

ゲストポータル用のISE 2.3 Facebookソーシャルメディアの設定

内容

[概要](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[ネットワーク図](#)

[コンフィギュレーション](#)

[1. Facebookアプリの構成](#)

[2. ISEとFacebookアプリの統合](#)

[3. 認証および許可ポリシーの設定](#)

[確認](#)

[トラブルシューティング](#)

[ISEでのデバッグ](#)

概要

このドキュメントでは、Cisco Identity Services Engine(ISE)2.3とFacebookクレデンシャルとの統合を、認証されたゲストアクセス用に設定する方法について説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- Identity Services Engine (ISE) の設定
- Facebookアプリの基本設定

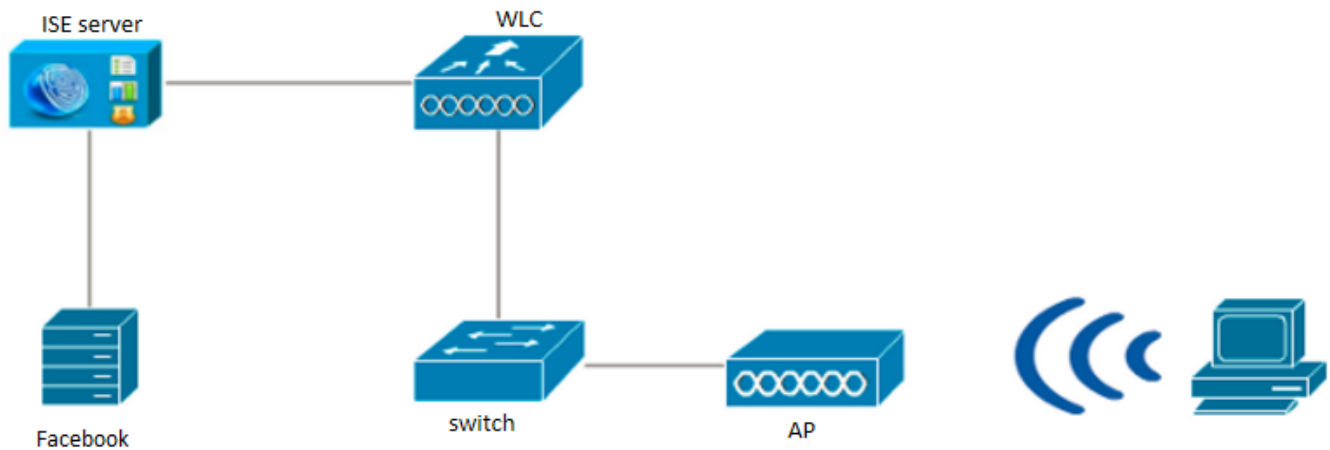
使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- Cisco ISE バージョン 2.3
- Facebookソーシャルログイン
- Cisco Wireless LAN Controller (WLC) バージョン 8.3.102.0

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。対象のネットワークが実稼働中である場合には、どのようなコマンドについても、その潜在的な影響について確実に理解しておく必要があります。

ネットワーク図

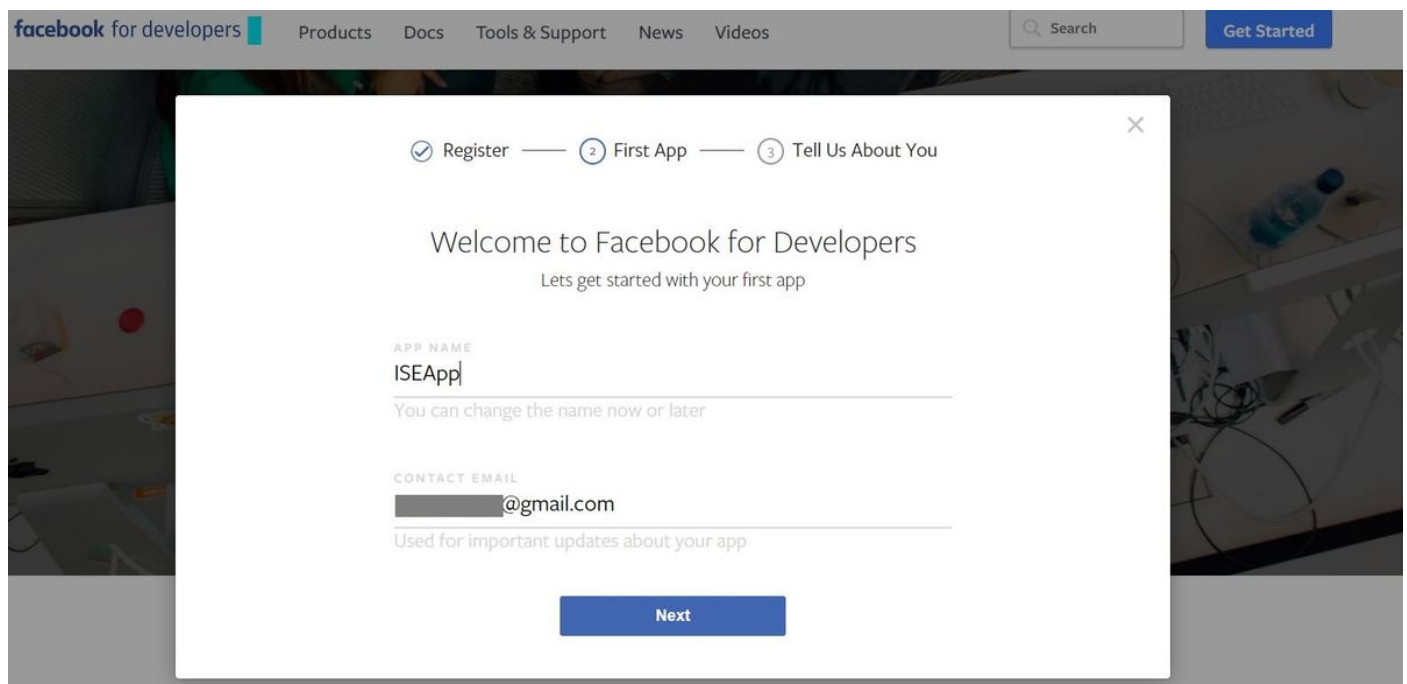


コンフィギュレーション

示されているFacebookアプリの設定は一例であり、シスコが推奨する設定ではありません。

1. Facebookアプリの構成

<https://developers.facebook.com>に移動し、新しいアプリを登録します。



アプリケーションのダッシュボードにApp IDとApp Secretキーが表示され、ISEで外部ソーシャルログインの作成に使用されます。



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

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

Dashboard


Click to see analytics for this app. ✕

Dashboard

 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
..... [Show](#)

 **Get Started with the Facebook SDK** [Choose Platform](#)

Use our quick start guides to set up the Facebook SDK for your iOS or Android app, Facebook Web Game or website.

作成したアプリを公開します。

← → ↻ 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 No 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. ISEとFacebookアプリの統合

FacebookアプリをCisco ISEと統合するには、次の情報を使用します。

[Administration] > [Identity Management] > [External Identity Sources] > [Social Login]に移動し、新しいストアを追加します。

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

ISEゲストポータルを[Allow social login]に設定します。

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"/>

ソーシャルログインを許可するようにISEゲストポータルを設定した後、ソーシャルログインにはURLが入力され、Facebookアプリの設定Valid OAuth redirect URLsに追加する必要があります。

The screenshot displays the Cisco Identity Services Engine (ISE) Administration console. The top navigation bar includes 'Home', 'Context Visibility', 'Operations', 'Policy', 'Administration', and 'Work Centers'. The left sidebar shows a tree view of 'External Identity Sources' with categories like Certificate Authentication Profile, Active Directory, and Social Login. The main content area is titled 'Social Login > FacebookApp' and contains the following configuration fields:

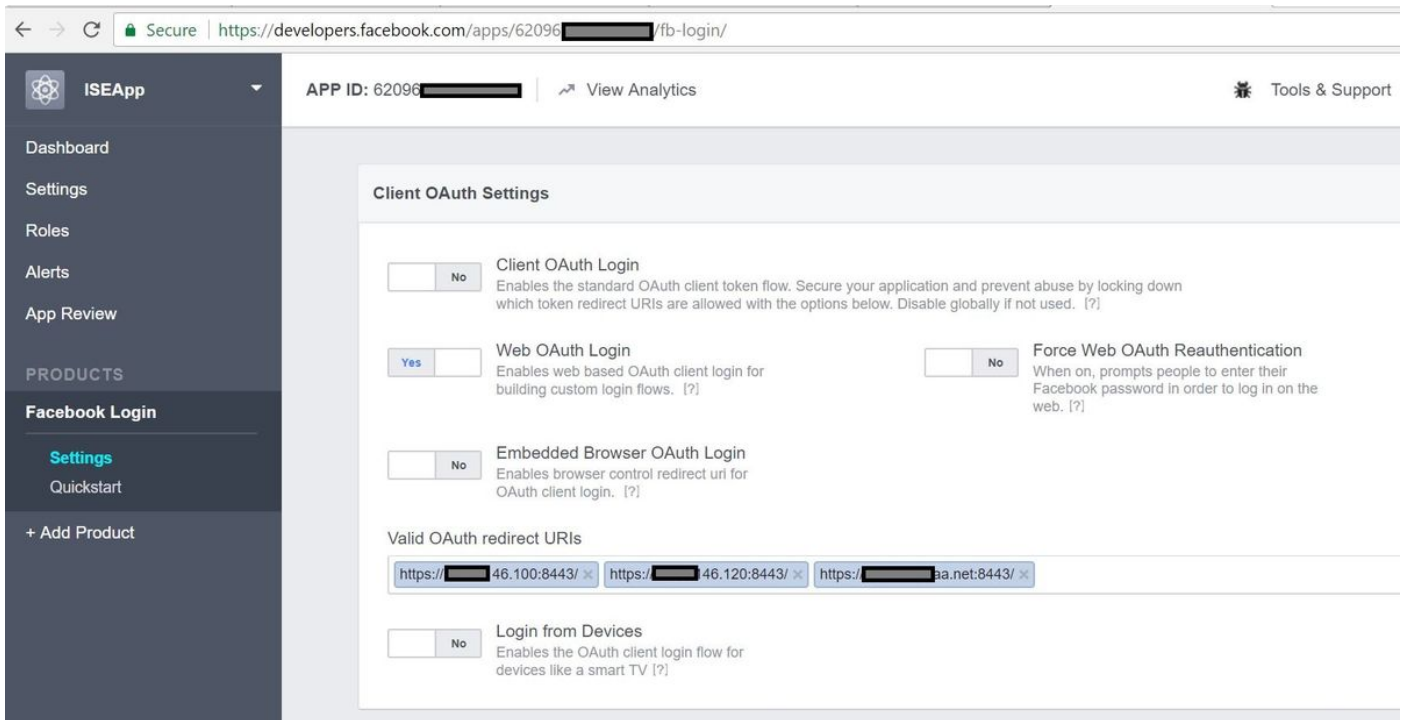
- Name: FacebookApp
- Description: (empty)
- Type: Facebook
- App ID: 62098 [redacted]
- App Secret: [redacted] (with a 'Show' button)
- Buttons: Cancel, Save
- Portal: Self-Registered Guest Portal (default)

Below the configuration fields, there is an information icon and a note: 'Add all these automated redirect URLs to the App settings.' The list of URLs is:

- https://[redacted]100:8443
- https://[redacted]120:8443
- https://[redacted]a.net:8443

製品からFacebookログインを追加し、有効なOAuthリダイレクトURLを追加します。

ISEポータルをFacebook外部ソーシャルログインに正常にバインドすると、URLがISEに自動的に生成されます。

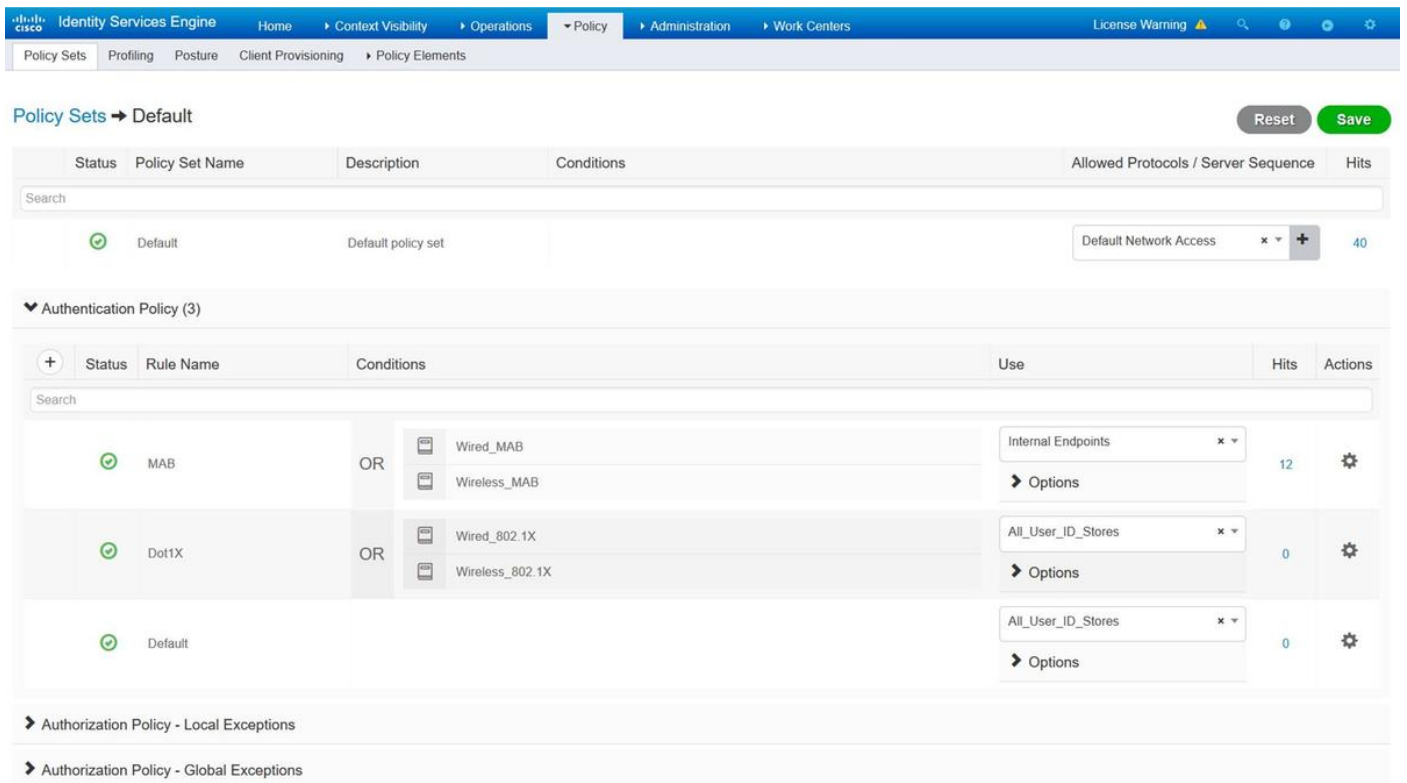


3. 認証および許可ポリシーの設定

ISE設定は、ゲストCWA (中央Web認証) と同じ設定手順に従います。

(ISE CWAの設定手順については、次のドキュメントを参照してください。

<https://www.cisco.com/c/en/us/support/docs/security/identity-services-engine/115732-central-web-auth-00.html>) を設定できます。



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	

Facebook IPアドレス範囲(31.13.0.0/16)がWLCリダイレクトACLから除外されていることを確認します

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

確認

ゲストユーザがリダイレクトされると、[Log in With Facebook]オプションが表示されます。



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?](#)

このボタンは、新しく作成されたアプリケーションを利用して、ユーザがFacebookクレデンシャルを入力するFacebookログインページにリダイレクトします。

facebook [Sign Up](#)

Log into Facebook

Log In

or

Create New Account

[Forgot account?](#)

[Not now](#)

認証に成功すると、ゲストユーザはISEポータルにリダイレクトし直します。



Welcome Message

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

Continue

ISE RADIUSライブログ :

The screenshot shows the Cisco Identity Services Engine (ISE) interface for RADIUS Live Logs. The top navigation bar includes Home, Context Visibility, Operations, Policy, Administration, and Work Centers. Below the navigation, there are several summary cards for Misconfigured Supplicants, Misconfigured Network Devices, RADIUS Drops, Client Stopped Responding, and Repeat Counter, all showing a count of 0. A table below displays the live log entries with the following columns: Time, Status, Details, Repeat, Identity, Endpoint ID, Posture St..., Endpoint Profile, Authentication, and Authorization Policy. The table contains several rows of log data, including entries for 'Ulugbek Yusubaliev' and 'E4.A4.71.85.FB.6A'.

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

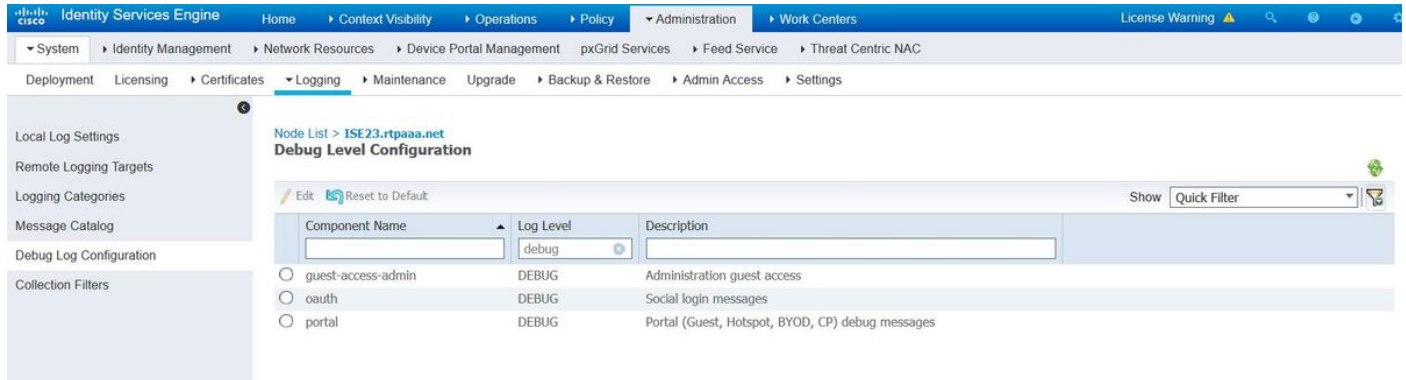
Authentication Details

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

トラブルシューティング

ISE でのデバッグ

ISEでデバッグを有効にするには、[Administration] > [System] > [Logging] > [Debug Log Configuration]に移動し、PSNノードを選択し、次のコンポーネントのログレベルを[DEBUG]に変更します。



The screenshot shows the Cisco Identity Services Engine (ISE) web interface. The breadcrumb navigation is Administration > System > Logging > Debug Log Configuration. The page title is "Node List > ISE23.rtpaaa.net Debug Level Configuration". There are buttons for "Edit" and "Reset to Default". A "Show" dropdown menu is set to "Quick Filter". 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

確認するログ : ise-psc.logおよびguest.log。ISE の CLI から、これらの最後の部分を直接表示できます。

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

Facebookアプリケーションへの接続中、ISEに接続タイムアウトのエラーが表示されます。

```
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
```

ISEノードに直接インターネット接続があることを確認します。

バグCSCve87511で対応するプロキシの[使用](#) 「プロキシサーバによるソーシャルログインサポート」