Ciscoworks IPS MC在Cisco IOS IPS的配置示例

目录

简介

CiscoWorks Management Center for IPS Sensors(IPS MC)是Cisco IPS设备的管理控制台。IPS MC版本2.2支持在Cisco IOS®软件路由器上调配入侵防御系统(IPS)功能。本文档介绍如何使用IPS MC 2.2配置Cisco IOS IPS。

有关如何使用IPS MC（包括如何使用IPS MC配置不基于Cisco IOS软件的设备）的详细信息，请参阅CiscoWorks Management Center for IPS Sensors文档，网址为：

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

先决条件

要求

本文档没有任何特定的要求。

使用的组件

本文档中的信息基于CiscoWorks Management Center for IPS Sensors(IPS MC)2.2版。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

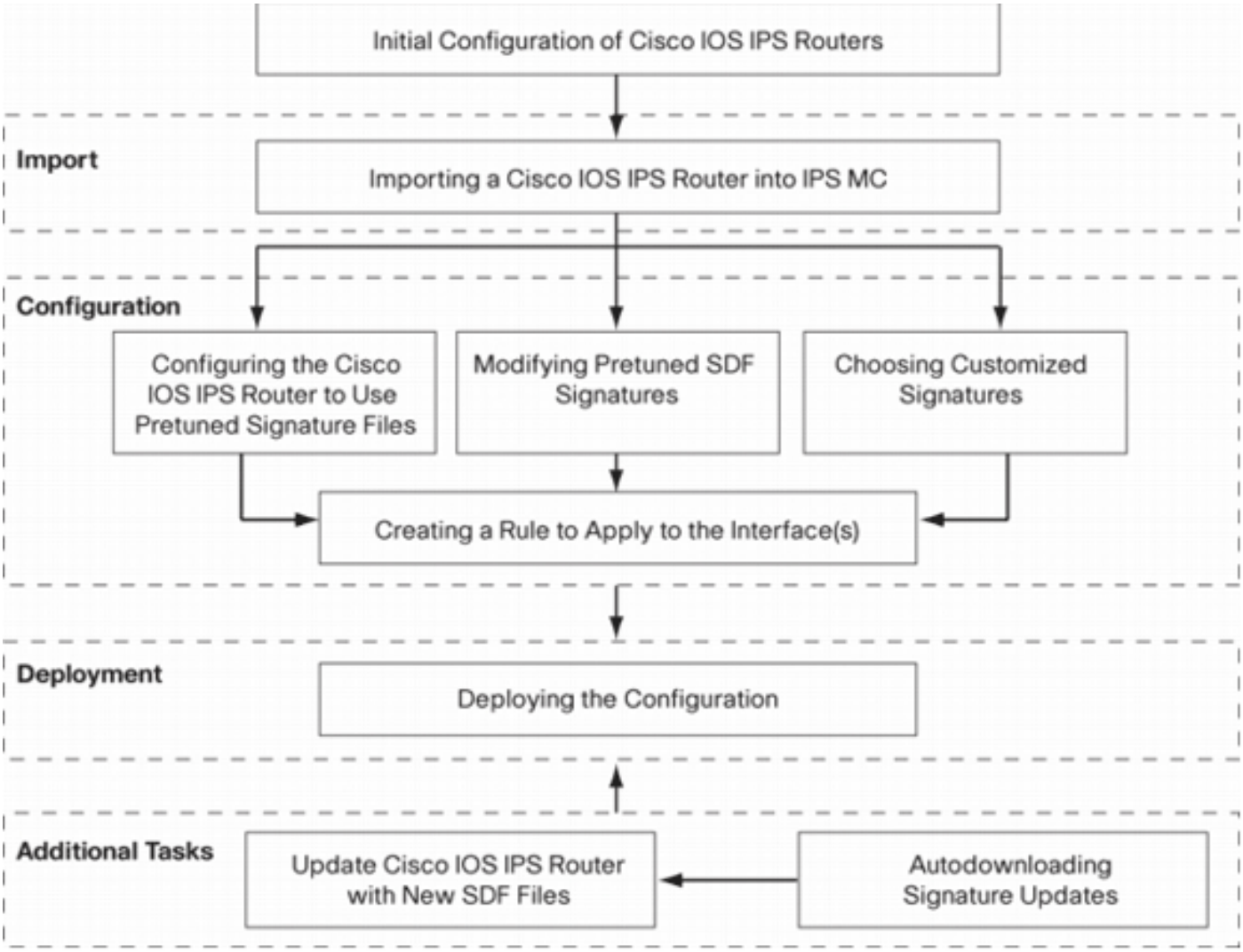
规则

有关文档约定的更多信息，请参考 Cisco 技术提示约定。

配置

基本了解配置任务

IPS MC用于管理一组Cisco IOS IPS路由器的配置。请注意，IPS MC不管理运行IPS的路由器发出的警报。思科建议使用思科安全监控、分析和响应系统（思科安全MARS）进行IPS监控。配置管理包括本文档中介绍的一系列任务。这些任务可分为三个阶段：导入、配置和部署，如此映像所示。



每个阶段都有自己的一套职责和功能：

- *导入* — 将路由器导入IPS MC。您必须先将路由器导入IPS MC，然后才能使用IPS MC进行配置。除非路由器上存在初始IPS配置，否则无法导入路由器（本文档稍后会提供详细信息）。
- *Configuration* — 配置设备。例如，您可以配置Cisco IOS IPS路由器，使其使用Cisco建议的预调签名文件之一。配置更改存储在IPS MC中，但在此阶段不发送到路由器。
- *部署* — 将配置更改传送到实际设备。在此阶段，您将配置任务中所做的更改提交给路由器。

- *其他任务*- IPS MC提供自动下载功能，可自动从Cisco.com下载签名更新。

您必须了解这种分阶段的方法，才能有效使用IPS MC。它不同于基于设备的管理GUI，如Cisco路由器和安全设备管理器(SDM)。 基于设备的GUI直接在单台路由器上运行，而IPS MC设计用于在全网范围内的路由器组（和其他IPS设备，如Cisco IPS 4200系列传感器）上运行。

本文档提供有关图中每项任务的信息，以帮助您使用IPS MC管理Cisco IOS IPS路由器。

Cisco IOS IPS路由器的初始配置

要成功将Cisco IOS IPS路由器导入或添加到IPS MC，您必须在Cisco IOS IPS路由器上执行某些初始配置步骤。本节介绍这些步骤。

您必须在Cisco IOS IPS路由器中启用安全外壳(SSH)协议，以便通过Cisco IPS MC进行配置、导入和部署。此外，必须启用安全设备事件交换(SDEE)协议以用于事件报告（尽管这些警报不会发送到IPS MC，因为IPS MC仅用于调配，而不用于报告）。 最后，您需要确保IPS路由器上的时钟设置与IPS MC同步。

要配置IOS IPS路由器，请完成以下步骤：

1. 为路由器创建本地用户名和密码。
```
Router#config terminal
Router(config)#username <username> password <password>
```

2. 在vty线路接口上启用本地登录。
```
Router#config terminal
Router(config)#line vty 0 15
Router(config-line)#login local
Router(config-line)#exit
```

   如果在vty线路配置下配置了传输输入或传输输出命令行界面(CLI)，请确保启用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密钥（如果密钥尚不存在）。SSH在生成加密密钥后自动启用。
```
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. 在路由器上启用SDEE。
```
Router(config)#ip ips notify sdee
```

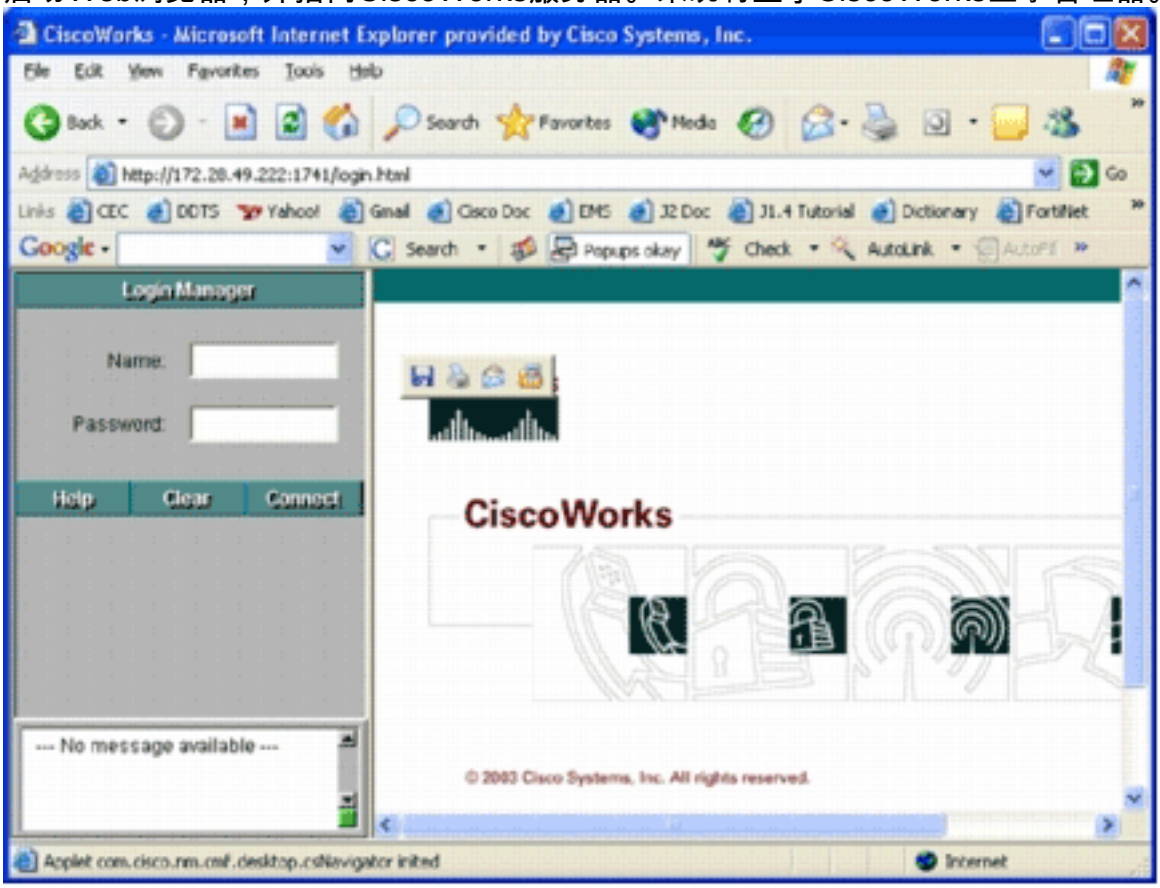
5. 启用HTTPS。IPS MC需要HTTP或HTTPS才能与路由器与SDEE通信以收集事件信息。
```
Router(config)#ip http authentication local
Router(config)#ip http secure-server
```

6. 使用外部网络时间协议(NTP)服务器或clock命令在IPS路由器上配置时钟设置。
   ```
   Router(config)#clock set hh:mm:ss day month year
   ```

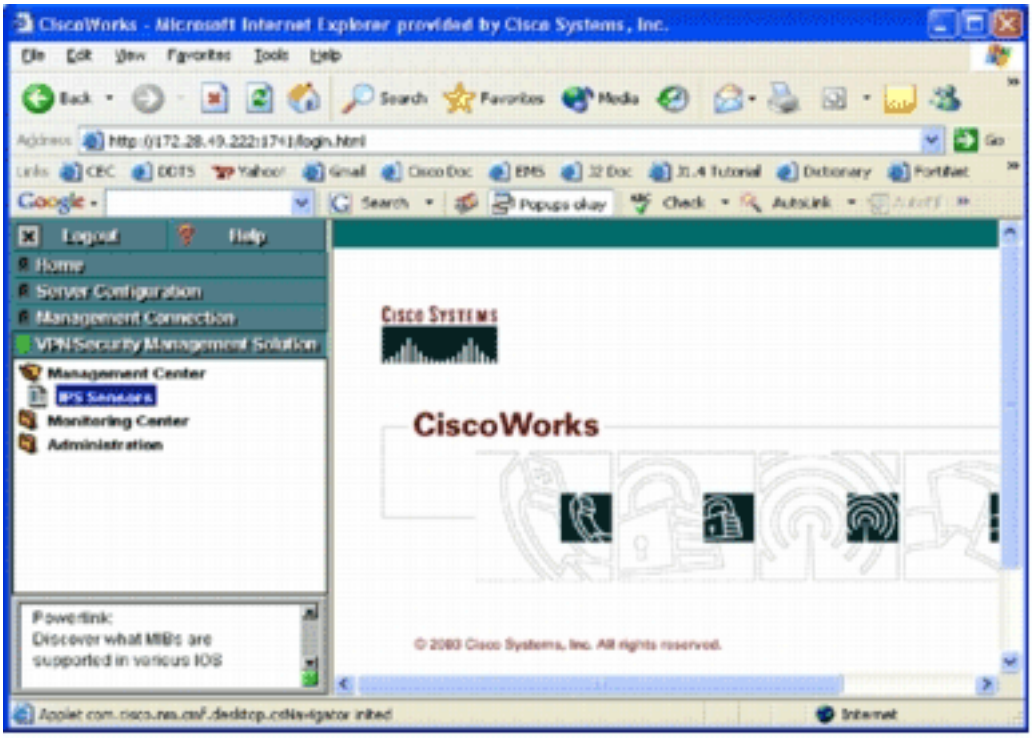
现在，Cisco IOS IPS路由器已准备就绪，可以导入IPS MC进行进一步配置和管理。

将Cisco IOS IPS路由器导入IPS MC

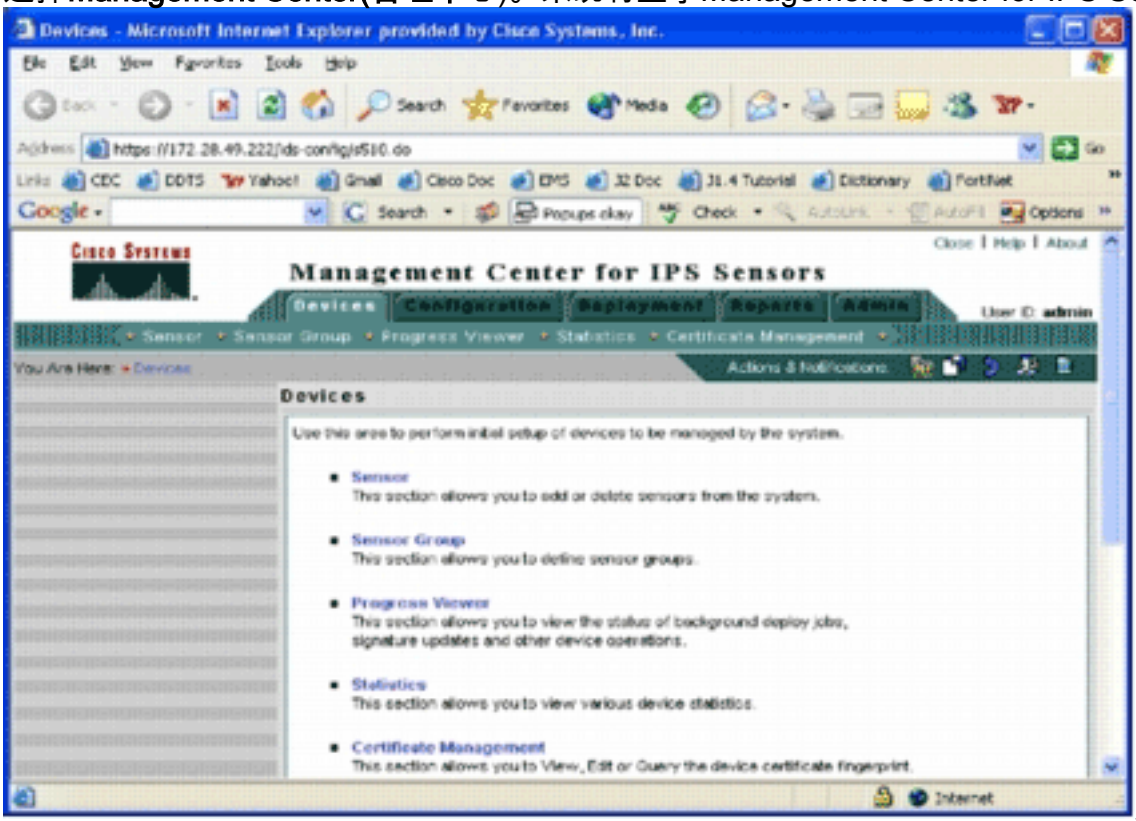
在路由器上完成初始配置后，可以将其添加（或导入）到IPS MC。

1. 启动Web浏览器，并指向CiscoWorks服务器。系统将显示CiscoWorks登录管理器。


注意：Web服务器的默认端口号为1741;因此，您应使用类似http://<*server ip address*>:1741/的URL。
2. 输入用户名和密码以登录。系统将显示CiscoWorks主页。

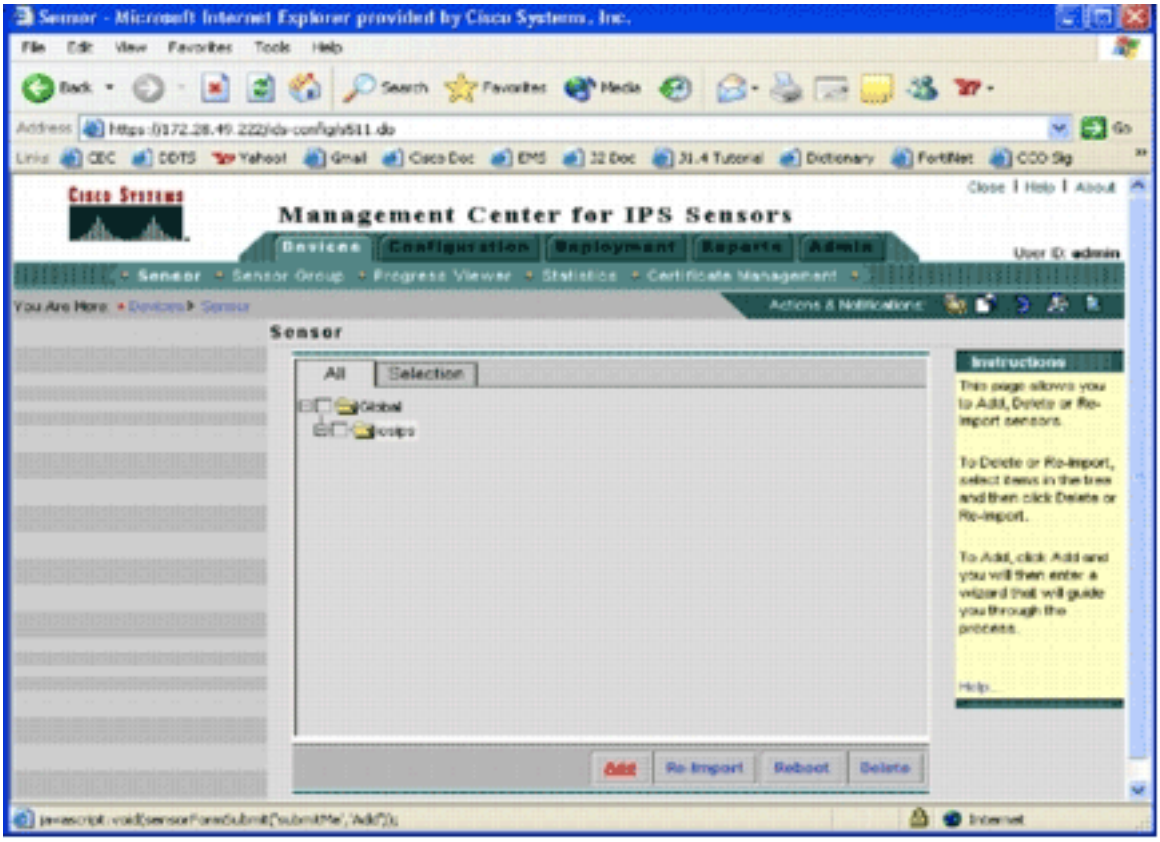


3. 在左侧导航窗格中，选择**VPN/Security Management Solution(VPN/安全管理解**决方案)，然后选择**Management Center(管理中**心)。系统将显示Management Center for IPS Sensors页面。

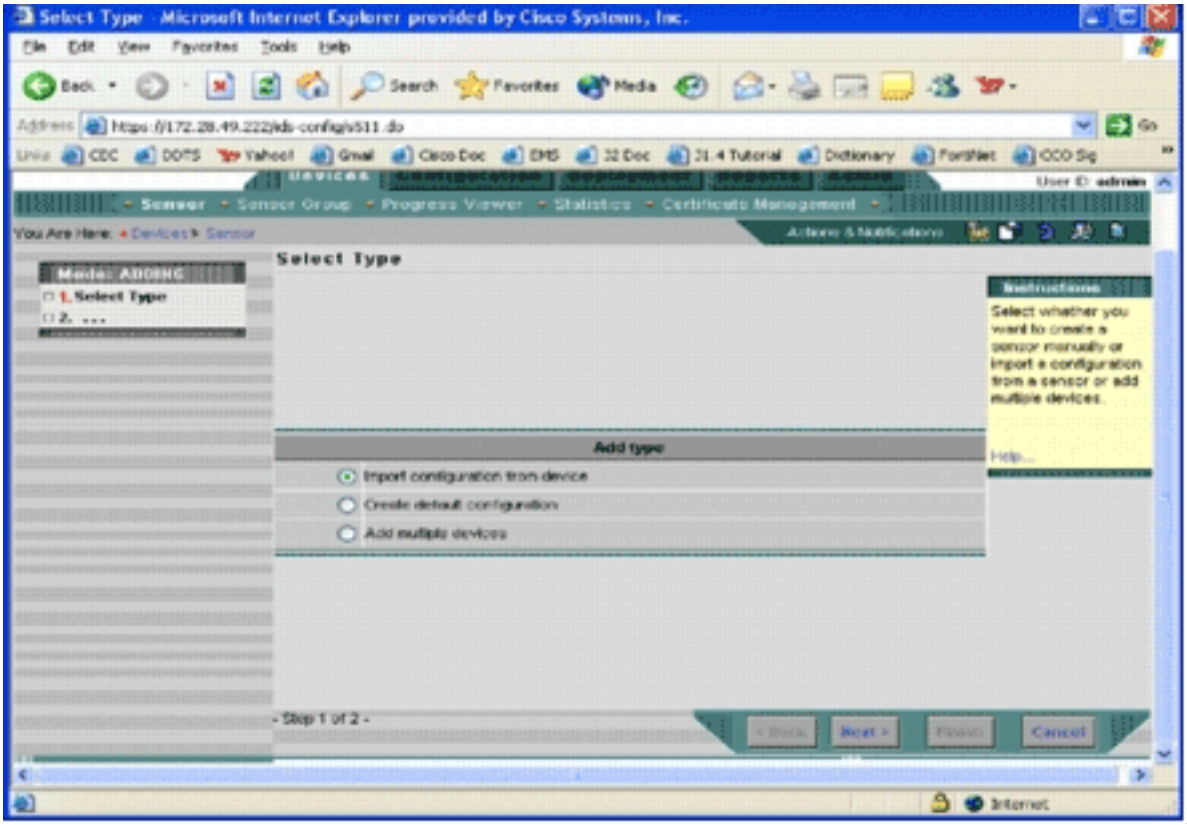


此页显示以下五个选项卡：*Devices* — 在Devices选项卡中，您可以对系统上的所有设备执行初始设置和管理。*配置* — 在“配置”选项卡中，可以执行调配功能。您可以在单个设备级别或组级别配置设备。一个设备组可以包含多个设备。必须保存通过配置任务所做的所有更改。配置功能不会立即对设备进行更改。您必须使用部署功能来部署更改。*部署* — 在部署选项卡中，您可以将配置更改部署到设备。计划功能可灵活控制配置更改何时生效。*报告* — 在“报告”选项卡中，可以生成各种系统操作报告。*Admin* — 在Admin选项卡中，您可以执行系统管理任务，如数据库管理、系统配置和许可证管理。

4. 单击**Devices**选项卡以添加新设备。系统将显示Sensor页面。



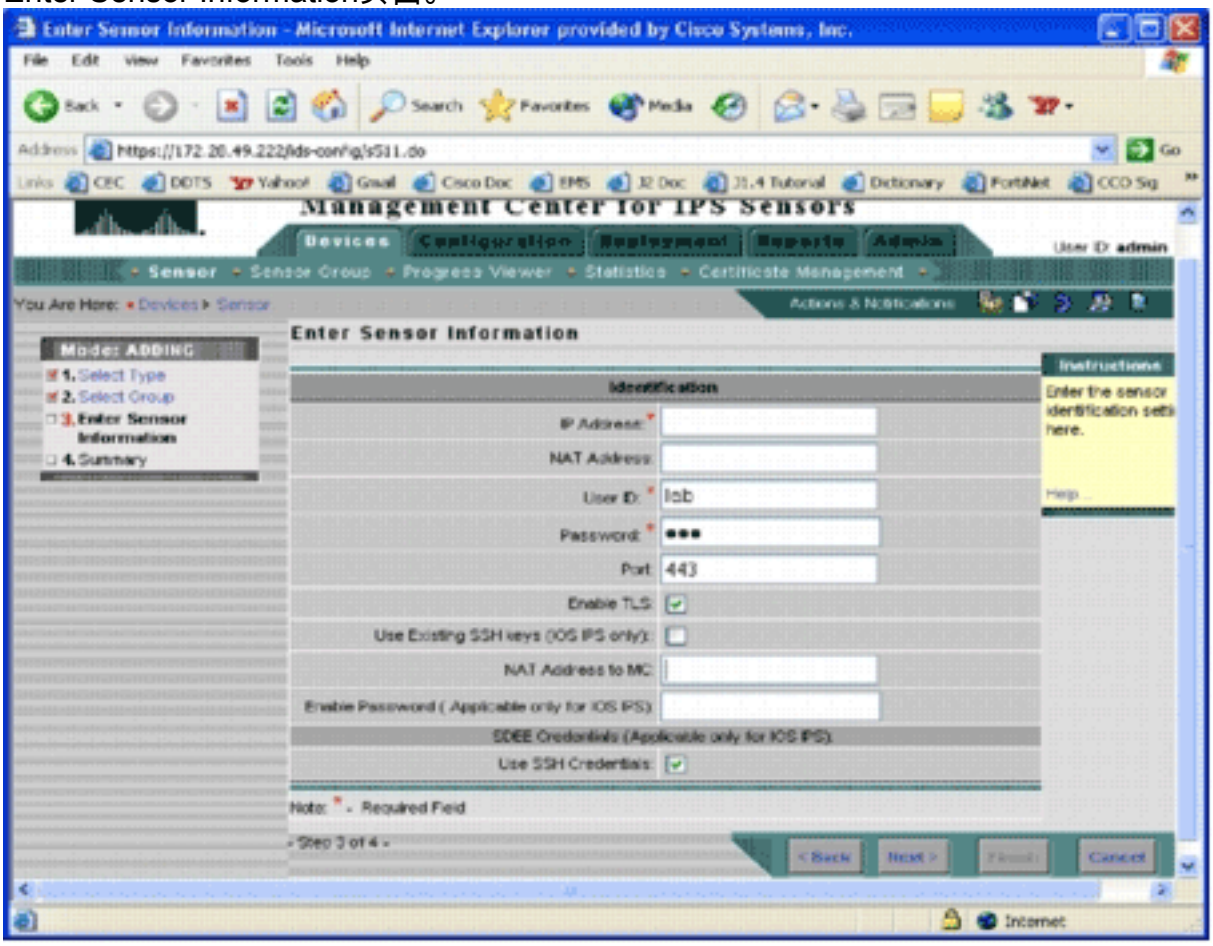
5. 单击 Add。系统将显示“选择类型”页面。



您必须通知IPS MC要执行的添加功能类型。此列表介绍了每个选项：*从设备导入配置* — 使用此选项可添加到当前在网络上运行的IPS MC设备。*创建默认配置* — 使用此选项添加当前未在网络上运行的设备。*Add multiple devices* — 使用此选项添加多个设备。您可以创建包含所有设备信息的.csv或.xml文件，然后将其导入IPS MC中，以一次性添加设备。**提示：**示例.csv格式和.xml格式文件位于：InstallDirectory\MDC\etc\ids\ and are named MultipleAddDevices-format.csv和MultipleAddDevices-format.xml。

6. 选择适当的Add type（添加类型）选项，然后单击**Next(下一步)**。
7. 选择要向其添加Cisco IOS IPS路由器的组，或使用默认全局组，然后单击**Next**。系统将显示

Enter Sensor Information页面。



8. 在“标识”(Identification)页面中，输入设备的标识信息。**注：如**果用户没有权限级别15的访问权限，则必须提供使能密码。在“标识”(Identification)页面的最后一行中，选中**使用SSH凭证(Use SSH Credentials)**复选框。
9. 单击 **Next**。系统将显示Add Sensor Summary。
10. 单击 **完成**。设备已成功添加到IPS MC。**注：如**果在导入过程中遇到错误，请确保检查以下项目：*必备配*置 — IPS MC与Cisco IOS IPS路由器通信需要这些配置。*连接* — 确保IPS MC可以到达Cisco IOS IPS路由器。*Clock* — 检查IPS MC和Cisco IOS IPS路由器上的时间。时间是用于身份验证的https证书的关键组件。时间必须在彼此之间的12小时内。（最佳实践最多需要几小时。）*Cisco IOS IPS Certificate* — 有时存储的Cisco IOS IPS证书不正确。要从Cisco IOS IPS删除证书，必须从Cisco IOS IPS路由器删除信任点。*Additional Configuration* — 如果**ip http timeout-policy配置了少量的最大请求**，如**ip http timeout-policy idle 600 life 86400 requests 1**，则必须增加最大请求数。例如：**ip http timeout-policy idle 600 life 86400 requests 8400**

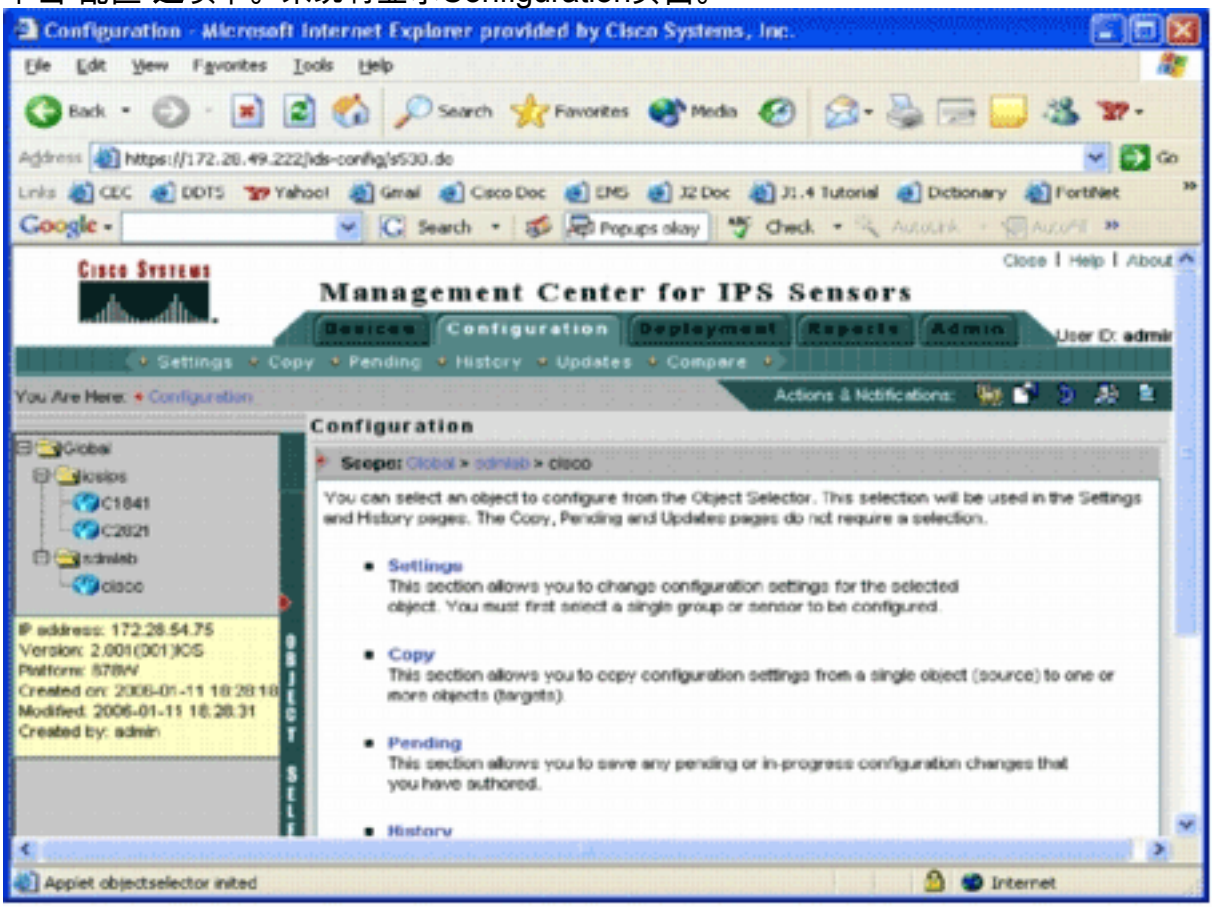
配置Cisco IOS IPS路由器以使用预调整的签名文件

将路由器导入IPS MC后，必须选择签名定义文件(SDF)（基于文本的文件，包括IPS路由器将使用的威胁签名）和触发每个签名时要执行的操作（例如，丢弃、TCP重置、警报）。

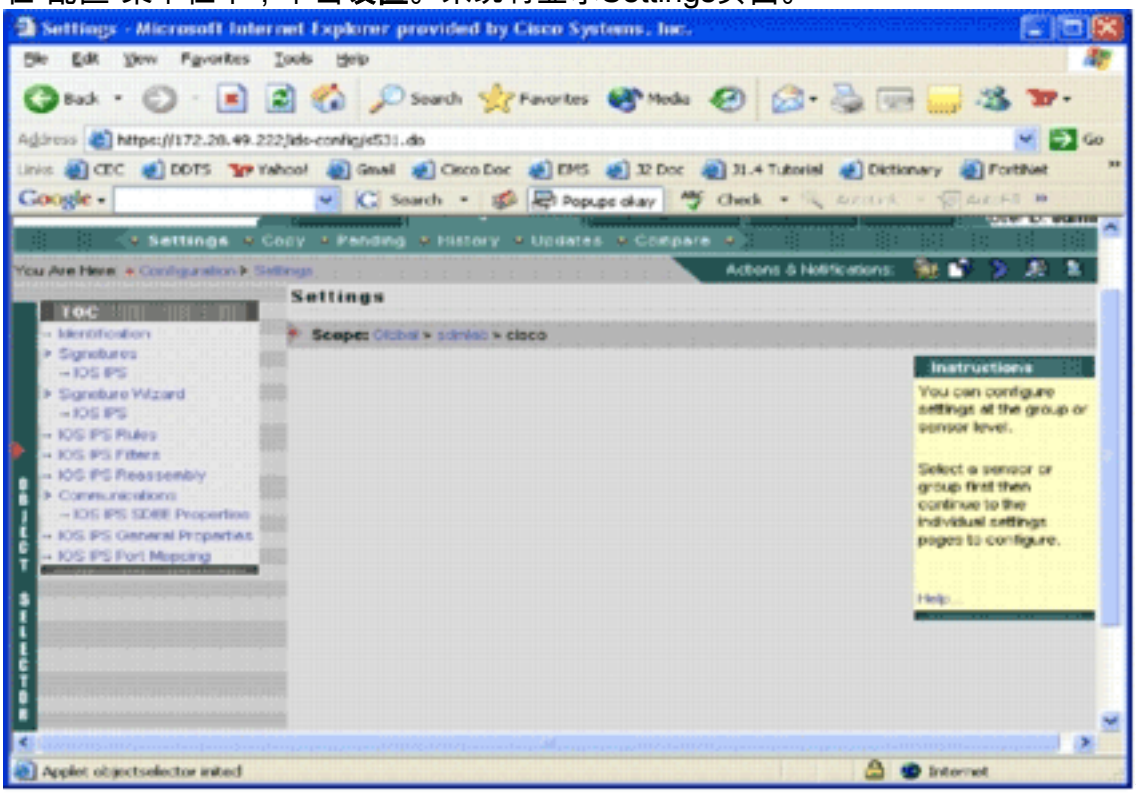
Cisco Systems®[建]议您使用Cisco预调SDF文件。目前，有三个此类文件：attack-drop.sdf、128MB.sdf和256MB.sdf。IPS MC可以从Cisco.com自动下载这些文件。有关详细信息，请参阅“自动下载签名更新”。

此过程以单台设备为例，从没有IPS配置的路由器开始。您也可以对组级别上的多台设备使用此步骤。

1. 单击“配置”**选**项卡。系统将显示Configuration页面。



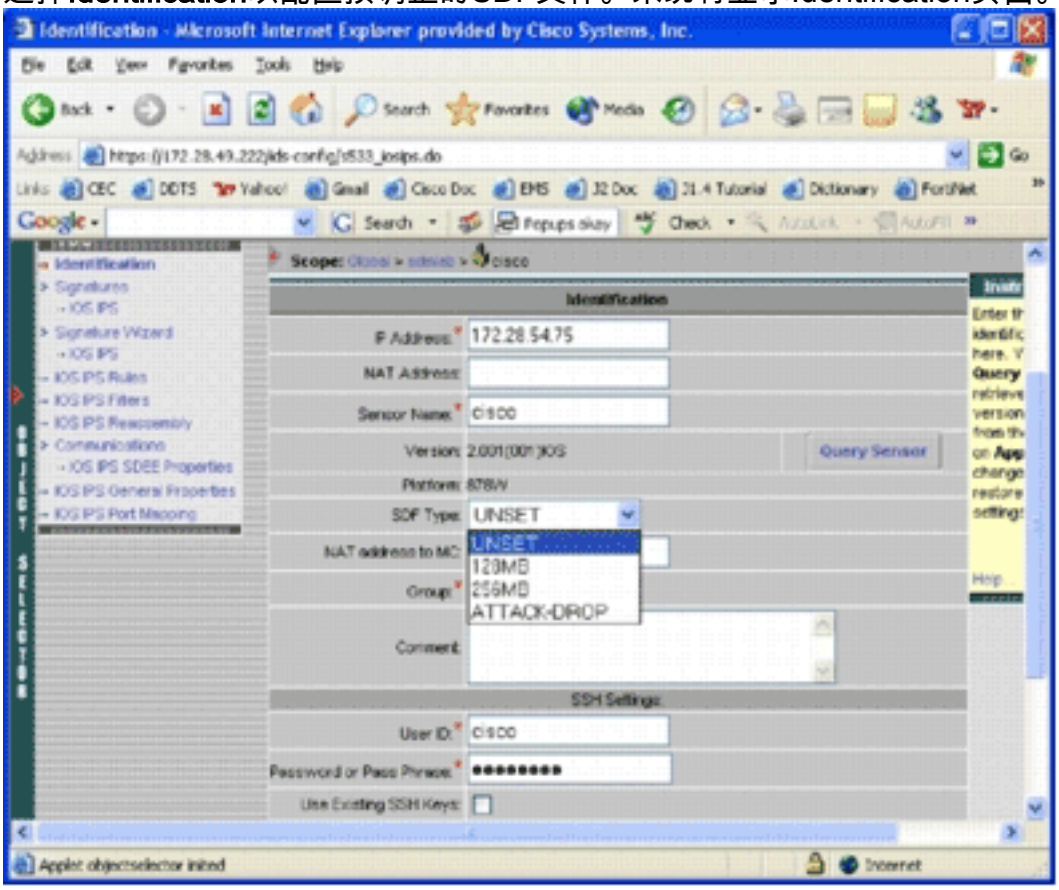
2. 从页面左侧的对象选择器中，选择要配置的Cisco IOS IPS路由器。**注意**：IPS MC 2.2中的大多数配置设置都可以在组级别以及单个设备级别进行配置。例如，全局组、iosip组和sdmlab组都是可配置的对象组。本示例使用sdmlab组的单个设备cisco。选择要配置的路由器后，位于“配置”页面顶部的路径栏会显示当前配置范围。例如，本示例的范围是*Global > sdmlab > cisco*。*cisco*是当前配置对象（即从对象选择器中选择的路由器）。
3. 在“配置”菜单栏中，单击**设置**。系统将显示Settings页面。



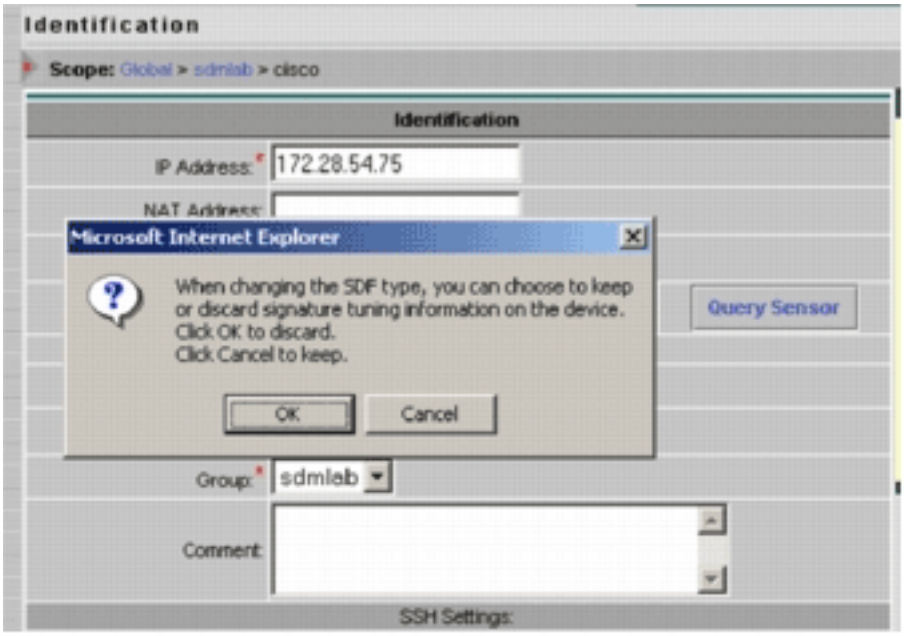
在“设置”(Settings)页面中，可以更改所选对象的配置设置。特定于Cisco IOS IPS路由器的配置设置位

于页面左侧的TOC部分。TOC部分下提供的任务列表：*标识*- Cisco IOS IPS路由器基本信息；可以在此处指定预调整的SDF文件*签名*— Cisco IOS IPS路由器签名*签名向导* — 添加自定义签名的签名向导*Cisco IOS IPS规则* — 用于配置用于应用于接口的Cisco IOS IPS规则*Cisco IOS IPS过滤器*- Cisco IOS IPS过滤器*Cisco IOS IPS重组* — 接口IP虚拟重组配置*Cisco IOS IPS SDEE属性* — 用于配置SDEE设置*Cisco IOS IPS常规属性* — 其他Cisco IOS IPS相关配置

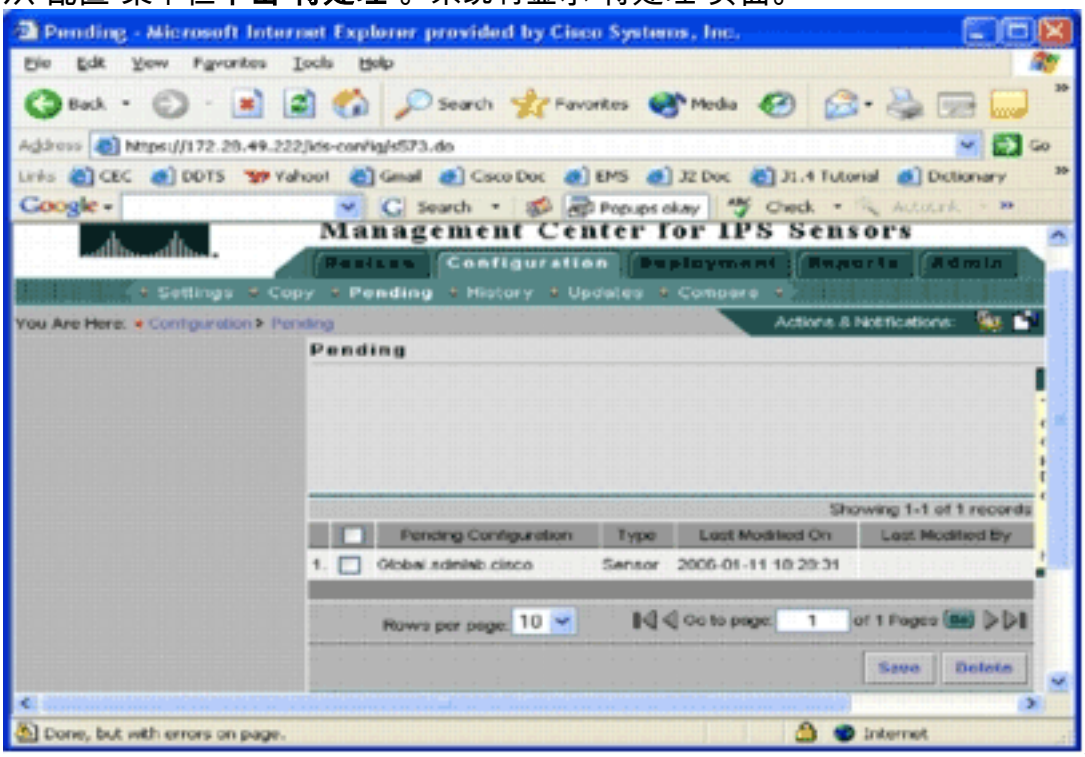
4. 选择**Identification**以配置预调整的SDF文件。系统将显示Identification页面。



5. 从SDF类型(SDF Type)下拉列表中，选择适当的预调整SDF，然后单击**应用**以应用更改。Cisco IOS IPS支持1600多个签名，超出路由器的内存容量，无法接受。SDF被开发为选择和加载最重要签名的一种便利方式。目前，您可以从三个SDF中进行选择。它们的大小不同，以便您能根据路由器的DRAM容量选择SDF文件。以下对可用选项进行了说明：UNSET — 未设置SDF类型。ATTACK-DROP — 此SDF适用于具有64 MB DRAM的路由器。256MB — 此SDF适用于具有256 MB DRAM的路由器。128MB — 此SDF适用于具有128 MB DRAM的路由器。**注意**：128-MB和256-MB SDF需要2.001引擎或更高版本。此信息在“设置”>“标**识UI”>“版本”字**段中。**警告**：IPS MC不包括Cisco IOS IPS路由器的内存管理功能。为Cisco IOS IPS路由器选择SDF文件时请小心。确保Cisco IOS IPS路由器有足够的内存来运行所选的SDF文件。**注意**：更改SDF类型时，可能会收到以下消息：*更改SDF类型时，您可以选择在设备上保留或放弃签名调整信息。单击确定放弃。单击取消保留。*



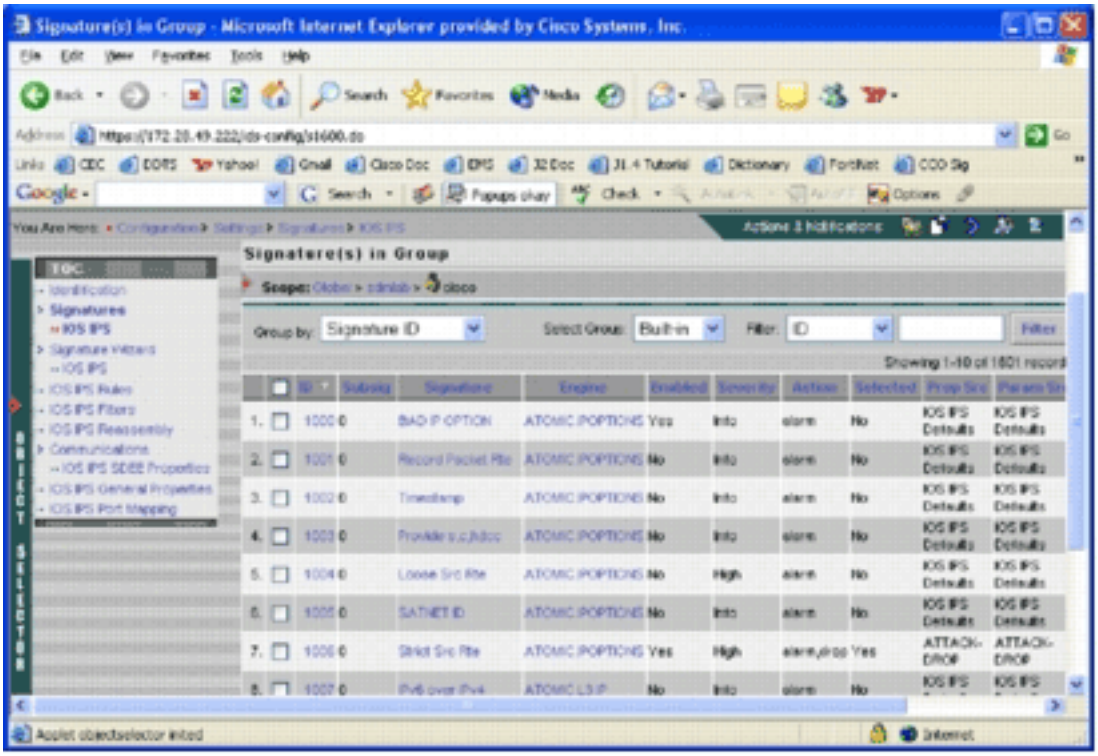
6. 单击**Cancel**以保留您的签名调整信息。现在您已成功为路由器 — 思科选择预调整的SDF，您可以执行其他签名调整，例如添加或编辑，甚至创建您自己的签名，或者可以跳过签名调整任务并直接转到[创建规则以应用到接口](#)。
7. 从“配置”菜单栏**单击“待处理”**。系统将显示“待处理”页面。



此时，配置任务已完成。但是，必须完成部署任务，才能将更改部署到目标设备。

修改预调整的SDF签名

为路由器选择预调整的SDF文件后，可以执行其他签名调整任务。您可以添加、编辑、删除和修改签名，以最符合您的需求，或在必要时创建您自己的签名。本示例使用IPS MC添加其他签名并修改操作。此图显示签名配置接口。



您可以使用签名配置来启用或禁用、选择或取消选择、添加签名、删除签名、更改签名操作和编辑签名参数。使用左侧的签名向导创建自定义签名。

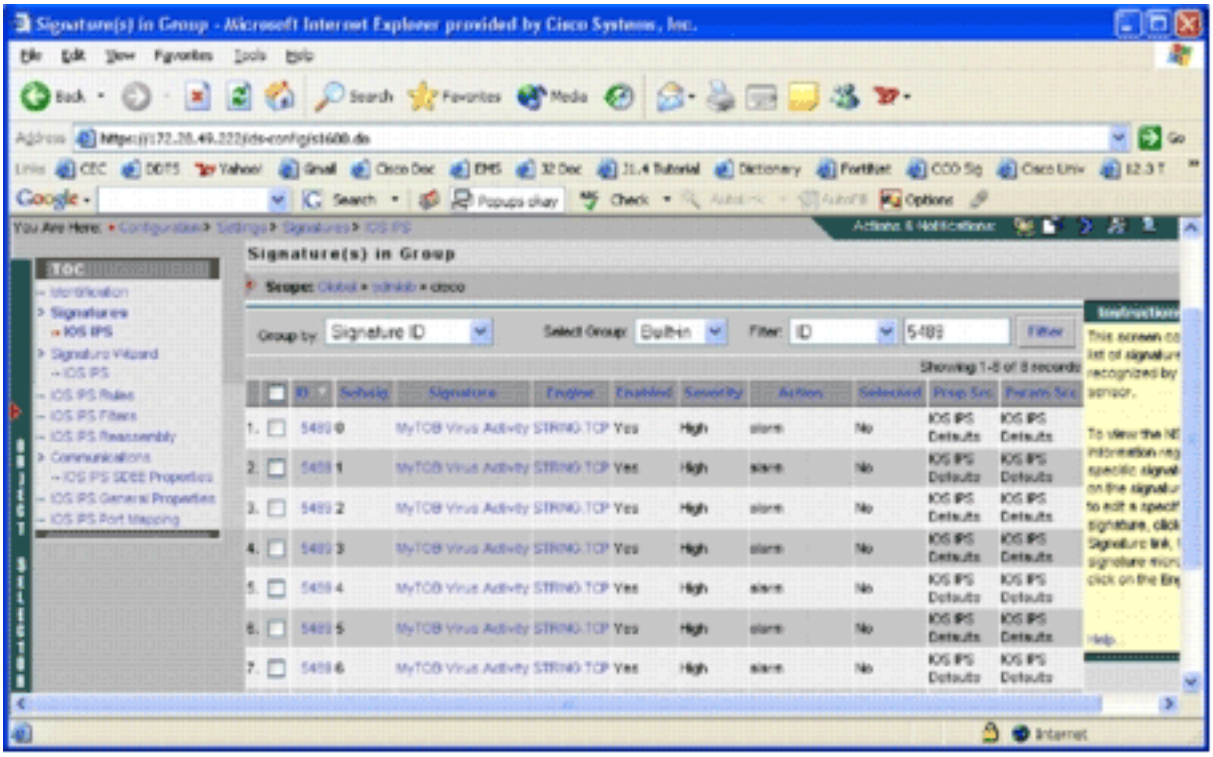
在签名配置用户界面中，某些信息默认显示。Selected是指签名是否包含在发送到路由器的SDF文件中。如果未选择签名，则不会添加签名。仅在选择签名时启用。禁用签名后，IPS引擎将不发送该特定签名的事件。如果未选择签名，则签名也会自动禁用。

最后两列（Prop Src和Param Src）告诉您签名及其参数分别来自何处。签名可能是从预调整的SDF文件或出厂默认文件中获取的，您可以在IOS-Sxxx.zip文件更新中找到（显示为IOS IPS默认值）。 这些值也适用于参数列。

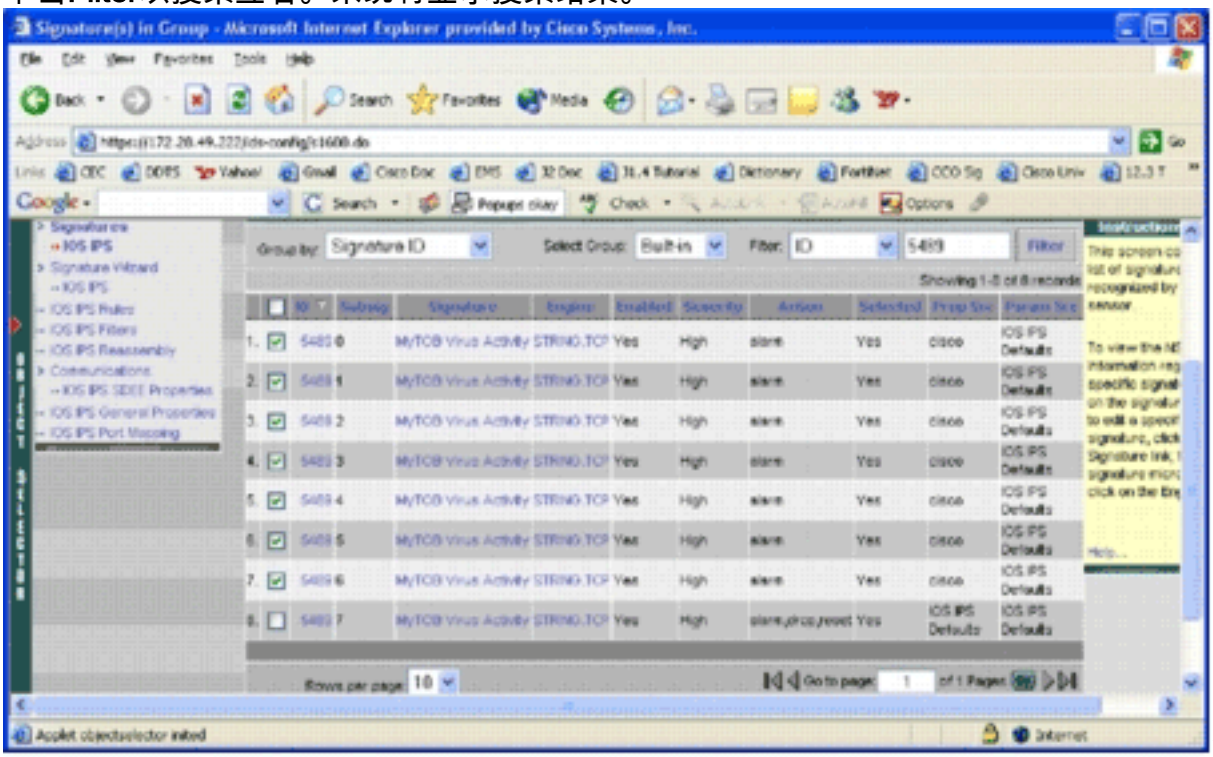
向Cisco IOS IPS路由器添加签名时，必须考虑内存注意事项。如果添加的签名数超过Cisco IOS IPS路由器可处理的签名数，IPS MC将无法将配置更改部署到设备。

要向Cisco IOS IPS路由器添加签名5489/x，请完成以下步骤：

1. 选择**Configuration**，然后使用Object Selector以选择要为其配置IPS签名的Cisco IOS IPS路由器。
2. 选择**Configuration > Settings > Signatures > IOS IPS**。系统将显示“组中的签名”页面。

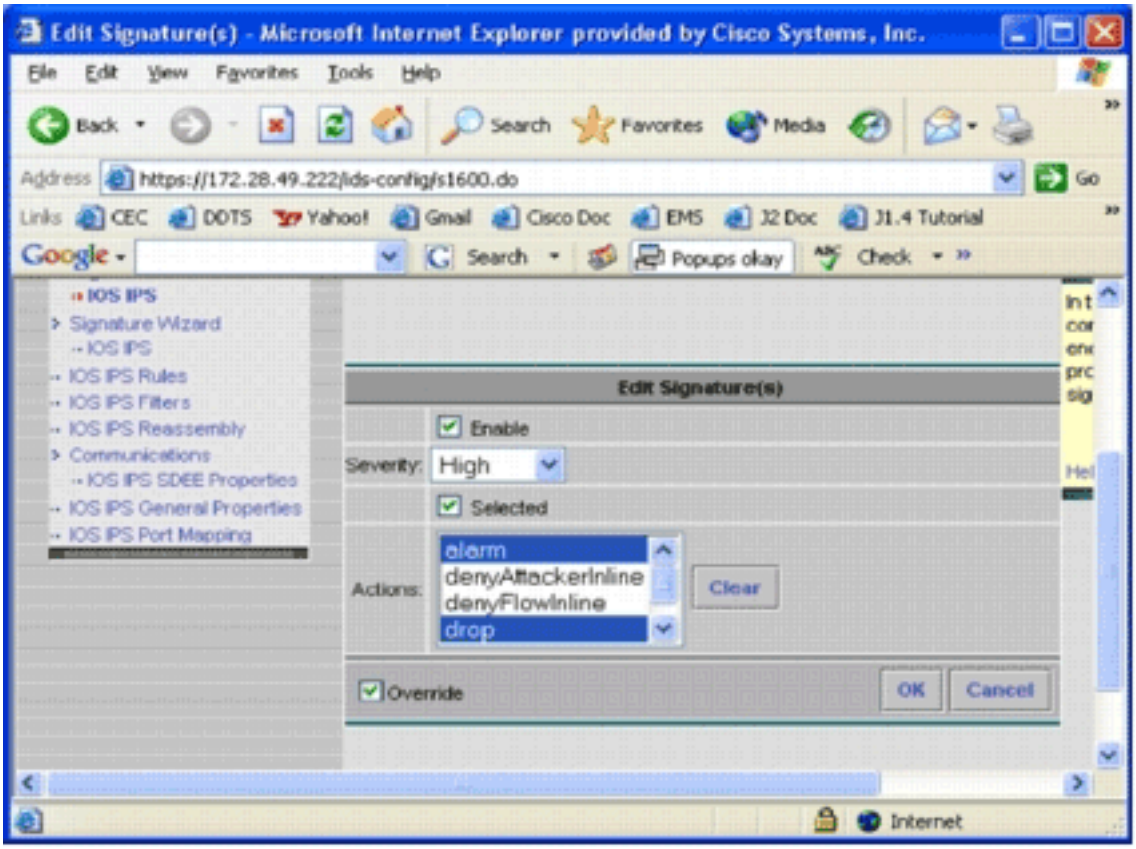


3. 在结果的签名列表中，选择Filter by ID（按ID过滤），然后键入签名ID 5489。
4. 单击**Filter**以搜索签名。系统将显示搜索结果。

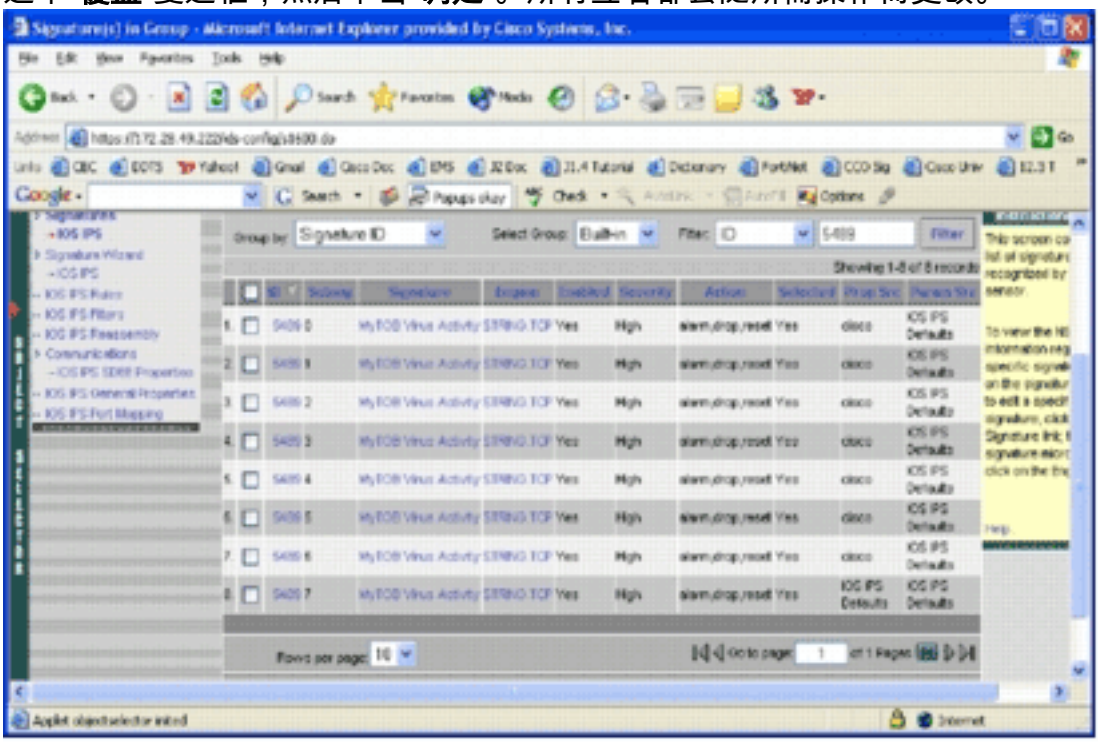


注意：IPS MC不支持Cisco SDM中的新分类。

5. 选中尚未选择的签名旁边的复选框，然后单击底**部工**具栏上的选择。
6. 单击**Edit**以更改签名操作。系统将显示Edit Signature(s)页面。



7. 选中选**定**复选框，然后从“操作”列表**中选择警**报、**丢弃**和**重置**。
8. 选中“**覆盖**”复选框，然后单击“**确定**”。所有签名都会随所需操作而更改。



9. 转到“待处理”任务并保存所有更改。配置任务将完成。**提示**：请密切注意“Prop Src”列。修改后，源设备更改为名为*cisco*的设备，这意味着所有调整信息与默认预调整的SDF文件分开保存。此机制使IPS MC能够保留自定义签名更改。

在上一节中，当您更改SDF文件类型时，IPS MC会询问您是否希望保留签名调整信息。这是引用的签名调整信息。

选择自定义签名

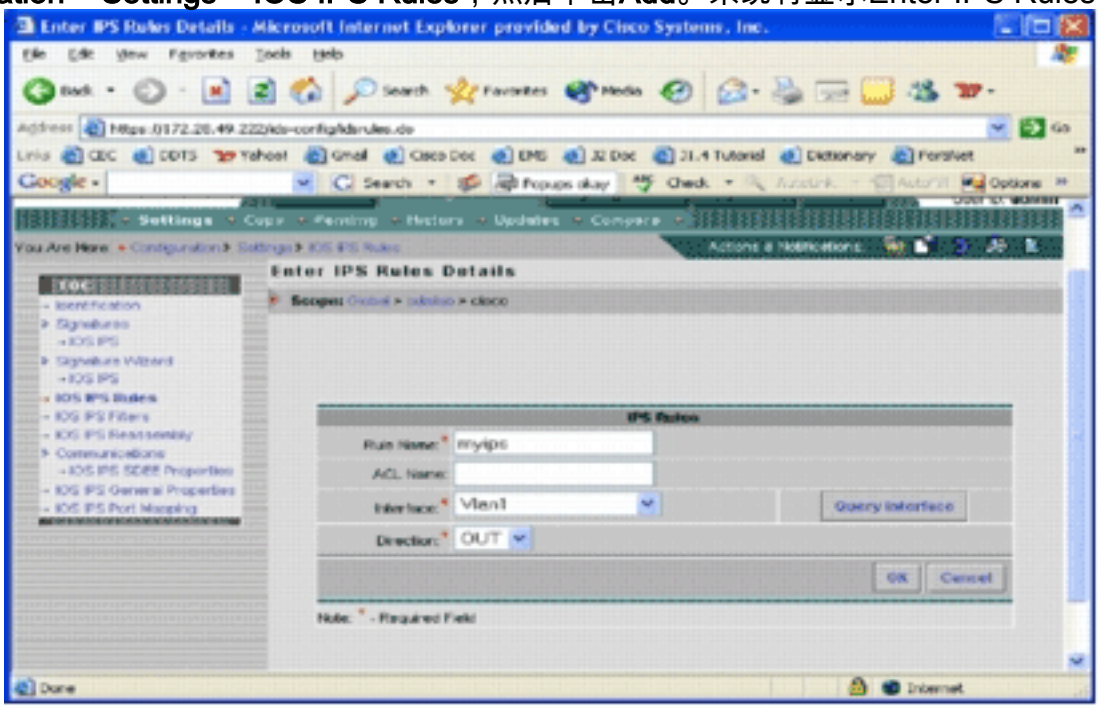
如果不想使用默认预调整的SDF文件，可以使用修改预调整的SDF签名一节中指定的步骤来为设备

选择调整签名。在标识页中，您需要确保SDF类型为UNSET。请参阅配置Cisco IOS IPS路由器以使用预调整的签名文件中的步骤3。

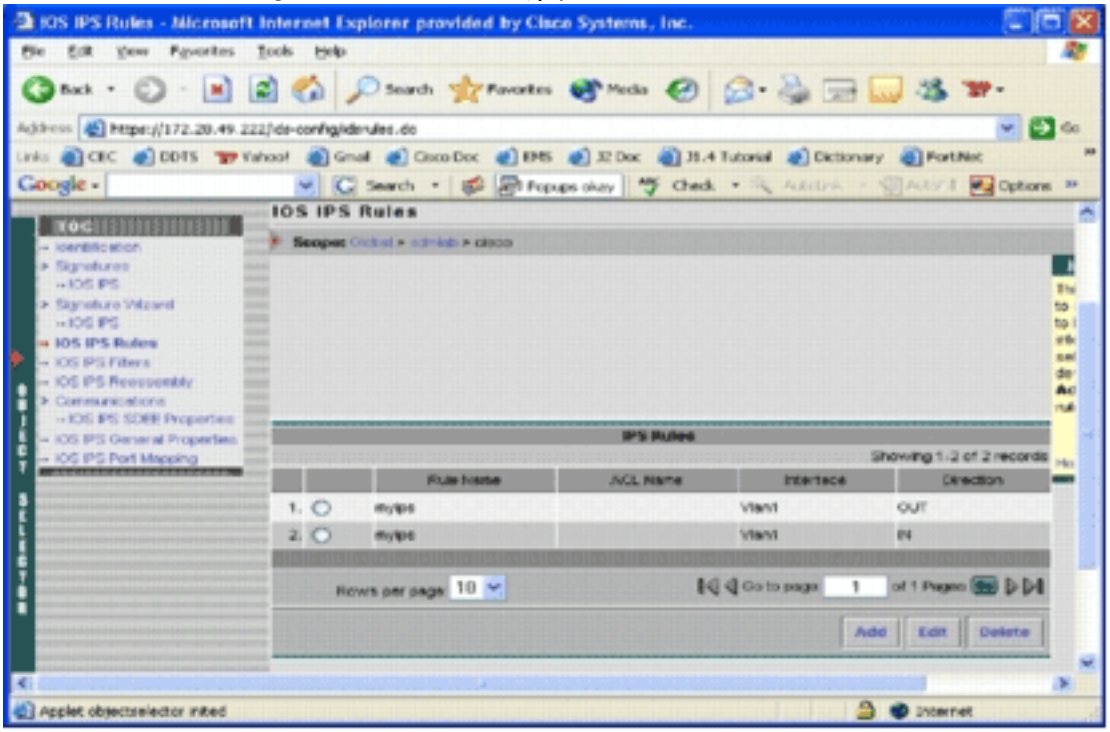
创建要应用于接口的规则

调整签名后，您需要在Cisco IOS路由器上启用IPS。要在路由器上启用IPS，必须创建IPS规则并将其应用到至少一个接口。

1. 选择**Configuration**，然后使用Object Selector以选择要配置的Cisco IOS IPS路由器。在路径栏中验证您的范围是在设备级别，而不是在组级别。
2. 选择**Configuration > Settings > IOS IPS Rules**，然后单击**Add**。系统将显示Enter IPS Rules Details页面。



3. 输入要应用规则和方向的规则名称和接口的信息。
4. Click **OK**.系统将显示IOS IPS Rules页面。



同样，您可以为接口创建两个方向的规则。

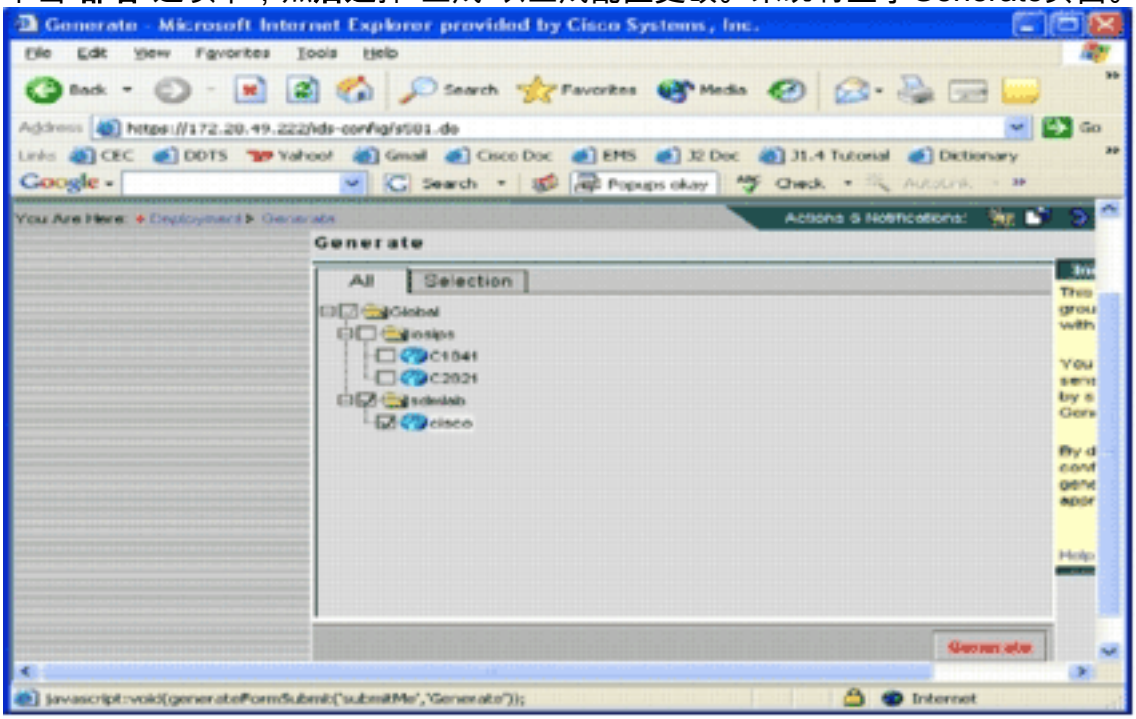
5. 您必须保存配置更改并完成部署流程，以便将更改传送到受影响的设备或设备组。您也可以执行其他IPS相关配置，但所有其他任务都是可选的，不是必需的。您可以在配置用户界面左侧找到所有选项。本文档不介绍可选配置选项。

部署配置

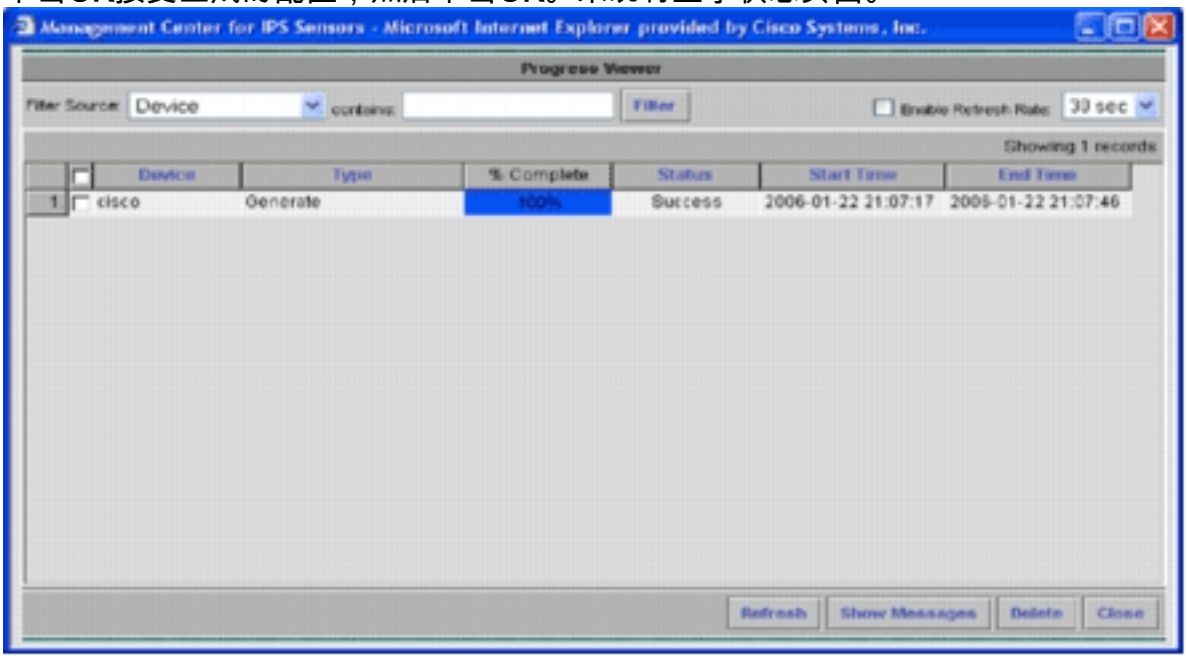
进行所有配置更改后，必须使用部署任务将更改提交到设备。您到目前为止所做的所有配置都保存在本地的IPS MC服务器上。

要部署配置更改，请转至“部署”页面，并完成以下步骤：

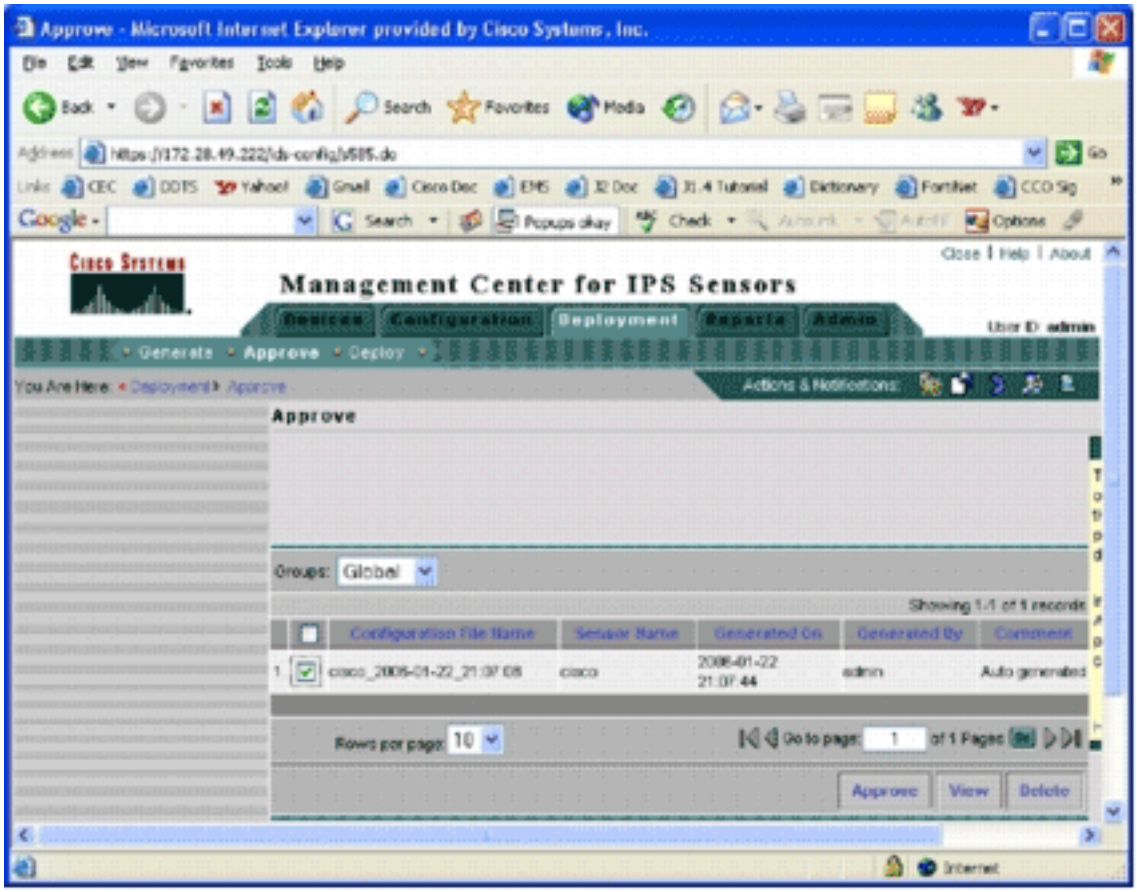
1. 单击“**部署**”选项卡，然**后选**择“生成”以生成配置更改。系统将显示Generate页面。



2. 选择刚*配*置的思科设备，然后单**击Generate**。
3. 单击**OK**接受生成的配置，然后单击**OK**。系统将显示状态页面。

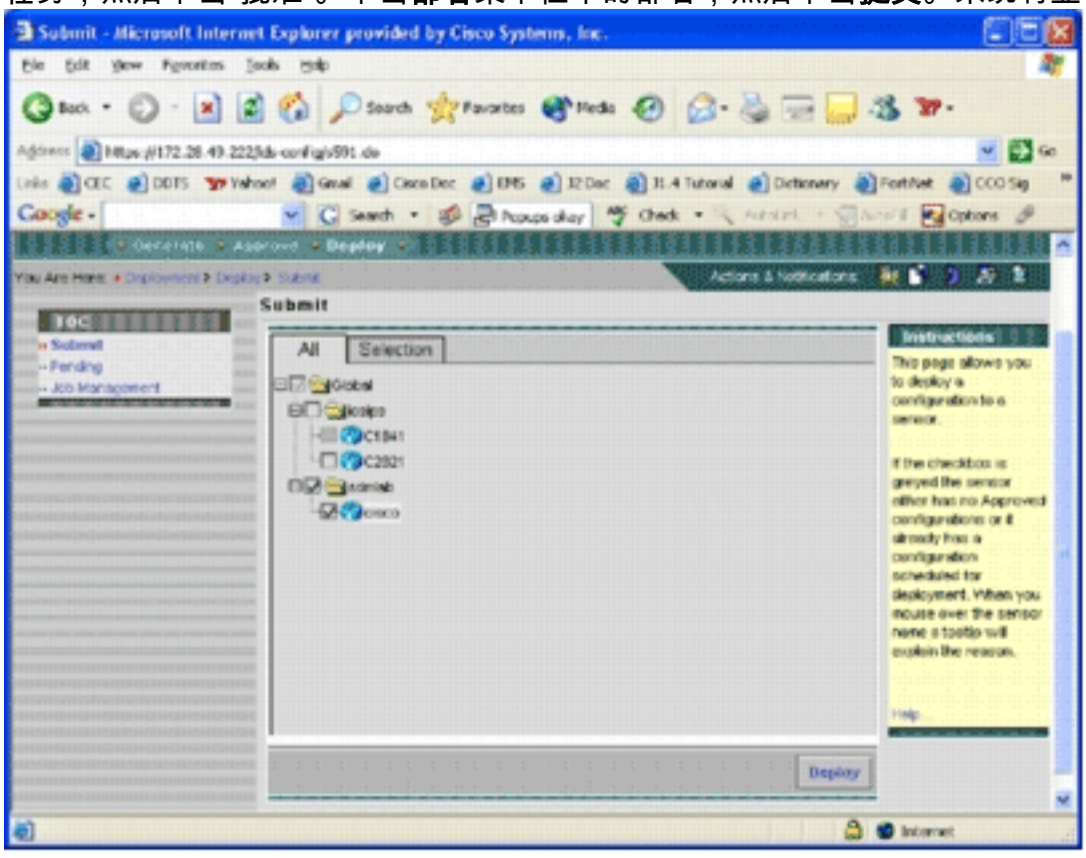


4. 单击**Refresh**，直到生成任务成功完成。
5. 单击“部署”菜单栏和sdmlab组中的**批准**，以查看需要批准的配置列表。系统将显示“批准”页面

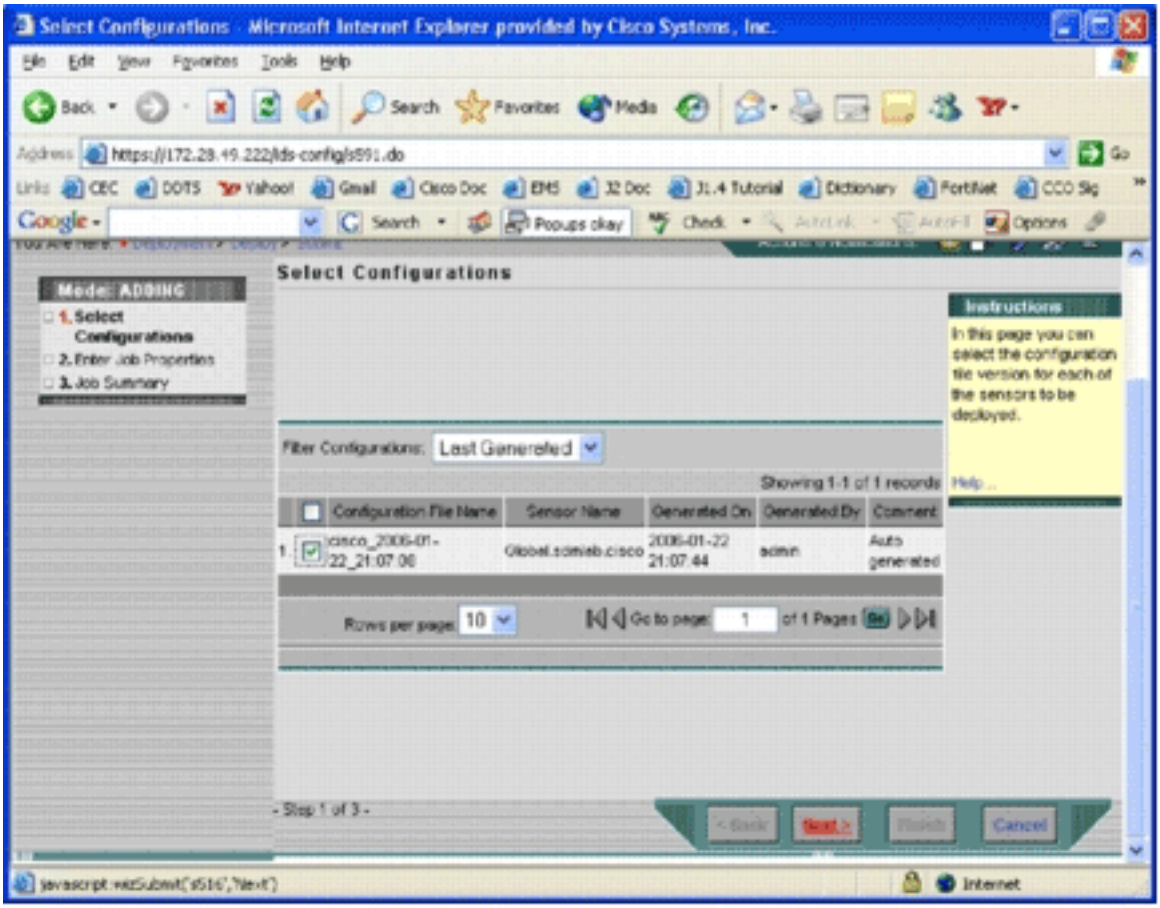


。

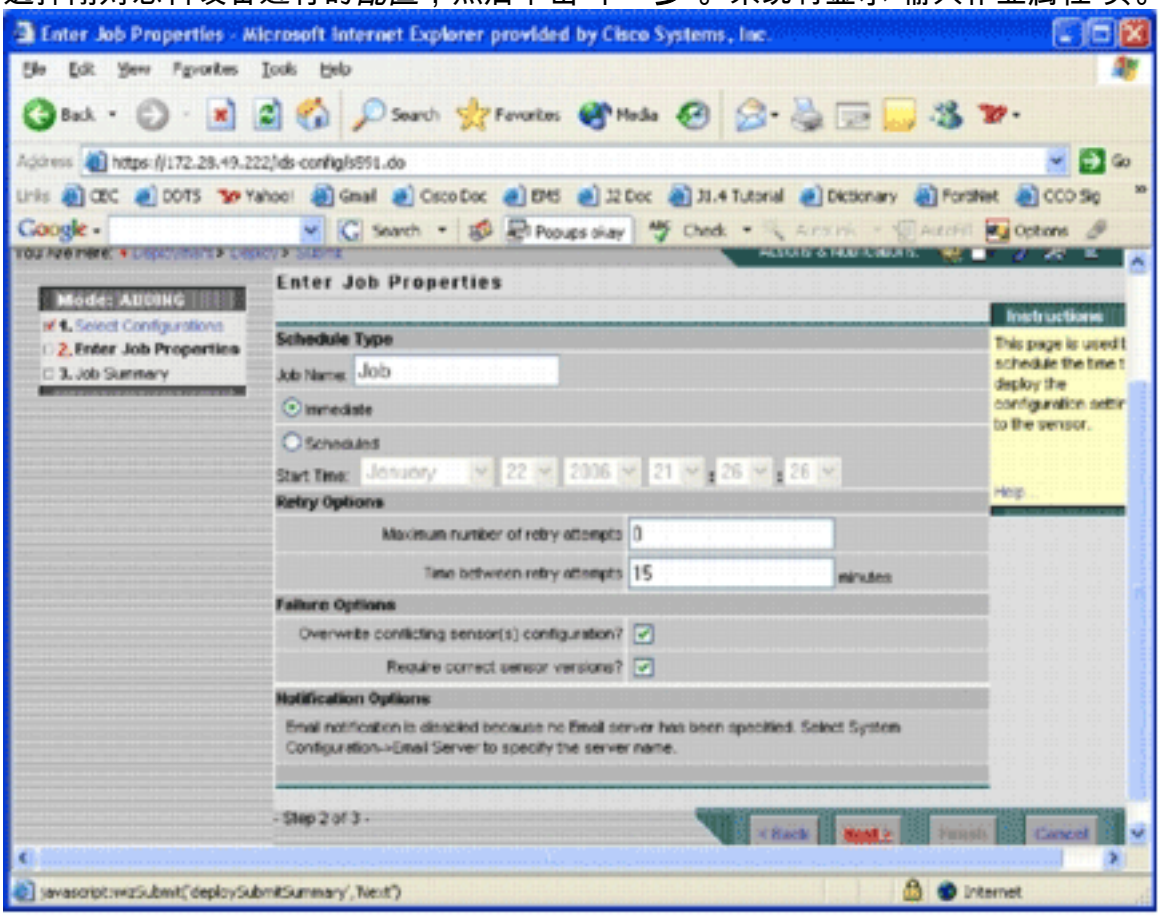
6. 选择任务，然后单击“批准”。单击**部署**菜单栏中的部署，然后单击**提交**。系统将显示“提交”页面。



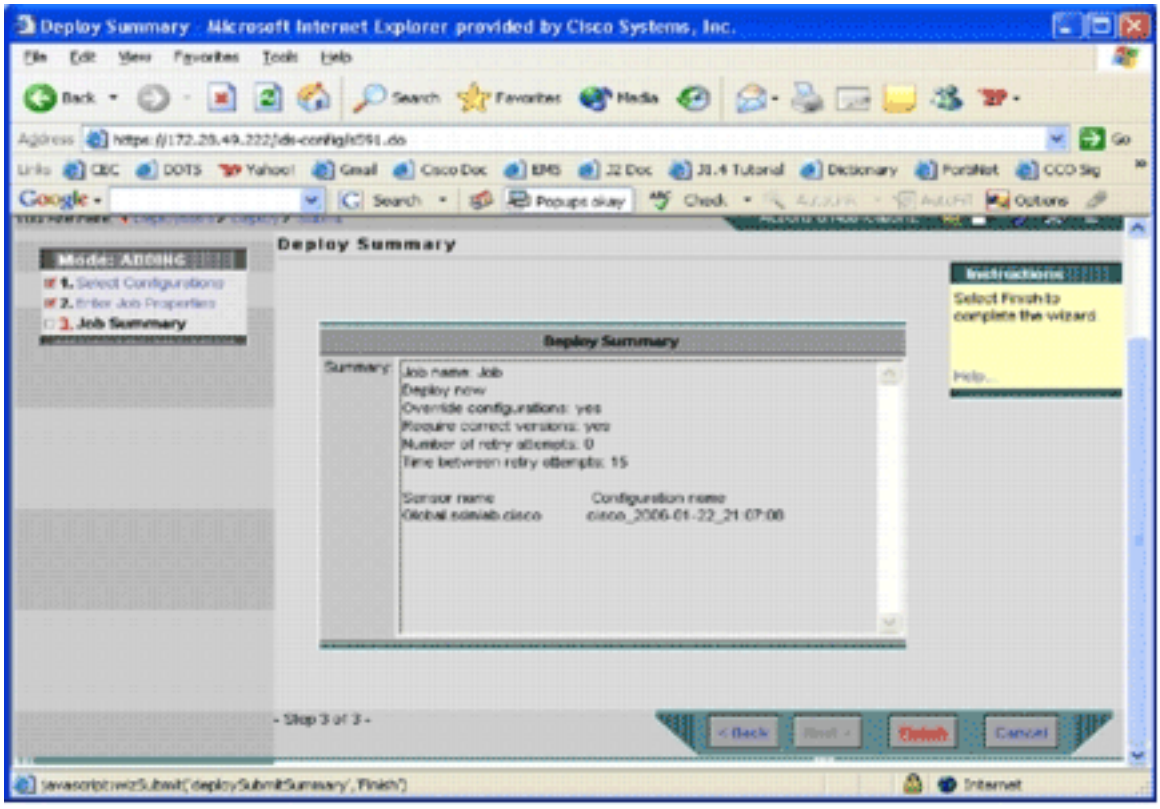
7. 选择要为其提交部署任务的设备。
8. 选择思科设备，然后单击**Deploy**。系统将显示“选择配置”页面。



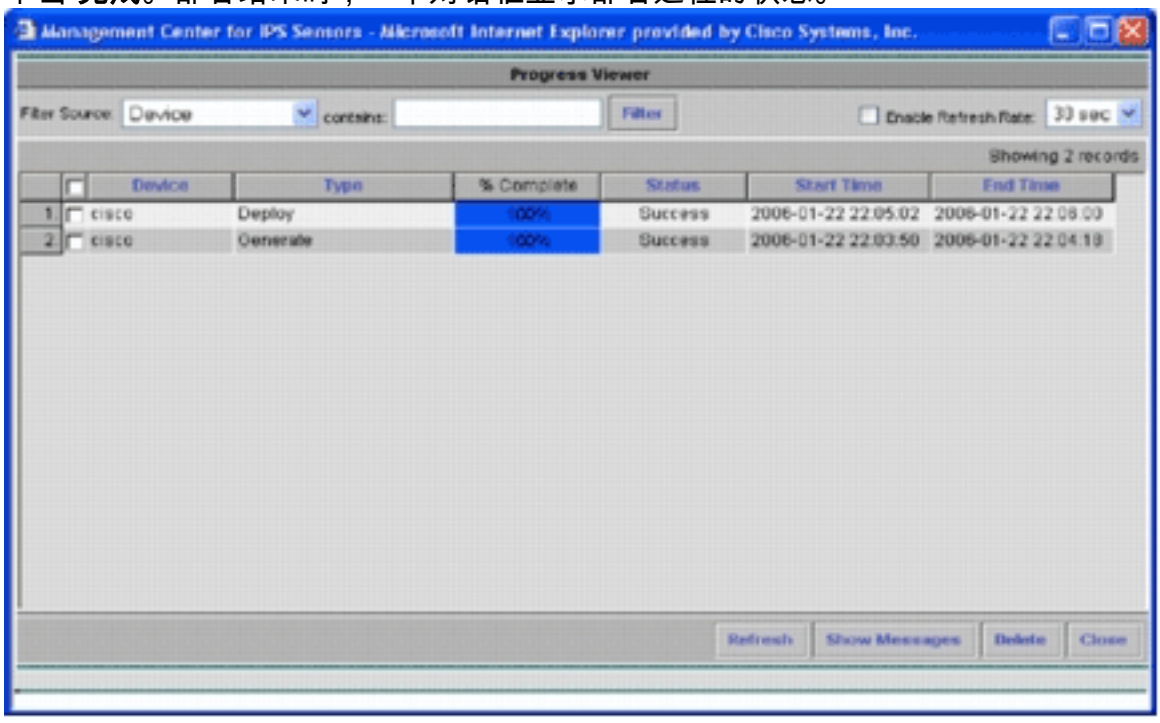
9. 选择刚对思科设备进行的*配置*，然后单击“下**一步**”。系统将显示“输入作业属性”页。



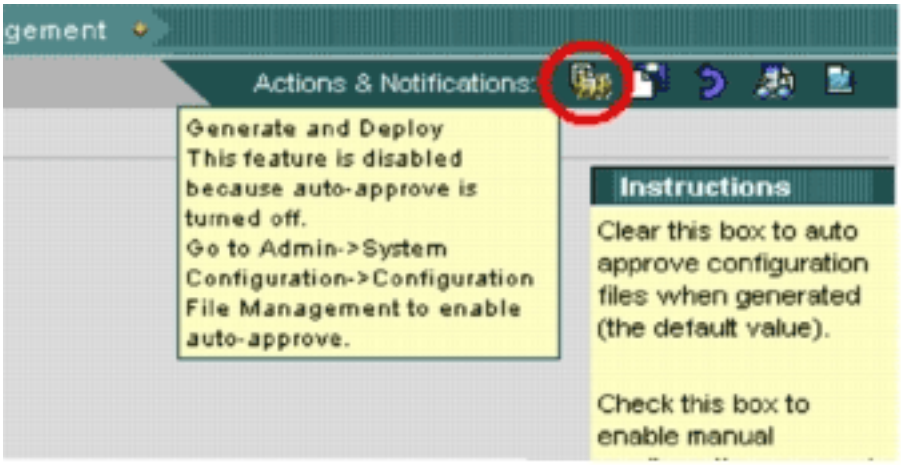
10. 您可以立即部署更改或安排任务在以后执行。在本例中，选择“立即”**选项**，然后单击“下**一步**”。系统将显示一个简要的作业摘要，并准备好进行部署。



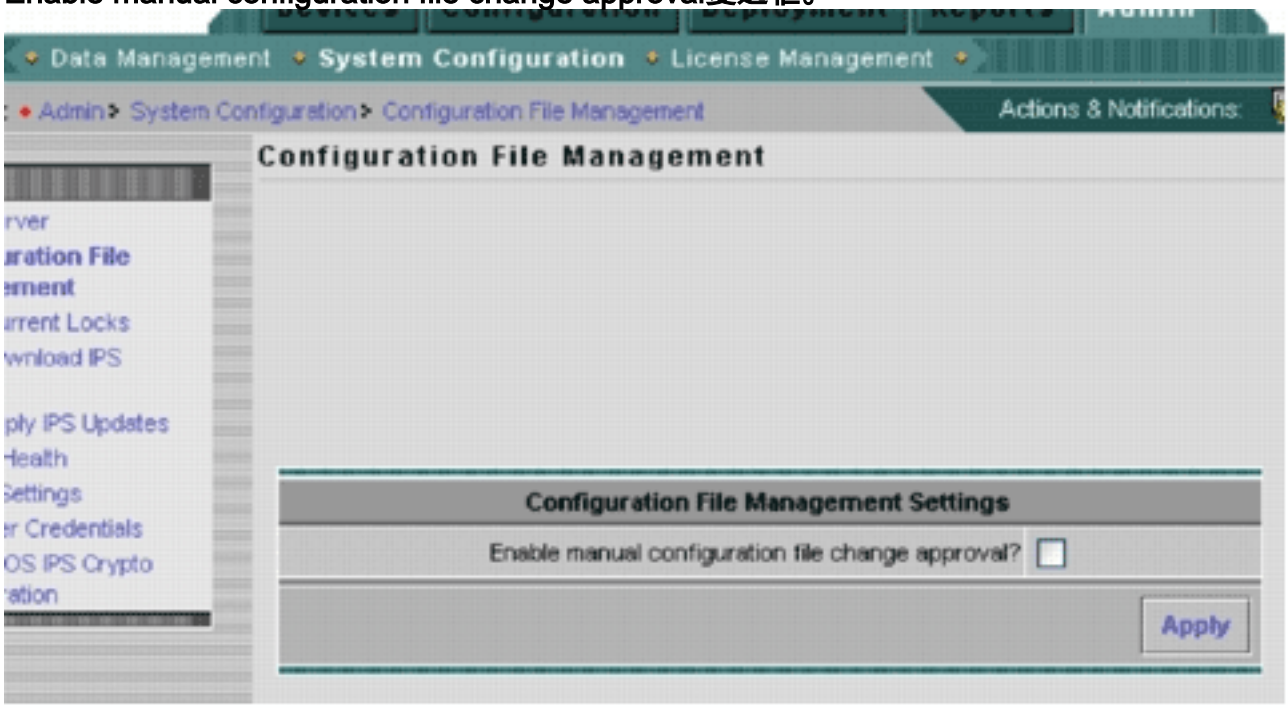
11. 单击 **完成**。部署结束时，一个对话框显示部署过程的状态。



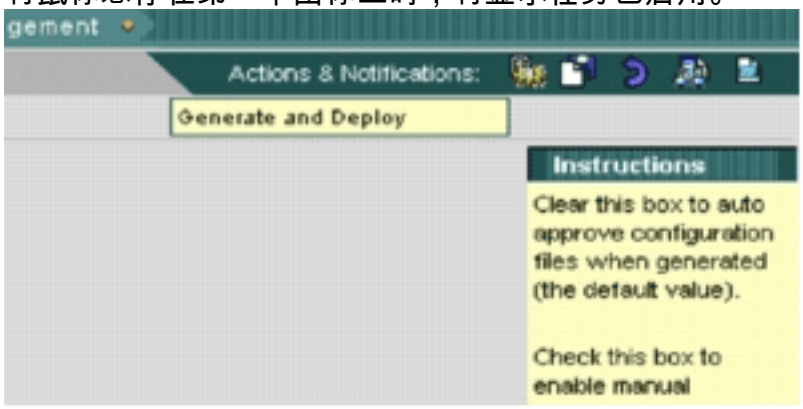
您已成功将Cisco IOS IPS配置部署到设备。配置多台设备时，可以在组级别进行配置更改，然后将更改应用到属于同一组的所有Cisco IOS IPS路由器。**提示：**此过程很长，但提供快速交付功能。使用此功能时，您无需执行“生成”>“批准”**>“部署”**过程。要使用该功能，请完成以下步骤：用户界面顶部有一行小图标。将鼠标悬停在第一个图标上，并查看此图像中显示的工具提



示：要启用生成和部署任务，请转到**Admin > System Configuration > Configuration File Management**，并取消选中**Enable manual configuration file change approval复选框。**



将鼠标悬停在第一个图标上时，将显示任务已启用。

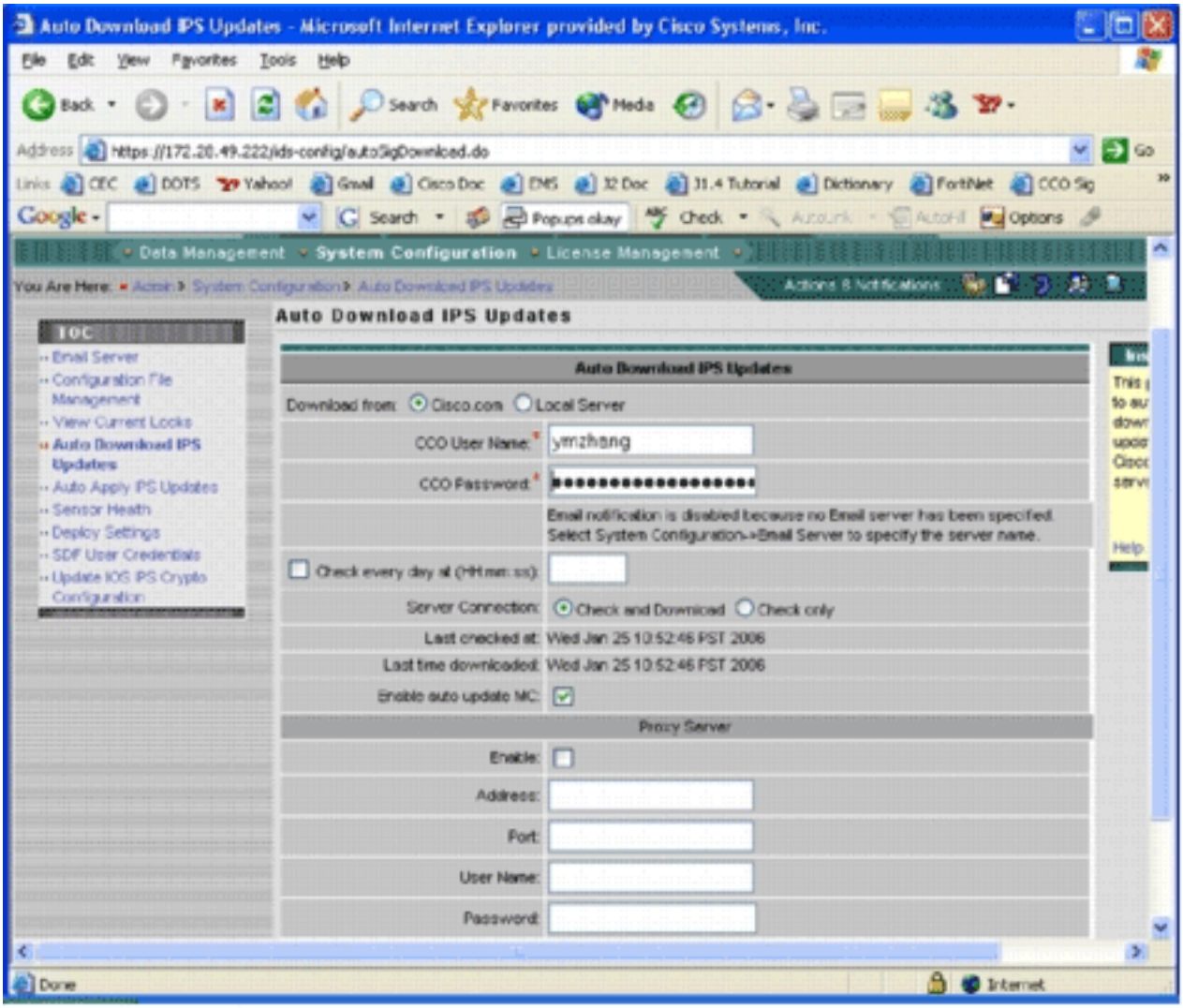


单击此图标。IPS MC自动生成配置更改并将其部署到设备。

自动下载签名更新

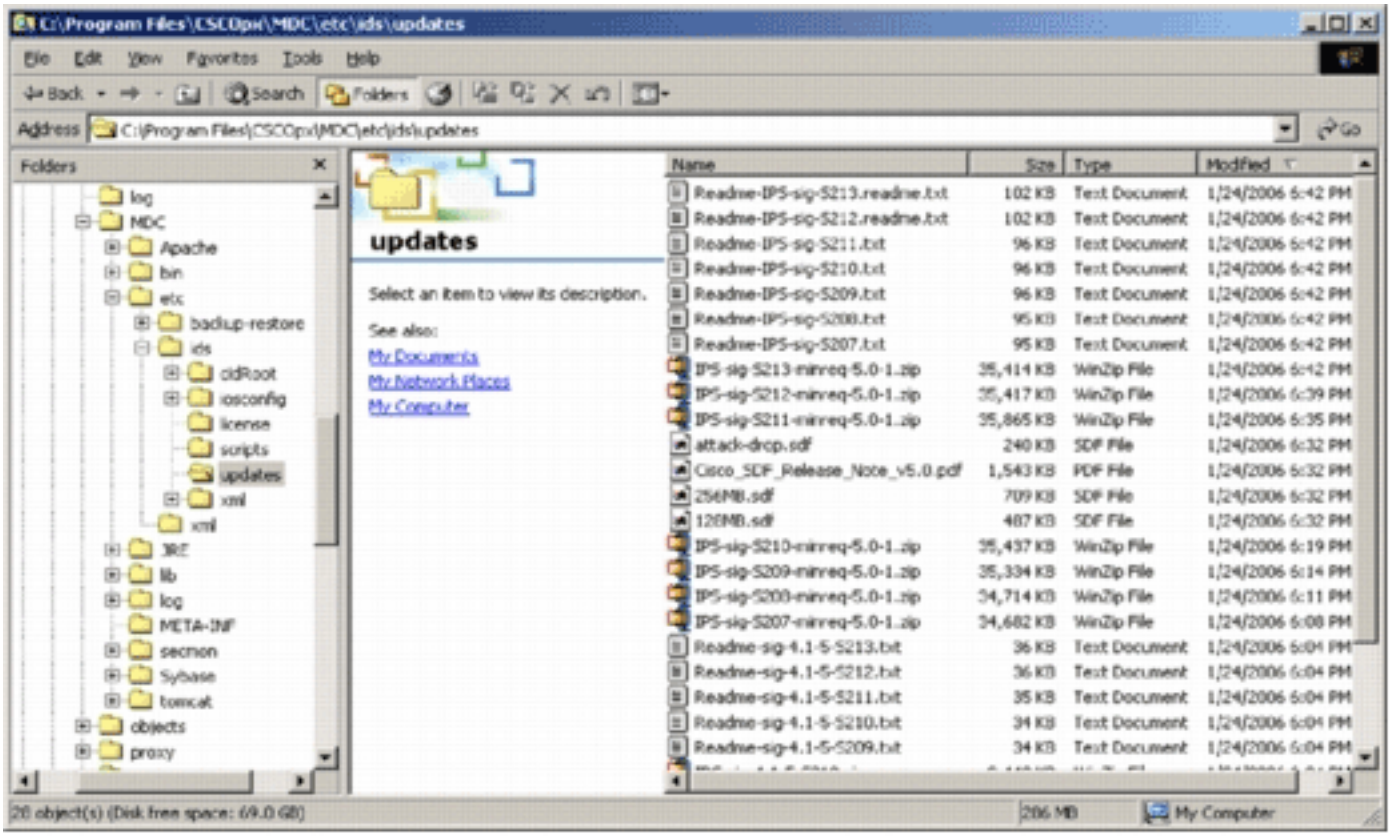
IPS MC支持从Cisco.com自动下载签名更新。它可以下载传感器平台以及Cisco IOS IPS平台的签名更新。要配置此功能，请转至**Admin > System Configuration > Auto Download IPS Updates**。

系统将显示Auto Download IPS Update页面。



您必须拥有有效的Cisco.com帐户才能下载此签名更新。要检查自动下载的文件，请转至IPS MC安装主目录。默认为\program files\CSCOpx\MDC\etc\ids\updates。

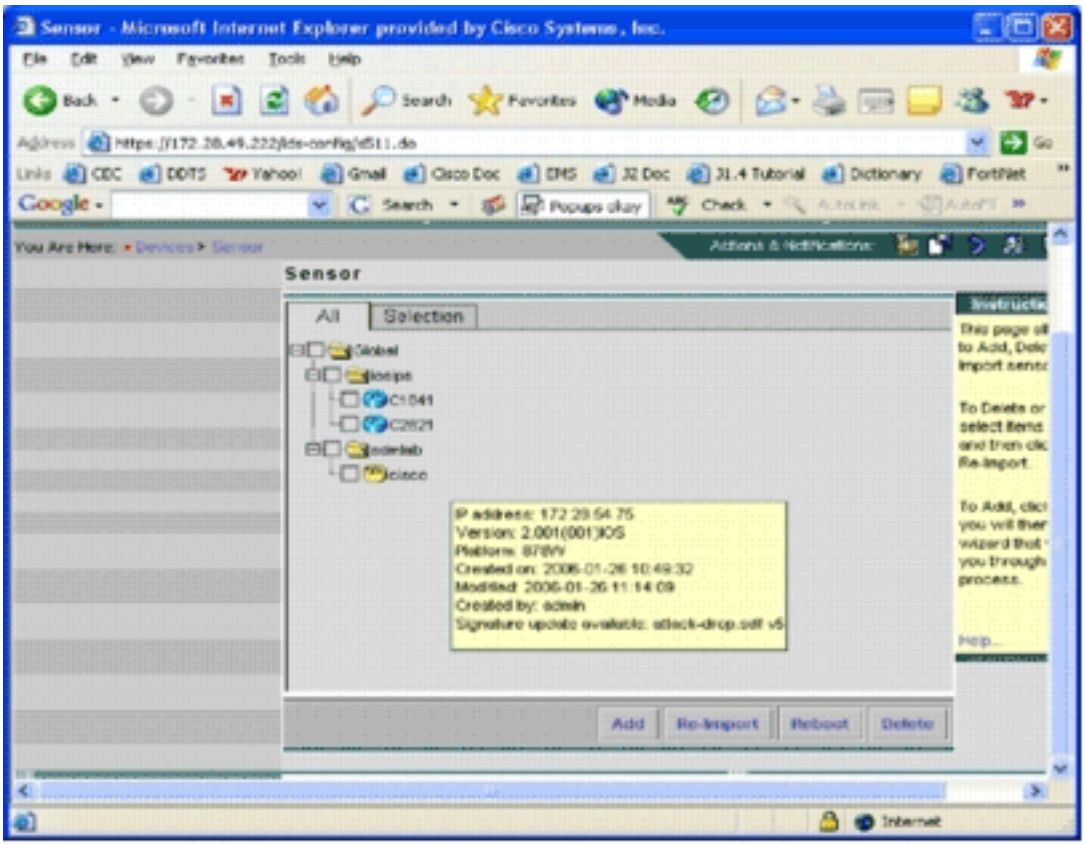
此图像显示此目录下下载文件的图像。



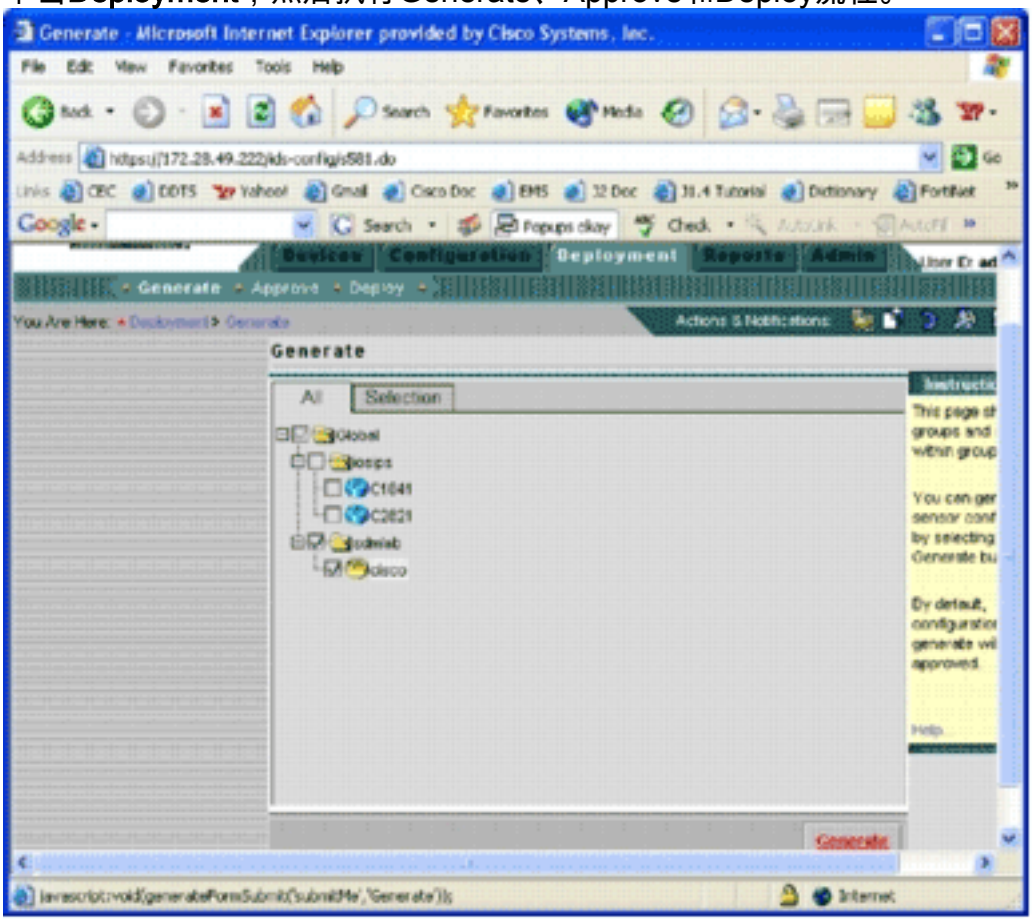
您可以看到传感器更新文件。下载Cisco IOS软件更新文件和预调SDF文件。

使用新的SDF文件更新Cisco IOS IPS路由器

对于使用预调SDF文件部署的Cisco IOS IPS路由器，只要通过自动下载或复制到更新目录中即可获得新版本的SDF文件，Cisco IPS MC就会识别新版本。用户界面刷新后，适用设备的设备图标变为黄色。



1. 单击**Deployment**，然后执行Generate、Approve和Deploy流程。



2. 成功部署后，Cisco IOS IPS路由器使用SDF文件的新版本。

相关信息

- Cisco Intrusion Prevention System