

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](#)

The screenshot shows the Cisco FMC Realms configuration page. The top navigation bar includes the Cisco FMC Realms logo and tabs for Overview, Analysis, Policies, Devices, Objects, AMP, and Intelligence. A secondary navigation bar contains links for Cloud Services, Realms (which is selected), Identity Sources, High Availability, eStreamer, Host Input Client, and Smart Software Manager On-Prem. Below this, there are sub-tabs for Realms, Realm Sequences, and Sync Results. On the right side of the page, there are buttons for 'Compare Realms' and 'Add Realm'. At the bottom, a table header is visible with columns: Name, Description, Type, Domain, AD Primary Domain, Base DN, and State.

Name	Description	Type	Domain	AD Primary Domain	Base DN	State
------	-------------	------	--------	-------------------	---------	-------

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

Add New Realm? ×

Name*

Dena-Directory

Description

Domain controller

Type

AD

AD Primary Domain

Dena.local

E.g. domain.com

Directory Username*

kheradmand@dena.local

E.g. user@domain.com

Directory Password*

••••••••

👁

Base DN

E.g. ou=group,dc=cisco,dc=com

Group DN

E.g. ou=group,dc=cisco,dc=com

Directory Server Configuration

^ 192.168.10.10:389

Hostname/IP Address*

192.168.10.10

Port*

389

Encryption

None

CA Certificate

Select certificate

+

Interface used to connect to Directory server ⓘ

☒ Resolve via route lookup

☐ Choose an interface

Default: Management/Diagnostic Interface

▼

Test

✔ Test connection succeeded

[Add another directory](#)

Cancel

Configure Groups and Users

Local identity Configuration

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

The screenshot shows the Cisco FMC (Firepower Management Center) interface for configuring local identity. The top navigation bar includes links for Overview, Analysis, Policies, Devices, Objects, AMP, Intelligence, Deploy, and a search icon. The user is logged in as 'admin'. The main content area is titled 'Local-identity' with the subtitle 'local users as a fallback solution'. A 'Local Users' table lists three users: Alex, Arman, and Raymond. A modal window titled 'Add New Realm' is open, showing the configuration for a new local realm. The 'Name' field is 'Local-identity' and the 'Description' is 'Local users as a fallback solution'. The 'Type' is set to 'LOCAL'. Below this, the 'Local User Configuration' section shows a user named 'Alex' with a 'Username' of 'Alex' and a 'Password' field. The 'Add another local user' link is visible. The modal has 'Cancel' and 'Save' buttons at the bottom. On the right side of the main interface, there are 'Save' and 'Cancel' buttons, and an 'Add Local User' button.

Local-identity
local users as a fallback solution

Local Users

Username
Alex
Arman
Raymond

Add New Realm

Name* Description

Type

Local User Configuration

^ Alex

Username

Password Confirm Password

[Add another local user](#)

Save **Cancel**

Add Local User

Active Directory Integration Configuration

➤ You can use comparison between Realms

▲ Previous ▼ Next (Difference 1 of 17)

Comparison Report + New Comparison Back

Local-identity (2025-01-27 11:41:50 by admin)	
Realm Configuration	
Name	Local-identity
Description	local users as a fallba...
Type	Local
User Download	
Download users and user groups for access control	Disabled

Dena-Directory (2025-01-27 12:21:48 by admin)	
Realm Configuration	
Name	Dena-Directory
Description	Domain controller
Type	AD
AD Primary Domain	dena.local
LDAP User name	kheradmand@dena.lo...
Base DN	DC=Dena,DC=local
Group DN	DC=Dena,DC=local
Group Attribute	Member
Directory Configurations	
Directory	
ID	0
Host Name	192.168.10.10
Port	389
Encryption	None
User Download	
Download users and user groups for access control	Enabled
Update hours	0
Update interval	24

Implement the Identity Policy

➤ Policies -> Identity

Click New Policy

The screenshot shows the Cisco FMC Identity management interface. The top navigation bar includes tabs for Overview, Analysis, Policies (selected), Devices, Objects, AMP, and Intelligence. On the right, there are links for Deploy, a search icon, a notification bell with 3 alerts, a settings gear, a help icon, and a user profile for 'admin'. Below the navigation bar, there are two main sections: 'Object Management' and 'Access Control'. In the 'Access Control' section, there are two buttons: 'Compare Policies' and 'New Policy'. The 'New Policy' button is being clicked, which has opened a modal window titled 'New Identity policy'. The modal contains two text input fields: 'Name' with the value 'ID-Policy' and 'Description' with the value 'AD-ID-Policy for VPN users'. At the bottom of the modal are 'Cancel' and 'Save' buttons. In the background, a table with columns 'Identity Policy', 'Status', and 'Last Modified' is visible, along with a message that says 'No policies created. Add a new policy'.

Identity Policy	Status	Last Modified
No policies created. Add a 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

Editing Rule - VPN-In

Name: VPN-In ☐ Enabled [Move](#)

Passive Authentication Realm: Dena-Directory Authentication Protocol: HTTP Basic Exclude HTTP User-Agents: None

Zones Networks VLAN Tags Ports [Realm & Settings](#)

Available Zones Search by name

DMZ
Inside-LAN
Internet

[Add to Source](#)
[Add to Destination](#)

Source Zones (1)
Internet

Destination Zones (1)
Inside-LAN

[Cancel](#) [Save](#)

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)

The screenshot displays the configuration page for a 'Captive-Portal' identity policy. At the top, the 'Name' field is set to 'Captive-Portal' and the 'Enabled' checkbox is checked. Below this, the 'Active Authentication' dropdown is visible. To the right, the 'Realm' is set to 'Dena-Directory'. A navigation bar at the bottom of the top section includes tabs for 'Zones', 'Networks', 'VLAN Tags', and 'Ports'. Below the navigation bar, the 'Realm' dropdown is set to 'Dena-Directory (AD)'. A checkbox labeled 'Identify as Special Identities/Guest if authentication cannot identify user' is present. The 'Authentication Protocol' dropdown is open, showing a list of options: 'Kerberos', 'HTTP Basic', 'NTLM', 'Kerberos', 'HTTP Negotiate', and 'HTTP Response Page'. The 'HTTP Response Page' option is highlighted in blue, and a mouse cursor is pointing at it.

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)

Rules

Active Authentication

Identity Source

Server Certificate *

None

+

Port *

885

(885 or 1025 - 65535)

Maximum login attempts *

3

(0 or greater. Use 0 to indicate unlimited login attempts)

Active Authentication Response Page

This page will be displayed if a user triggers an identity rule with HTTP Response Page as the Authentication Type.

System-provided

* Required when using Active Authentication

ID-Policy

AD-ID-Policy for VPN users

Rules

Active Authentication

Identity Source

Identity Mapping Filter

IPv4-Private-192.168.0.0-16

+

IPv4-Private-All-RFC1918

admin-PCs

any-ipv4

any-ipv6

Cisco-Servers

Internal-DHCP-Server

IPv4-Benchmark-Tests

IPv4-Link-Local

IPv4-Multicast

IPv4-Private-10.0.0.0-8

IPv4-Private-172.16.0.0-12

IPv4-Private-192.168.0.0-16

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

The screenshot shows the Cisco Firepower Management Center interface. The top navigation bar includes tabs for Overview, Analysis, Policies, Devices, Objects, AMP, and Intelligence. The 'Policies' tab is selected. The main content area displays the 'Default-Block-Policy' configuration page. The 'Rules' tab is active, and the 'Default-Block-Policy' is selected. The 'Identity Policy' dropdown menu is open, showing 'ID-Policy' selected. The 'OK' button is highlighted.

#	Name	Source Zones	Dest Zones	Source Networks	Dest Networks	VLAN Tags	Users	Applicat...	Source Ports	Dest Ports	URLs	Source Dynamic Attributes	Destinat... Dynamic Attributes	Action
Mandatory - Default-Block-Policy (-)														
There are no rules in this section. Add Rule or Add Category														
Default - Default-Block-Policy (-)														
There are no rules in this section. Add Rule or Add Category														