

配置访客门户的ISE 2.3 Facebook社交媒体

目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[网络图](#)

[配置](#)

[1.配置Facebook应用](#)

[2.将ISE与Facebook应用集成](#)

[3.配置身份验证和授权策略](#)

[验证](#)

[故障排除](#)

[ISE上的调试](#)

简介

本文档介绍如何配置思科身份服务引擎(ISE)2.3与Facebook凭证的集成，以用于经过身份验证的访客访问。

先决条件

要求

Cisco 建议您了解以下主题：

- 身份服务引擎(ISE)配置
- 基本Facebook应用配置

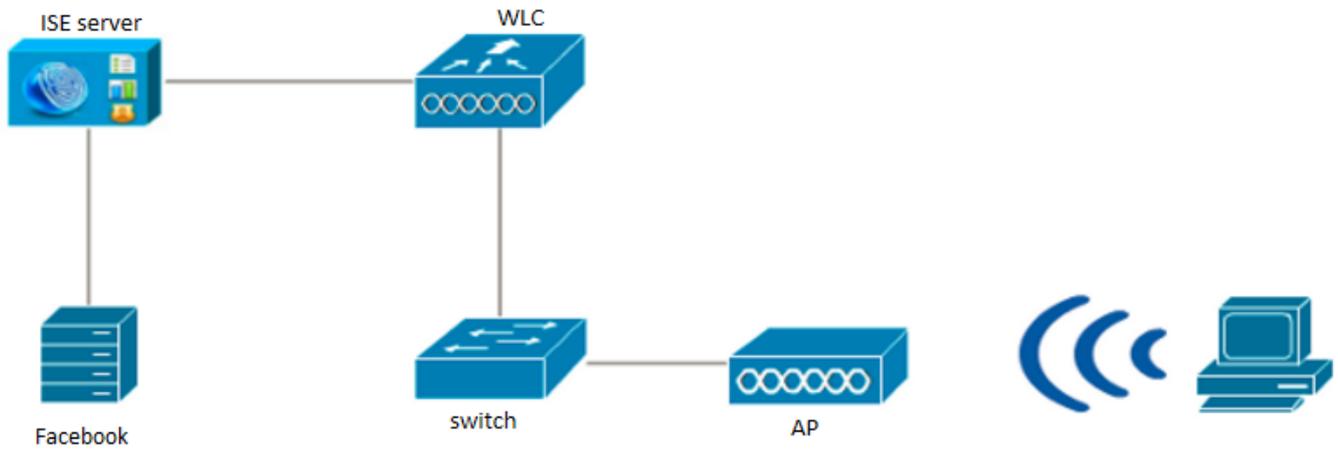
使用的组件

本文档中的信息基于以下软件和硬件版本：

- 思科ISE版本2.3
- Facebook社交登录
- 思科无线局域网控制器(WLC)版本8.3.102.0

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

网络图

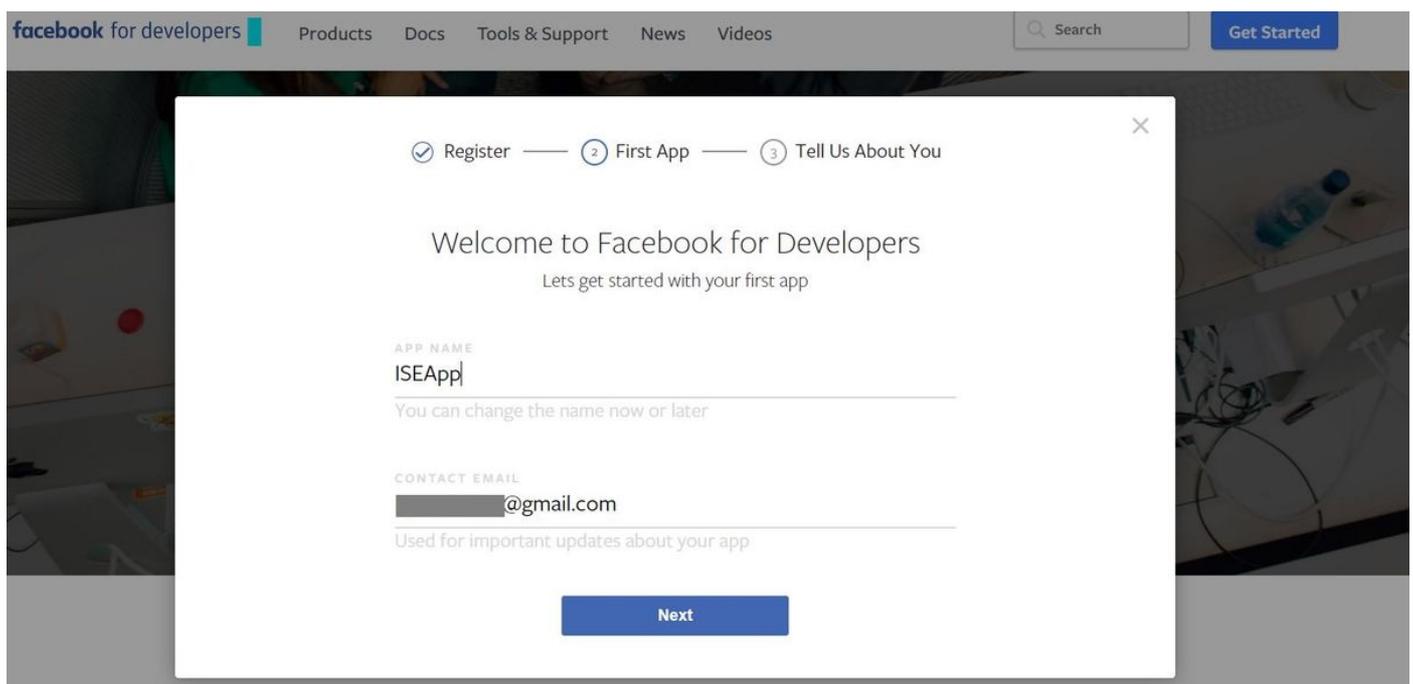


配置

显示的Facebook应用配置是一个示例，而不是思科推荐的配置。

1.配置Facebook应用

转到<https://developers.facebook.com>，注册新应用。



应用的控制面板显示**应用ID**和**应用密钥**，将在ISE上用于创建外部社交登录。

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: API Version v2.10, App ID 62096[redacted], and an App Secret. A blue notification bubble 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).

将创建的应用公开。

The screenshot shows the 'Make ISEApp public?' dialog in the Facebook Developer Dashboard. The URL is [https://developers.facebook.com/apps/62096\[redacted\]/review-status/](https://developers.facebook.com/apps/62096[redacted]/review-status/). The dialog has a 'Yes' button and a text field. Below the dialog, there is a 'Submit Items for Approval' section with a 'Start a Submission' button. The 'Approved Items' section is currently empty. The left sidebar is the same as in the previous screenshot.

2. 将ISE与Facebook应用集成

使用以下信息将Facebook应用与思科ISE集成。

导航至**管理>身份管理>外部身份源>社交登录**并添加新存储。

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

将ISE访客门户配置为允许社交登录。

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"/>

在配置ISE访客门户以允许社交登录后，社交登录将填充URL，并需要添加到Facebook应用设置(有效OAuth重定向URL)。

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 > FacebookApp

Social Login

Name * FacebookApp

Description

Type * Facebook

App ID * 62098[REDACTED]

App Secret * [REDACTED] Show

Cancel Save

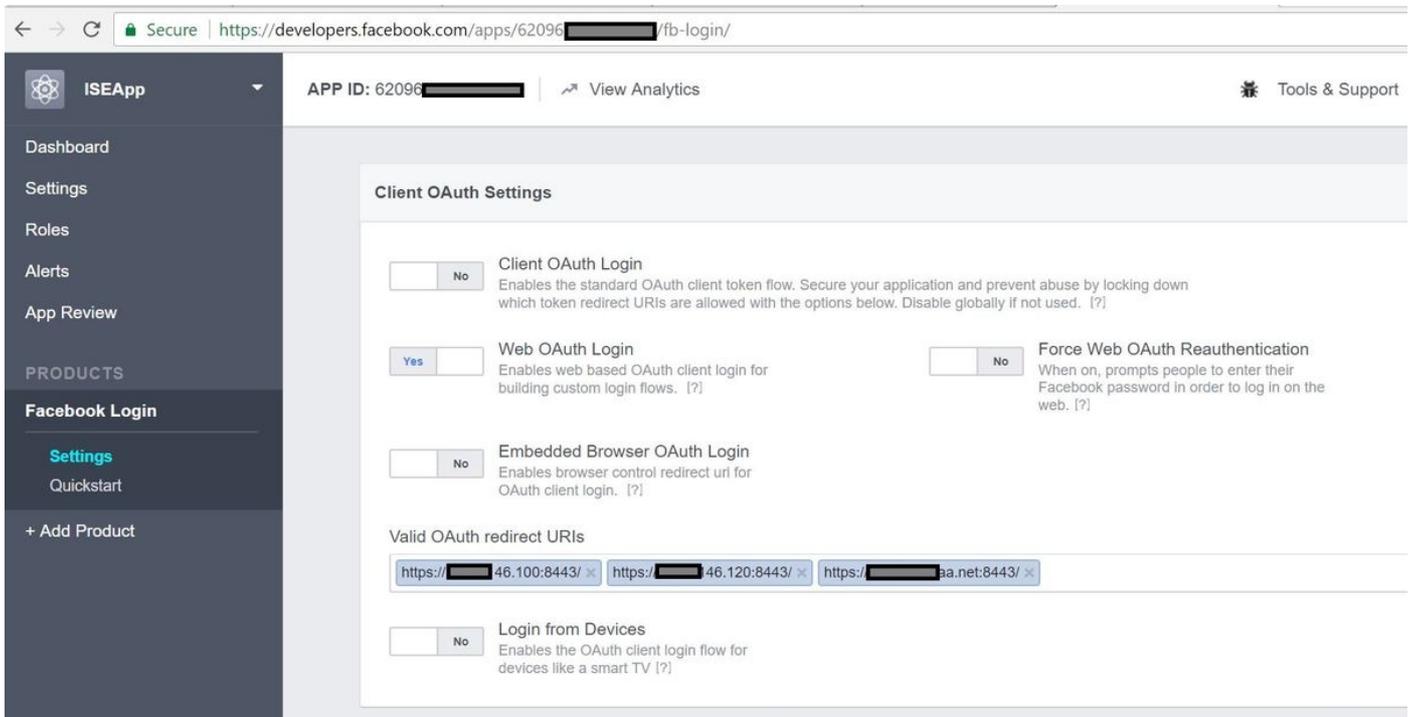
Portal Self-Registered Guest Portal (default) x

i Add all these automated redirect URLs to the App settings.

```
https://[REDACTED]100:8443
https://[REDACTED]120:8443
https://[REDACTED]a.net:8443
```

从产品添加Facebook登录并添加有效OAuth重定向URL。

成功将ISE门户与Facebook外部社交登录绑定后，URL将在ISE上自动生成。

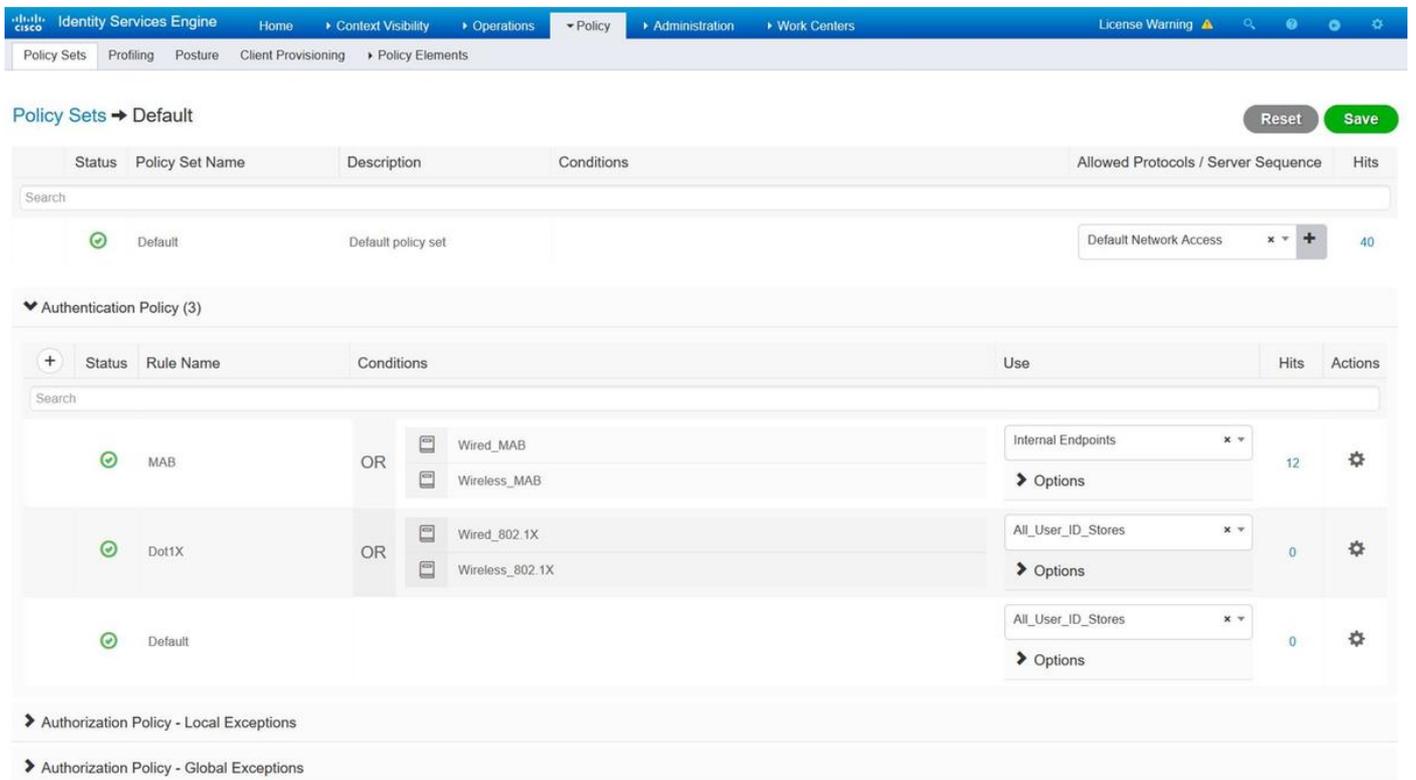


3.配置身份验证和授权策略

ISE配置遵循与访客CWA (中央网络身份验证) 相同的配置步骤。

(有关ISE CWA的配置步骤，请参阅以下文档：

<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	

确保Facebook IP地址范围(31.13.0.0/16)已从WLC重定向ACL中排除

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

验证

当访客用户被重定向后，系统会显示“使用Facebook登录”选项。



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?](#)

此按钮利用新创建的应用并重定向到用户将在其中输入其facebook凭据的facebook登录页面。

facebook [Sign Up](#)

Log into Facebook

Log In

or

Create New Account

[Forgot account?](#)

[Not now](#)

身份验证成功后，访客用户重定向回ISE门户。



Welcome Message

Click **Continue** to connect to the network.
You're very close to gaining network access.

Continue

ISE Radius实时日志 :

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

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

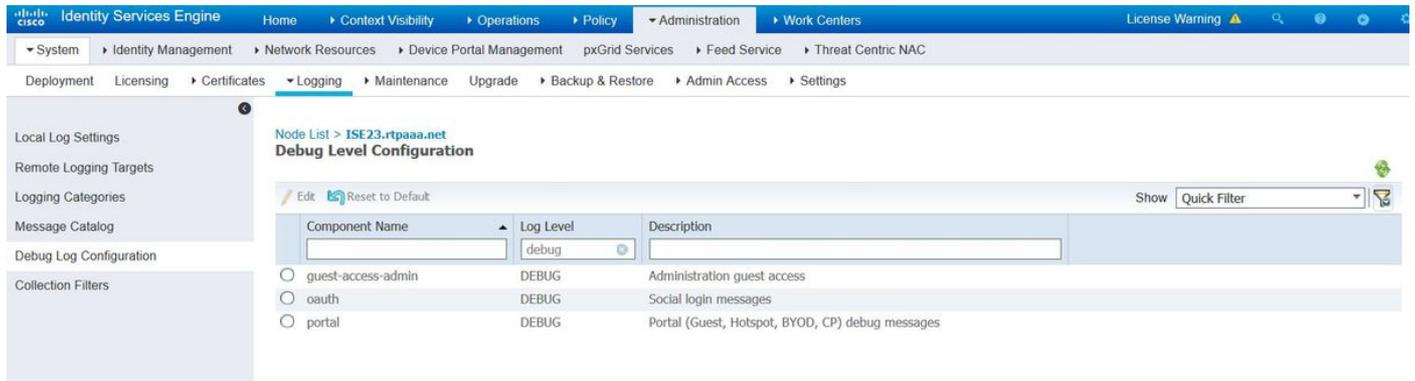
Authentication Details

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

故障排除

ISE上的调试

要在ISE上启用调试，请导航至**Administration > System > Logging > Debug Log Configuration**，选择PSN节点，并将以下组件的日志级别更改为**DEBUG**：



要检查的日志 — `ise-psc.log`和`guest.log`。您可以直接从ISE的CLI跟踪它们：

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

在连接到Facebook应用期间，ISE显示连接超时错误：

```
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
```

确保ISE节点具有直接互联网连接。

使用Bug CSCve87511上的代理地址 "代理服务器的社交登录支持"