Ejemplo de Configuración de CiscoWorks IPS MC en Cisco IOS IPS

Contenido

Introducción

CiscoWorks Management Center for IPS Sensors (IPS MC) es la consola de gestión para los dispositivos Cisco IPS. La versión 2.2 de IPS MC admite el aprovisionamiento de la función Intrusion Prevention System (IPS) en los routers de software Cisco IOS®. Este documento describe cómo utilizar IPS MC 2.2 para configurar Cisco IOS IPS.

Para obtener más información sobre cómo utilizar IPS MC (que incluye cómo utilizarlo para configurar dispositivos que no se basan en el software Cisco IOS), consulte la documentación de CiscoWorks Management Center para sensores IPS en esta URL:

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

Prerequisites

Requirements

No hay requisitos específicos para este documento.

Componentes Utilizados

La información de este documento se basa en la versión 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.

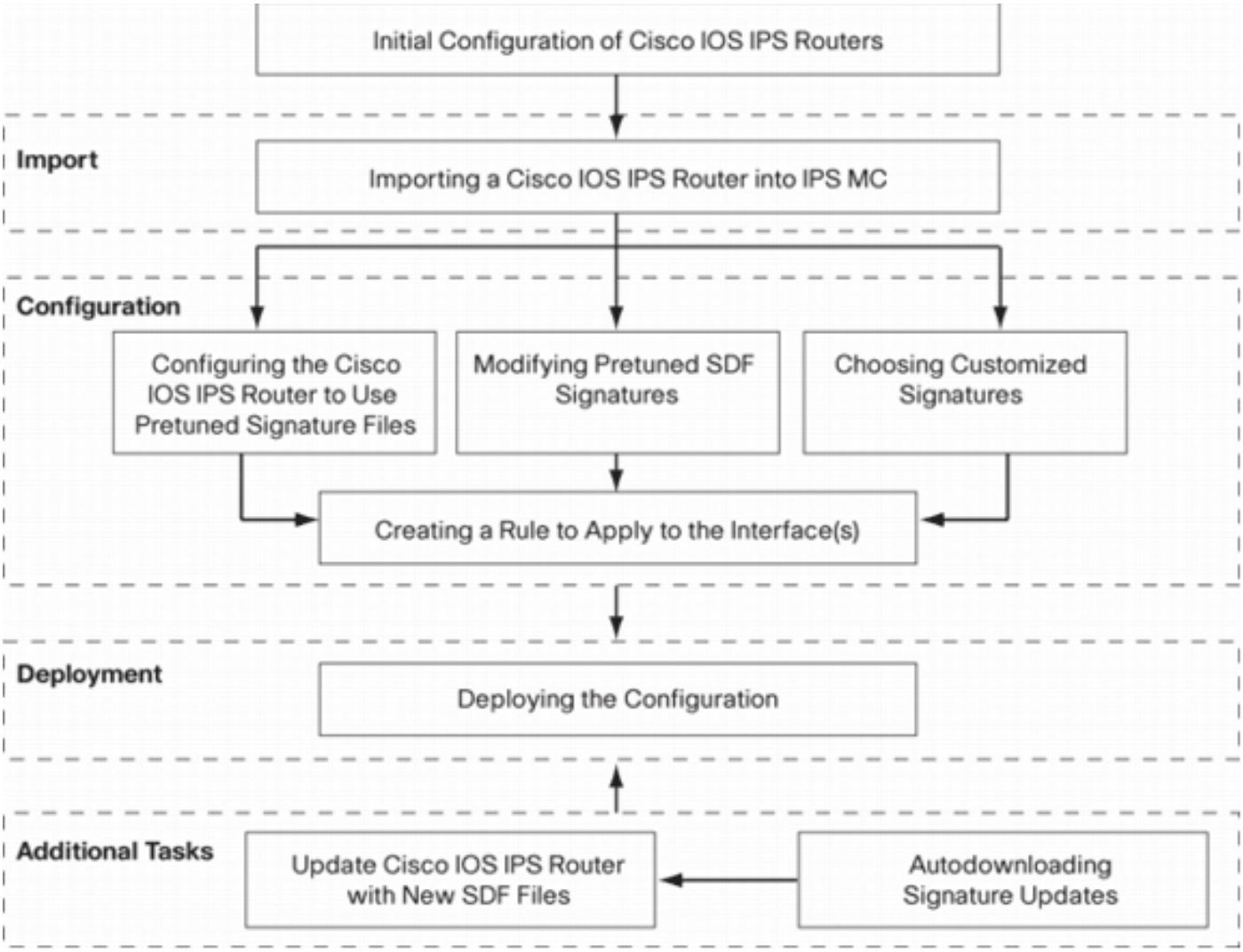
Convenciones

Consulte Convenciones de Consejos Técnicos de Cisco para obtener más información sobre las convenciones sobre documentos.

Configurar

Comprensión básica de las tareas de configuración

IPS MC se utiliza para administrar la configuración de un grupo de routers Cisco IOS IPS. Tenga en cuenta que IPS MC no gestiona las alertas de los routers que ejecutan IPS. Cisco recomienda Cisco Security Monitoring, Analysis and Response System (Cisco Security MARS) para la supervisión de IPS. La administración de la configuración consta de una serie de tareas descritas en este documento. Estas tareas se pueden dividir en tres fases: importar, configurar e implementar como se muestra en esta imagen.



Cada fase tiene su propio conjunto de responsabilidades y funciones:

- *Importar*: importe un router en IPS MC. Debe importar un router a IPS MC antes de poder utilizar IPS MC para configurarlo. No se puede importar un router a menos que exista una configuración IPS inicial en el router (los detalles se proporcionan más adelante en este documento).
- *Configuración*: configure el dispositivo. Por ejemplo, puede configurar un router IPS de Cisco IOS para utilizar uno de los archivos de firma preconfigurados recomendados de Cisco. Los cambios de configuración se almacenan en IPS MC, pero no se envían al router en esta fase.
- *Implementación*: proporcione cambios de configuración al dispositivo real. Durante esta fase, se realizan los cambios realizados en las tareas de configuración en los routers.
- *Tareas adicionales*: IPS MC proporciona una función de descarga automática para descargar automáticamente las actualizaciones de firma de Cisco.com.

Debe comprender este enfoque por fases para utilizar con eficacia IPS MC. Es diferente de las GUI de gestión basadas en dispositivos, como Cisco Router y Security Device Manager (SDM). Las GUI basadas en dispositivos actúan directamente en un único router, mientras que IPS MC está diseñado para funcionar en grupos de routers (y otros dispositivos IPS como Cisco IPS 4200 Series Sensors) en toda la red.

Este documento proporciona información sobre cada una de las tareas del diagrama para ayudarle a utilizar IPS MC para administrar routers IPS de Cisco IOS.

Configuración Inicial de Cisco IOS IPS Routers

Para importar o agregar correctamente un router IPS de Cisco IOS a IPS MC, debe realizar ciertos pasos de configuración inicial en los routers IPS de Cisco IOS. En esta sección se describen esos pasos.

Debe habilitar el protocolo Secure Shell (SSH) en un router IPS de Cisco IOS para la configuración, importación e implementación a través de Cisco IPS MC. Además, el protocolo de intercambio de eventos de dispositivos de seguridad (SDEE) se debe habilitar para los informes de eventos (aunque estas alertas no se envían a IPS MC porque IPS MC se utiliza sólo para el aprovisionamiento, no para la generación de informes). Por último, debe asegurarse de que la configuración del reloj en el router IPS esté sincronizada con el IPS MC.

Complete estos pasos para configurar sus routers IOS IPS:

1. Cree un nombre de usuario local y una contraseña para el router.
```
Router#config terminal
Router(config)#username <username> password <password>
```

2. Habilite el inicio de sesión local en la interfaz de líneas vty.
```
Router#config terminal
Router(config)#line vty 0 15
Router(config-line)#login local
Router(config-line)#exit
```

   Si la interfaz de línea de comandos (CLI) de entrada de transporte o salida de transporte está configurada en la configuración de línea vty, asegúrese de que SSH esté habilitado. Por ejemplo:
```
Router#conf terminal
Router(config)#line vty 0 15
Router(config-line)#transport input ssh telnet
Router(config-line)#exit
```

3. Genere una clave RSA de 1024 bits (si todavía no existe una clave).SSH se habilita automáticamente después de la generación de claves de criptografía.
```
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. Habilite SDEE en el router.
```
Router(config)#ip ips notify sdee
```

5. Habilitar HTTPS.Se requiere HTTP o HTTPS para que IPS MC se comunique con el router con SDEE para recopilar información de eventos.
```
Router(config)#ip http authentication local
Router(config)#ip http secure-server
```

6. Utilice el servidor o el comando clock del protocolo de tiempo de red (NTP) externo para configurar la configuración del reloj en el router IPS.

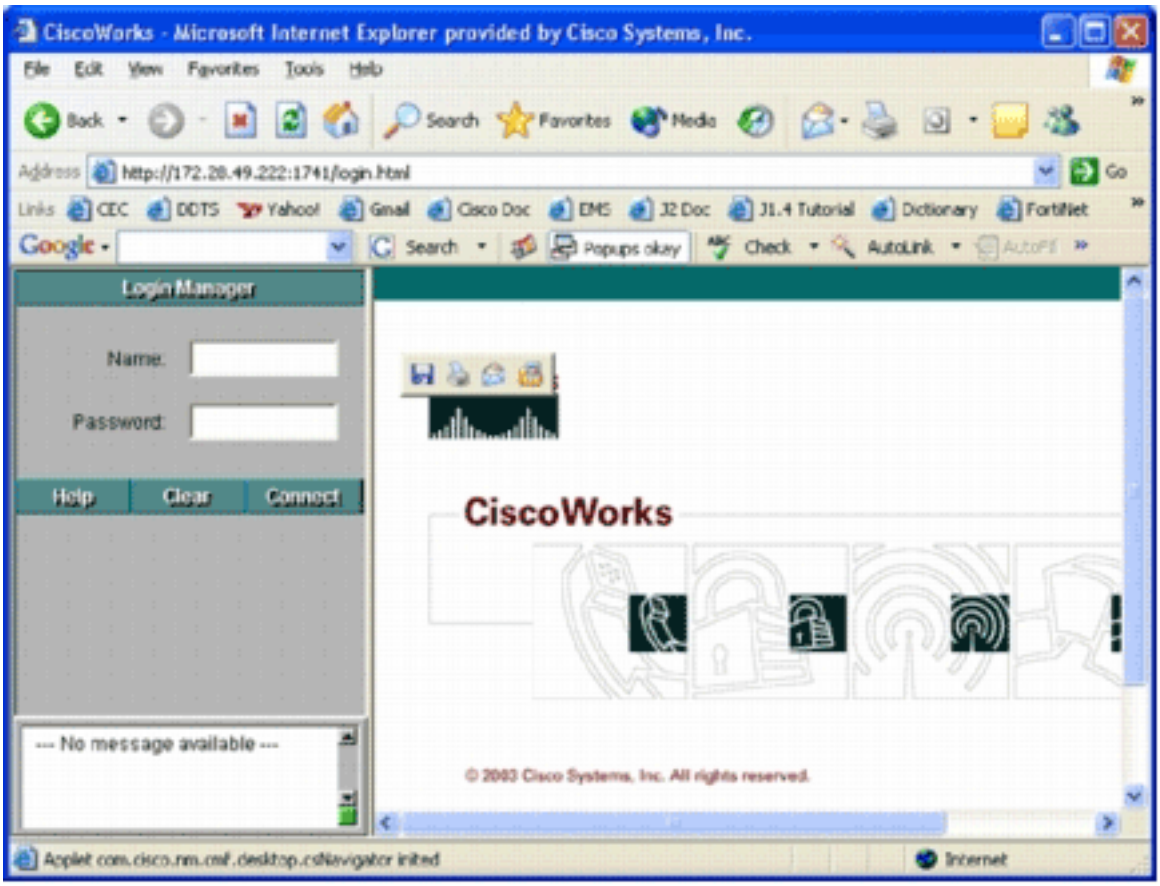
```
Router(config)#clock set hh:mm:ss day month year
```

Ahora, el router IPS de Cisco IOS está listo y se puede importar a IPS MC para una configuración y gestión adicionales.

Importar un router IPS de Cisco IOS a IPS MC

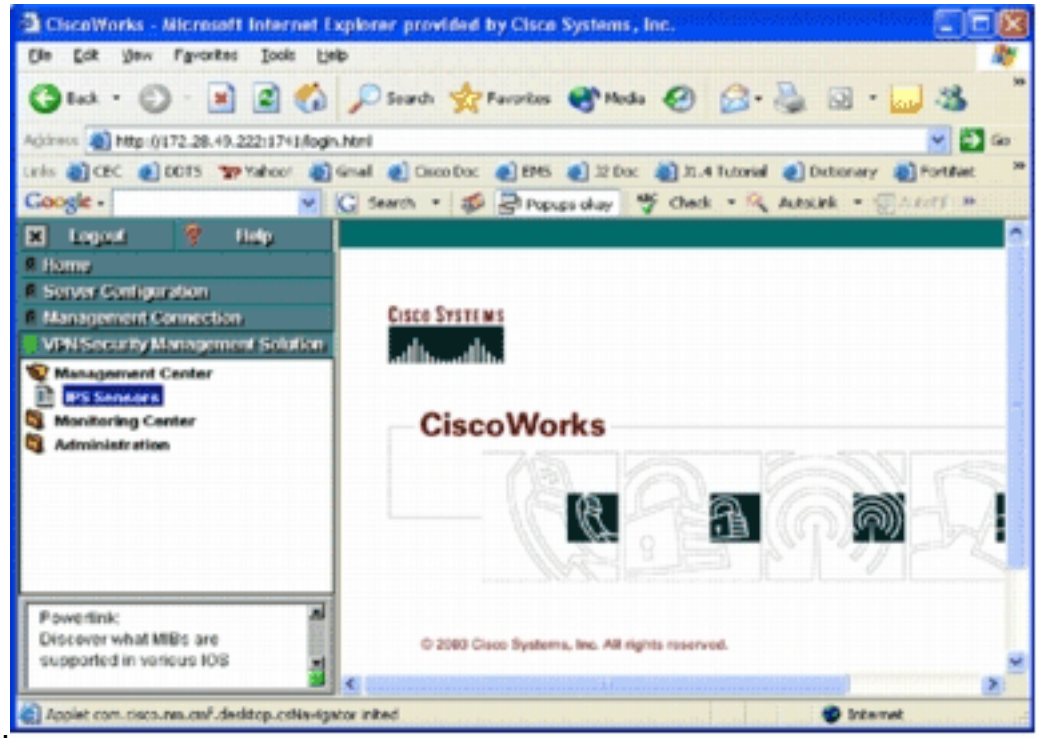
Una vez completada la configuración inicial en el router, puede agregarla (o importarla) en IPS MC.

1. Inicie el explorador web y señale al servidor de CiscoWorks.Aparece el Administrador de inicio de sesión de CiscoWorks.



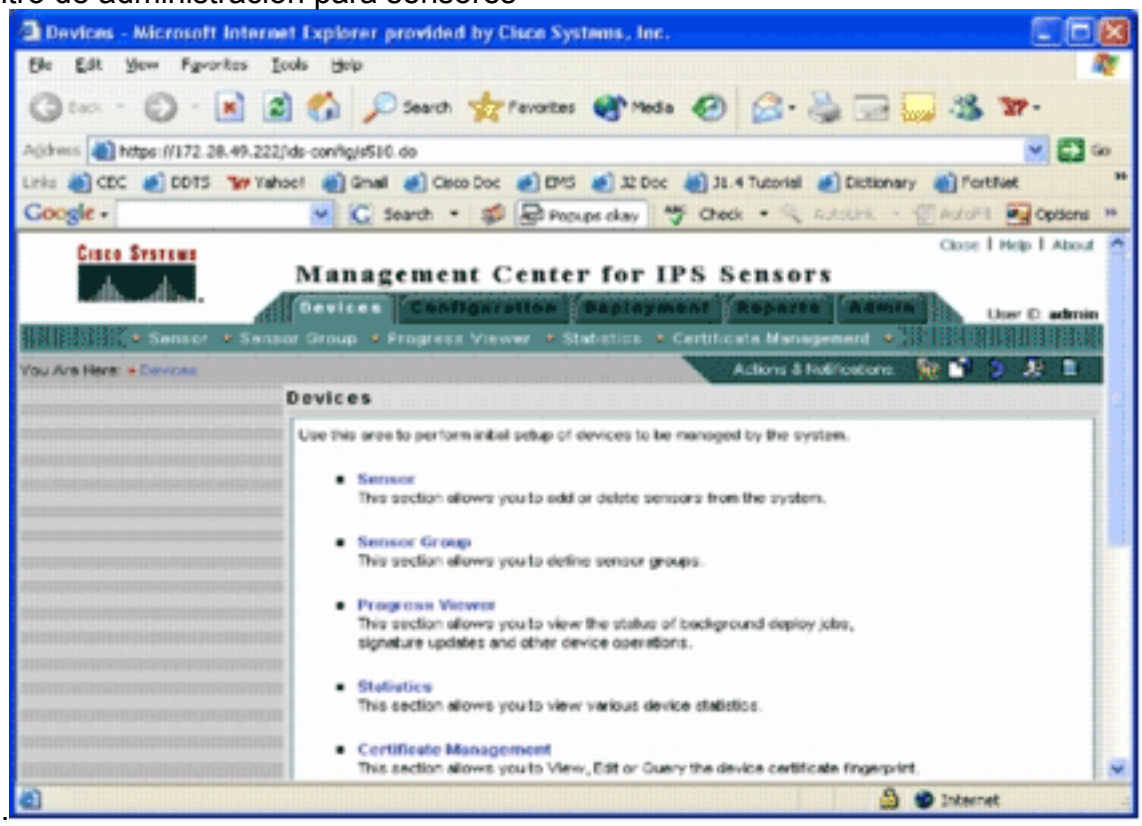
Nota: El número de puerto predeterminado del servidor web es 1741; por lo tanto, debe utilizar una URL similar a http://<*dirección ip del servidor*>:1741/.

2. Introduzca su nombre de usuario y contraseña para iniciar sesión.Aparecerá la página principal de



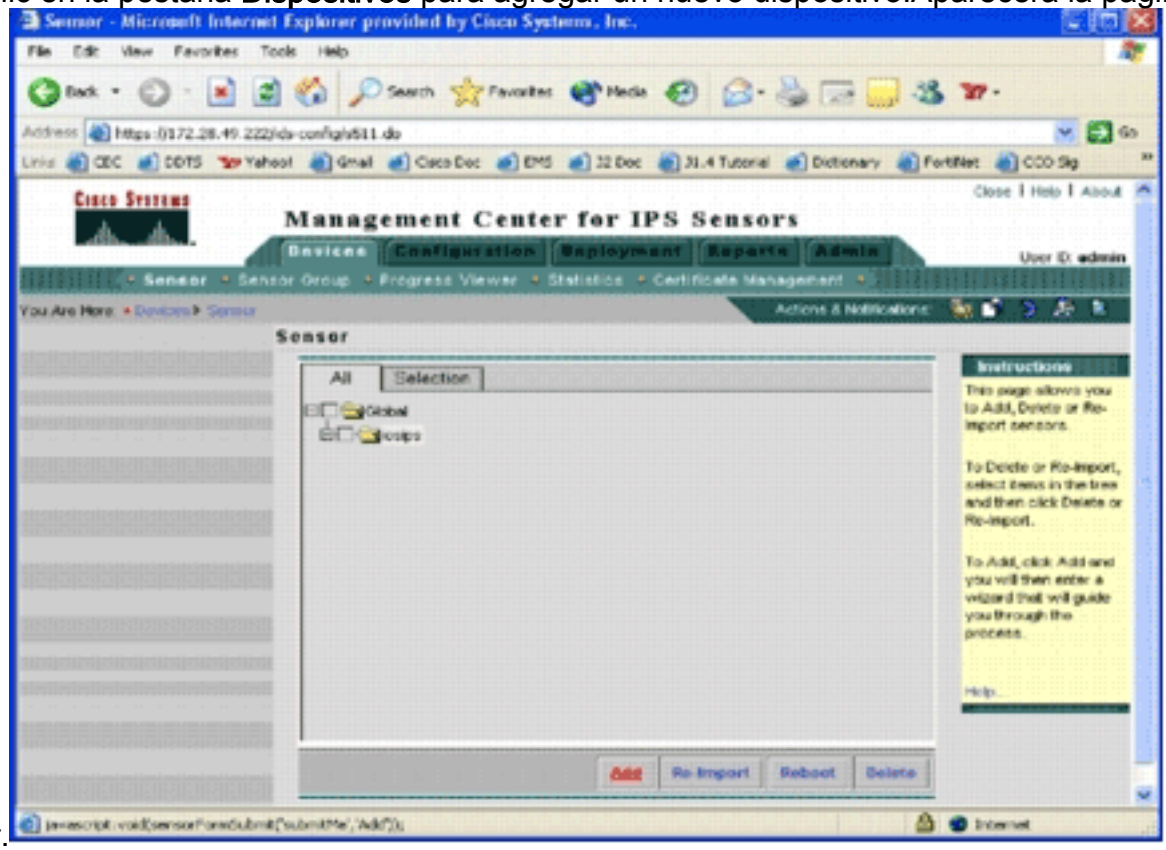
CiscoWorks.

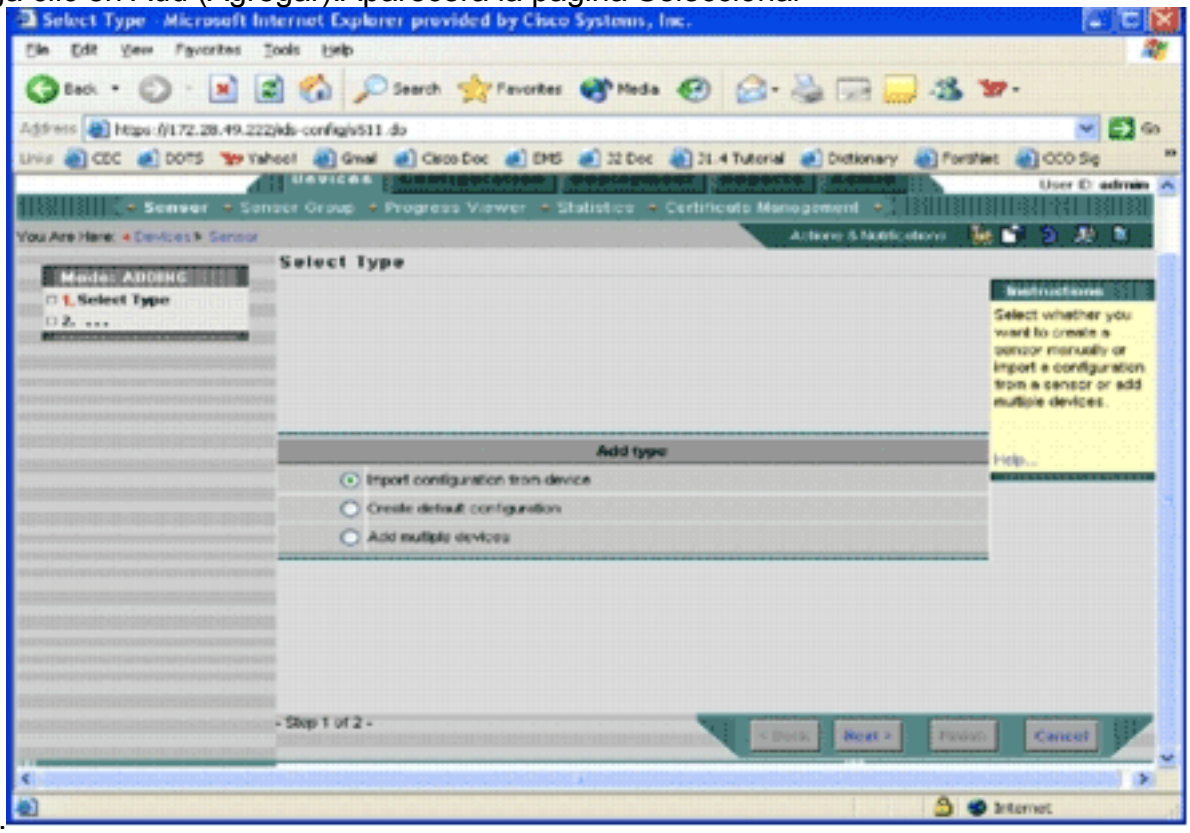
3. En el panel de navegación izquierdo, elija **VPN/Solución de administración de seguridad** y luego elija **Management Center**.Aparecerá la página Management Center for IPS Sensors (Centro de administración para sensores



IPS).Esta página muestra estas cinco fichas:*Dispositivos*: en la ficha Dispositivos, puede realizar la configuración inicial y administrar todos los dispositivos del sistema.*Configuración*: en la ficha Configuración, puede realizar funciones de aprovisionamiento. Puede configurar dispositivos a nivel de dispositivo individual o de grupo. Un grupo de dispositivos puede contener varios dispositivos. Se deben guardar todos los cambios realizados mediante tareas de configuración. La función de configuración no realiza cambios inmediatamente en los dispositivos. Debe utilizar la función de implementación para implementar los cambios.*Implementación*: en la ficha Implementación, puede implementar los cambios de

configuración en los dispositivos. La capacidad de programación proporciona un control flexible del momento en que deben aplicarse los cambios de configuración.*Informes*: en la ficha Informes, puede generar varios informes de operaciones del sistema.*Admin*: en la ficha Admin, puede realizar tareas de administración del sistema, como la administración de bases de datos, la configuración del sistema y la administración de licencias.

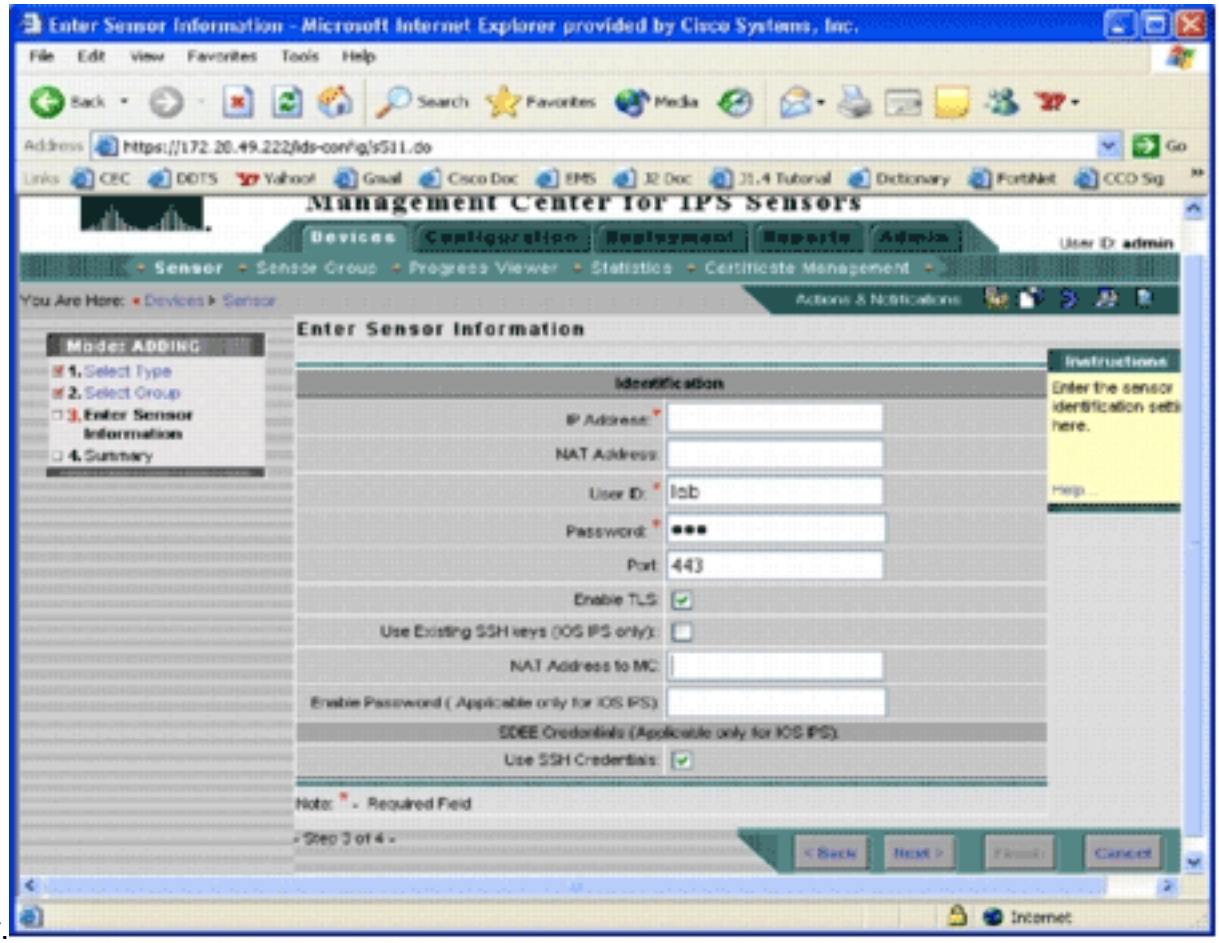
4. Haga clic en la pestaña **Dispositivos** para agregar un nuevo dispositivo.Aparecerá la página 

Sensor.
5. Haga clic en Add (Agregar).Aparecerá la página Seleccionar 

tipo.Debe informar a IPS MC sobre el tipo de función de adición que desea realizar. Esta lista describe

cada opción:*Importar configuración desde el dispositivo*: utilice esta opción para agregar a los dispositivos IPS MC que se ejecutan actualmente en la red.*Crear configuración predeterminada*: utilice esta opción para agregar dispositivos que todavía no se ejecutan en la red.*Agregar varios dispositivos*: utilice esta opción para agregar varios dispositivos. Puede crear un archivo .csv o .xml que contenga toda la información del dispositivo y después importarlo a IPS MC para agregar los dispositivos al mismo tiempo.**Sugerencia:** Los archivos de formato .csv y .xml de ejemplo se encuentran en: InstallDirectory\MDC\etc\ids\ and are named MultipleAddDevices-format.csv y MultipleAddDevices-format.xml, respectivamente.

6. Elija la opción Add type apropiada y haga clic en **Next**.
7. Seleccione el grupo al que desea agregar el router IPS de Cisco IOS o utilice el grupo global predeterminado y, a continuación, haga clic en **Siguiente**.Aparecerá la página Introducir información del sensor.



8. En la página Identificación, introduzca la información de identificación del dispositivo.**Nota:** Si el usuario no tiene derechos de acceso de nivel de privilegio 15, debe proporcionar la contraseña de habilitación. En la última fila de la página Identificación, marque la casilla de verificación **Usar credenciales SSH**.
9. Haga clic en Next (Siguiente).Aparece el cuadro Add Sensor Summary (Agregar resumen de sensor).
10. Haga clic en Finish (Finalizar).El dispositivo se ha agregado correctamente a IPS MC.**Nota:** Si detecta errores durante el proceso de importación, asegúrese de comprobar estos elementos:*Configuración previa*: estas configuraciones son necesarias para que IPS MC se comunique con los routers IPS de Cisco IOS.*Conectividad*: asegúrese de que IPS MC pueda alcanzar los routers Cisco IOS IPS.*Reloj*: verifique las horas en el IPS MC y el router IPS de Cisco IOS. La hora es un componente crítico del certificado https que se utiliza para la autenticación. Los horarios deben estar dentro de las 12 horas. (Las prácticas recomendadas son, como máximo, unas pocas horas.)*Certificado IPS de Cisco IOS*: a

veces, el certificado IPS de Cisco IOS almacenado es incorrecto. Para eliminar un certificado de Cisco IOS IPS, debe quitar el punto de confianza del router Cisco IOS IPS.*Configuración adicional*: si **ip http timeout-policy** se configura con un número bajo de solicitudes máximas, como **ip http timeout-policy idle 600 life 86400 requests 1**, debe aumentar el número máximo de solicitud. Por ejemplo: **ip http timeout-policy idle 600 life 86400 requests 8400**

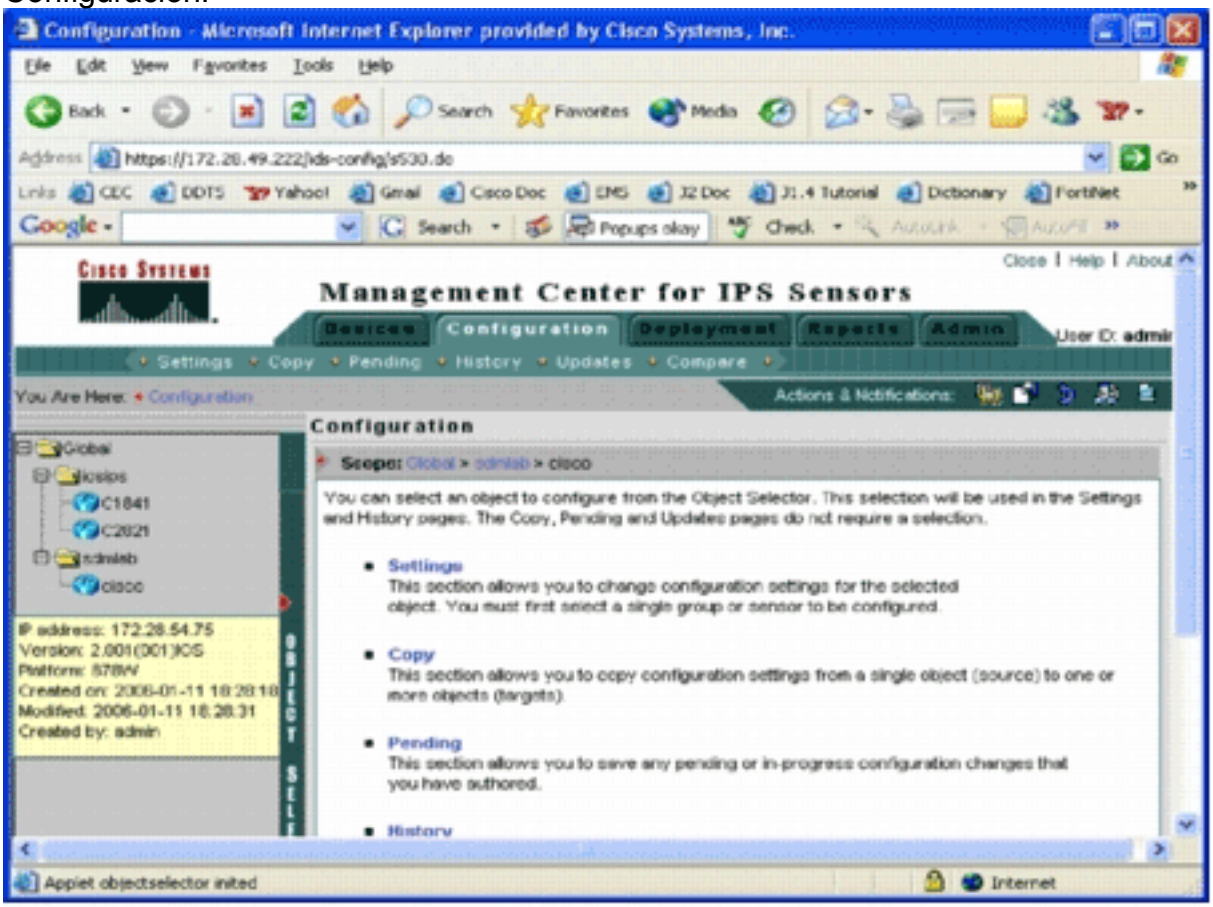
Configuración del router IPS de Cisco IOS para utilizar los archivos de firma preconfigurados

Después de importar el router a IPS MC, debe seleccionar el archivo de definición de firma (SDF) (un archivo basado en texto que incluye las firmas de amenaza que utilizará el router IPS) y la acción que se debe realizar cuando se activa cada firma (por ejemplo, descartar, reinicio TCP, alarma).

Cisco Systems® recomienda que utilice los archivos SDF preconfigurados de Cisco. Actualmente, hay tres de estos archivos: attack-drop.sdf, 128MB.sdf y 256MB.sdf. IPS MC puede descargar automáticamente estos archivos de Cisco.com. Consulte Actualizaciones de firma de descarga automática para obtener más información.

Este procedimiento utiliza un único dispositivo como ejemplo y comienza con un router sin configuración IPS. También puede utilizar este procedimiento para varios dispositivos en un nivel de grupo.

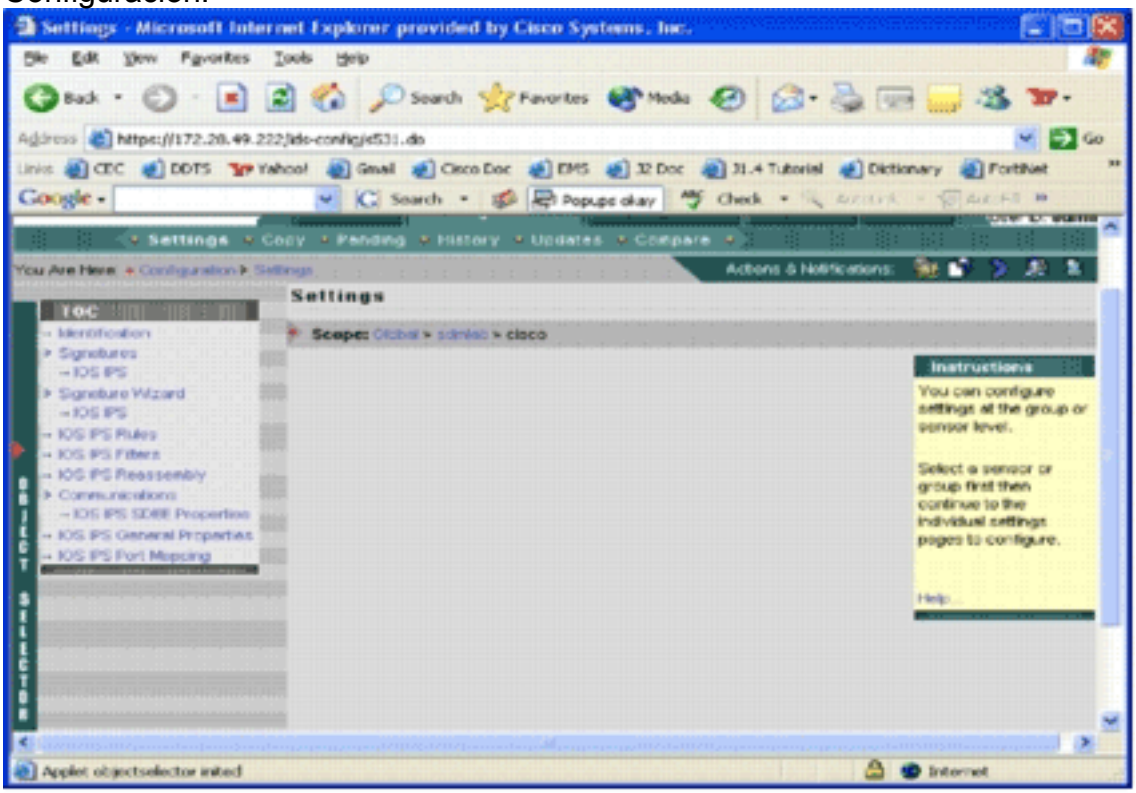
1. Haga clic en la pestaña **Configuración**.Aparecerá la página Configuración.



2. En el Selector de objetos ubicado en el lado izquierdo de la página, elija el router IPS de Cisco IOS que desea configurar.**Nota:** La mayoría de los ajustes de configuración en IPS MC

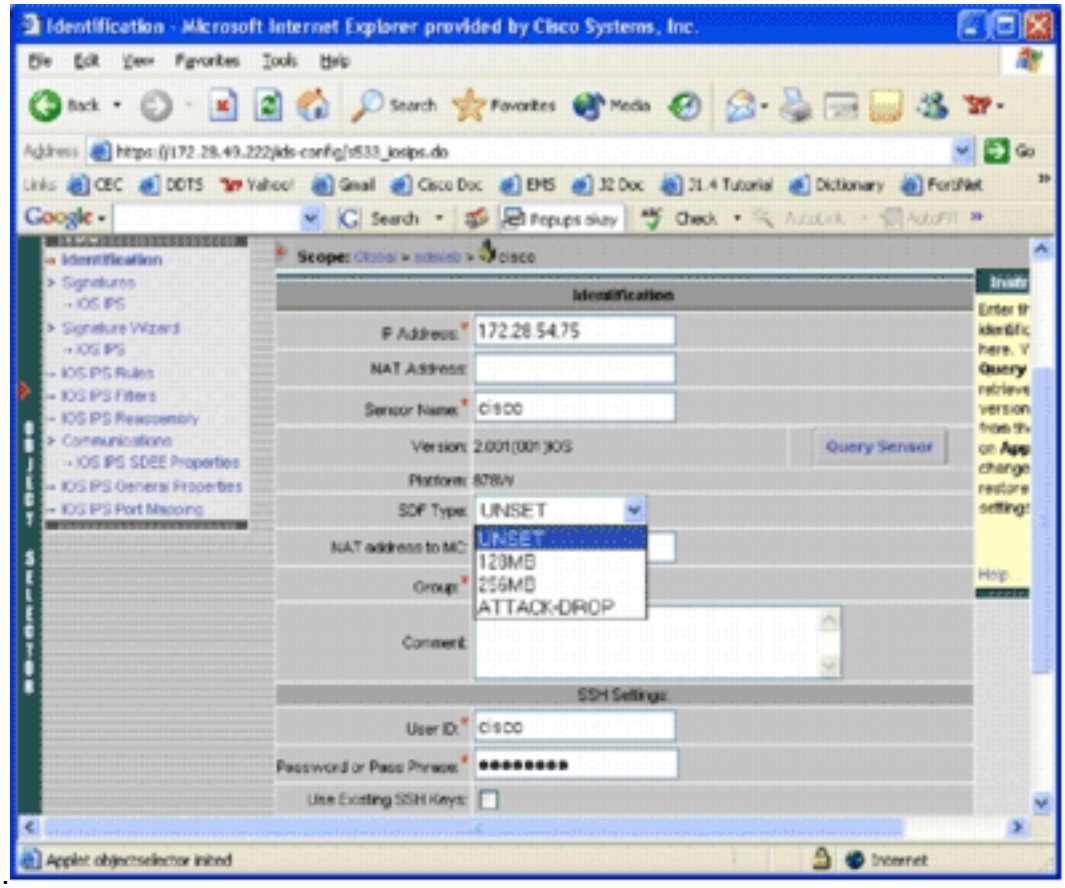
2.2 se pueden configurar en el nivel de grupo y en el nivel de dispositivo individual. Por ejemplo, los grupos global, iosips y sdmlab son todos grupos de objetos configurables. Este ejemplo utiliza un dispositivo-cisco individual del grupo sdmlab.Una vez que seleccione el router que desea configurar, la barra de ruta situada en la parte superior de la página Configuración muestra el alcance de configuración actual. Por ejemplo, el alcance de este ejemplo es *Global > sdmlab > cisco*. *cisco* es el objeto de configuración actual (es decir, el router seleccionado en el Selector de objetos).

3. En la barra de menús Configuración, haga clic en **Configuración**.Aparecerá la página Configuración.



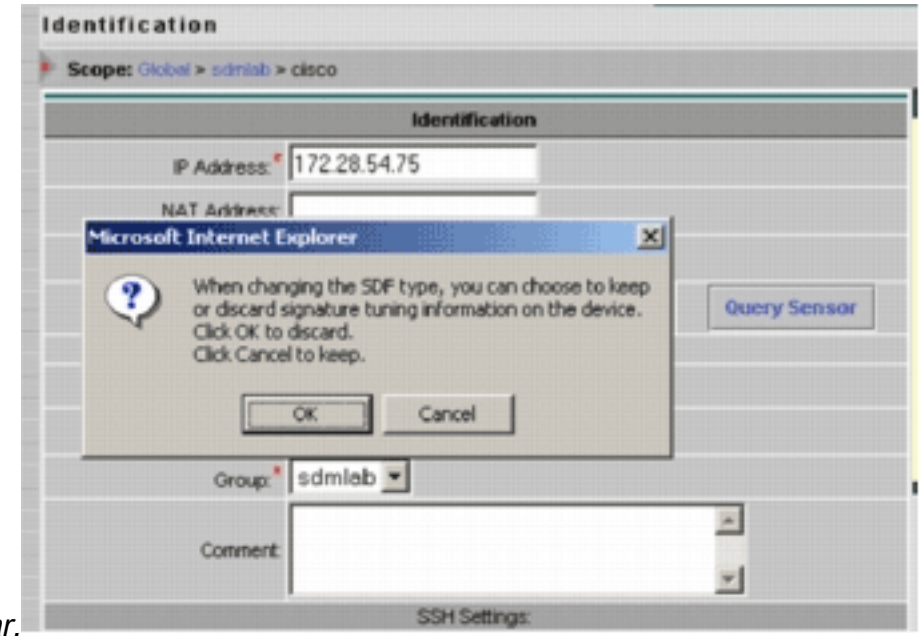
En la página Configuración, puede cambiar la configuración del objeto seleccionado. Los parámetros de configuración específicos de los routers IPS de Cisco IOS se encuentran en la sección TOC ubicada en el lado izquierdo de la página. A continuación se muestra una lista de las tareas disponibles en la sección TOC:*Identificación*: información básica del router IPS de Cisco IOS; aquí puede especificar un archivo SDF predefinido*Firma*: firmas del router IPS de Cisco IOS*Asistente para firmas*: Asistente para firmas para agregar firmas personalizadas*Reglas IPS de Cisco IOS*: para configurar reglas IPS de Cisco IOS que se utilizan para aplicar a interfaces*Filtros IPS de Cisco IOS*: filtros IPS de Cisco IOS*Reensamblado de Cisco IOS IPS*: configuración de reensamblado virtual de IP de interfaz*Propiedades de Cisco IOS IPS SDEE*: para configurar la configuración de SDEE*Propiedades generales de Cisco IOS IPS*: configuraciones adicionales relacionadas con Cisco IOS IPS

4. Elija **Identificación** para configurar los archivos SDF preconfigurados.Aparecerá la página

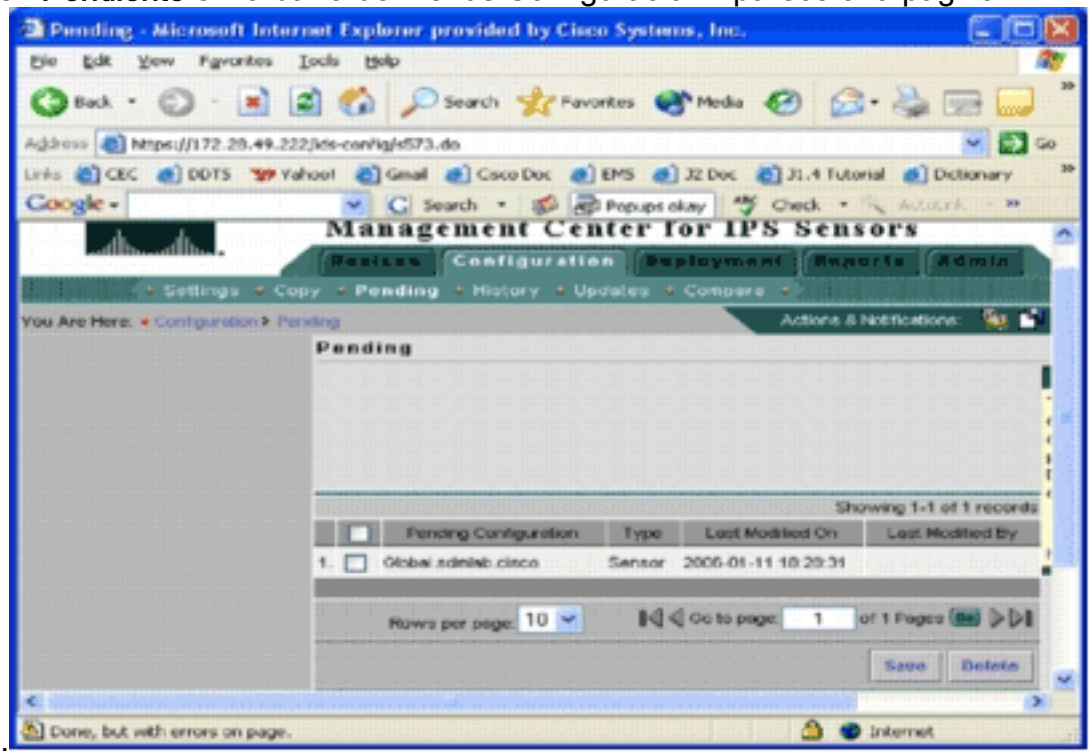


Identificación.

5. En la lista desplegable SDF Type (Tipo de SDF), elija el SDF adecuado preconfigurado y, a continuación, haga clic en **Apply** para aplicar los cambios.Cisco IOS IPS admite más de 1600 firmas, lo que supera la capacidad de memoria de los routers para aceptar. Los SDF se han desarrollado como una forma conveniente de seleccionar y cargar las firmas más vitales. Actualmente, puede elegir entre tres SDF. El tamaño varía para permitirle seleccionar un archivo SDF según la capacidad de DRAM de sus routers. Las opciones disponibles se describen a continuación:UNSET: el tipo SDF no está configurado.ATTACK-DROP: este SDF es para routers con 64 MB de DRAM.256MB: este SDF es para routers con 256 MB de DRAM.128 MB: este SDF es para routers con 128 MB de DRAM.**Nota:** Los SDF de 128 y 256 MB requieren un motor de 2,001 o más. Esta información está disponible en el campo **Settings > Identification UI > Version .Advertencia:** IPS MC no incluye funciones de administración de memoria para los routers Cisco IOS IPS. Tenga cuidado al seleccionar los archivos SDF para el router IPS de Cisco IOS. Asegúrese de que el router IPS de Cisco IOS tenga memoria suficiente para ejecutar el archivo SDF seleccionado.**Nota:** Cuando cambie el tipo SDF, puede recibir este mensaje: *Al cambiar el tipo de SDF, puede elegir mantener o descartar la información de ajuste de firma en el dispositivo. Haga clic en Aceptar para descartar. Haga clic en Cancelar para*



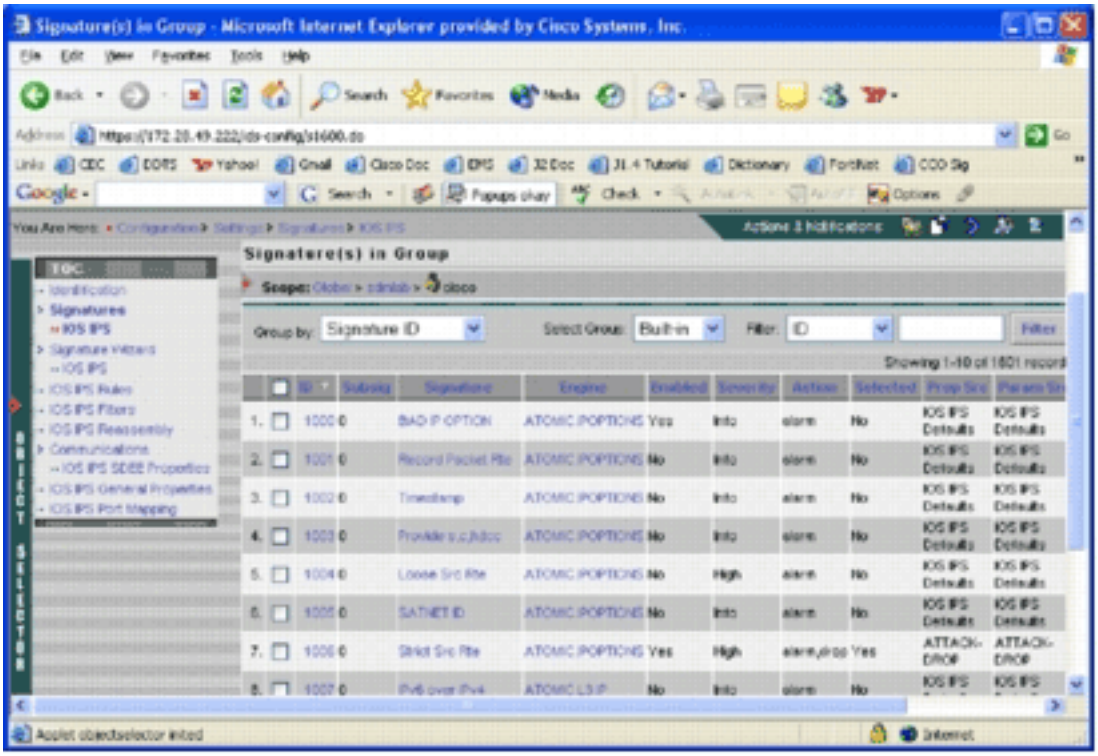
continuar.

6. Haga clic en **Cancelar** para mantener la información de ajuste de la firma.Ahora que ha elegido correctamente un SDF preconfigurado para el router-cisco, puede realizar ajustes de firma adicionales como agregar o editar, o incluso crear sus propias firmas, o puede omitir las tareas de ajuste de firma e ir directamente a Creación de una Regla para Aplicar a las Interfaces.
7. Haga clic en **Pendiente** en la barra de menús Configuración.Aparecerá la página Pendiente. 

En este momento, se completa la tarea de configuración. Sin embargo, debe completar la tarea de implementación para implementar los cambios en el dispositivo de destino.

Modificar las firmas SDF predeterminadas

Después de seleccionar un archivo SDF preconfigurado para un router, puede realizar tareas adicionales de ajuste de firma. Puede agregar, editar, eliminar y modificar firmas para que se ajusten mejor a sus necesidades, o puede crear sus propias firmas cuando sea necesario. Este ejemplo utiliza IPS MC para agregar firmas adicionales y modificar las acciones. Esta imagen muestra la interfaz de configuración de firma.



Puede utilizar la configuración de firma para habilitar o deshabilitar, seleccionar o anular la selección, agregar una firma, eliminar una firma, cambiar acciones de firma y editar parámetros de firma. Utilice el Asistente para firmas situado a la izquierda para crear firmas personalizadas.

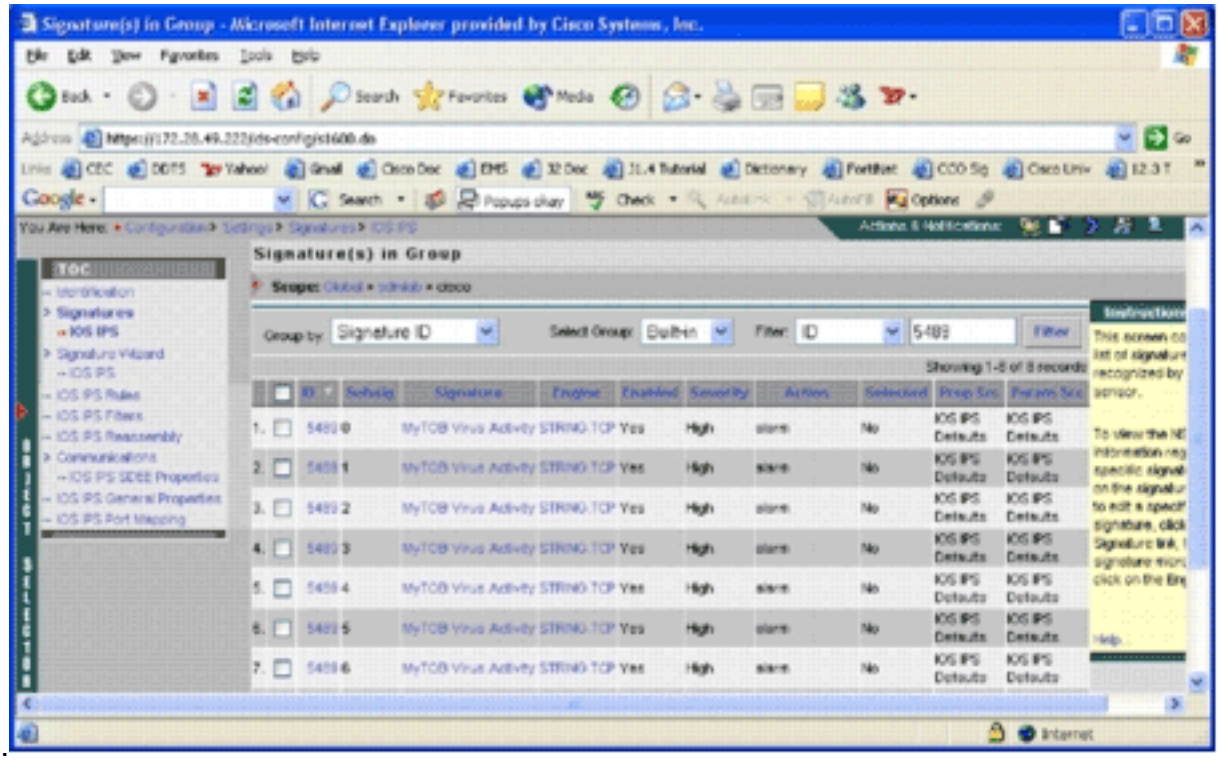
En la interfaz de usuario de configuración de firma, se muestra cierta información de forma predeterminada. Selected hace referencia a si la firma se incluirá en el archivo SDF enviado al router. Si no se selecciona una firma, no se agregará. Habilitado sólo se aplica si se selecciona una firma. Cuando se desactiva una firma, los motores IPS no enviarán eventos para esa firma específica. Si una firma no está seleccionada, también se inhabilita automáticamente.

Las dos últimas columnas (Prop Src y Param Src) indican de dónde proceden la firma y su parámetro, respectivamente. La firma podría haberse tomado de archivos SDF preconfigurados o de los valores predeterminados de fábrica que puede encontrar en las actualizaciones del archivo IOS-Sxxx.zip (se muestra como valores predeterminados de IOS IPS). Estos valores también se aplican a la columna de parámetros.

Mientras agrega firmas a los routers IPS de Cisco IOS, se deben tener en cuenta las consideraciones de memoria. Si agrega más firmas de las que puede procesar el router IPS de Cisco IOS, IPS MC no podrá implementar los cambios de configuración en los dispositivos.

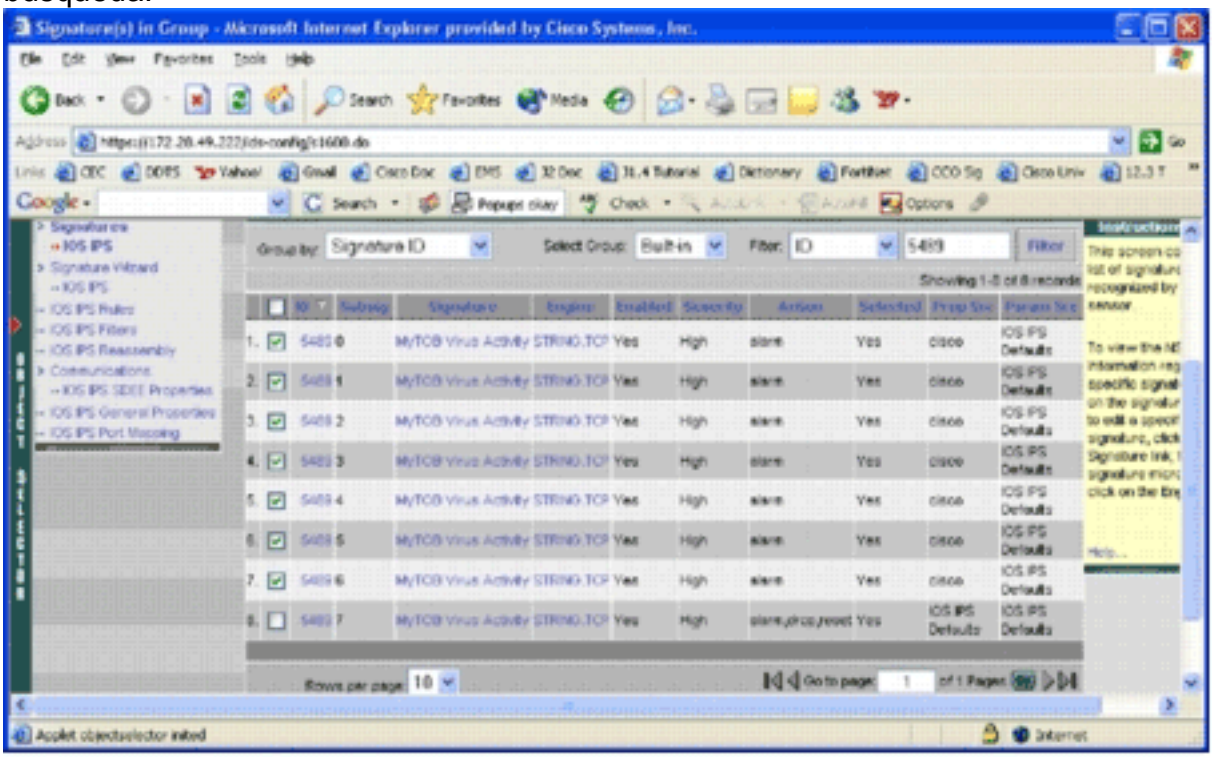
Complete estos pasos para agregar firmas 5489/x al router IPS de Cisco IOS:

1. Seleccione **Configuration**, y luego utilice el Selector de objetos para seleccionar el router IPS de Cisco IOS para el que desea configurar las firmas IPS.
2. Elija **Configuration > Settings > Signations > IOS IPS**.Aparece la firma de la página



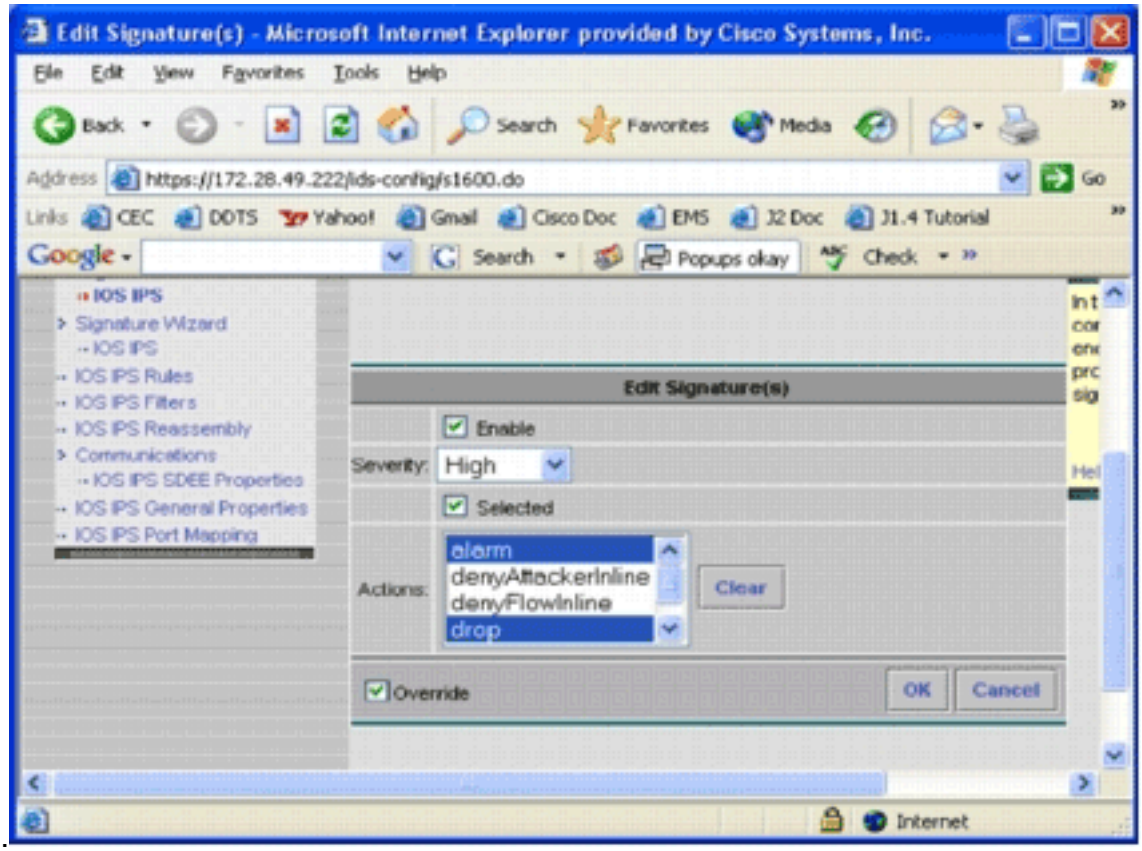
Grupo.

3. En la lista de firmas resultante, seleccione Filtrar por ID y escriba ID de firma 5489.
4. Haga clic en **Filtro** para buscar firmas.Aparecerán los resultados de la búsqueda.



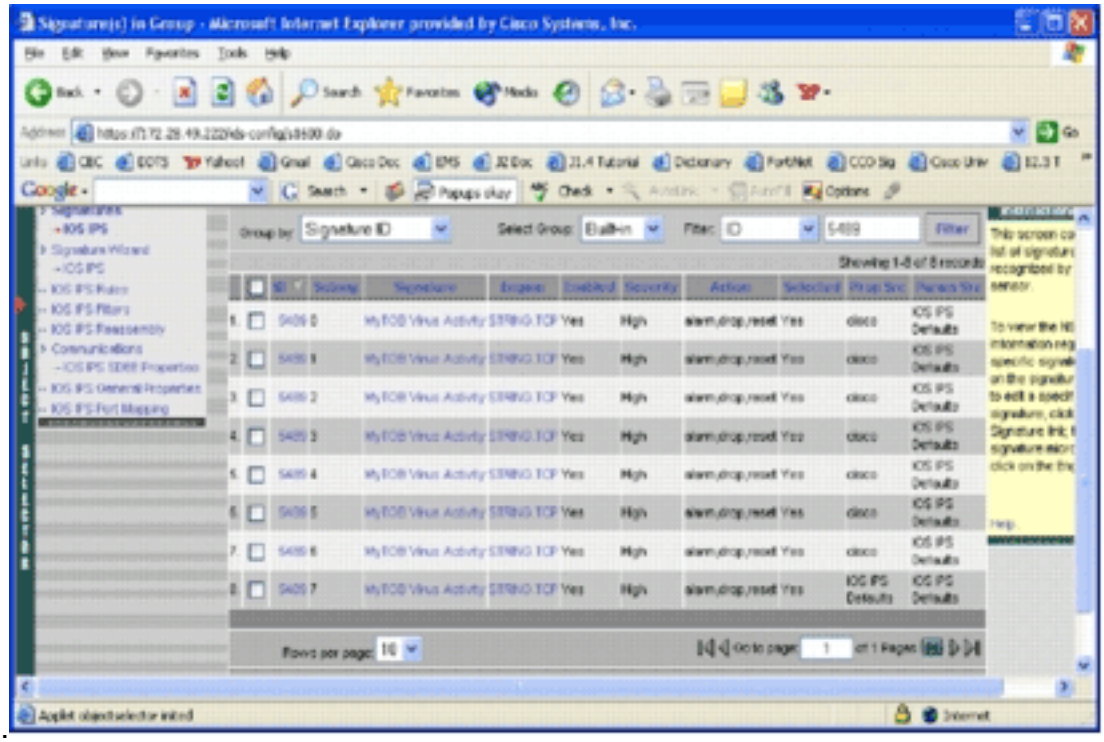
Nota: IPS MC no admite la nueva categorización disponible en Cisco SDM.

5. Marque la casilla de verificación junto a las firmas que no se han seleccionado y haga clic en **Seleccionar** en la barra de herramientas inferior.
6. Haga clic en **Editar** para cambiar las acciones de firma.Aparecerá la página Editar



firmas.

7. Marque la casilla de verificación **Selected** y seleccione **alarm**, **drop** y **reset** en la lista Acciones.
8. Marque la casilla de verificación **Override** y, a continuación, haga clic en **OK**.Todas las firmas se modifican con las acciones


deseadas.

9. Vaya a la tarea Pendiente y guarde todos los cambios. Esto completa la tarea de configuración.**Sugerencia:** Preste mucha atención a la columna Prop Src. Después de la modificación, el origen cambió al dispositivo denominado *cisco*, lo que significa que toda la información de ajuste se guarda por separado de los archivos SDF preconfigurados predeterminados. Este mecanismo ofrece a IPS MC la capacidad de conservar los cambios de firma personalizados.

En la sección anterior, cuando cambió los tipos de archivo SDF, el MC IPS le preguntó si deseaba mantener la información de ajuste de firmas. Esta es la información de ajuste de firma a la que se hace referencia.

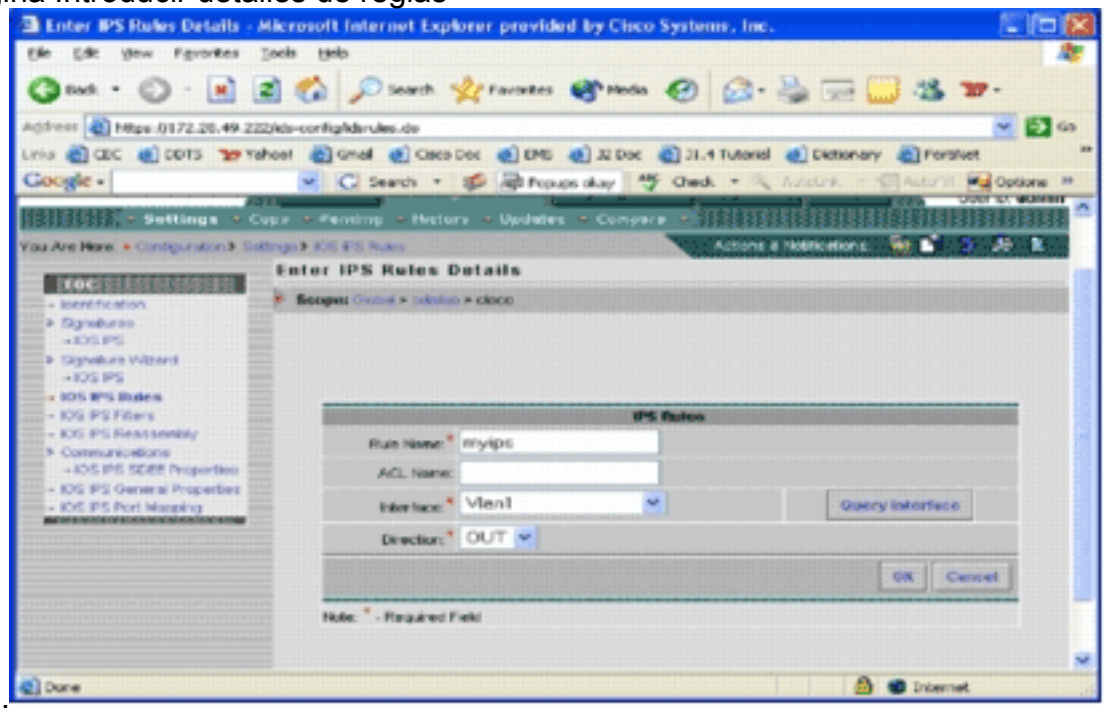
Seleccionar firmas personalizadas

Si no desea utilizar los archivos SDF preconfigurados predeterminados, puede utilizar los pasos especificados en la sección Modificar firmas SDF Predeterminadas para seleccionar firmas de ajuste para sus dispositivos. En la página de identificación, debe asegurarse de que el tipo SDF es UNSET. Consulte el paso 3 en Configure el Cisco IOS IPS Router para Utilizar los Archivos de Firma Predeterminados.

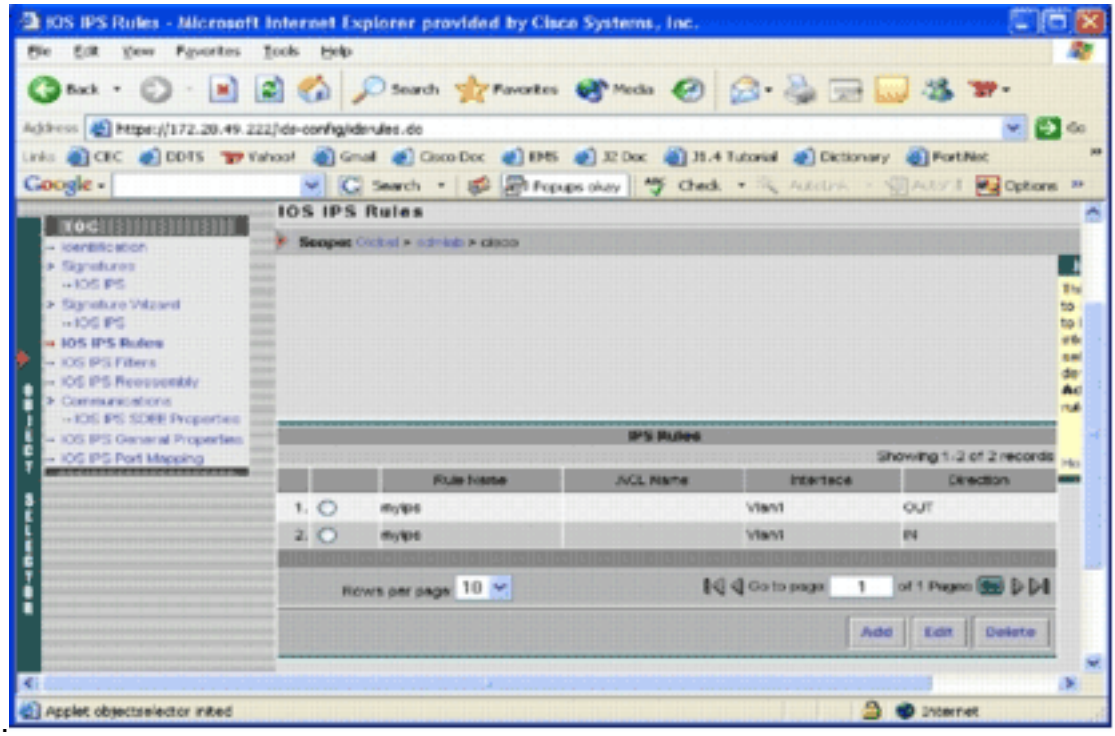
Crear una regla para aplicar a las interfaces

Después de ajustar la firma, debe habilitar IPS en los routers Cisco IOS. Para habilitar IPS en el router, debe crear una regla IPS y aplicarla al menos a una interfaz.

1. Seleccione **Configuration** y luego utilice el Selector de objetos para seleccionar el router IPS de Cisco IOS que desea configurar. Verifique en la barra de trayectoria que su alcance se encuentra en el nivel del dispositivo, no en un nivel de grupo.
2. Seleccione **Configuration > Settings > IOS IPS Rules** y luego haga clic en **Add**.Aparecerá la página Introducir detalles de reglas IPS.



3. Introduzca la información para el nombre de regla y la interfaz a la que desea aplicar la regla y dirección.
4. Click OK.Aparecerá la página Reglas IPS de



IOS. De manera similar, puede crear reglas para ambas direcciones para una interfaz.

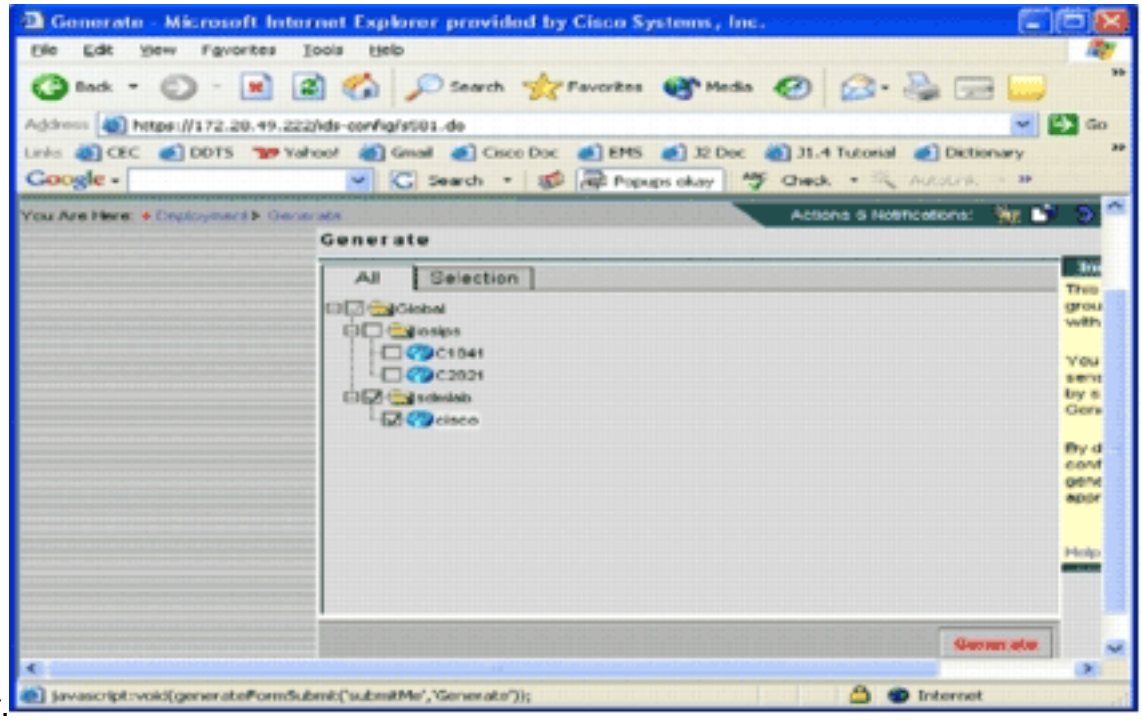
5. Debe guardar los cambios de configuración y pasar por el proceso de implementación para entregar los cambios al dispositivo o grupo de dispositivos afectados.También puede realizar otras configuraciones relacionadas con IPS, pero todas las demás tareas son opcionales y no son necesarias. Puede encontrar todas las opciones a la izquierda de la interfaz de usuario de configuración. Este documento no cubre las opciones de configuración opcionales.

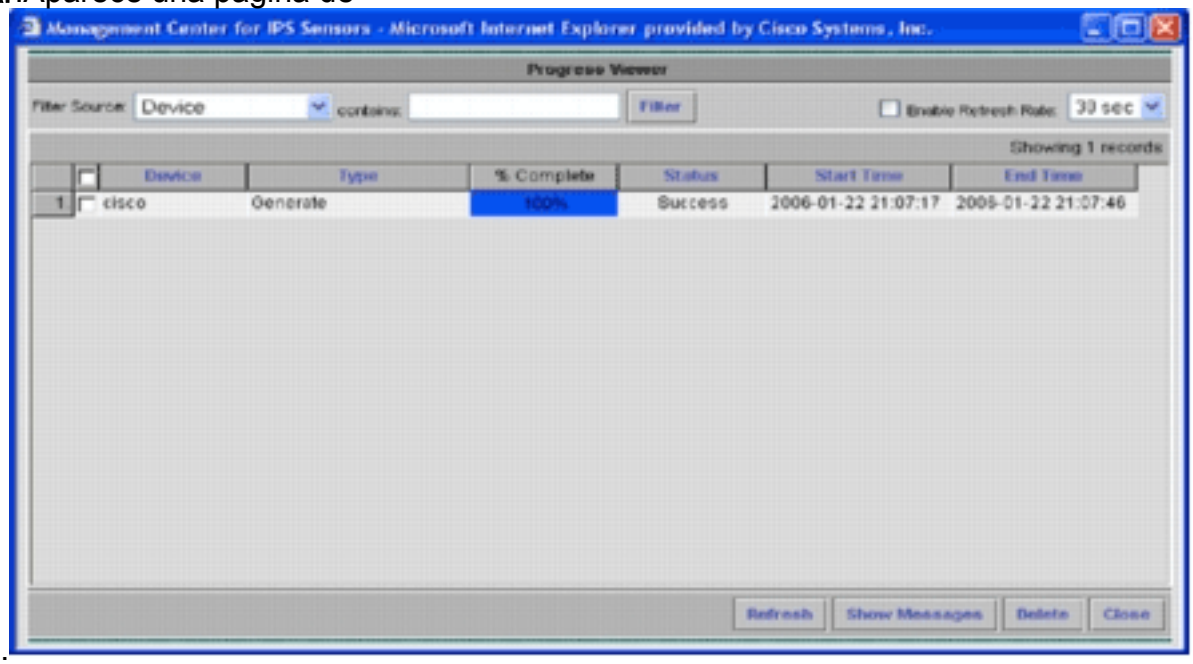
Implementación de la configuración

Después de realizar todos los cambios de configuración, debe utilizar la tarea de implementación para registrar los cambios en los dispositivos. Todas las configuraciones que ha realizado hasta ahora se guardan localmente en el servidor IPS MC.

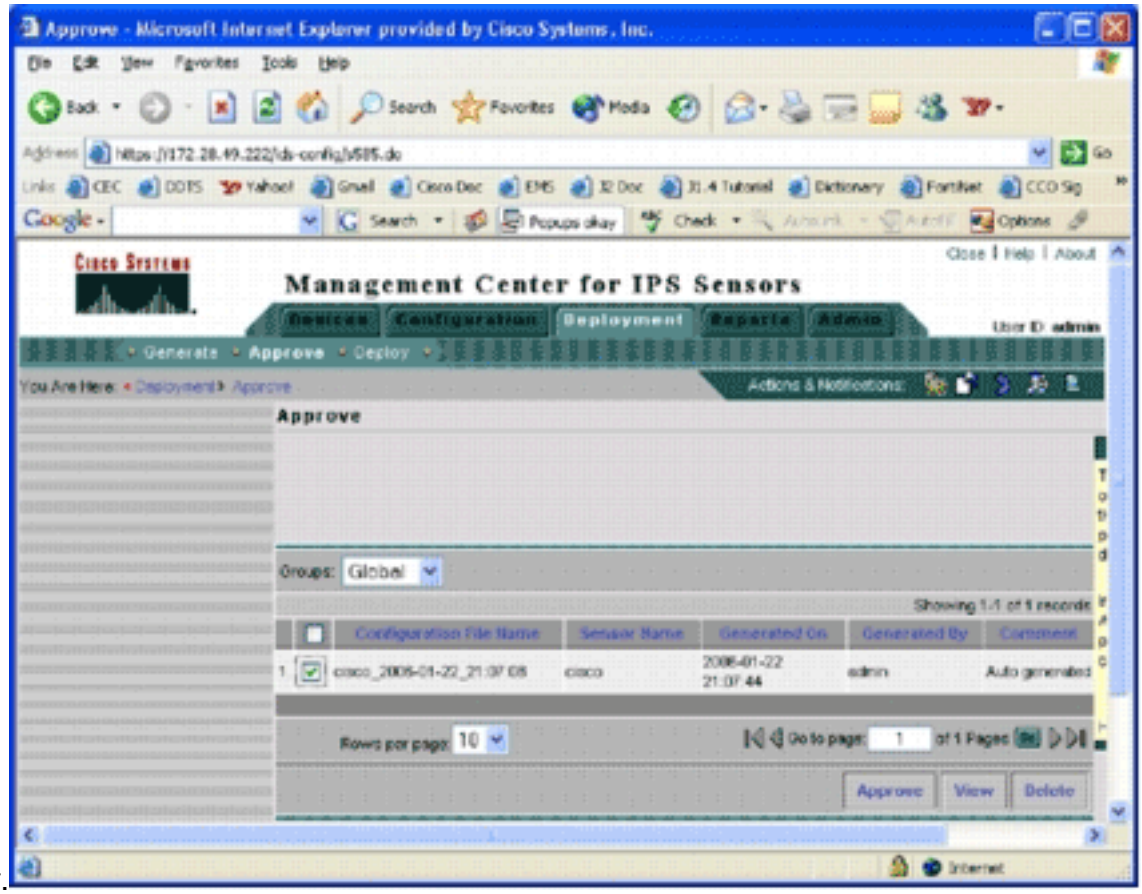
Para implementar los cambios de configuración, vaya a la página Implementación y complete estos pasos:

1. Haga clic en la pestaña **Implementación** y elija **Generar** para generar cambios de configuración.Aparecerá la página

Generar. 

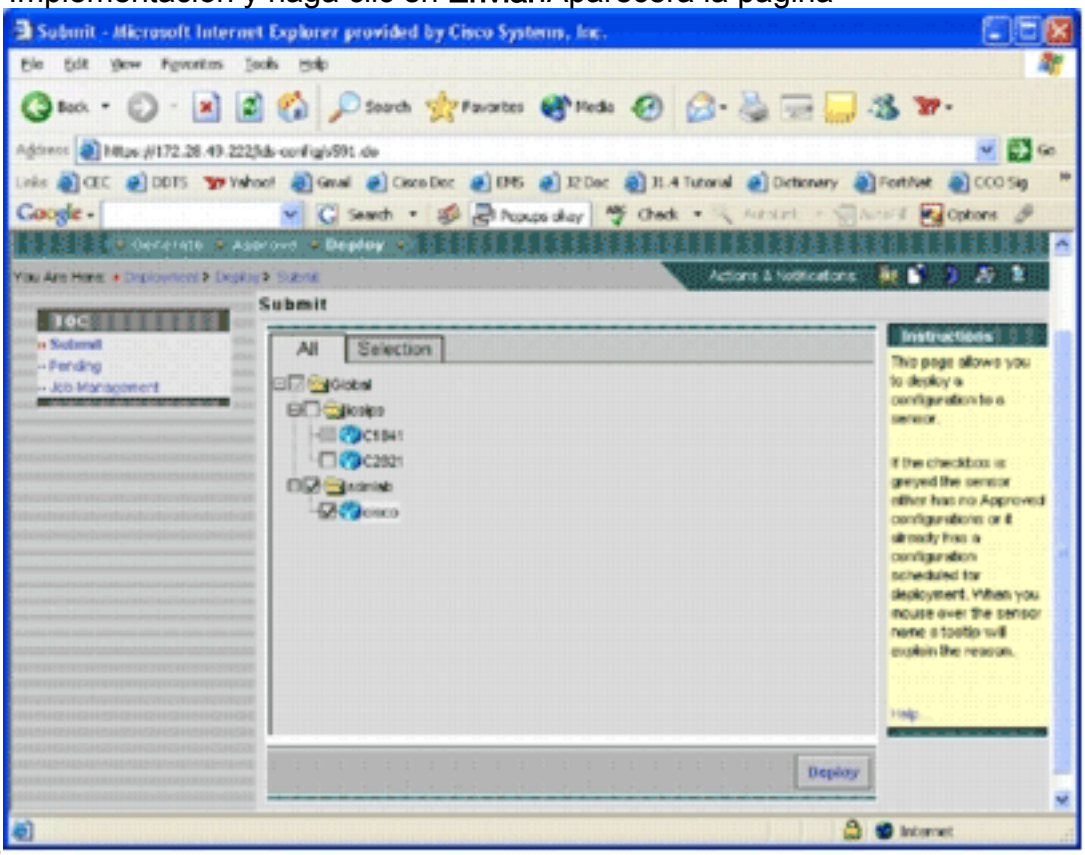
2. Elija el dispositivo *cisco* que acaba de configurar y haga clic en **Generar**.
3. Haga clic en **Aceptar** para aceptar la configuración generada y después haga clic en **Aceptar**.Aparece una página de estado. 

4. Haga clic en **Actualizar** hasta que la tarea de generación se complete correctamente.
5. Haga clic en **Aprobar** en la barra de menús Implementación y en el grupo sdmlab para ver una lista de configuraciones que necesitan aprobación.Aparecerá la página



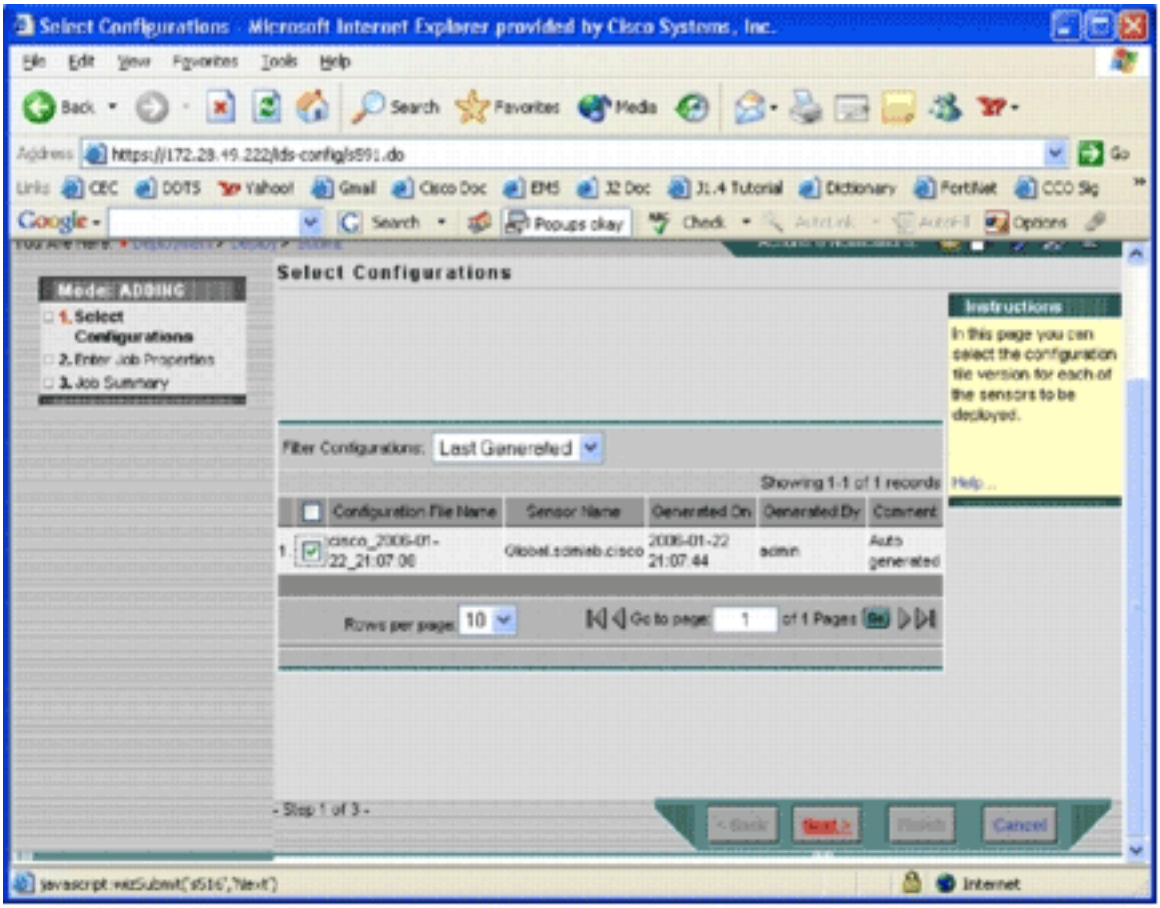
Aprobar.

6. Elija las tareas y haga clic en **Aprobar**.Haga clic en **Implementar** ubicado en la barra de menús Implementación y haga clic en **Enviar**.Aparecerá la página

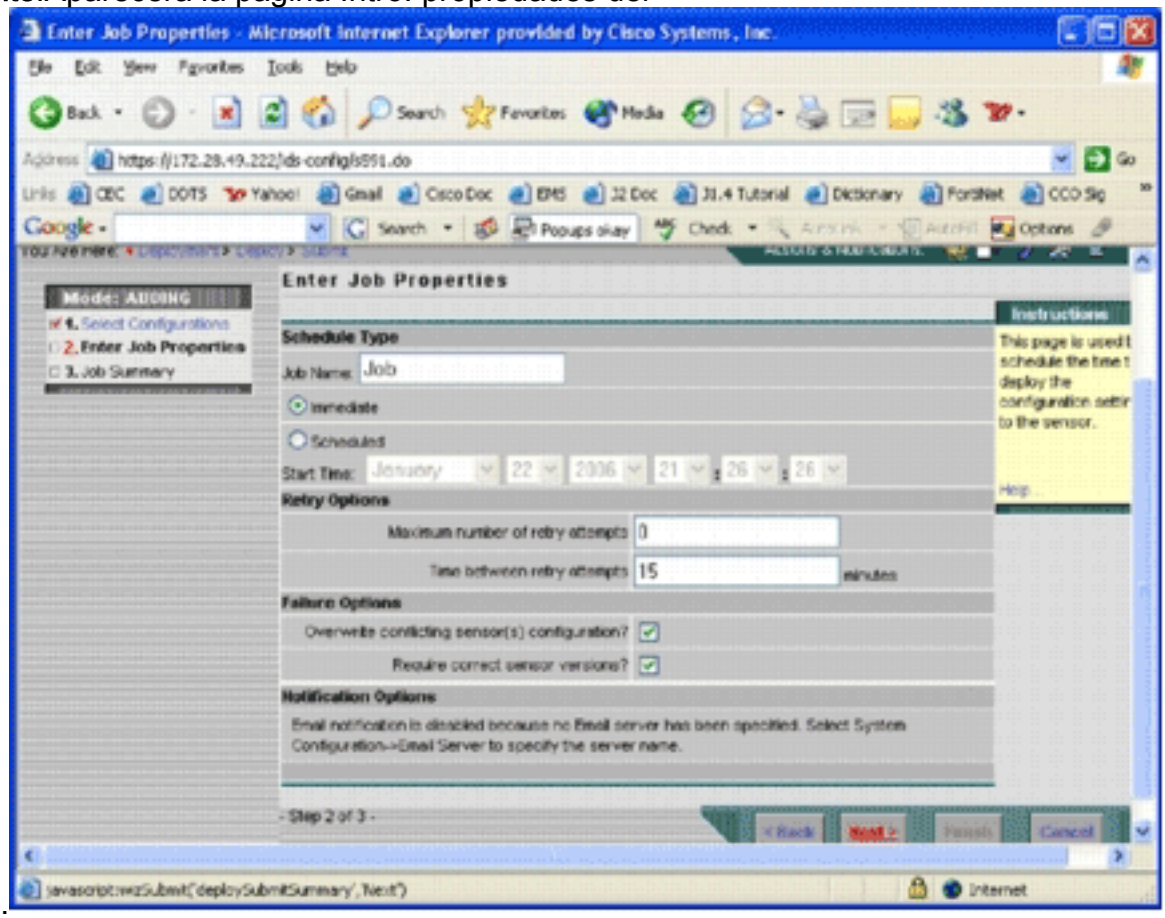


Enviar.

7. Elija los dispositivos para los que desea enviar la tarea de implementación.
8. Seleccione el dispositivo *cisco* y haga clic en **Implementar**.Aparecerá la página Seleccionar configuraciones.

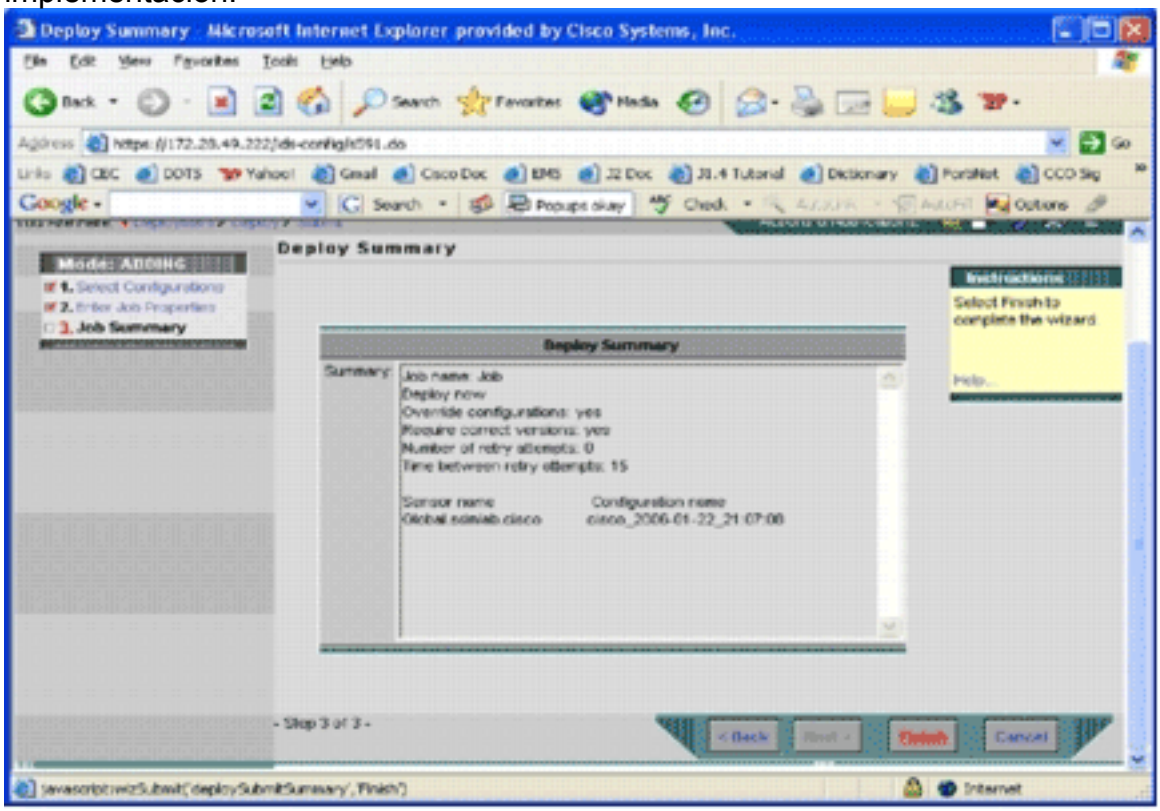


9. Elija la configuración que acaba de realizar en el dispositivo *cisco* y haga clic en **Siguiente**.Aparecerá la página Intro. propiedades del trabajo.

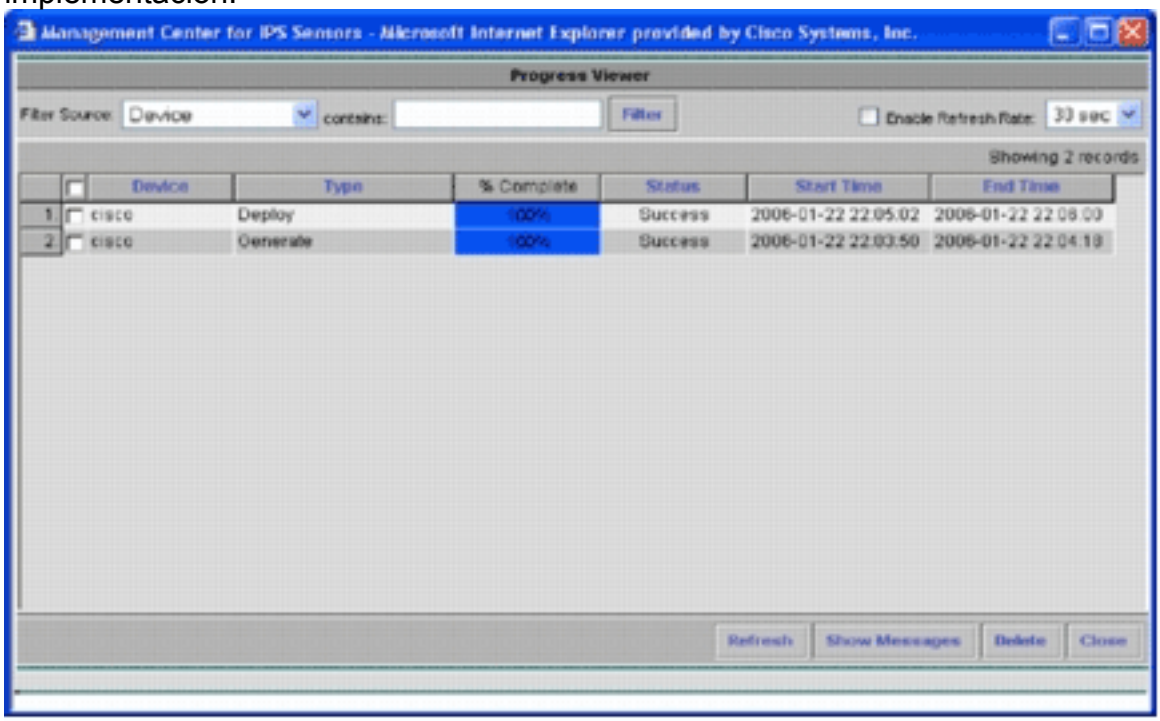


10. Puede implementar inmediatamente los cambios o programar una tarea para que lo haga más adelante. En este ejemplo, elija la opción **Inmediate** y luego haga clic en **Next**.Se muestra un breve resumen del trabajo que está listo para su

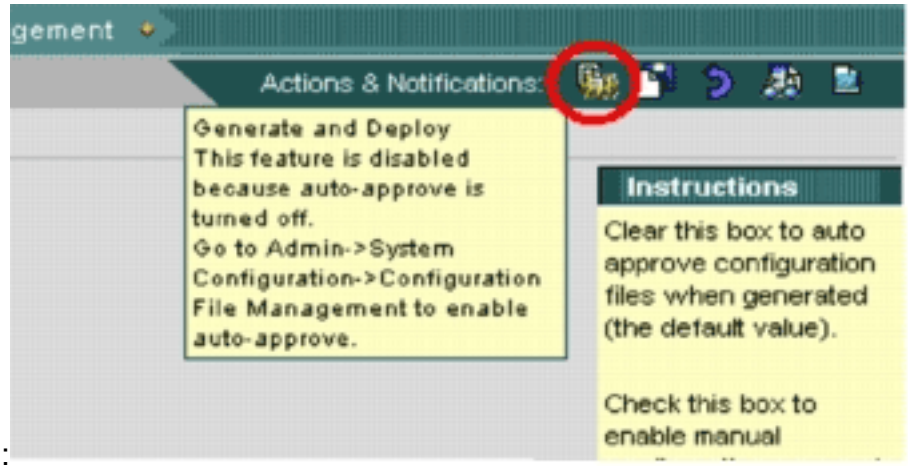
implementación.



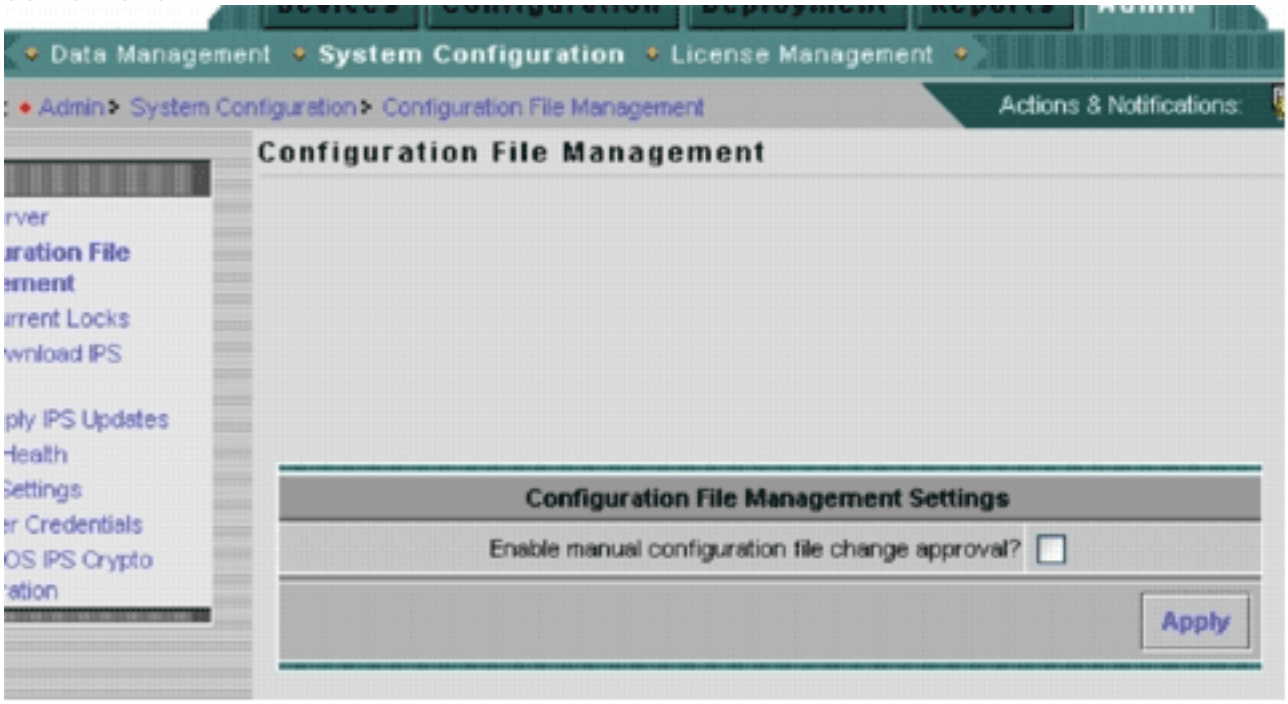
11. Haga clic en Finish (Finalizar).Al final de la implementación, un cuadro de diálogo muestra el estado del proceso de implementación.

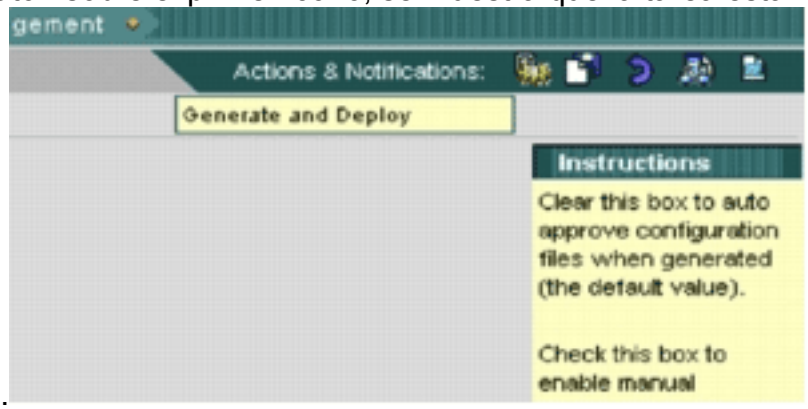


Ha implementado correctamente las configuraciones de Cisco IOS IPS en el dispositivo. Cuando configura varios dispositivos, puede realizar cambios de configuración en el nivel de grupo y luego aplicar los cambios a todos los routers IPS de Cisco IOS que pertenecen al mismo grupo.**Sugerencia:** Este proceso es largo, pero hay disponible una función de entrega rápida. Cuando utilice esta función, no tendrá que pasar por el proceso **Generate > Apruebe > Deploy**. Complete estos pasos para utilizar la función:En la parte superior de la interfaz de usuario hay una fila de iconos pequeños. Con el ratón sobre el primer icono, y vea la sugerencia de la herramienta que se muestra en esta

imagen: 

Para habilitar la tarea Generar e Implementar, vaya a **Admin > System Configuration > Configuration File Management**, y desmarque la casilla de verificación **Enable manual configuration file change authorization**.



Con el ratón sobre el primer icono, se muestra que la tarea está activada. 

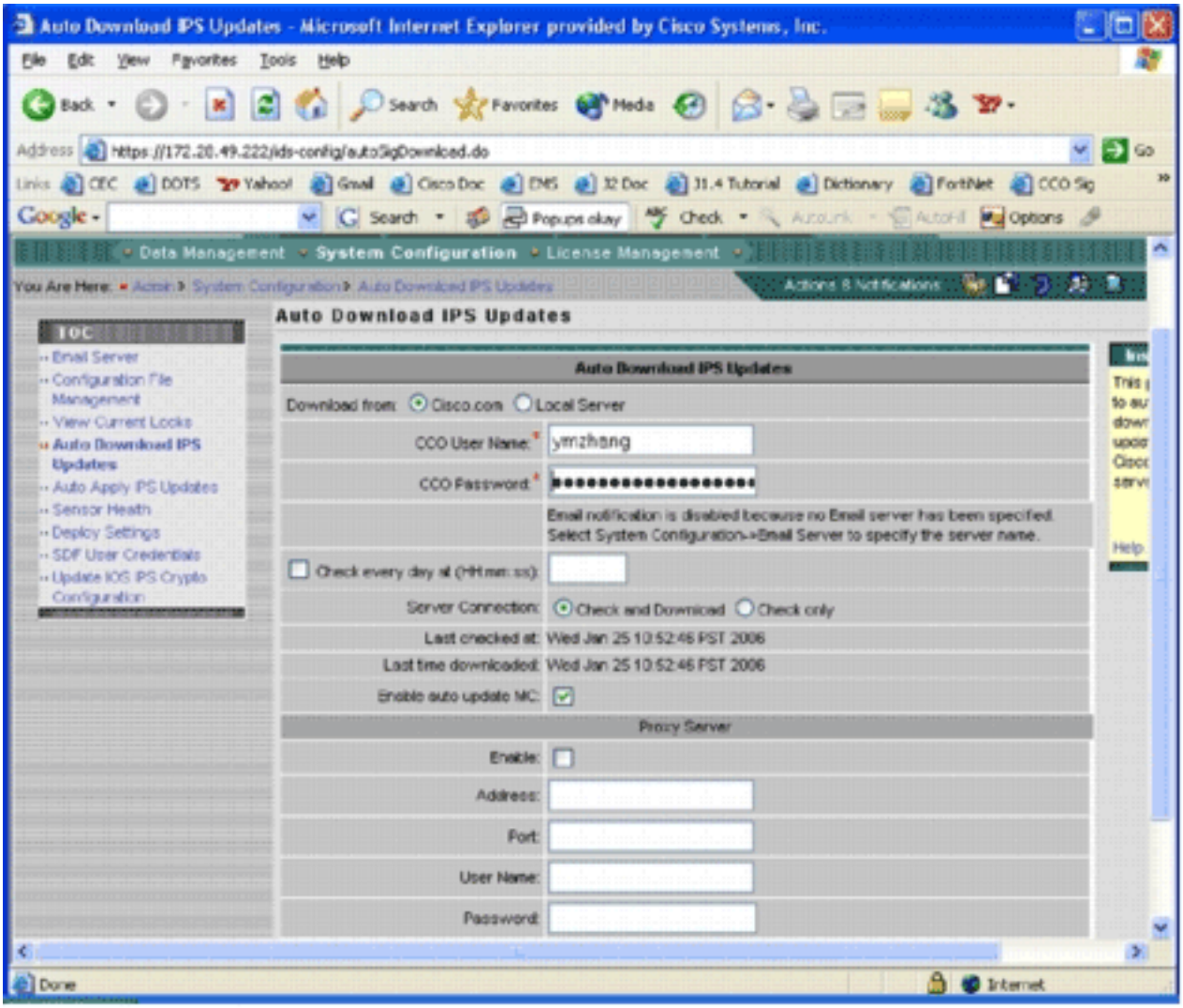
Haga clic en este icono.IPS MC genera automáticamente los cambios de configuración e los implementa en los dispositivos.

Descarga automática de actualizaciones de firmas

IPS MC admite la descarga automática de actualizaciones de firmas desde Cisco.com. Puede

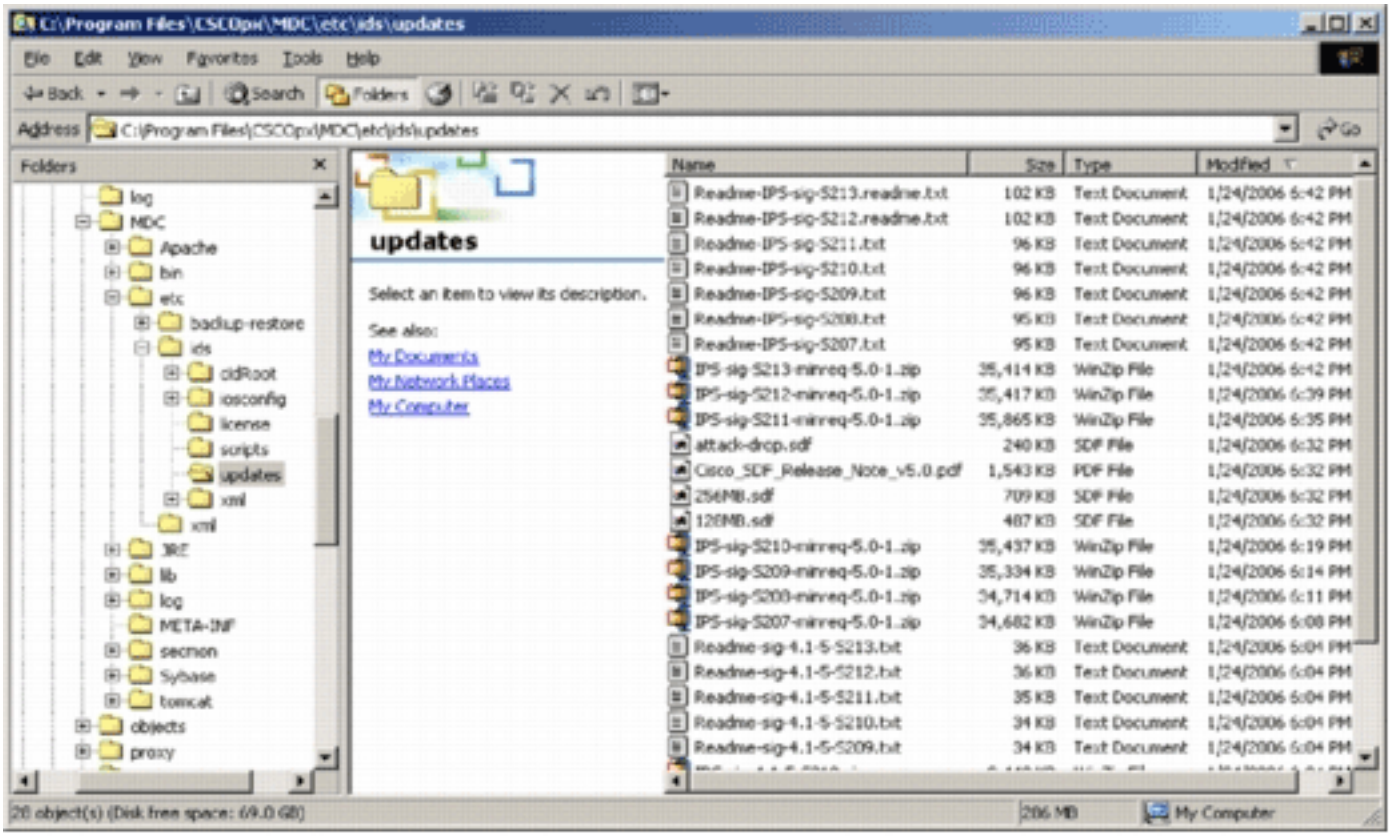
descargar actualizaciones de firmas para las plataformas de sensores, así como para las plataformas IPS de Cisco IOS. Para configurar esta función, vaya a **Admin > System Configuration > Auto Download IPS Updates**.

Aparecerá la página Auto Download IPS Update (Actualización de IPS de descarga automática).



Debe tener una cuenta válida de Cisco.com para descargar esta actualización de firma. Para verificar los archivos descargados automáticamente, vaya al directorio de inicio de instalación de IPS MC. De forma predeterminada, es \program files\CSCOpx\MDC\etc\ids\updates.

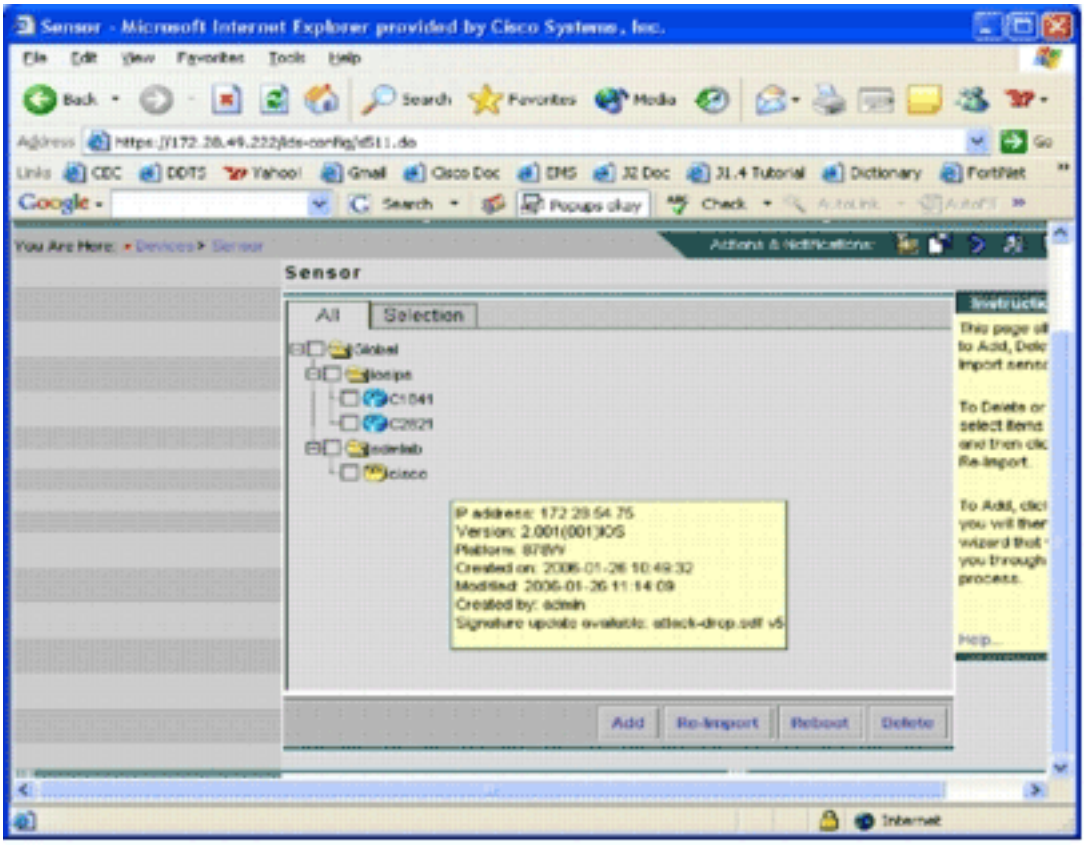
Esta imagen muestra una imagen de los archivos descargados en este directorio.



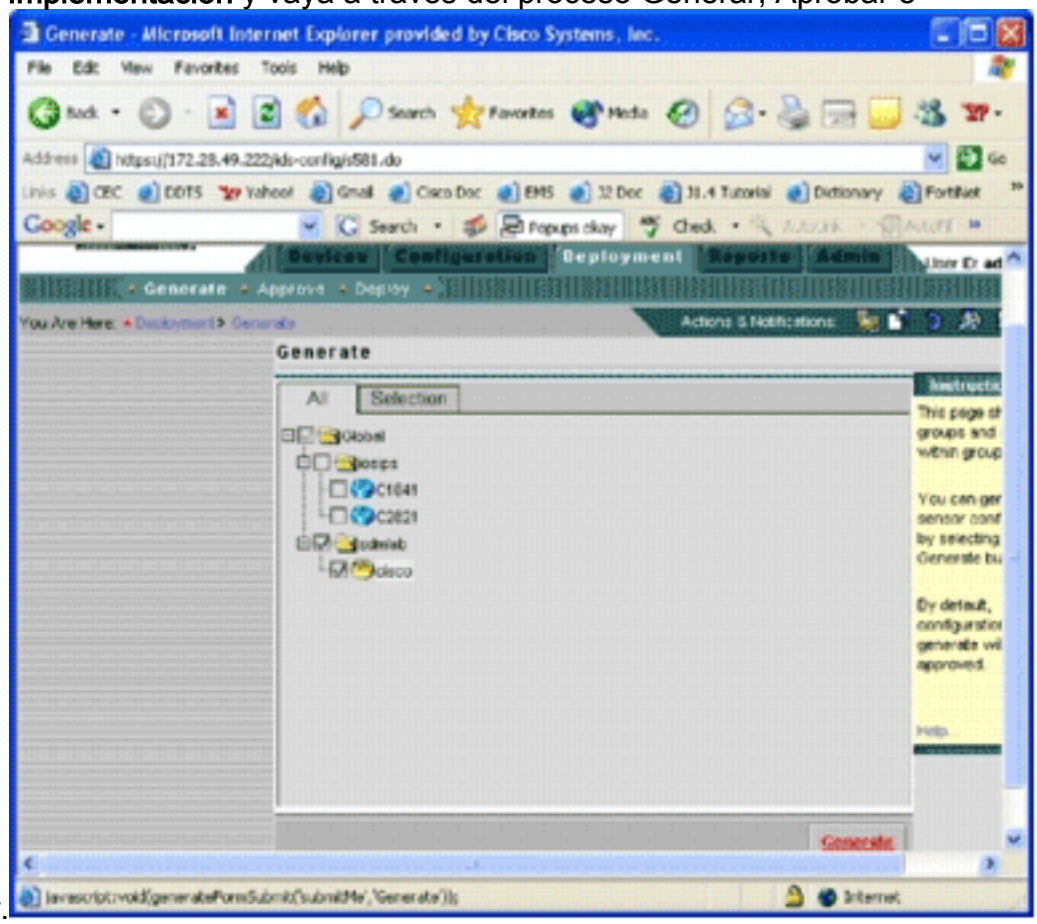
Puede ver los archivos de actualización del sensor. Se descargan el archivo de actualización del software Cisco IOS y los archivos SDF preconfigurados.

Actualización del router IPS de Cisco IOS con nuevos archivos SDF

Para los routers IPS de Cisco IOS implementados con archivos SDF preconfigurados, tan pronto como una nueva versión de los archivos SDF esté disponible a través de la descarga automática o copiada al directorio de actualizaciones, Cisco IPS MC reconoce la nueva versión. Después de actualizar la interfaz de usuario, los iconos de dispositivo para los dispositivos aplicables se vuelven amarillos.



1. Haga clic en **Implementación** y vaya a través del proceso Generar, Aprobar e Implementar.



2. Después de una implementación exitosa, el router IPS de Cisco IOS utiliza una nueva versión de los archivos SDF.

Información Relacionada

- Cisco Intrusion Prevention System