Securing Networks with

Cisco FTD

Chapter 21

Identity Policy

and

Active Directory Integration

Mohsen Kheradmand

Identity Policy

- A “Identity Policy” contains identity rules, they associate the traffic with the Realm and the authentication method
  - Realm : (authoritative identity source like Active directory)
  - Authentication method : (active, passive or no authentication)

Use case:

a) By identifying the user, you can correlate threat, endpoint, and network intelligence with user identity information

- ❑ For example, identify who owns the host targeted by an intrusion event, and who initiated an attack or port scan
- ❑ Also identify high bandwidth users and users who are accessing undesirable web sites or applications.

b) You can also write access rules based on user name or user group name

- Selectively allowing or blocking access to resources based on user identity

Identity Policy

You can obtain user identity using the following methods:

- Passive authentication:
  - ✓ For all types of connections , without prompting for username and password
  - ✓ You can passively obtain user-to-IP address mappings from the following sources:
    - Remote access VPN logins.
    - Cisco Identity Services Engine (ISE)
- Active authentication :
  - ✓ For HTTP connections only, prompt for username and password (Captive portal)
    - When you configure the directory server for the identity policy, the system downloads user and group membership information from the directory server.
    - This information is refreshed every 24 hours
    - If you need to force an update, click **Objects** > **Identity Sources**, then **edit** the realm , Click **Save**,

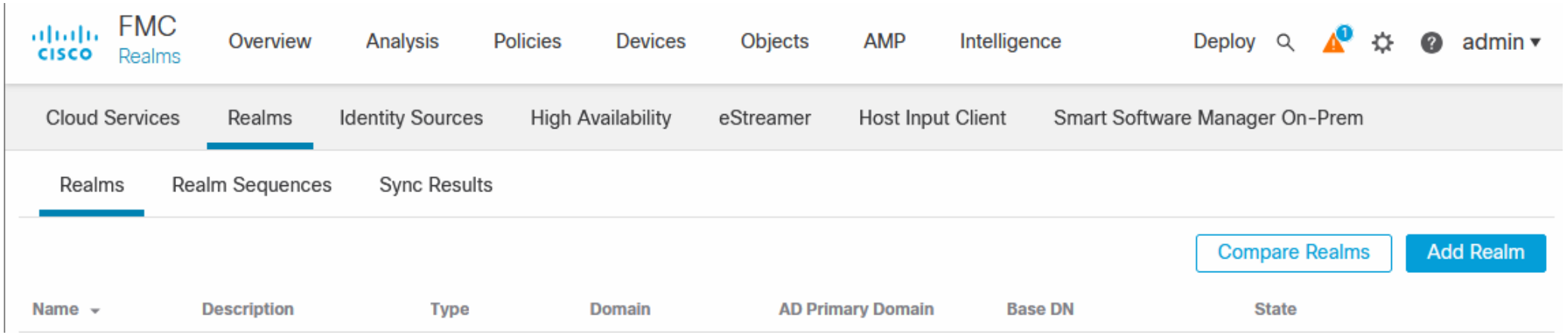
Active Directory Integration Configuration

- System -> Integration -> Realms -> Add Realm

3 types of realm supported by Cisco FMC:

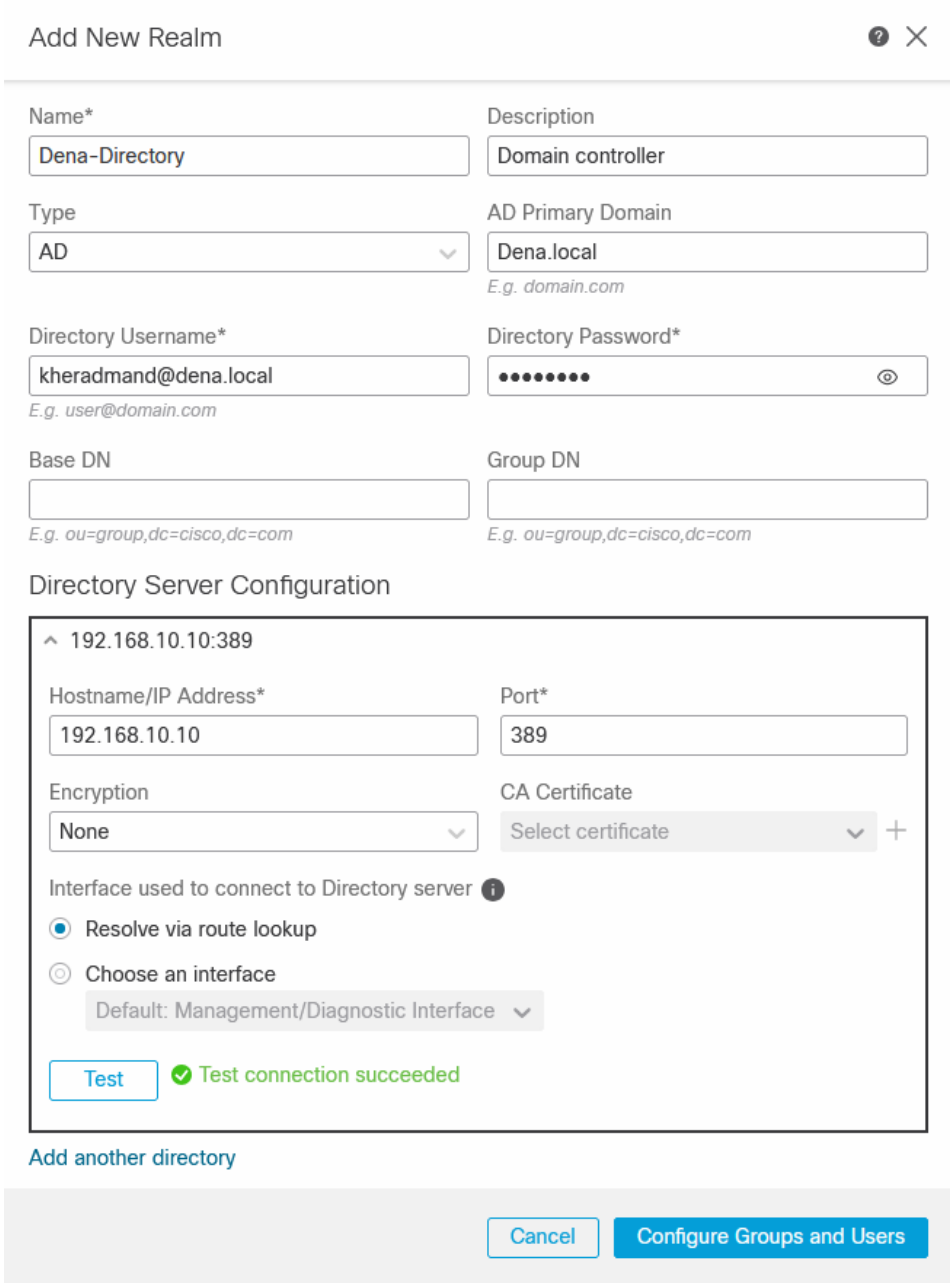
- Active Directory
- LDAP
- Local

Click Add Realm



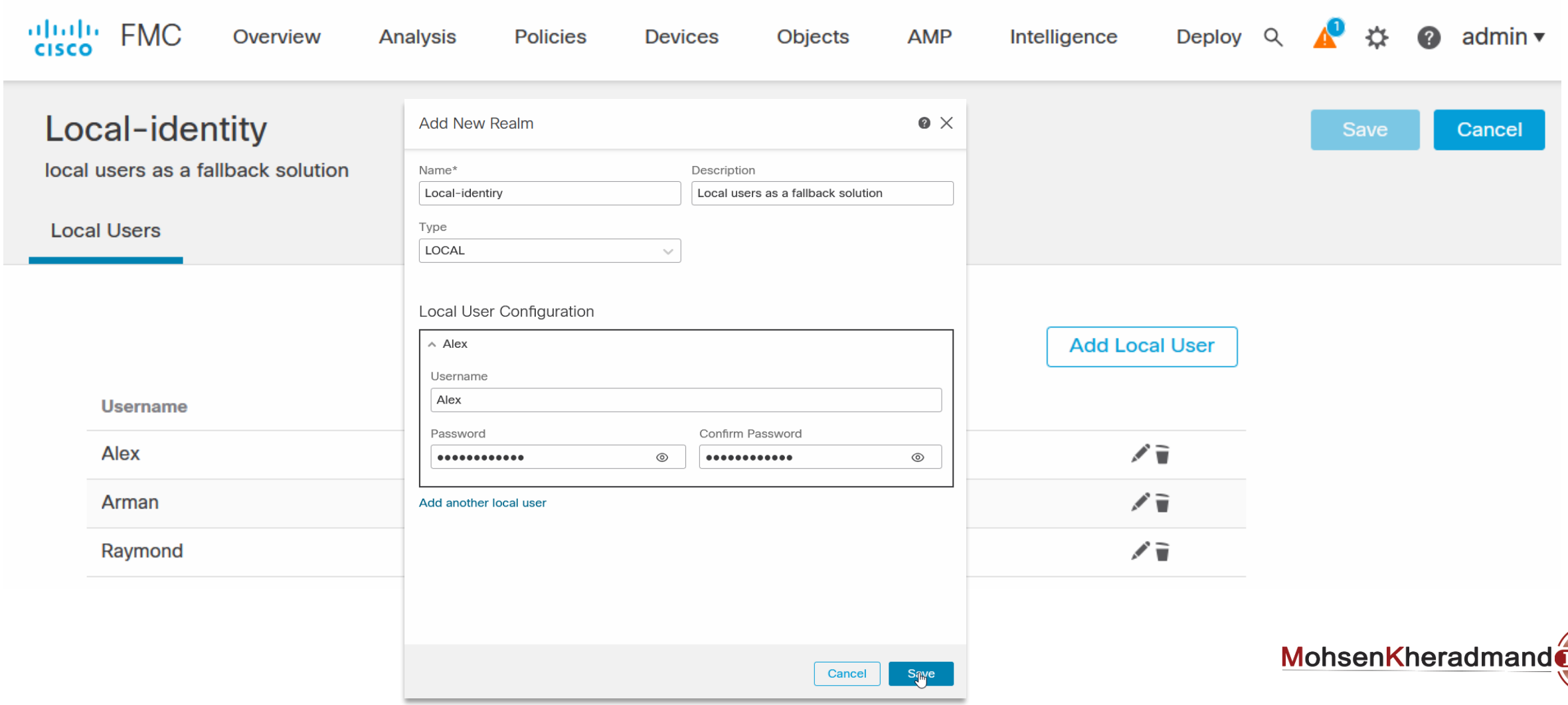
Active Directory Integration Configuration

- Enter a name and description for this AD Realm
- From Type select AD (other types are LDAP and Local
- AD Primary Domain : enter domain DNS name
- Directory username : enter a username of active directory
- Directory Password: the password of the entered username
- Hostname/IP Address : the address of domain controller
- Encryption : None (you can choose some CA Cert)
- Click Test to make sure the connectivity is OK
- Click Configure Groups and Users



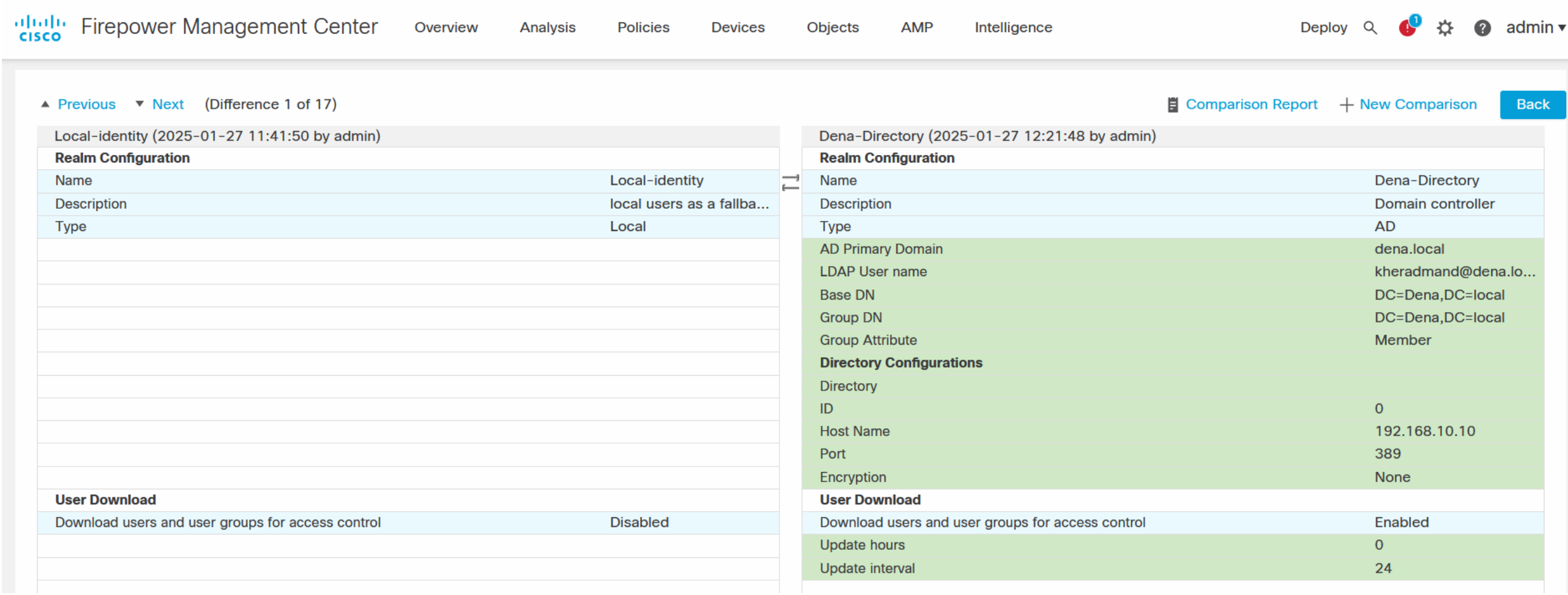
Local identity Configuration

- You can add a Local-identity as a fallback solution and enter some Username/Password inside that



Active Directory Integration Configuration

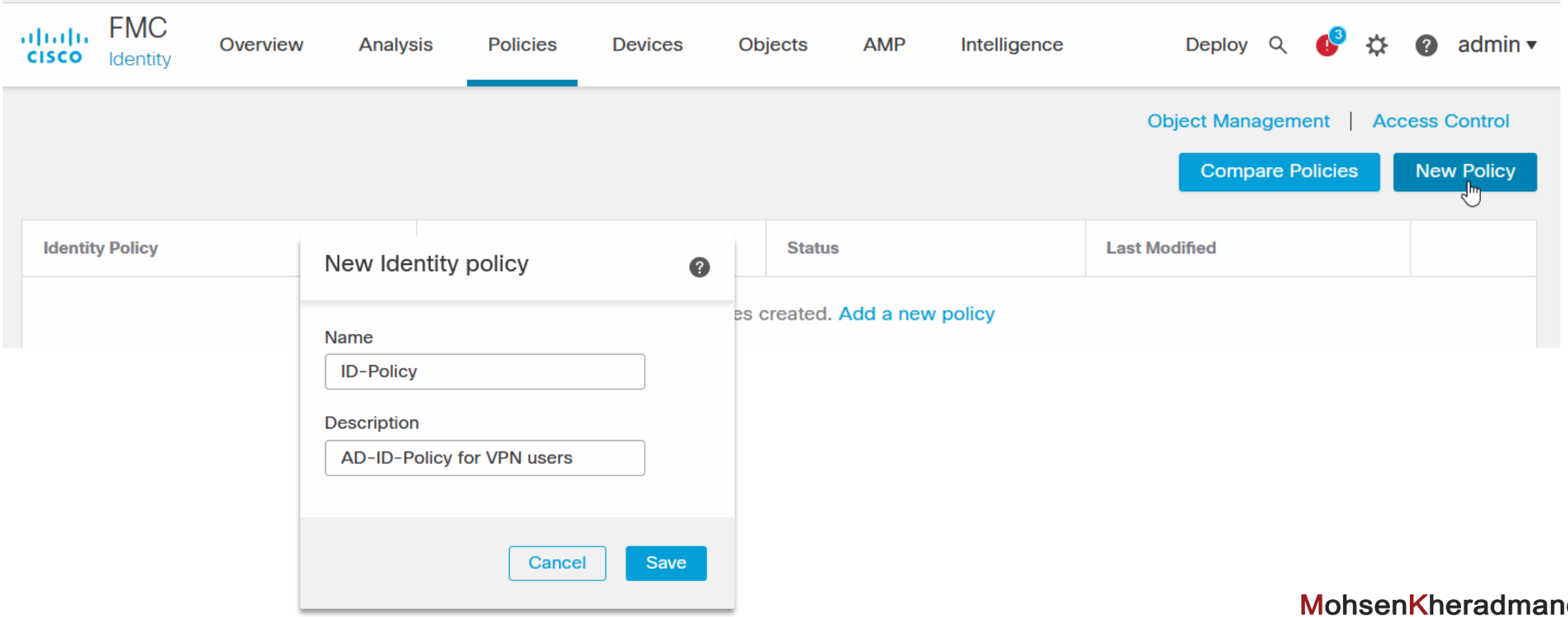
- You can use comparison between Realms



Implement the Identity Policy

- Policies -> Identity

  Click New Policy



Implement the Identity Policy

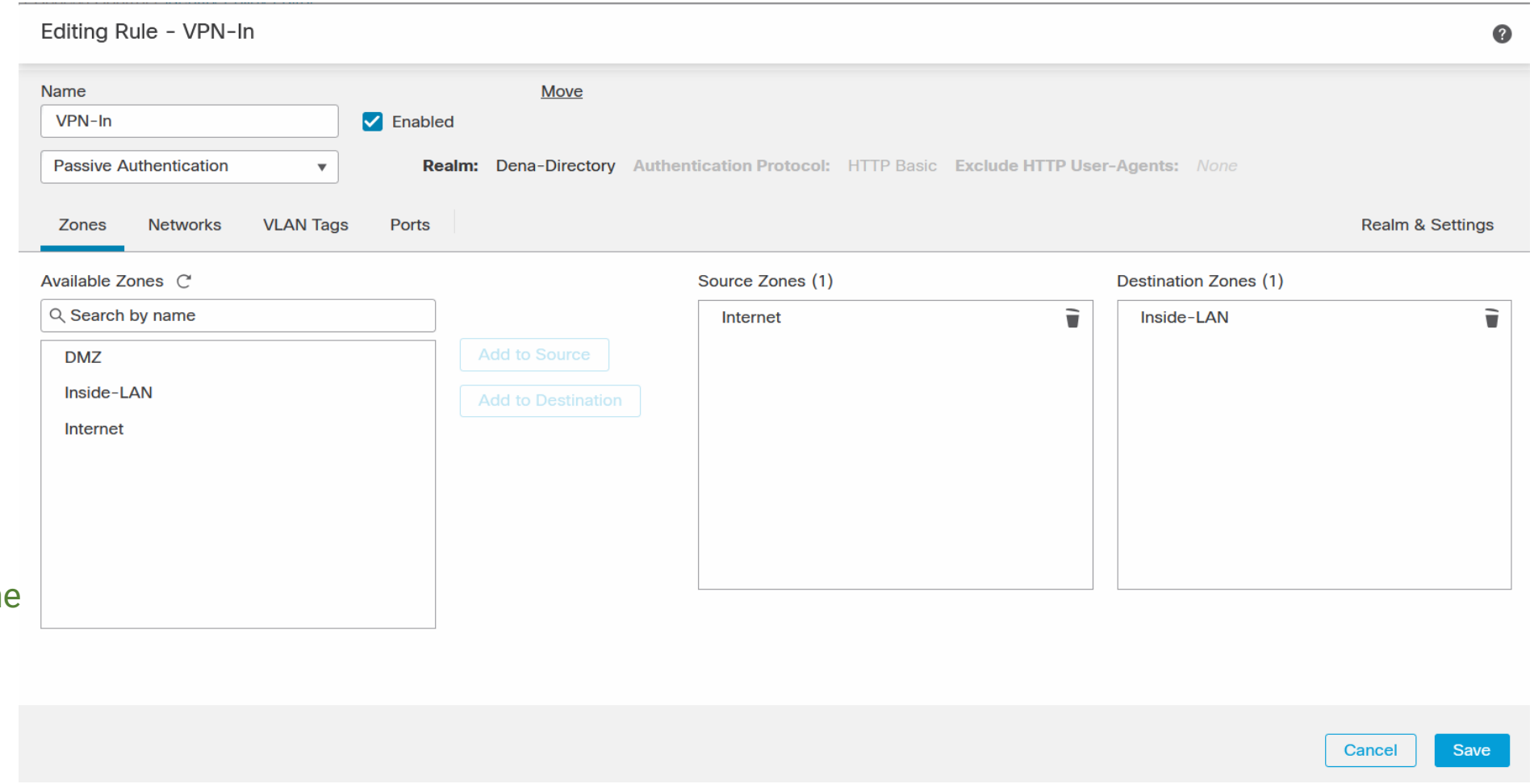
Create a Rule

- Enter a name
- Select one of the :
  - Passive authentication
  - Active authentication
  - No authentication

- Click Realm & Setting
  - ✓ Select AD Realm

- Configure :
  - ✓ Source / Destination Zone
  - ✓ Networks /ports / VLAN

- Click Save

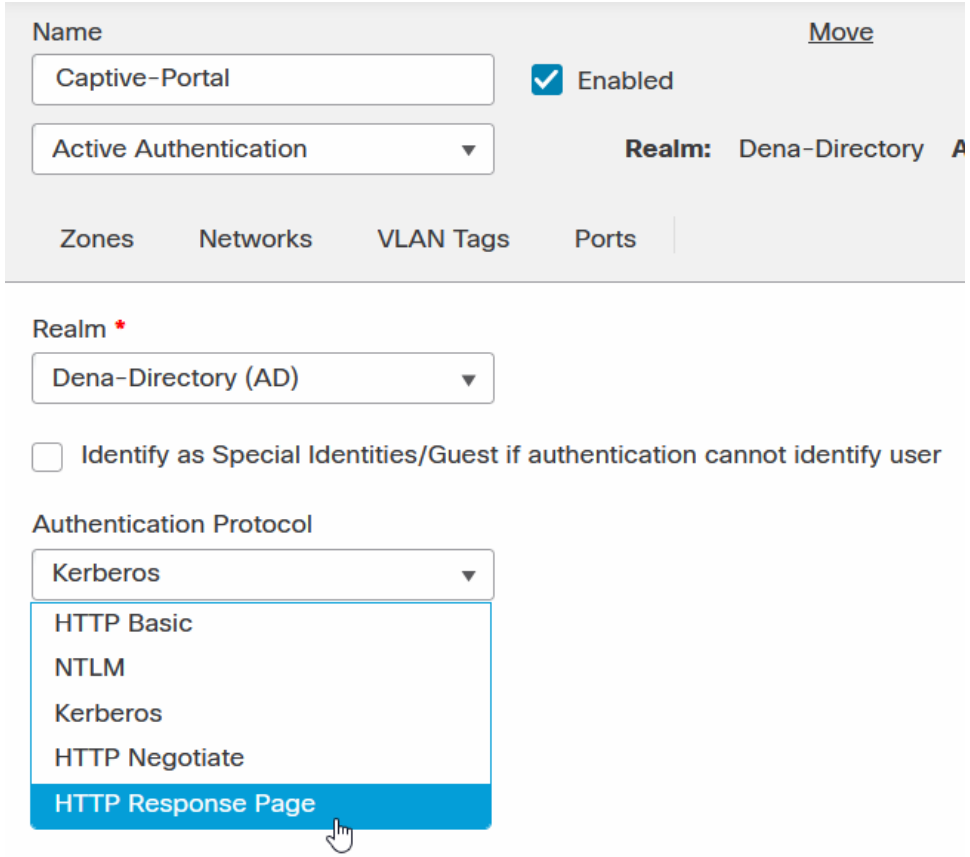


MohsenKheradmand MK

Implement the Identity Policy

Authentication protocols :

- HTTP basic : authenticate users using an unencrypted HTTP Basic Authentication (BA) connection ,
- NTLM : authenticate users using a NT LAN Manager (NTLM) connection. This selection is available only when you select an AD realm. User Authentication happens transparently without prompts for credentials
- Kerberos : is available only when you select an AD realm for a server with secure LDAP (LDAPS) enabled
- HTTP Negotiate : allow the captive portal server to choose between HTTP Basic, Kerberos, or NTLM for the authentication connection
- HTTP Response Page : similar to HTTP basic type, user is prompted to fill the authentication , but HTML form which can be customized.



- Note : If you use captive portal, you should configure a DNS record for captive portal device (the FQDN of the captive portal is same as host name of captive portal)

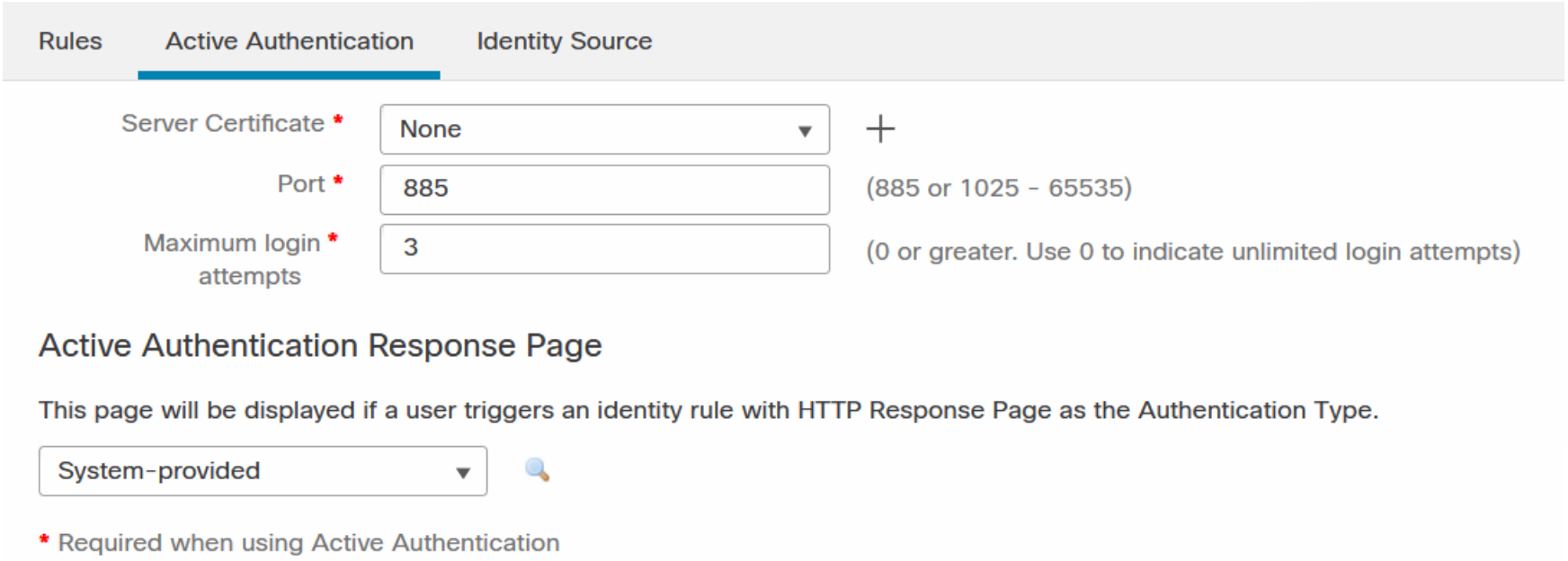
Implement the Identity Policy

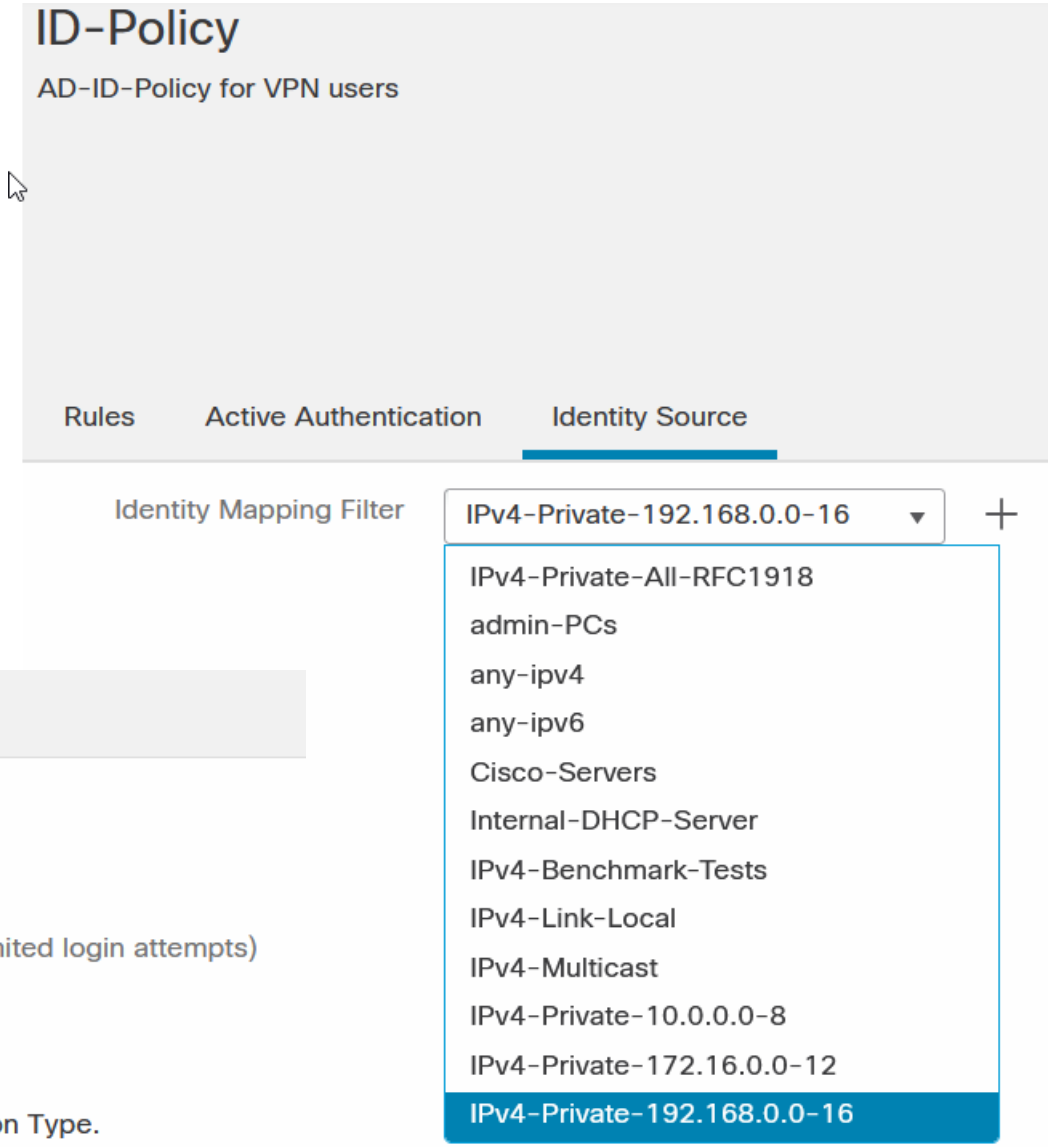
Active Authentication

- Select a certificate for Captive Portal device
- Enter a port and maximum login attempts
- You can create custom HTTP response page

Identity source

- An identity mapping filter can be used to limit the networks to which an identity rules apply (you can limit the networks they monitor)





Implement the Identity Policy

Integrate in ACP

- Policies > Access Control >Access Control
- Click the policy you want to use ID policy in it
- Click Identity policy > select your ID policy and click save then Deploy