# Configura autenticazione attiva FDM (Captive Portal)

## Sommario



## Introduzione

In questo documento viene descritto un esempio di configurazione per Firepower Device Manager (FDM) con integrazione Active Authentication (Captive-Portal). In questa configurazione viene utilizzato Active Directory (AD) come certificato di origine e autofirmato.

## Prerequisiti

### Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Cisco Firepower Threat Defense (FTD)
- Active Directory (AD)
- Certificati autofirmati.
- SSL (Secure Sockets Layer)

### Componenti usati

Le informazioni di questo documento si basano sulla seguente versione del software:

- Firepower Threat Defense 6.6.4
- Active Directory
- test PC

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.

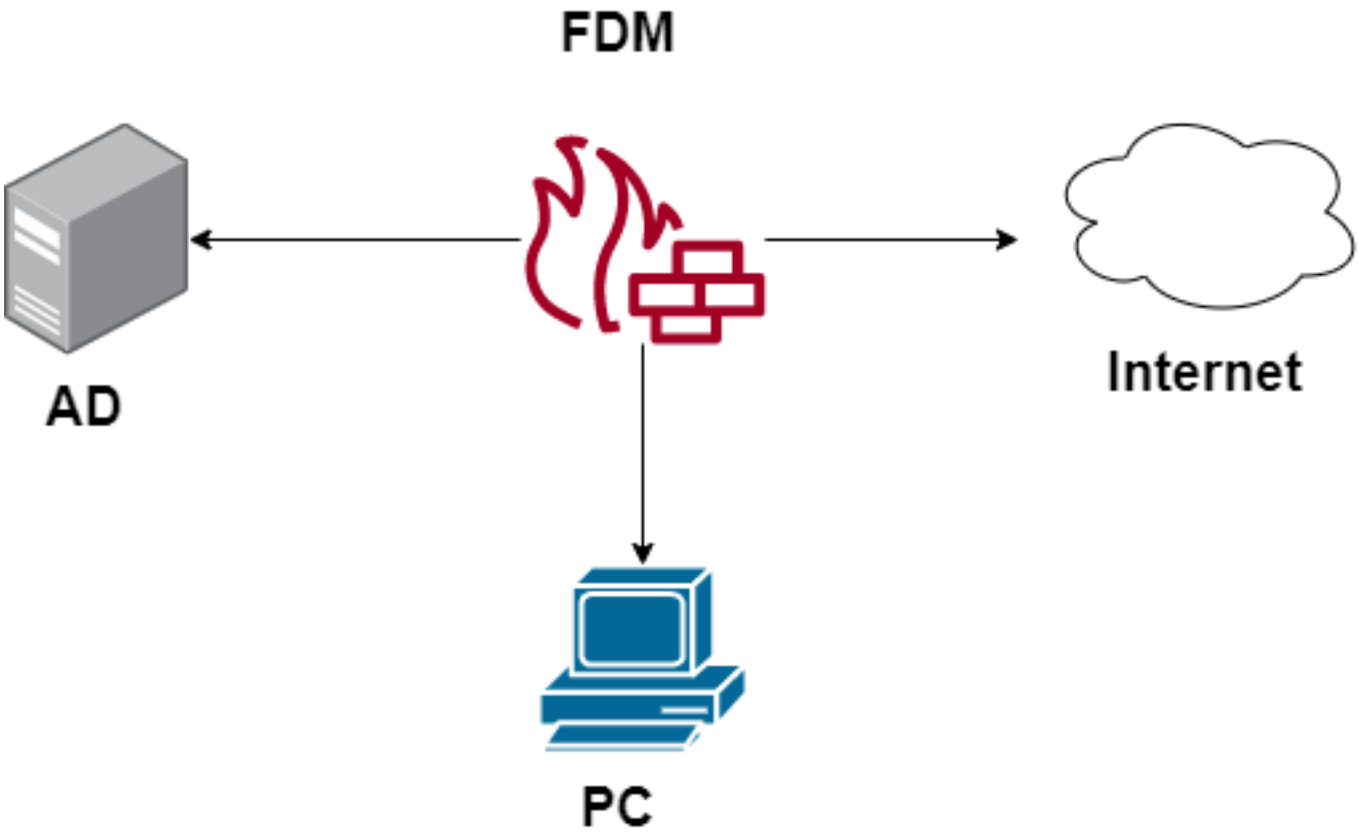
## Premesse

### Definizione dell'identità utente tramite autenticazione attiva

L'autenticazione è l'atto di confermare l'identità di un utente. Con l'autenticazione attiva, quando un flusso di traffico HTTP proviene da un indirizzo IP per il quale il sistema non dispone di mapping utente-identità, è possibile decidere se autenticare l'utente che ha avviato il flusso di traffico nella directory configurata per il sistema. Se l'autenticazione ha esito positivo, l'indirizzo IP viene considerato come avente l'identità dell'utente autenticato.

La mancata autenticazione non impedisce l'accesso alla rete per l'utente. Le regole di accesso determinano in ultima analisi il tipo di accesso da concedere a questi utenti.

## Esempio di rete




# Configurazione

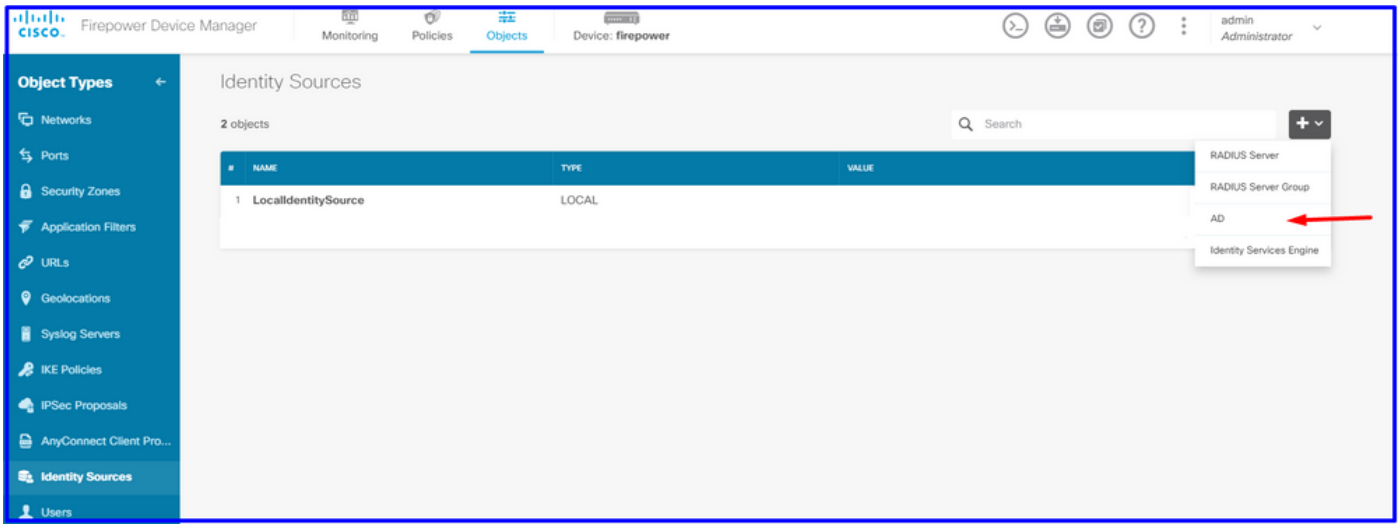
### Implementazione dei criteri di identità

Per abilitare l'acquisizione dell'identità dell'utente, in modo che l'utente associato a un indirizzo IP sia noto, è necessario configurare diversi elementi

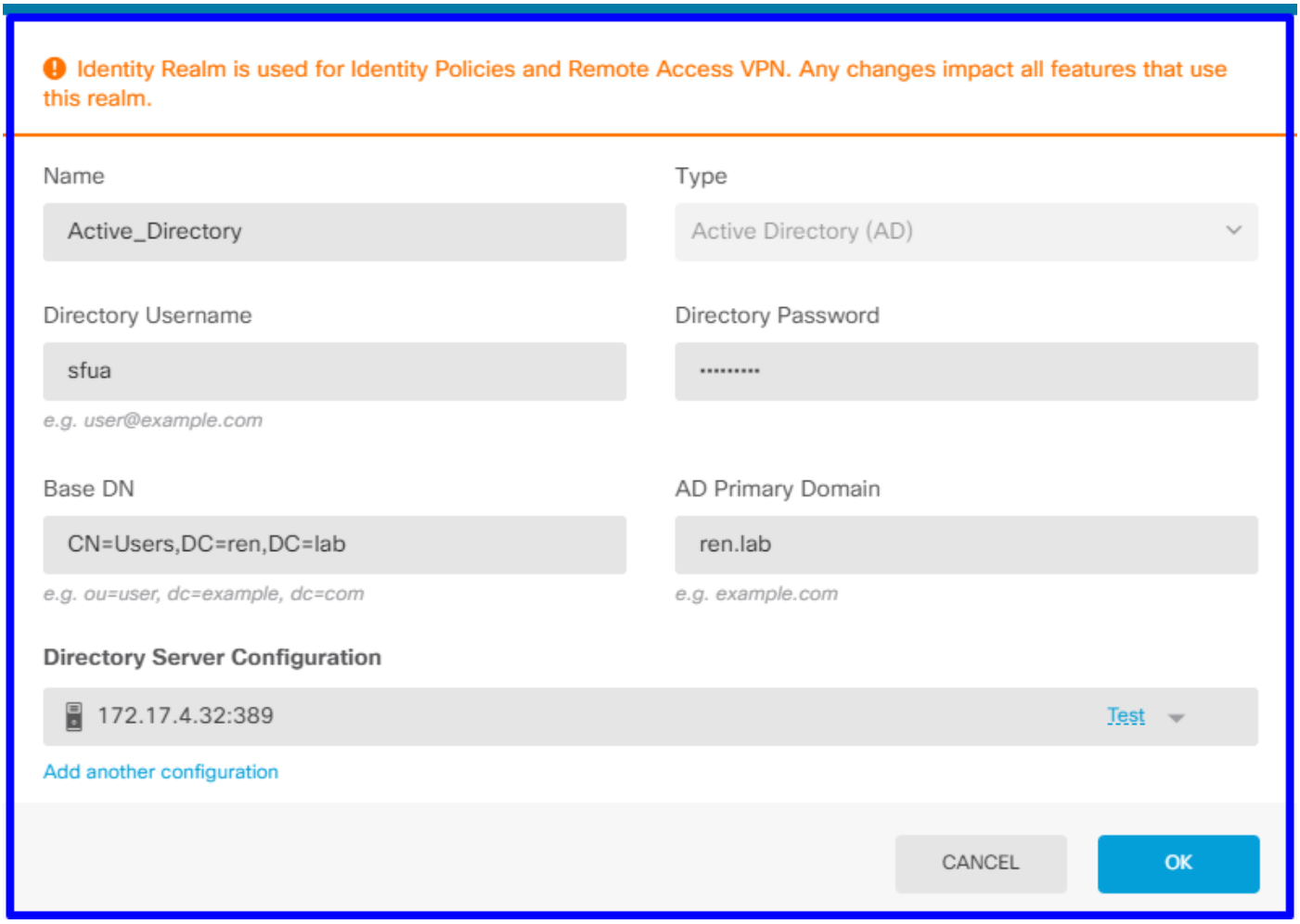
**Passaggio 1.** Configurare il realm di identità AD

Sia che l'identità dell'utente venga raccolta in modo attivo (tramite la richiesta di autenticazione utente) che passivo, è necessario configurare il server Active Directory (AD) che dispone delle informazioni sull'identità dell'utente.

Passare a **Oggetti** > **Identity Services** e selezionare l'opzione **AD** per aggiungere Active Directory.




Aggiungere la configurazione di Active Directory:

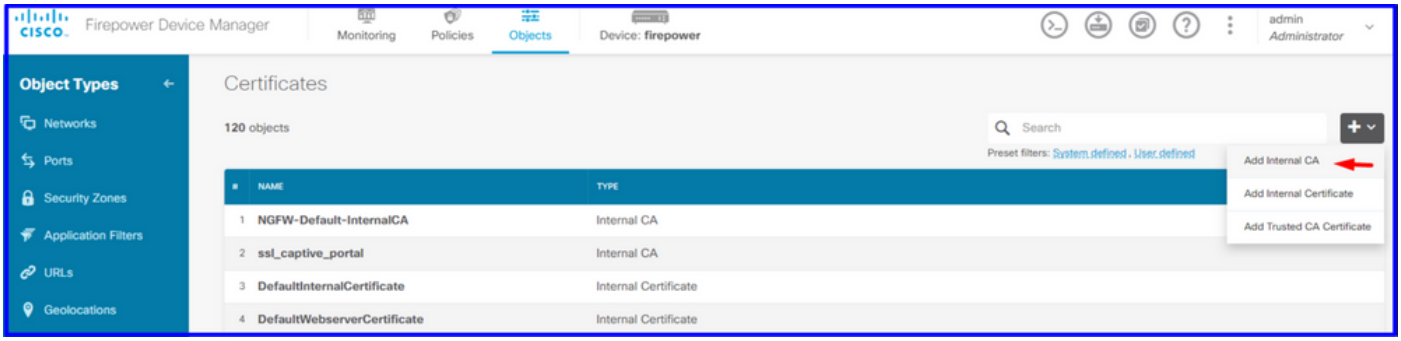



**Passaggio 2.** Creare certificati autofirmati

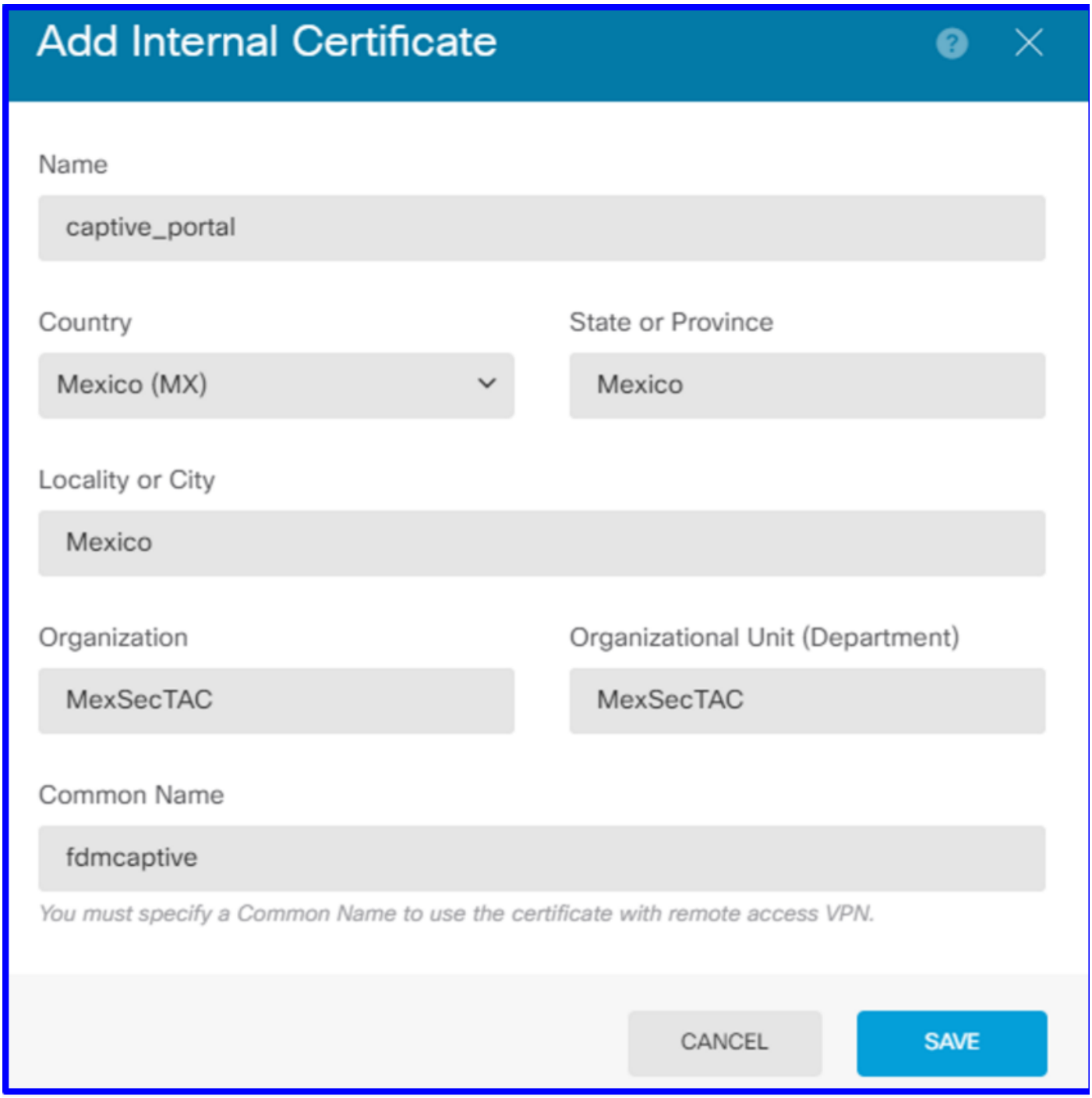
Per creare una configurazione Portale vincolato, sono necessari due certificati, uno per il portale vincolato e uno per la decrittografia SSL.

Èpossibile creare un certificato autofirmato come illustrato in questo esempio.

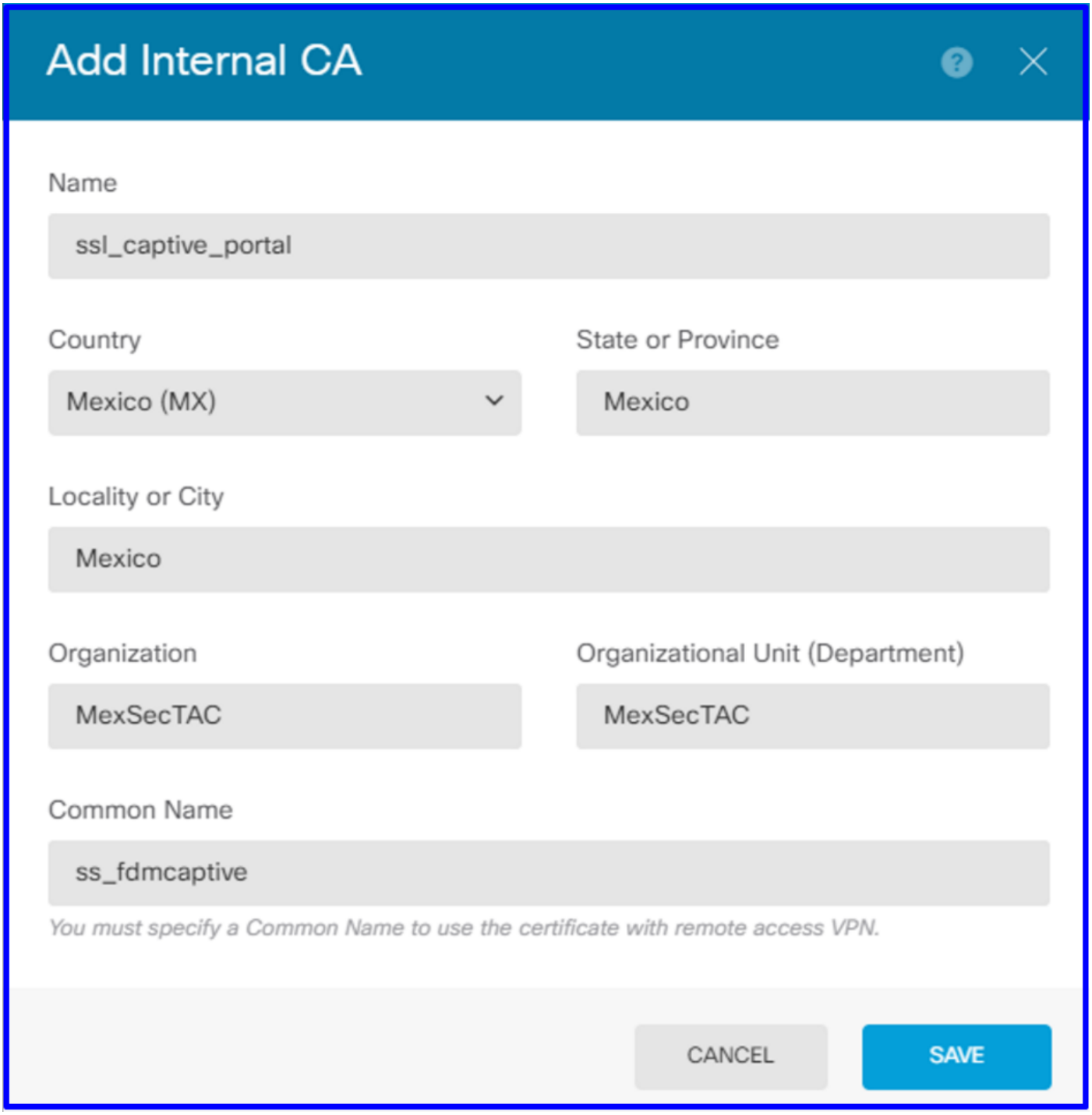
Selezionare **Oggetti** > **Certificati**




Certificato autofirmato portale vincolato:




Certificato autofirmato SSL:

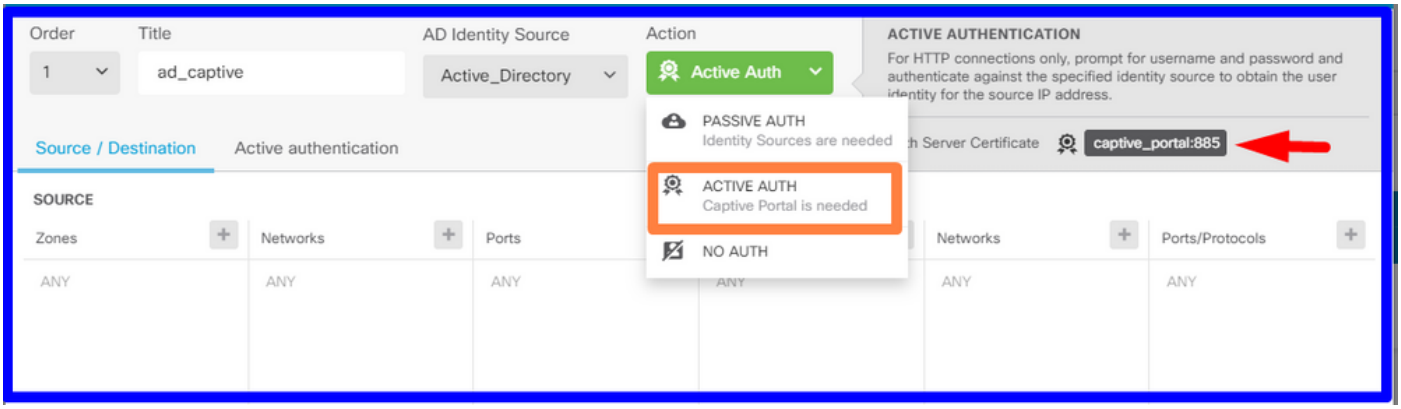



**Passaggio 3.** Crea regola di identità

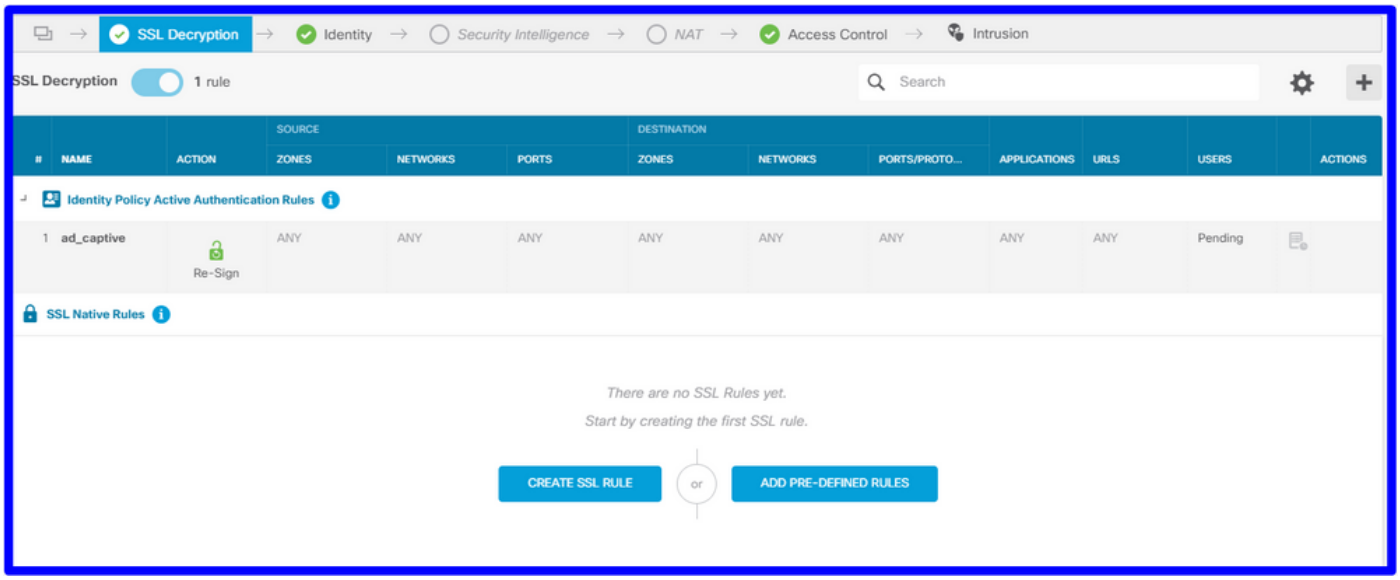
Passare a **Criteri** > **Identità >** pulsante **[+]** per aggiungere una nuova regola di identità.

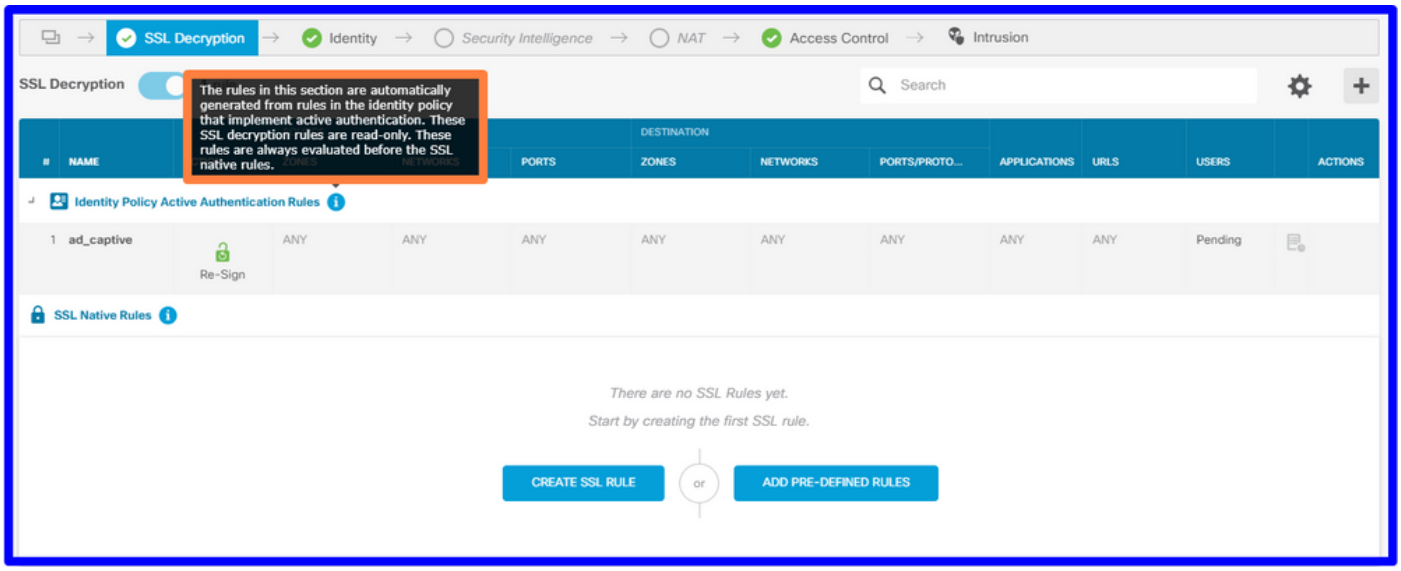
Per configurare l'autenticazione attiva, è necessario creare il criterio di identità. Il criterio deve includere gli elementi seguenti:

- Origine identità AD: Stesso valore aggiunto al passaggio numero 1
- Azione: AUTENTICAZIONE ATTIVA
- Certificato server: Lo stesso certificato autofirmato creato prima di [In questo scenario captive_portal]
- Tipo: HTTP Basic (in questo scenario di esempio)



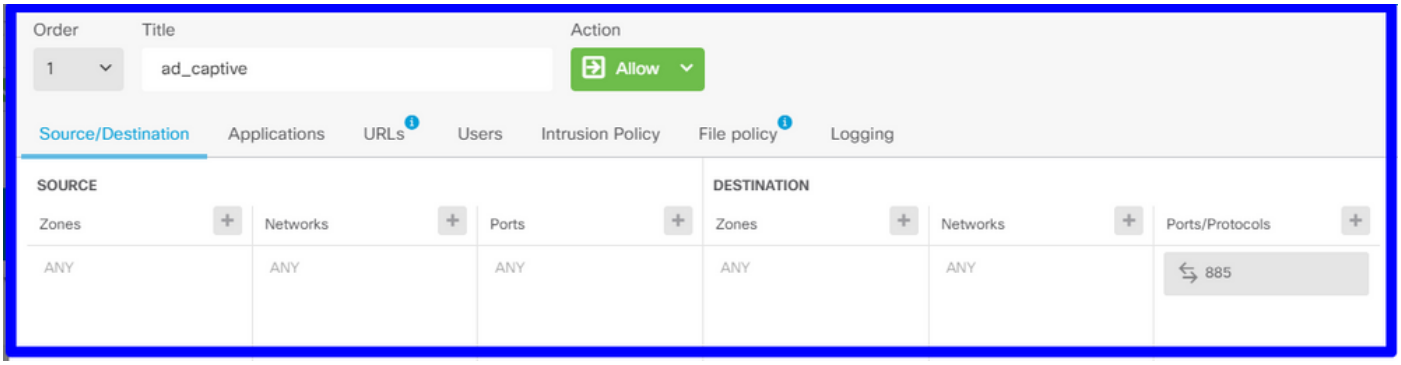

Dopo la creazione del criterio di identità come autenticazione attiva, crea automaticamente una regola SSL. Per impostazione predefinita, questa regola viene impostata come qualsiasi con **Decrittografa-Rifiuta**, ovvero non sono presenti modifiche SSL nella regola.



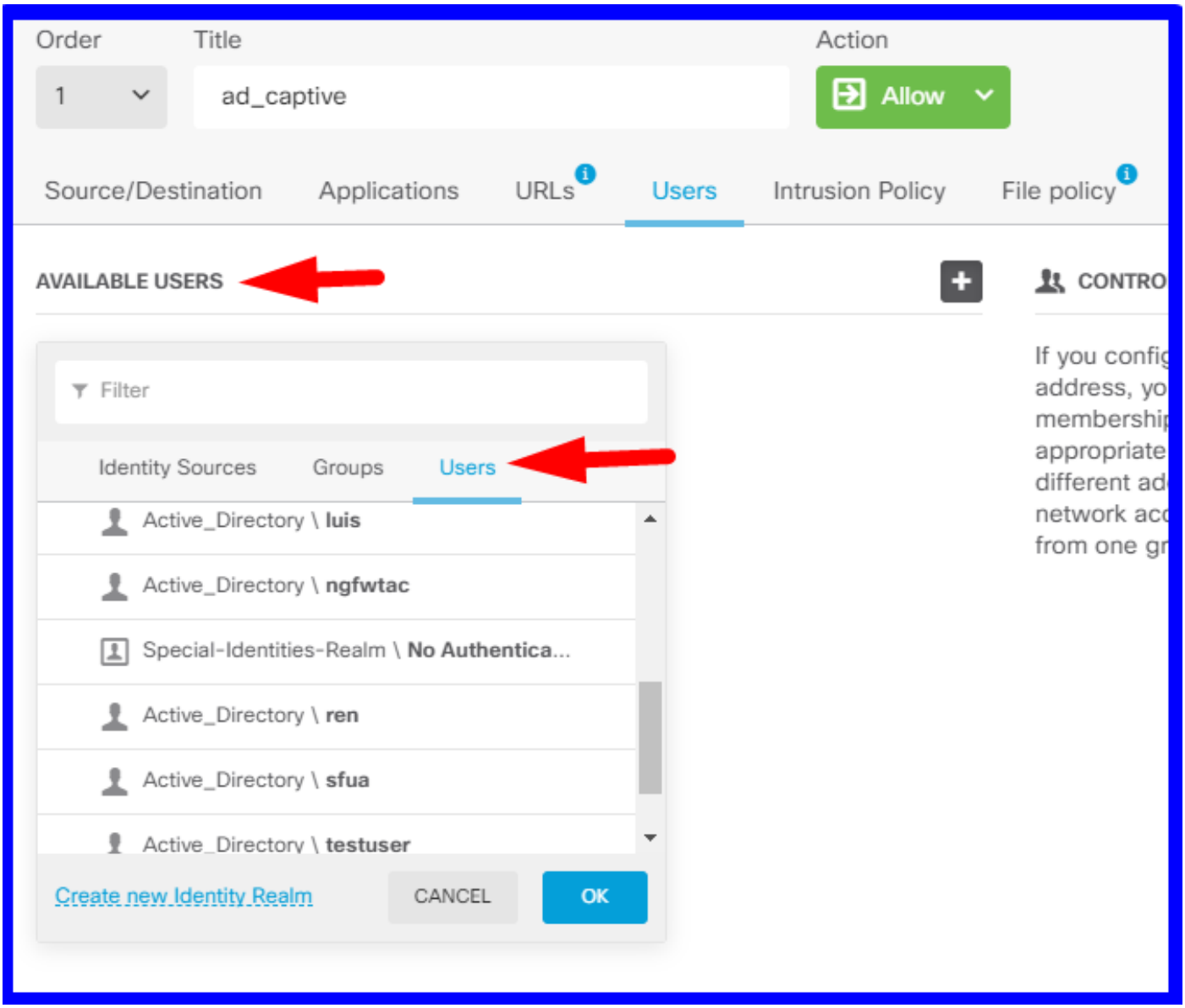




**Passaggio 4.** Creare una regola di accesso in Criteri di controllo di accesso

Ènecessario consentire la **porta 885/tcp** che reindirizza il traffico all'autenticazione captive portal. Passare a **Policy > Controllo d'accesso** e aggiungere la regola di accesso.



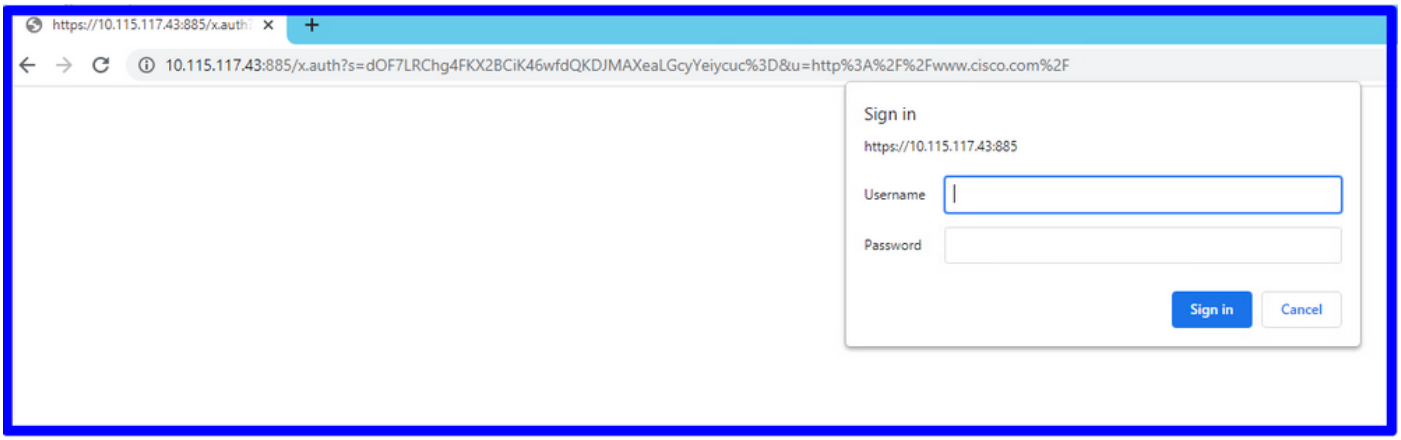

Se è necessario verificare se gli utenti sono stati scaricati da AD, è possibile modificare la regola di accesso e passare alla sezione **Utenti**, quindi in **UTENTI DISPONIBILI**, è possibile verificare quanti utenti sono già presenti in FDM.



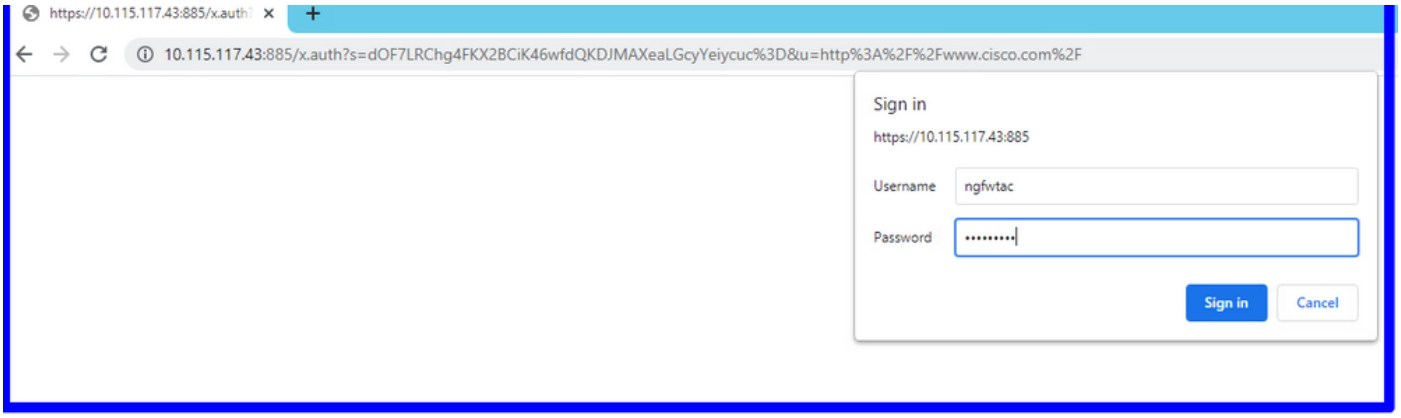

Ricordarsi di distribuire le modifiche alla configurazione.

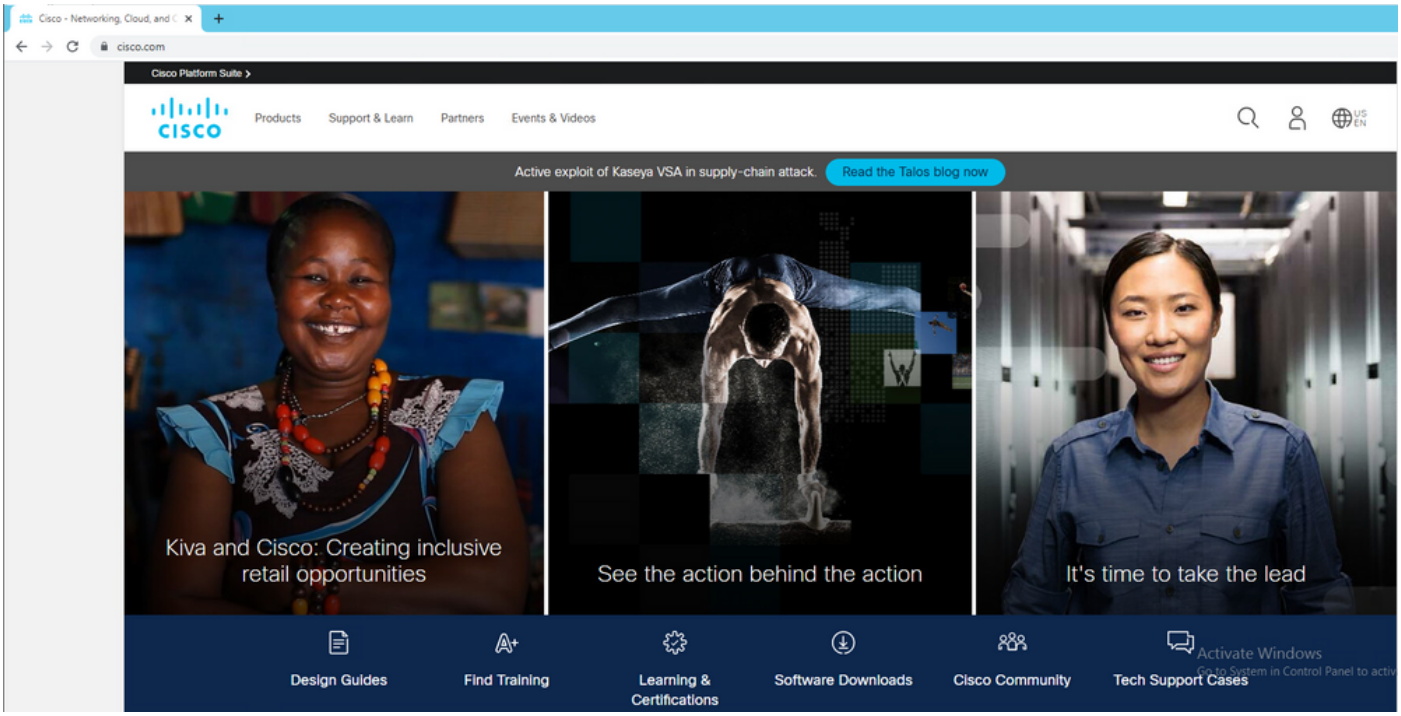
## Verifica

Verificare che il dispositivo dell'utente riceva la casella di controllo quando si accede a un sito HTTPS.




Immettere le credenziali dell'utente AD.




# Risoluzione dei problemi

Èpossibile utilizzare lo script **user_map_query.pl** per verificare che FDM disponga del mapping di indirizzi IP utente

```
user_map_query.pl -u username ---> for users
```

```
user_map_query.pl -i x.x.x.x  ---> for ip addresses
root@firepower:~# user_map_query.pl -u ngfwtac
WARNING: This script was not tested on this major version (6.6.0)! The results may be
unexpected.
Current Time: 06/24/2021 20:45:54 UTC
Getting information on username(s)...
---
User #1: ngfwtac
---
ID:         8
Last Seen:  06/24/2021 20:44:03 UTC
 for_policy: 1
 Realm ID:   4

==============================
|          Database          |
==============================

##) IP Address [Realm ID]
 1) ::ffff:10.115.117.46 [4]

##) Group Name (ID) [realm: Realm Name (ID)]
 1) Domain Users (12) [realm: Active_Directory (4)]
```

In modalità clish è possibile configurare:

system support identity-debug per verificare se il reindirizzamento ha esito positivo.

```
> system support identity-debug
Enable firewall-engine-debug too? [n]: y
Please specify an IP protocol:
Please specify a client IP address: 10.115.117.46
Please specify a client port:
Please specify a server IP address:
Please specify a server port:
Monitoring identity and firewall debug messages

10.115.117.46-55809 > 72.163.47.11-53 17 AS 1-1 I 1 deleting firewall session flags = 0x10001,
fwFlags = 0x100
10.115.117.46-55809 > 72.163.47.11-53 17 AS 1-1 I 1 Logging EOF as part of session delete with
rule_id = 1 ruleAction = 2 ruleReason = 0
10.115.117.46-50611 > 142.250.138.94-443 6 AS 1-1 I 0 Got end of flow event from hardware with
flags 00010001. Rule Match Data: rule_id 0, rule_action 0 rev_id 0, rule_flags 2
10.115.117.46-50611 > 142.250.138.94-443 6 AS 1-1 I 0 Logging EOF for event from hardware with
rule_id = 1 ruleAction = 2 ruleReason = 0
10.115.117.46-50611 > 142.250.138.94-443 6 AS 1-1 I 0 : Received EOF, deleting the snort
session.
10.115.117.46-50611 > 142.250.138.94-443 6 AS 1-1 I 0 deleting firewall session flags = 0x10003,
fwFlags = 0x114
10.115.117.46-65489 > 72.163.47.11-53 17 AS 1-1 I 1 deleting firewall session flags = 0x10001,
fwFlags = 0x100
10.115.117.46-65489 > 72.163.47.11-53 17 AS 1-1 I 1 Logging EOF as part of session delete with
rule_id = 1 ruleAction = 2 ruleReason = 0
10.115.117.46-65489 > 173.36.131.10-53 17 AS 1-1 I 1 deleting firewall session flags = 0x10001,
fwFlags = 0x100
10.115.117.46-65489 > 173.36.131.10-53 17 AS 1-1 I 1 Logging EOF as part of session delete with
rule_id = 1 ruleAction = 2 ruleReason = 0

10.115.117.46-53417 > 72.163.47.11-53 17 AS 1-1 I 0 deleting firewall session flags = 0x10001,
fwFlags = 0x100
10.115.117.46-53417 > 72.163.47.11-53 17 AS 1-1 I 0 Logging EOF as part of session delete with
rule_id = 1 ruleAction = 2 ruleReason = 0
10.115.117.46-63784 > 72.163.47.11-53 17 AS 1-1 I 1 Starting authentication (sfAuthCheckRules
```

```
params) with zones 2 -> 3, port 63784 -> 53, geo 16671760 -> 16671778
10.115.117.46-63784 > 72.163.47.11-53 17 AS 1-1 I 1 looked for user_id with realm_id 4 auth_type
2, returning realm_id 4 auth_type 2 user_id 8
10.115.117.46-63784 > 72.163.47.11-53 17 AS 1-1 I 1 found active binding for user_id 8 in realm
4
10.115.117.46-63784 > 72.163.47.11-53 17 AS 1-1 I 1 matched auth rule id = 2023803385 user_id =
8 realm_id = 4
10.115.117.46-63784 > 72.163.47.11-53 17 AS 1-1 I 1 new firewall session
10.115.117.46-63784 > 72.163.47.11-53 17 AS 1-1 I 1 using HW or preset rule order 4, 'Default
Action', action Allow and prefilter rule 0
10.115.117.46-63784 > 72.163.47.11-53 17 AS 1-1 I 1 HitCount data sent for rule id: 1,
10.115.117.46-63784 > 72.163.47.11-53 17 AS 1-1 I 1 allow action
10.115.117.46-50619 > 142.250.138.94-443 6 AS 1-1 I 0 Starting authentication (sfAuthCheckRules
params) with zones 2 -> 3, port 50619 -> 443, geo 16671760 -> 16671778
10.115.117.46-50619 > 142.250.138.94-443 6 AS 1-1 I 0 looked for user_id with realm_id 4
auth_type 2, returning realm_id 4 auth_type 2 user_id 8
10.115.117.46-50619 > 142.250.138.94-443 6 AS 1-1 I 0 found active binding for user_id 8 in
realm 4
10.115.117.46-50619 > 142.250.138.94-443 6 AS 1-1 I 0 matched auth rule id = 2023803385 user_id
= 8 realm_id = 4
10.115.117.46-50619 > 142.250.138.94-443 6 AS 1-1 I 0 new firewall session
10.115.117.46-50619 > 142.250.138.94-443 6 AS 1-1 I 0 using HW or preset rule order 4, 'Default
Action', action Allow and prefilter rule 0
10.115.117.46-50619 > 142.250.138.94-443 6 AS 1-1 I 0 HitCount data sent for rule id: 1,
10.115.117.46-50619 > 142.250.138.94-443 6 AS 1-1 I 0 allow action
```

Riferimento:

https://www.cisco.com/c/en/us/td/docs/security/firepower/660/fdm/fptd-fdm-config-guide-660/fptd-fdm-identity.html#id_71535

https://www.cisco.com/c/en/us/td/docs/security/firepower/660/fdm/fptd-fdm-config-guide-660/fptd-fdm-identity-sources.html#task_83008ECD0DBF4E388B28B6247CB2E64B