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
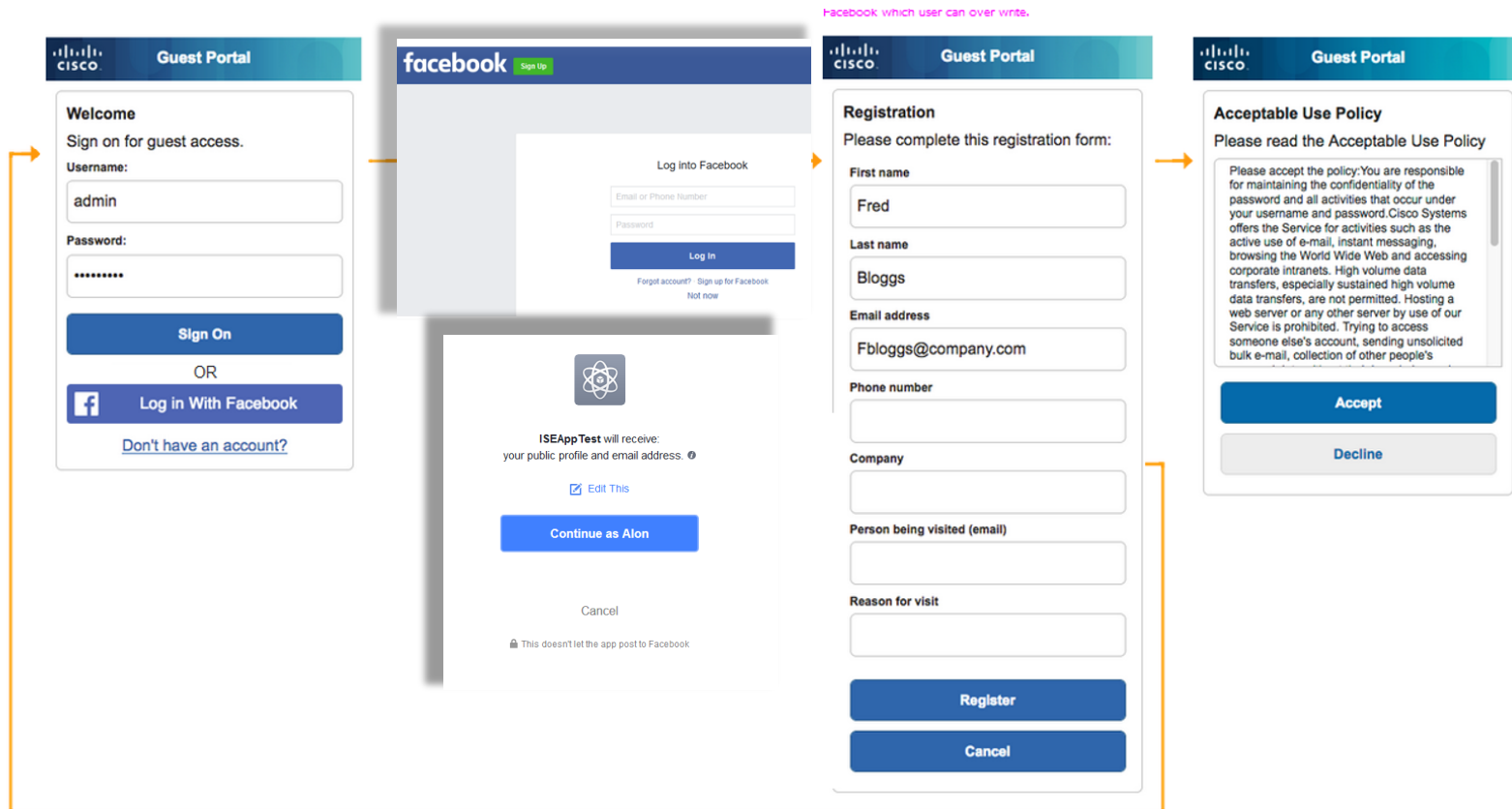
social media flows

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

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)

More info
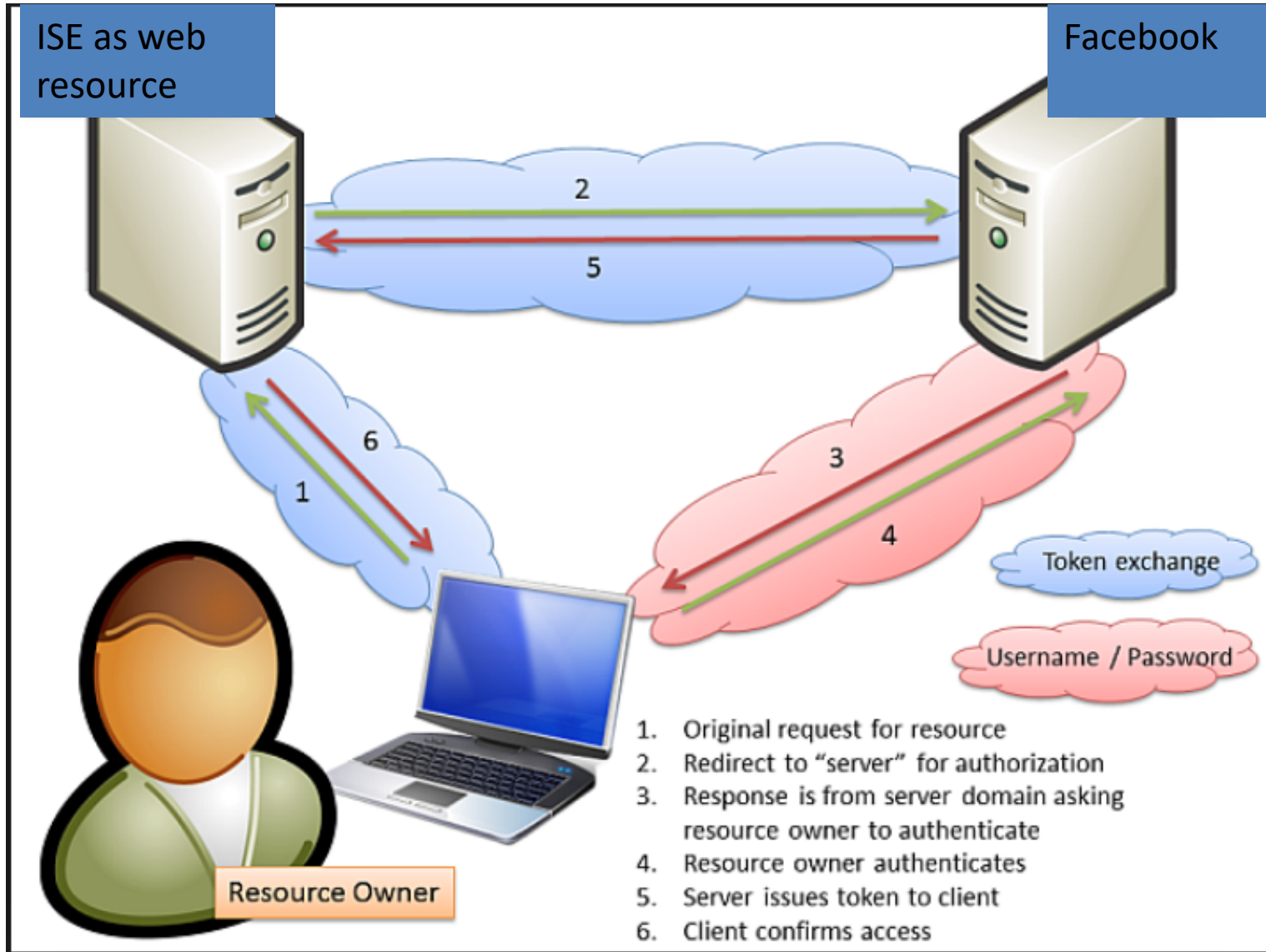
- how-to guide and FAQ

- 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

ISE as web resource

Facebook

Token exchange

Username / Password

1. Original request for resource
2. Redirect to "server" for authorization
3. Response is from server domain asking resource owner to authenticate
4. Resource owner authenticates
5. Server issues token to client
6. Client confirms access

Resource Owner
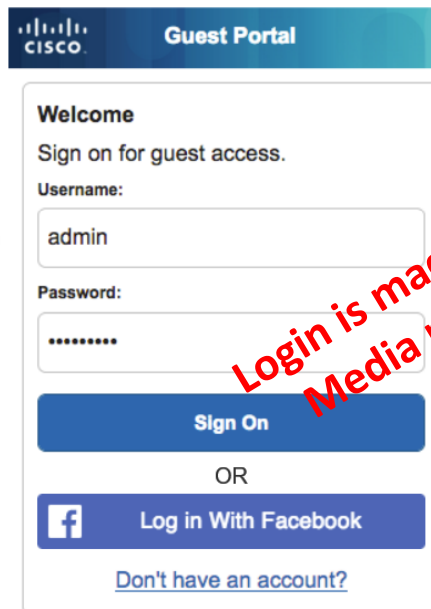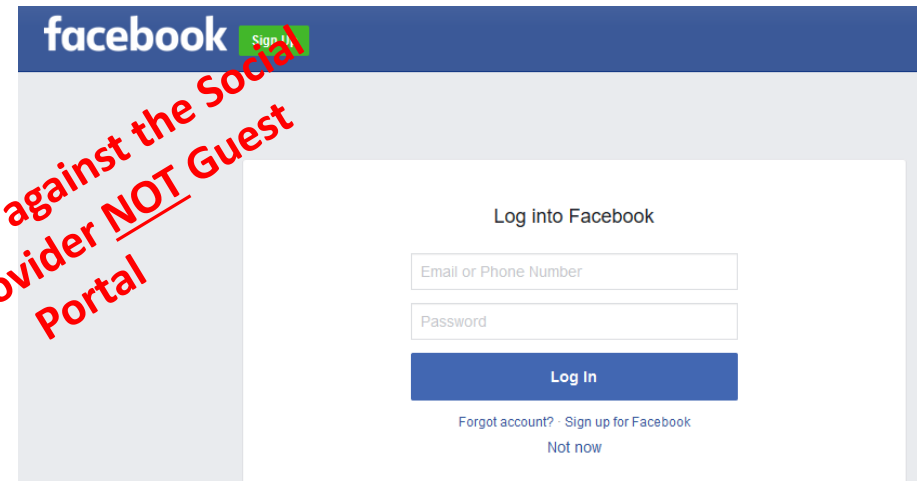
Guest OAuth Authentication

- 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

Login is made against the Social Media provider NOT Guest Portal

ISE 2.3 as a OAuth application – the flow
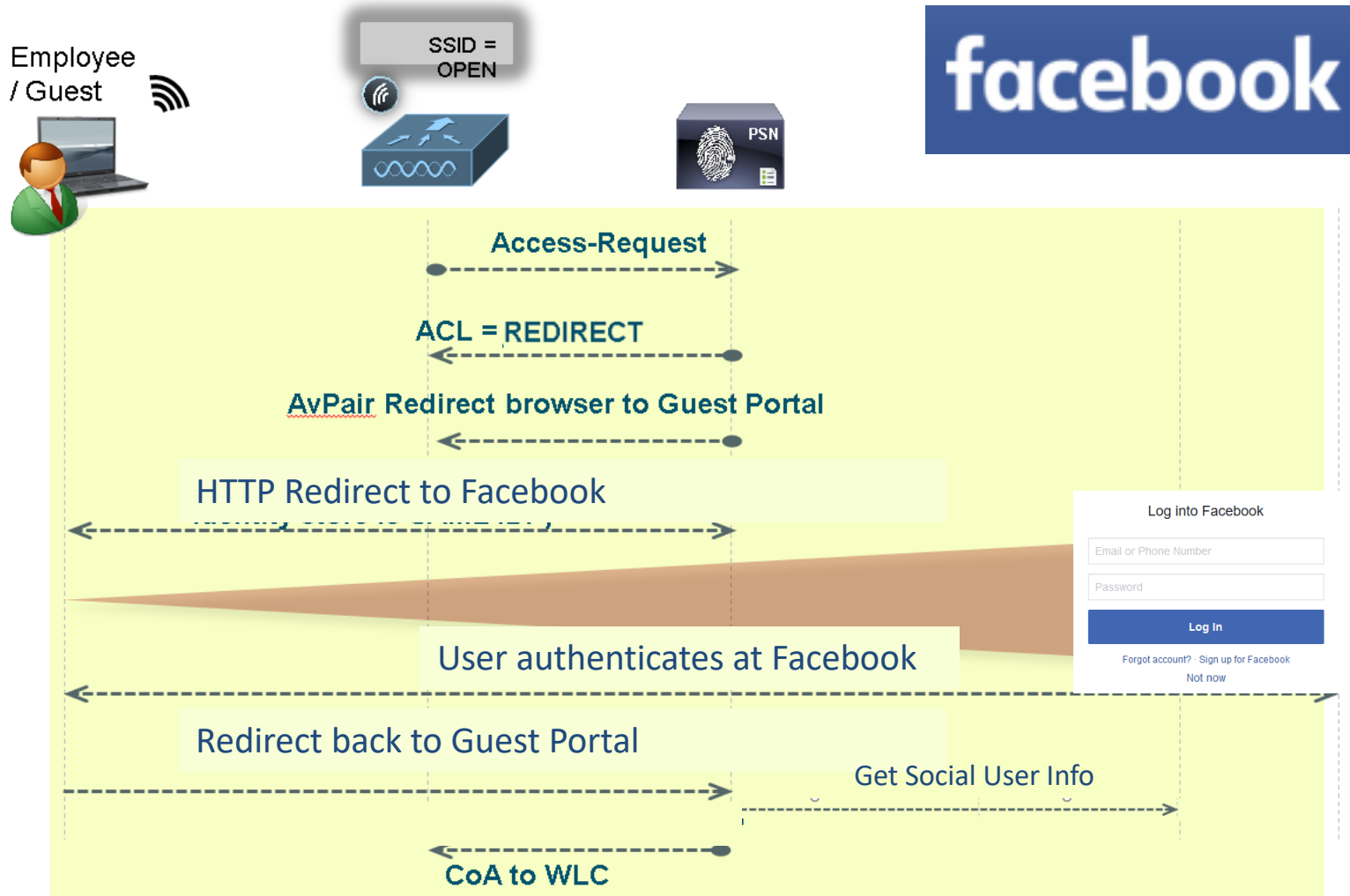
OAuth (Social media) Configurations

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/

Don't forget to make public:

Creating Social login as Ext. Identity Store

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

Selecting the Social Login in Gust Portal

Update URI list of ISE deployment at Facebook site

Dashboard
Settings
Roles
Alerts
App Review

PRODUCTS

Facebook Login

  Settings
  Quickstart

+ Add Product

Add ISE deployment URIs

Client OAuth Settings

| No | Client OAuth Login |
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. [?]

| Yes | Web OAuth Login |
Enables web based OAuth client login for building custom login flows. [?]

| No | Force Web OAuth Reauthentication |
When on, prompts people to enter their Facebook password in order to log in on the web. [?]

| No | Embedded Browser OAuth Login |
Enables browser control redirect uri for OAuth client login. [?]

Valid OAuth redirect URIs

https://albarak.cisco.com:8443/ ✕   https:10.56.24.62:8443/ ✕

Registration Form Settings

WLC ACLs configuration

- Should open up facebook.com using name based ACLs

Q&A

- Questions & Answers

CISCO