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

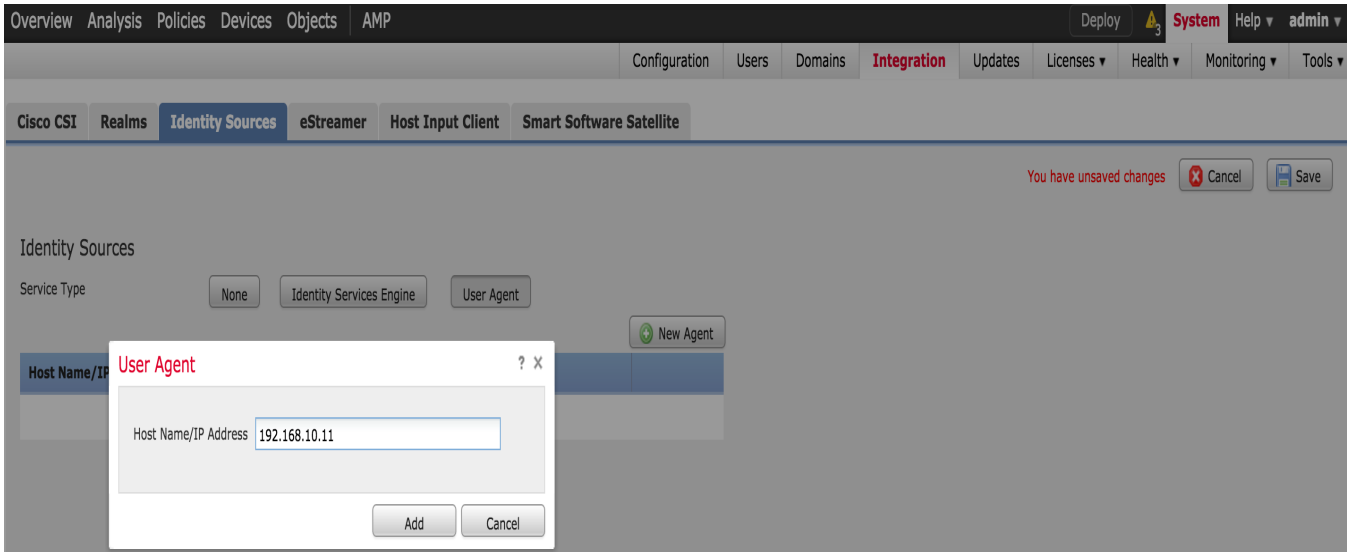
1. Configure the FirePOWER User Agent for Single-Sign-On

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

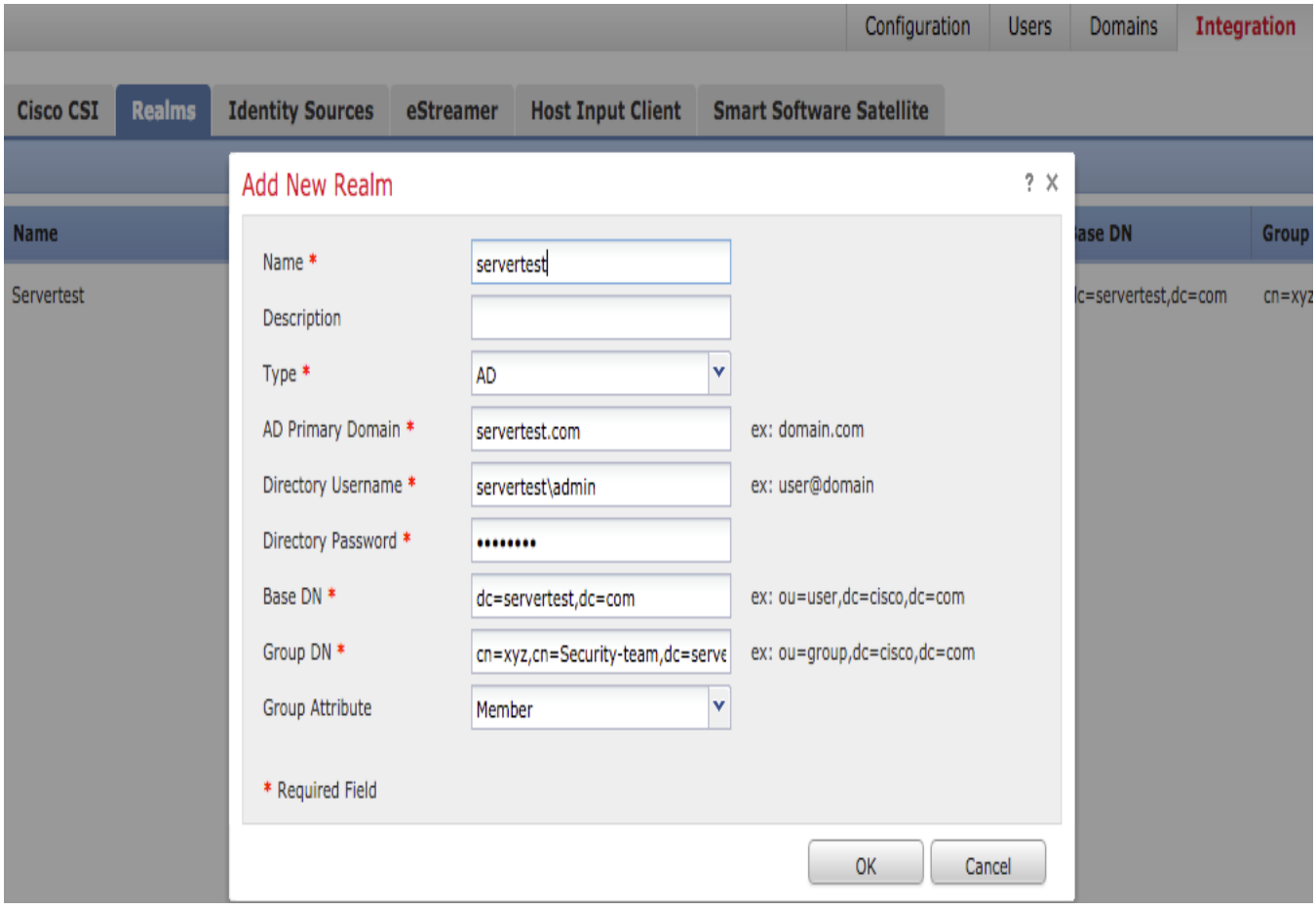
changes.



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



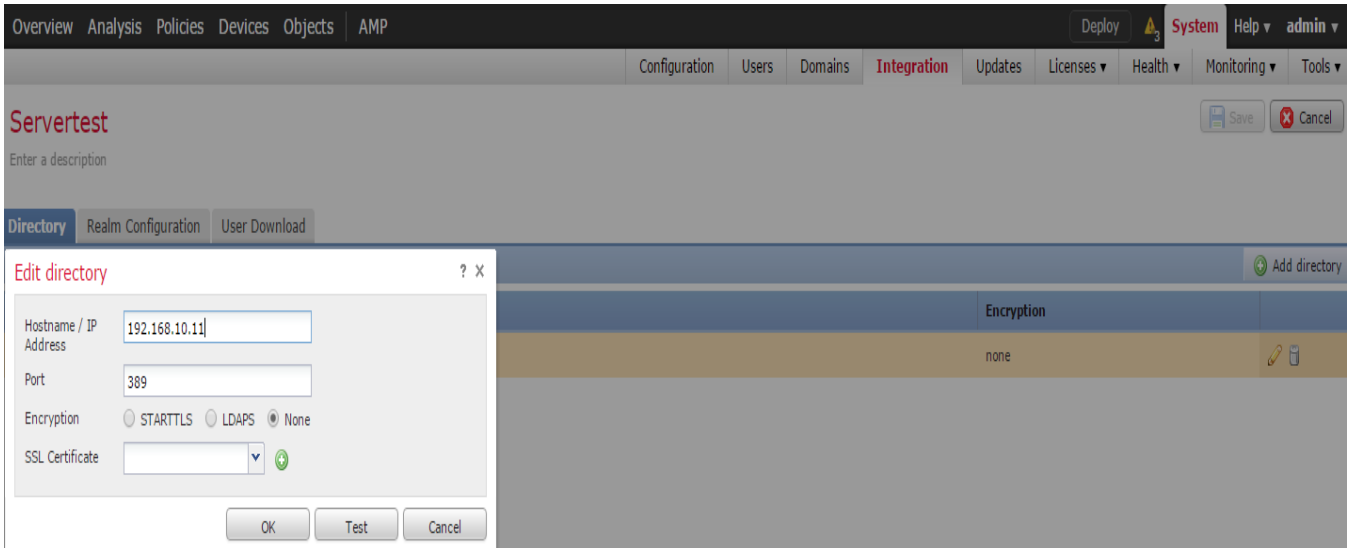
Below article can help you to figure out the Base DN, Group DN values.

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 Direcotory'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...



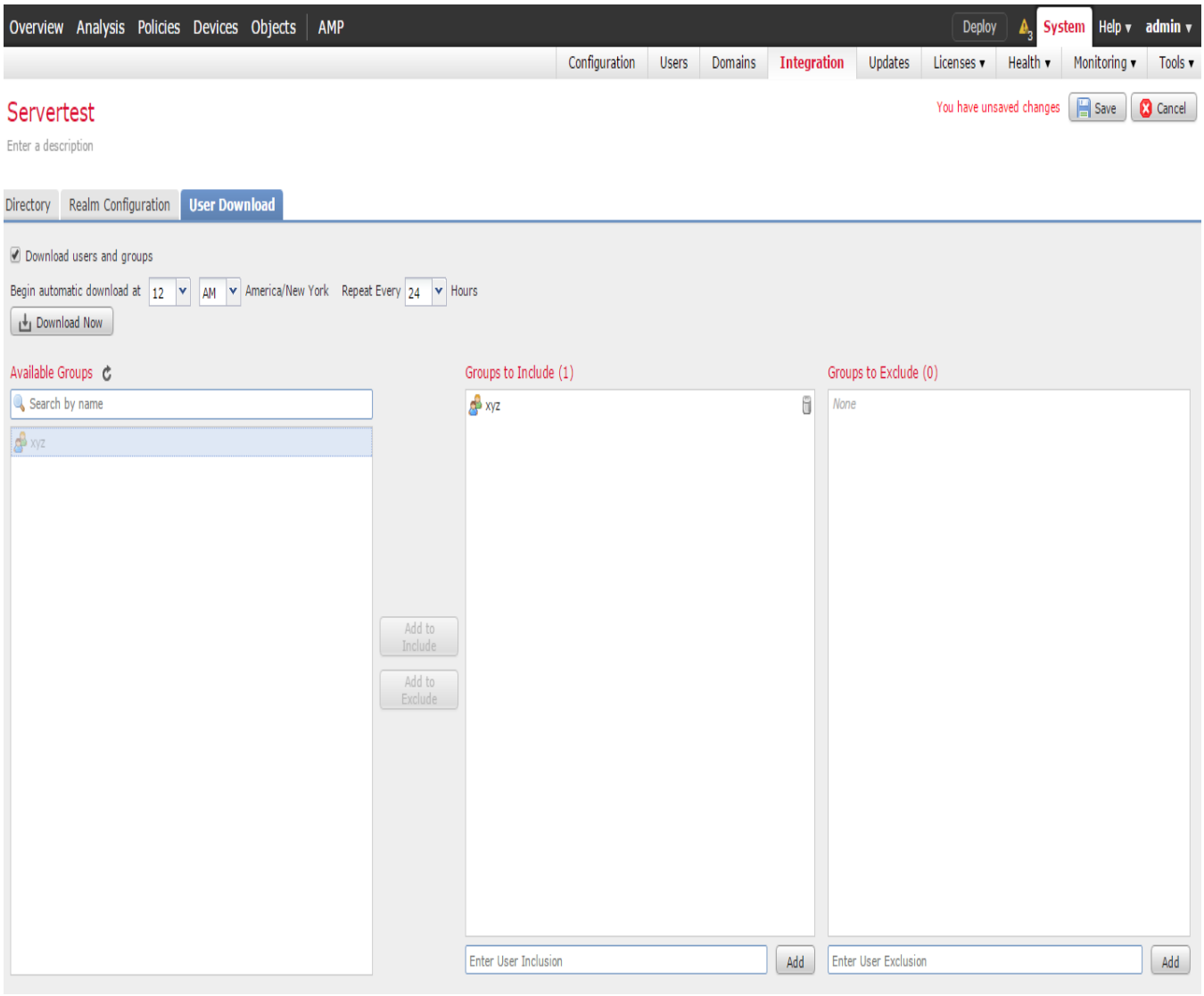
Click on **Test** button to verify if FMC is able to connect to AD server.

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

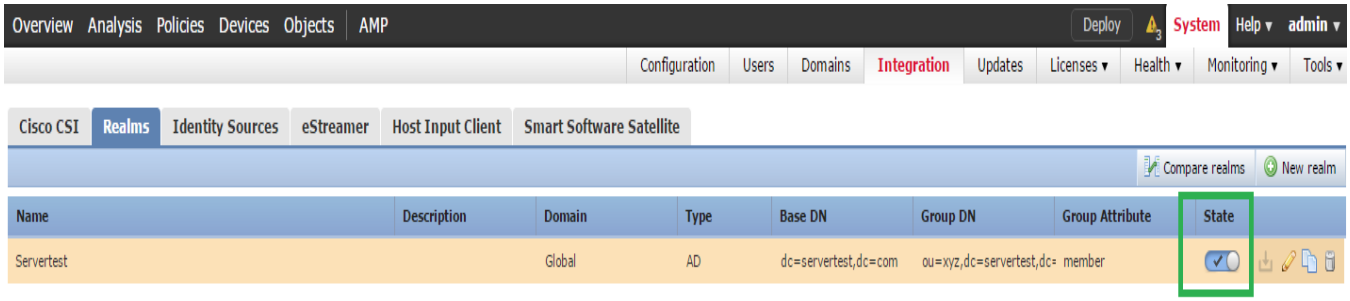
Go to **User Download** option to fetch the user database from the AD server.

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 -



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.

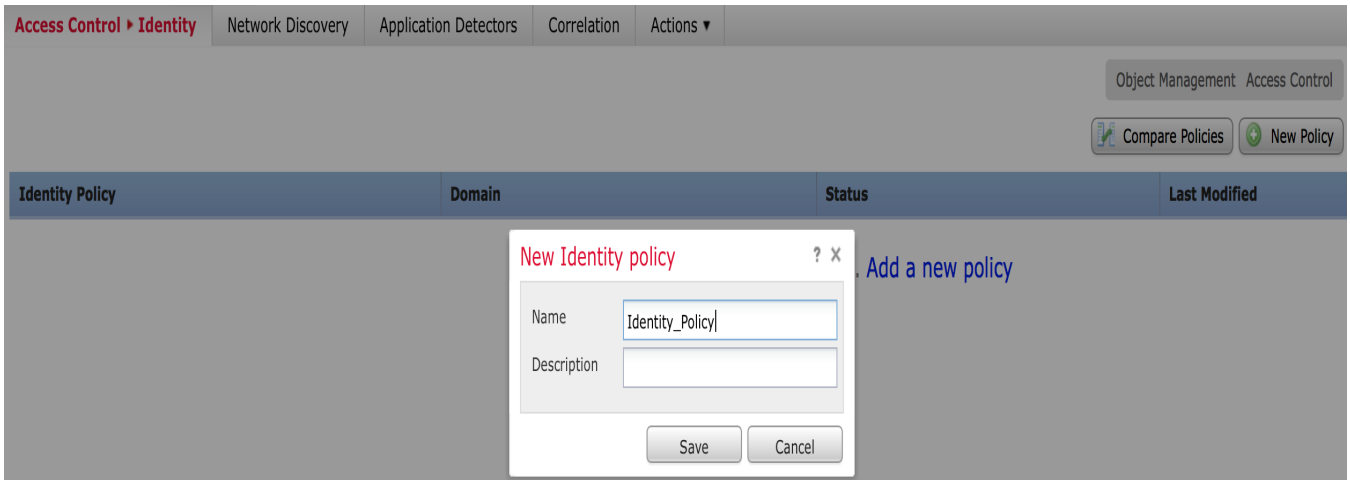
4. **HTTP Response page** – this is similar to HTTP basic type, however here user will be prompted to fill the authentication in a HTML form which can be customise.

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

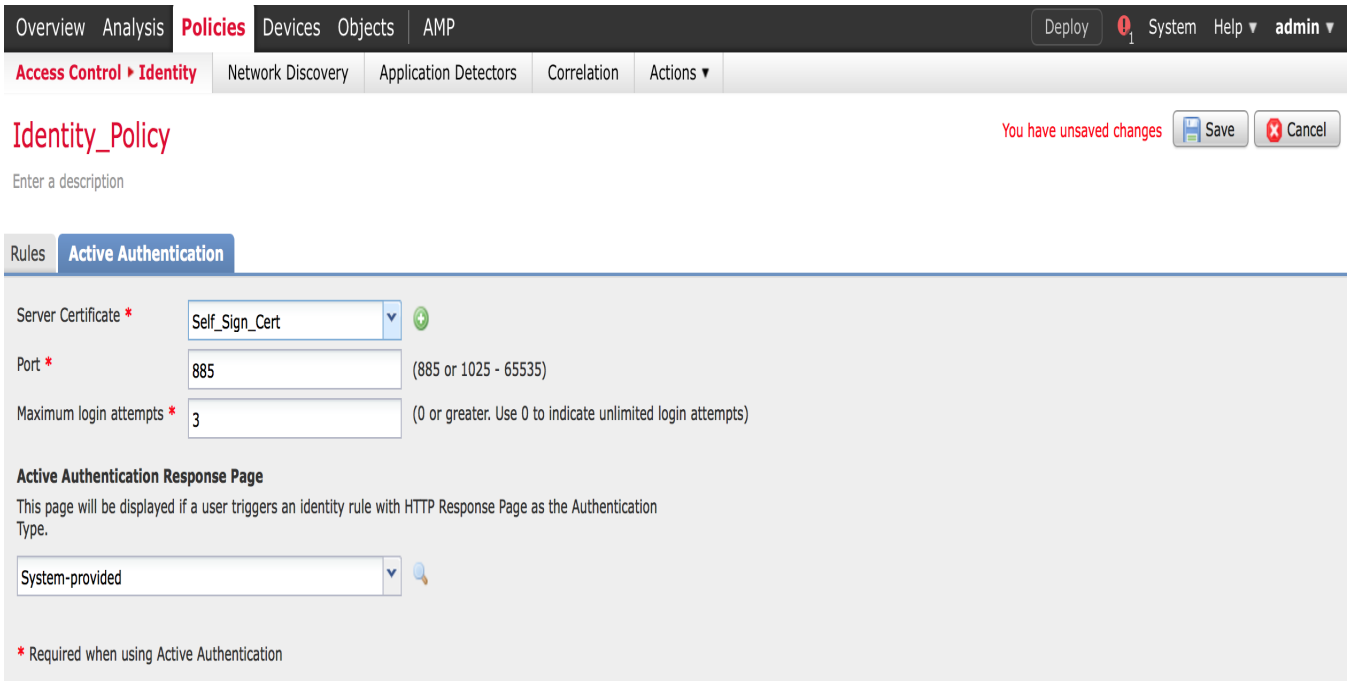
To securely share the credential with the routed sensor, we need to install either self-signed server certificate or publicly-signed server certificate in the identity policy.

```
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 s
```

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

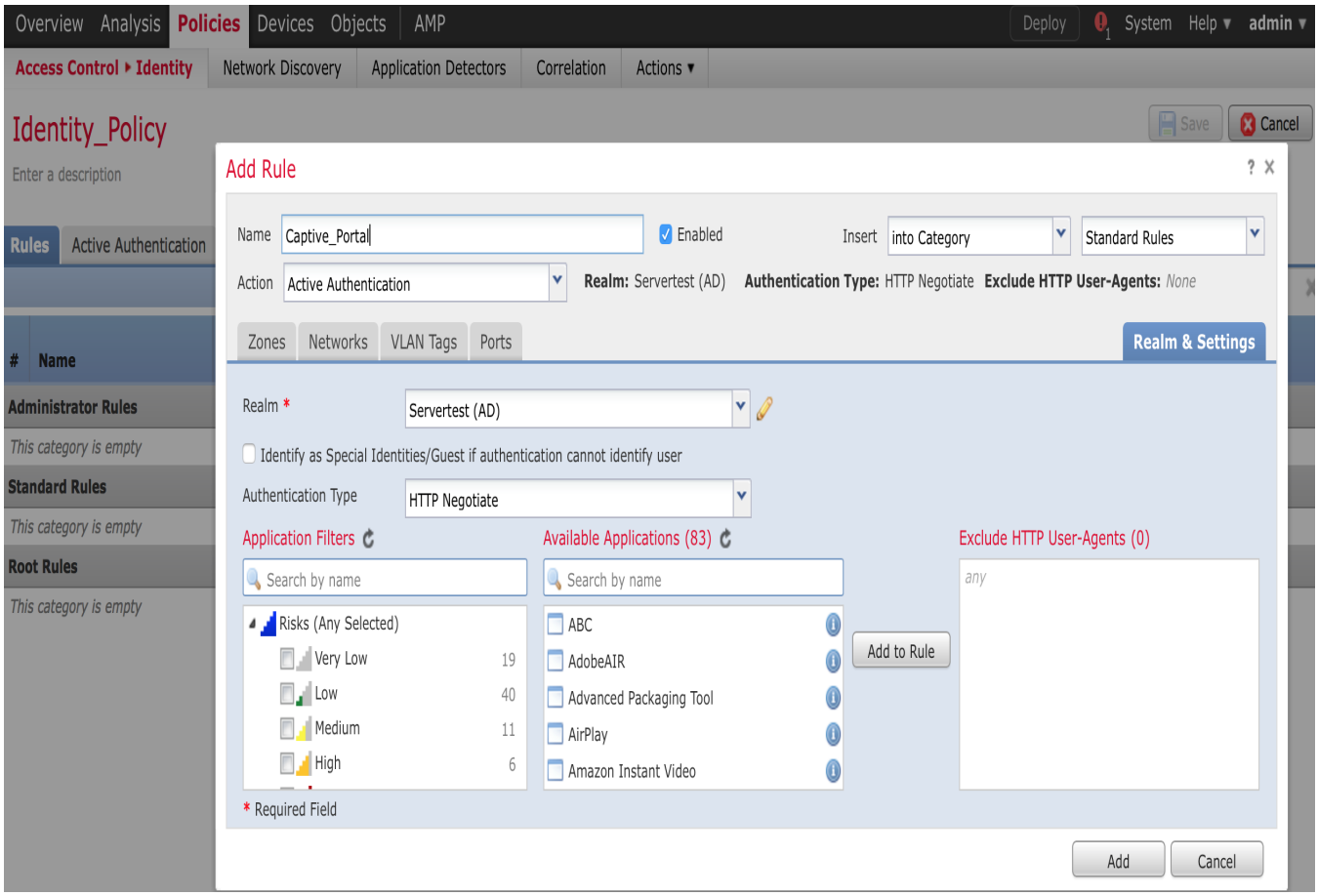


Now go to **Active Authentication** tab & in **Server Certificate** option, click on **icon (+)** and upload the certificate & private key which we generated in preivous step using openssl.



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 wan to enable the user authentication.

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



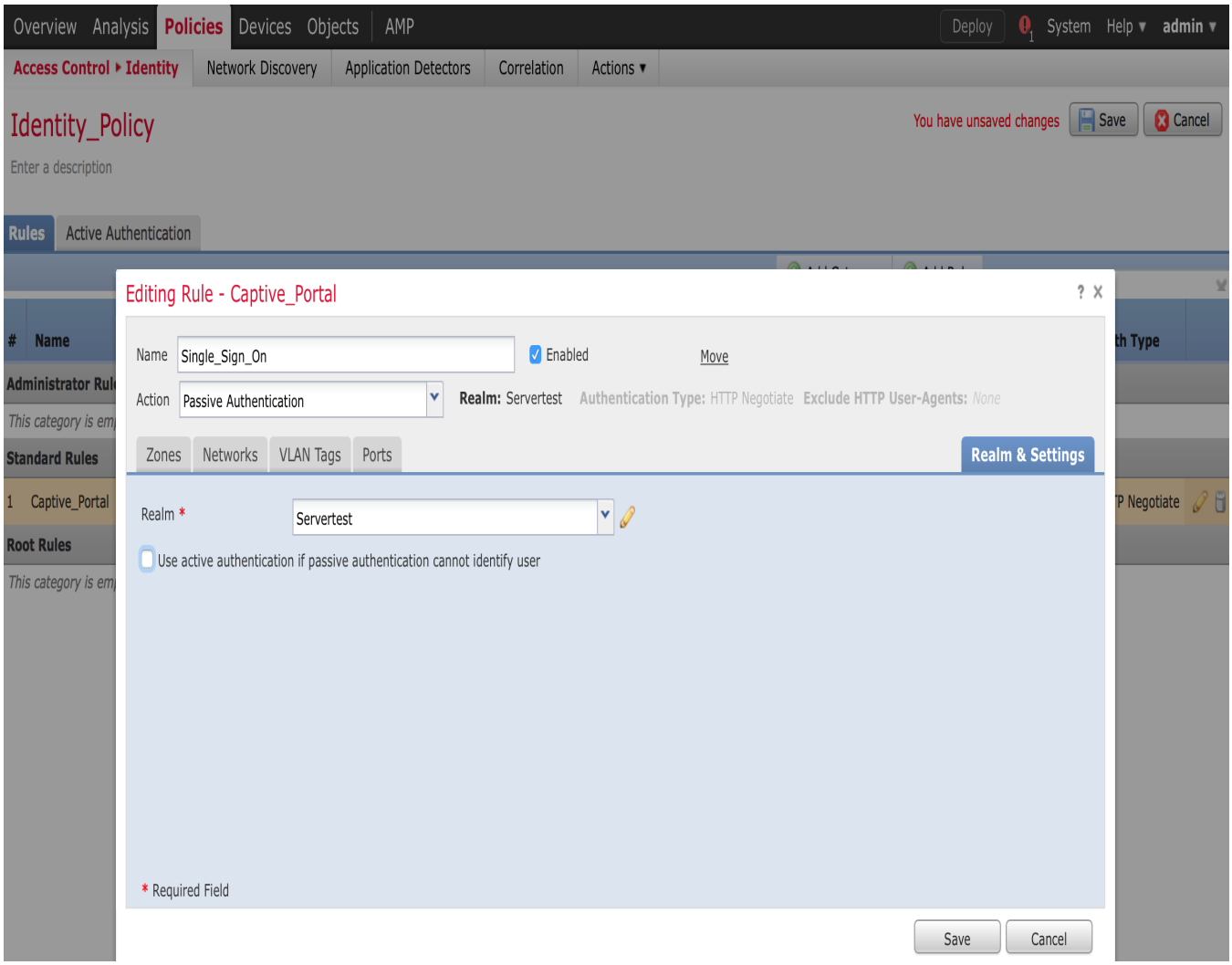
4.2 Single-Sign-On (Passive Authentication)

In passive authentication, When a domain user logins 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.

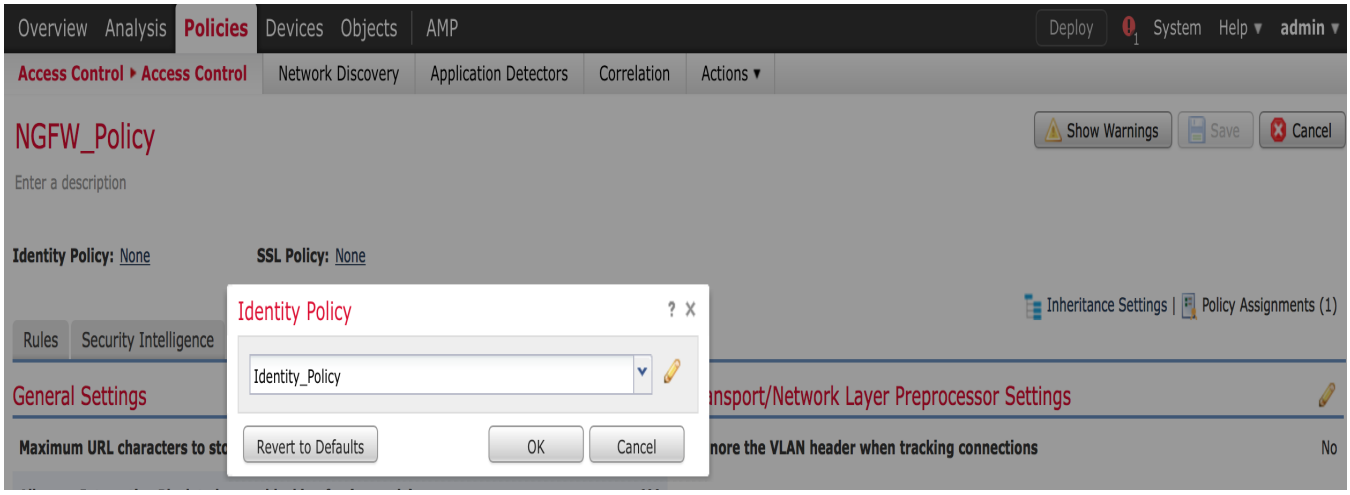
Here we can choose fall back method as **Active authentication if passive authentication cannot identify the user identity**.



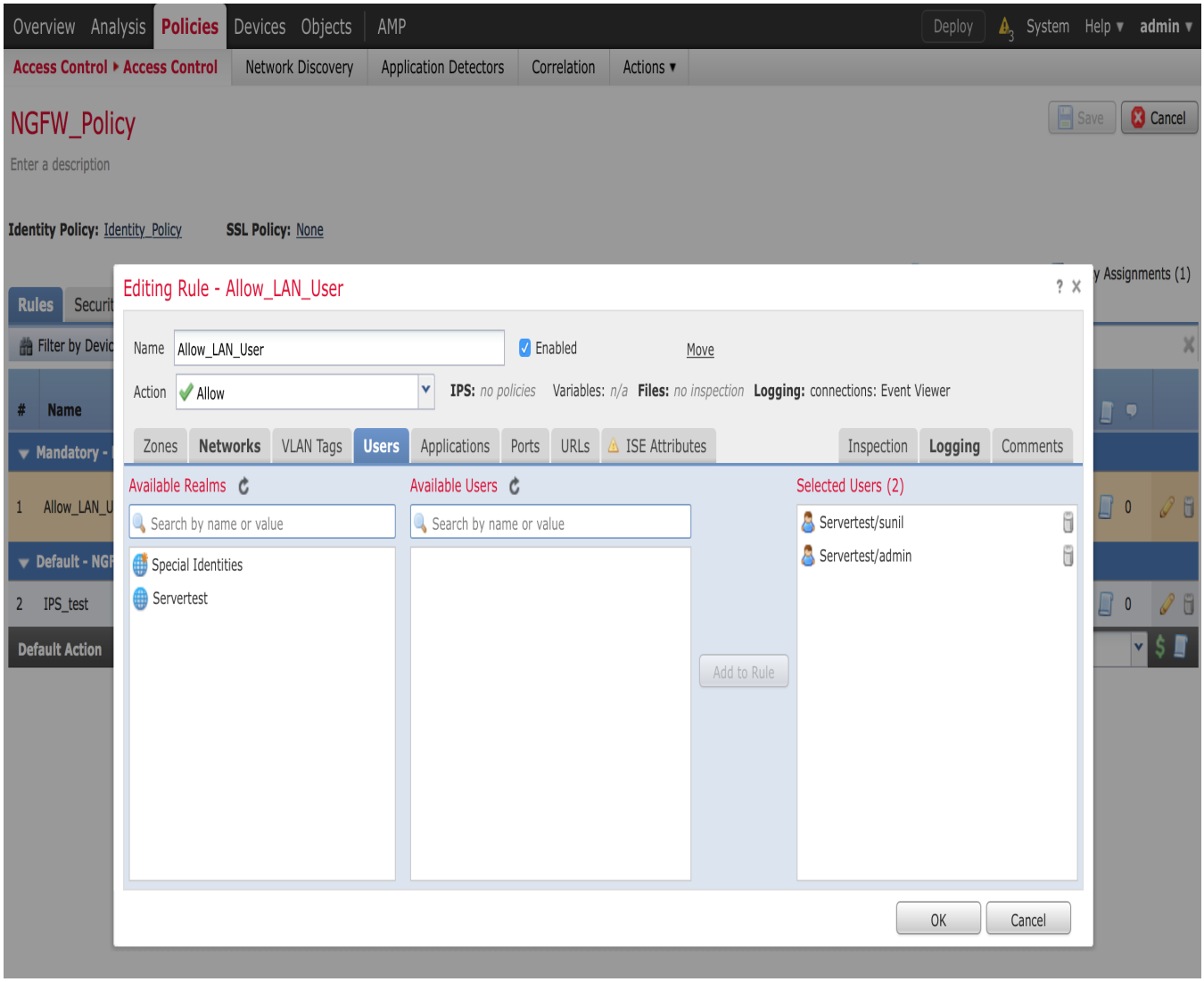
5. Configure the Access Control Policy

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.

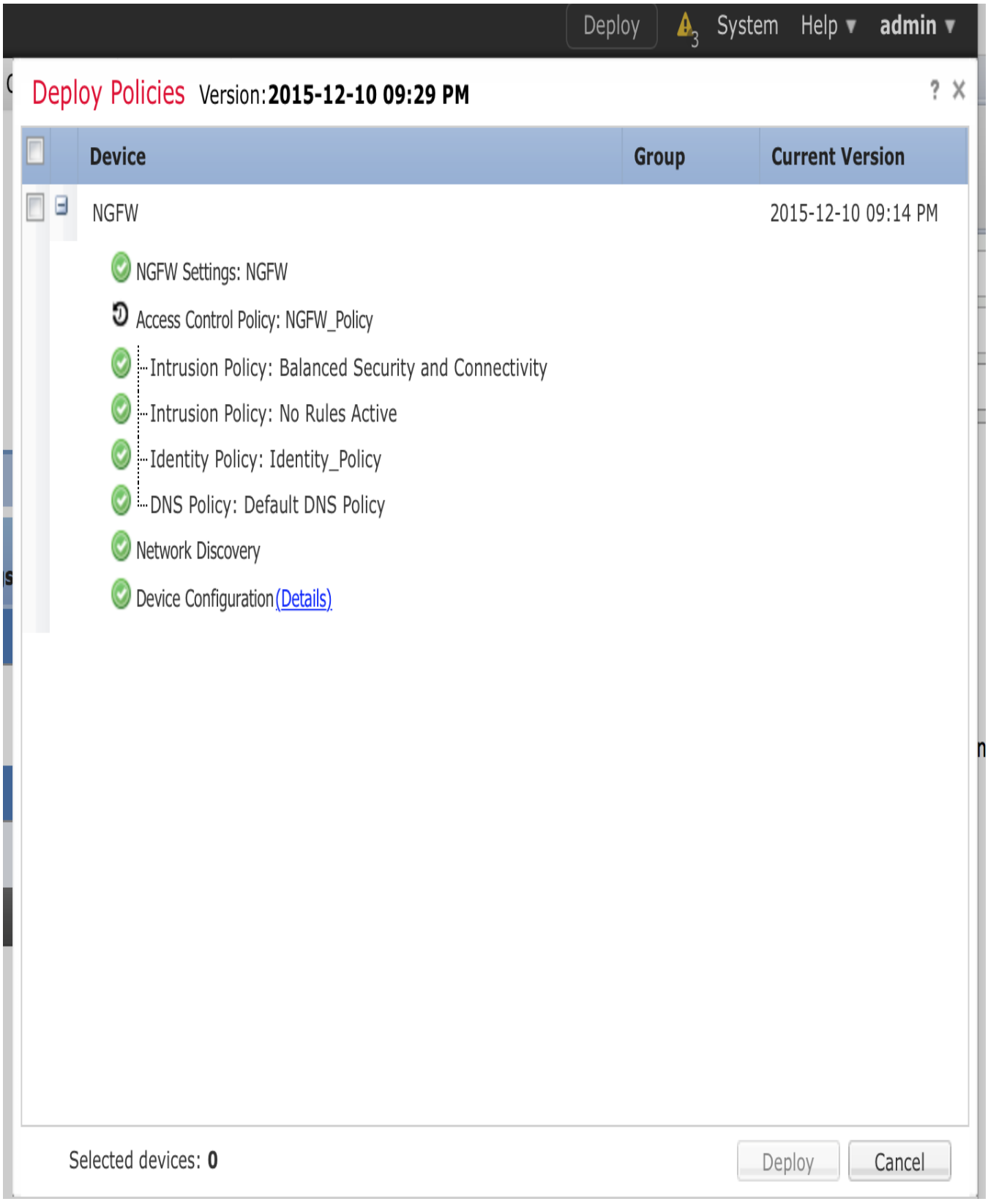


Click on **Add rule** button to add a new rule, go to **Users** and select the users for which access control rule will enforce. Click on **OK** button and click on **Save** button to save the changes.



6. Deploy the Access Control Policy

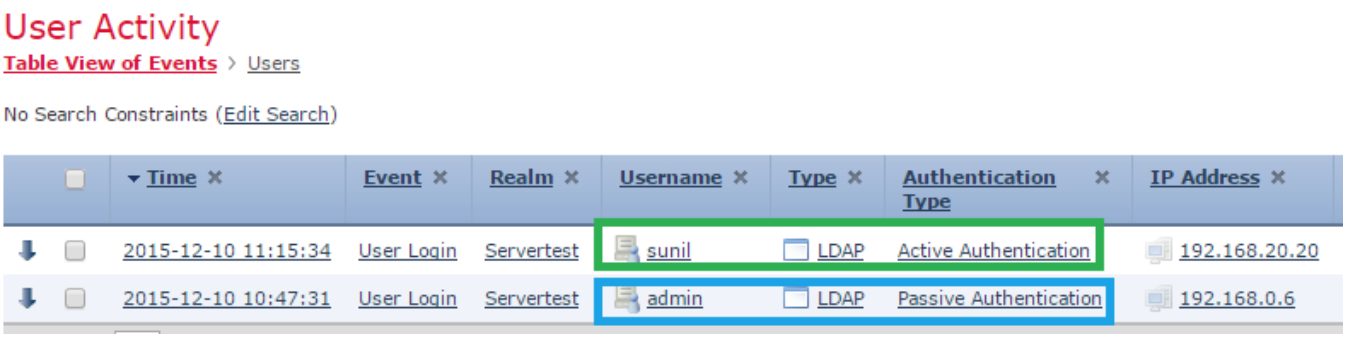
Navigate to **Depoly** option, choose the **Device** and click on **Depoly** option to push the configuration change to the sensor. Monitor the Deployment of policy from the **Message Center Icon (icon between Depoly and System option)** option and make sure, policy should apply successfully.



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)**



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