

# Configure Active Directory Integration with Firepower Appliance for Single-Sign-On & Captive Portal Authentication

## Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Components Used](#)

[Background Information](#)

[Configure](#)

[Step 1. Configure the Firepower User Agent for Single-Sign-On](#)

[Step 2. Integrate the Firepower Management Center \(FMC\) with User Agent](#)

[Step 3. Integrate Firepower with Active Directory](#)

[Step 3.1 Create the Realm](#)

[Step 3.2 Add the Directory Server](#)

[Step 3.3 Modify the Realm Configuration](#)

[Step 3.4 Download User database](#)

[Step 4. Configure the Identity Policy](#)

[Step 4.1 Captive portal \(Active Authentication\)](#)

[Step 4.2 Single-Sign-On \(Passive Authentication\)](#)

[Step 5. Configure the Access Control Policy](#)

[Step 6. Deploy the Access Control Policy](#)

[Step 7. Monitor user events & Connections events](#)

[Verify and Troubleshoot](#)

[Verify Connectivity between FMC and User Agent \(Passive Authentication\)](#)

[Verify Connectivity between FMC and Active Directory](#)

[Verify Connectivity between Firepower Sensor and End system \(Active Authentication\)](#)

[Verify Policy configuration & Policy Deployment](#)

[Analyse the Events logs](#)

[Related Information](#)

## Introduction

This document describes the configuration of Captive portal authentication (Active Authentication) and Single-Sign-On (Passive Authentication).

## Prerequisites

## Requirements

Cisco recommends that you have knowledge of these topics:

- Sourcefire Firepower devices
- Virtual device models
- Light Weight Directory Service (LDAP)
- Firepower UserAgent

## Components Used

The information in this document is based on these software and hardware versions:

- Firepower Management Center (FMC) version 6.0.0 and higher
- Firepower sensor version 6.0.0 and higher

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

## Background Information

Captive Portal Authentication or Active Authentication prompts a login page and user credentials are required for a host to get the internet access.

Single-Sign-On or Passive Authentication provides seamless authentication to a user for network resources and internet access without multiple user credential occurrences. The Single-Sign-on authentication can be achieved either by Firepower user agent or NTLM browser authentication.

---

**Note:** For Captive Portal Authentication, appliance must be in routed mode.

---

## Configure

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

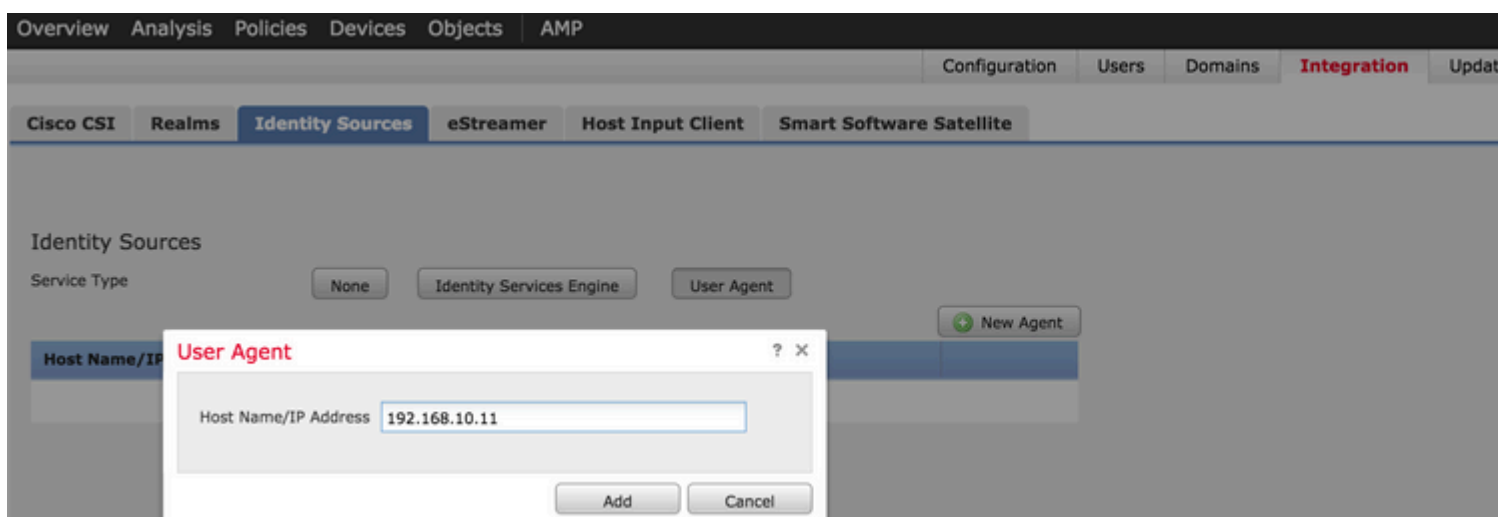
This article explains how to configure Firepower User Agent in a Windows machine:

#### [Installation and Uninstallation of Sourcefire User Agent](#)

### Step 2. Integrate the Firepower Management Center (FMC) with User Agent

Log in to Firepower Management Center, navigate to **System > Integration > Identity Sources**. Click the **New Agent** option. Configure the IP address of User Agent system & click the **Add** button.

Click the **Save** button to save the changes.



## Step 3. Integrate Firepower with Active Directory

### Step 3.1 Create the Realm

Log in to the FMC, navigate to **System > Integration > Realm**. Click the **Add 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 the system starts a search in LDAP database.

**Group DN:** group DN

**Group Attribute:** Member

The screenshot shows the 'Add New Realm' configuration page in the Cisco FMC. The page has a navigation bar at the top with tabs for Configuration, Users, Domains, Integration, and Update. Below the navigation bar, there are tabs for Cisco CSI, Realms, Identity Sources, eStreamer, Host Input Client, and Smart Software Satellite. The 'Realms' tab is selected. On the left, there is a table with columns 'Name' and 'Description'. The table contains one entry: 'servertest-1'. On the right, there is a form titled 'Add New Realm' with the following fields:

- Name: Servertest
- Description: (empty)
- Type: AD
- AD Primary Domain: servertest.com (example: domain.com)
- Directory Username: servertest\admin (example: user@domain)
- Directory Password: (masked with dots)
- Base DN: dc=servertest,dc=com (example: ou=user,dc=cisco)
- Group DN: cn=TAC,ou=Security-Team,dc=ser (example: ou=group,dc=cisco)
- Group Attribute: Member

A legend at the bottom left of the form indicates that an asterisk (\*) denotes a required field. An 'OK' button is located at the bottom right of the form.

This article helps you to figure out the Base DN and Group DN values.

### [Identify Active Directory LDAP Object Attributes](#)

### Step 3.2 Add the Directory Server

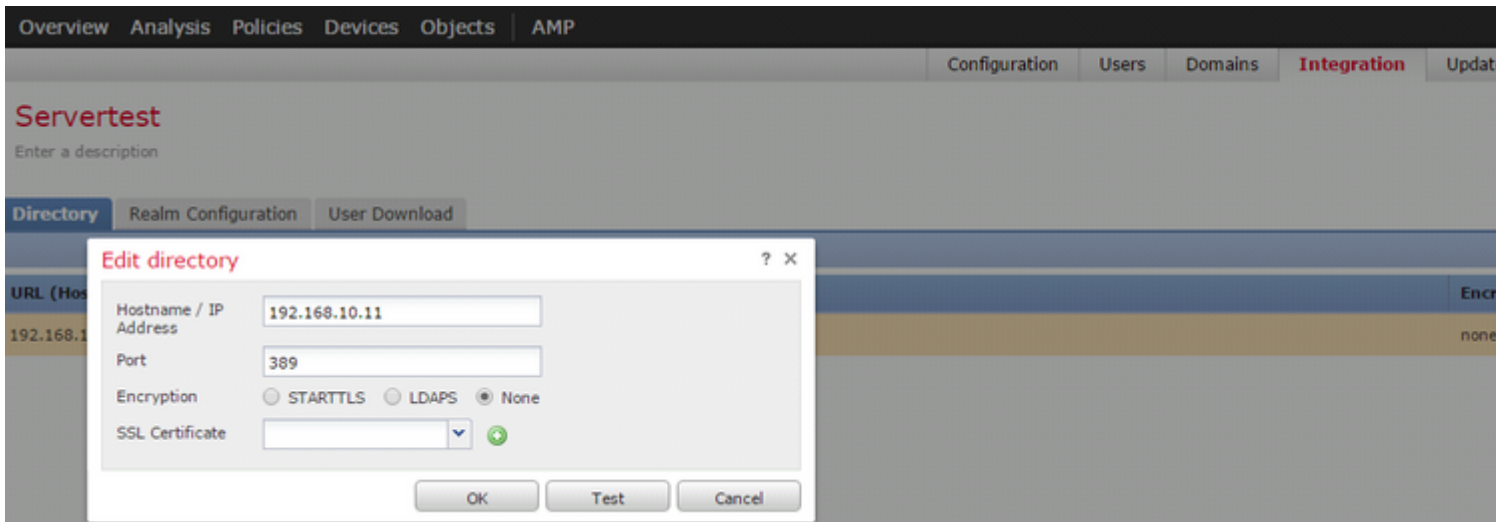
Click the **Add** button in order to navigate to next step and thereafter Click the **Add directory** option.

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

**Port:** 389 (Active Directory LDAP port number )

**Encryption/SSL Certificate:** (optional) To encrypt the connection between FMC & AD server , refer to the article: [Verification of Authentication Object on FireSIGHT System for Microsoft AD Authentication](#)

## Over SSL/TLS



Click the **Test** button in order to verify if FMC is able to connect to the AD server.

### **Step 3.3 Modify the Realm Configuration**

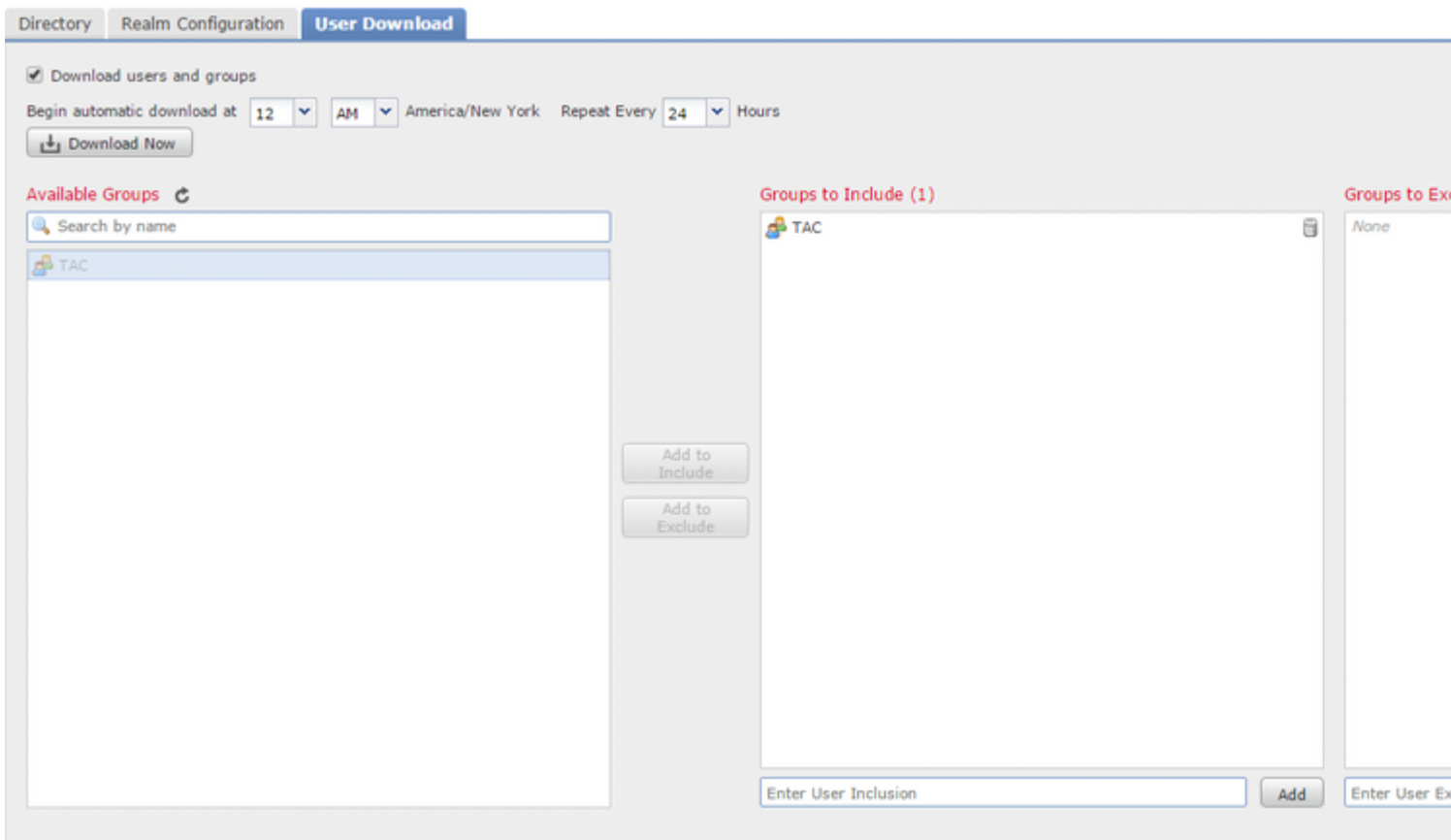
Navigate to **Realm Configuration** in order to verify integration configuration of AD server and you can modify the AD configuration.

### **Step 3.4 Download User database**

Navigate 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 frequently FMC contacts AD to download user database.

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



As shown in the image, enable the AD state:

Overview   Analysis   Policies   Devices   Objects   AMP					
Dashboards ▾   Reporting   Summary ▾					
Cisco CSI   Realms   Identity Sources   eStreamer   Host Input Client   Smart Software Satellite					
Name	Description	Domain	Type	Base DN	Group DN
servertest-1		Global	AD	dc=servertest,dc=com	cn=TAC,ou=Sec

## Step 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.

### Step 4.1 Captive portal (Active Authentication)

Active Authentication asks for username/password at the browser to identify a user identity to allow any connection. Browser authenticates user with an authentication page or authenticates silently with NTLM authentication. NTLM uses the web browser to send and receive authentication information. Active Authentication uses various types to verify the identity of the user. Different types of Authentication are:

1. **HTTP Basic:** In this method, the browser prompts for user credentials.
2. **NTLM:** NTLM uses windows workstation credentials and negotiates it with Active directory through a web browser. You need to enable the NTLM authentication in the browser. User Authentication happens transparently without prompts for credentials. It provides a single sign-on experience for

users.

3. **HTTP Negotiate:**In this type, the system tries to authenticate with NTLM. If it fails, then the sensor uses HTTP Basic authentication type as a fallback method and prompts a dialog box for user credentials.
4. **HTTP Response page:** This is similar to HTTP basic type, however, here user is prompted to fill the authentication in an HTML form which can be customized.

Each browser has a specific way to enable the NTLM authentication and hence they adhere to browser guidelines in order to enable the NTLM authentication.

To securely share the credential with the routed sensor, you 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 2048
```

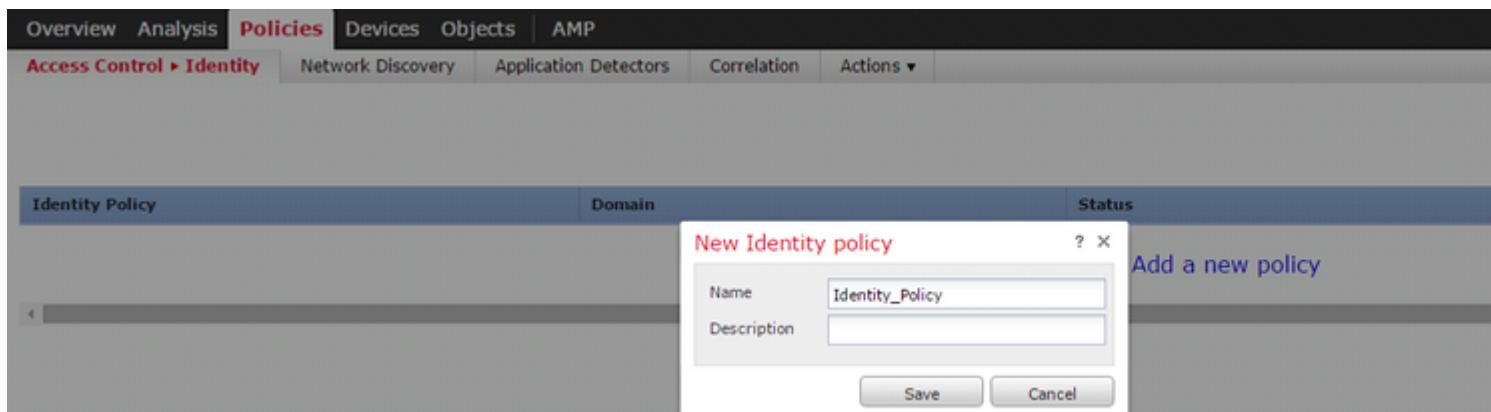
Step 2. Generate Certificate Signing Request (CSR)

```
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
```

Navigate to **Policies > Access Control > Identity**. Click the **Add Policy** & give a name to policy and save it.



Navigate to **Active Authentication** tab & in the **Server Certificate** option, click the **icon (+)** and upload the certificate & private key which you generated in the previous step with openssl.



Overview Analysis **Policies** Devices Objects AMP

Access Control ► Identity Network Discovery Application Detectors Correlation Actions ▼

## Identity\_Policy

Enter a description

Rules **Active Authentication**

Server Certificate \* Self\_Sign\_Cert +

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

Now click the **Add rule** button & give a name to the Rule & choose the 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 you have configured in the previous step and authentication type that best suits your environment.

Overview Analysis **Policies** Devices Objects AMP

Access Control ► Identity Network Discovery Application Detectors Correlation Actions ▼

## Identity\_Policy

Enter a description

Rules Active Authentication

**Add Rule**

Name: Captive\_Portal  Enabled Insert: into Category Standards

Action: Active Authentication **Realm:** Servertest (AD) **Authentication Type:** HTTP Negotiate **Exclude HTTP User-Agent:**

Zones Networks VLAN Tags Ports

**Realm \*** Servertest (AD) ✎

Identify as Special Identities/Guest if authentication cannot identify user

**Authentication Type** HTTP Negotiate

**Application Filters** **Available Applications (83)** **Exclude HTTP User-Agent**

Search by name

**Risks (Any Selected)**

<input type="checkbox"/> Very Low	19
<input type="checkbox"/> Low	40
<input type="checkbox"/> Medium	11
<input type="checkbox"/> High	6

Search by name

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

**Add to Rule**

\* Required Field

## ASA configuration for Captive Portal

For ASA Firepower module, Configure these commands on the ASA in order to configure the captive portal.

```
ASA(config)# captive-portal global port 1055
```

Ensure that the server port, TCP 1055 is configured in the **port** option of the Identity Policy **Active Authentication** tab.

In order to verify the active rules and their hit counts, run the command:

```
ASA# show asp table classify domain captive-portal
```

---

**Note:** Captive portal command is available in ASA version 9.5(2) and later.

---

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

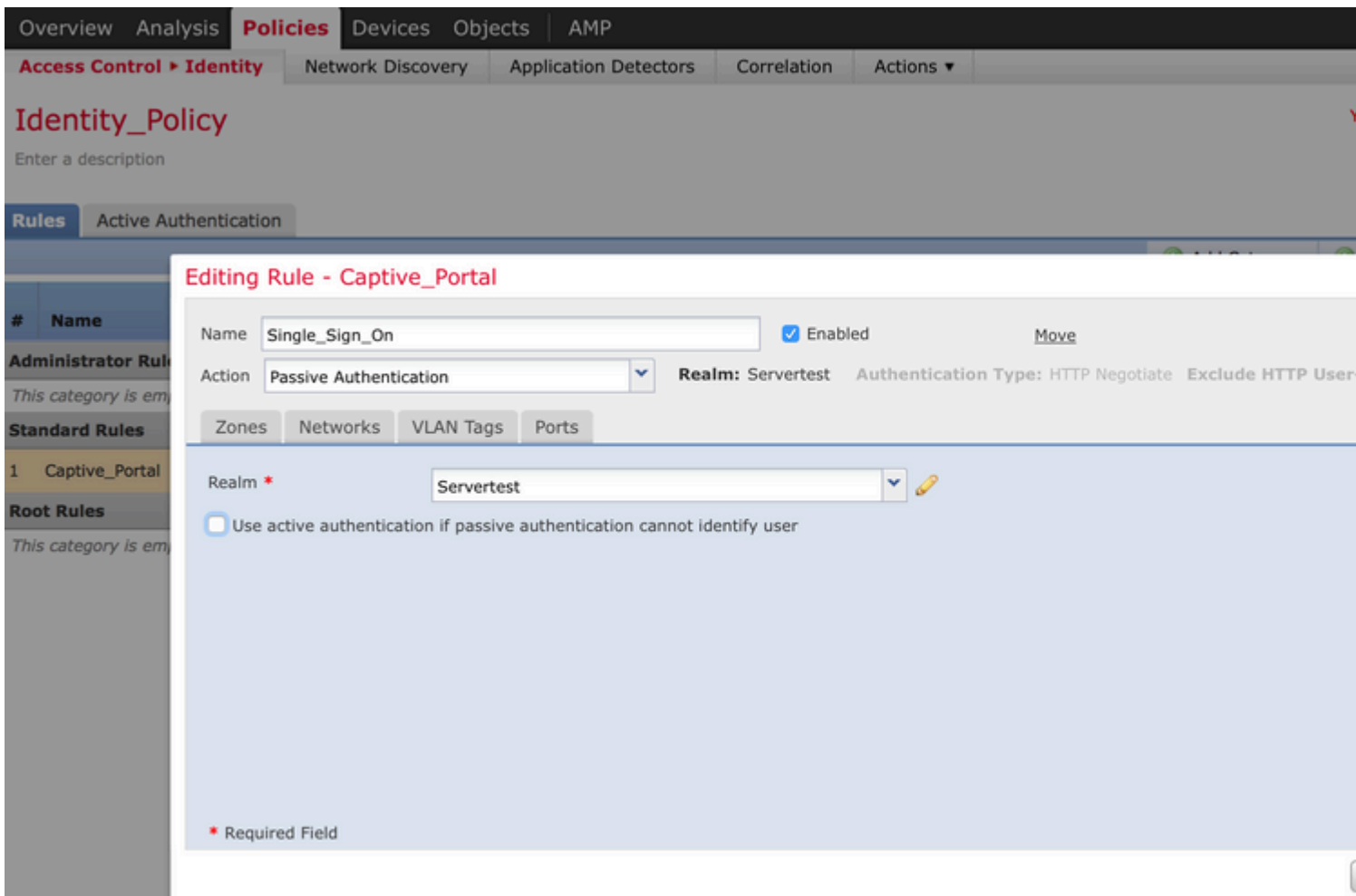
In passive authentication, when a domain user logs in and is able to authenticate the AD, the Firepower User Agent polls the User-IP mapping details from the security logs of AD and shares this information with Firepower Management Center (FMC). FMC sends these details to the sensor in order to enforce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

Click the **Add rule** button & give a name to the Rule & choose the **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 you have configured in the previous step and authentication type which best suits your environment, as shown in this image.

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

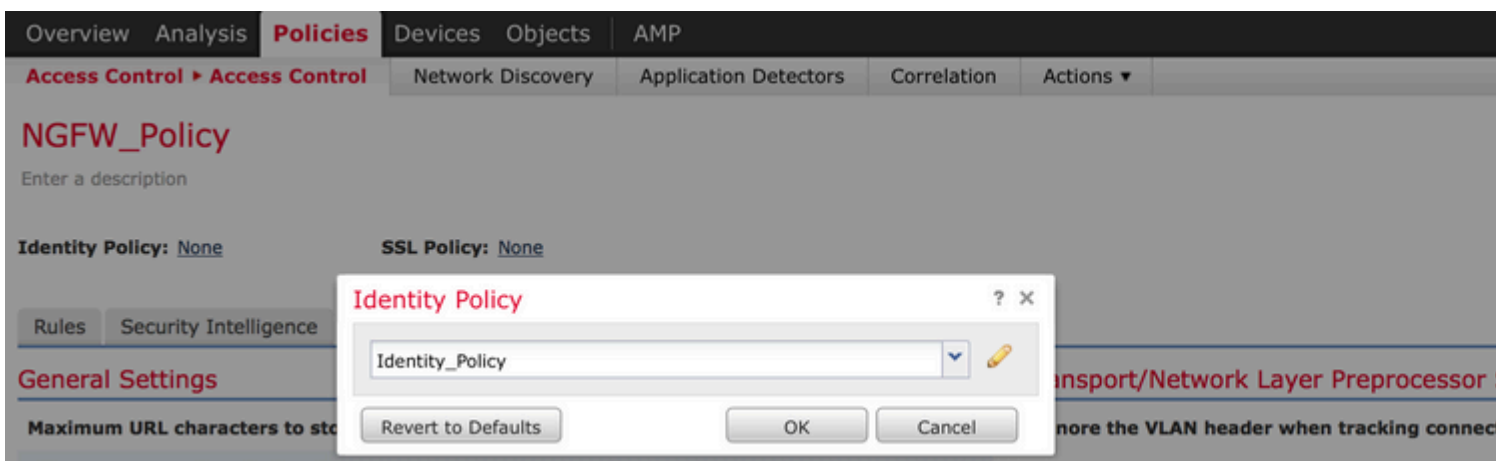




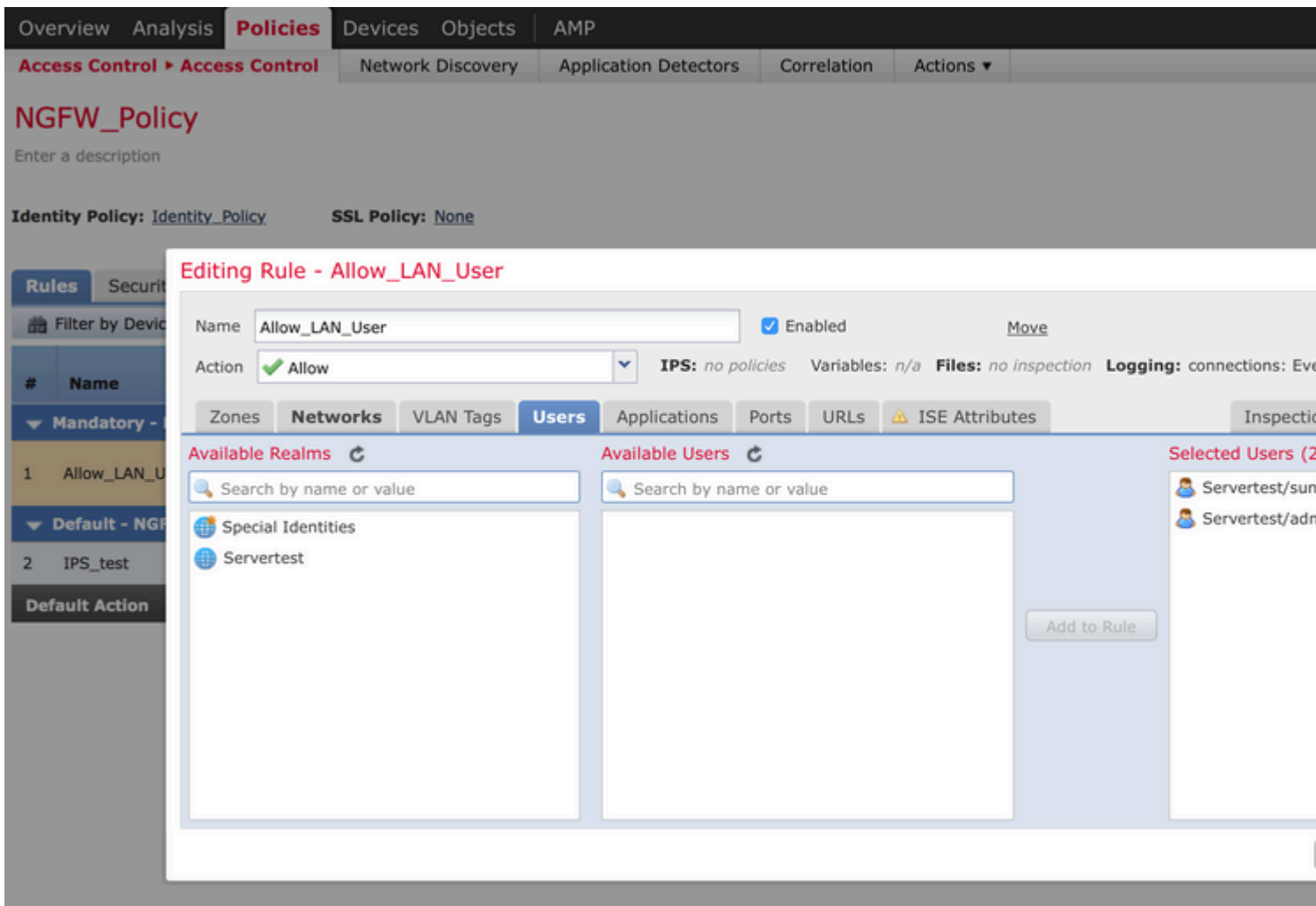
## Step 5. Configure the Access Control Policy

Navigate to **Policies > Access Control > Create/Edit** a Policy.

Click the **Identity Policy** (left-hand side upper corner), choose the Identify Policy that you have configured in the previous step and click the **OK** button, as shown in this image.



Click the **Add rule** button to add a new rule. Navigate to **Users** and select the users for which access control rule enforces, as shown in this image. Click **OK** and click **Save** in order to save the changes.



## Step 6. Deploy the Access Control Policy

Navigate to **Deploy** option, choose the **Device** and click the **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 ensure that policy must apply successfully, as shown in this image.

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

Device	Group
NGFW	
<input checked="" type="checkbox"/> NGFW Settings: NGFW	
<input type="checkbox"/> Access Control Policy: NGFW_Policy	
<input checked="" type="checkbox"/> Intrusion Policy: Balanced Security and Connectivity	
<input checked="" type="checkbox"/> Intrusion Policy: No Rules Active	
<input checked="" type="checkbox"/> Identity Policy: Identity_Policy	
<input checked="" type="checkbox"/> DNS Policy: Default DNS Policy	
<input checked="" type="checkbox"/> Network Discovery	
<input checked="" type="checkbox"/> Device Configuration ( <a href="#">Details</a> )	

Selected devices: 0

## Step 7. Monitor user events & Connections events

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

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

## User Activity

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

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

	Time	Event	Realm	Username	Type	Authentication Type	IP Address
↓	2015-12-10 11:15:34	User Login	Servertest	sunil	LDAP	Active Authentication	192.168.2
↓	2015-12-10 10:47:31	User Login	Servertest	admin	LDAP	Passive Authentication	192.168.0

Navigate to **Analysis > Connections > Events**, to monitor the type of traffic that is used by the user.

Overview **Analysis** Policies Devices Objects AMP

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

Bookmark This Page

### Connection Events (switch workflow)

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

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

Jump to...

	First Packet	Last Packet	Action	Initiator IP	Initiator User	Responder IP	Access Control Rule
↓	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
↓	2015-12-11 10:31:59		Allow	192.168.20.20	sunil (Servertest\sunil, LDAP)	74.201.154.156	Allow LAN User
↓	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
↓	2015-12-11 09:46:28		Allow	192.168.20.20	sunil (Servertest\sunil, LDAP)	173.194.207.113	Allow LAN User
↓	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
↓	2015-12-11 09:46:07		Allow	192.168.20.20	sunil (Servertest\sunil, LDAP)	173.194.207.113	Allow LAN User
↓	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

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

## Verify and Troubleshoot

Navigate to **Analysis > Users** in order to verify the User authentication/Authentication type/User-IP mapping/access rule associated with the traffic flow.

### Verify Connectivity between FMC and User Agent (Passive Authentication)

Firepower Management Center (FMC) uses TCP port 3306, in order to receive user activity log data from the User Agent.

In order to verify the FMC service status, use this command in the FMC.

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

Run packet capture on the FMC in order to verify connectivity with the User Agent.

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

Navigate to **Analysis > Users > User Activity** in order to verify whether the FMC receives user login details from the User Agent.

## Verify Connectivity between FMC and Active Directory

FMC uses TCP port 389 in order to retrieve User Database from the Active directory.

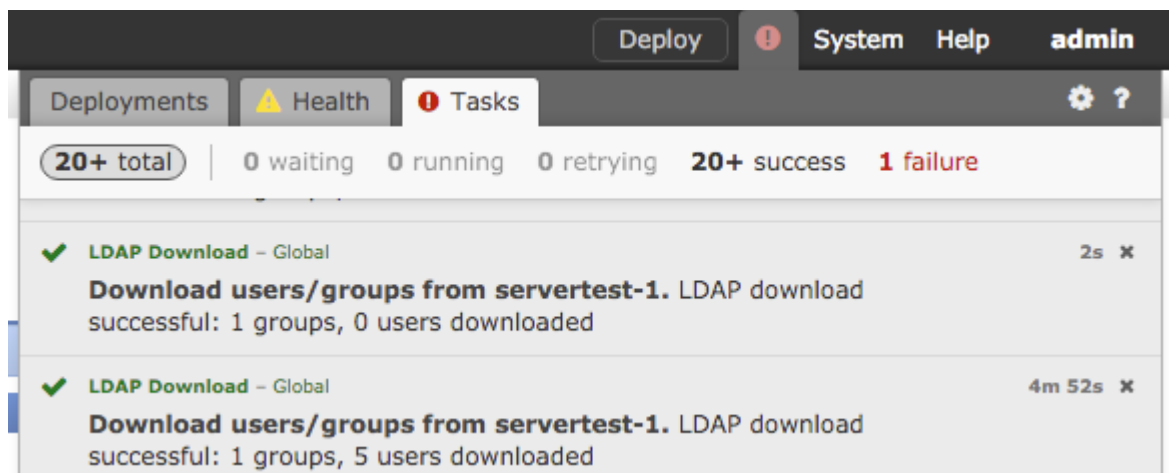
Run packet capture on the FMC to verify connectivity with the Active Directory.

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

Ensure that the user credential used in FMC Realm configuration has sufficient privilege to fetch the AD User database.

Verify the FMC realm configuration, and ensure that the users/groups are downloaded and user session timeout is configured correctly.

Navigate to **Message Center > Tasks** and ensure that the task **users/groups download** completes successfully , as shown in this image.



## Verify Connectivity between Firepower Sensor and End system (Active Authentication)

For active authentication, ensure that the certificate and port are configured correctly in FMC Identity policy. By default, Firepower sensor listens on TCP port 885 for active authentication.

## Verify Policy configuration & Policy Deployment

Ensure that the Realm, Authentication type, User agent and Action fields are configured correctly in Identity Policy.

Ensure that the Identity policy is correctly associated with the Access Control policy.

Navigate to **Message Center > Tasks** and ensure that the Policy Deployment completes successfully.

## Analyse the Events logs

Connection and the User Activity events can be used to diagnose whether the user login is successful or not. These events

can also verify which Access Control rule is applied on the flow.

Navigate to **Analysis > User** to check the user events logs.

Navigate to **Analysis > Connection Events** to check the connection events.

### Related Information

- [Technical Support & Documentation - Cisco Systems](#)