

## Access Control / Firewall

# Configure Active Directory Integration with FirePOWER Appliance for Single-Sign-On & Captive portal Authentication.



by [sunilk6](#) on 12-12-2015 01:44 AM  
- edited on 12-23-2015 04:28 AM

### Table of Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Components Used](#)

[Configuration Setps](#)

1. [Configure the FirePOWER User Agent for Single-Sign-On](#)
2. [Integration of FirePOWER Management Center \(FMC\) with User Agent](#)
3. [FirePOWER integration with Active Directory](#)
4. [Configure the Identity Policy](#)
  - 4.1 [Captive portal \(Active Authentication\)](#)
  - 4.2 [Single-Sign-On \(Passive Authentication\)](#)
5. [Configure the Access Control Policy](#)
6. [Deploy the Access Control Policy](#)
7. [Monitor user events & Connections events](#)

## Introduction

Captive Portal Authentication (Active Authentication) will prompt a login page and will ask for user credentials before a user can get the internet access.

Sign-sign-On (Passive Authentication) is seamless authentication to get internet. The Sign-sign-on authentication can be achieve either by FirePOWER user agent or NTLM browser authentication.

## Prerequisites

### Requirements

Cisco recommends that you have knowledge on Sourcefire FirePOWER devices, virtual device models, Light Weight Directory Service (LDAP), FirePOWER UserAgent.  
For Captive Portal Authentication, Appliance should be in routed mode.

### Components Used

FirePOWER Management Center (FMC) version 6.0.0 and above  
FirePOWER sensor version 6.0.0 and above

## Configuration Setps

### 1. Configure the FirePOWER User Agent for Single-Sign-On

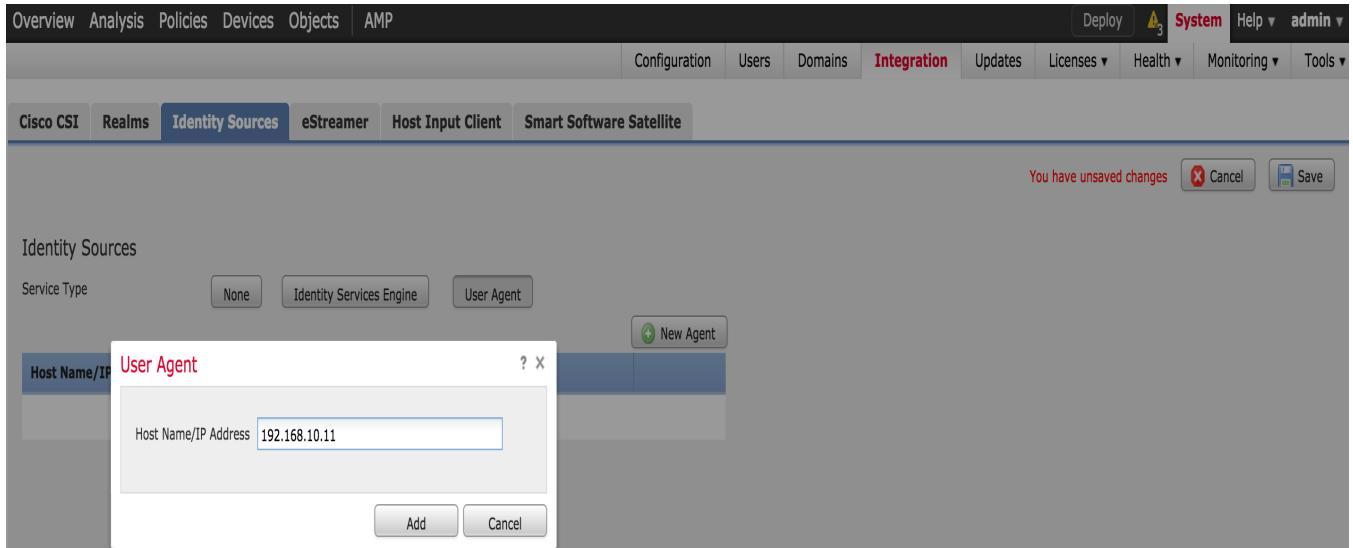
Please follow the Below article to configure FirePOWER User Agent in a Windows machine -

<http://www.cisco.com/c/en/us/support/docs/security/firesight-management-center/118131-technote-sourc...>

### 2. Integration of FirePOWER Management Center (FMC) with User Agent

Login to FirePOWER Management Center, go to **System > Integration > Identity Sources** > click on "New Agent" option. Configure the IP address of User Agent system & click **Add** button & click on **Save** button to save the

changes.



### 3. FirePOWER integration with Active Directory

Login to FMC, go to **System > Integration > Realm** > click on **Add a new realm** option.

**Name & Description** – Give a name/description to uniquely identify realm.

**Type** - AD

**AD Primary Domain** - Domain name of Active Directory

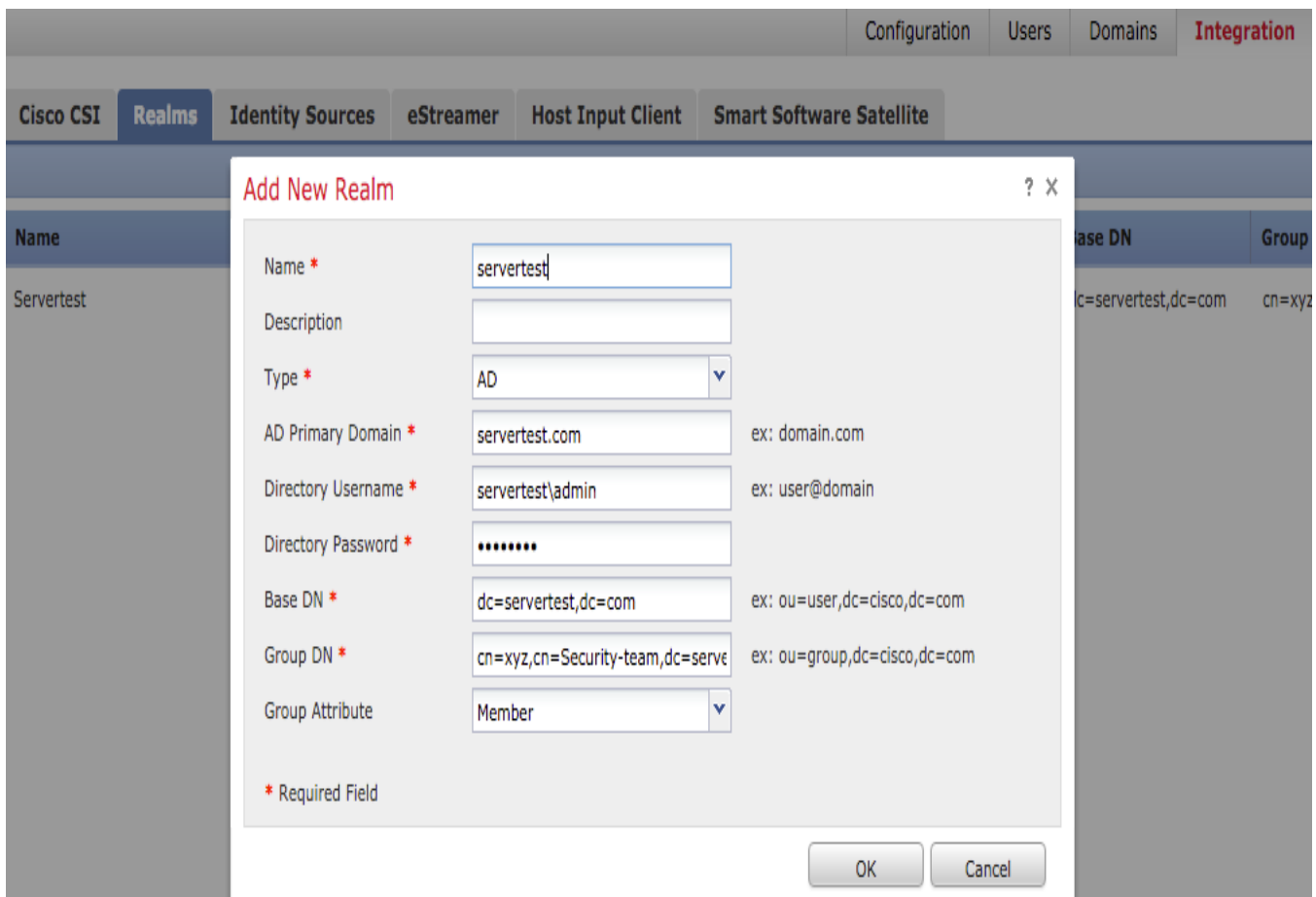
**Directory Username** - <username>

**Directory Password** - <password>

**Base DN** - Domain or Specific OU DN from where system will start search in LDAP database.

**Group DN** – group DN

**Group Attribute** – Member



Below article can help you to figure out the Base DN, Group DN values.

## Identify Active Directory LDAP Object Attributes

Click on **add** button to move to next step. Click on **Add directory** option.

**Hostname/IP Address** – configure the IP address/ hostname of AD server.

**Port** - 389 (Active Directory's LDAP port number)

**Encryption/SSL Certificate** - (optional) To encrypt the connection between FMC & AD server. Below article will help you to configure this -

<http://www.cisco.com/c/en/us/support/docs/security/firesight-management-center/118635-technote-fires...>

The screenshot displays the Cisco FirePOWER Management Center (FMC) interface. The main window shows the 'Integration' tab with a table for 'Add directory'. The table has columns for 'Encryption' and 'none'. A dialog box titled 'Edit directory' is open, showing the following configuration:

- Hostname / IP Address: 192.168.10.11
- Port: 389
- Encryption:  STARTTLS  LDAPS  None
- SSL Certificate: [Dropdown menu]

Buttons for 'OK', 'Test', and 'Cancel' are visible at the bottom of the dialog box.

Click on **Test** button to verify if FMC is able to connect to AD server.

Go to "**Realm Configuration**" to verify integration configuration of AD server. We can do the editing from here.

Go to **User Download** option to fetch the user database from the AD server.

Enable the check box to download **Download users and groups** and define the time interval about how frequent, FMC will contact AD to download user database.

Select the group and put it into the Include option for which you want to configure the authentication.

Enable the AD state -

Name	Description	Domain	Type	Base DN	Group DN	Group Attribute	State
Servertest		Global	AD	dc=servertest,dc=com	ou=xyz,dc=servertest,dc=member		<input checked="" type="checkbox"/>

## 4. Configure the Identity Policy

An identity policy performs user authentication. If the user does not authenticate, access to network resources is refused. This enforces Role Based Access Control (RBAC) to your organization's network and resources.

### 4.1 Captive portal (Active Authentication)

Active Authentication asks for username/password at the browser to identify a user identity for allowing any connection. Browser authenticates user either asking user credential by a pop up window/authentication page or silently with NTLM authentication. NTLM uses the web browser to send and receive authentication information. Active Authentication uses various type to verify the identity of user. Authentication type are -

1. **HTTP Basic** - In this method, browser prompts for user credentials.
2. **NTLM** - NTLM uses windows workstation credentials and negotiate it with Active directory using web browser. We need to enable the NTLM authentication in the browser. User Authentication will happen transparently without prompting credentials. It provides a single sign-on experience for users.
3. **HTTP Negotiate** - In this type, system will try to authenticate using NTLM, if it fails then sensor will use HTTP

Basic authentication type as a fallback method and will prompt a dialog box for user credentials.

4. **HTTP Response page** – this is similar to HTTP basic type, however here user will be prompted to fill the authentication in a HTML form which can be customise.

Each browser has specific way to enable the NTLM authentication so follow browser guidelines to enable the NTLM authentication.

To securely share the credential with the routed sensor, we need to install either self-signed server certificate or publicly-signed server certificate in the identity policy.

Generate a simple self-signed certificate using openssl -

Step 1. Generate the Private key

```
openssl genrsa -des3 -out server.key 1024
```

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 365 -in server.csr -signkey server.key -out
```

Now go to **Policies > Access Control > Identity**. Click on **Add Policy** & give a name to policy and save it.

The screenshot displays the Cisco FirePOWER management interface. At the top, there are navigation tabs: 'Access Control > Identity', 'Network Discovery', 'Application Detectors', 'Correlation', and 'Actions'. On the right, there are buttons for 'Object Management', 'Access Control', 'Compare Policies', and 'New Policy'. Below this is a table with columns: 'Identity Policy', 'Domain', 'Status', and 'Last Modified'. A modal dialog box titled 'New Identity policy' is open in the center. It contains two input fields: 'Name' (with the text 'Identity\_Policy') and 'Description'. At the bottom of the dialog are 'Save' and 'Cancel' buttons. To the right of the dialog, there is a blue link that says 'Add a new policy'.

Now go to **Active Authentication** tab & in **Server Certificate** option, click on icon (+) and upload the certificate & private key which we generated in previous step using openssl.

Overview Analysis **Policies** Devices Objects AMP Deploy 1 System Help admin

Access Control Identity Network Discovery Application Detectors Correlation Actions

## Identity\_Policy

You have unsaved changes Save Cancel

Enter a description

Rules **Active Authentication**

Server Certificate \*  +

Port \*  (885 or 1025 - 65535)

Maximum login attempts \*  (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.

?

\* Required when using Active Authentication

Now click on **Add rule** button & give a name to the Rule & choose action as **Active Authentication**. Define the source/destination zone, source/destination network for which you want to enable the user authentication.

Select the **Realm** which we have configured in previous step and authentication type which best suits your environment.

Overview Analysis **Policies** Devices Objects AMP Deploy 1 System Help admin

Access Control Identity Network Discovery Application Detectors Correlation Actions

## Identity\_Policy

Enter a description

Rules **Active Authentication**

**Add Rule** ? X

Name   Enabled Insert into Category

Action  **Realm:** Srvtest (AD) **Authentication Type:** HTTP Negotiate **Exclude HTTP User-Agents:** None

Zones Networks VLAN Tags Ports **Realm & Settings**

Realm \*  ?

Identify as Special Identities/Guest if authentication cannot identify user

Authentication Type

Application Filters Available Applications (83) Exclude HTTP User-Agents (0)

**Risks (Any Selected)**

Very Low	19
Low	40
Medium	11
High	6

- ABC
- AdobeAIR
- Advanced Packaging Tool
- AirPlay
- Amazon Instant Video

Add to Rule

\* Required Field

Add Cancel

### 4.2 Single-Sign-On (Passive Authentication)

In passive authentication, When a domain user logs in and able to authenticate the AD. FirePOWER User Agent polls the User-IP mapping details from the security logs of AD and share this information with FirePOWER Management Center (FMC). FMC sends these details to sensor to enforce the access control.

click on **Add rule** button & give a name to the Rule & choose **Action** as **Passive Authentication**. Define the source/destination zone, source/destination network for which you want to enable the user authentication.

Select the **Realm** which we have configured in previous step and authentication type which best suites your environment.

Here we can choose fall back method as **Active authentication if passive authentication cannot identify the user identity**.

The screenshot displays the Cisco FirePOWER GUI. The main window shows the configuration for 'Identity\_Policy'. A modal dialog titled 'Editing Rule - Captive\_Portal' is open, showing the following details:

- Name:** Single\_Sign\_On (with an 'Enabled' checkbox and a 'Move' link)
- Action:** Passive Authentication (dropdown menu)
- Realm:** Servertest
- Authentication Type:** HTTP Negotiate
- Exclude HTTP User-Agents:** None
- Realm & Settings:**
  - Realm:** Servertest (dropdown menu)
  - Use active authentication if passive authentication cannot identify user

Buttons for 'Save' and 'Cancel' are visible at the bottom of the dialog. The background shows the 'Identity\_Policy' configuration page with a 'Show Warnings' button and 'Save'/'Cancel' buttons.

## 5. Configure the Access Control Policy

Go to **Policies > Access Control > Create/Edit** a Policy

Click on **Identity Policy** (left-hand side upper corner), choose the Identify Policy which we have configured in previous step and choose **OK** button.

The screenshot displays the Cisco FirePOWER GUI for the 'NGFW\_Policy' configuration. The 'Identity Policy' dropdown menu is open, showing 'Identity\_Policy' as the selected option. The background shows the 'NGFW\_Policy' configuration page with a 'Show Warnings' button and 'Save'/'Cancel' buttons. The 'Identity Policy' dropdown menu has 'Identity\_Policy' selected, and there are 'Revert to Defaults', 'OK', and 'Cancel' buttons at the bottom.

Click on **Add rule** button to add a new rule, go to **Users** and select the users for which access control rule will enforce. Click on **OK** button and click on **Save** button to save the changes.

The screenshot displays the Cisco FirePOWER management interface. The main window shows the 'Policies' configuration page for 'NGFW\_Policy'. A modal dialog titled 'Editing Rule - Allow\_LAN\_User' is open. In this dialog, the rule name is 'Allow\_LAN\_User', it is checked as 'Enabled', and the action is set to 'Allow'. The 'Users' tab is active, showing a list of available users. Two users, 'Servertest/sunil' and 'Servertest/admin', are selected and listed in the 'Selected Users (2)' section. The dialog includes search fields for 'Available Realms' and 'Available Users', and buttons for 'Add to Rule', 'OK', and 'Cancel'.

## 6. Deploy the Access Control Policy

Navigate to **Deploy** option, choose the **Device** and click on **Deploy** option to push the configuration change to the sensor. Monitor the Deployment of policy from the **Message Center Icon (icon between Deploy and System option)** option and make sure, policy should apply successfully.



Deploy
⚠️ 3
System
Help ▾
admin ▾

Deploy Policies
Version: 2015-12-10 09:29 PM
?
X

	Device	Group	Current Version
☐	NGFW		2015-12-10 09:14 PM
✔	NGFW Settings: NGFW		
⌚	Access Control Policy: NGFW_Policy		
✔	Intrusion Policy: Balanced Security and Connectivity		
✔	Intrusion Policy: No Rules Active		
✔	Identity Policy: Identity_Policy		
✔	DNS Policy: Default DNS Policy		
✔	Network Discovery		
✔	Device Configuration ( <a href="#">Details</a> )		

Selected devices: 0
Deploy
Cancel

## 7. Monitor user events & Connections events

Currently active user sessions are available in the **Analysis > Users > Users** section.

User Activity monitoring helps us to figure out which user has associated with which IP address and how is user detected by system either by active or passive authentication (**Analysis > Users > User Activity**)

## User Activity

[Table View of Events](#) > [Users](#)

No Search Constraints ([Edit Search](#))

<input type="checkbox"/>	Time	Event	Realm	Username	Type	Authentication Type	IP Address
<input type="checkbox"/>	2015-12-10 11:15:34	User Login	Servertest	sunil	LDAP	Active Authentication	192.168.20.20
<input type="checkbox"/>	2015-12-10 10:47:31	User Login	Servertest	admin	LDAP	Passive Authentication	192.168.0.6

Go to **Analysis > Connections > Events**, to monitor the type of traffic being used by user

Overview **Analysis** Policies Devices Objects AMP Deploy System Help admin

Context Explorer **Connections > Events** Intrusions Files Hosts Users Vulnerabilities Correlation Custom Search

[Bookmark This Page](#) [Report Designer](#) [Dashboard](#) [View Bookmarks](#) [Search](#)

### Connection Events (switch workflow)

[Connections with Application Details](#) > [Table View of Connection Events](#)

2015-12-05 00:17:00 - 2015-12-12 01:22:07

Expanding

Search Constraints ([Edit Search](#) [Save Search](#))

Disabled Columns

Jump to...

<input type="checkbox"/>	First Packet	Last Packet	Action	Initiator IP	Initiator User	Responder IP	Access Control Rule	Ingress Interface	Egress Interface	Count
<input type="checkbox"/>	2015-12-11 10:31:59	2015-12-11 10:34:19	Allow	192.168.20.20	sunil (Servertest\sunil, LDAP)	74.201.154.156	Allow LAN User	Inside-2	Outside	1
<input type="checkbox"/>	2015-12-11 10:31:59		Allow	192.168.20.20	sunil (Servertest\sunil, LDAP)	74.201.154.156	Allow LAN User	Inside-2	Outside	1
<input type="checkbox"/>	2015-12-11 09:46:28	2015-12-11 09:46:29	Allow	192.168.20.20	sunil (Servertest\sunil, LDAP)	173.194.207.113	Allow LAN User	Inside-2	Outside	1
<input type="checkbox"/>	2015-12-11 09:46:28		Allow	192.168.20.20	sunil (Servertest\sunil, LDAP)	173.194.207.113	Allow LAN User	Inside-2	Outside	1
<input type="checkbox"/>	2015-12-11 09:46:07	2015-12-11 09:46:58	Allow	192.168.20.20	sunil (Servertest\sunil, LDAP)	173.194.207.113	Allow LAN User	Inside-2	Outside	1
<input type="checkbox"/>	2015-12-11 09:46:07		Allow	192.168.20.20	sunil (Servertest\sunil, LDAP)	173.194.207.113	Allow LAN User	Inside-2	Outside	1
<input type="checkbox"/>	2015-12-11 09:45:46	2015-12-11 09:46:36	Allow	192.168.20.20	sunil (Servertest\sunil, LDAP)	173.194.207.113	Allow LAN User	Inside-2	Outside	1

Last login on Thursday, 2015-12-10 at 11:17:25 AM from 10.65.39.169

Right-click for menu

