Configure Active Directory Integration with Firepower Appliance

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 the User Agent
- Step 3. IntegrateFirepower 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 the 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 andTroubleshoot

- 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 and Policy Deployment
- Analyze the Events Logs

Related Information

Introduction

This document describes how to configure 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, the appliance must be in routed mode.

Configure

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

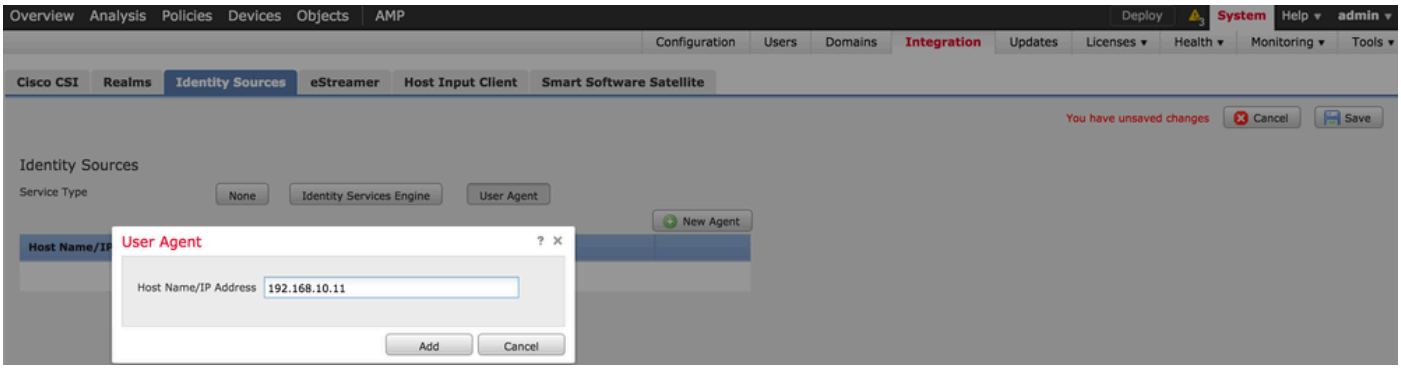
This article explains how to configure Firepower User Agent in a Windows machine:

Installation and Uninstallation of Sourcefire User Agent

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

Log in to Firepower Management Center, navigate to **System > Integration > Identity Sources**. Clickthe **New Agent** option. Configure the **IP address** of User Agent system and 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**. Clickthe **Add New Realm** option.

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

Type: AD

AD Primary Domain: Domain name of Active Directory

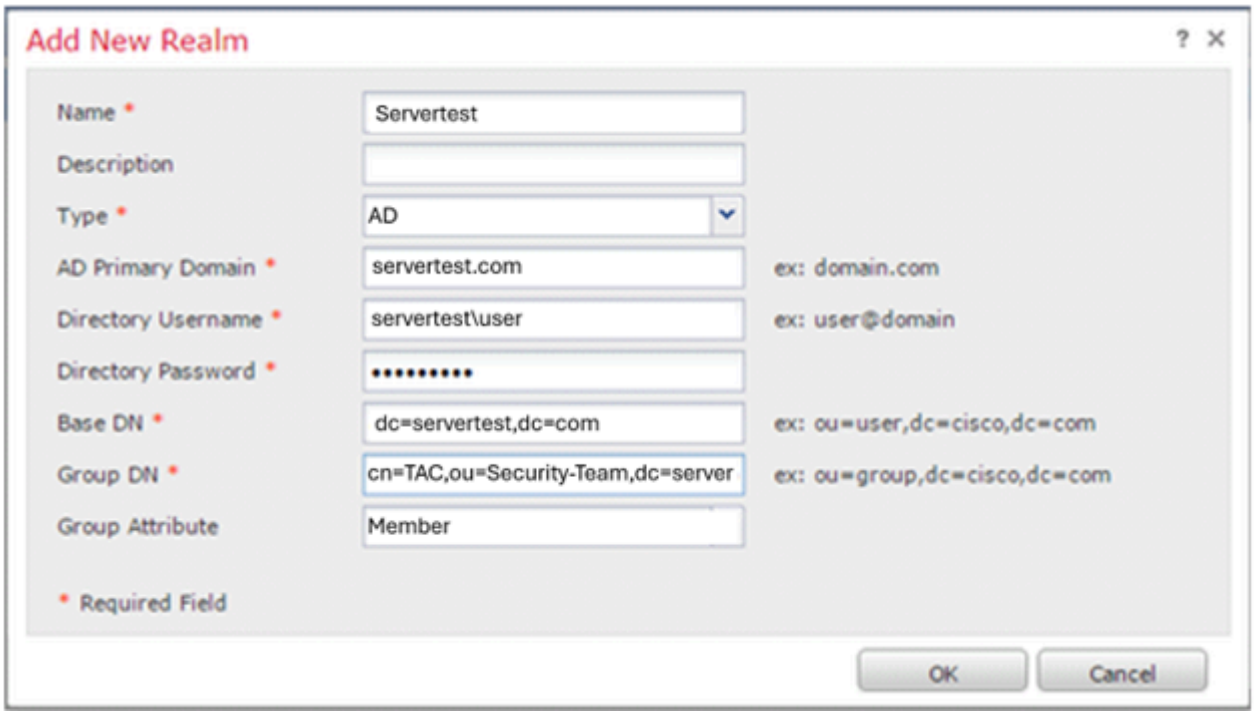
Directory Username: <username>

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



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

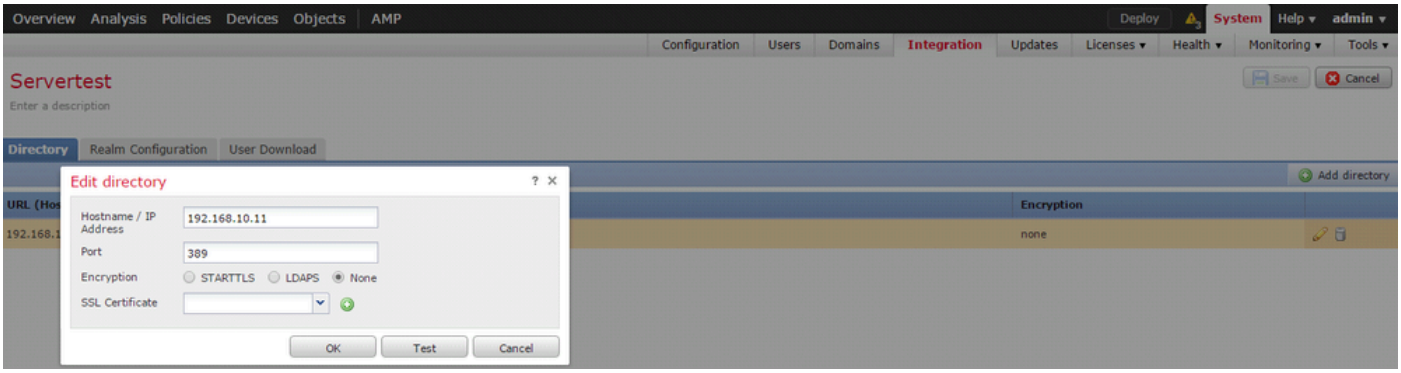
Click the **Add** button in order to navigate to next step and thereafter, click the **Add directory** option.

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

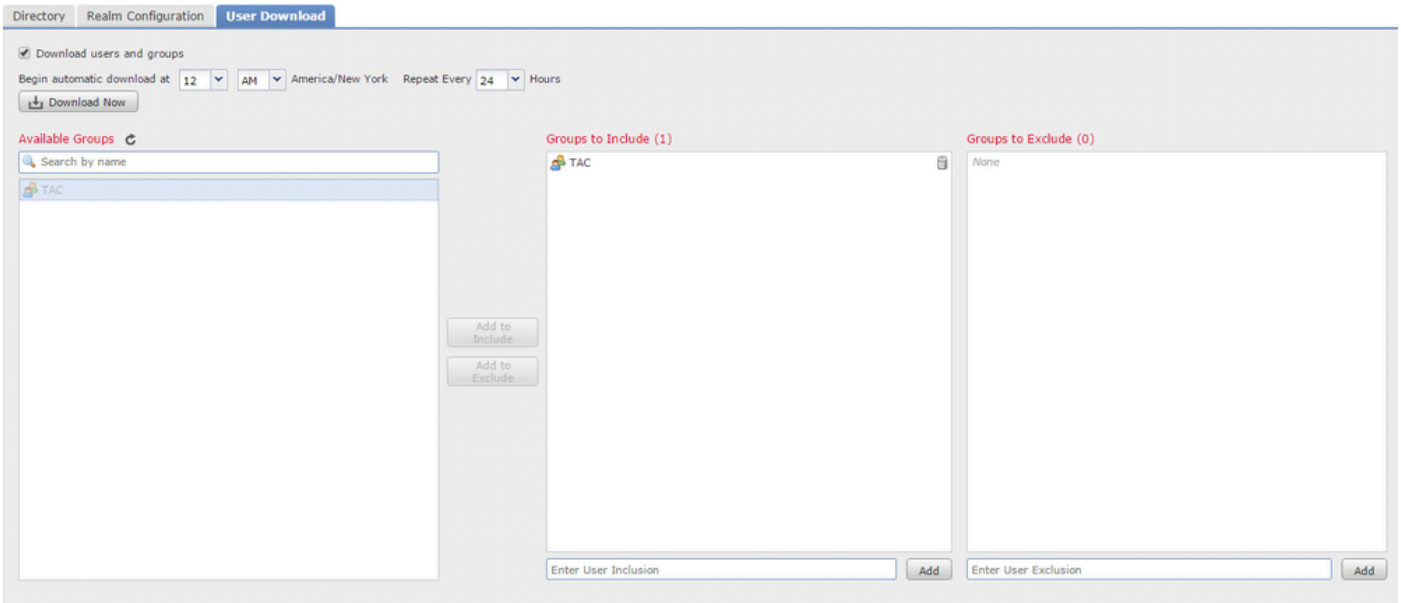
Navigate to **Realm Configuration** in order to verify integration configuration of AD server and you can modify the AD configuration.

Step 3.4 Download the User Database

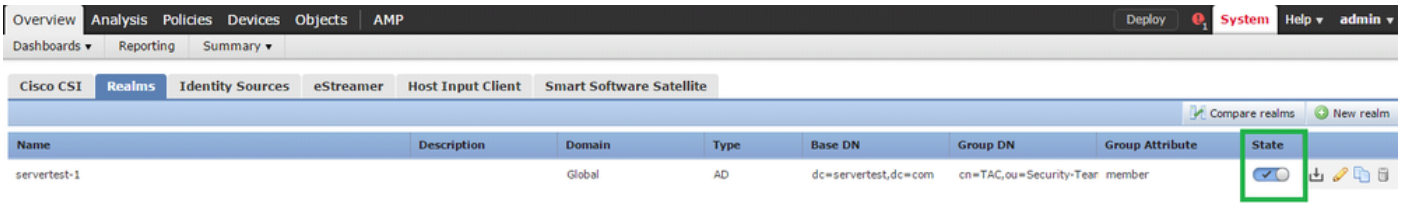
Navigate to **User Download** option to fetch the user database from the AD server.

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:



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. The 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.

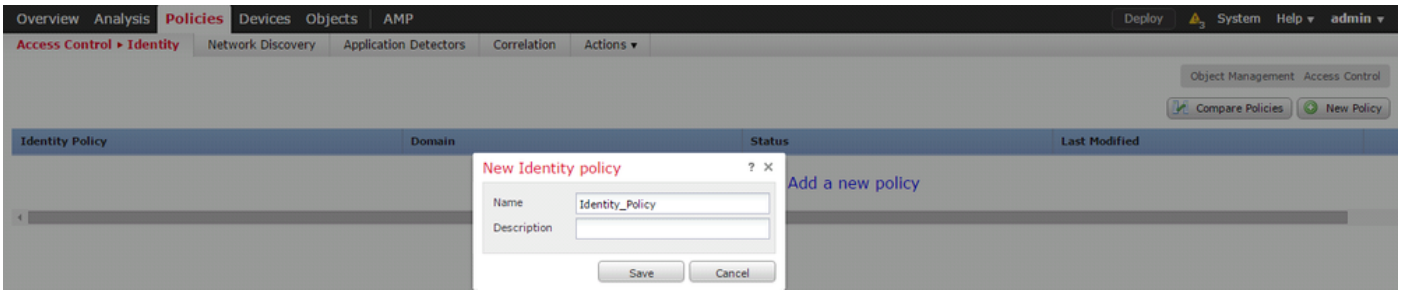
```
Generate a simple self-signed certificate using openSSL -

Step 1.   Generate the Private key
               openssl genrsa -des3 -out server.key 2048

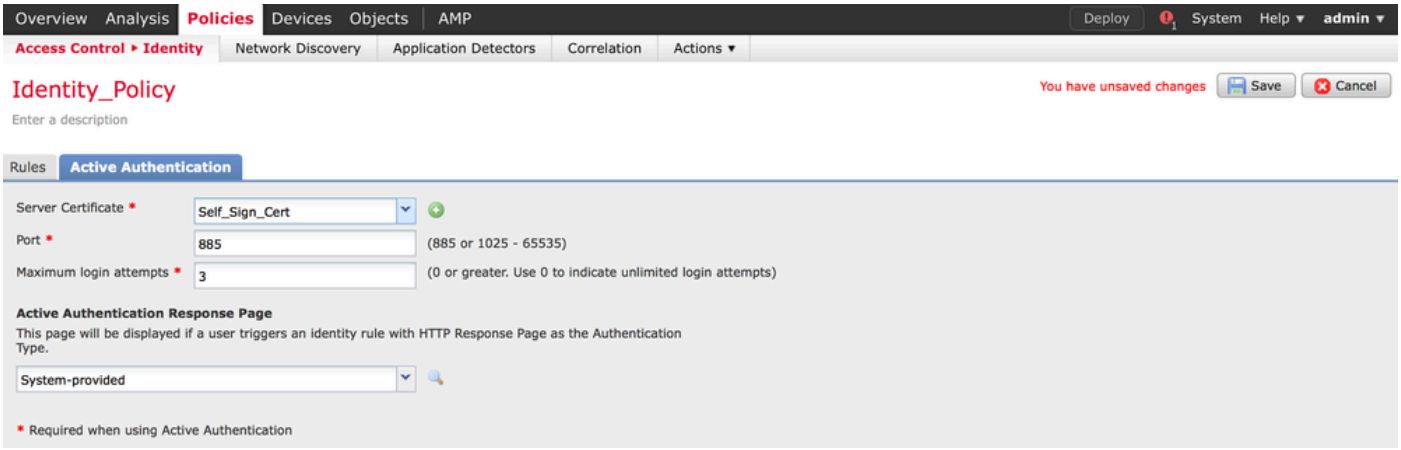
Step 2.   Generate Certificate Signing Request (CSR)
               openssl req -new -key server.key -out server.csr

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** and give a **name** to policy and **save** it.

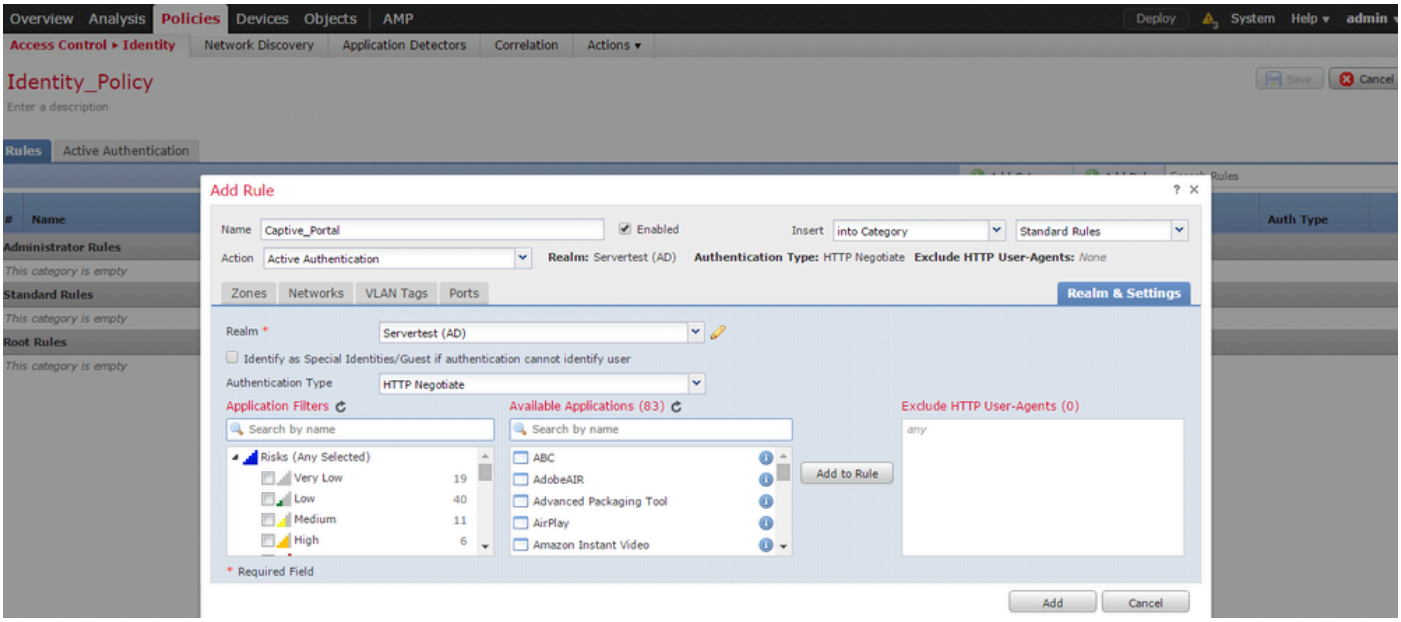


Navigate to **Active Authentication** tab and in the **Server Certificate** option, click the **icon (+)** and upload the **certificate** and **private key** which you generated in the previous step with openSSL.



Now, click the **Add rule** button and give a **name** to the Rule and 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.



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: The captive portal command is available in ASA version 9.5(2) and later.

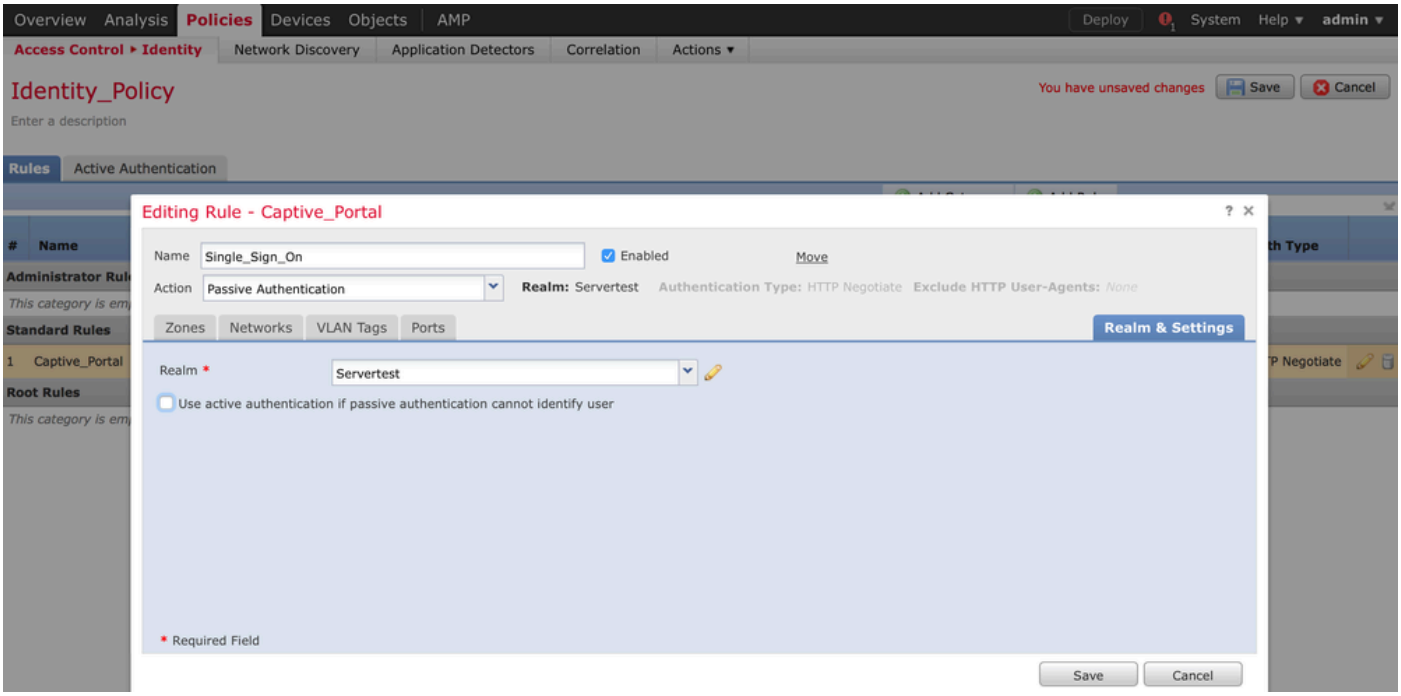
Step 4.2 Single-Sign-On (Passive Authentication)

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 and give a name to the Rule and 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 suites your environment, as shown in this image.

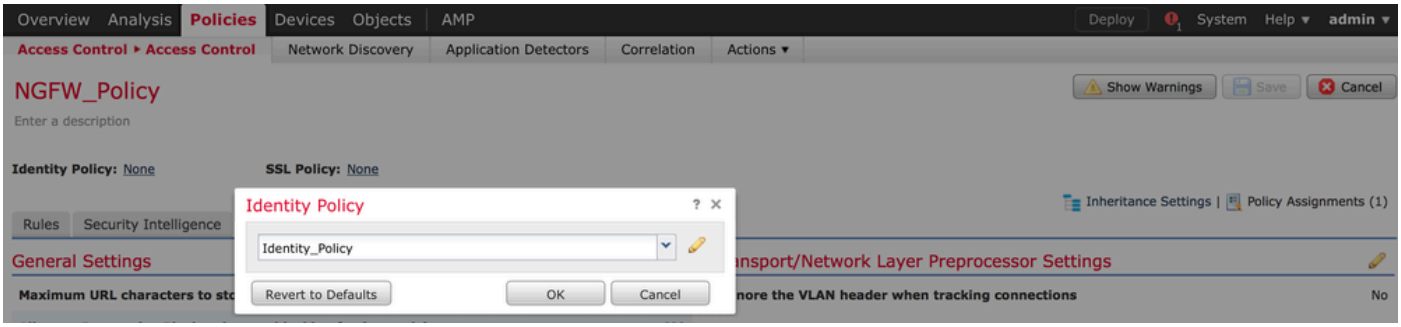
Here you can choose fallback method as **Active authentication if passive authentication cannot identify the user identity**.



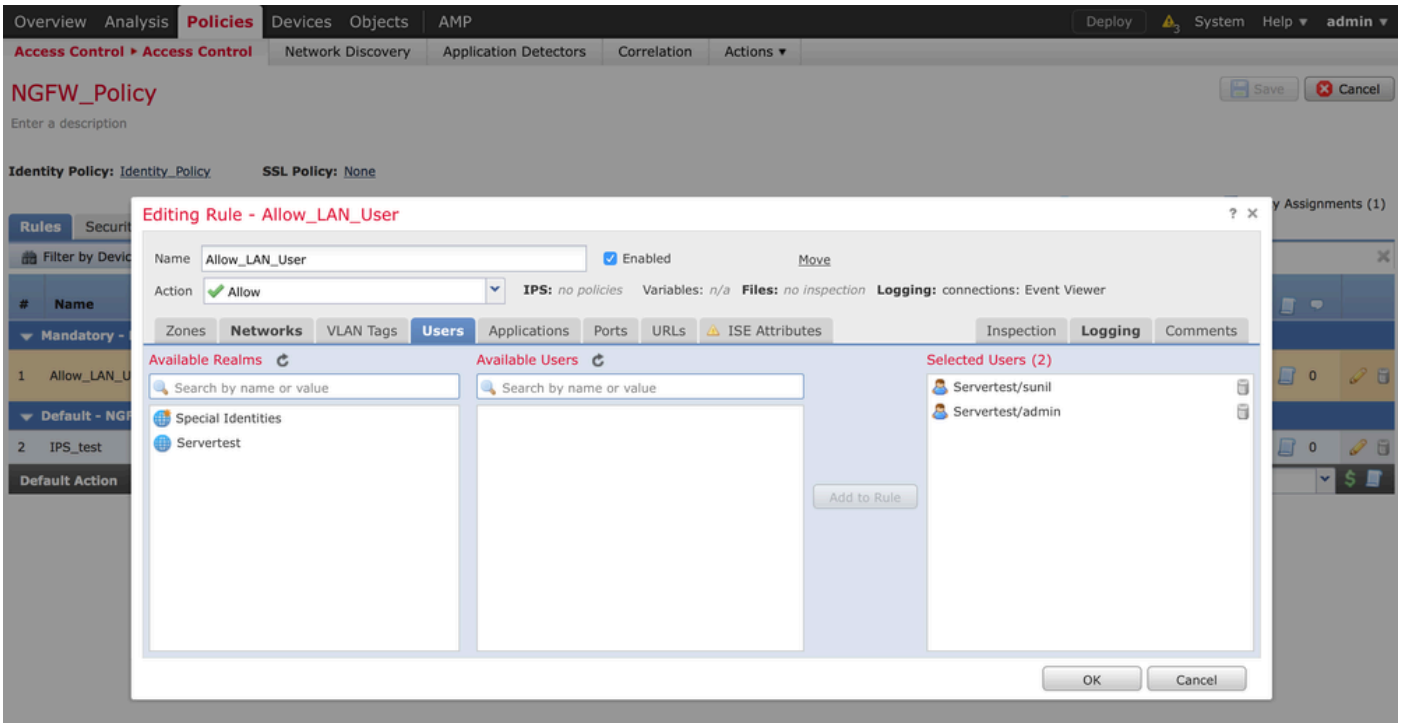
Step 5. Configure the Access Control Policy

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.

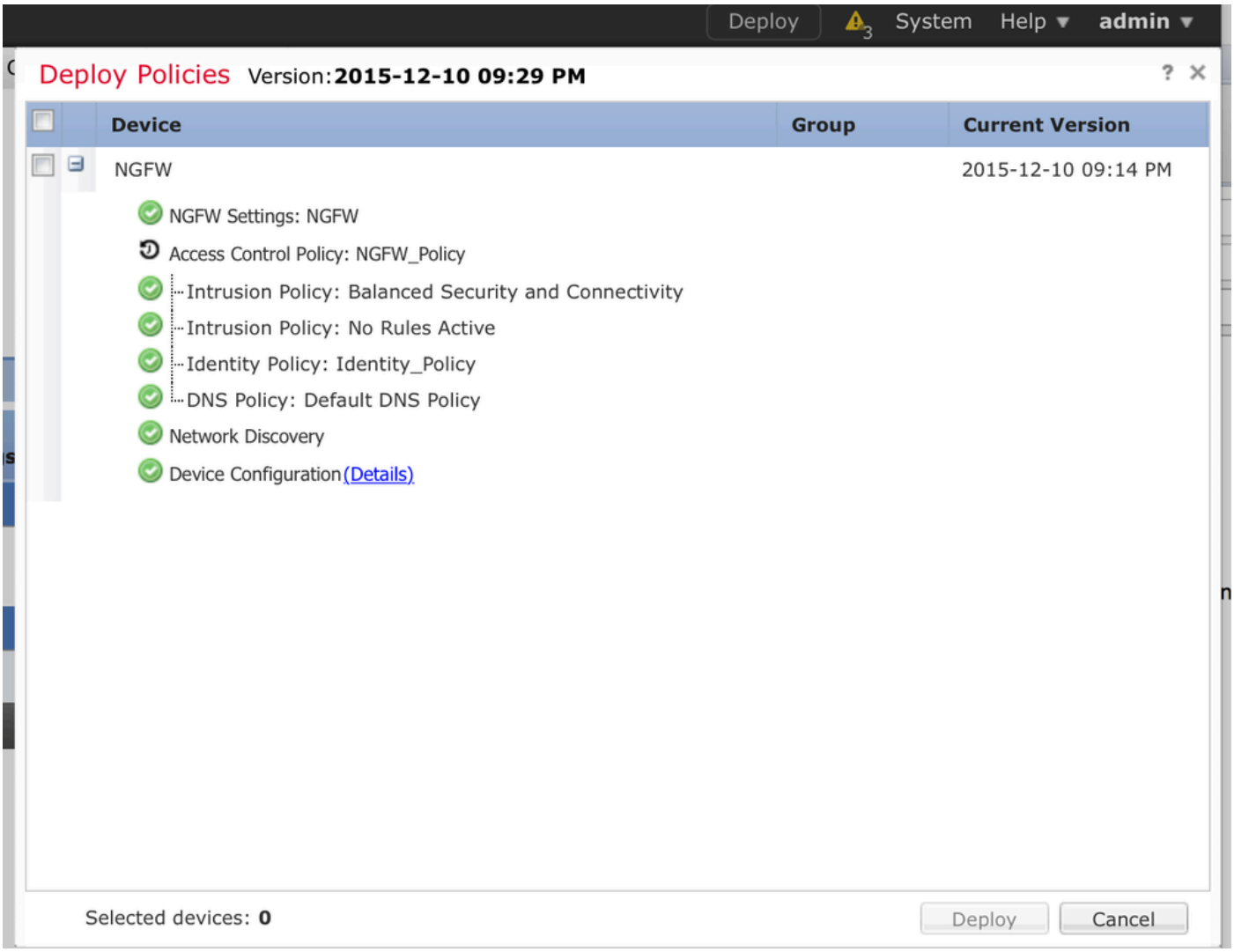


Click the **Add rule** button to add a new rule. Navigate to **Users** and select the **users** for which access control rule enforces, as shown in this image. Click **OK** and click **Save** in order to save the changes.



Step 6. Deploy the Access Control Policy

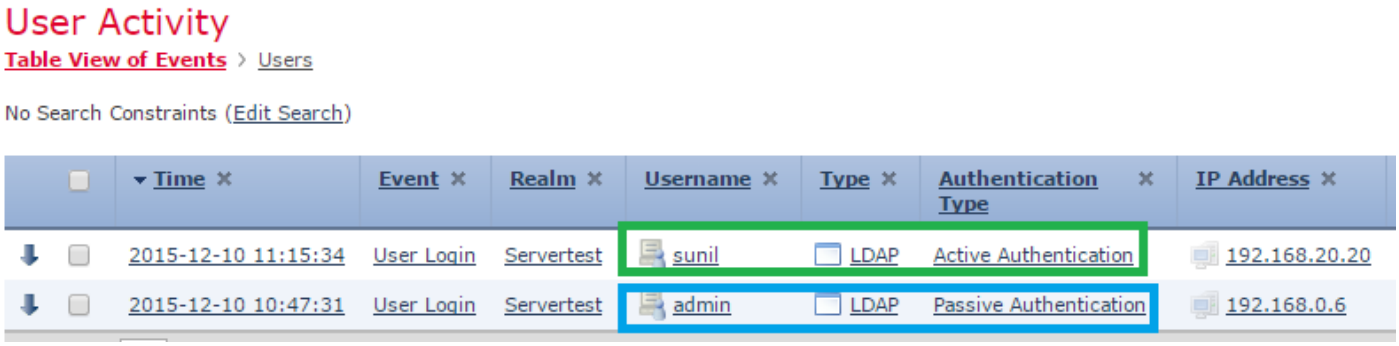
Navigate to **Deploy** option. Choose the **Device** and click the **Deploy** option to push the configuration change to the sensor. Monitor the Deployment of policy from the **Message Center Icon** (icon between Deploy and System option) option and ensure that policy must apply successfully, as shown in this image.



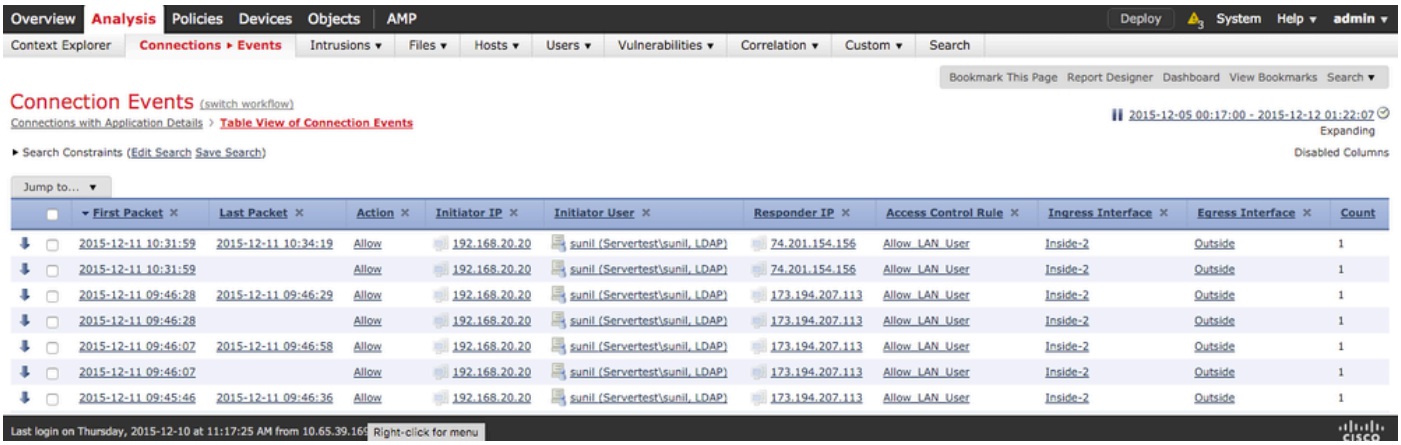
Step 7. Monitor User Events & Connections Events

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**.



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



Verify and Troubleshoot

Navigate to **Analysis > Users** in orderto 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.

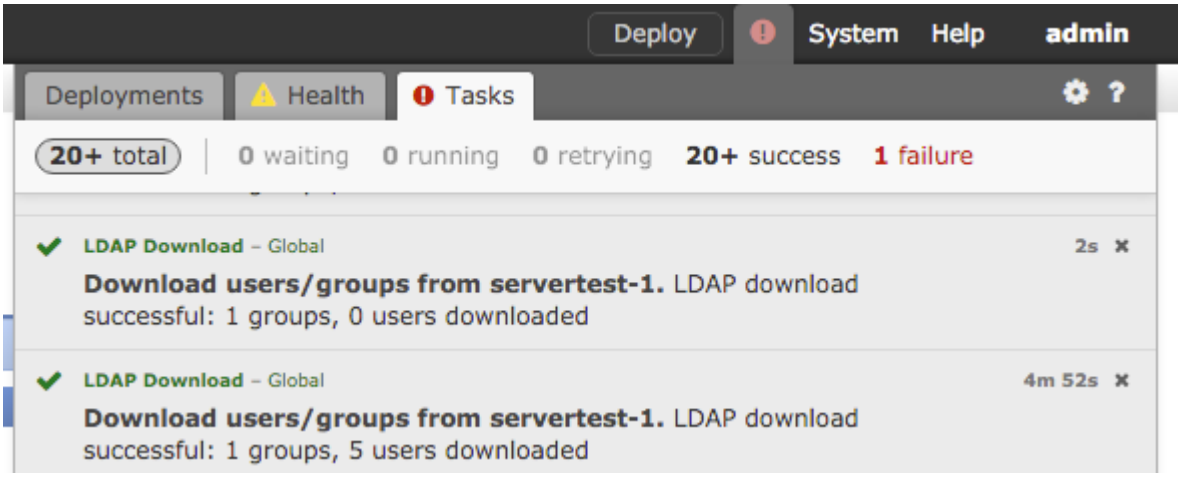
Run **packet capture** on the FMC to verify connectivity with the Active Directory.

```
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 the 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 and 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.

Analyze 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 and Documentation