

ISE 2.3 Beta training: Facebook Social media for guest portals

June 2017



Agenda

- Main use cases list
- OAuth Concept
- Dive into the use cases
- Troubleshooting
- Q&A

Benefits of social media login

- The ability for your guests to quickly connect to your guest system without the need for credentials or registration (can be required if needed)).
- Gain visibility into who is using your guest network by using analytics through social media providers tools.
- Connect with your guests through the social media application for marketing purposes.

ISE Guest portal as OAuth application

OAuth is an [open standard](#) for access delegation, commonly used as a way for Internet users to grant websites or applications access to their information on other websites but without giving them the passwords.^[1] This mechanism is used by companies such as Google, Facebook, Microsoft and Twitter to permit the users to share information about their accounts with third party applications or websites.

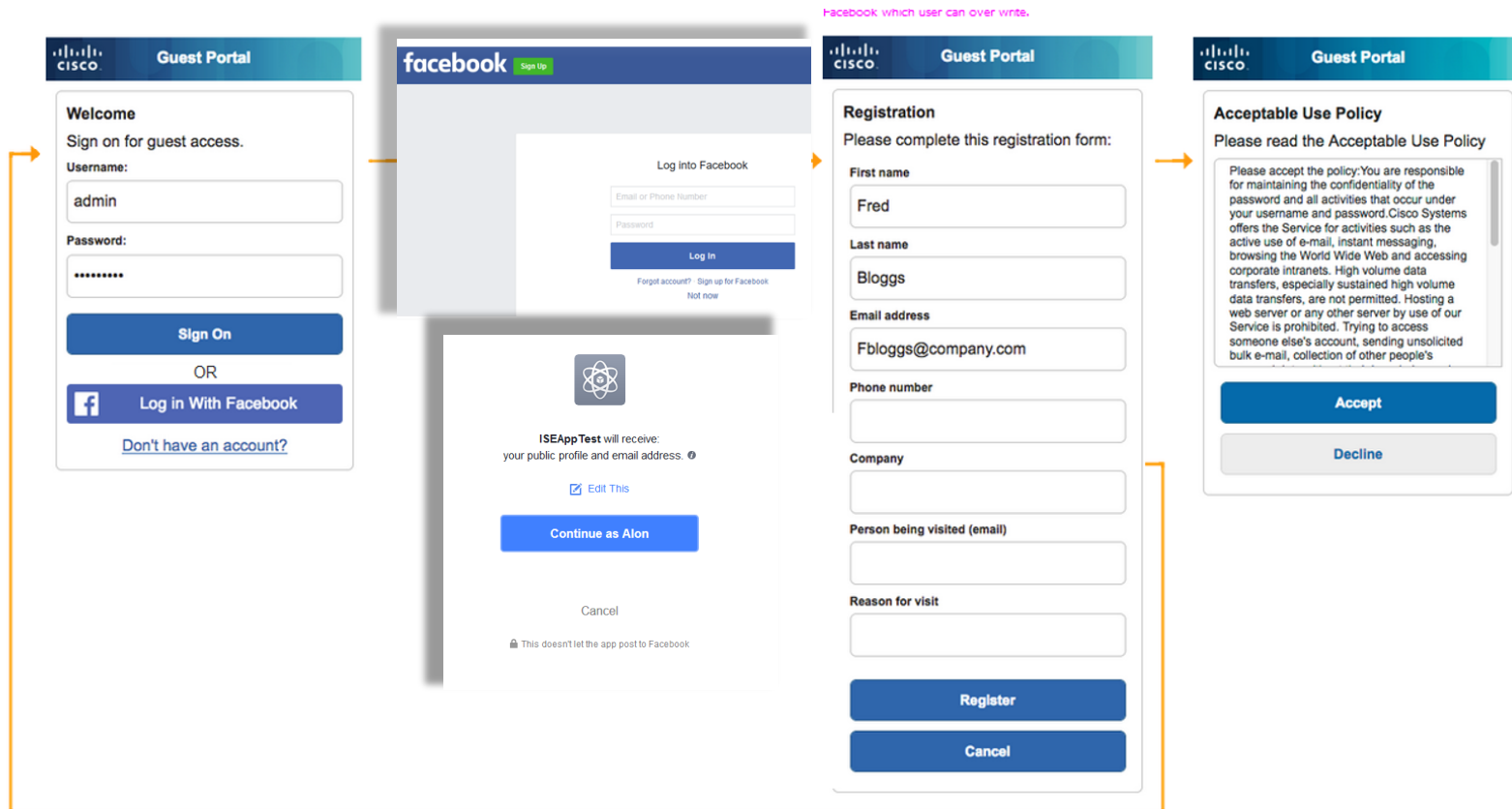
use case 1:

As Tim, the network administrator, I would like the ability to use social networks such as Facebook as my authentication source for guest users so that I can provide a more seamless user experience to my guests.

use case 2:

As David, an end user, when I connect to a guest network, I would like an option to use my social login to connect to the network, instead of having to register myself and create separate credentials each time I use the guest service.

Guest with Social Login - Flow experience



social media flows

1. **Social media login without registration**
2. **Social Media login with registration**
3. **Social Media login with registration and sponsor approval**




What happens when the device comes back in with new network session?

- Depending on how the authorization rules are setup the next time they come in 1 of 2 things will happen
- authorization rule (if guestendpoint then permit access). If endpoint is no longer in that group (removed manually or guest account expired) then will be redirected back to guest page to register again
- Redirected back to guest page which will auto login with token or go through registration again

What info is captured? Live logs

Live logs will have the facebook username and social media identifier

The screenshot displays a live log interface with a table of authentication events and a detailed view of a selected event.

Time	Status	Details	Repeat ...	Identity
Jun 07, 2017 08:09:55.852 PM	✓			jason kunst
Jun 07, 2017 08:00:37.018 PM	✓			tme ise
Jun 07, 2017 07:42:57.327 PM	✓			jason kunst

Other Attributes	
ConfigVersionId	79
SocialMediaIdentifier	https://www.facebook.com/10213161358285391
IpAddress	10.1.100.6
PortalName	Self-Registered Guest Portal (default)
PsnHostName	ise-1.demo.local
GuestUserName	jason kunst

What info is captured? Guest reports

Guest reports have Facebook username (as of 6/13/17 first, last, full name and email address are missing and being developed)

The screenshot displays the Cisco Identity Services Engine (ISE) interface for viewing a Master Guest Report. The top navigation bar includes 'Home', 'Context Visibility', 'Operations', 'Policy', 'Administration', and 'Work Centers'. The left sidebar contains a 'Reports' section with sub-items like 'Audit', 'Device Administration', 'Diagnostics', 'Endpoints and Users', and 'Guest'. The main content area shows the 'Master Guest Report' for the period from 2017-06-06 00:00:00.0 to 2017-06-13 18:19:36.0. A table lists the reports with columns for 'Logged At', 'Guest User Name', 'IP Address', 'Operation', and 'AUP Acceptance'. The third row of the table shows a report from 2017-06-06 19:14:55.464 with the guest user name 'jason kunst', which is highlighted with a red box. The table also includes a search filter for 'Last 7 Days' and a 'My Reports' button.

Logged At	Guest User Name	IP Address	Operation	AUP Acceptance
2017-06-07 20:00:39.111	tme ise	10.1.100.6	AUP	Guest user has accepted the use policy
2017-06-07 19:50:01.671		10.1.100.6	AUP	Indicates that a sponsor user accepted u...
2017-06-07 19:49:59.913		10.1.100.6	Login	
2017-06-06 19:14:55.464	jason kunst	10.1.100.6	AUP	Guest user has accepted the use policy

More info

- how-to guide and FAQ
- <https://communities.cisco.com/docs/DOC-73960>

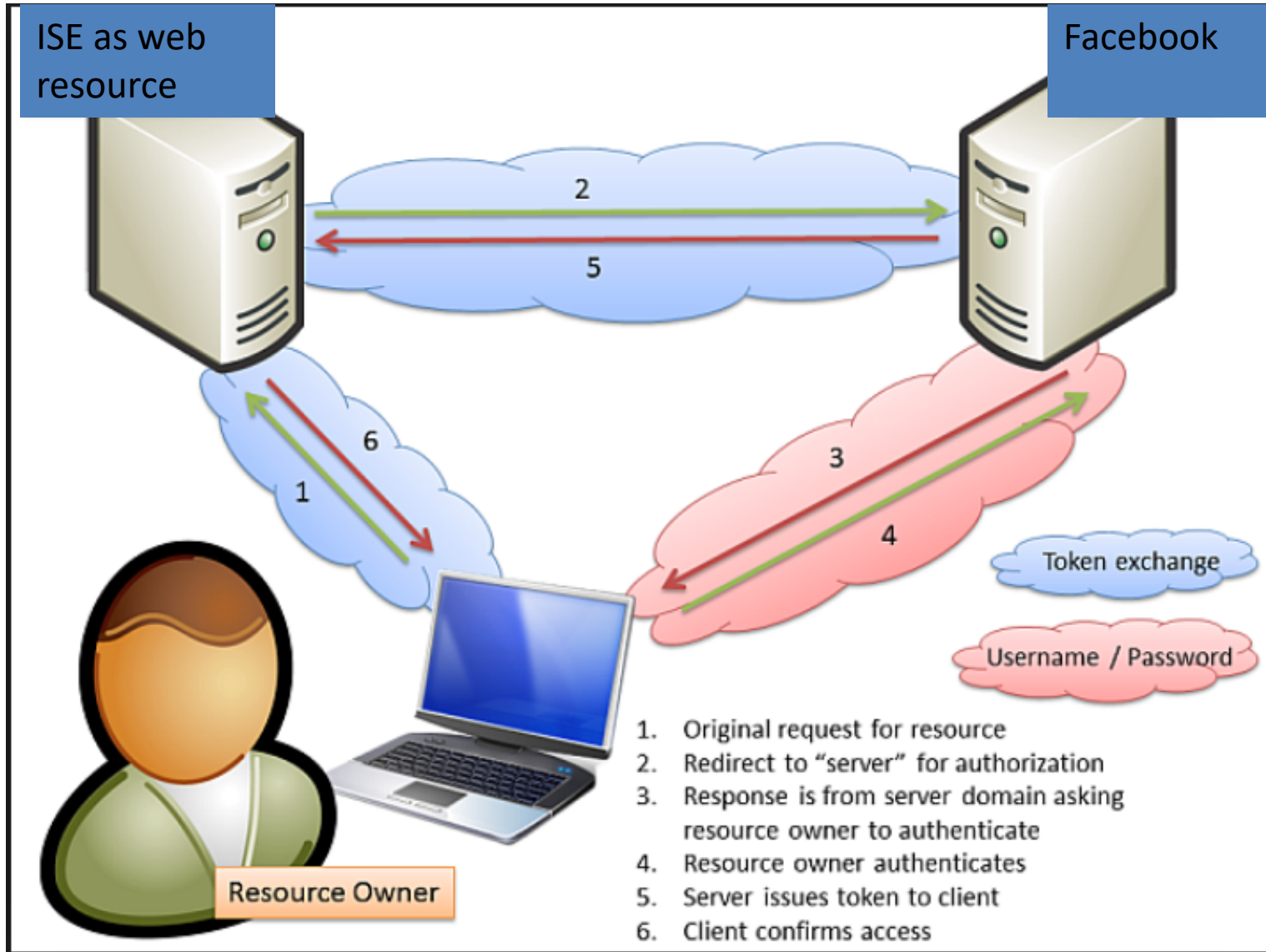
Which Social Media providers are supported?

Only Facebook social media is supported in ISE 2.3 release



OAuth flow

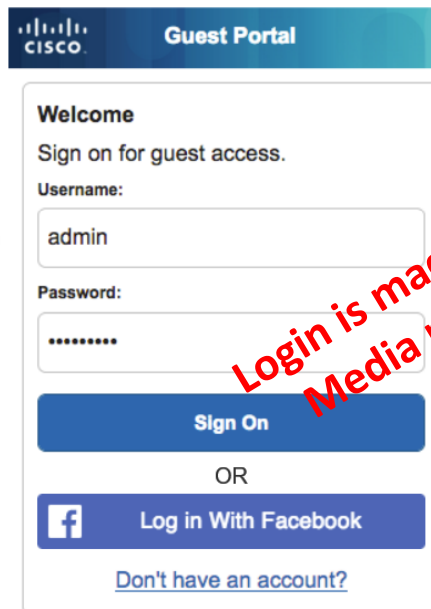
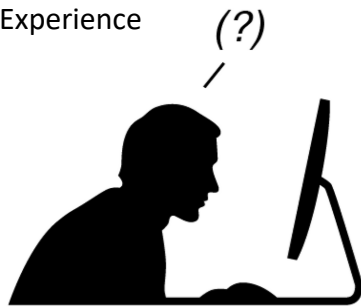
OAuth Flow



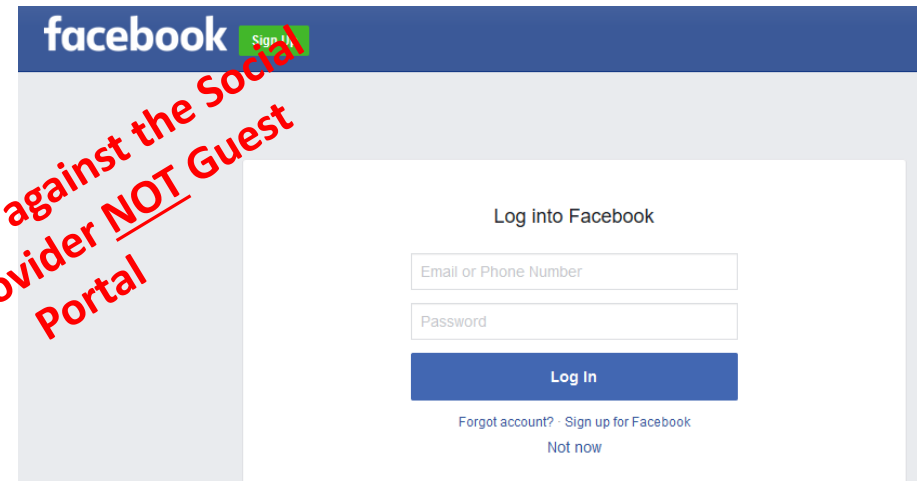
Guest OAuth Authentication

- ISE 2.3 allows performing authentication against Facebook only on CWA Guest flow with or w/o sponsor approval
- Authentication is made (as usual) via the browser
- Once user is authenticated, the flow continues as usual

User Experience

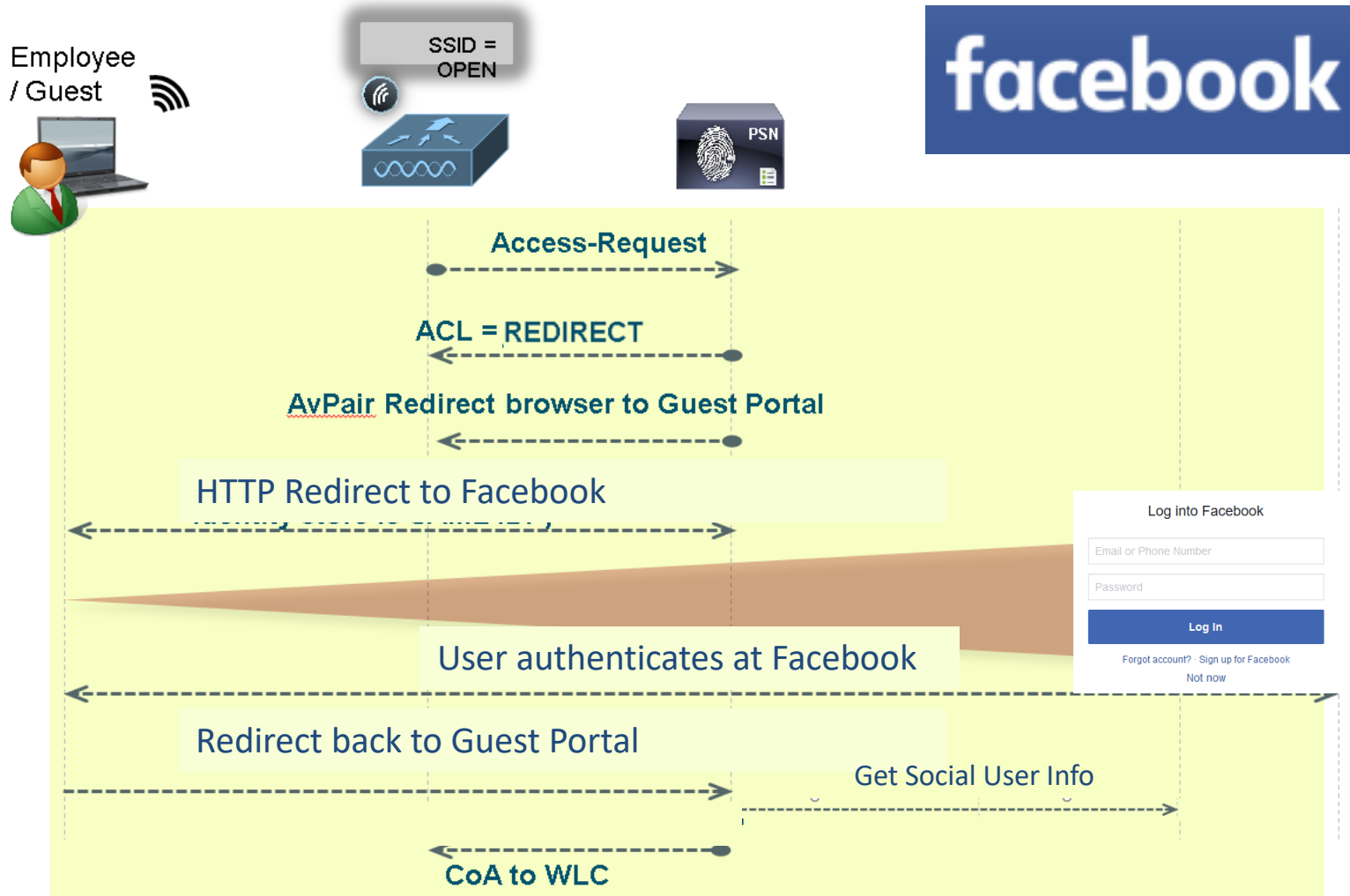


The screenshot shows the Cisco Guest Portal login interface. At the top, there is a Cisco logo and the text "Guest Portal". Below this, a "Welcome" message is followed by "Sign on for guest access." The form includes a "Username:" field with the text "admin" and a "Password:" field with masked characters. A blue "Sign On" button is positioned below the password field. Underneath, the word "OR" is centered. A blue button with the Facebook logo and the text "Log in With Facebook" is shown. At the bottom, there is a link that says "Don't have an account?".



The screenshot shows the Facebook login page. At the top, there is a blue header with the Facebook logo and a "Sign Up" button. Below this, the text "Log into Facebook" is centered. There are two input fields: "Email or Phone Number" and "Password". A blue "Log In" button is positioned below the password field. At the bottom, there are links for "Forgot account?", "Sign up for Facebook", and "Not now". A large red watermark is overlaid diagonally across the page, reading "Login is made against the Social Media provider NOT Guest Portal".

ISE 2.3 as a OAuth application – the flow



OAuth (Social media) Configurations

Using OAuth at ISE Portals - configuration steps

1. Create Facebook application (at Facebook)
2. Create Facebook Social Login (as external Identity Source)
3. Select Facebook Social Login at the Portal configuration
3. Update URI list of ISE deployment at Facebook site

Creating Facebook application

Go to: <https://developers.facebook.com/>

The screenshot shows the Facebook Developer Dashboard for an application named 'FirstSEApp'. The top navigation bar includes the app name, APP ID: 239243356550787, and a 'View Analytics' link. A dark sidebar on the left contains navigation options: Dashboard, Settings, Roles, Alerts, App Review, PRODUCTS, Facebook Login, and + Add Product. The main content area displays the app's profile, including a blue callout box that says 'Click to see analytics for this app.' Below this, the app's logo is shown, followed by the text 'FirstSEApp' and 'This app is public and available to all users [?]'. Further down, the API Version is listed as 'v2.8' and the App ID is '239243356550787'. The App Secret is displayed as a series of dots with a 'Show' button next to it.

Don't forget to make public:

This screenshot shows the same Facebook Developer Dashboard for 'FirstSEApp', but with a dialog box open. The dialog box is titled 'Make FirstSEApp public?' and contains a 'Yes' button followed by a checked checkbox. To the right of the checkbox, the text reads 'Your app is currently **live** and available to the public.' The sidebar on the left is visible, with 'App Review' highlighted. The top navigation bar shows the app name and APP ID: 239243356550787.

Creating Social login as Ext. Identity Store

▸ Identities Groups **External Identity Sources** Identity Source Sequences ▸ Settings

External Identity Sources

- ▶ Certificate Authentication Profile
 - Active Directory
 - LDAP
 - ODBC
 - RADIUS Token
 - RSA SecurID
- ▶ SAML Id Providers
- ▶ **Social Login**

Social Login > social_login1111

Social Login

Name *

Description

Type *

App ID *

Secret Key *

Portal

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

https://10.56.60.80:8443
 https://ahoroviz-dev-01.cisco.com:8443



Get the App ID and Secret Key from the newly created application at Facebook...

Selecting the Social Login in Guest Portal

Identity Services Engine Home Context Visibility Operations Policy Administration Work Centers

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 Settings

Guest Portals

Guest Types

Sponsor Groups

Sponsor Portals

Portal & Page 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 [Configure](#)

Show guest form after social login

Allow guests to change password after login

Allow the following identity-provider guest portal to be used for login [?](#)

Self-Registration Page Settings

Self-Registration Success Settings

Acceptable Use Policy (AUP) Page Settings

Guest Change Password Settings

Guest Device Registration Settings

Update URI list of ISE deployment at Facebook site

The screenshot shows the Cisco ISE management interface. On the left is a dark sidebar with navigation items: Dashboard, Settings, Roles, Alerts, App Review, PRODUCTS, Facebook Login (with sub-items Settings and Quickstart), and + Add Product. The main content area is titled 'Client OAuth Settings' and contains three sections, each with a toggle switch and descriptive text:

- Client OAuth Login**: Toggle set to 'No'. Description: 'Enables the standard OAuth client token flow. Secure your application and prevent abuse by locking down which token redirect URIs are allowed with the options below. Disable globally if not used. [?]'
- Web OAuth Login**: Toggle set to 'Yes'. Description: 'Enables web based OAuth client login for building custom login flows. [?]'
- Force Web OAuth Reauthentication**: Toggle set to 'No'. Description: 'When on, prompts people to enter their Facebook password in order to log in on the web. [?]'

Below these settings is a section titled 'Valid OAuth redirect URIs' with a yellow highlight. It contains two entries, each in a yellow box with a close button (X):

- `https://albarak.cisco.com:8443/`
- `https:10.56.24.62:8443/`

Red text 'Add ISE deployment URIs' is overlaid on the left side of the main content area, with a blue arrow pointing from it to the 'Valid OAuth redirect URIs' section.

Registration Form Settings

▼ **Registration Form Settings**

Assign to guest type ▼

Configure guest types at:
[Work Centers](#) > [Guest Access](#) > [Configure](#) > [Guest Types](#)

Account valid for: ▼ Maximum: 5 DAYS

Require a registration code

Fields to include	Required
<input checked="" type="checkbox"/> User name <small>i</small>	<input type="checkbox"/> Username field will not be shown during social login
<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 type="checkbox"/>
<input checked="" type="checkbox"/> Phone number	<input type="checkbox"/>
<input checked="" type="checkbox"/> Company	<input type="checkbox"/>
<input checked="" type="checkbox"/> Location	<input checked="" type="checkbox"/>

Guests can choose from these locations to set their time zone:

Username will be unchecked and disabled if Social Login only

WLC ACLs configuration

The screenshot shows the Cisco WLC Security configuration page for the Access Control List (ACL) named `ACL_REDIRRECT`. The configuration is under the `Access Control Lists > Edit` section. The `General` tab is selected, showing the Access List Name as `ACL_REDIRRECT` and Deny Counters as `0`.

The ACL rules are displayed in a table with the following columns: `Seq`, `Action`, `Source IP/Mask`, `Destination IP/Mask`, `Protocol`, `Source Port`, `Dest Port`, `DSCP`, `Direction`, and `Number of Hits`. A red box highlights the `Destination IP/Mask` column for the first rule, which is `31.13.0.0`. An arrow points from this box to a text box labeled "Facebook IP address".

Seq	Action	Source IP/Mask	Destination IP/Mask	Protocol	Source Port	Dest Port	DSCP	Direction	Number of Hits
<u>1</u>	Permit	0.0.0.0 /	31.13.0.0 /	Any	Any	Any	Any	Any	2485
<u>2</u>	Permit	0.0.0.0 /	255.255.0.0 /	Any	Any	Any	Any	Any	3031
<u>3</u>	Permit	31.13.0.0 /	0.0.0.0 /	Any	Any	Any	Any	Any	0
<u>4</u>	Permit	255.255.0.0 /	0.0.0.0 /	TCP	Any	Any	Any	Any	0
		0.0.0.0 /	10.56.62.70 /	TCP	Any	Any	Any	Any	0
		0.0.0.0 /	255.255.255.255 /	TCP	Any	Any	Any	Any	0

- Should open up facebook.com using name based ACLs

Q&A

- Questions & Answers

