# Configure ISE 2.3 Facebook Social Media for Guest Portals

## Contents

## 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
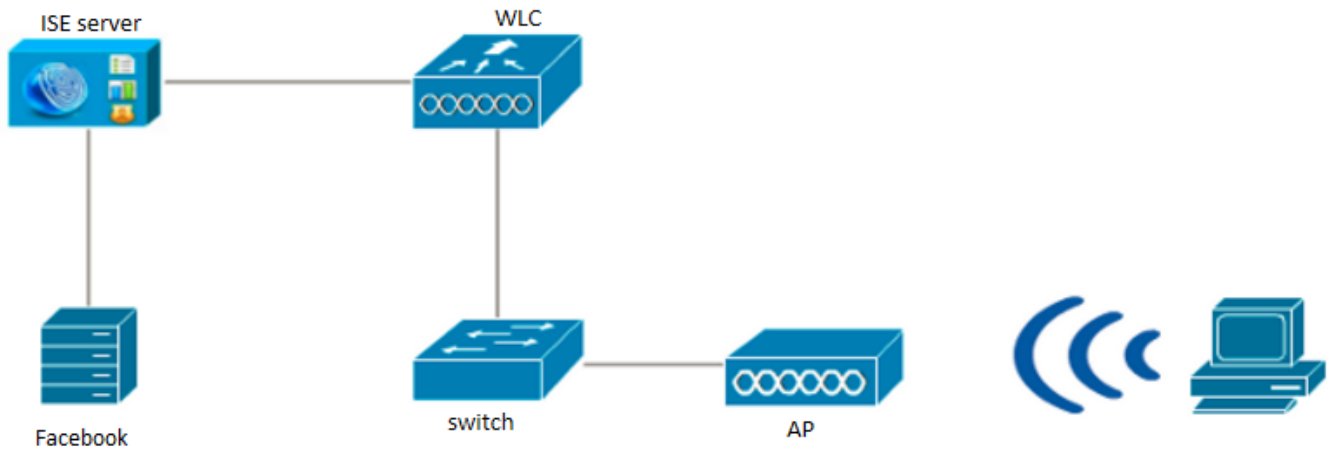- Basic Facebook App configuration

### 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.
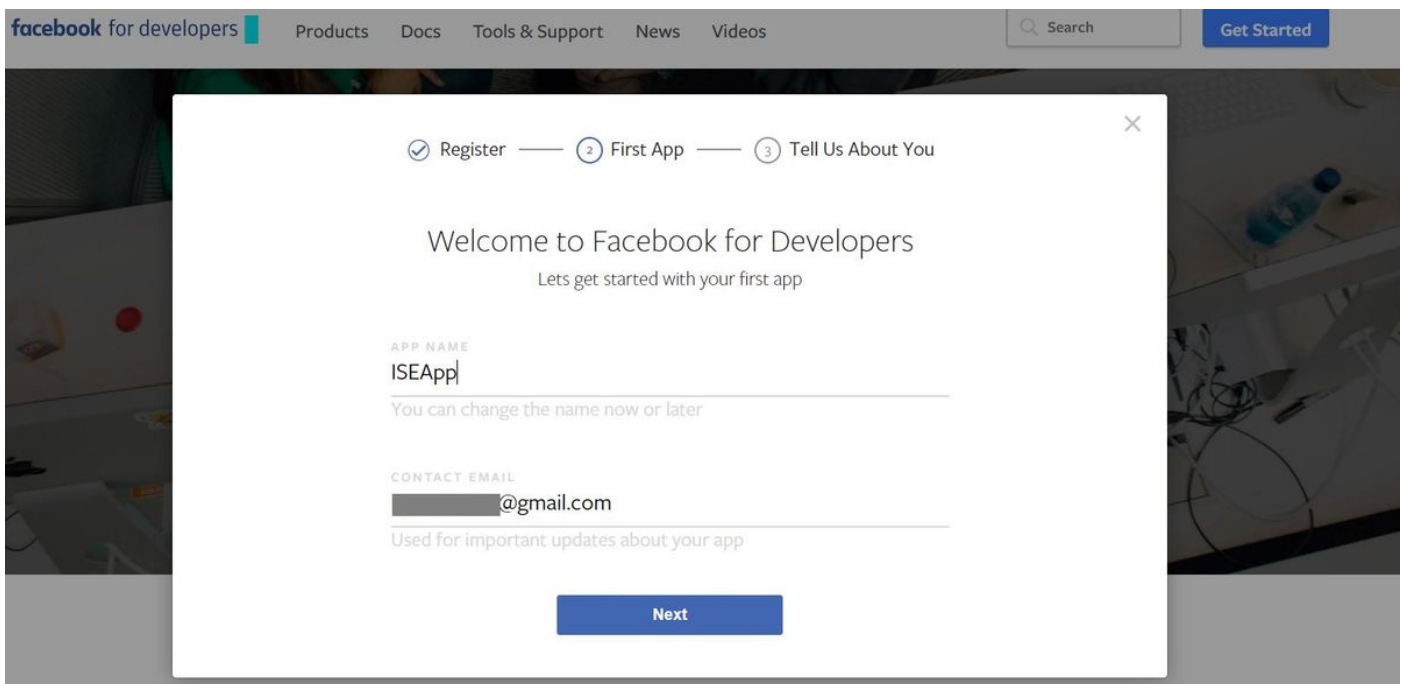
### Network Diagram

# 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.

cisco Identity Services Engine   Home   ▸ Context Visibility   ▸ Operations   ▸ Policy   ▾ Administration   ▸ Work Centers

▸ System   ▾ Identity Management   ▸ Network Resources   ▸ Device Portal Management   pxGrid Services   ▸ Feed Service   ▸ Threat Centric NAC

▸ Identities   Groups   External Identity Sources   Identity Source Sequences   ▸ Settings

**External Identity Sources**

- ▸ Certificate Authentication Profile
- ▾ Active Directory
  - AD
- LDAP
- ODBC
- RADIUS Token
- RSA SecurID
- SAML Id Providers
- Social Login

Social Login > New

**Social Login**

| | |
|---|---|
| Name * | FacebookApp |
| Description | |
| Type * | Facebook |
| App ID * | 62096▨▨▨▨ |
| App Secret * | ••••••••••••••••••••••••••••••••••   Show |

Cancel   Submit

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.
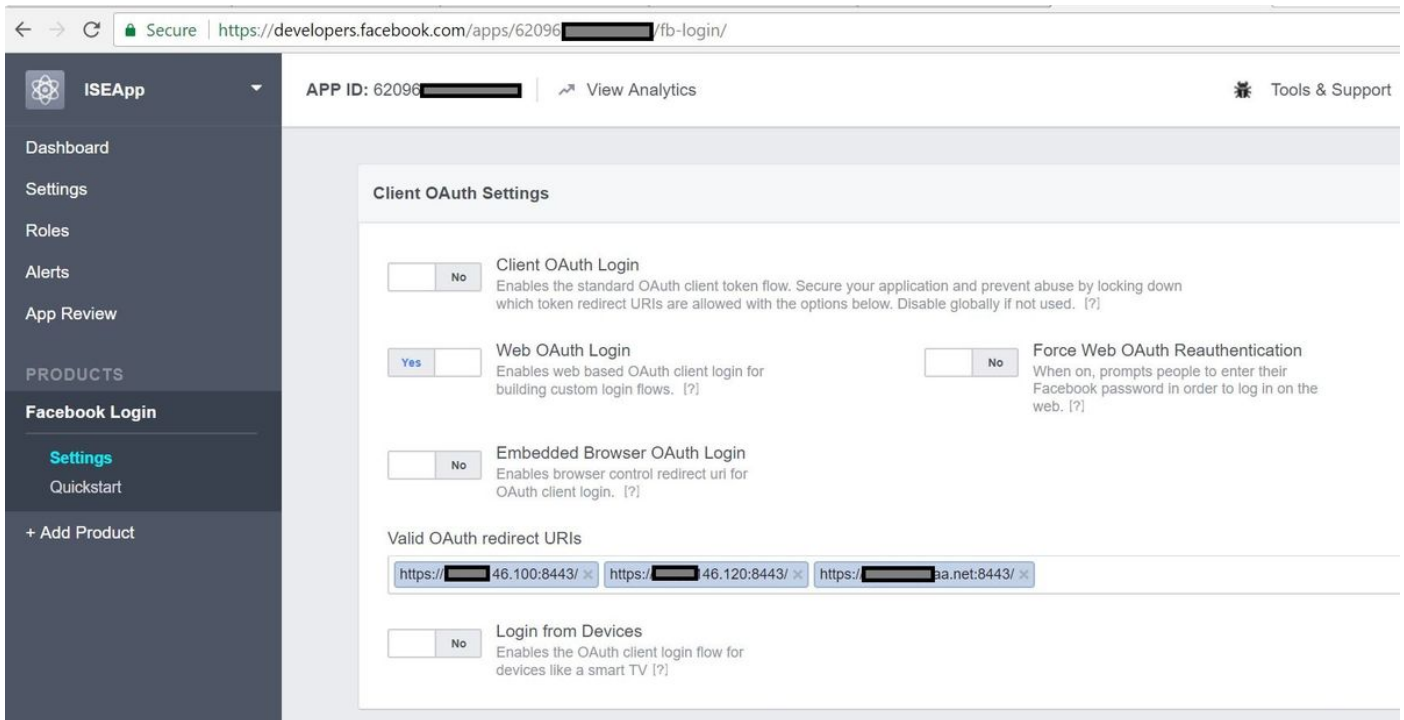
# 3. Configure Authentication and Authorization policies

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:

https://www.cisco.com/c/en/us/support/docs/security/identity-services-engine/115732-central-web-auth-00.html )

Policy Sets   Profiling   Posture   Client Provisioning   ▸ Policy Elements

| | Status | | | | | All_User_ID_Stores | × ▾ | 0 | ⚙ |
|---|---|---|---|---|---|---|---|---|---|
| | ⊘ | Default | | | | ❯ Options | | | |

❯ Authorization Policy - Local Exceptions

❯ Authorization Policy - Global Exceptions

❮ Authorization Policy (12)

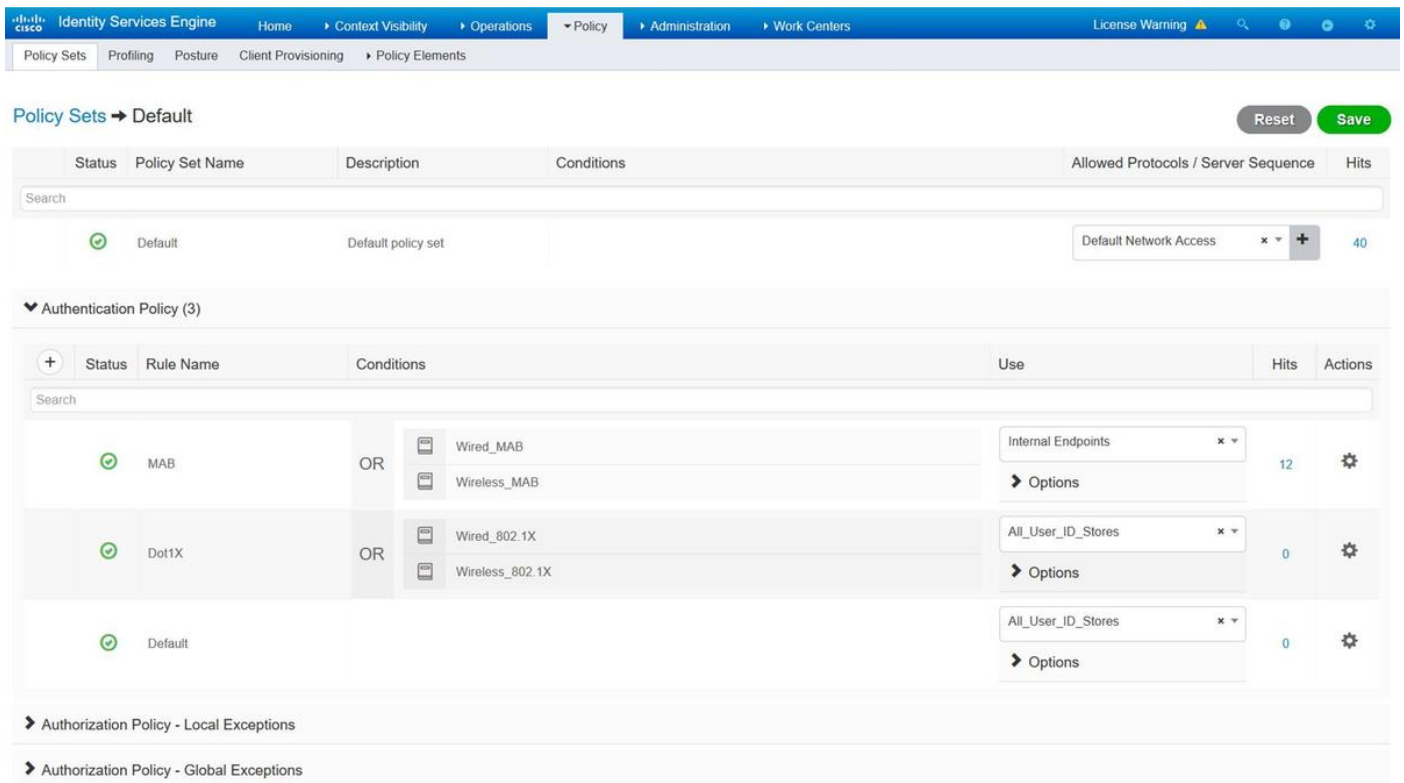| + | Status | Rule Name | Conditions | | Results Profiles | Security Groups | | | Hits | Actions |
|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | | | |
| ✎ | ⊘ | Wi-Fi_Guest_Access | AND | 🖥 Guest_Flow  🖥 Wireless_MAB | ×PermitAccess + | Guests | × ▾ + | | 5 | ⚙ |
| ✎ | ⊘ | Wi-Fi_Redirect_to_Guest_Login | | 🖥 Wireless_MAB | ×Cisco_WebAuth_Wireless + | Select from list | ▾ + | | 12 | ⚙ |

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

**Security**

Access Control Lists > Edit     < Back    Add

▾ AAA
  General
  ▾ RADIUS
    Authentication
    Accounting
    Fallback
    DNS
    Downloaded AVP
  ▸ TACACS+
  LDAP
  Local Net Users
  MAC Filtering
  ▾ Disabled Clients
  User Login Policies
  AP Policies
  Password Policies

▸ Local EAP

  Advanced EAP

▸ Priority Order

▸ Certificate

▾ Access Control Lists
  Access Control Lists
  CPU Access Control Lists
  FlexConnect ACLs
  Layer2 ACLs

▸ Wireless Protection Policies

▸ Web Auth

  TrustSec SXP

  Local Policies

▸ Advanced

**General**

Access List Name        Redirect-ACL

Deny Counters           0

| Seq | Action | Source IP/Mask | Destination IP/Mask | Protocol | Source Port | Dest Port | DSCP | Direction | Number of Hits | |
|---|---|---|---|---|---|---|---|---|---|---|
| 1 | Permit | 0.0.0.0 / 0.0.0.0 | 0.0.0.0 / 0.0.0.0 | UDP | Any | Any | Any | Any | 2391 | ▾ |
| 2 | Permit | 0.0.0.0 / 0.0.0.0 | 0.0.0.0 / 0.0.0.0 | ICMP | Any | Any | Any | Any | 161 | ▾ |
| 3 | Permit | 0.0.0.0 / 0.0.0.0 | ▬0.0 / 255.255.0.0 | Any | Any | Any | Any | Any | 1360 | ▾ |
| 4 | Permit | ▬0.0 / 255.255.0.0 | 0.0.0.0 / 0.0.0.0 | Any | Any | Any | Any | Any | 1884 | ▾ |
| 5 | Permit | 0.0.0.0 / 0.0.0.0 | 31.13.0.0 / 255.255.0.0 | Any | Any | Any | Any | Any | 708 | ▾ |
| 6 | Permit | 31.13.0.0 / 255.255.0.0 | 0.0.0.0 / 0.0.0.0 | Any | Any | Any | Any | Any | 844 | ▾ |
| 7 | Deny | 0.0.0.0 / 0.0.0.0 | 0.0.0.0 / 0.0.0.0 | Any | Any | Any | Any | Any | 7424 | ▾ |

# 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.

**Welcome Message**

Click **Continue** to connect to the network.

You're very close to gaining network access.

Continue

ISE Radius Live Logs:



| Time | Status | Details | Repeat ... | Identity | Endpoint ID | Posture St... | Endpoint Profile | Authenticat... | Authorization Policy |
|---|---|---|---|---|---|---|---|---|---|
| | | | | Identity | Endpoint ID | Posture Status | Endpoint Profile | Authentication | Authorization Policy |
| Aug 21, 2017 10:04:06.404 AM | | | 0 | Ulugbek Yusubaliev | E4:A4:71:85:FB:6A | | Windows10-Workstation | Default | Default >> Wi-Fi_Guest_Ac |
| Aug 21, 2017 10:04:06.397 AM | | | | Ulugbek Yusubaliev | E4:A4:71:85:FB:6A | | Windows10-Workstation | Default | Default >> Wi-Fi_Guest_Ac |
| Aug 21, 2017 10:04:06.385 AM | | | | | E4:A4:71:85:FB:6A | | | | |
| Aug 21, 2017 10:04:05.766 AM | | | | Ulugbek Yusubaliev | E4:A4:71:85:FB:6A | | | | |
| Aug 21, 2017 10:01:07.080 AM | | | | E4:A4:71:85:FB:6A | E4:A4:71:85:FB:6A | | Intel-Device | Default >> M... | Default >> Wi-Fi_Redirect_ |
| Aug 21, 2017 09:59:59.321 AM | | | | E4:A4:71:85:FB:6A | E4:A4:71:85:FB:6A | | Intel-Device | Default >> M... | Default >> Wi-Fi_Redirect_ |
| Aug 21, 2017 09:59:59.302 AM | | | | | E4:A4:71:85:FB:6A | | | | |
| Aug 21, 2017 09:59:49.261 AM | | | | E4:A4:71:85:FB:6A | E4:A4:71:85:FB:6A | | | Default >> M... | Default >> Wi-Fi_Redirect_ |

## Identity Services Engine

### Overview

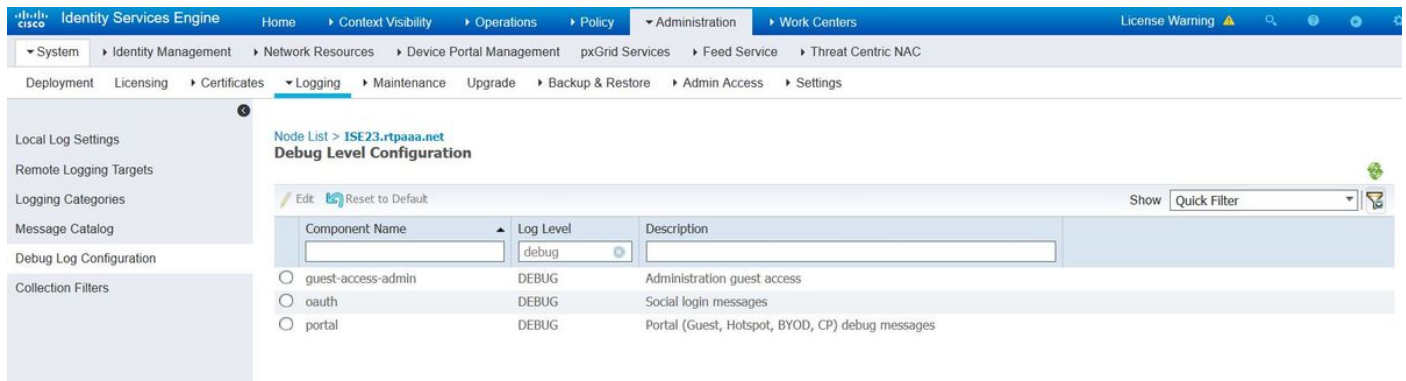| | |
|---|---|
| Event | 5236 Authorize-Only succeeded |
| Username | Ulugbek Yusubaliev |
| Endpoint Id | E4:A4:71:85:FB:6A ⊕ |
| Endpoint Profile | Windows10-Workstation |
| Authentication Policy | Default |
| Authorization Policy | Default >> Wi-Fi_Guest_Access |
| Authorization Result | Guests,PermitAccess |

### Authentication Details

| | |
|---|---|
| Source Timestamp | 2017-08-21 10:04:06.395 |
| Received Timestamp | 2017-08-21 10:04:06.397 |
| Policy Server | ISE23 |
| Event | 5236 Authorize-Only succeeded |
| Username | Ulugbek Yusubaliev |
| User Type | GuestUser |
| Endpoint Id | E4:A4:71:85:FB:6A |
| Calling Station Id | e4-a4-71-85-fb-6a |
| Endpoint Profile | Windows10-Workstation |
| Authentication Identity Store | FacebookApp |
| Identity Group | GuestEndpoints |
| Audit Session Id | 0e249a0500000007599af5b2 |
| Authentication Method | Authorize Only |
| Service Type | Authorize Only |
| Network Device | WLC |

# Troubleshoot

# 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](link)    "Social Login support with proxy server"