配置Active Directory與ASDM的整合，以實現單點登入和強制網路門戶身份驗證（機箱內管理）

目錄

簡介

本文檔介紹使用ASDM（自適應安全裝置管理器）在Firepower模組上配置強制網路門戶身份驗證（主動身份驗證）和單點登入（被動身份驗證）。

必要條件

需求

思科建議您瞭解以下主題：

- ASA（自適應安全裝置）防火牆和ASDM知識
- FirePOWER模組知識

- 輕量級目錄服務(LDAP)
- Firepower使用者代理

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- 運行軟體版本5.4.1及更高版本的ASA FirePOWER模組(ASA 5506X/5506H-X/5506W-X、ASA 5508-X、ASA 5516-X)。
- 運行軟體版本6.0.0及更高版本的ASA FirePOWER模組(ASA 5515-X、ASA 5525-X、ASA 5545-X、ASA 555-X)。

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

背景資訊

強制網路門戶身份驗證或主動身份驗證提示登入頁面，主機需要使用者憑據才能訪問Internet。

單點登入或被動身份驗證為使用者提供無縫的網路資源和網際網路訪問身份驗證，而無需多次輸入使用者憑證。單點登入身份驗證可通過Firepower使用者代理或NTLM瀏覽器身份驗證實現。

注意：強制網路門戶身份驗證，ASA應處於路由模式。

附註：Captive portal命令在ASA 9.5(2)版及更高版本中可用。

設定

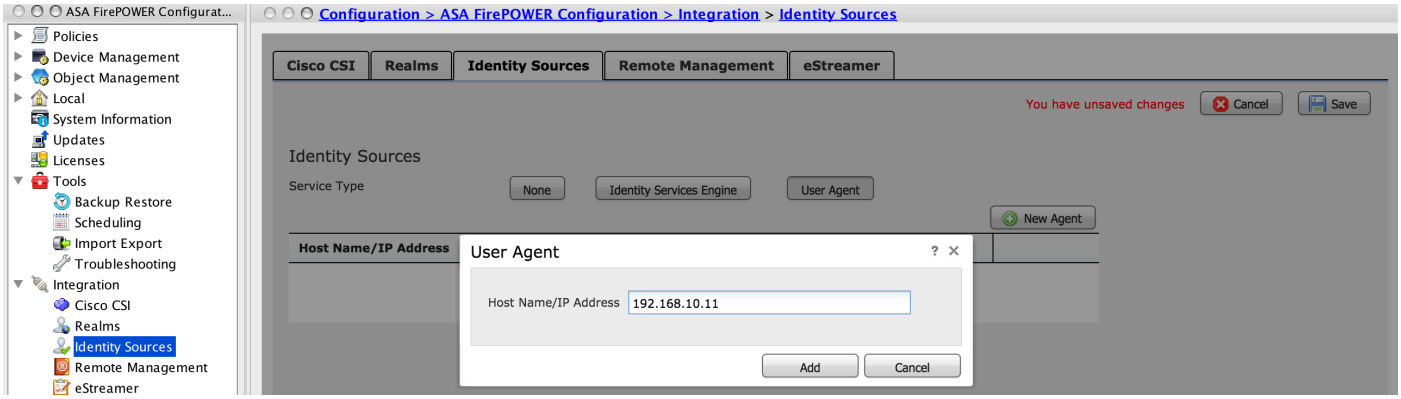
步驟1.配置Firepower使用者代理進行單點登入。

本文說明如何在Windows電腦中配置Firepower使用者代理：

[安裝和解除安裝Sourcefire使用者代理]

步驟2. 將Firepower模組(ASDM)與使用者代理整合。

登入到ASDM，導航到**Configuration > ASA FirePOWER Configuration > Integration > Identity Sources**，然後點選**User Agent**選項。按一下**User Agent**選項並配置使用者代理系統的IP地址之後。按一下**Add**，如下圖所示：



按一下Save按鈕儲存更改。

步驟3.將Firepower與Active Directory整合。

步驟3.1建立領域。

登入到ASDM，導航到Configuration > ASA FirePOWER Configuration > Integration > Realms。按一下**新增新領域**。

名稱和說明：提供名稱/說明以唯一標識領域。

文字：AD

AD主域：Active Directory的域名（NETBIOS名稱）。

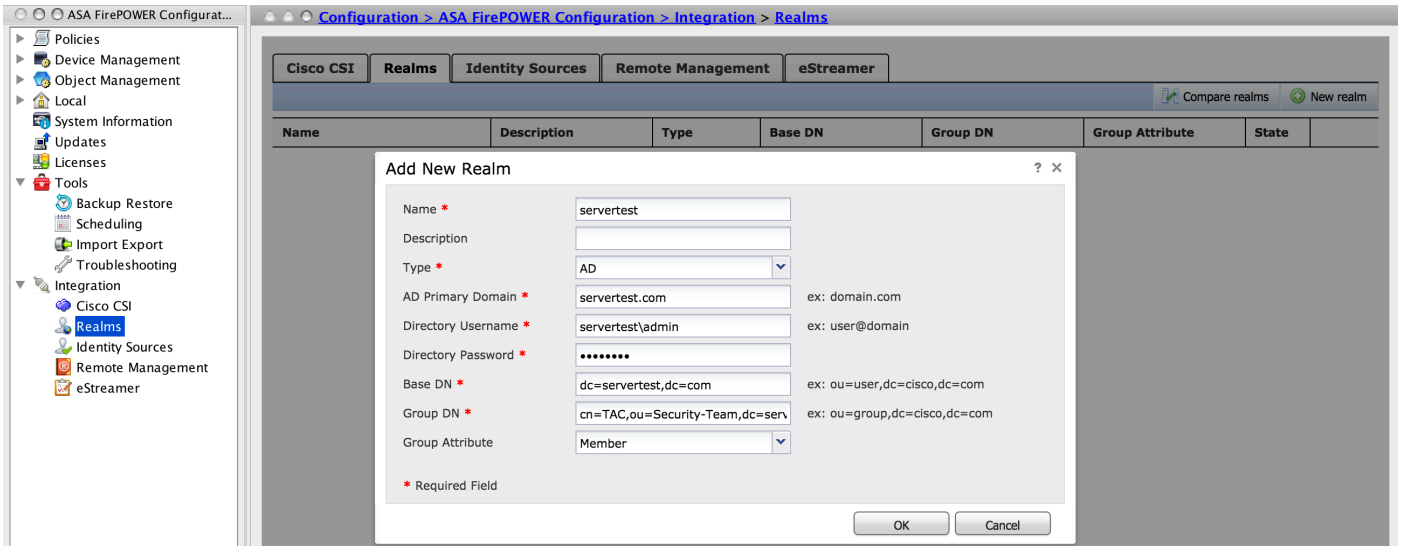
目錄使用者名：指定<*username*>。

目錄密碼： 指定<*password*>。

基本DN:系統從LDAP資料庫中開始搜尋的域或特定OU DN。

組DN:指定組DN。

組屬性：從下拉選單中指定Member選項。



按一下「OK」以儲存組態。

本文可以幫助您確定基本DN和組DN值。

[確定Active Directory LDAP對象屬性]

第3.2步新增目錄伺服器IP地址/主機名。

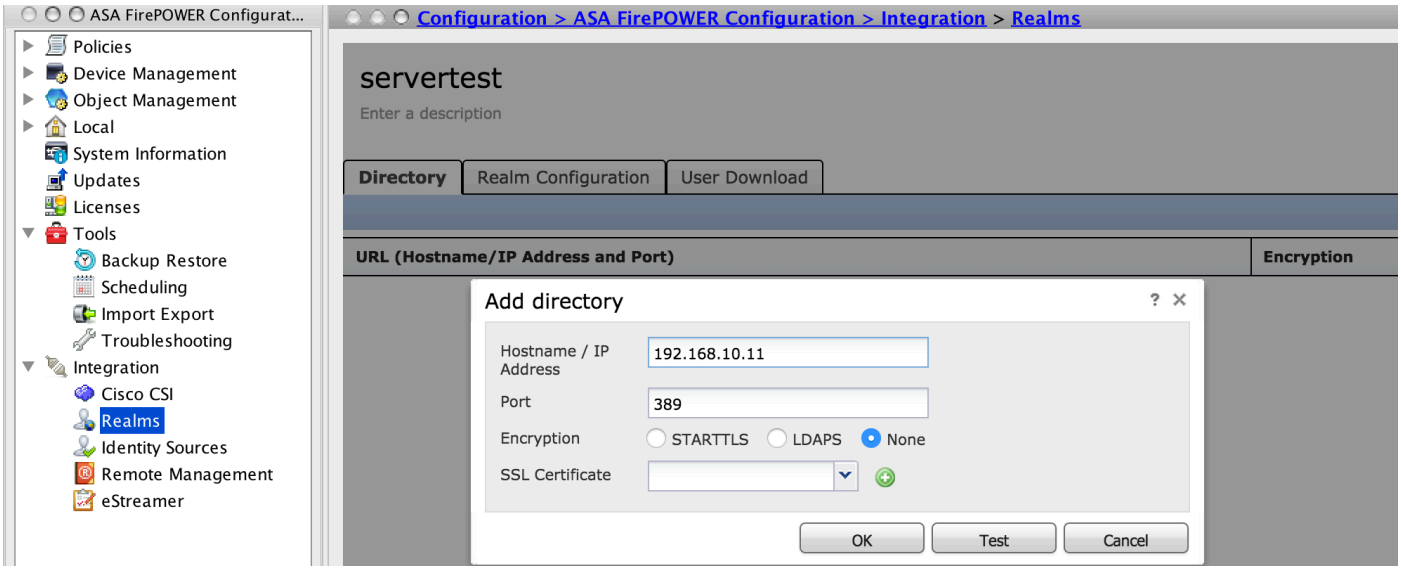
要指定AD伺服器IP/主機名，請按一下**Add directory**。

主機名/IP地址：配置AD伺服器的IP地址/主機名。

連接埠：指定Active Directory LDAP埠號（預設值389）。

Encryption/SSL Certificate：（可選）若要加密FMC與AD伺服器之間的連線，請參閱以下文章：

[驗證通過SSL/T進行Microsoft AD身份驗證的FireSIGHT系統上的身份驗證對象……]



按一下 **測試** 以驗證FMC與AD伺服器的連線。現在，按一下**OK**儲存配置。

步驟3.3修改領域配置。

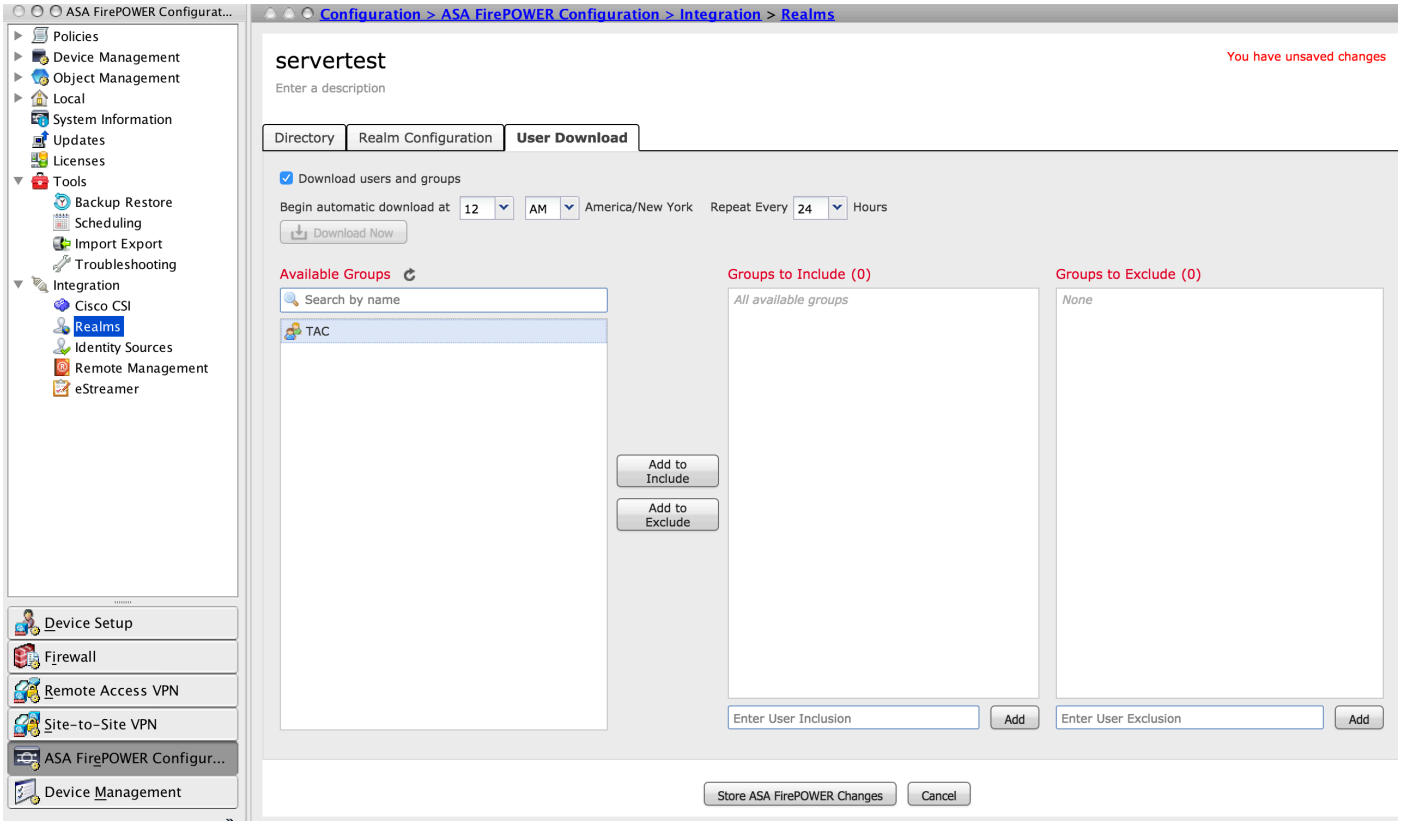
若要修改和驗證AD伺服器的整合配置，請導航到**領域配置**。

步驟3.4下載使用者資料庫。

導航到**User Download**，從AD伺服器獲取使用者資料庫。

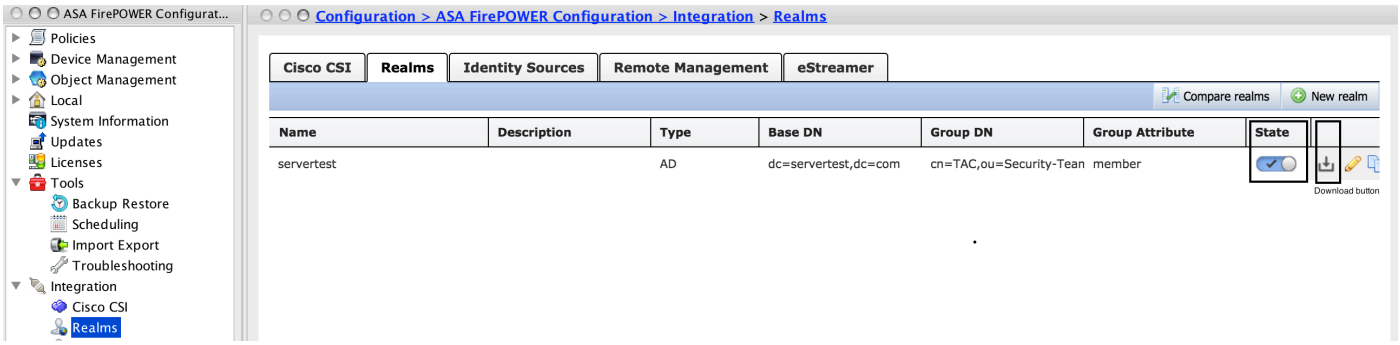
啟用此覈取方塊可下載**下載使用者和組**，並定義有關Firepower模組聯絡AD伺服器下載使用者資料庫的頻率的時間間隔。

選擇組並將其新增到要為其配置身份驗證的**Include**選項。預設情況下，如果您不選擇包括組，則會選擇所有組。



按一下**儲存ASA Firepower更改**以儲存領域配置。

啟用領域狀態並按一下下載按鈕可下載使用者和組，如下圖所示。



步驟4.配置身份策略。

身份策略執行使用者身份驗證。如果使用者未進行身份驗證，則拒絕訪問網路資源。這會對組織的網路和資源實施基於角色的訪問控制(RBAC)。

步驟4.1強制網路門戶（主動身份驗證）。

Active Authentication在瀏覽器中要求輸入使用者名稱和密碼，以標識允許任何連線的使用者身份。瀏覽器通過呈現身份驗證頁面或使用NTLM身份驗證以靜默方式驗證使用者。 NTLM使用Web瀏覽器來傳送和接收身份驗證資訊。主動身份驗證使用各種型別來驗證使用者的身份。不同型別的身份驗證包括：

1. **HTTP基本資訊：在此方法中，瀏覽器會提示輸入使用者憑證。**
2. **NTLM: NTLM使用Windows工作站憑據，並使用Web瀏覽器與Active Directory進行協商。您需要在瀏覽器中啟用NTLM身份驗證。使用者身份驗證以透明方式進行，不提示憑據。它為使用者提供單點登入體驗。**

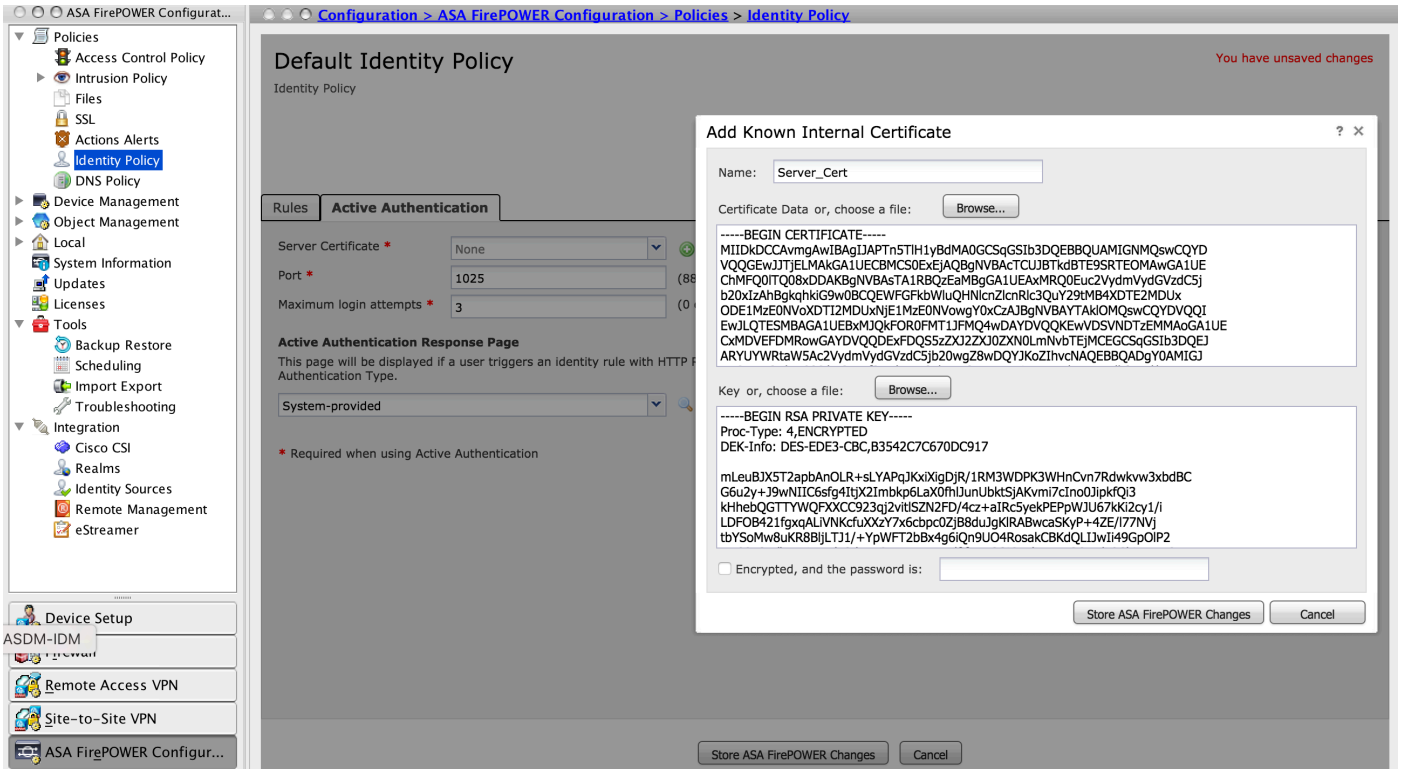
3. **HTTP協商：在此型別**中，系統嘗試使用NTLM進行身份驗證，如果失敗，則感測器使用HTTP基本身份驗證型別作為回退方法，並提示一個對話方塊來獲取使用者憑據。
4. **「HTTP響應」頁：這與HTTP基本型別類似，但是，在此提示使用者將身份驗證填寫到可自定義的HTML表單中。**

每個瀏覽器都有啟用NTLM身份驗證的特定方法，因此，您可以按照瀏覽器指南啟用NTLM身份驗證。

要安全地與路由感測器共用憑據，需要在身份策略中安裝自簽名伺服器證書或公開簽名的伺服器證書。

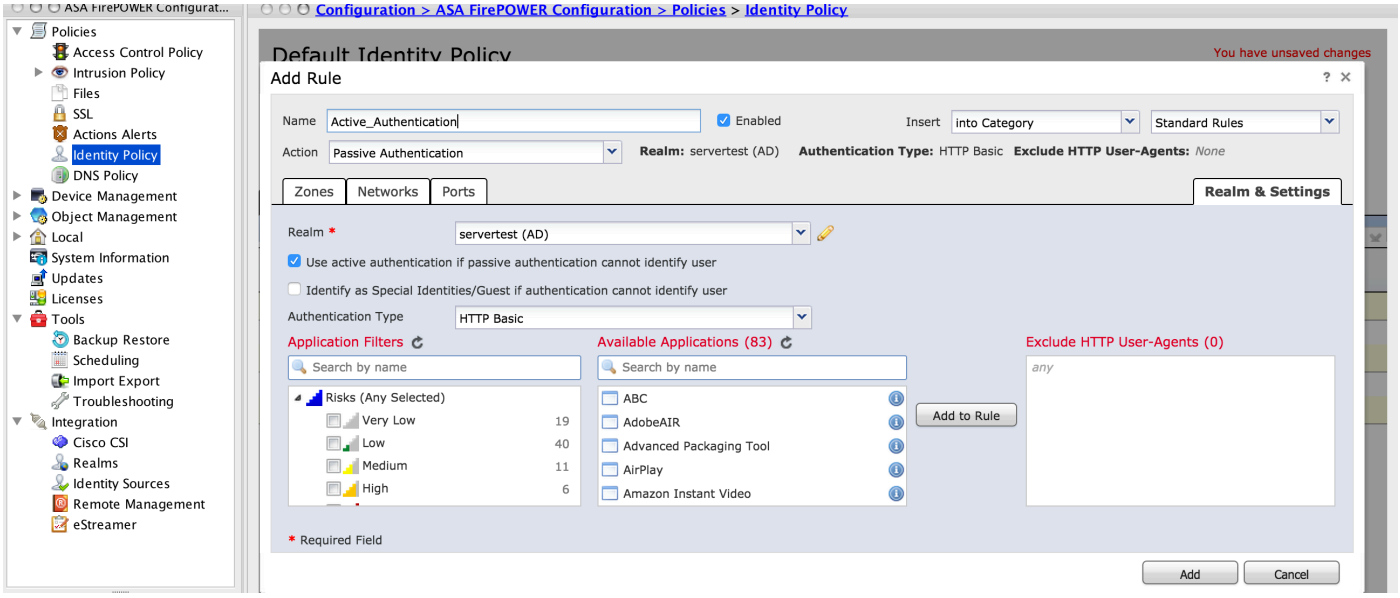
```
Generate a simple self-signed certificate using openSSL -

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
```

導航到**Configuration > ASA FirePOWER Configuration > Policies > Identity Policy**.現在導覽至**Active Authentication**索引標籤，然後在**Server Certificate**選項中，**按一下圖示(+)** 並使用openSSL上傳在上一步中產生的憑證和私密金鑰，如下圖所示：



現在，按一下**Add rule**為規則指定一個名稱，並選擇操作作為**Active Authentication**。定義要為其啟用使用者身份驗證的源/目標區域、源/目標網路。

導航到**Realm & Settings**選項卡。從已在上一步中配置的下拉選單中選擇**Realm**，然後從最適合網路環境的下拉選單中選擇**Authentication Type**。



步驟4.2強制網絡門戶的ASA配置。

步驟1.定義將重定向到Sourcefire以進行檢查的相關流量。

```
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
```

步驟2.在ASA上配置此命令以啟用強制網路門戶。

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

Active AuthenticationportTCP 1025

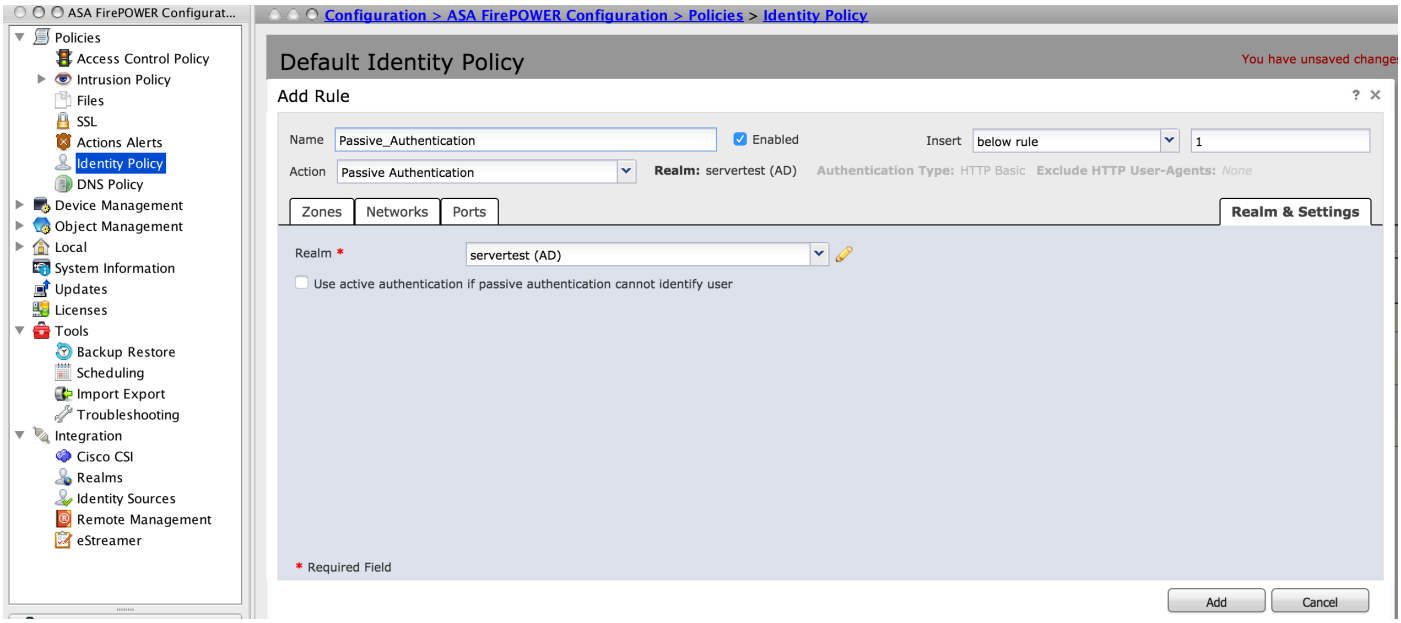
步驟4.3單點登入（被動身份驗證）。

在被動身份驗證中，當域使用者登入並能夠對AD進行身份驗證時，Firepower使用者代理從AD的安全日誌中輪詢使用者 — IP對映詳細資訊並與Firepower模組共用此資訊。Firepower模組使用這些詳細資訊實施訪問控制。

要配置被動身份驗證規則，請按一下**Add rule**為規則指定一個名稱，然後選擇**Action**作為**Passive Authentication**。定義要為其啟用使用者身份驗證的源/目標區域、源/目標網路。

導航至 **領域和設定** 頁籤。選擇 **領域** 下拉選單中，檢視您在上一步中配置的下拉選單。

如果被動驗證無法識別使用者身分，您可以在此選**擇回退方法作為主**動驗證，如下圖所示：

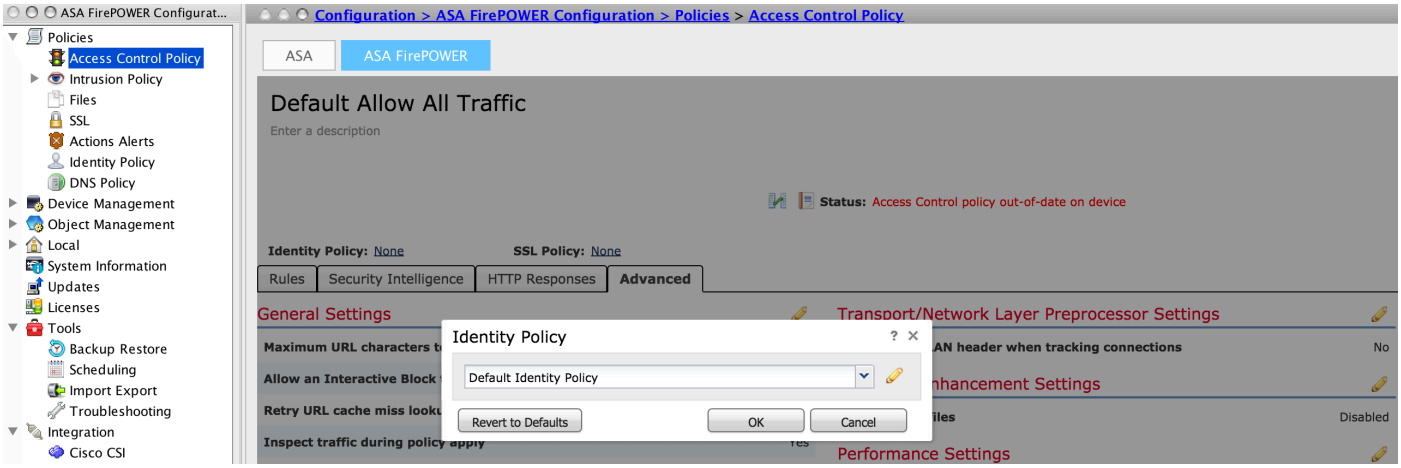


現在，按一下**儲存ASA Firepower更改**以儲存身份策略的配置。

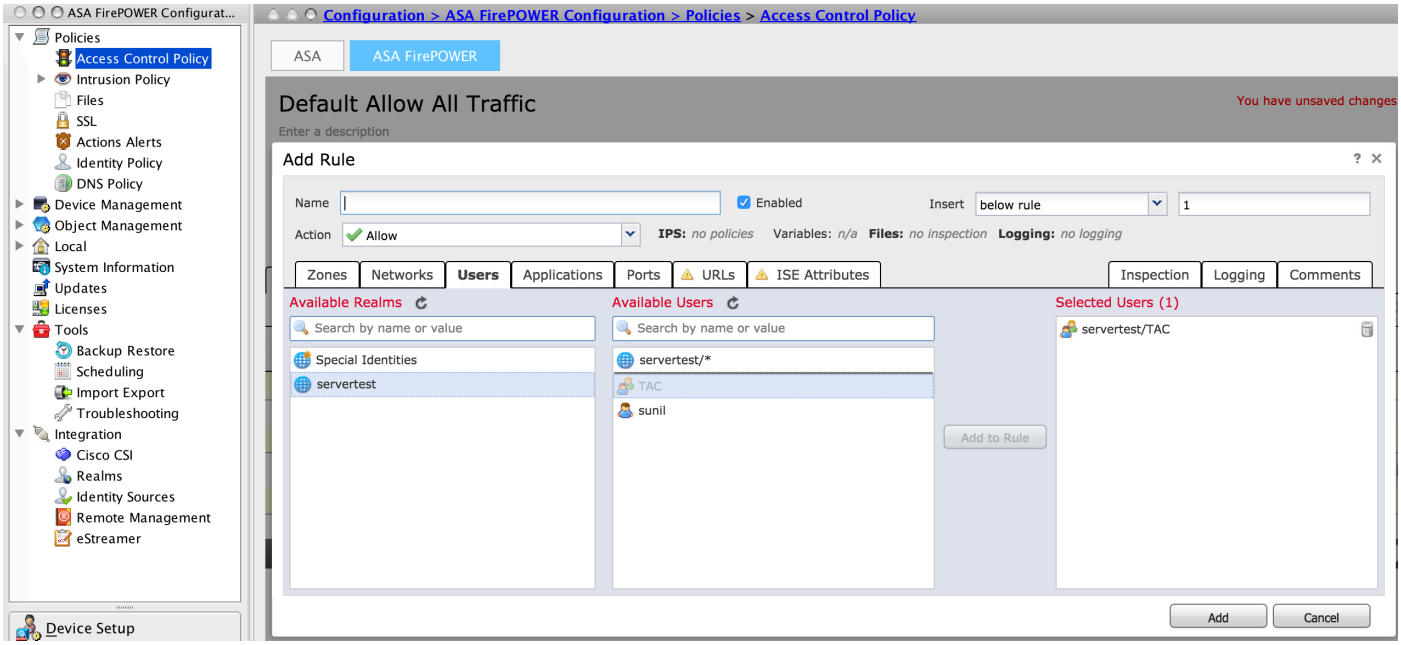
步驟5.配置訪問控制策略。

導航到Configuration > ASA FirePOWER Configuration > Policies > Access Control Policy。

按一下**Identity Policy**（左側上角），從下拉選單中選擇Identify Policy已在上一步中配置，然後按一下**OK**，如下圖所示。



按一下 **新增規則** 要新增新規則，請導航至 **使用者** 並選擇將為其強制執行訪問控制規則的使用者，如本圖所示，然後按一下**Add**.



按一下 **儲存ASA Firepower更改** 儲存訪問控制策略的配置。

步驟6.部署訪問控制策略。

您必須部署訪問控制策略。在應用策略之前，您會看到模組上的訪問控制策略已過期的指示。若要將更改部署到感測器，請按一下**部署**並選擇**部署FirePOWER更改選項**，然後在彈出視窗中按一下**部署**。

> **附註**：在5.4.x版本中，要將訪問策略應用到感測器，您需要點選Apply ASA FirePOWER Changes

> **附註**：導航到Monitoring > ASA Firepower Monitoring > Task Status。確保任務必須完成應用配置更改。

步驟7.監視使用者事件。

導航到**Monitoring > ASA FirePOWER Monitoring > Real-Time Eventing**，監控使用者使用的流量型別。

驗證

使用本節內容，確認您的組態是否正常運作。

導覽至**Analysis > Users**，以驗證與流量相關的使用者驗證/驗證型別/使用者 — IP對應/存取規則。

Firepower模組和使用者代理之間的連線（被動身份驗證）

Firepower模組使用TCP埠3306，以便從使用者代理接收使用者活動日誌資料。

為了驗證Firepower模組的服務狀態，請在FMC中使用此命令。

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

在FMC上運行資料包捕獲，以驗證與使用者代理的連線。

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

FMC和Active Directory之間的連線

Firepower模組使用TCP埠389從Active Directory中檢索使用者資料庫。

在Firepower模組上運行資料包捕獲以驗證與Active Directory的連線。

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

確保領域配置中使用的使用者憑據具有獲取AD的使用者資料庫的足夠許可權。

驗證領域配置，並確保已下載使用者/組並且正確配置使用者會話超時。

導航到Monitoring ASA Firepower Monitoring Task Status（監控ASA Firepower監控任務狀態），並確保任務使用者/組下載成功完成，如下圖所示。

ASA與終端系統之間的連線（主動身份驗證）

主動身份驗證，確保在Firepower模組身份策略和ASA（captive-portal命令）中正確配置證書和埠。預設情況下，ASA和Firepower模組偵聽TCP埠885上的活動身份驗證。

若要驗證活動規則及其命中計數，請在ASA上運行此命令。

```
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

確保在身份策略中正確配置領域、身份驗證型別、使用者代理和操作欄位。

確保身份策略與訪問控制策略正確關聯。

導航到Monitoring > ASA Firepower Monitoring > Task Status並確保策略部署成功完成。

疑難排解

目前尚無適用於此組態的具體疑難排解資訊。

相關資訊

- 技術支援與文件 - Cisco Systems
- 配置與Firepower裝置整合的Active Directory以實現單點登入和強制網路門戶身份驗證