

為訪客門戶配置ISE 2.3 Facebook社群媒體

目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[網路圖表](#)

[組態](#)

[1.配置Facebook應用](#)

[2.將ISE與Facebook應用整合](#)

[3.配置身份驗證和授權策略](#)

[驗證](#)

[疑難排解](#)

[ISE上的調試](#)

簡介

本文檔介紹如何配置思科身份服務引擎(ISE)2.3與Facebook憑據的整合，以實現經過身份驗證的訪客訪問。

必要條件

需求

思科建議您瞭解以下主題：

- 身份服務引擎(ISE)配置
- 基本Facebook應用配置

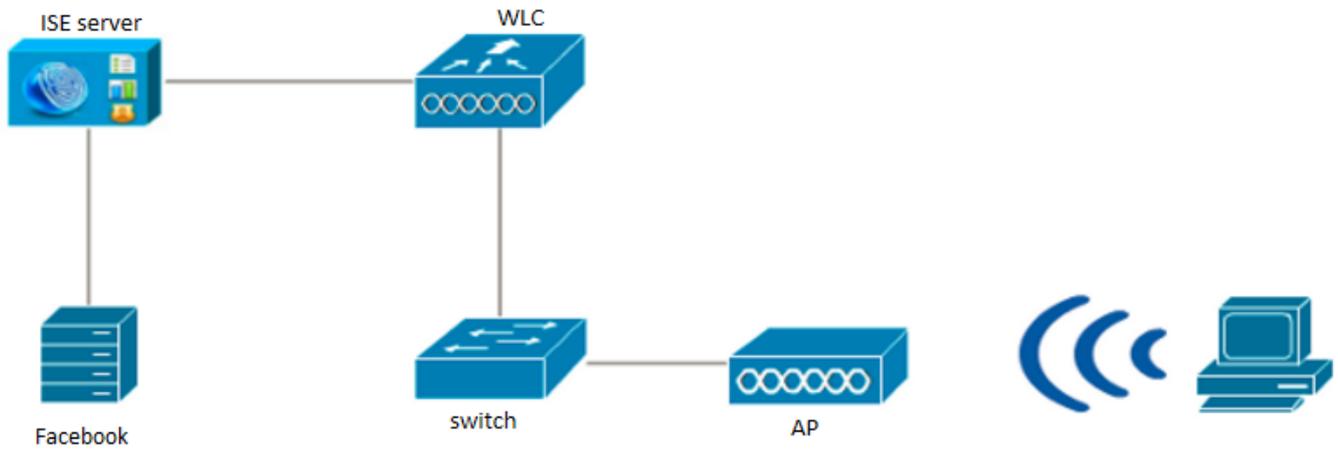
採用元件

本文中的資訊係根據以下軟體和硬體版本：

- Cisco ISE版本2.3
- Facebook社交登入
- Cisco無線LAN控制器(WLC)版本8.3.102.0

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

網路圖表

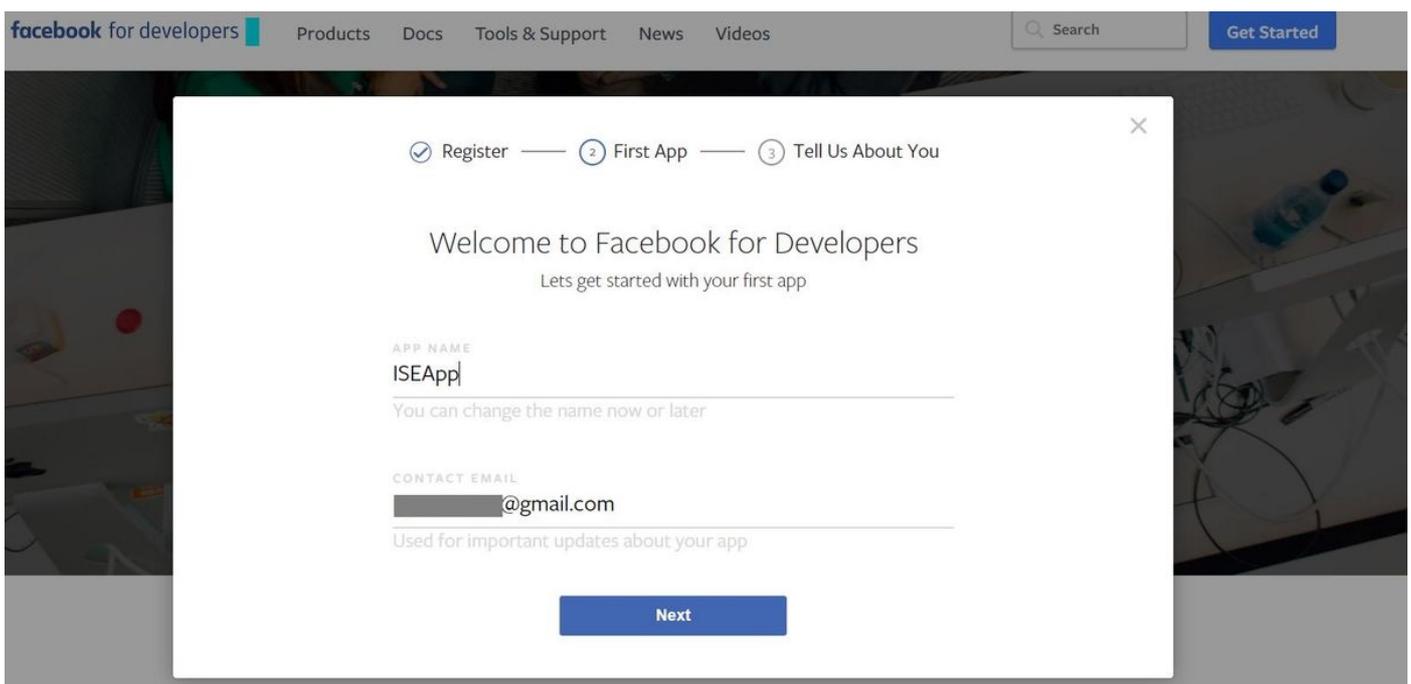


組態

提供的Facebook應用配置是一個示例，不是思科建議的配置。

1.配置Facebook應用

轉到<https://developers.facebook.com>，然後註冊新應用。



應用的控制面板顯示應用ID和應用Secret金鑰，該金鑰將在ISE上用於建立外部社交登入。

Secure | https://developers.facebook.com/apps/62096[redacted]/dashboard/

ISEApp | APP ID: 62096[redacted] | View Analytics | Tools & Support | Docs

Dashboard

Click to see analytics for this app. X

ISEApp 

This app is in development mode and can only be used by app admins, developers and testers [?]

API Version [?] v2.10 | App ID 62096[redacted]

App Secret [redacted] [Show](#)

 **Get Started with the Facebook SDK**

Use our quick start guides to set up the Facebook SDK for your iOS or Android app, Facebook Web Game or website. [Choose Platform](#)

使建立的應用程式公開。

Secure | https://developers.facebook.com/apps/62096[redacted]/review-status/

ISEApp | APP ID: 62096[redacted] | View Analytics | Tools & Support | Docs

Dashboard

Settings

Roles

Alerts

App Review

PRODUCTS

+ Add Product

Make ISEApp public?

Yes Your app is currently **live** and available to the public.

Submit Items for Approval

Some Facebook integrations require approval before public usage. Before submitting your app for review, please consult our [Platform Policy and Review Guidelines](#). [Start a Submission](#)

Approved Items [?]

LOGIN PERMISSIONS

2. 將ISE與Facebook應用整合

使用以下資訊將Facebook應用與思科ISE整合。

導航到Administration > Identity Management > External Identity Sources > Social Login並新增新儲存。

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

配置ISE訪客門戶以允許社交登入。

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

Facebook FacebookApp +

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"/>

配置ISE訪客門戶以允許社交登入後，社交登入將使用URL填充，並且需要新增到Facebook應用設定Valid OAuth redirect 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

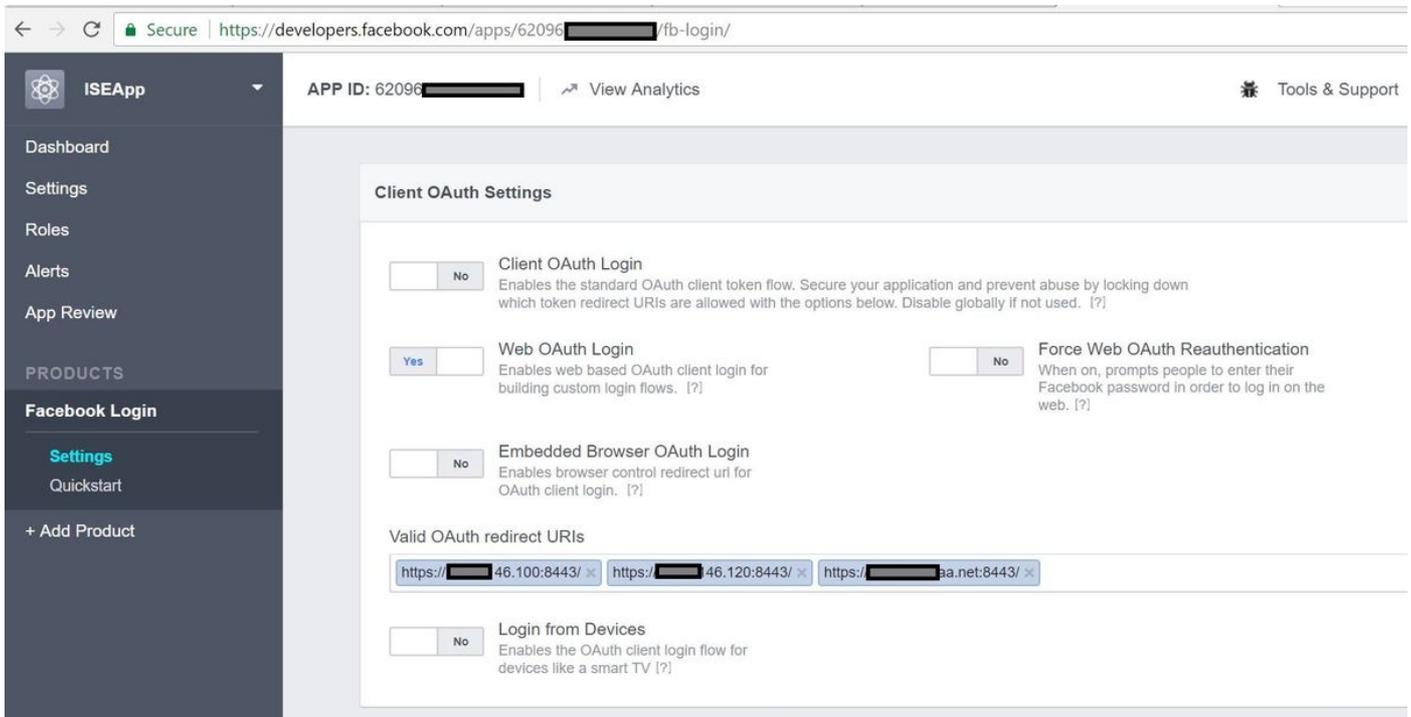
Portal Self-Registered Guest Portal (default) x

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

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

從「產品」新增Facebook Login並新增有效的OAuth重定向URL。

成功將ISE門戶與Facebook外部社交登入繫結後，將在ISE上自動生成URL。

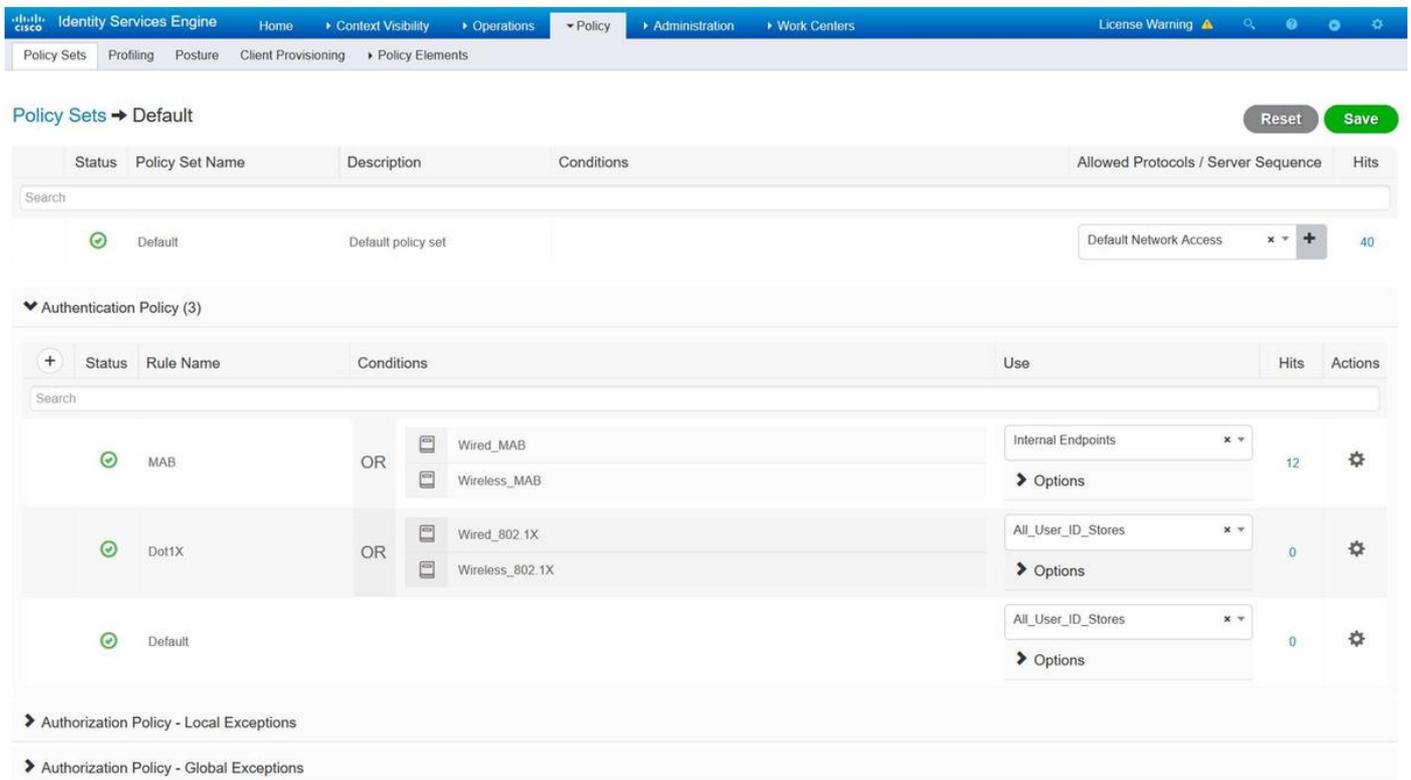


3. 配置身份驗證和授權策略

ISE配置遵循與訪客CWA (中央Web身份驗證) 相同的配置步驟。

(有關ISE CWA的配置步驟，請參閱以下文檔：

<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	

確保已將Facebook ip位址範圍(31.13.0.0/16)從WLC重新導向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

驗證

在重定向訪客使用者後，會向他們顯示「使用Facebook登入」選項。



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?](#)

此按鈕利用新建立的應用程式，重定向到facebook登入頁面，使用者將在其中輸入其facebook憑據。

facebook [Sign Up](#)

Log into Facebook

Log In

or

[Create New Account](#)

[Forgot account?](#)

[Not now](#)

身份驗證成功後，訪客使用者重定向回ISE門戶。



Welcome Message

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

Continue

ISE Radius即時日誌 :

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	Posture Status	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_

Overview

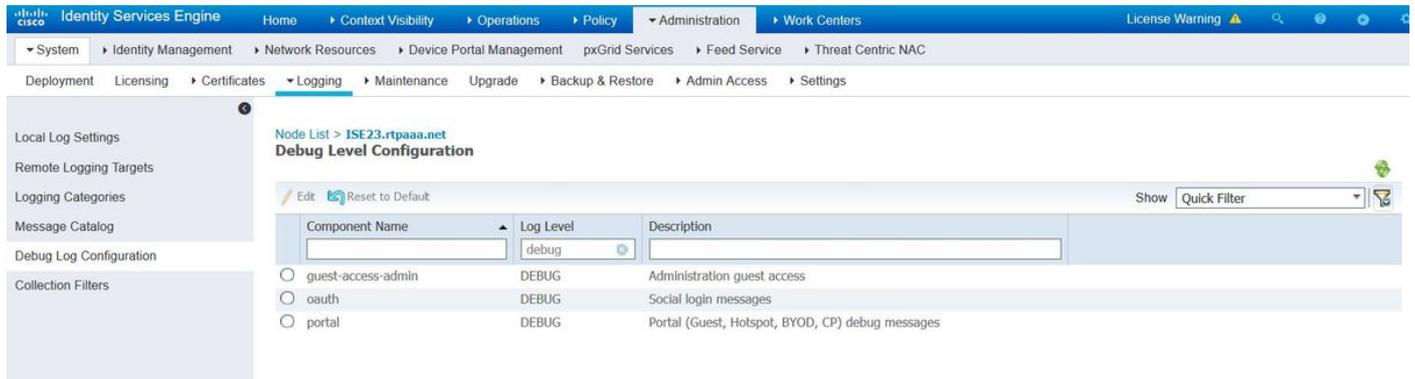
Event	5236 Authorize-Only succeeded
Username	Ulugbek Yusubaliev
Endpoint Id	E4:A4:71:85:FB:6A ⓘ
Endpoint Profile	Windows10-Workstation
Authentication Policy	Default
Authorization Policy	Default >> Wi-Fi_Guest_Access
Authorization Result	Guests_PermitAccess

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

ISE上的調試

要在ISE上啟用調試，請導航到Administration > System > Logging > Debug Log Configuration，選擇PSN節點並將以下元件的日誌級別更改為DEBUG:



要檢查的日誌 — ise-psc.log和guest.log。您可以直接從ISE的CLI對其進行跟蹤：

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

在連線到Facebook應用期間，ISE顯示連線超時錯誤：

```
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
```

確保ISE節點具有直接網際網路連線。

在Bug CSCve87511上使用[代理地址](#) "代理伺服器的社交登入支援"