.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

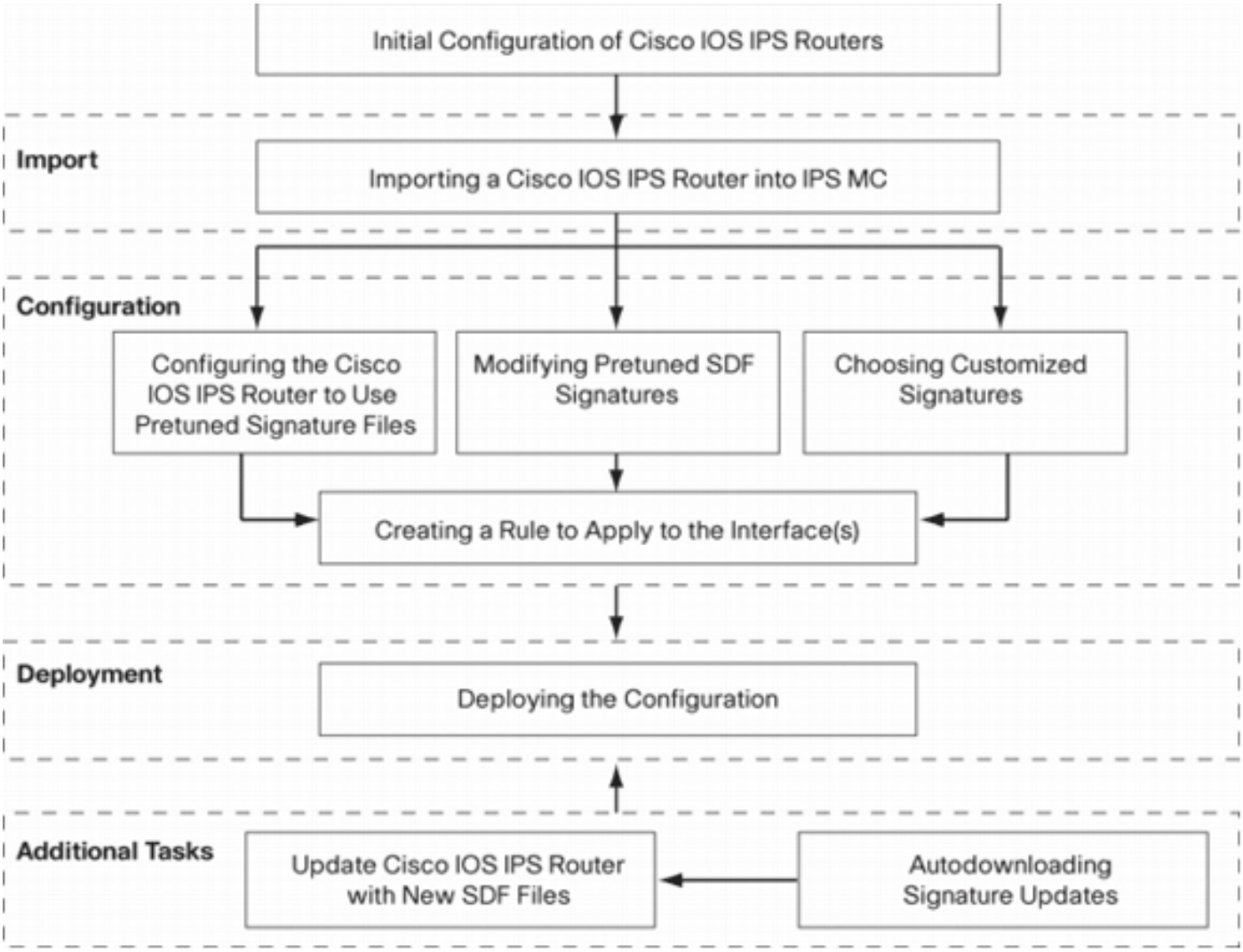
Convenzioni

Fare riferimento a Cisco Technical Tips Conventions per ulteriori informazioni sulle convenzioni dei documenti.

Configurazione

Informazioni di base sui task di configurazione

IPS MC viene utilizzato per gestire la configurazione di un gruppo di router IPS Cisco IOS. Si noti che IPS MC non gestisce gli avvisi provenienti dai router che eseguono IPS. Cisco consiglia Cisco Security Monitoring, Analysis and Response System (Cisco Security MARS) per il monitoraggio IPS. La gestione della configurazione è costituita da una serie di attività descritte in questo documento. Queste attività possono essere suddivise in tre fasi: importazione, configurazione e distribuzione come illustrato in questa immagine.



Ciascuna fase ha le proprie responsabilità e funzioni:

- *Importa*: importa un router in IPS MC. È necessario importare un router in IPS MC prima di poterlo utilizzare per configurarlo. Non è possibile importare un router a meno che non esista una configurazione IPS iniziale sul router (i dettagli sono illustrati più avanti in questo documento).
- *Configurazione (Configuration*) - Consente di configurare il dispositivo. Ad esempio, è possibile configurare un router Cisco IOS IPS in modo che utilizzi uno dei file di firma pretuned consigliati da Cisco. Le modifiche alla configurazione vengono archiviate in IPS MC, ma non inviate al router in questa fase.
- *Distribuzione*: consente di apportare modifiche alla configurazione del dispositivo effettivo. Durante questa fase, i router ricevono le modifiche apportate durante le attività di configurazione.
- *Attività aggiuntive*: IPS MC fornisce una funzione di download automatico per scaricare automaticamente gli aggiornamenti delle firme da Cisco.com.

Per utilizzare in modo efficace IPS MC, è necessario comprendere questo approccio in più fasi. È diversa dalle interfacce grafiche di gestione basate sui dispositivi, come Cisco Router e Security Device Manager (SDM). Le interfacce grafiche basate sui dispositivi agiscono direttamente su un singolo router, mentre IPS MC è progettato per funzionare su gruppi di router (e altri dispositivi IPS come i sensori Cisco IPS serie 4200) in tutta la rete.

In questo documento vengono fornite informazioni su ciascuna delle attività incluse nel diagramma che consentono di utilizzare MC IPS per gestire i router IPS di Cisco IOS.

Configurazione iniziale dei router IPS Cisco IOS

Per importare o aggiungere correttamente un router IPS Cisco IOS al MC IPS, è necessario eseguire alcune operazioni di configurazione iniziale sui router IPS Cisco IOS. In questa sezione vengono descritti i passaggi.

Ènecessario abilitare il protocollo SSH (Secure Shell) in un router Cisco IOS IPS per la configurazione, l'importazione e la distribuzione tramite Cisco IPS MC. È inoltre necessario attivare il protocollo SDEE (Security Device Event Exchange) per la creazione di report sugli eventi, sebbene questi avvisi non vengano inviati a IPS MC perché IPS MC viene utilizzato solo per il provisioning, non per la creazione di report. Infine, è necessario verificare che l'impostazione dell'orologio sul router IPS sia sincronizzata con il MC IPS.

Per configurare i router IPS per IOS, completare la procedura seguente:

1. Creare un nome utente e una password locali per il router.
   ```
   Router#config terminal
   Router(config)#username <username> password <password>
   ```

2. Abilitare l'accesso locale all'interfaccia delle linee vty.
   ```
   Router#config terminal
   Router(config)#line vty 0 15
   Router(config-line)#login local
   Router(config-line)#exit
   ```

   Se l'interfaccia della riga di comando (CLI) di input o output del trasporto è configurata in configurazione riga vty, verificare che SSH sia abilitato. Ad esempio:
   ```
   Router#conf terminal
   Router(config)#line vty 0 15
   Router(config-line)#transport input ssh telnet
   Router(config-line)#exit
   ```

3. Generare una chiave RSA a 1024 bit (se non esiste già una chiave).SSH viene abilitato automaticamente dopo la generazione della chiave di crittografia.
   ```
   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. Abilitare SDEE sul router.
   ```
   Router(config)#ip ips notify sdee
   ```

5. Abilita HTTPS.Per la comunicazione tra IPS MC e il router con SDEE per la raccolta delle informazioni sugli eventi, è necessario il protocollo HTTP o HTTPS.
   ```
   Router(config)#ip http authentication local
   Router(config)#ip http secure-server
   ```

6. Usare il server Network Time Protocol (NTP) esterno o il comando clock per configurare

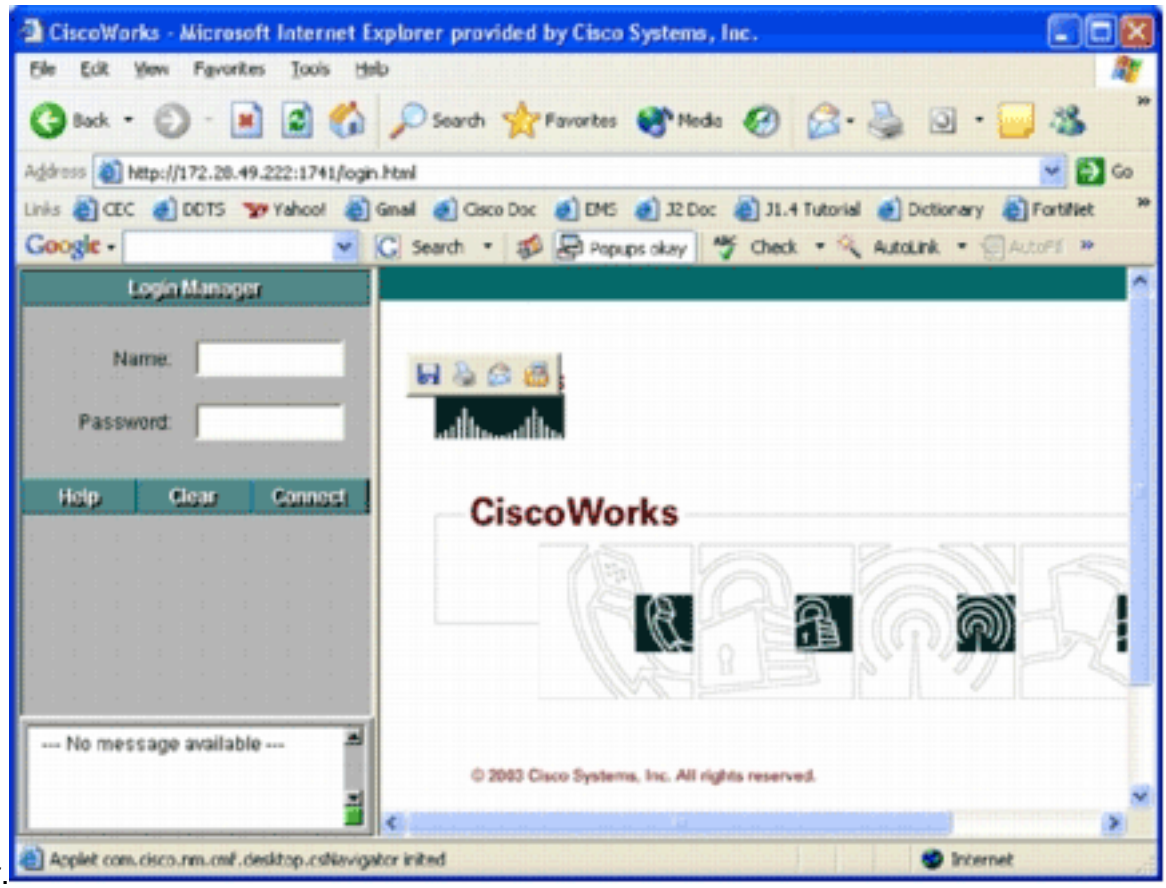
l'impostazione dell'orologio sul router IPS.

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

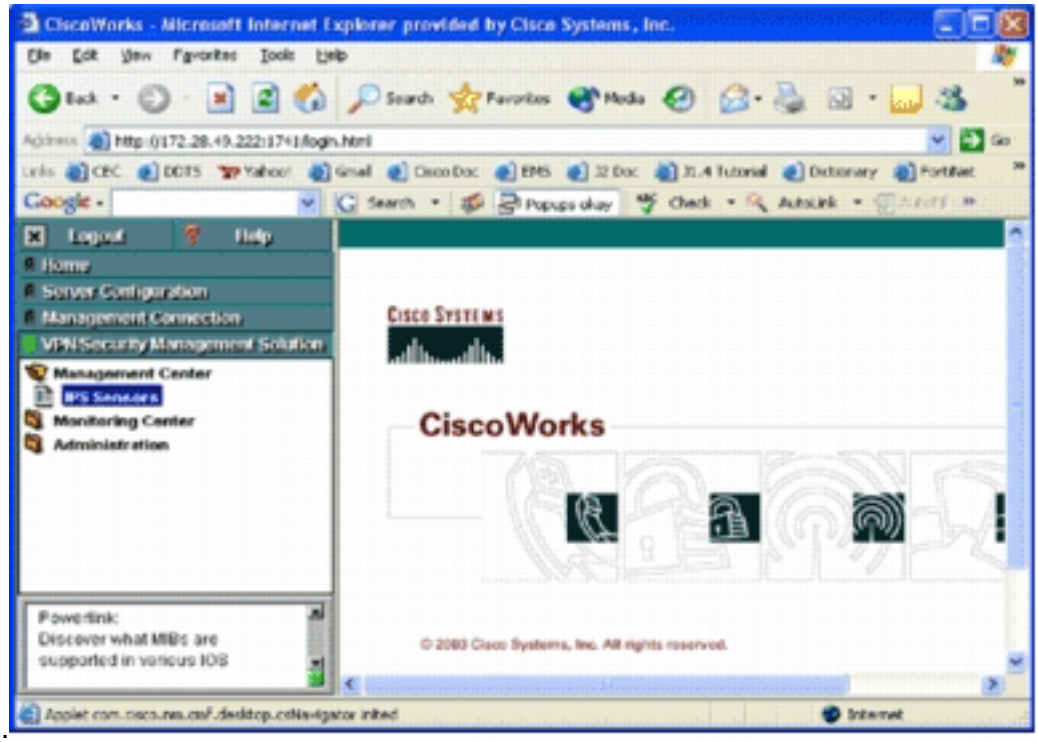
A questo punto, il router IPS Cisco IOS è pronto e può essere importato in IPS MC per un'ulteriore configurazione e gestione.

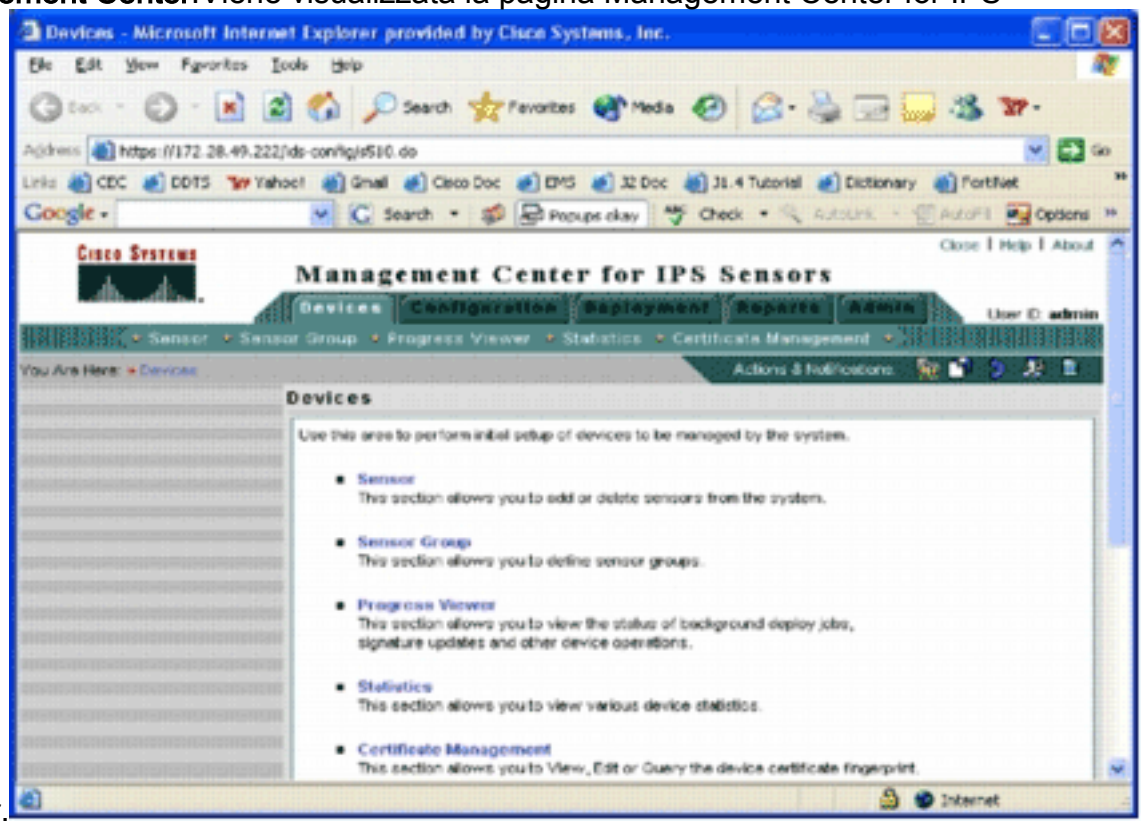
Importazione di un router IPS Cisco IOS in IPS MC

Dopo aver completato la configurazione iniziale sul router, è possibile aggiungerla (o importarla) in IPS MC.

1. Avviare il browser Web e scegliere il server CiscoWorks.Viene visualizzato CiscoWorks Login Manager. 

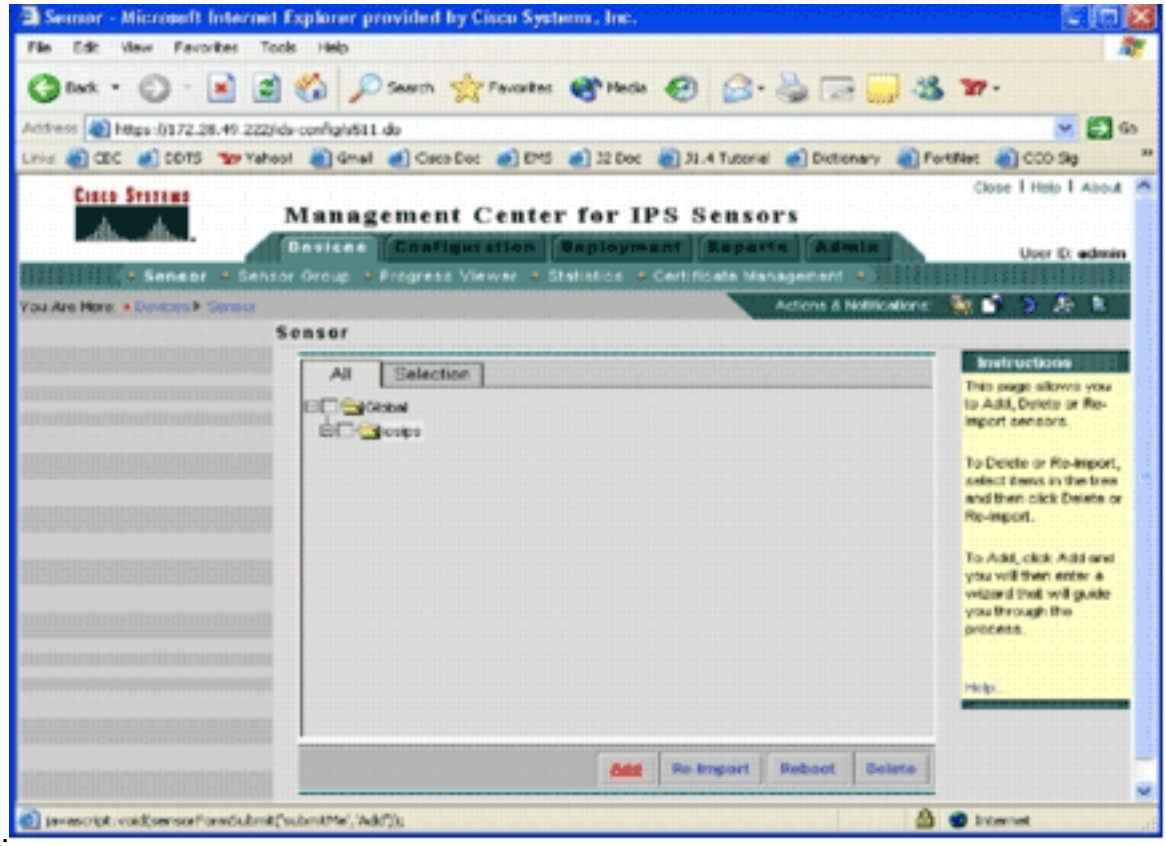
Nota: il numero di porta predefinito del server Web è 1741. pertanto, è consigliabile utilizzare un URL simile a http://<*indirizzo ip server*>:1741/.
2. Immettere il nome utente e la password per accedere.Viene visualizzata la pagina principale

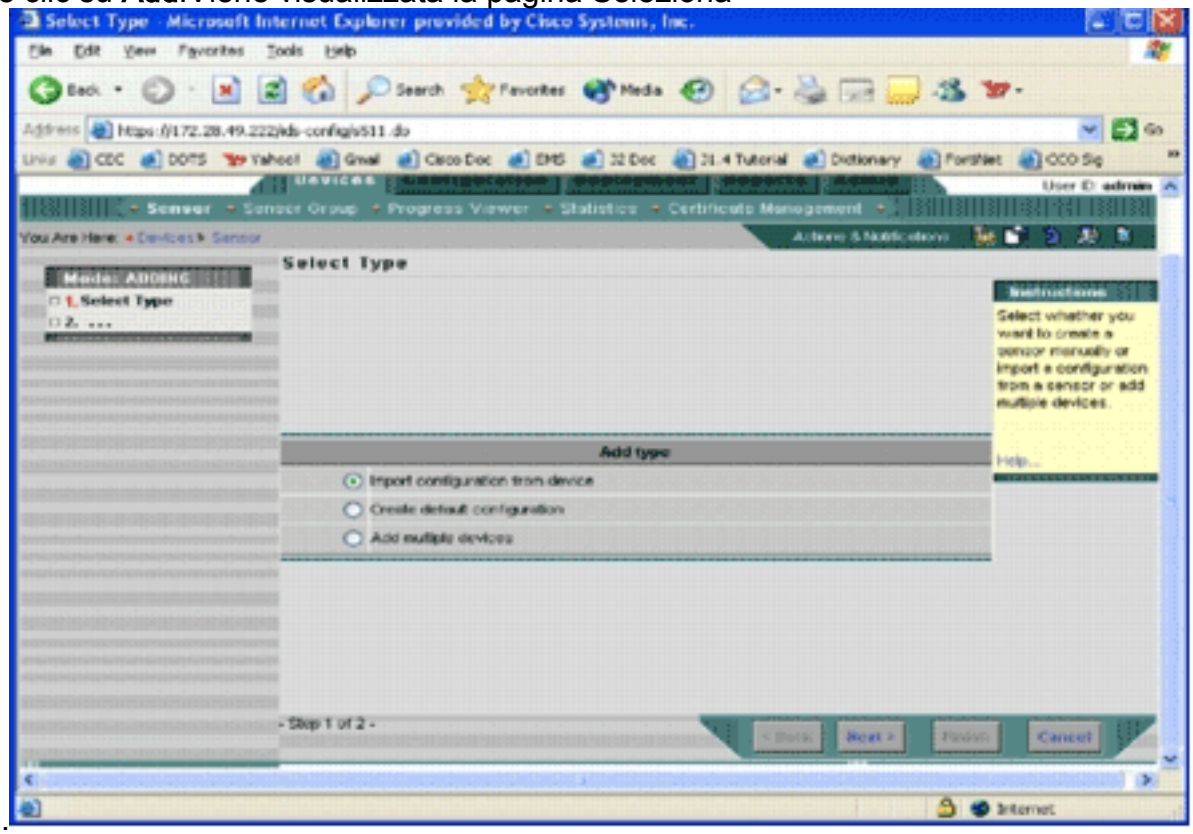
di CiscoWorks. 

3. Nel riquadro di navigazione a sinistra, scegliere **VPN/Security Management Solution**, quindi **Management Center**.Viene visualizzata la pagina Management Center for IPS Sensor. 

In questa pagina vengono visualizzate le cinque schede seguenti:*Dispositivi*: nella scheda Dispositivi è possibile eseguire la configurazione iniziale di tutti i dispositivi del sistema e gestirli.*Configurazione*: nella scheda Configurazione è possibile eseguire le funzioni di provisioning. È possibile configurare i dispositivi a livello di singolo dispositivo o di gruppo. Un gruppo di dispositivi può contenere più dispositivi. Tutte le modifiche apportate tramite le attività di configurazione devono essere salvate. La funzione di configurazione non apporta modifiche immediate ai dispositivi. Per distribuire le modifiche, è necessario utilizzare la funzione di distribuzione.*Distribuzione*: nella scheda Distribuzione è possibile distribuire le modifiche della configurazione ai dispositivi. La funzionalità di pianificazione consente un

controllo flessibile del momento in cui le modifiche alla configurazione devono avere effetto.*Report*: nella scheda Report è possibile generare vari report sul funzionamento del sistema.*Amministrazione*: nella scheda Amministrazione è possibile eseguire attività di amministrazione del sistema, ad esempio la gestione del database, la configurazione del sistema e la gestione delle licenze.

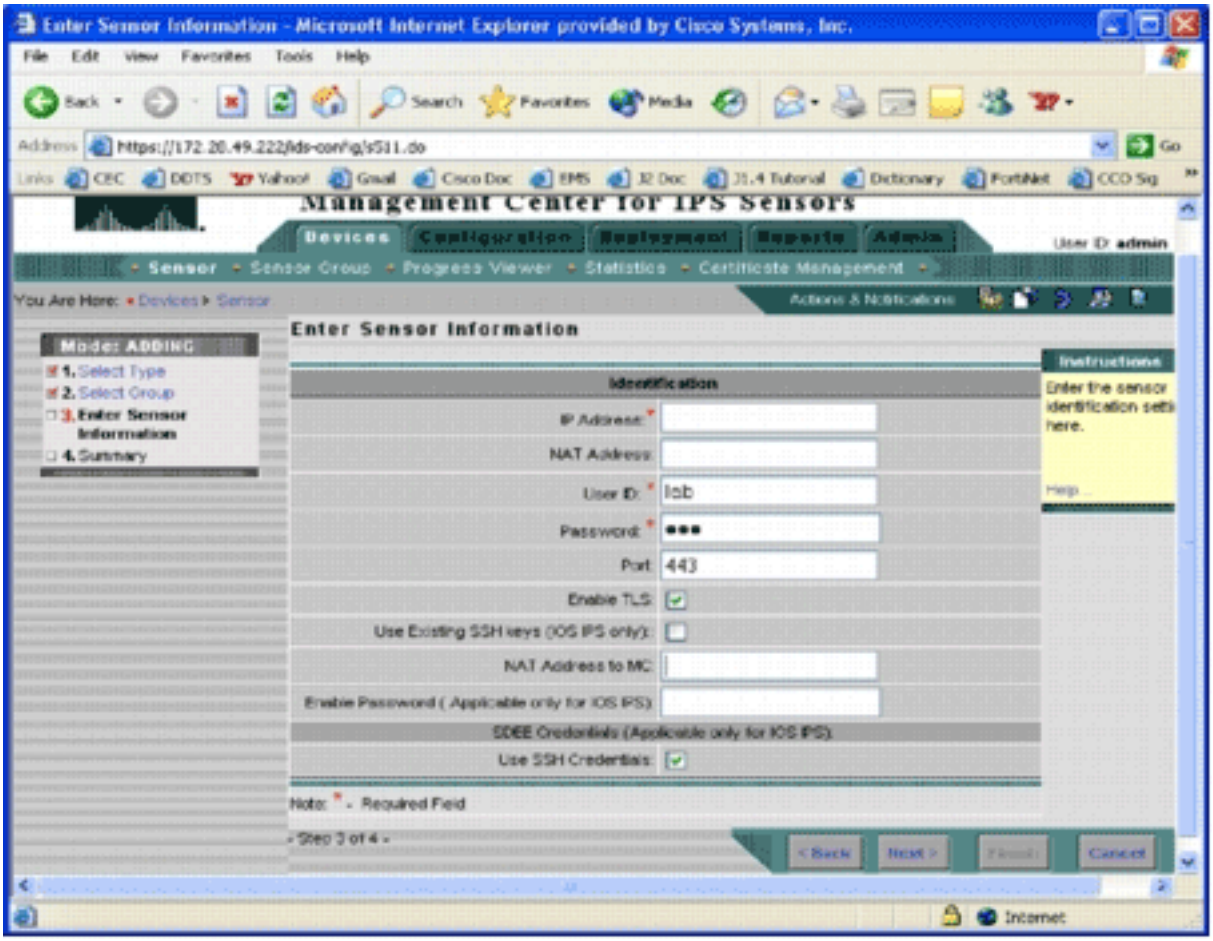
4. Per aggiungere una nuova periferica, fare clic sulla scheda **Periferiche**.Viene visualizzata la pagina 

Sensore.
5. Fare clic su **Add**.Viene visualizzata la pagina Seleziona 

tipo.Ènec

essario indicare a IPS MC il tipo di funzione di aggiunta che si desidera eseguire. Nell'elenco seguente vengono descritte le opzioni disponibili:*Importa configurazione da dispositivo*: utilizzare questa opzione per aggiungere dispositivi MC IPS attualmente in esecuzione in rete.*Crea configurazione predefinita (Create default configuration*) - Utilizzate questa opzione per aggiungere dispositivi che non sono ancora in esecuzione sulla rete.*Aggiungi più dispositivi (Add multiple devices*) - Utilizzate questa opzione per aggiungere più dispositivi. È possibile creare un file con estensione csv o xml contenente tutte le informazioni sui dispositivi e quindi importarlo in IPS MC per aggiungere i dispositivi contemporaneamente.**Suggerimento:** i file di esempio in formato .csv e .xml si trovano in: InstallDirectory\MDC\etc\ids\ e sono denominati, rispettivamente, MultipleAddDevices-format.csv e MultipleAddDevices-format.xml.

6. Selezionate l'opzione appropriata per l'aggiunta del testo e fate clic su **Avanti** (**Next**).
7. Selezionare il gruppo a cui si desidera aggiungere il router Cisco IOS IPS o utilizzare il gruppo globale predefinito e quindi fare clic su **Avanti**.Viene visualizzata la pagina Invio delle informazioni sul
sensore.



8. Nella pagina Identificazione, immettere le informazioni di identificazione per il dispositivo.**Nota:** se l'utente non dispone di diritti di accesso con livello di privilegio 15, è necessario fornire la password enable. Nell'ultima riga della pagina Identificazione, selezionare la casella di controllo **Usa credenziali SSH**.
9. Fare clic su **Next** (Avanti).Viene visualizzato Add Sensor Summary.
10. Fare clic su **Finish** (Fine).Aggiunta del dispositivo al MC IPS completata.**Nota:** se si verificano errori durante il processo di importazione, verificare quanto segue:*Configurazione prerequisiti*: queste configurazioni sono necessarie per consentire la comunicazione tra IPS MC e router IPS Cisco IOS.*Connettività*: verificare che IPS MC possa raggiungere i router IPS di Cisco IOS.*Orologio*: verificare gli orari sul MC IPS e sul router IPS Cisco IOS. L'ora è

un componente critico del certificato https utilizzato per l'autenticazione. Gli orari devono essere compresi tra 12 ore. È consigliabile utilizzare un massimo di poche ore.*Certificato IPS Cisco IOS*: a volte il certificato IPS Cisco IOS memorizzato non è corretto. Per eliminare un certificato da IPS Cisco IOS, è necessario rimuovere il trust point dal router IPS Cisco IOS.*Configurazione aggiuntiva*: se **ip http timeout-policy** è configurato con un numero basso di richieste massime, ad esempio **ip http timeout-policy inattivo 600 life 86400 request 1**, è necessario aumentare il numero massimo di richieste. Ad esempio: **ip http timeout-policy idle 600 life 86400 richieste 8400**

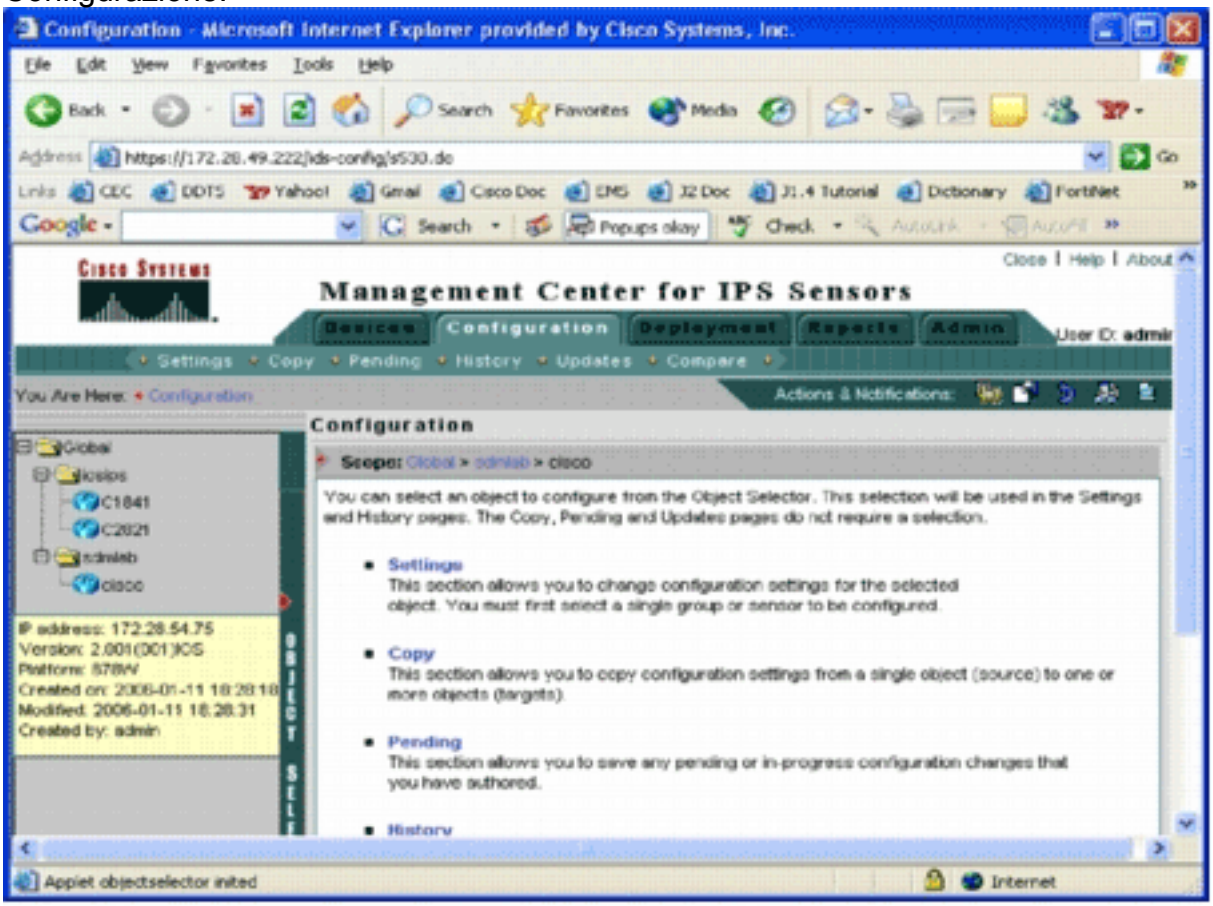
Configurazione del router IPS Cisco IOS per l'utilizzo dei file delle firme ritirate

Dopo aver importato il router in IPS MC, è necessario selezionare il file di definizione della firma (SDF, Signature Definition File) (un file di testo che include le firme di minaccia che verranno utilizzate dal router IPS) e l'azione da eseguire quando viene attivata ogni firma (ad esempio, drop, reimpostazione TCP, allarme).

Cisco Systems® consiglia di utilizzare i file SDF premessi da Cisco. Attualmente esistono tre file di questo tipo: attack-drop.sdf, 128 MB.sdf e 256 MB.sdf. IPS MC può scaricare automaticamente questi file da Cisco.com. Per ulteriori informazioni, vedere Download automatico degli aggiornamenti delle firme.

Questa procedura utilizza un singolo dispositivo come esempio e inizia con un router senza configurazione IPS. Questa procedura può essere utilizzata anche per più dispositivi a livello di gruppo.

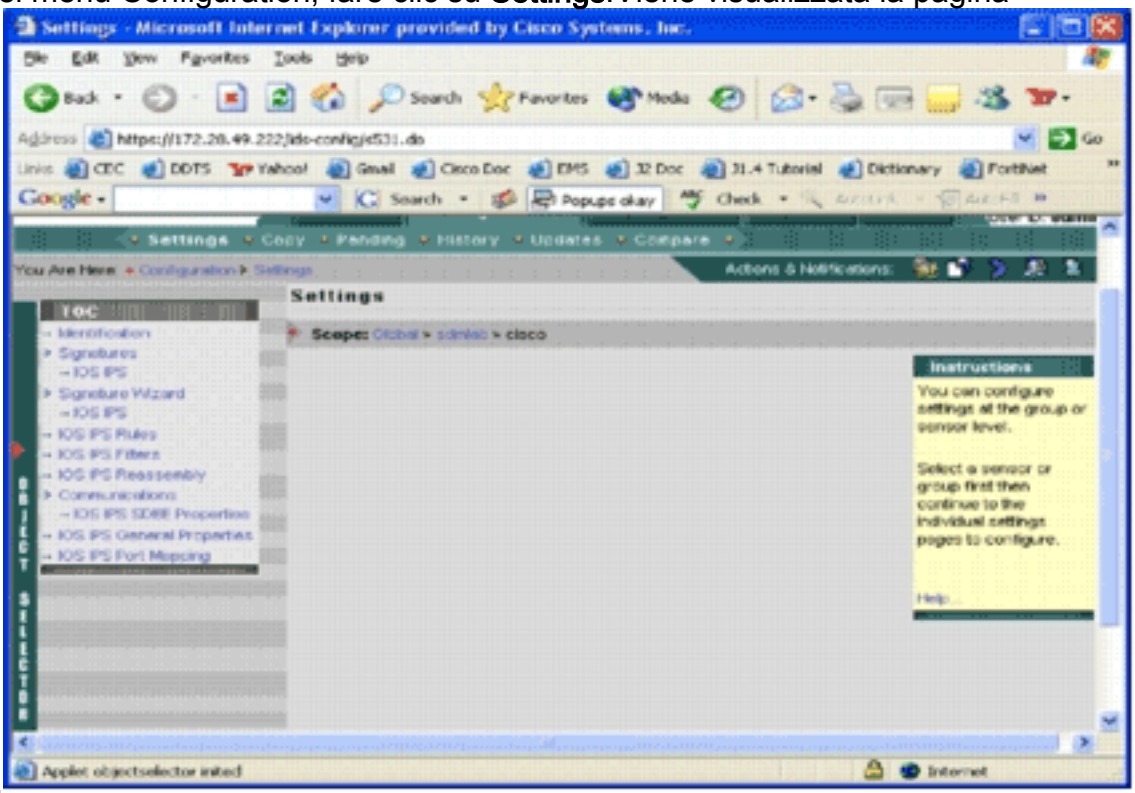
1. Fare clic sulla scheda **Configurazione**.Viene visualizzata la pagina Configurazione.



2. Dal selettore oggetti sul lato sinistro della pagina, scegliere il router Cisco IOS IPS da

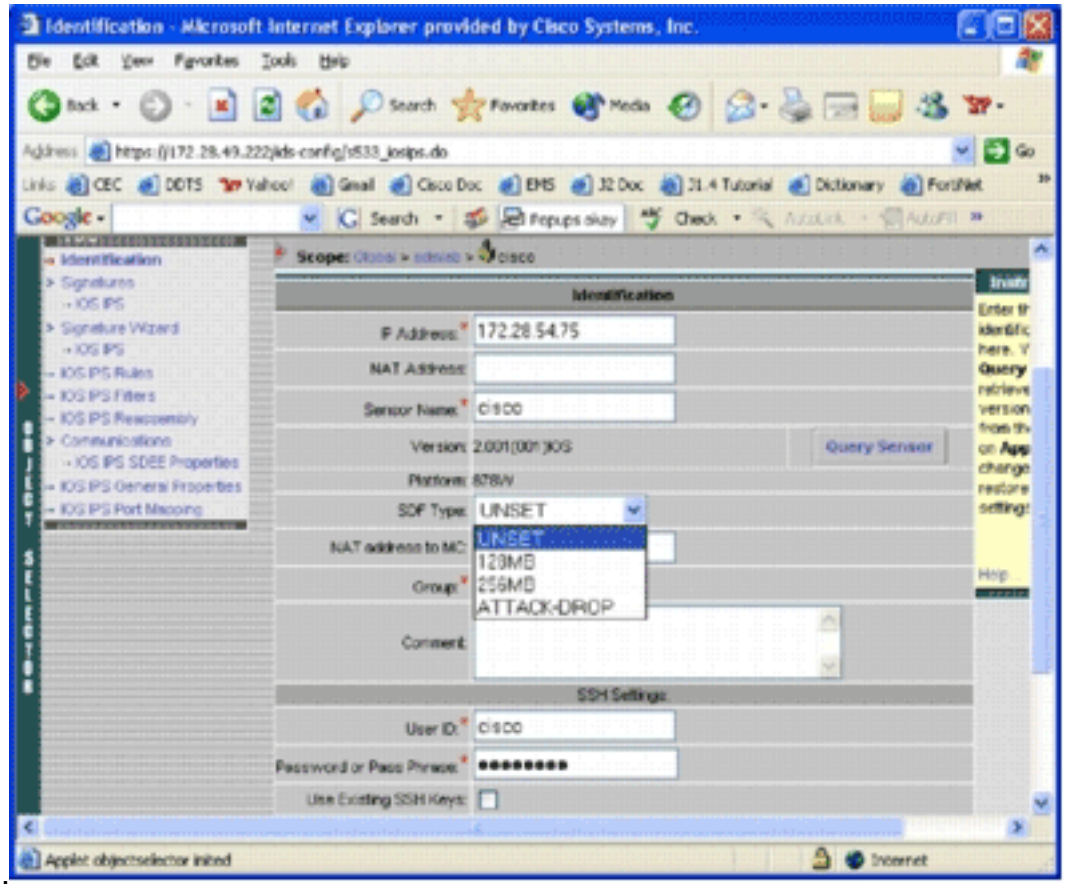
configurare.**Nota:** la maggior parte delle impostazioni di configurazione in IPS MC 2.2 può essere configurata a livello di gruppo e a livello di singolo dispositivo. Ad esempio, i gruppi globali, iosips e sdmlab sono tutti gruppi di oggetti configurabili. In questo esempio viene utilizzato un singolo dispositivo cisco di un gruppo sdmlab.Dopo aver selezionato il router da configurare, la barra dei percorsi nella parte superiore della pagina Configurazione visualizza l'ambito di configurazione corrente. Ad esempio, l'ambito di questo esempio è *Globale > sdmlab > cisco*. *cisco* è l'oggetto configurazione corrente (ossia il router selezionato da Selettore oggetti).

3. Dalla barra dei menu Configuration, fare clic su **Settings**.Viene visualizzata la pagina Impostazioni.



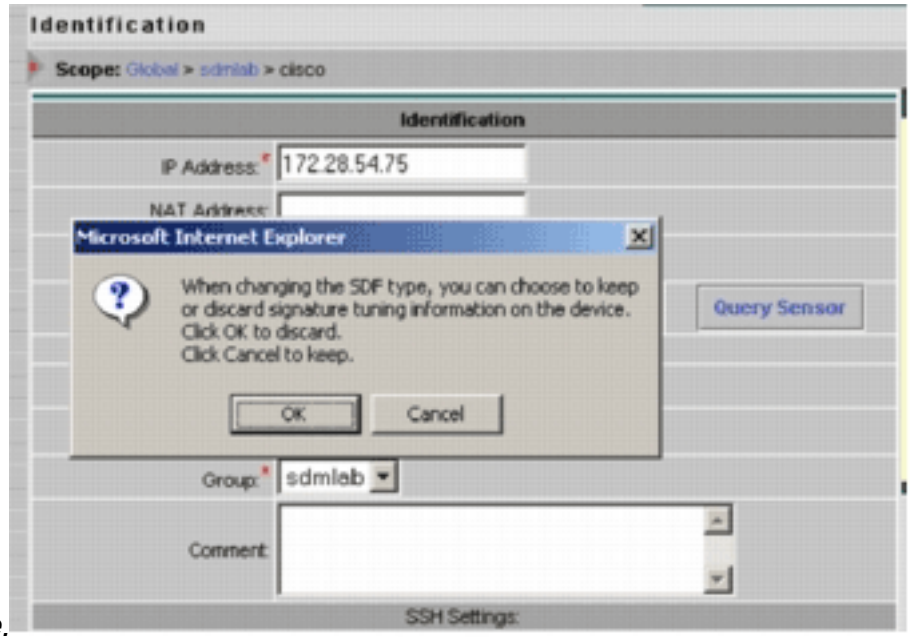
Nella pagina Impostazioni è possibile modificare le impostazioni di configurazione per l'oggetto selezionato. Le impostazioni di configurazione specifiche dei router IPS Cisco IOS sono indicate nella sezione TOC sul lato sinistro della pagina. Di seguito è riportato un elenco delle attività disponibili nella sezione Sommario:*Identificazione*: informazioni di base sul router Cisco IOS IPS; è possibile specificare qui un file SDF non aggiornato*Firma*: firme del router Cisco IOS IPS*Creazione guidata Firma*: una procedura guidata per aggiungere firme personalizzate*Regole IPS Cisco IOS*: per configurare le regole IPS Cisco IOS da applicare alle interfacce*Filtri IPS Cisco IOS*—Filtri IPS Cisco IOS*Riassemblaggio IPS Cisco IOS*: configurazione del riassemblaggio virtuale dell'interfaccia IP*Proprietà Cisco IOS IPS SDEE*: per configurare le impostazioni SDEE*Proprietà generali IPS Cisco IOS* - Configurazioni aggiuntive correlate a Cisco IOS IPS

4. Scegliere **Identification** (Identificazione) per configurare i file SDF non sincronizzati.Viene visualizzata la pagina

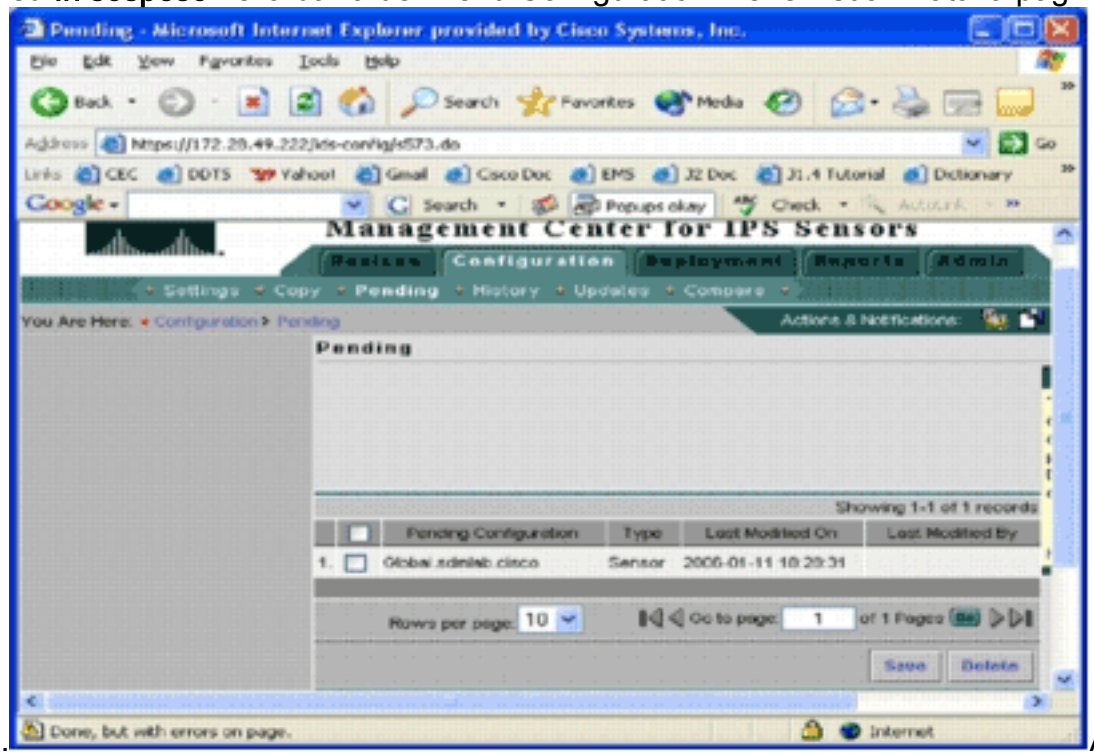


Identificazione.

5. Dall'elenco a discesa Tipo di SDF, scegliere il SDF pretuned appropriato, quindi fare clic su **Applica** per applicare le modifiche.Cisco IOS IPS supporta più di 1600 firme, un valore che supera la capacità di memoria che i router possono accettare. Le SDF sono state sviluppate per facilitare la selezione e il caricamento delle firme più importanti. Attualmente è possibile scegliere tra tre SDF. Le dimensioni variano per consentire la selezione di un file SDF in base alla capacità DRAM dei router. Le scelte disponibili sono descritte di seguito:UNSET - Il tipo SDF non è impostato.ATTACK-DROP: questo SDF è destinato ai router con 64 MB di DRAM.256 MB - Questa SDF è destinata ai router con 256 MB di DRAM.128 MB - Questa SDF è destinata ai router con 128 MB di DRAM.**Nota:** gli SDF da 128 e 256 MB richiedono un motore da 2.001 o superiore. Queste informazioni sono disponibili nel campo **Impostazioni > IU identificazione > Versione**.**Avviso:** IPS MC non include funzioni di gestione della memoria per i router IPS Cisco IOS. Fare attenzione quando si selezionano i file SDF per il router Cisco IOS IPS. Verificare che il router IPS Cisco IOS disponga di memoria sufficiente per eseguire il file SDF selezionato.**Nota:** quando si modifica il tipo di SDF, potrebbe essere visualizzato questo messaggio: *Quando si modifica il tipo di SDF, è possibile scegliere di mantenere o eliminare le informazioni di ottimizzazione della firma sul dispositivo. Fare clic su OK per ignorare. Fare clic su Annulla per*



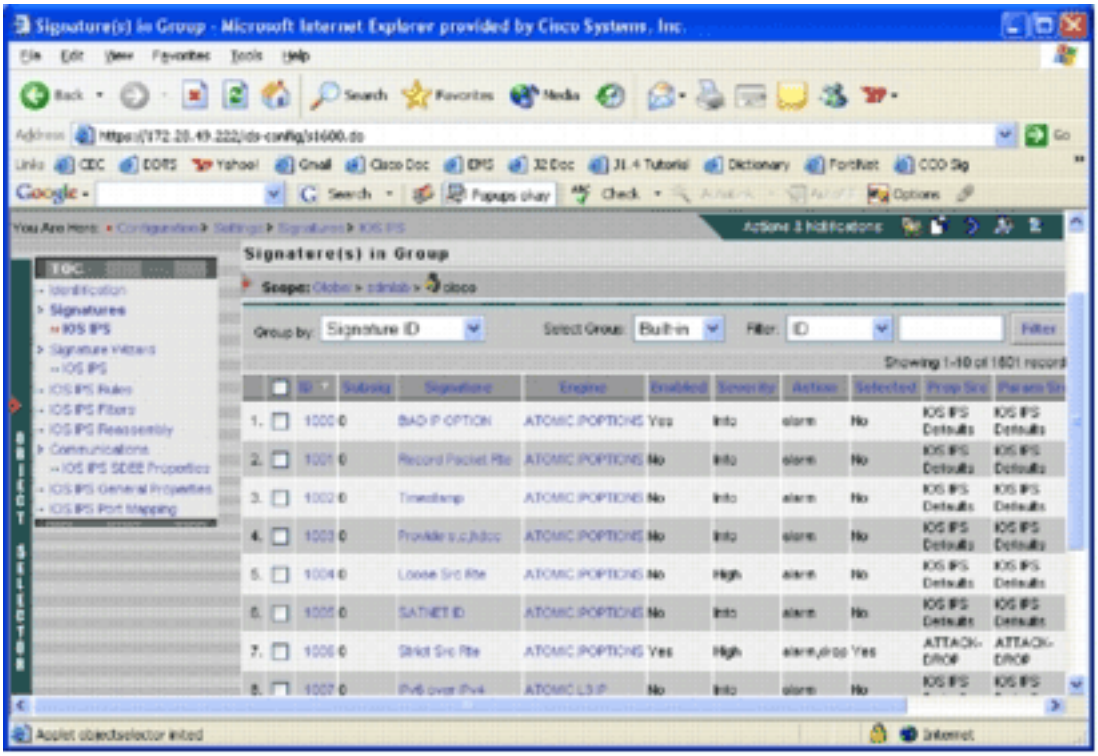
continuare.

6. Per mantenere le informazioni di ottimizzazione della firma, fare clic su **Annulla**.Dopo aver scelto correttamente un SDF preassemblato per il router-cisco, è possibile eseguire ulteriori operazioni di tuning della firma, ad esempio aggiungere o modificare, o persino creare firme personalizzate, oppure ignorare le operazioni di tuning della firma e andare direttamente a Creare una regola da applicare alle interfacce.
7. Fare clic su **In sospeso** nella barra dei menu Configuration.Viene visualizzata la pagina In sospeso. 

A questo punto, l'attività di configurazione è completata. È tuttavia necessario completare l'attività di distribuzione per distribuire le modifiche nel dispositivo di destinazione.

Modifica firme SDF in pre-esecuzione

Dopo aver selezionato un file SDF non valido per un router, è possibile eseguire ulteriori attività di ottimizzazione della firma. È possibile aggiungere, modificare, eliminare e modificare le firme in base alle proprie esigenze oppure creare firme personalizzate quando necessario. In questo esempio viene utilizzato IPS MC per aggiungere ulteriori firme e modificare le azioni. Questa immagine mostra l'interfaccia di configurazione della firma.



Èpossibile utilizzare la configurazione della firma per attivare o disattivare, selezionare o deselezionare, aggiungere una firma, eliminare una firma, modificare le azioni per la firma e modificare i parametri di firma. Utilizzare la procedura guidata Firma a sinistra per creare firme personalizzate.

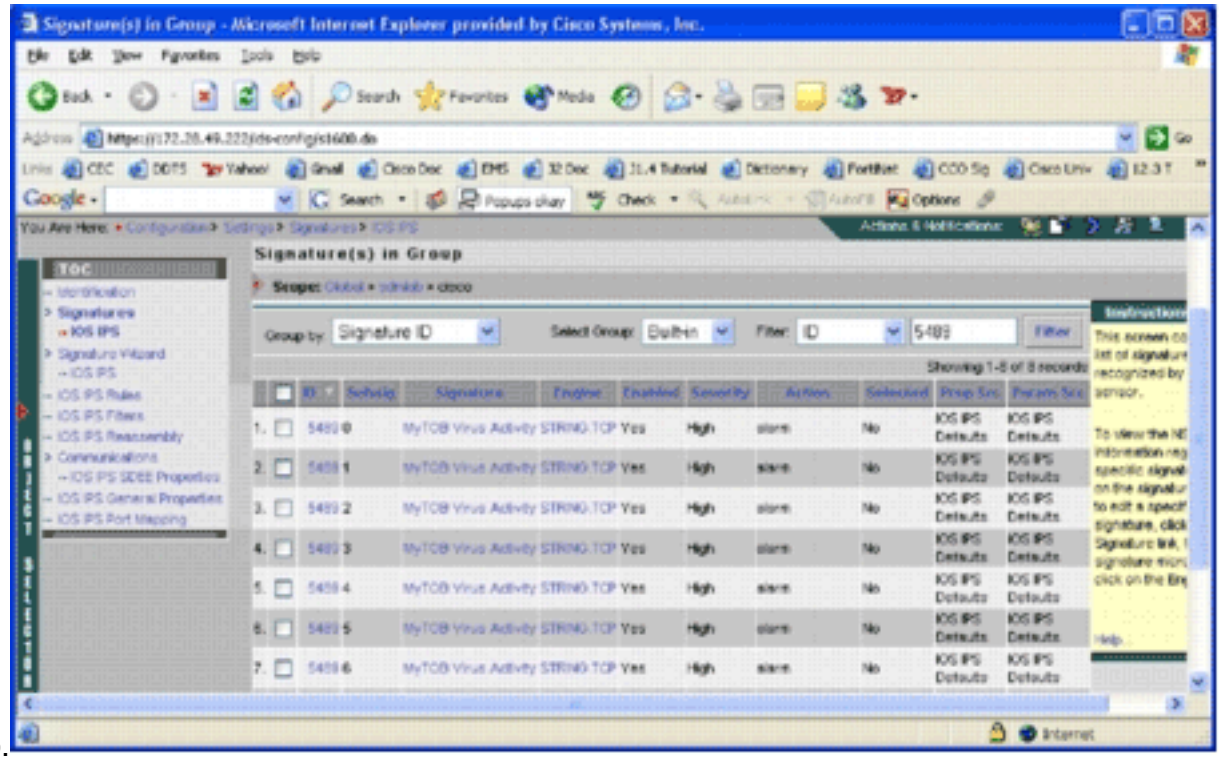
Per impostazione predefinita, nell'interfaccia utente di configurazione della firma vengono visualizzate alcune informazioni. Selezionata indica se la firma verrà inclusa nel file SDF inviato al router. Se non è selezionata, la firma non verrà aggiunta. L'opzione Attivato viene applicata solo se è selezionata una firma. Quando una firma è disattivata, i motori IPS non inviano eventi per quella firma specifica. Se una firma non è selezionata, viene disattivata automaticamente.

Le ultime due colonne (Prop Src e Param Src) indicano rispettivamente da dove provengono la firma e i relativi parametri. È possibile che la firma sia stata ricavata da file SDF non più validi o dai valori predefiniti di fabbrica disponibili negli aggiornamenti del file IOS-Sxxx.zip (visualizzati come valori predefiniti di IOS IPS). Questi valori si applicano anche alla colonna dei parametri.

Quando si aggiungono firme ai router IPS Cisco IOS, è necessario tenere conto delle considerazioni sulla memoria. Se si aggiungono più firme di quante possano essere elaborate dal router IPS Cisco IOS, IPS MC non sarà in grado di distribuire le modifiche della configurazione ai dispositivi.

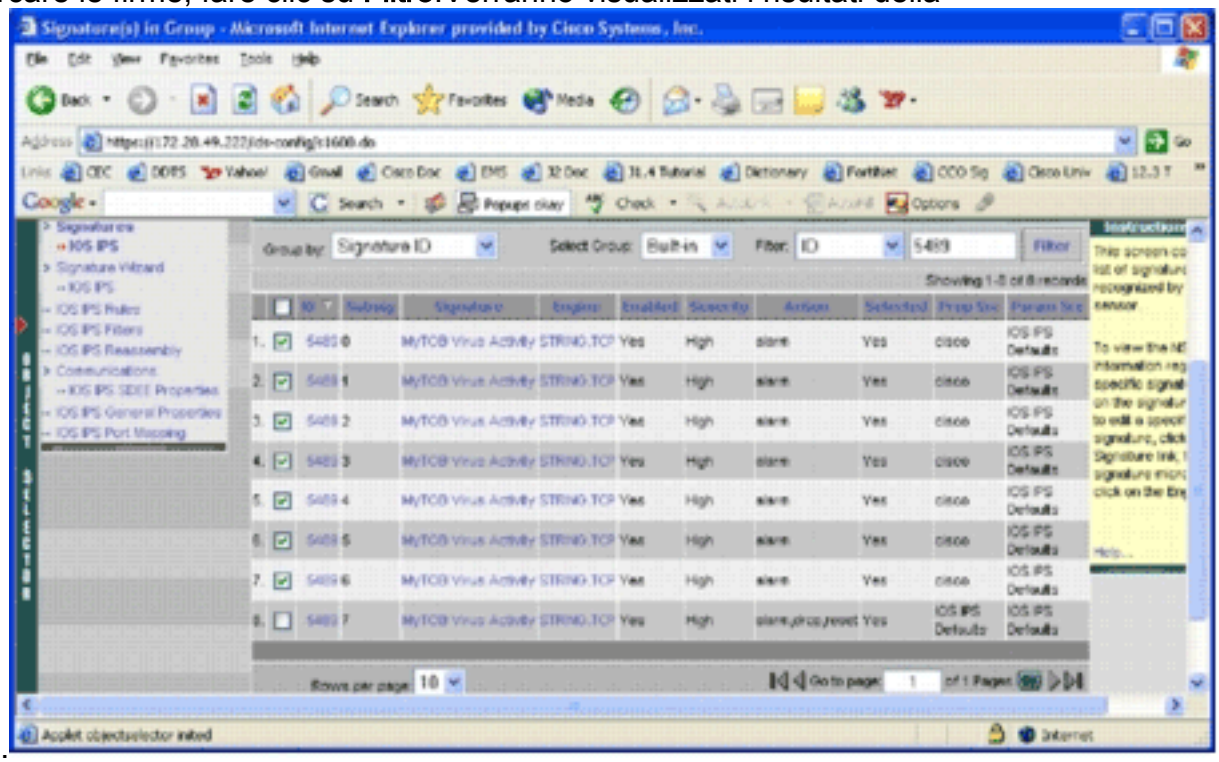
Completare questi passaggi per aggiungere le firme 5489/x al router Cisco IOS IPS:

1. Selezionare **Configuration**, quindi utilizzare il selettore oggetti per selezionare il router IPS Cisco IOS per cui si desidera configurare le firme IPS.
2. Scegliere **Configurazione > Impostazioni > Firme > IOS IPS**.Verrà visualizzata la pagina Firme nel



gruppo.

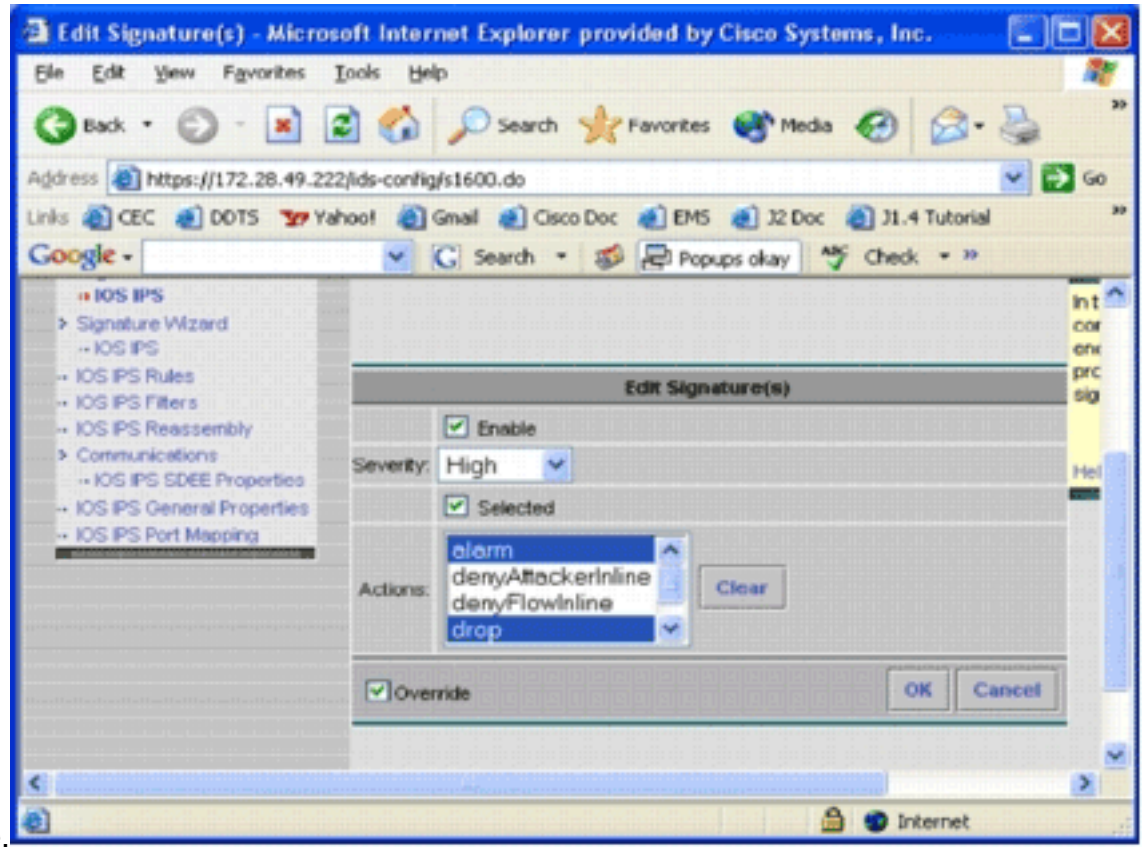
3. Nell'elenco di firme risultante selezionare Filtra per ID e digitare ID firma 5489.
4. Per cercare le firme, fare clic su **Filtro**.Verranno visualizzati i risultati della

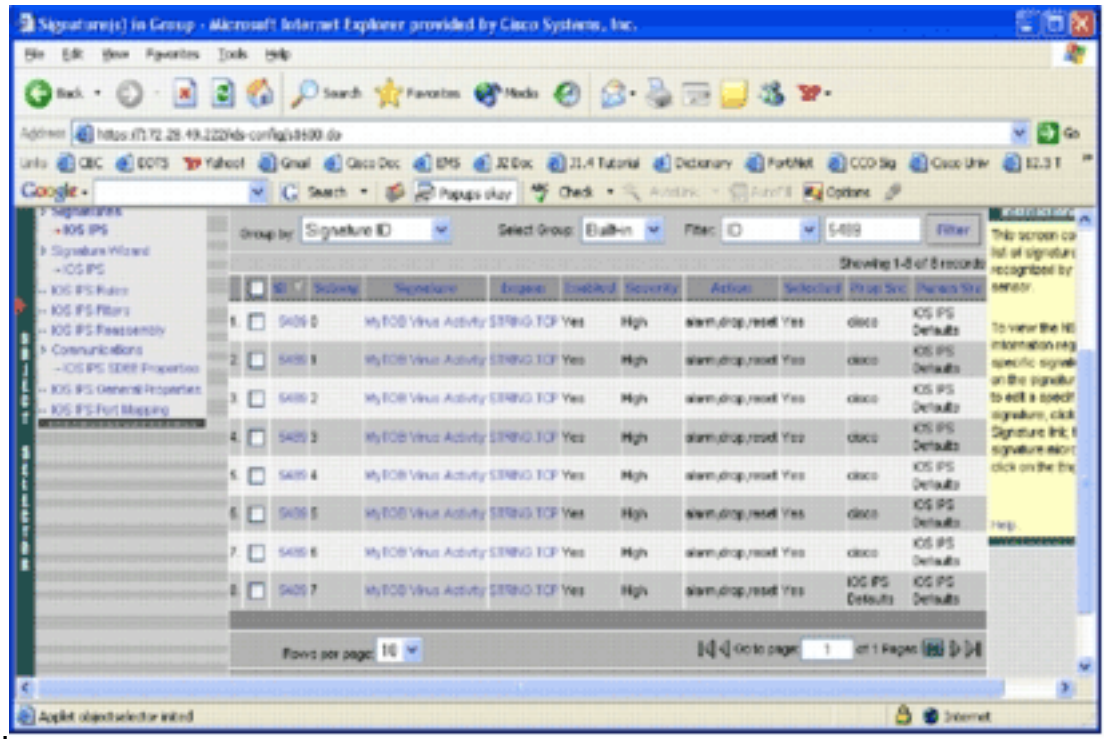


ricerca.

Nota: IPS MC non supporta nuove classificazioni disponibili in Cisco SDM.

5. Selezionare la casella di controllo accanto alle firme non selezionate e fare clic su **Seleziona** nella barra degli strumenti inferiore.
6. Per modificare le azioni relative alla firma, fare clic su **Modifica**.Viene visualizzata la pagina Modifica

firma/e. 

7. Selezionare la casella di controllo **Selezionato** e selezionare **allarme**, **rilascio** e **reimpostazione** dall'elenco Azioni.
8. Selezionare la casella di controllo **Sostituisci** e quindi fare clic su **OK**.Tutte le firme vengono modificate con le azioni desiderate. 
9. Passare all'attività In sospeso e salvare tutte le modifiche. Il task di configurazione è stato completato.**Suggerimento:** prestare particolare attenzione alla colonna Prop Src. Dopo la modifica, l'origine viene modificata nel dispositivo *cisco*, il che significa che tutte le informazioni di ottimizzazione vengono salvate separatamente dai file SDF predefiniti. Questo meccanismo consente a IPS MC di mantenere le modifiche alle firme personalizzate.

Nella sezione precedente, quando sono stati modificati i tipi di file SDF, IPS MC ha chiesto se si desidera mantenere le informazioni di ottimizzazione della firma. Informazioni sul tuning della

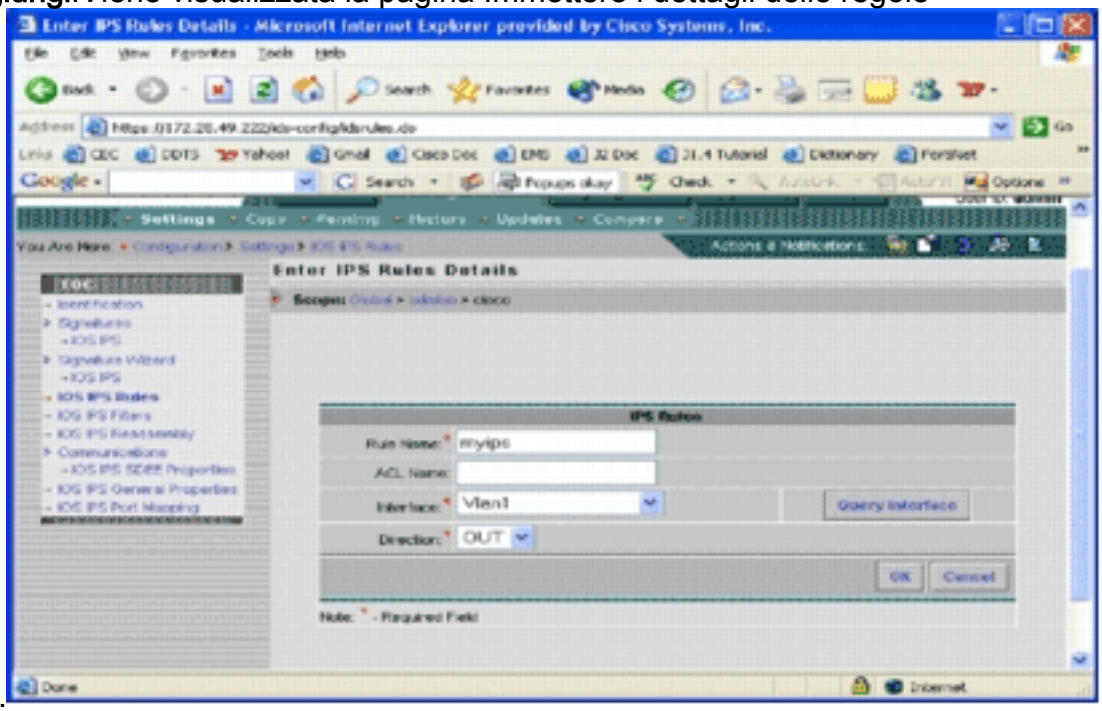
firma a cui si fa riferimento.

Scegli firme personalizzate

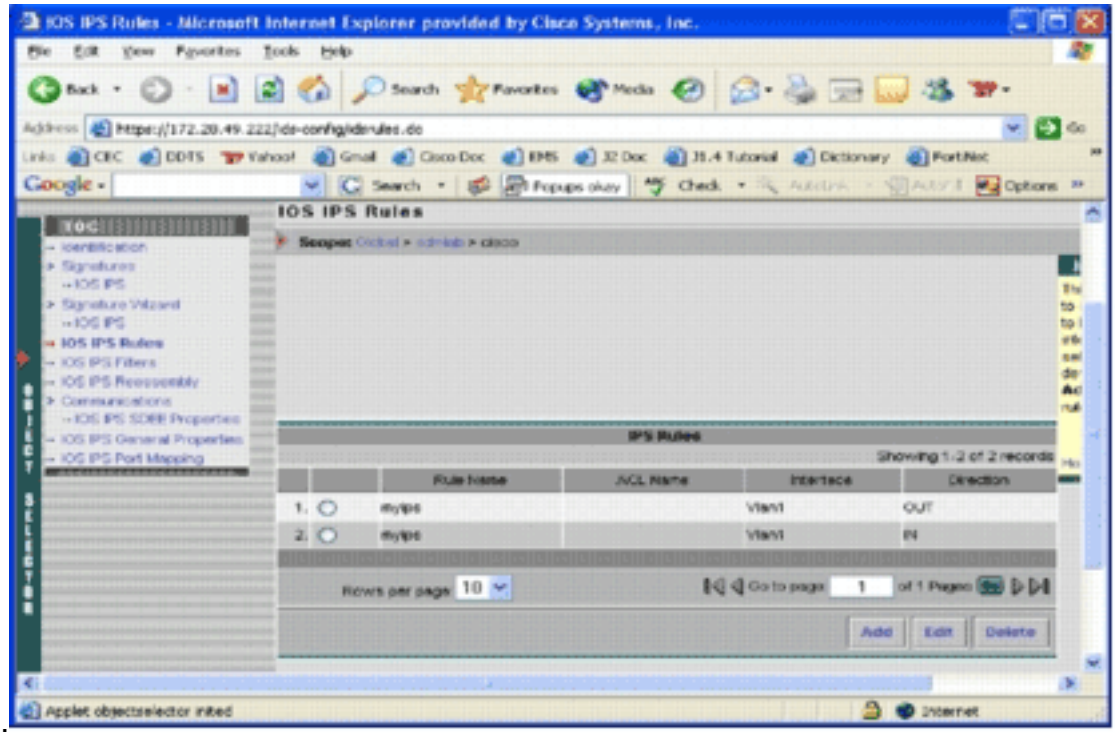
Se non si desidera utilizzare i file SDF con conservazione predefinita, è possibile utilizzare i passaggi specificati nella sezione Modifica firme SDF con conservazione per selezionare le firme di ottimizzazione per i dispositivi. Nella pagina di identificazione, accertatevi che il tipo di SDF sia UNSET. Fare riferimento al passaggio 3 di Configurazione del router Cisco IOS IPS per l'utilizzo dei file delle firme ritirate.

Crea una regola da applicare alle interfacce

Dopo aver regolato la firma, è necessario abilitare l'IPS sui router Cisco IOS. Per abilitare il protocollo IPS sul router, è necessario creare una regola IPS e applicarla ad almeno un'interfaccia.

1. Selezionare **Configuration**, quindi utilizzare il selettore oggetti per selezionare il router Cisco IOS IPS da configurare. Verificare nella barra del percorso che l'ambito sia a livello di dispositivo e non di gruppo.
2. Selezionare **Configurazione > Impostazioni > Regole IPS IOS**, quindi fare clic su **Aggiungi**.Viene visualizzata la pagina Immettere i dettagli delle regole IPS. 

3. Immettere le informazioni relative al nome e all'interfaccia della regola a cui si desidera applicare la regola e la direzione.
4. Fare clic su **OK**.Viene visualizzata la pagina Regole IPS



IOS. Analogamente, potete creare regole per entrambe le direzioni di un'interfaccia.

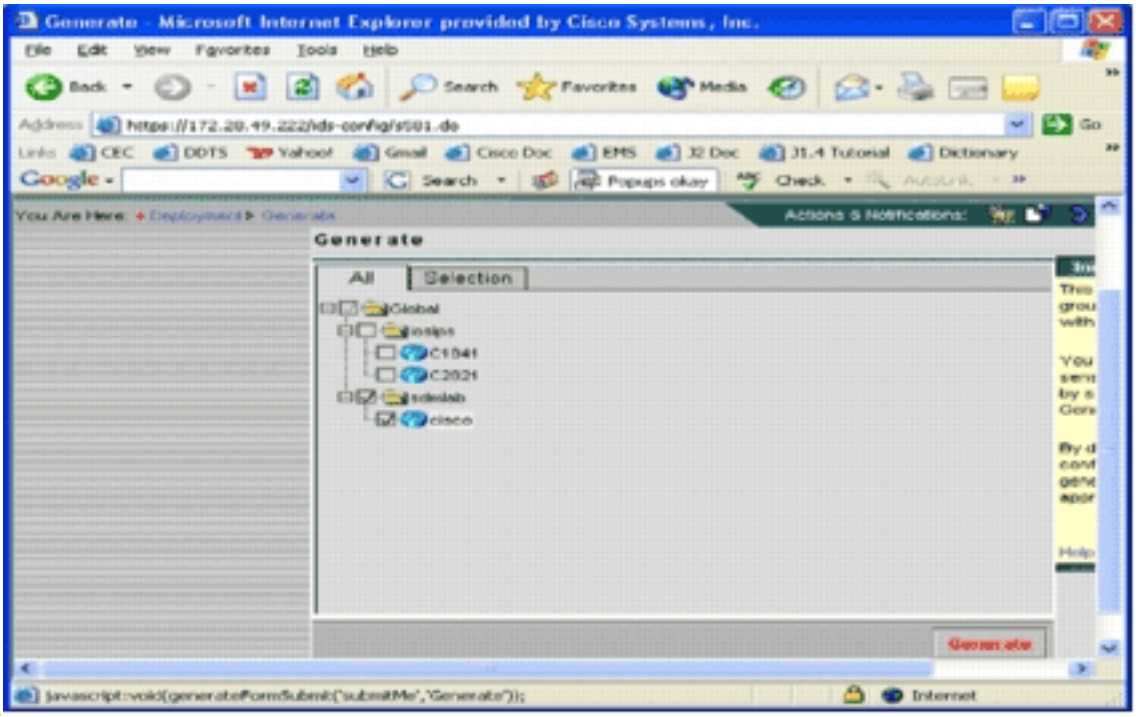
5. Ènecessario salvare le modifiche alla configurazione e completare il processo di distribuzione per apportare le modifiche al dispositivo o al gruppo di dispositivi interessato.Èpossibile eseguire anche altre configurazioni relative a IPS, ma tutte le altre attività sono facoltative e non obbligatorie. Tutte le opzioni sono disponibili a sinistra dell'interfaccia utente di configurazione. Questo documento non descrive le opzioni di configurazione opzionali.

Distribuire la configurazione

Dopo aver apportato tutte le modifiche alla configurazione, è necessario utilizzare l'attività di distribuzione per eseguire il commit delle modifiche nei dispositivi. Tutte le configurazioni effettuate finora vengono salvate localmente sul server MC IPS.

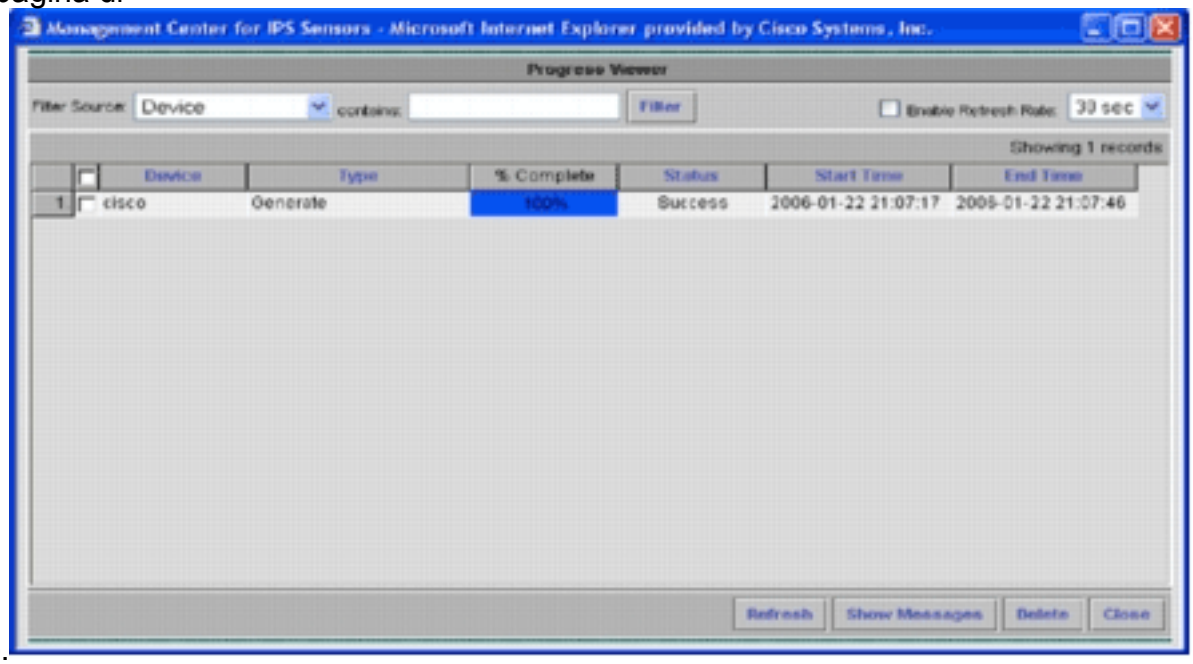
Per distribuire le modifiche alla configurazione, andare alla pagina Distribuzione e completare i seguenti passaggi:

1. Fare clic sulla scheda **Distribuzione** e scegliere **Genera** per generare le modifiche alla configurazione.Viene visualizzata la pagina



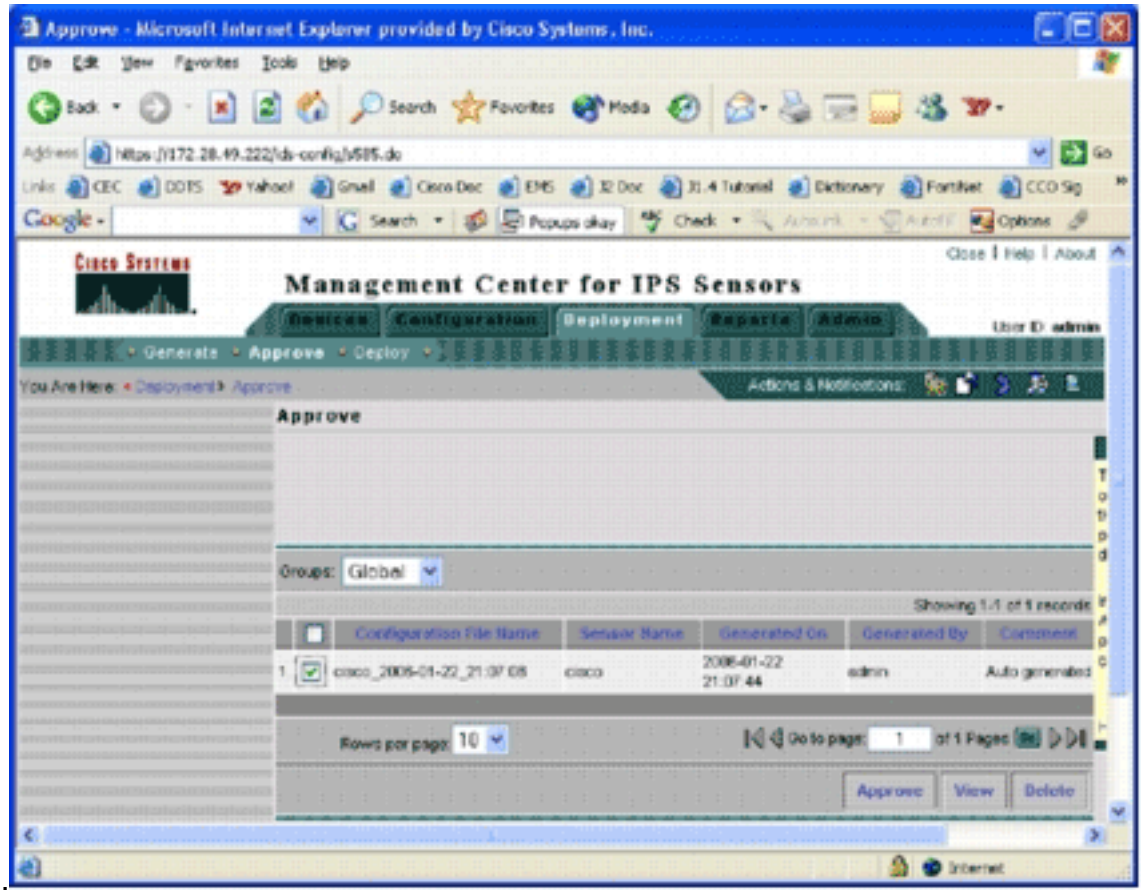
Genera.

2. Selezionare il dispositivo *cisco* appena configurato e fare clic su **Generate** (Genera).
3. Fare clic su **OK** per accettare la configurazione generata e quindi su **OK**.Viene visualizzata una pagina di



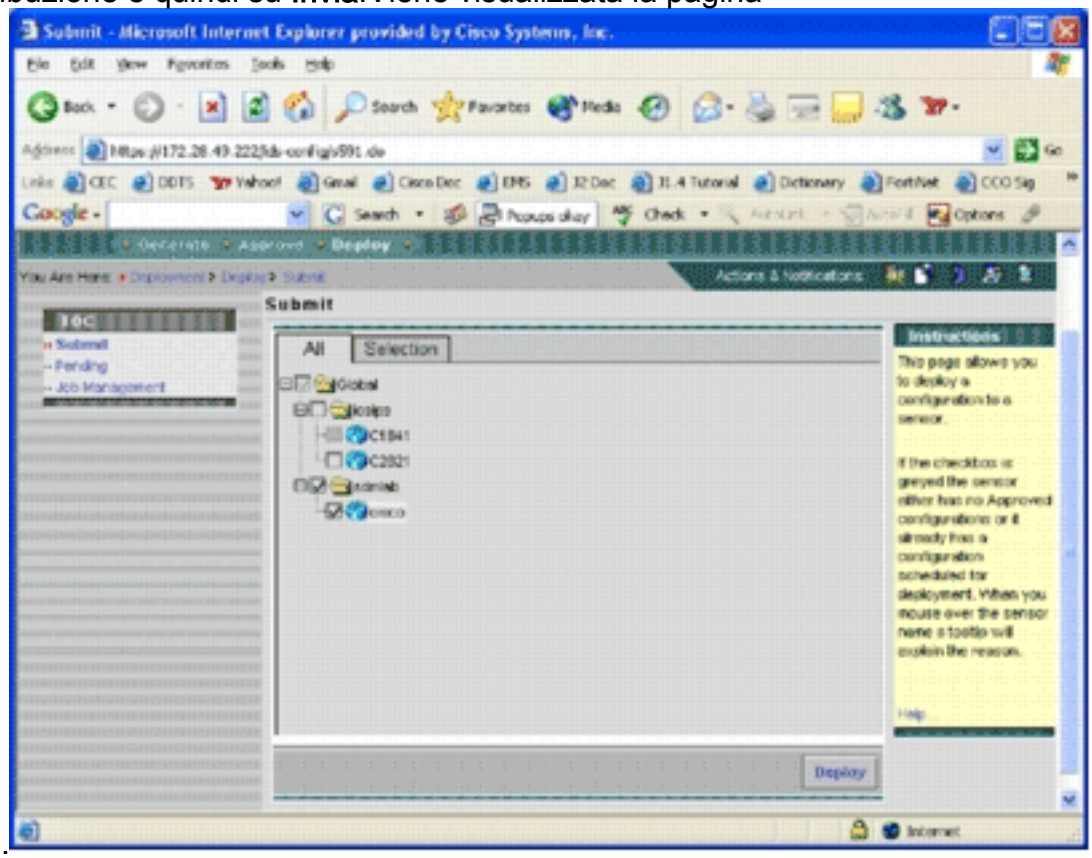
stato.

4. Fare clic su **Aggiorna** fino al completamento dell'attività di generazione.
5. Fare clic su **Approva** nella barra dei menu Distribuzione e nel gruppo sdmlab per visualizzare un elenco di configurazioni che richiedono approvazione.Viene visualizzata la pagina



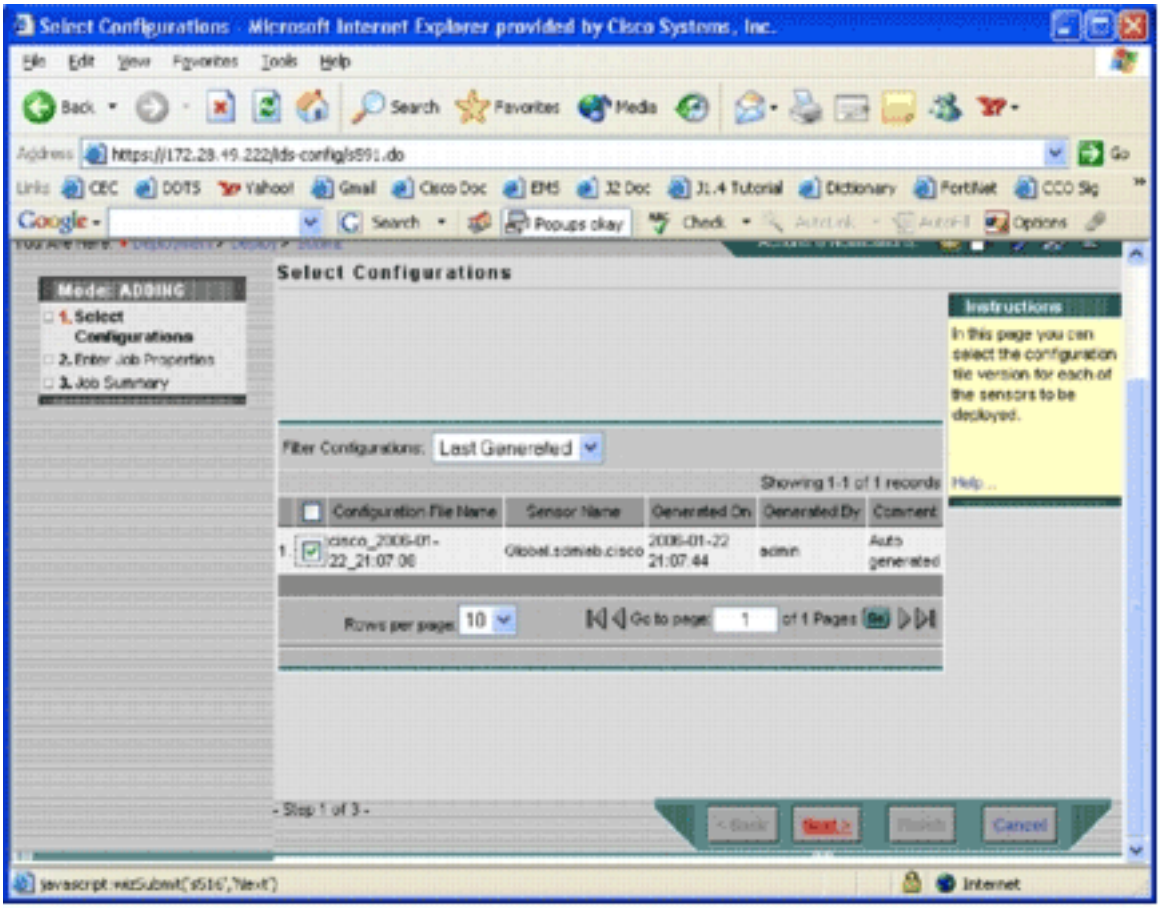
Approva.

6. Scegliere le attività e fare clic su **Approva**.Fare clic su **Distribuisci** nella barra dei menu Distribuzione e quindi su **Invia**.Viene visualizzata la pagina

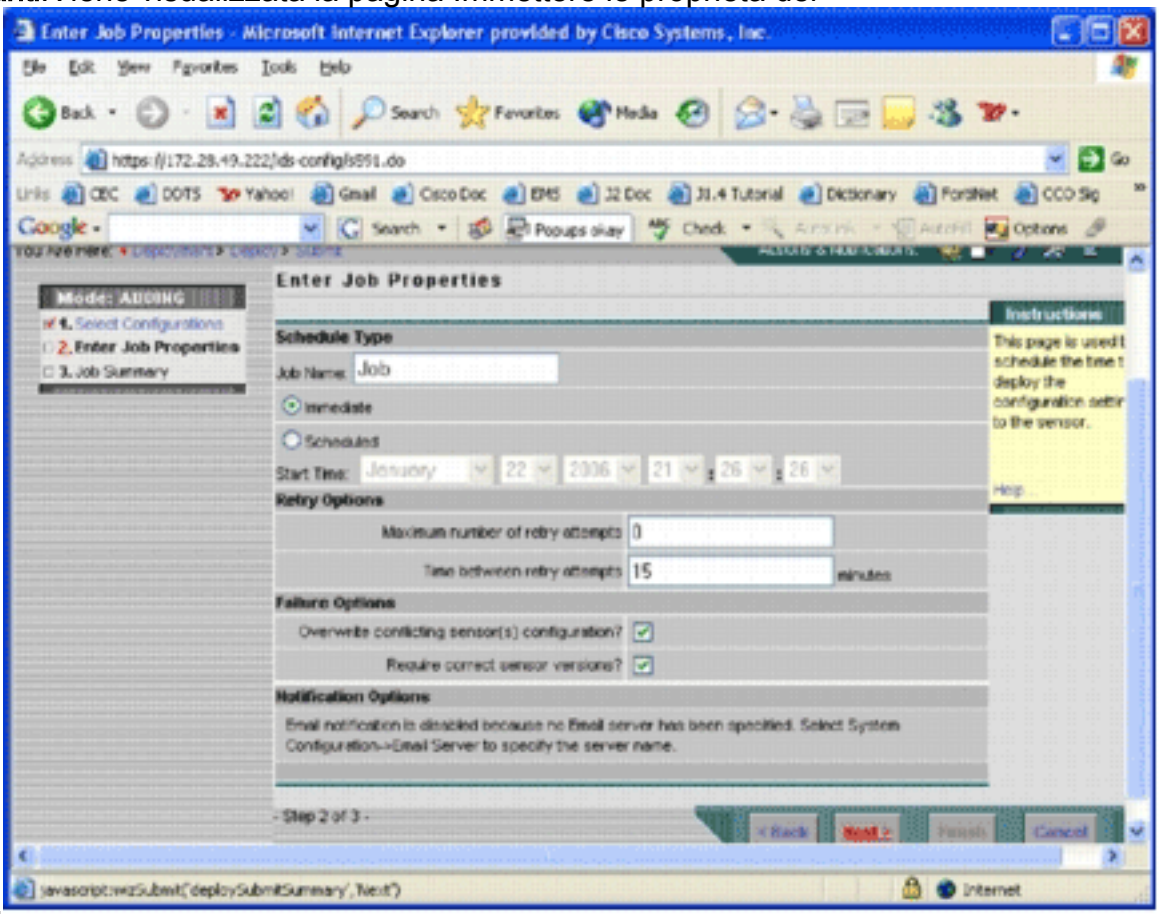


Invia.

7. Scegliere i dispositivi per i quali si desidera inviare l'attività di distribuzione.
8. Selezionare il dispositivo *cisco* e fare clic su **Distribuisci**.Viene visualizzata la pagina Seleziona configurazioni.

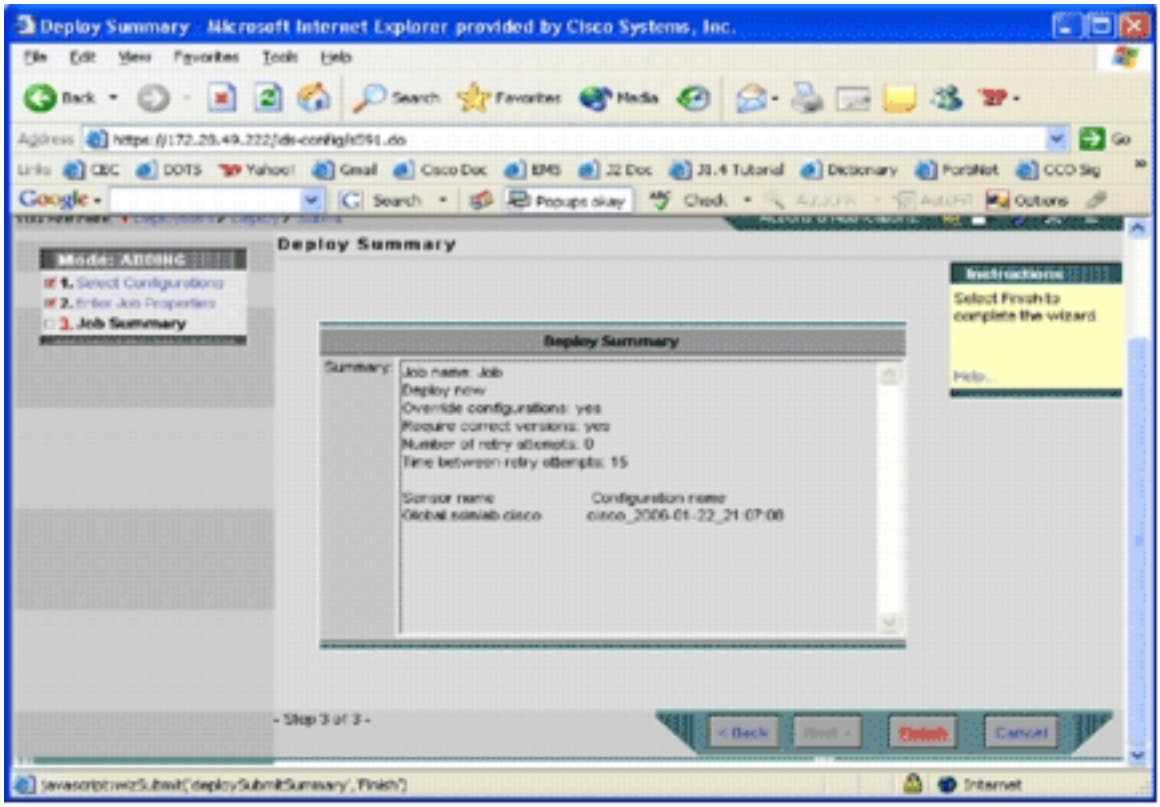


9. Selezionare la configurazione appena eseguita per il dispositivo *cisco* e fare clic su **Avanti**.Viene visualizzata la pagina Immettere le proprietà del job.

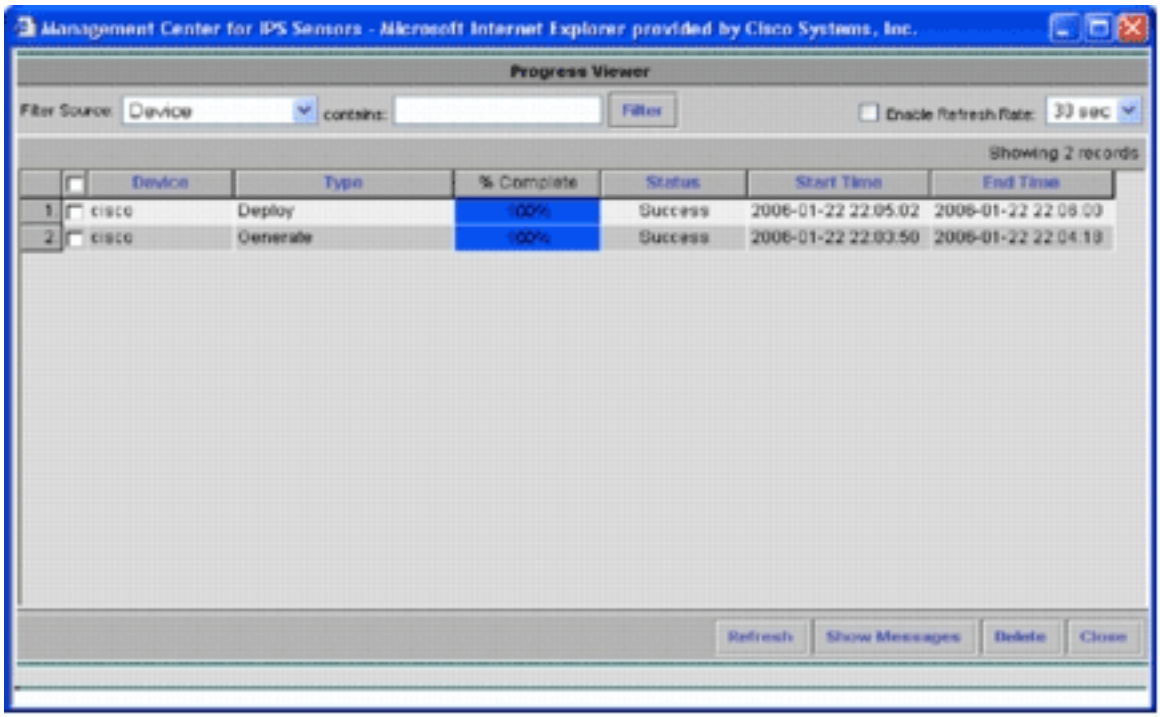


10. È possibile distribuire immediatamente le modifiche oppure pianificare un'attività in modo che venga eseguita in un secondo momento. In questo esempio scegliere l'opzione **Immediata** e quindi fare clic su **Avanti**.Viene visualizzato un breve riepilogo del processo

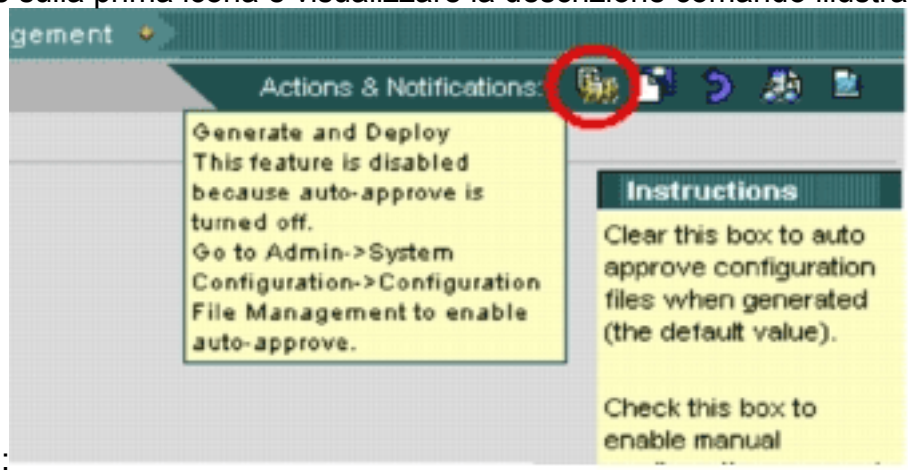
pronto per la distribuzione.



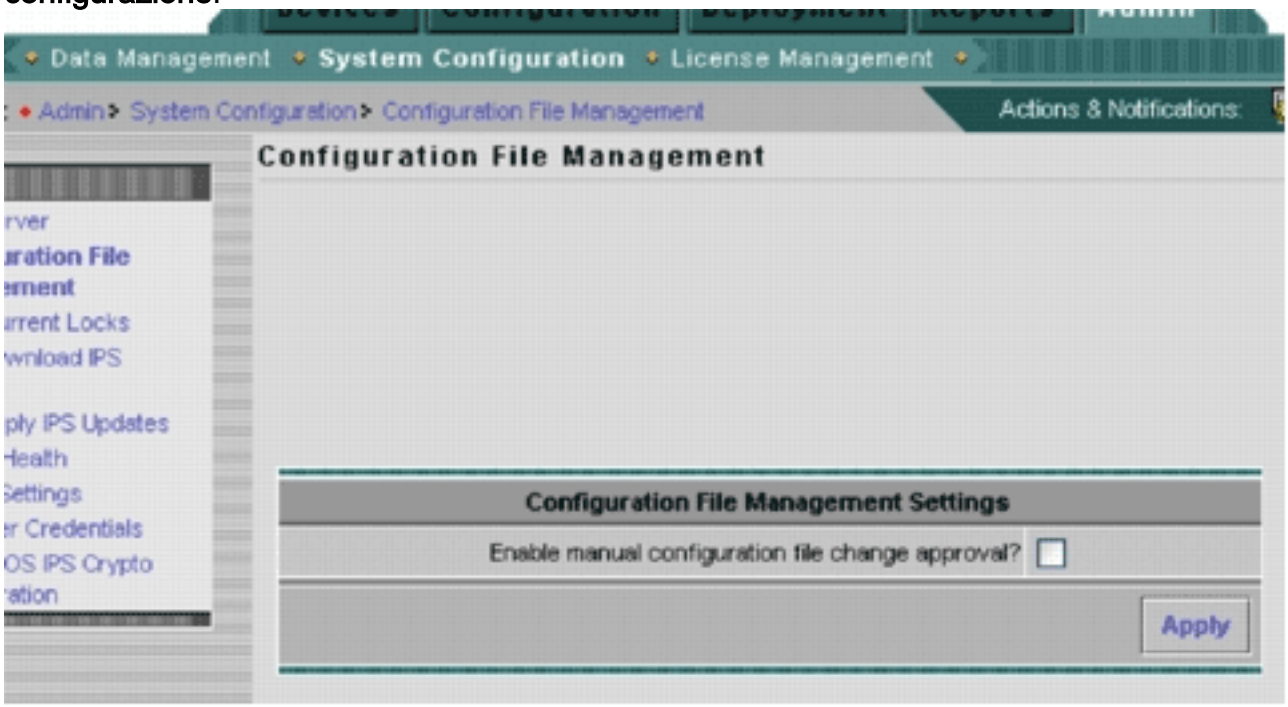
11. Fare clic su **Finish** (Fine).Al termine della distribuzione, una finestra di dialogo mostra lo stato del processo di distribuzione.

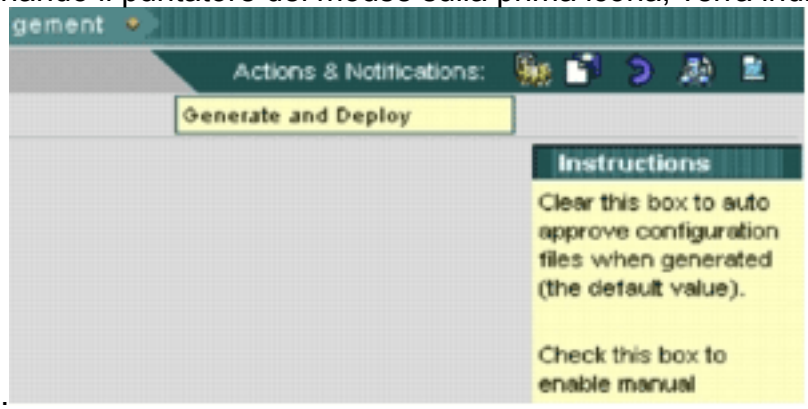


La distribuzione delle configurazioni IPS Cisco IOS nel dispositivo è stata completata. Quando si configurano più dispositivi, è possibile apportare modifiche alla configurazione a livello di gruppo e quindi applicare le modifiche a tutti i router Cisco IOS IPS appartenenti allo stesso gruppo.**Suggerimento:** questo processo è lungo, ma è disponibile una funzione di consegna rapida. Quando si utilizza questa funzione, non è necessario eseguire il processo **Genera > Approva > Distribuisci**. Per utilizzare la funzione, completare i seguenti passaggi:Nella parte superiore dell'interfaccia utente è presente una fila di icone piccole. Posizionare il puntatore

del mouse sulla prima icona e visualizzare la descrizione comando illustrata in questa immagine: 

Per abilitare il task Genera e distribuisci, selezionare **Amministrazione > Configurazione di sistema > Gestione file di configurazione** e deselezionare la casella di controllo **Abilita approvazione modifica manuale file di configurazione**.



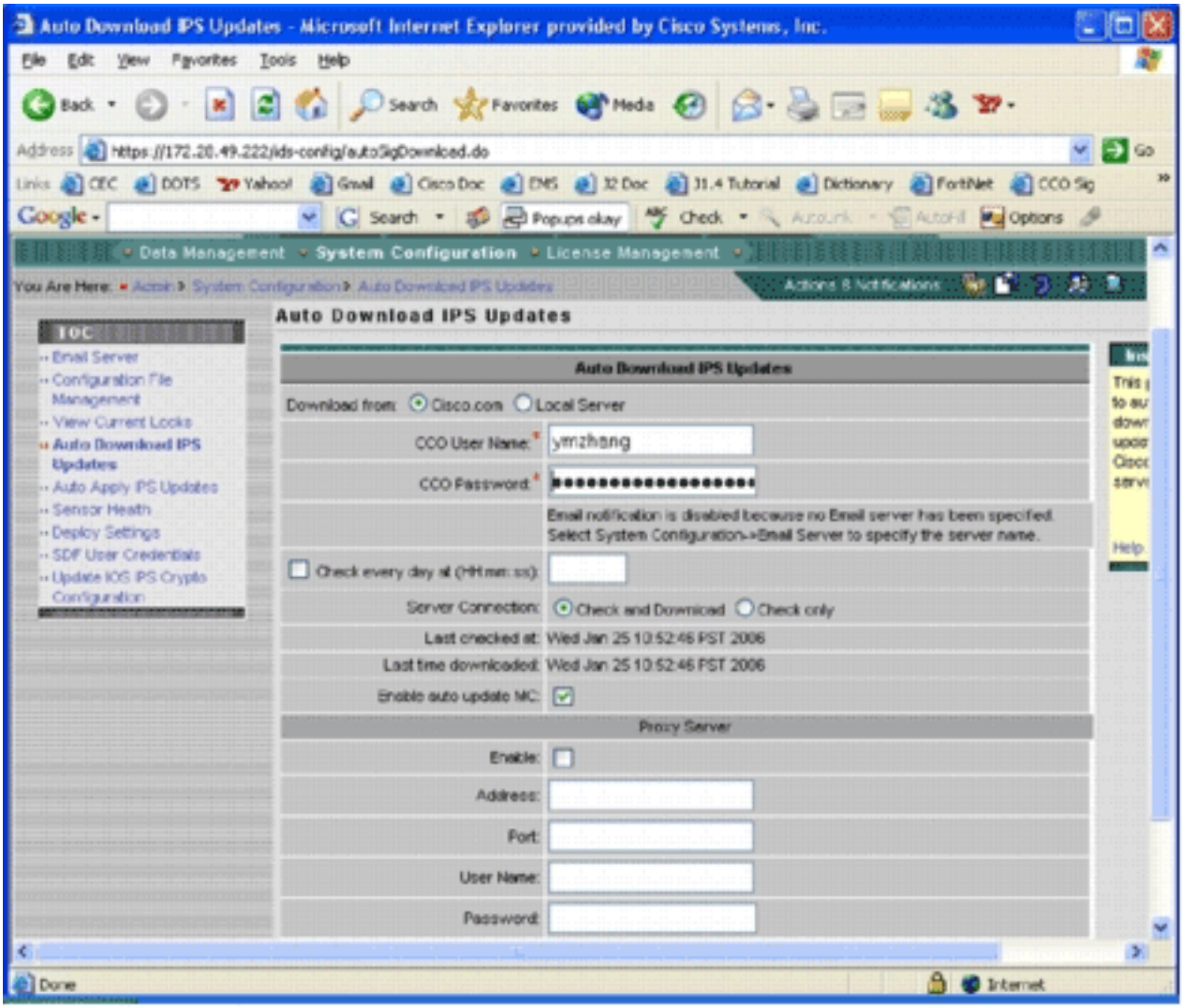
Posizionando il puntatore del mouse sulla prima icona, verrà indicato che l'operazione è attivata. 

Fare clic su questa icona.IPS MC genera automaticamente le modifiche alla configurazione e le distribuisce ai dispositivi.

Aggiornamenti firma download automatico

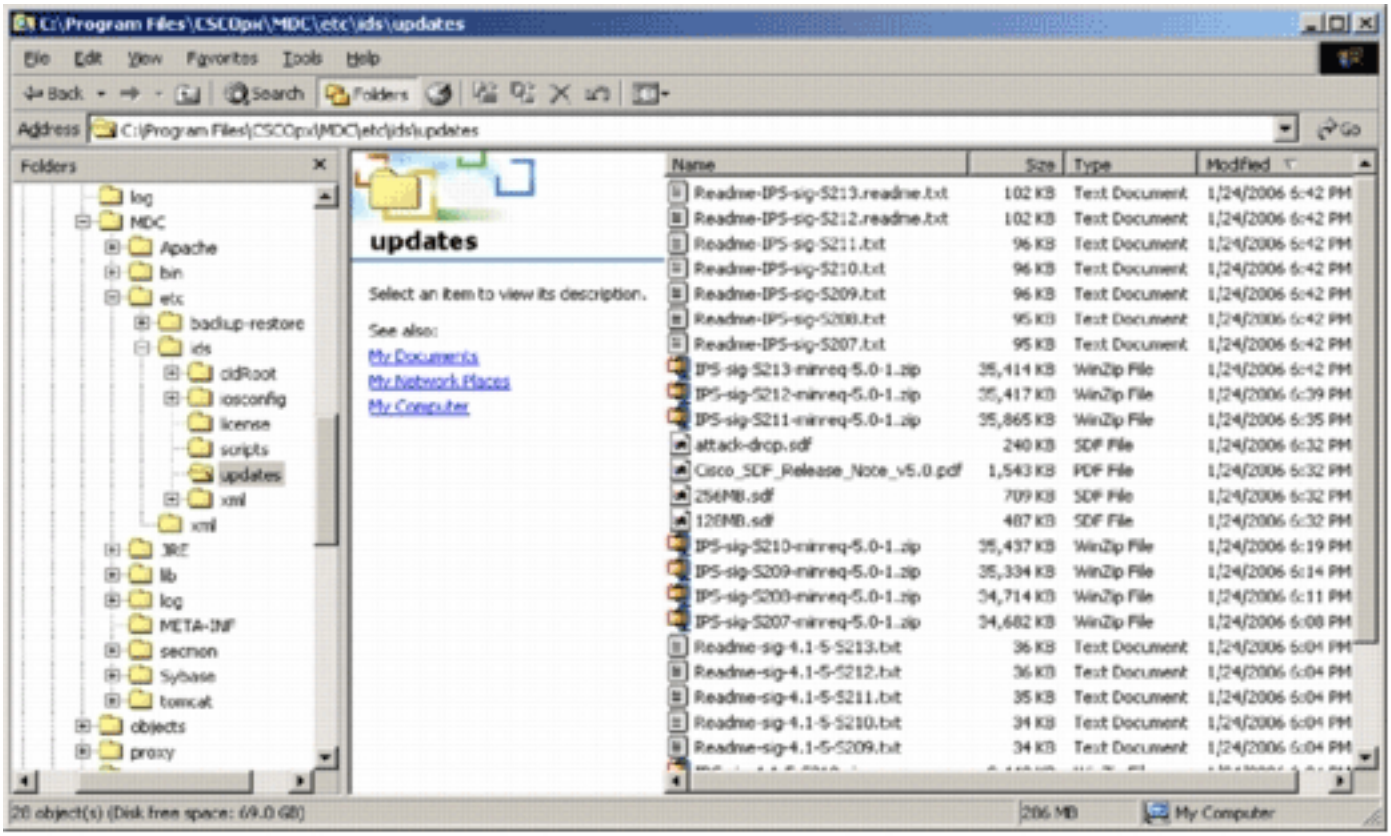
IPS MC supporta il download automatico degli aggiornamenti delle firme da Cisco.com. Può scaricare aggiornamenti delle firme per le piattaforme dei sensori e per le piattaforme Cisco IOS IPS. Per configurare questa funzione, scegliere **Amministrazione > Configurazione di sistema > Download automatico aggiornamenti IPS**.

Viene visualizzata la pagina Download automatico aggiornamento IPS.



Per scaricare l'aggiornamento della firma è necessario disporre di un account Cisco.com valido. Per controllare i file scaricati automaticamente, passare alla directory principale di installazione di IPS MC. Per impostazione predefinita è \program files\CSCOpx\MDC\etc\ids\updates.

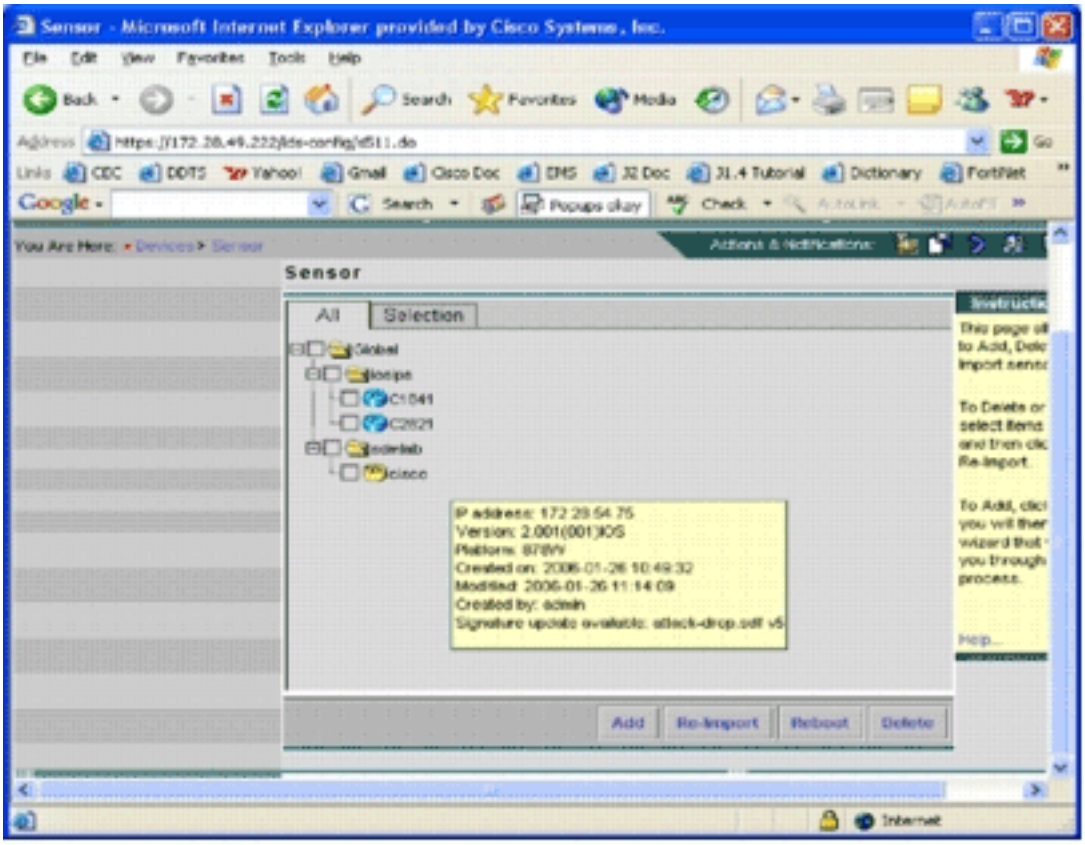
Questa immagine mostra un'immagine dei file scaricati in questa directory.



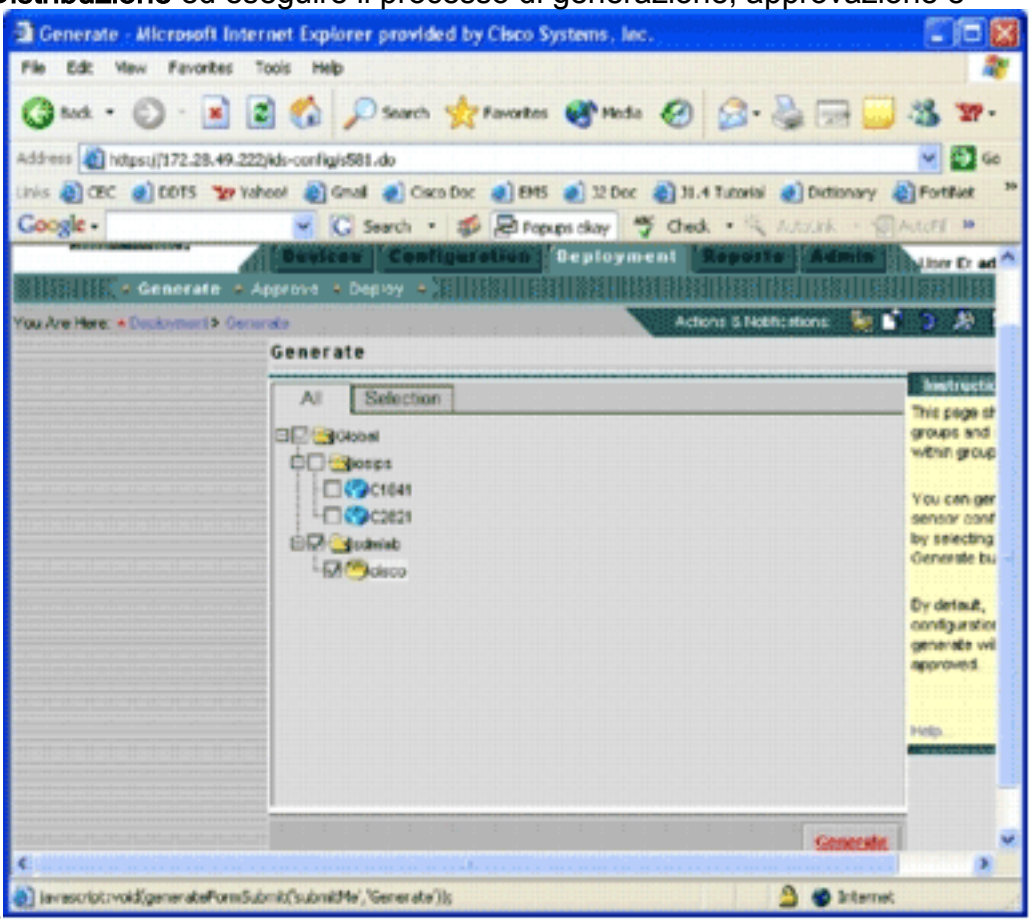
Potete vedere i file di aggiornamento del sensore. Vengono scaricati il file di aggiornamento del software Cisco IOS e i file SDF non utilizzati.

Aggiorna il router IPS Cisco IOS con i nuovi file SDF

Per i router IPS Cisco IOS distribuiti con file SDF non appena una nuova versione dei file SDF è disponibile tramite il download automatico o copiata nella directory degli aggiornamenti, Cisco IPS MC riconosce la nuova versione. Dopo un aggiornamento dell'interfaccia utente, le icone dei dispositivi applicabili diventano gialle.



1. Fare clic su **Distribuzione** ed eseguire il processo di generazione, approvazione e distribuzione.



2. Dopo la corretta distribuzione, il router IPS Cisco IOS utilizza una nuova versione dei file SDF.

Informazioni correlate

- Cisco Intrusion Prevention System