Configure ISE 2.3 Facebook Social Media for Guest Portals

Contents

Introduction
Prerequisites
Requirements
Components Used
Network Diagram
Configuration
1. Configure Facebook App
2. Integrate ISE with the Facebook app
3. Configure Authentication and Authorization policies
Verify
Troubleshoot
Debugs on ISE

Introduction

This document describes how to configure Cisco Identity Services Engine (ISE) 2.3 integration with Facebook credentials for authenticated guest access.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Identity Services Engine (ISE) configuration
- Basic Facebook App configuration

Components Used

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

- Cisco ISE Version 2.3
- Facebook Social Login
- Cisco Wireless LAN Controller (WLC) Version 8.3.102.0

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, make sure that you understand the potential impact of any command.

Network Diagram
Configuration

The Facebook app configuration presented is an example and not a Cisco recommended configuration.

1. Configure Facebook App

Go to https://developers.facebook.com, and register the new App.

The dashboard of the application shows App ID and App Secret key, which will be used on ISE to create the External Social login.
Make the created app public.

2. Integrate ISE with the Facebook app

Use the information mentioned below in order to integrate the Facebook App with Cisco ISE.

Navigate to Administration > Identity Management > External Identity Sources > Social Login and add new store.
Configure the ISE Guest Portal to Allow social login.
After configuring the ISE Guest Portal to allow social login, the social login will be populated with URLs and needs to be added to the Facebook App settings, **Valid OAuth redirect URLs**.
Add Facebook Login from Products and add Valid OAuth redirect URLs.

URLs will be automatically generated on ISE after successfully binding the ISE Portal with Facebook External Social login.
3. Configure Authentication and Authorization policies

The ISE Configuration follows the same configuration steps as Guest CWA (Central Web Authentication).

(For configuration steps on ISE CWA please refer to document below:

Make sure that the Facebook ip address range (31.13.0.0/16) is excluded from the WLC redirect ACL.

Verify

Once the guest user is redirected they are presented with the Log in With Facebook option.
This button takes advantage of the newly created application and redirects to the Facebook login page where the user will enter their Facebook credentials.

After successful authentication, the guest user redirects back to the ISE Portal.
ISE Radius Live Logs:
## Troubleshoot

### Overview

<table>
<thead>
<tr>
<th>Event</th>
<th>5236 Authorize-Only succeeded</th>
</tr>
</thead>
<tbody>
<tr>
<td>Username</td>
<td>Ulugbek Yusubaliev</td>
</tr>
<tr>
<td>Endpoint Id</td>
<td>E4.A4.71.85.FB.6A</td>
</tr>
<tr>
<td>Endpoint Profile</td>
<td>Windows10-Workstation</td>
</tr>
<tr>
<td>Authentication Policy</td>
<td>Default</td>
</tr>
<tr>
<td>Authorization Policy</td>
<td>Default &gt;&gt;&gt; Wi-Fi_Guest_Access</td>
</tr>
<tr>
<td>Authorization Result</td>
<td>Guests_PermitAccess</td>
</tr>
</tbody>
</table>

### Authentication Details

<table>
<thead>
<tr>
<th>Source Timestamp</th>
<th>2017-08-21 10:04:06.395</th>
</tr>
</thead>
<tbody>
<tr>
<td>Received Timestamp</td>
<td>2017-08-21 10:04:06.397</td>
</tr>
<tr>
<td>Policy Server</td>
<td>ISE23</td>
</tr>
<tr>
<td>Event</td>
<td>5236 Authorize-Only succeeded</td>
</tr>
<tr>
<td>Username</td>
<td>Ulugbek Yusubaliev</td>
</tr>
<tr>
<td>User Type</td>
<td>GuestUser</td>
</tr>
<tr>
<td>Endpoint Id</td>
<td>E4.A4.71.85.FB.6A</td>
</tr>
<tr>
<td>Calling Station Id</td>
<td>e4-a4.71-85-fb-6a</td>
</tr>
<tr>
<td>Endpoint Profile</td>
<td>Windows10-Workstation</td>
</tr>
<tr>
<td>Authentication Identity Store</td>
<td>FacebookApp</td>
</tr>
<tr>
<td>Identity Group</td>
<td>GuestEndpoints</td>
</tr>
<tr>
<td>Audit Session Id</td>
<td>0e249a050000007599af5b2</td>
</tr>
<tr>
<td>Authentication Method</td>
<td>Authorize Only</td>
</tr>
<tr>
<td>Service Type</td>
<td>Authorize Only</td>
</tr>
<tr>
<td>Network Device</td>
<td>WLC</td>
</tr>
</tbody>
</table>
Debugs on ISE

In order to enable debugs on ISE, navigate to Administration > System > Logging > Debug Log Configuration, select the PSN node and change the log level of the following components to DEBUG:

Logs to be checked - ise-psc.log and guest.log. You can tail them directly from CLI of ISE:

```
ise23-1/admin# show logging application ise-psc.log tail
```

During the connection to the Facebook App, ISE shows connection timed out error:

```
2017-08-21 08:28:18,003 DEBUG  [admin-http-pool22][] com.cisco.cpm.oauth.OAuthClient -:::- Got error while checking OAuth settings for AppId: [123456789] and secret key: ****
2017-08-21 08:28:18,003 ERROR  [admin-http-pool22][] admin.restui.features.social.SocialLoginUIApi -:::- ERROR connect timed out
```

Make sure the ISE Node has a direct internet connection.

Using proxy addressed on Bug CSCve87511 "Social Login support with proxy server"