

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

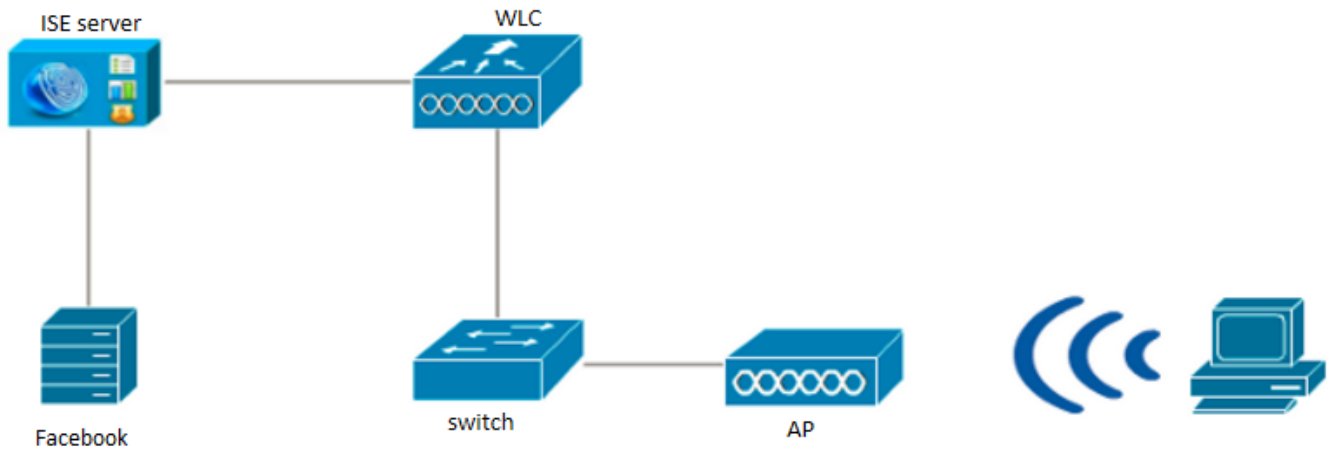
Components Used

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

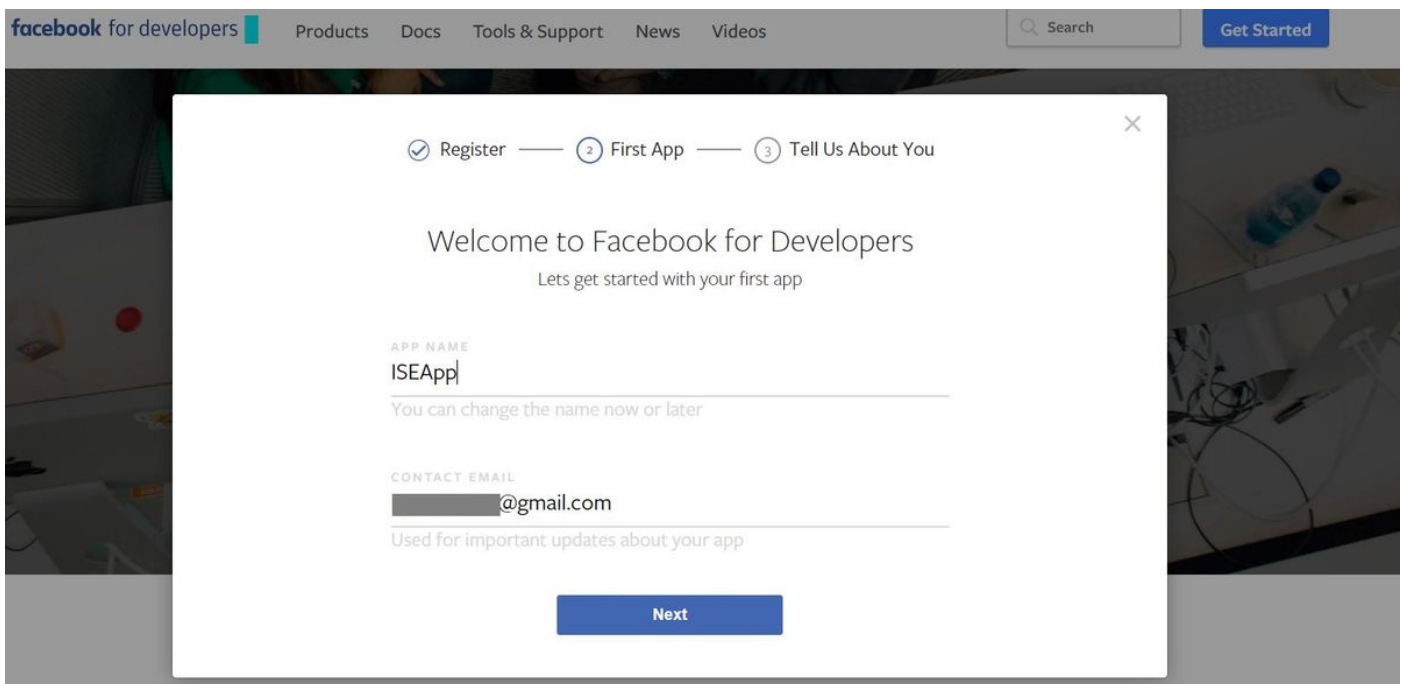


Configuration

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.

The screenshot shows the Facebook Developer Dashboard for an application named 'ISEApp'. The URL in the browser is [https://developers.facebook.com/apps/62096\[redacted\]/dashboard/](https://developers.facebook.com/apps/62096[redacted]/dashboard/). The app is currently in development mode. Key details include:

- APP ID: 62096[redacted]
- API Version: v2.10
- App ID: 62096[redacted]
- App Secret: [redacted]

A blue notification box at the top says "Click to see analytics for this app." Below the app details, there is a section titled "Get Started with the Facebook SDK" with a "Choose Platform" button. The left sidebar contains navigation options: Dashboard, Settings, Roles, Alerts, App Review, and PRODUCTS (+ Add Product).

Make the created app public.

The screenshot shows the Facebook Developer Dashboard for the 'ISEApp' at the review status page. The URL is [https://developers.facebook.com/apps/62096\[redacted\]/review-status/](https://developers.facebook.com/apps/62096[redacted]/review-status/). The main content area displays:

- Make ISEApp public?** A dialog with a "Yes" button and the text: "Your app is currently **live** and available to the public."
- Submit Items for Approval** A section with a "Start a Submission" button and text: "Some Facebook integrations require approval before public usage. Before submitting your app for review, please consult our **Platform Policy and Review Guidelines**."
- Approved Items** A section with a link to "Approved Items [?]"

The left sidebar is the same as in the previous screenshot. At the bottom, there is a section for "LOGIN PERMISSIONS".

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.

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.

Identity Services Engine Home Context Visibility Operations Policy Administration Work Centers License Warning

Network Access Guest Access TrustSec BYOD Profiler Posture Device Administration PassiveID

Overview Identities Identity Groups Ext Id Sources Administration Network Devices Portals & Components Manage Accounts Policy Elements Policy Sets Reports Custom Portal Files

Guest Portals

Guest Types Sponsor Groups Sponsor Portals

Portals Settings and Customization

Portal Name: * Self-Registered Guest Portal (default) Description: Guests are allowed to create their own accounts and access the network us Portal test URL

Save Close

Language File

Portal Behavior and Flow Settings

Use these settings to specify the guest experience for this portal.

Portal Page Customization

Customize portal pages by applying a theme and specifying field names and messages displayed to users.

Portal & Page Settings

Guest Flow (Based on settings)

Portal Settings

Login Page Settings

Require an access code:

Maximum failed login attempts before rate limiting: (1 - 999)

Time between login attempts when rate limiting: minutes (1 - 3000)

Include an AUP as link

Require acceptance

Allow guests to create their own accounts

Allow social login

Show Registration form after social login (i)

Allow guests to change password after login (i)

Allow the following identity-provider guest portal to be used for login (i)

There are no guest portals configured to use a SAML Id Provider as the Authentication Method.

Registration Form Settings

Assign to guest type:

Configure guest types at:
Work Centers > Guest Access > Configure > Guest Types

Account valid for: Days Maximum: 5 DAYS

Require a registration code:

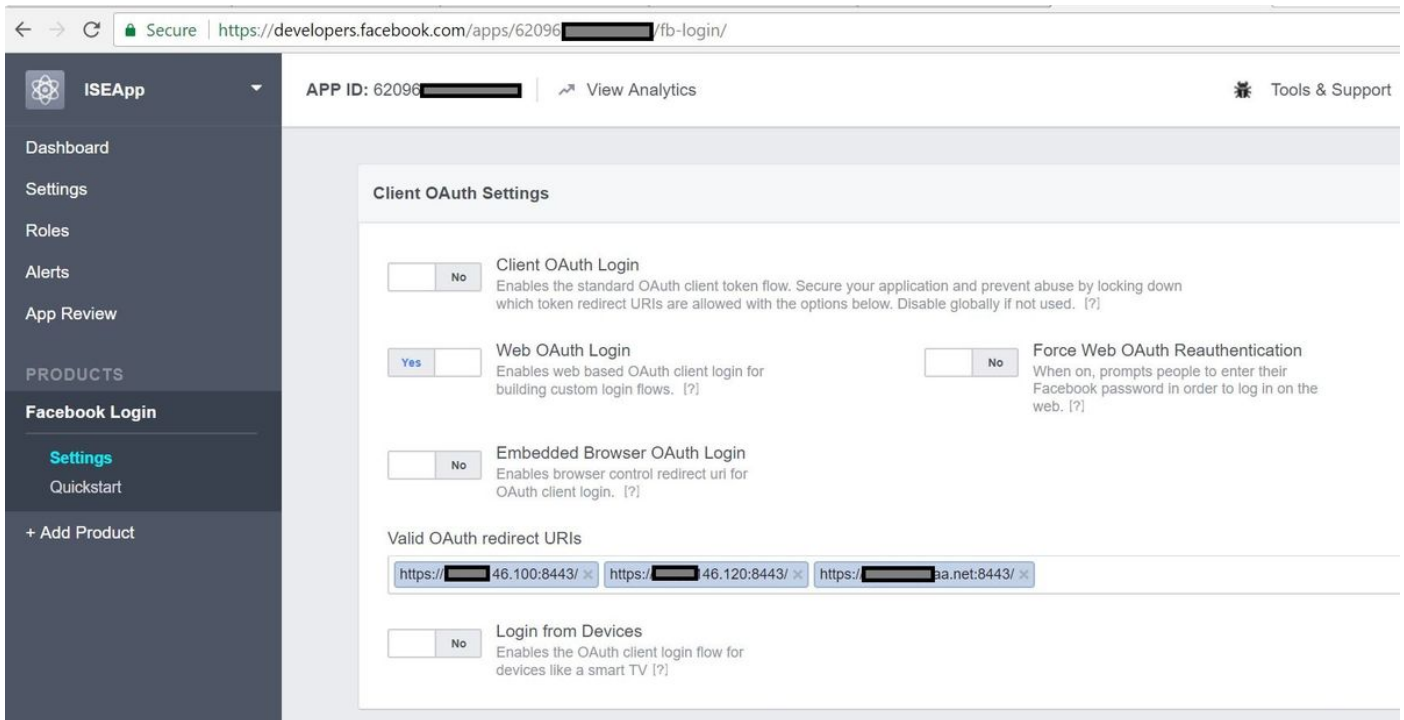
Fields to include	Required
<input checked="" type="checkbox"/> User name (i)	<input type="checkbox"/>
<input checked="" type="checkbox"/> First name	<input type="checkbox"/>
<input checked="" type="checkbox"/> Last name	<input type="checkbox"/>
<input checked="" type="checkbox"/> Email address	<input checked="" type="checkbox"/>

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**.

The screenshot shows the Cisco Identity Services Engine (ISE) interface. The top navigation bar includes 'Identity Services Engine' and various menu items like 'Home', 'Context Visibility', 'Operations', 'Policy', 'Administration', and 'Work Centers'. Below this, a secondary navigation bar lists 'System', 'Identity Management', 'Network Resources', 'Device Portal Management', 'pxGrid Services', 'Feed Service', and 'Threat Centric NAC'. A third navigation bar shows 'Identities', 'Groups', 'External Identity Sources', 'Identity Source Sequences', and 'Settings'. The 'External Identity Sources' section is active, showing a tree view with categories like 'Certificate Authentication Profile', 'Active Directory', 'Social Login', etc. The 'Social Login' category is expanded, and the 'FacebookApp' configuration page is displayed. The page title is 'Social Login > FacebookApp'. The 'Social Login' section contains the following fields: 'Name' (FacebookApp), 'Description' (empty), 'Type' (Facebook), 'App ID' (62098...), 'App Secret' (masked with dots), and 'Portal' (Self-Registered Guest Portal (default)). There are 'Show', 'Cancel', and 'Save' buttons. Below the form, a message states: 'Add all these automated redirect URLs to the App settings.' followed by a list of three URLs: 'https://[redacted]:100:8443', 'https://[redacted]:120:8443', and 'https://[redacted].a.net:8443'.

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.

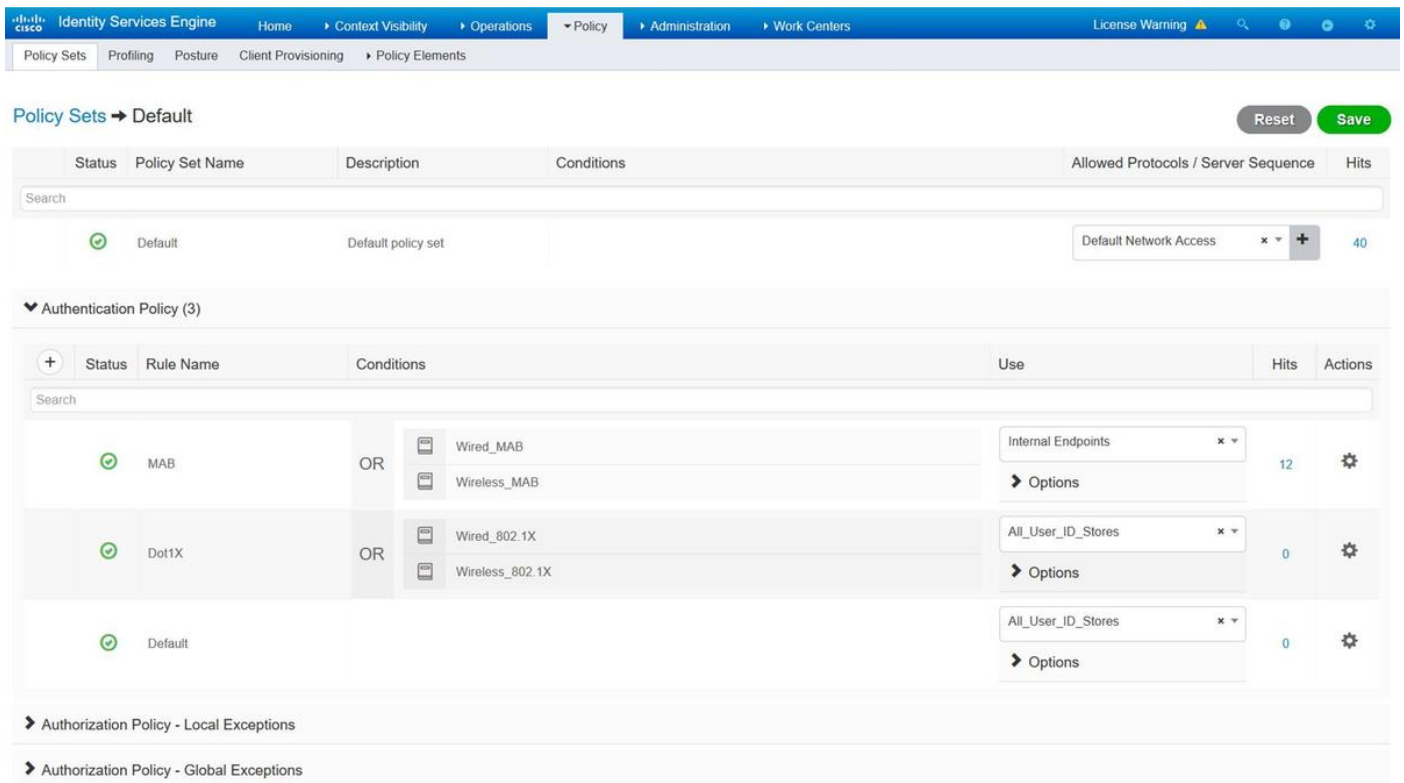


3. Configure Authentication and Authorization policies

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>)



Identity Services Engine

Home > Context Visibility > Operations > Policy > Administration > Work Centers

License Warning

Policy Sets Profiling Posture Client Provisioning > Policy Elements

Search

Default

All_User_ID_Stores 0

Options

Authorization Policy - Local Exceptions

Authorization Policy - Global Exceptions

Authorization Policy (12)

Status	Rule Name	Conditions	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

MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK

Save Configuration | Ping

Security

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

Access Control Lists > Edit

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	0.0.0.0 / 255.255.0.0	Any	Any	Any	Any	Any	1360
4	Permit	0.0.0.0 / 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.



Welcome

Welcome to the Guest Portal. Sign on with the username and password provided to you.

Username:

Password:

[Please read the terms and conditions.](#)

I agree to the terms and conditions

Sign On

OR

Log in With Facebook

[Don't have an account?](#)

This button takes advantage of the newly created application and redirects to the facebook login page where the user will enter their facebook credentials.



Sign Up

Log into Facebook

Log In

or

Create New Account

[Forgot account?](#)

[Not now](#)

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:

Identity Services Engine | Home | Context Visibility | Operations | Policy | Administration | Work Centers | License Warning

RADIUS | Threat-Centric NAC Live Logs | TACACS | Troubleshoot | Adaptive Network Control | Reports

Live Logs | Live Sessions

Misconfigured Supplicants: 0 | Misconfigured Network Devices: 0 | RADIUS Drops: 0 | Client Stopped Responding: 0 | Repeat Counter: 0

Refresh: Every 1 minute | Show: Latest 100 records | Within: Last 24 hours

Refresh | Reset Repeat Counts | Export To | Filter | Settings

Time	Status	Details	Repeat ...	Identity	Endpoint ID	Posture St...	Endpoint Profile	Authenticat...	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_GuestT_Ac
Aug 21, 2017 10:04:06.397 AM				Ulugbek Yusubaliev	E4:A4:71:85:FB:6A		Windows10-Workstation	Default	Default >> Wi-Fi_GuestT_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_

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

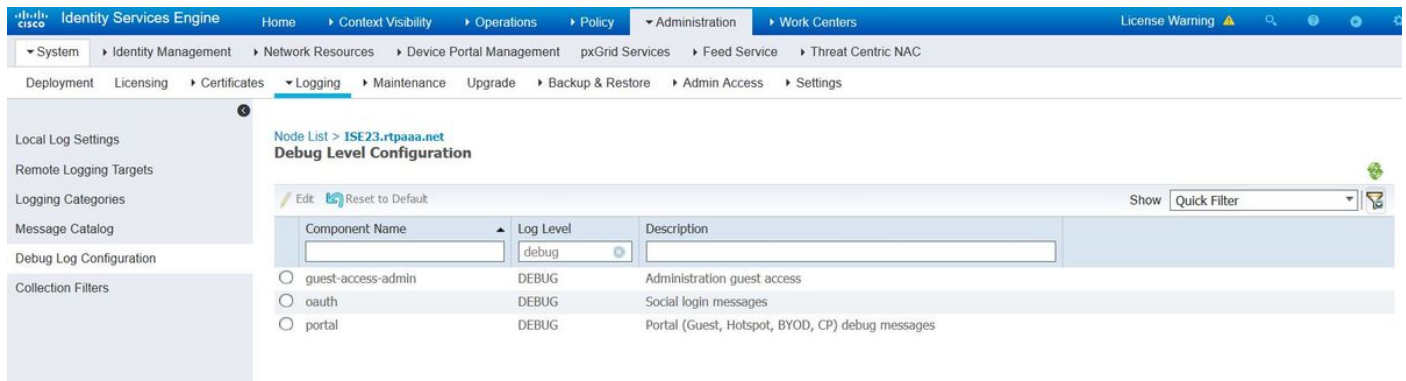
Authentication Details

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	<u>FacebookApp</u>
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**:



The screenshot shows the Cisco Identity Services Engine (ISE) Administration console. The navigation path is Administration > System > Logging > Debug Log Configuration. The page title is "Node List > ISE23.rtpaaa.net Debug Level Configuration". There are "Edit" and "Reset to Default" buttons. A "Show Quick Filter" dropdown is visible. The main content is a table with the following data:

Component Name	Log Level	Description
<input type="radio"/> guest-access-admin	DEBUG	Administration guest access
<input type="radio"/> oauth	DEBUG	Social login messages
<input type="radio"/> portal	DEBUG	Portal (Guest, Hotspot, BYOD, CP) debug messages

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"