配置与ASDM的Active Directory集成，以实现单点登录和强制网络门户身份验证（机上管理）

目录

简介
先决条件
要求
使用的组件
背景信息
配置
步骤1.为单点登录配置Firepower用户代理。
步骤2.将Firepower模块(ASDM)与用户代理集成。
步骤3.将Firepower与Active Directory集成。
第3.1步创建领域。
第3.2步添加目录服务器IP地址/主机名。
第3.3步修改领域配置。
第3.4步下载用户数据库。
步骤4.配置身份策略。
步骤5.配置访问控制策略。
步骤6.部署访问控制策略。
步骤7.监控用户事件。
验证
Firepower模块与用户代理之间的连接（被动身份验证）
FMC和Active Directory之间的连接
ASA和终端系统之间的连接（主动身份验证）
策略配置和策略部署
故障排除
相关信息

简介

本文档介绍使用ASDM（自适应安全设备管理器）在Firepower模块上配置强制网络门户身份验证（主动身份验证）和单点登录（被动身份验证）。

先决条件

要求

Cisco 建议您了解以下主题：

- ASA（自适应安全设备）防火墙和ASDM知识
- FirePOWER模块知识

- 轻量级目录服务(LDAP)
- Firepower用户代理

使用的组件

本文档中的信息基于以下软件和硬件版本：

- 运行软件版本5.4.1及更高版本的ASA FirePOWER模块(ASA 5506X/5506H-X/5506W-X、ASA 5508-X、ASA 5516-X)。
- 运行软件版本6.0.0及更高版本的ASA FirePOWER模块(ASA 5515-X、ASA 5525-X、ASA 5545-X、ASA 5555-X)。

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。

背景信息

强制网络门户身份验证或主动身份验证提示登录页面和用户凭证是主机访问互联网所必需的。

单点登录或被动身份验证为用户提供网络资源和互联网访问的无缝身份验证，无需多次输入用户凭证。单点登录身份验证可通过Firepower用户代理或NTLM浏览器身份验证实现。

> **注意**：强制网络门户身份验证，ASA应处于路由模式。

> **注意**：ASA 9.5(2)版及更晚版本中提供强制网络门户命令。

配置

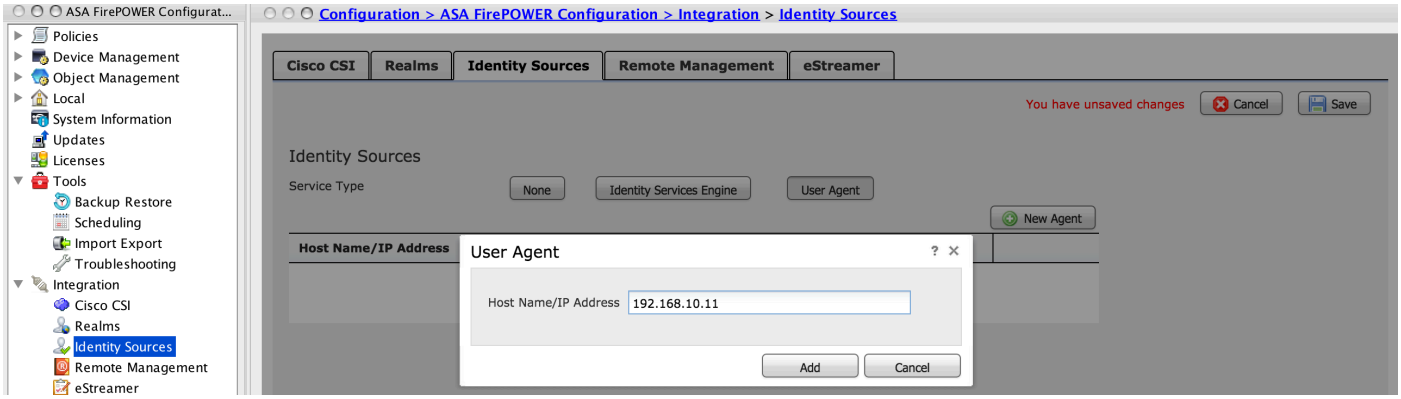
步骤1.为单点登录配置Firepower用户代理。

本文说明如何在Windows计算机中配置Firepower用户代理：

[安装和卸载Sourcefire用户代理]

第二步： 将Firepower模块(ASDM)与用户代理集成。

登录到ASDM，导航至**Configuration > ASA FirePOWER Configuration > Integration > Identity Sources，然**后单击**User Agent**选项。单击“用户代理”选项并配置用户代理系统的IP地址后。单击**Add**，如图所示：



单击“Save”按钮保存更改。

步骤3.将Firepower与Active Directory集成。

第3.1步创建领域。

登录到ASDM，导航至Configuration > ASA FirePOWER Configuration > Integration > Realms。单击“添加新领域”。

名称和说明：提供名称/说明以唯一标识领域。

类型：AD

AD主域：Active Directory的域名（NETBIOS名称）。

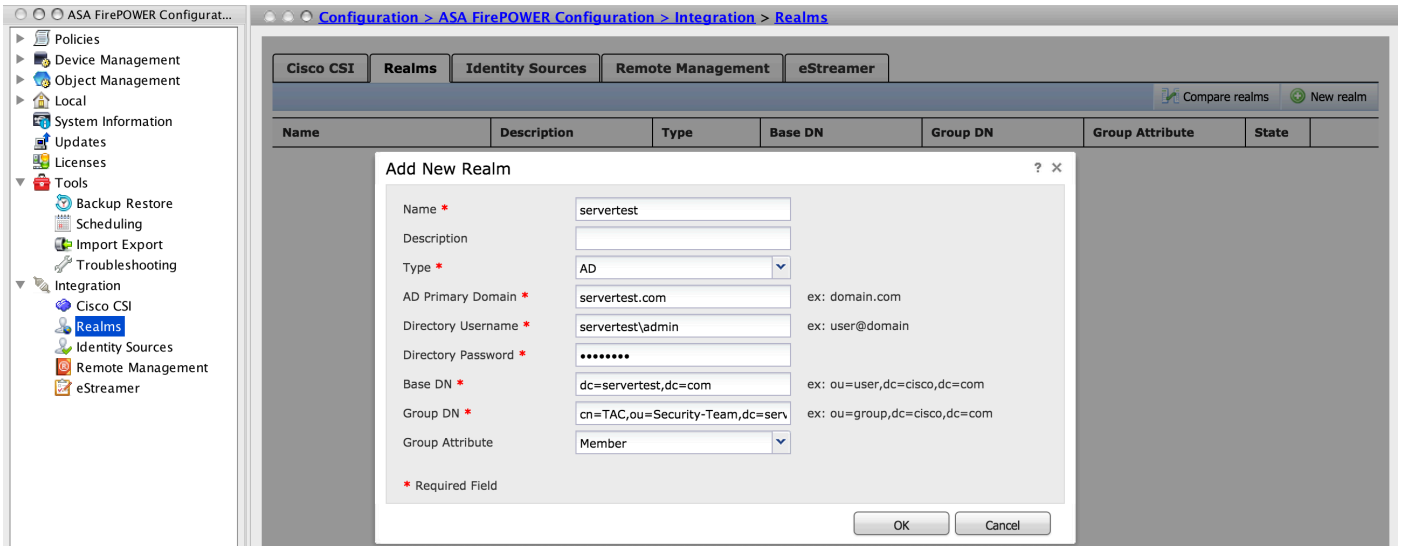
目录用户名：指定<*username*>。

目录密码： 指定<*password*>。

基本DN:系统将从其开始在LDAP数据库中搜索的域或特定OU DN。

组DN:指定组DN。

组属性：从下拉列表中指定选项Member。



单击“**确定**”保存配置。

本文可帮助您了解基本DN和组DN值。

[识别Active Directory LDAP对象属性]

第3.2步添加目录服务器IP地址/主机名。

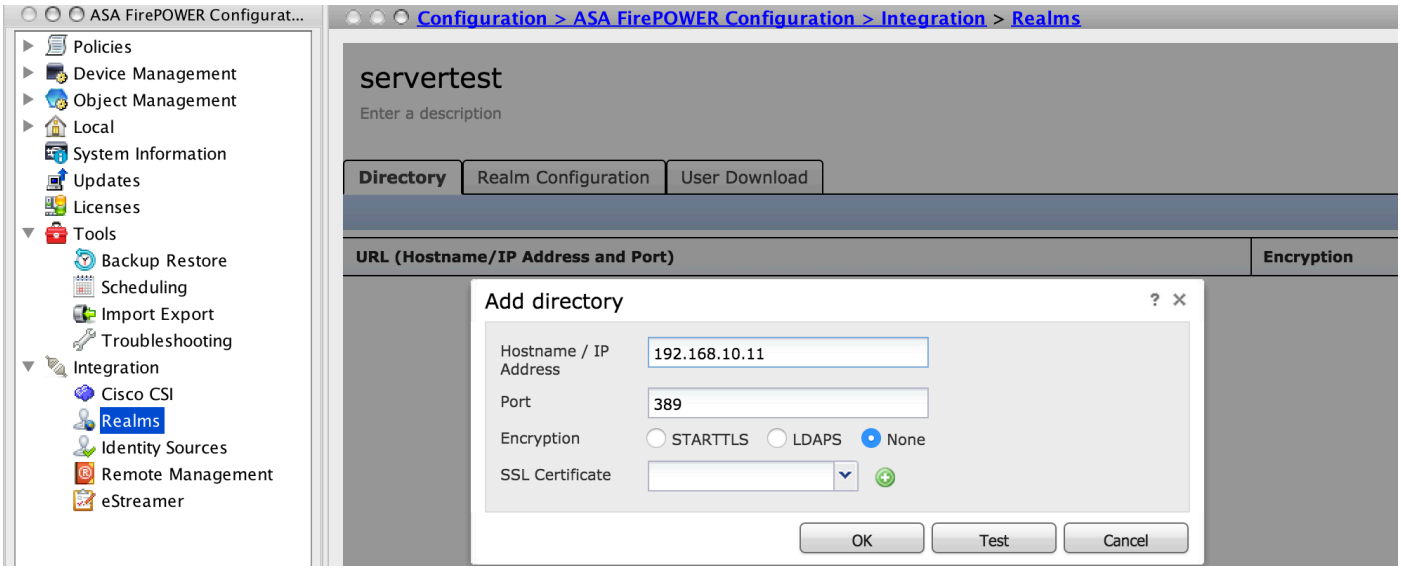
要指定AD服务器IP/主机名，请单击“添**加目录”**。

主机名/IP地址：配置AD服务器的IP地址/主机名。

端口： 指定Active Directory LDAP端口号（默认值389）。

加密/SSL证书：(可选)要加密FMC和AD服务器之间的连接，请参阅以下文章：

[验证FireSIGHT系统上的身份验证对象以通过SSL/T进行Microsoft AD身份验证……]



单击 **测试** 以验证FMC与AD服务器的连接。现在，单**击“**确定”保存配置。

第3.3步修改领域配置。

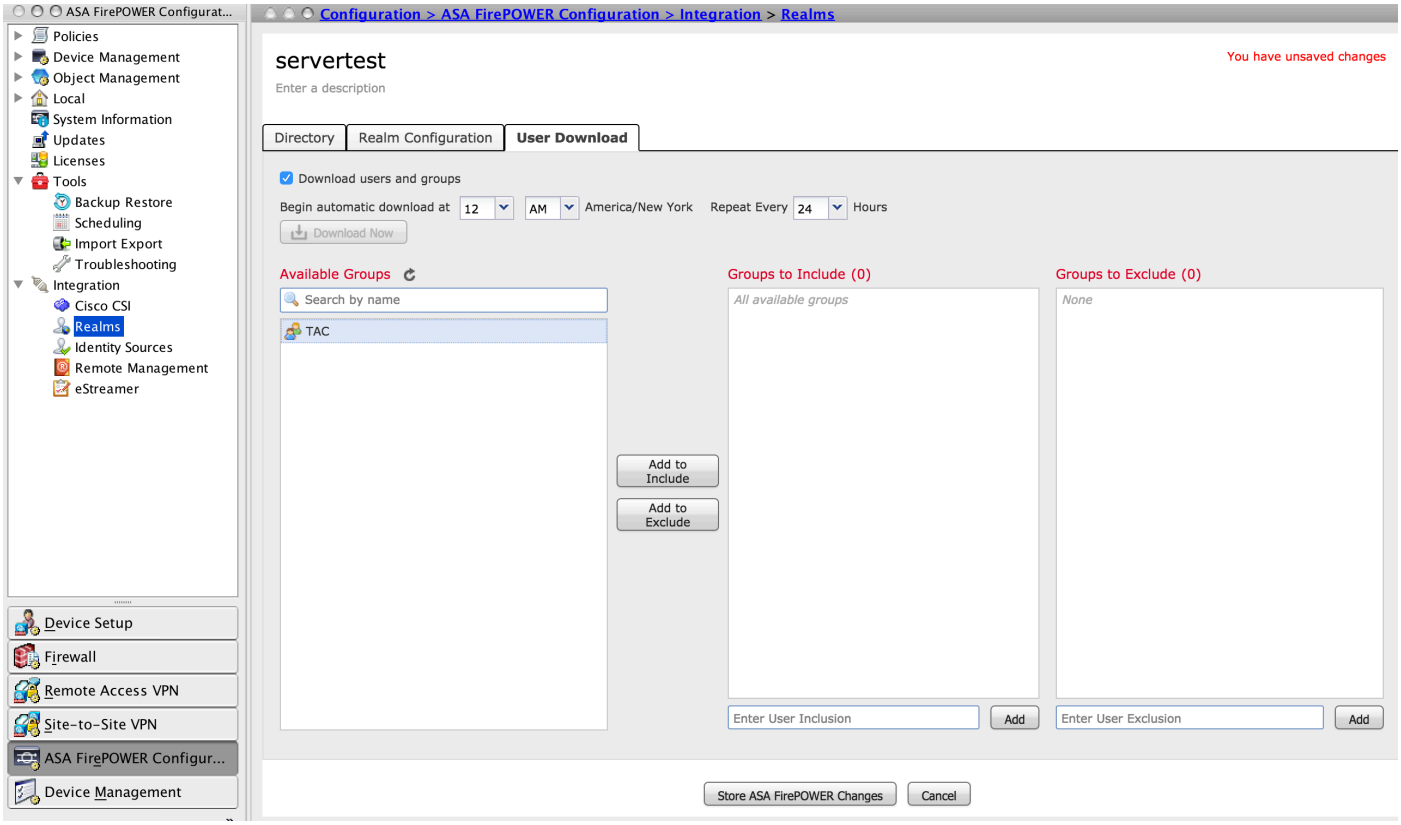
要修改和验证AD服务器的集成配置，请导航至领域**配置**。

第3.4步下载用户数据库。

导航至**用户下**载，从AD服务器获取用户数据库。

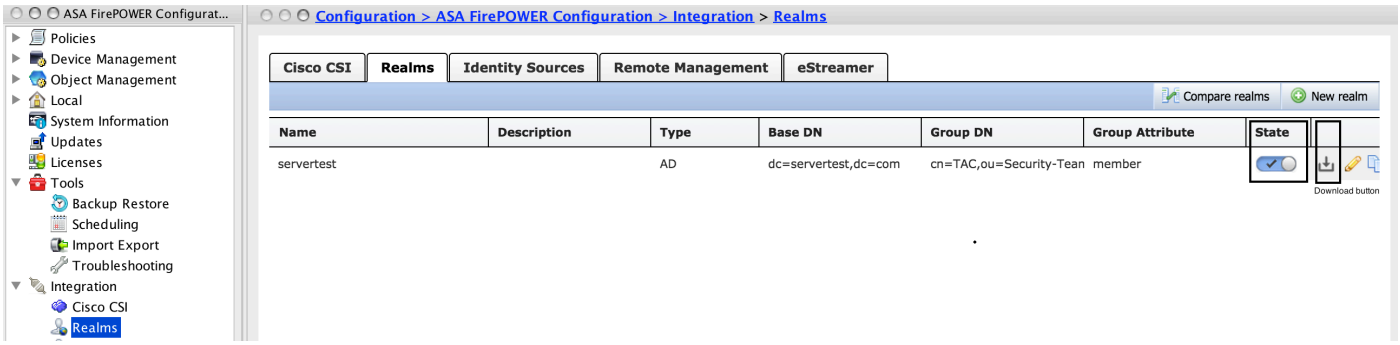
启用此复选框可下载“**下载用户和组”**，并定义有关Firepower模块与AD服务器联系以下载用户数据库的频率的时间间隔。

选择组并将其添加到要为其配置身份验证的**Include**选项。默认情况下，如果不选择包括组，则会选择所有组。



单击“Store ASA Firepower Changes(存储ASA Firepower更改)”以保存领域配置。

启用领域状态，然后点击下载按钮下载用户和组，如图所示。



步骤4.配置身份策略。

身份策略执行用户身份验证。如果用户不进行身份验证，则拒绝访问网络资源。这会对组织的网络和资源实施基于角色的访问控制(RBAC)。

第4.1步强制网络门户（主动身份验证）。

主动身份验证要求在浏览器上输入用户名和密码，以识别用户身份以允许任何连接。浏览器通过显示身份验证页面或以静默方式使用NTLM身份验证对用户进行身份验证。 NTLM使用Web浏览器发送和接收身份验证信息。主动身份验证使用各种类型来验证用户的身份。不同类型的身份验证包括：

1. **HTTP基本：在此方法中，浏览器会提示输入用户凭据。**
2. **NTLM: NTLM使用Windows工作站凭据，并使用Web浏览器与Active Directory协商。您需要在浏览器中启用NTLM身份验证。用户身份验证以透明方式进行，不提示凭证。它为用户提供单点登录体验。**

3. **HTTP协商**：在此类型中，系统尝试使用NTLM进行身份验证，如果失败，则传感器使用HTTP基本身份验证类型作为回退方法并提示对话框输入用户凭据。
4. **HTTP响应页：这类似于HTTP基本类型，但是，此处会提示用户在可自定义的HTML表单中填写身份验证。**

每个浏览器都有启用NTLM身份验证的特定方法，因此，您可以遵循浏览器指南以启用NTLM身份验证。

要安全地与路由传感器共享凭证，您需要在身份策略中安装自签名服务器证书或公签名服务器证书。

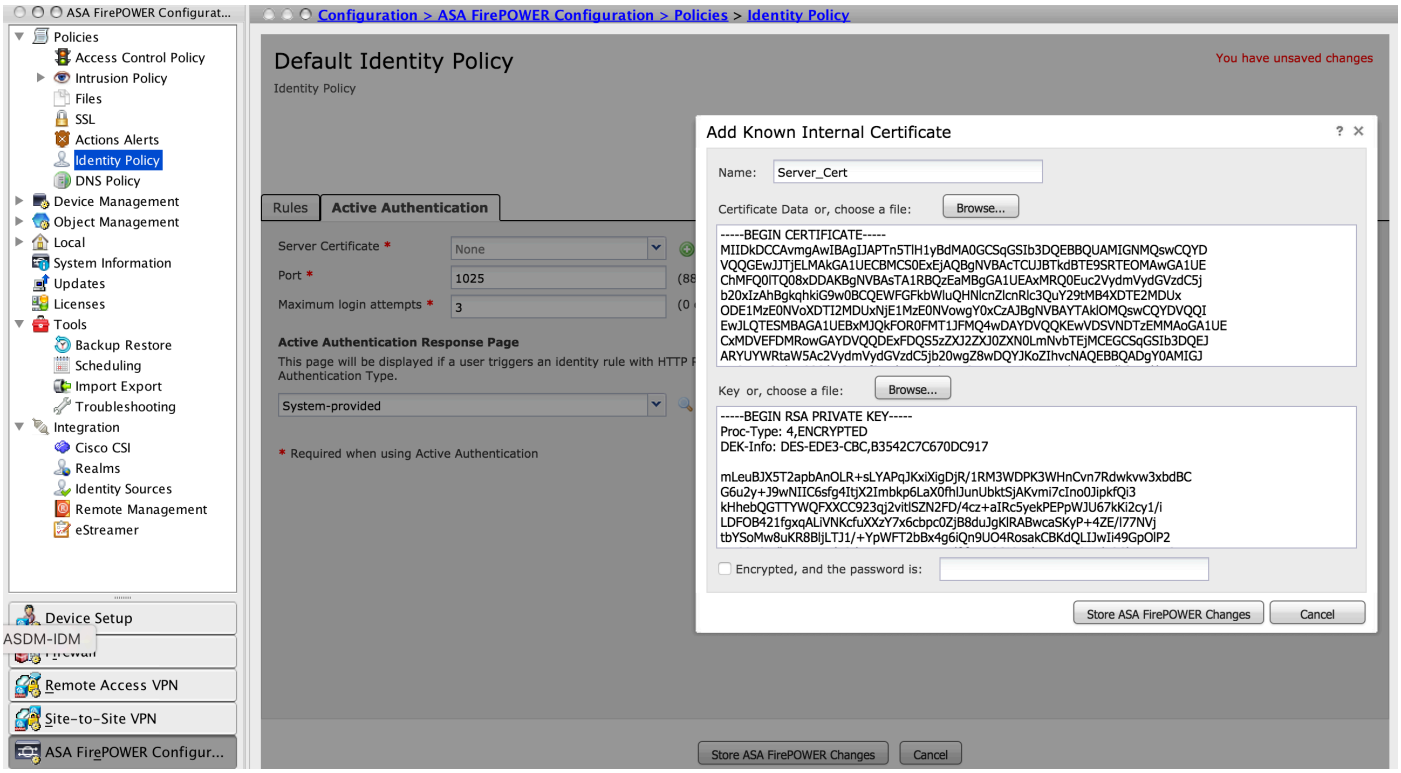
```
Generate a simple self-signed certificate using openSSL -

Step 1.   Generate the Private key
              openssl genrsa -des3 -out server.key 2048

Step 2.   Generate Certificate Signing Request (CSR)
              openssl req -new -key server.key -out server.csr

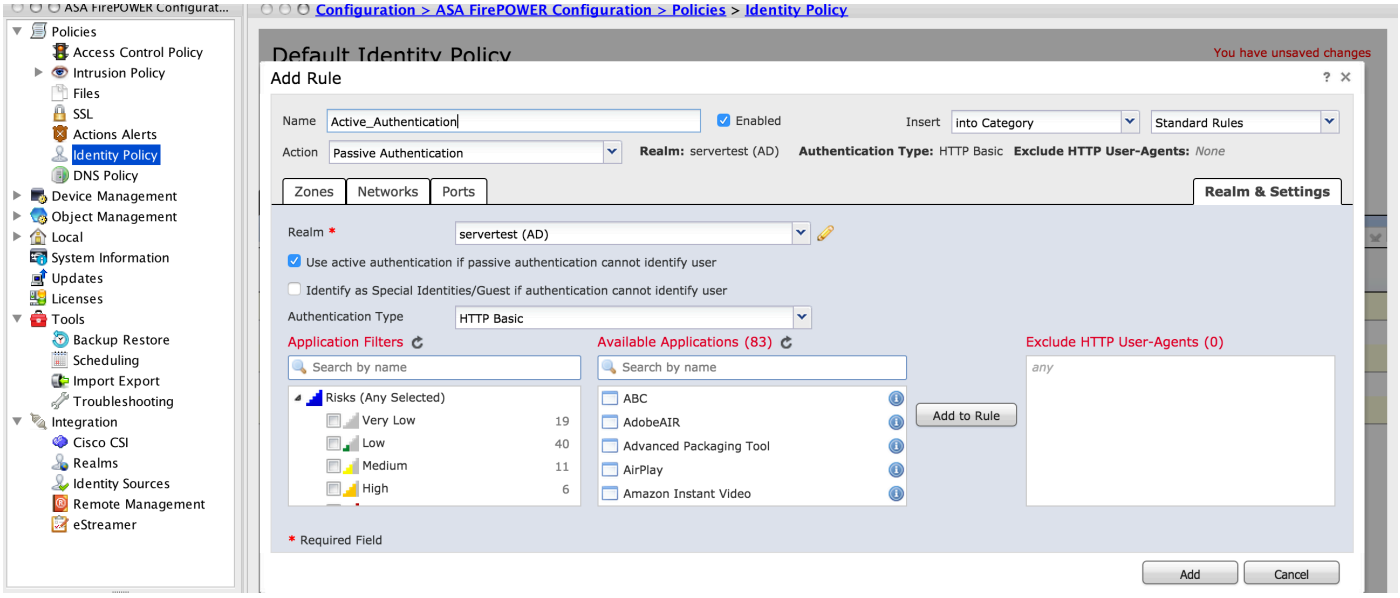
Step 3.   Generate the self-signed Certificate.
openssl x509 -req -days 3650 -sha256 -in server.csr -signkey server.key -out server.crt
```

导航至**Configuration > ASA FirePOWER Configuration > Policies > Identity Policy**。现在导航至**Active Authentication**选项卡，在Server Certificate**选**项中，单**击图标(+)** 并上传您在上一步中使用openSSL生成的证书和私钥，如图所示：



现在，单击**Add rule(添**加规则)为Rule（规则）指定名称，并选择该操作作为**Active Authentication(活动身**份)。定义要为其启用用户身份验证的源/目标区域、源/目标网络。

导航至领域**和设置选**项卡。从上一步中配置的下拉列表中选择**Realm**，然后从最适合您的网络环境的下拉列表中选择**Authentication Type**。



第4.2步强制网络门户的ASA配置。

步骤1.定义将重定向到Sourcefire进行检查的相关流量。

```
ASA(config)# access-list SFR_ACL extended permit ip 192.168.10.0 255.255.255.0 any
ASA(config)#
ASA(config)# class-map SFR_CMAP
ASA(config-cmap)# match access-list SFR_ACL
```

```
ASA(config)# policy-map global_policy
ASA(config-pmap)# class SFR_CMAP
ASA(config-pmap-c)# sfr fail-open
ASA(config)#service-policy global_policy global
```

步骤2.在ASA上配置此命令以启用强制网络门户。

```
ASA(config)# captive-portal interface inside port 1025
```

Active AuthenticationTCP 1025

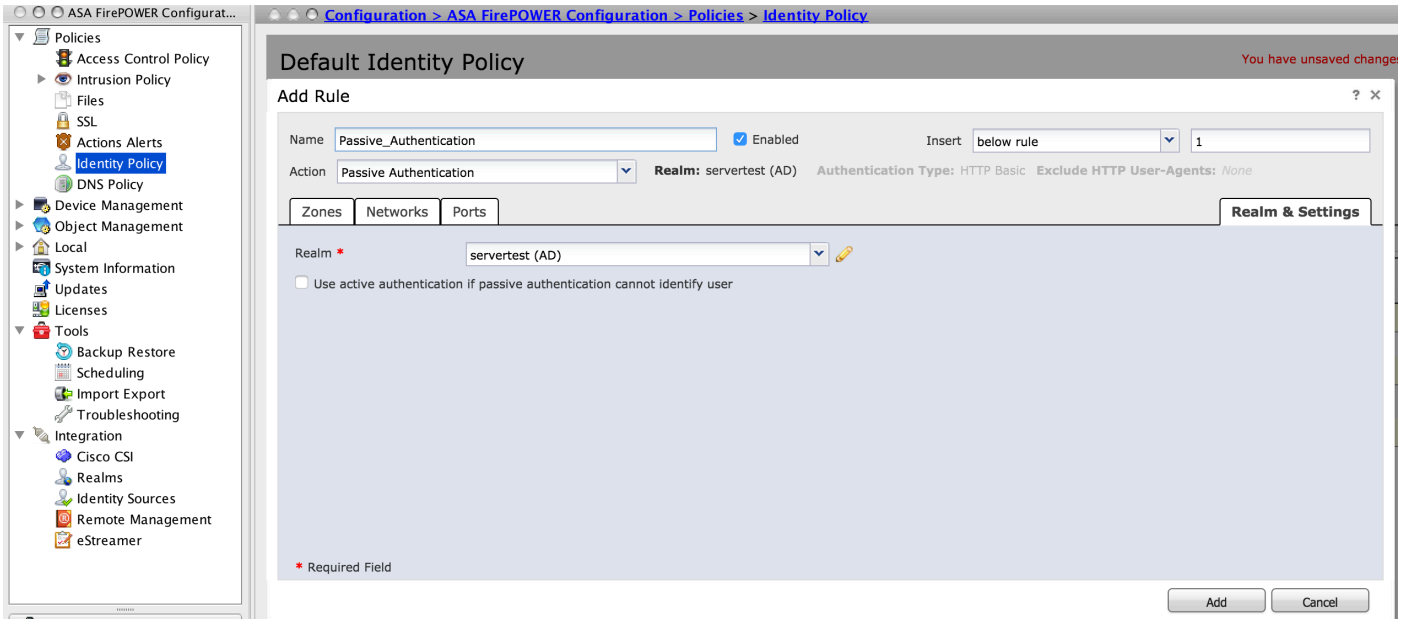
第4.3步单点登录（被动身份验证）。

在被动身份验证中，当域用户登录并能够对AD进行身份验证时，Firepower用户代理会从AD的安全日志轮询用户 — IP映射详细信息，并与Firepower模块共享此信息。Firepower模块使用这些详细信息来实施访问控制。

要配置被动身份验证规则，请单击**Add rule**为规则指定名称，然后选择**Action** 作为**Passive Authentication**。定义要为其启用用户身份验证的源/目标区域、源/目标网络。

导航至 **领域和设置** 选项卡选择 **领域** 从上一步配置的下拉列表。

如图所示，如果被动身份验证无**法识别用户身份，则可以选择回退方法作**为主动身份验证：

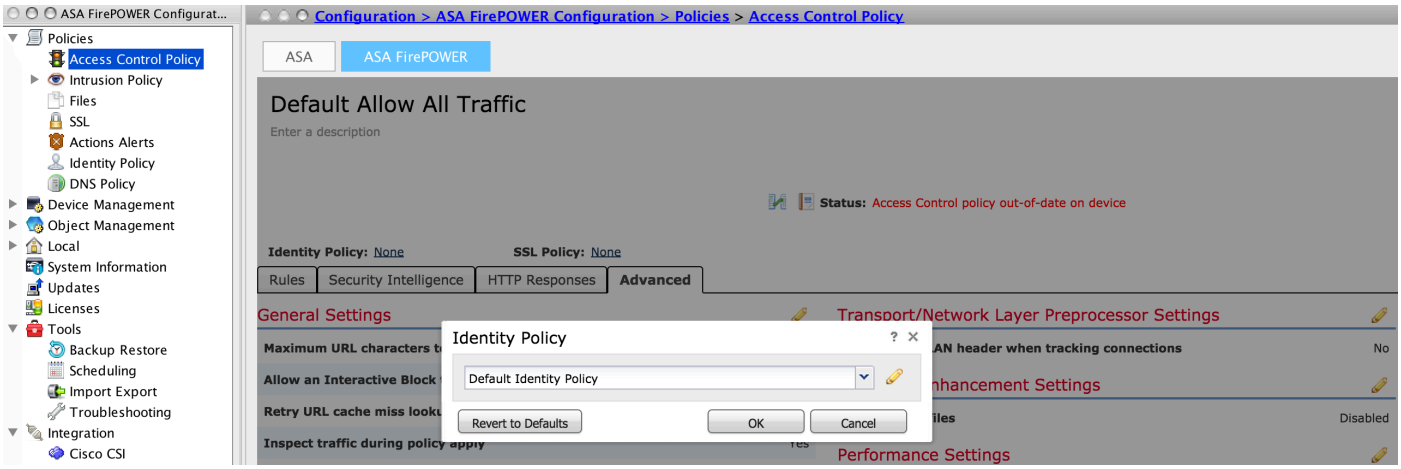


现在，单击**Store ASA Firepower Changes(存储ASA Firepower更**改)以保存身份策略的配置。

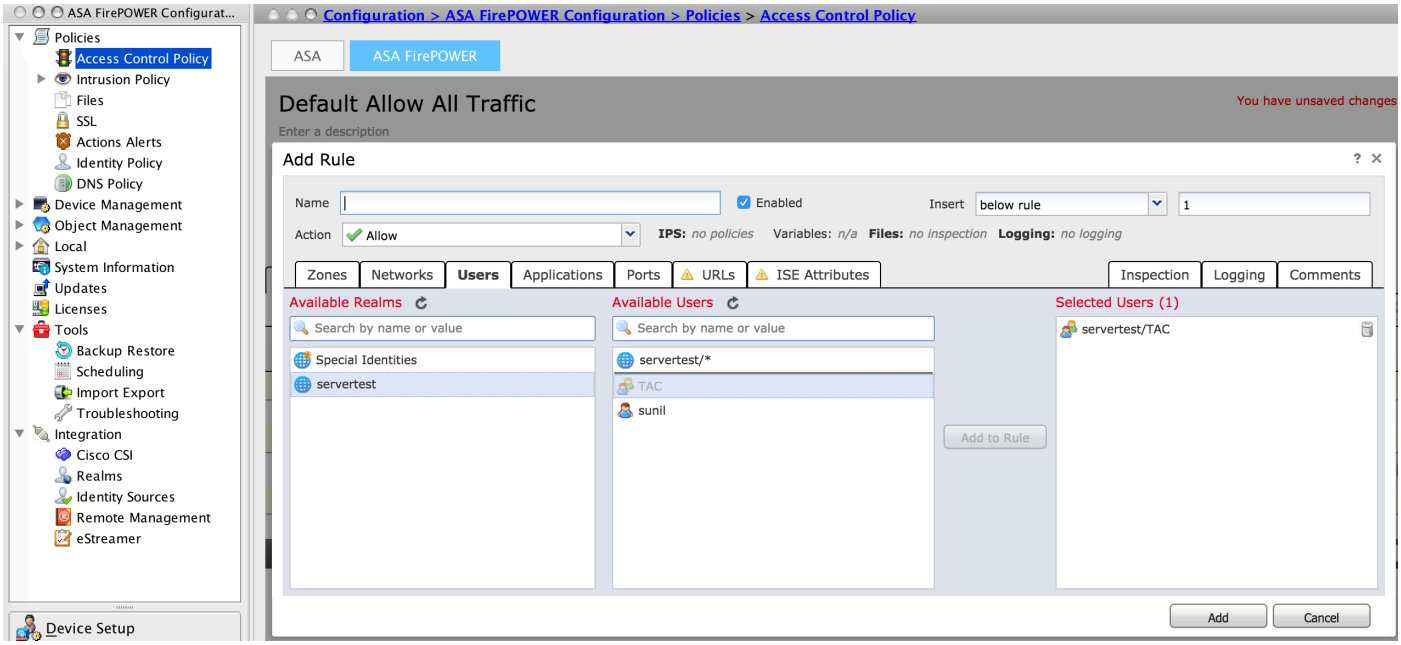
步骤5.配置访问控制策略。

导航至**Configuration > ASA FirePOWER Configuration > Policies > Access Control Policy。**

单击**Identity Policy**（左上角），从下拉列表中选择您在上一步中配置的Identify Policy，然后单击**OK**，如下图所示。



点击 **添加规则** 要添加新规则，请导航至 **用户** 并选择要为其实施访问控制规则的用户，如此图所示，然后单击**Add。**



点击 **存储ASA Firepower更改** 保存访问控制策略的配置。

步骤6.部署访问控制策略。

您必须部署访问控制策略。在应用策略之前，您将在模块上看到指示访问控制策略已过期。要将更改部署到传感器，请单击**部署**并选择**部署FirePOWER更改**选项，然后在弹出窗口中单击**部署**。

> **注意**：在版本5.4.x中，要将访问策略应用于传感器，您需要点击Apply ASA FirePOWER Changes（应用ASA FirePOWER更改）

> **注意**：导航至Monitoring > ASA Firepower Monitoring > Task Status。确保任务必须完成配置更改的应用。

步骤7.监控用户事件。

导航至**Monitoring > ASA FirePOWER Monitoring > Real-Time Eventing**，以监控用户使用的流量类型。

验证

使用本部分可确认配置能否正常运行。

导航至**Analysis > Users**，以验证与流量关联的用户身份验证/身份验证类型/用户 — IP映射/访问规则。

Firepower模块与用户代理之间的连接（被动身份验证）

Firepower模块使用TCP端口3306，以便从用户代理接收用户活动日志数据。

要验证Firepower模块的服务状态，请在FMC中使用此命令。

```
admin@firepower:~$ netstat -tan | grep 3306
```

在FMC上运行数据包捕获，以验证与用户代理的连接。

```
admin@firepower:~$ sudo tcpdump -i eth0 -n port 3306
```

FMC和Active Directory之间的连接

Firepower模块使用TCP端口389从Active Directory检索用户数据库。

在Firepower模块上运行数据包捕获，以验证与Active Directory的连接。

```
admin@firepower:~$ sudo tcpdump -i eth0 -n port 389
```

确保领域配置中使用的用户凭据具有获取AD用户数据库的足够权限。

验证领域配置，并确保已下载用户/组并正确配置用户会话超时。

导航至Monitoring ASA Firepower Monitoring Task Status（监控ASA Firepower监控任务状态），并确保任务用户/组下载成功完成，如此图所示。

ASA和终端系统之间的连接（主动身份验证）

主动身份验证，确保证书和端口在Firepower模块身份策略和ASA（captive-portal命令）中配置正确。 默认情况下，ASA和Firepower模块会侦听TCP端口885上的主动身份验证。

要验证活动规则及其命中计数，请在ASA上运行此命令。

```
ASA# show asp table classify domain captive-portal

Input Table
in  id=0x2aaadf516030, priority=121, domain=captive-portal, deny=false
   hits=10, user_data=0x0, cs_id=0x0, flags=0x0, protocol=6
   src ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any
   dst ip/id=19.19.19.130, mask=255.255.255.255, port=1025, tag=any, dscp=0x0
   input_ifc=inside, output_ifc=identity

Output Table:

L2 - Output Table:

L2 - Input Table:

Last clearing of hits counters: Never
```

策略配置和策略部署

确保在身份策略中正确配置领域、身份验证类型、用户代理和操作字段。

确保身份策略与访问控制策略正确关联。

导航至Monitoring > ASA Firepower Monitoring > Task Status，并确保策略部署成功完成。

故障排除

目前没有针对此配置的故障排除信息。

相关信息

- 技术支持和文档 - Cisco Systems
- 配置Active Directory与Firepower设备的集成，以进行单点登录和强制网络门户身份验证