



# Technical Guide

## Social Media Authentication

Released: 2018-08-21

Doc Rev No: R7

## Table of Contents

<b>1.</b>	<b>Introduction .....</b>	<b>3</b>
<b>2.</b>	<b>Overview .....</b>	<b>4</b>
<b>3.</b>	<b>Social Media Authentication .....</b>	<b>5</b>
3.1	Sign in with Facebook Account .....	5
3.2	Sign in with LINE Account .....	12
3.3	Verification.....	12
<b>4.</b>	<b>Controller Configuration .....</b>	<b>14</b>
4.1	Service Zone Configuration.....	14
4.2	Social Media Login Mechanism and Limitation .....	15
<b>5.</b>	<b>Social Account Log .....</b>	<b>16</b>
5.1	User Events .....	16
5.2	Social Media Account Quota List .....	16
5.3	Social Media Account Information .....	17
<b>6.</b>	<b>Conclusion .....</b>	<b>17</b>
<b>7.</b>	<b>Remarks .....</b>	<b>18</b>

# ***1.Introduction***

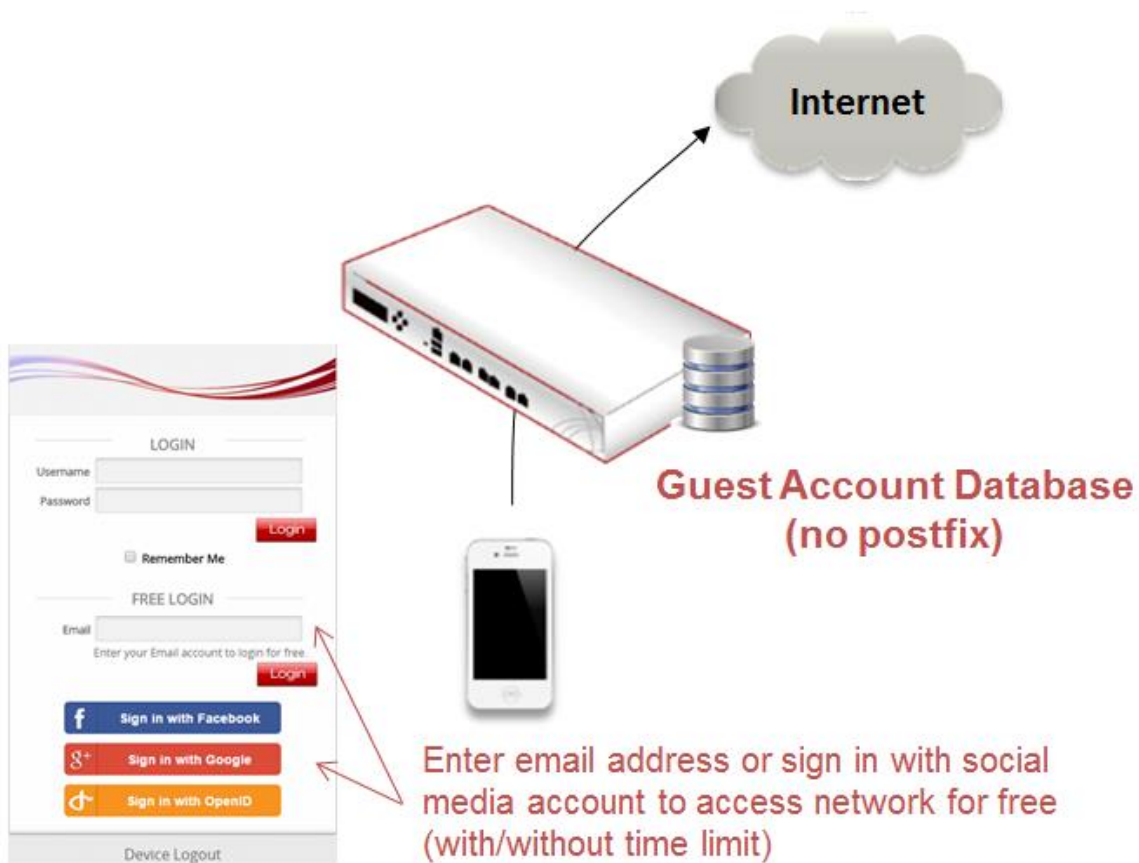
This technical guide is aimed at explaining the practical setup flow of Social Media Authentication on the Controller. Using social media accounts for authentication has become an upcoming trend in public Wi-Fi networks. The Social Media Authentication feature on the Controller allows users to login with their existing social media accounts such as Facebook for Internet access without having to provide other credentials.

With this technical guide, network administrators can easily setup and configure for Social Media Authentication on the Controller for providing free Wi-Fi service to users.

## 2. Overview

The Social Media Authentication feature on the Controller supports login through a variety of social media including Facebook, LINE, Weibo, OpenID and VK. Administrators can set usage constraints such as access time, access limit per day and reactivation time. In addition, users who login using social media authentication will be assigned to a group as preset by the administrator, and a group policy can be enforced on these users to further govern their Wi-Fi usage.

Social Media Authentication, along with Guest (Free) Authentication, are two authentication options provided on the Controller that the administrators can use to provide free Wi-Fi service to short-term users. See the diagram below for how these two login options will display on the default General Login Page.



### 3. Social Media Authentication

Controller's Social Media Authentication allows Wi-Fi users to access internet without going through the tedious process of account registration. When a user chooses a specific social media for login on the login page, he/she will be redirected to the login page of that social media. Once the user logs in successfully with their social media account, they will be redirected to the login successful page shown by the Controller. Communication between the Controller and the social media supported is through API. Thus, the administrator has to apply for an application from the social media's developers websites, and enter the API credentials into the Controller.

The image displays two screenshots of a web-based configuration interface for Social Media Authentication.

**Top Screenshot: Social Media Login Configuration**

- Navigation:** SYSTEM, **USERS**, DEVICES, NETWORK, UTILITIES, STATUS.
- Left Menu:** Groups, Authentication Servers, Internal Authentication, **External Authentication**, POP3, LDAP, RADIUS, NT Domain, SIP, **Social Media**, On-Demand Accounts, Schedule, Policies, Blacklists, Privilege Lists, Additional Controls.
- Main Content:**
  - Social Media Login:** When Social Media Login is enabled, the controller collects information from the clients. Please enable Disclaimer or customized login page to include claims and reminders.
  - Group:** Visitor (dropdown)
  - Social Media Account Information:** View (button)
  - Social Media Account Access Time:** Unlimited (selected), Limited (radio button)
  - Punishment List:** View (button)
  - Buttons:** Apply, Cancel
- Section Header:** Social API Credentials

**Bottom Screenshot: Social API Credentials Configuration**

- Navigation:** SYSTEM, **USERS**, DEVICES, NETWORK, UTILITIES, STATUS.
- Left Menu:** Same as the top screenshot.
- Main Content:**
  - Punishment List:** View (button)
  - Buttons:** Apply, Cancel
  - Social API Credentials:**
    - Line Login:** [checkbox]
    - Line App ID:** [text input]
    - Line App Secret:** [text input]
    - Facebook Login:** [checkbox]
    - Facebook App ID:** [text input]
    - Facebook App Secret:** [text input]
    - Google+ Sign-in:** [checkbox]
    - Google Project Client ID:** [text input]
    - Google Project Client Secret:** [text input]
    - Upload JSON data (optional):** Browse... No file selected.
    - Weibo Login:** [checkbox]
    - Weibo App ID:** [text input]
    - Weibo App Secret:** [text input]
    - OpenID Login:** [checkbox]
  - Buttons:** Apply, Cancel

#### 3.1 Sign in with Facebook Account

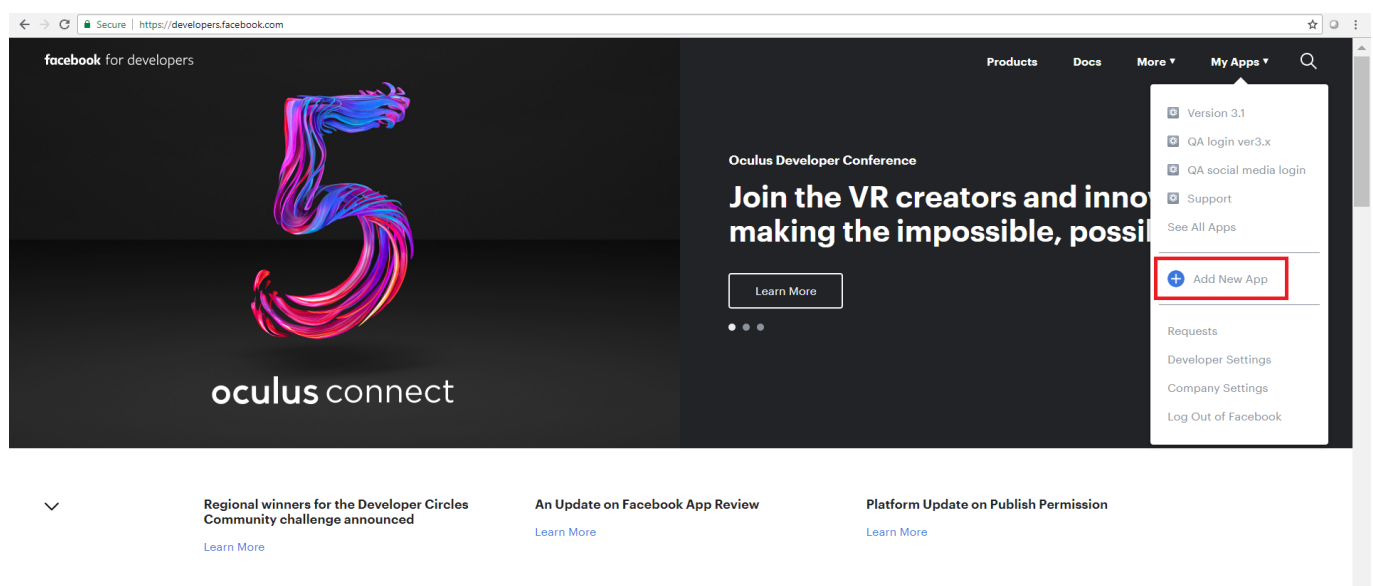
Administrators are to visit the Facebook for Developers website (<https://developers.facebook.com/>) to apply for a "Facebook Login" App. Administrators should first login to Facebook Developers with a

registered Facebook Account if they're new to the platform. To create an App, follow the instructions below. The instructions given here are based on Facebook API Version 3.1. Different settings may apply for other API Versions.

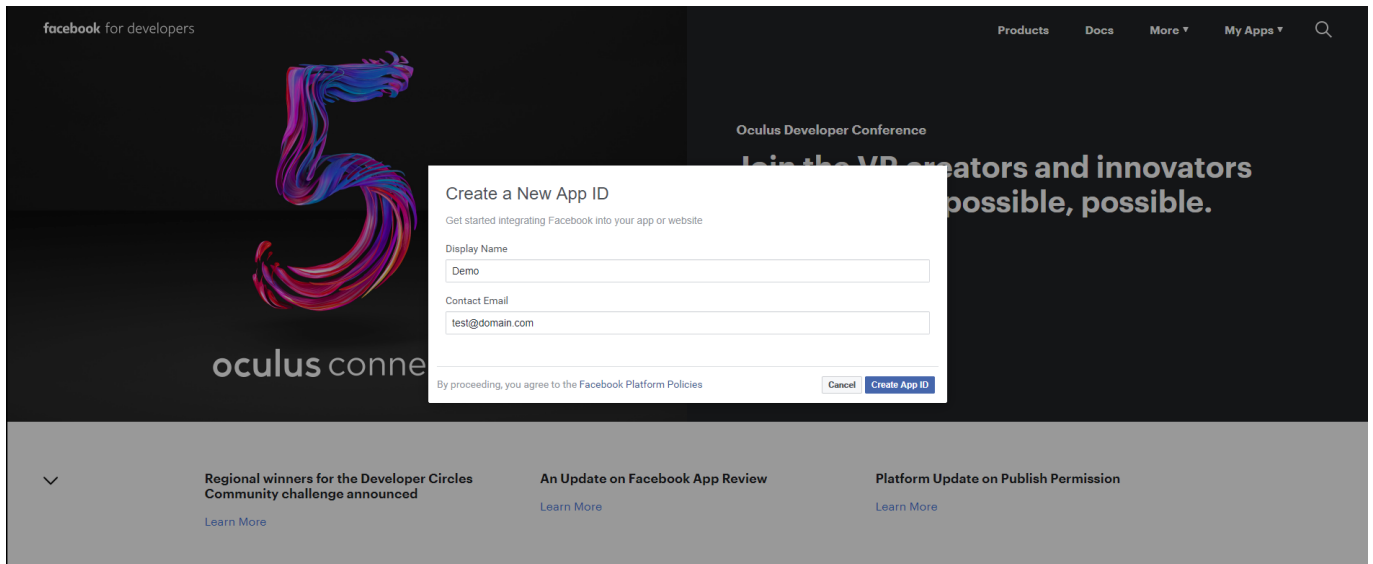
There are two things to note here. For newer API versions such as v3.1, the use of HTTPS for Redirect URIs and the JavaScript SDK is mandatory, and the use of HTTPS will become mandatory for all apps on October 6, 2018 according to Facebook (<https://developers.facebook.com/docs/facebook-login/security/>). In addition, a valid SSL/TLS certificate has to be obtained and uploaded to the Controller for use.

On the upper right corner, move the cursor to "My Apps" for the drop-down menu to be displayed. Since the account being used for demonstration here has already had Apps created, we will click on "Add New App".

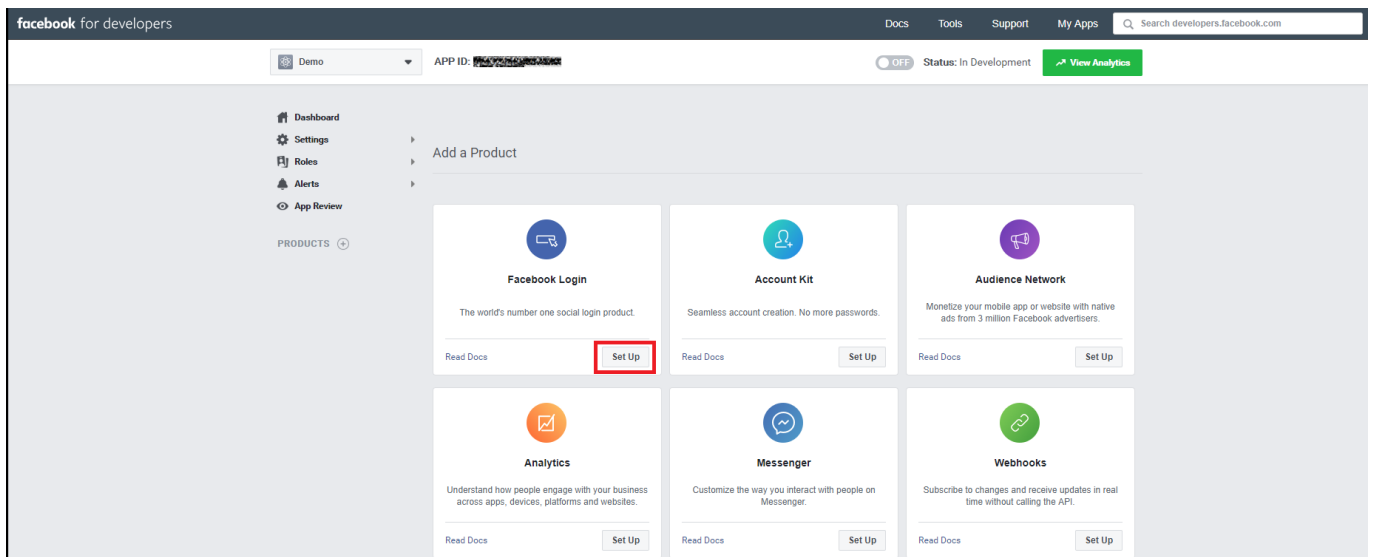
1. Under "My Apps", click on "Add New App"



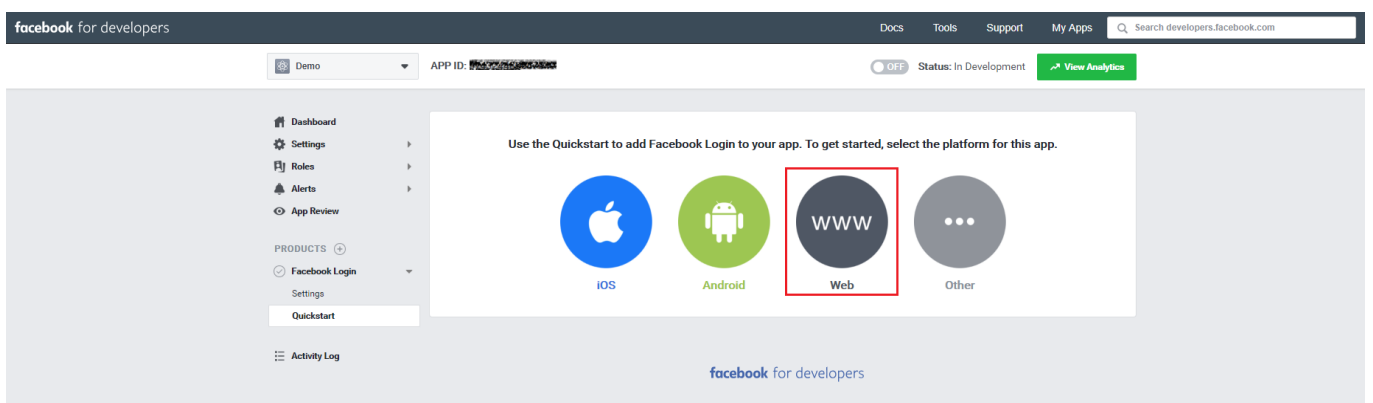
2. In the pop-up window, fill in preferred Display Name and Contact Email to create App ID.



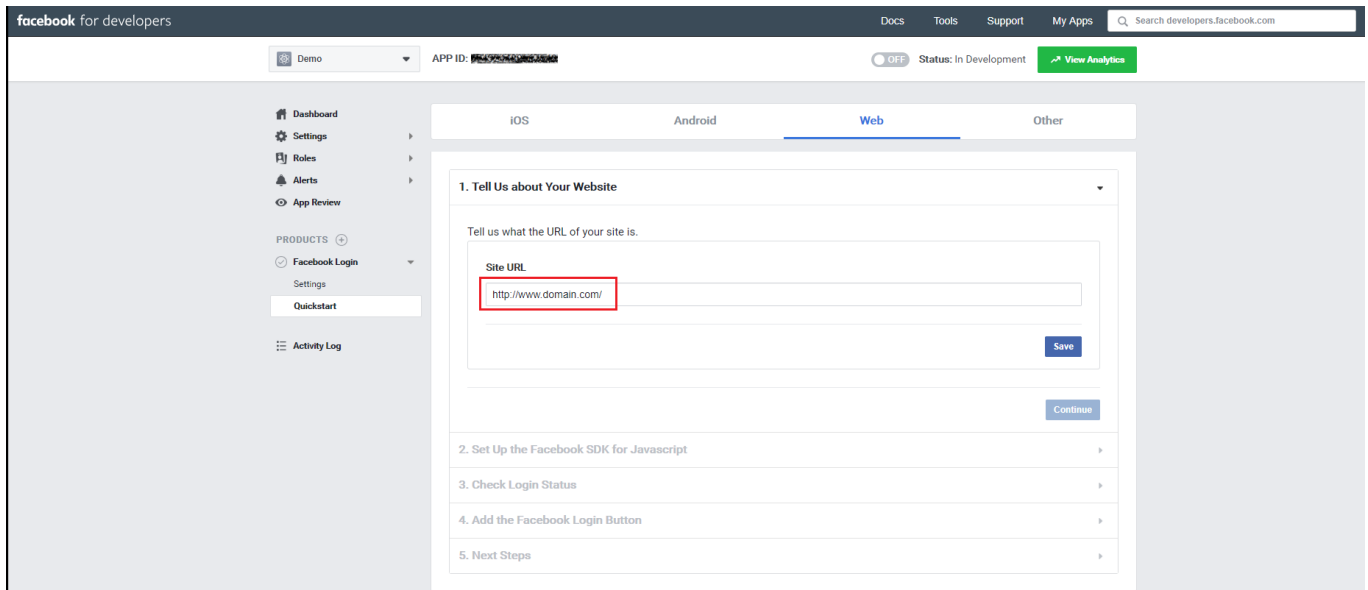
3. Add a Facebook Login by clicking on Set Up in the Facebook Login box.



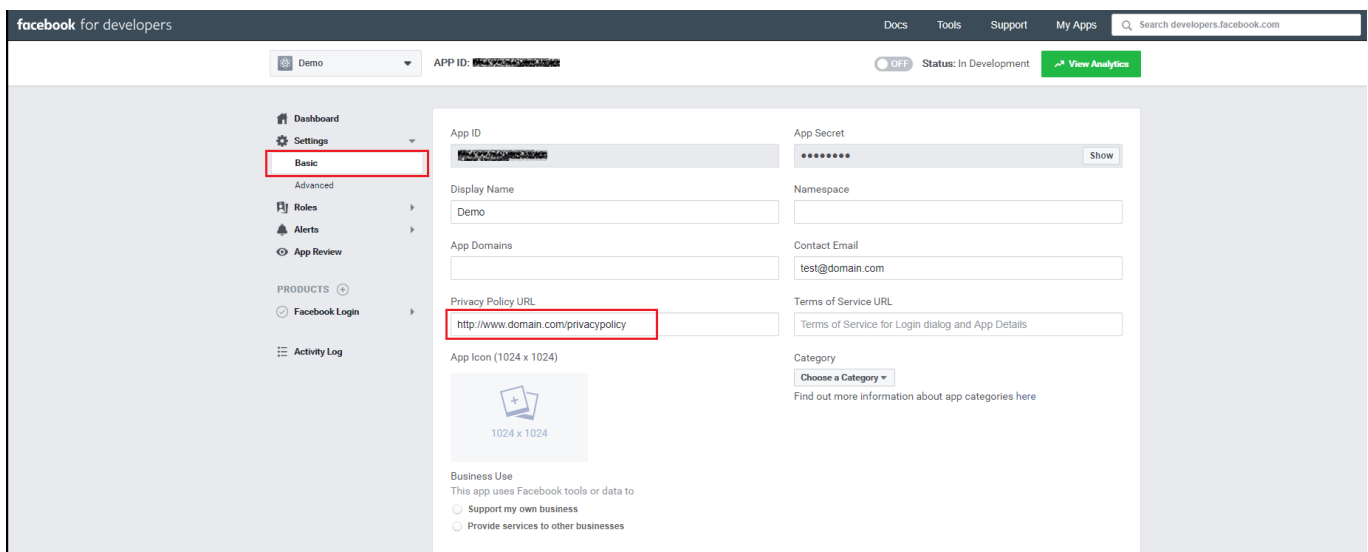
4. Select Web



5. Enter URL of one's website. This could be the domain name on the SSL/TLS certificate to be used.

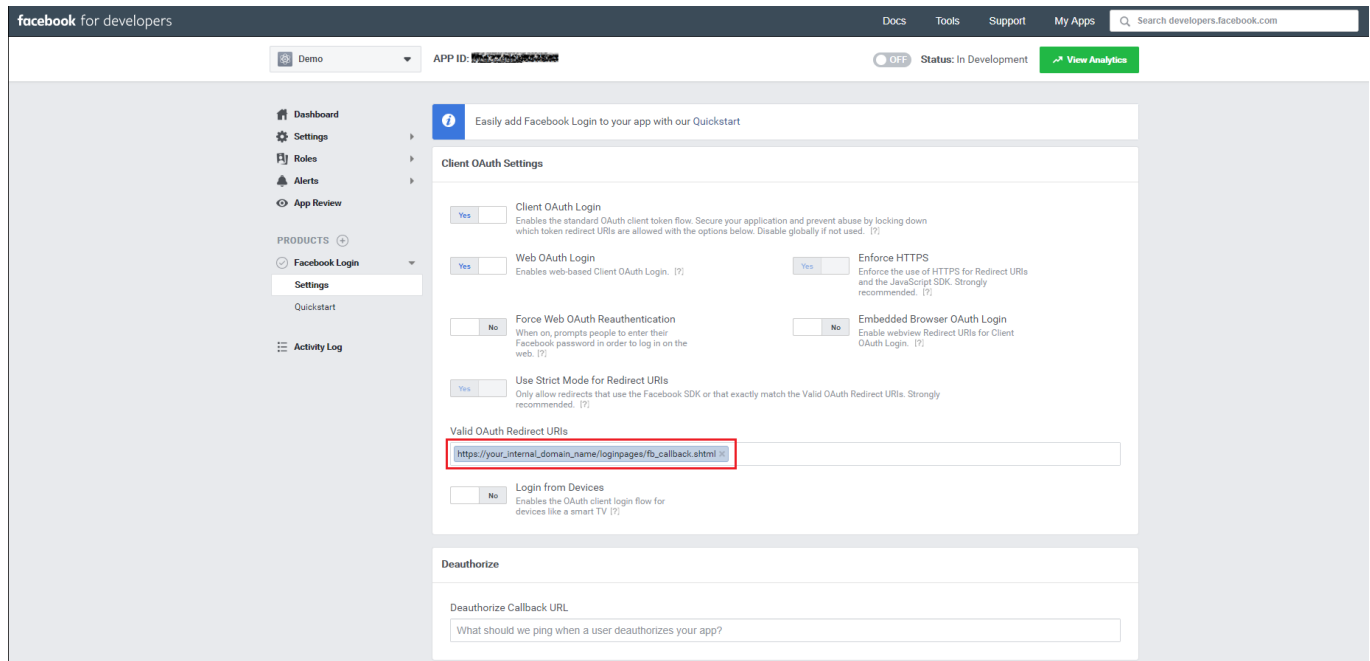


6. Go to Settings > Basic and enter one's own Privacy Policy URL. Facebook would check if the URL is valid.

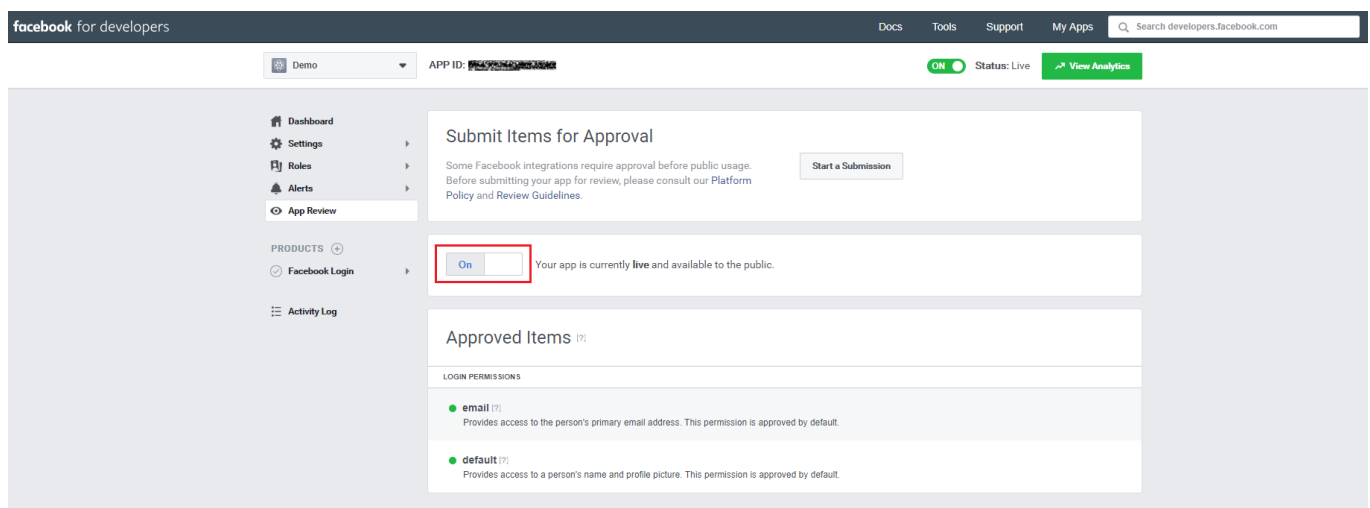


7. Go to Facebook Login > Settings and add [https://your internal domain name/loginpages/fb\\_callback.shtml](https://your internal domain name/loginpages/fb_callback.shtml) to the "Valid OAuth redirect URIs". Remember to use the internal domain name on the valid SSL/TLS certificate that will be uploaded to the Controller.

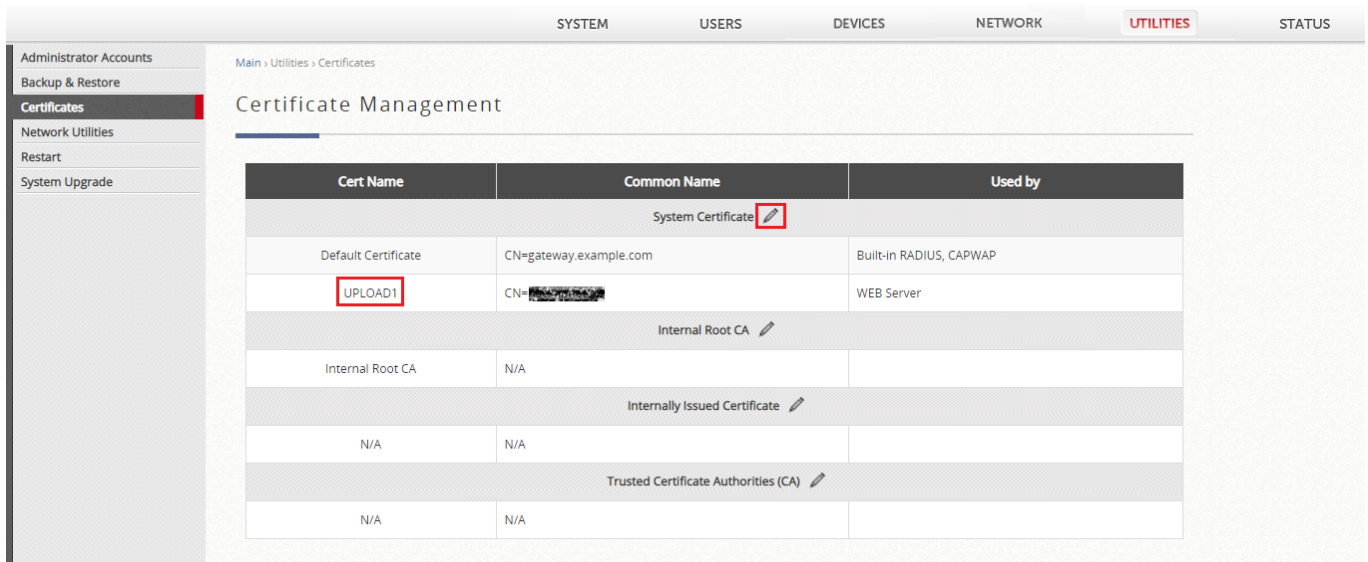




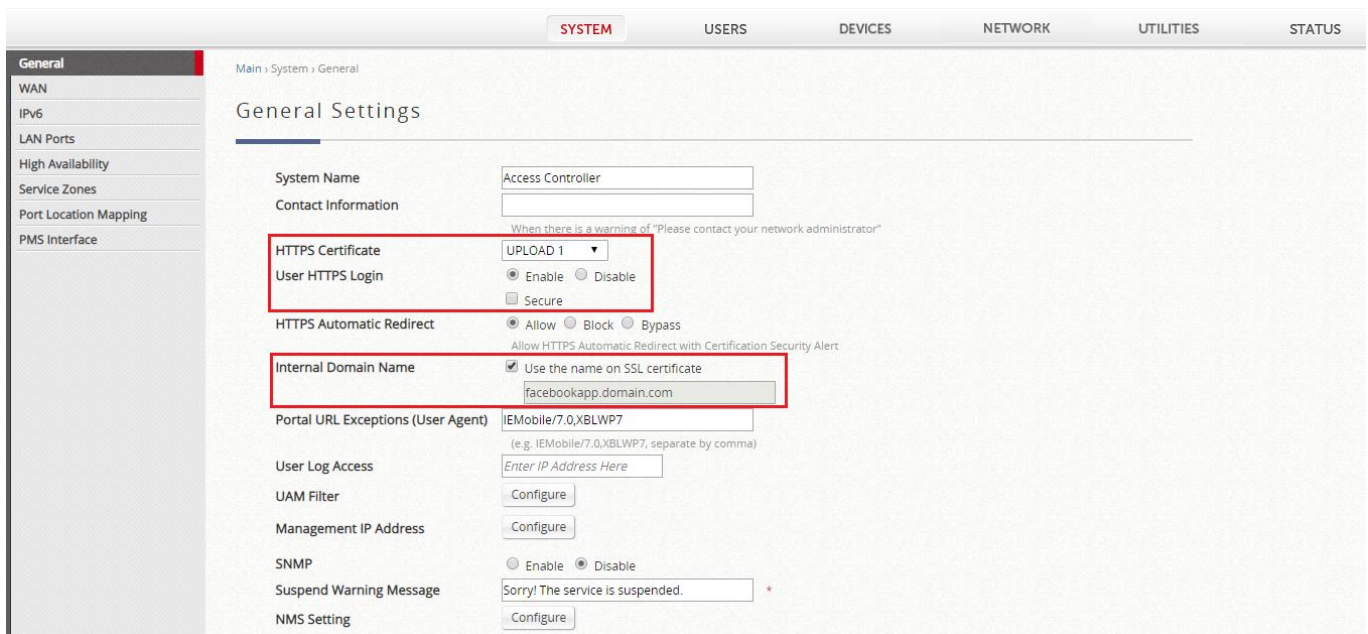
8. Go to the “App Review” page and make the App public.



9. Now, from the Controller’s WMI, go to **Utilities > Certificates** and upload a valid SSL/TLS certificate. Once uploaded, the certificate will be displayed as UPLOAD1 if it is the first uploaded certificate.



10. Go to **System > General Settings**. Choose UPLOAD 1 as HTTPS Certificate and enable User HTTPS Login. For Internal Domain Name, use the name on SSL certificate, or manually type in the internal domain name if a wildcard certificate is used. Reboot the Controller as asked.



11. Now return to the Facebook Login App that has been created. Go to Settings > Basic to copy the App ID and Secret.

facebook for developers

Docs Tools Support My Apps Search developers.facebook.com

Demo APP ID: [REDACTED] ON Status: Live View Analytics

Dashboard Settings Basic Advanced Roles Alerts App Review PRODUCTS Facebook Login Activity Log

App ID [REDACTED] App Secret [REDACTED] Show

Display Name Demo Namespace

App Domains Contact Email test@domain.com

Privacy Policy URL http://www.domain.com/privacypolicy Terms of Service URL Terms of Service for Login dialog and App Details

App Icon (1024 x 1024)

Business Use This app uses Facebook tools or data to Support my own business Provide services to other businesses

12. From the WMI of the Controller, go to **Users > External Authentication > Social Media**, enable Facebook Login and paste the App ID and Secret.

SYSTEM

USERS

DEVICES

NETWORK

UTILITIES

STATUS

Groups

Authentication Servers

Internal Authentication

External Authentication

POP3

LDAP

RADIUS

NT Domain

SIP

Social Media

On-Demand Accounts

Schedule

Policies

Blacklists

Privilege Lists

Additional Controls

Main > Users > External Authentication > Social Media Login

When Social Media Login is enabled, the controller collects information from the clients. Please enable Disclaimer or customized login page to include claims and reminders.

Social Media Login

Group

Group 1

Social Media Account Information

View

Social Media Account Access Time

☒ Unlimited ☐ Limited

Punishment List

View

Apply

Cancel

Social API Credentials

Line Login

☐

Line App ID

Line App Secret

Facebook Login

☒

Facebook App ID

\*

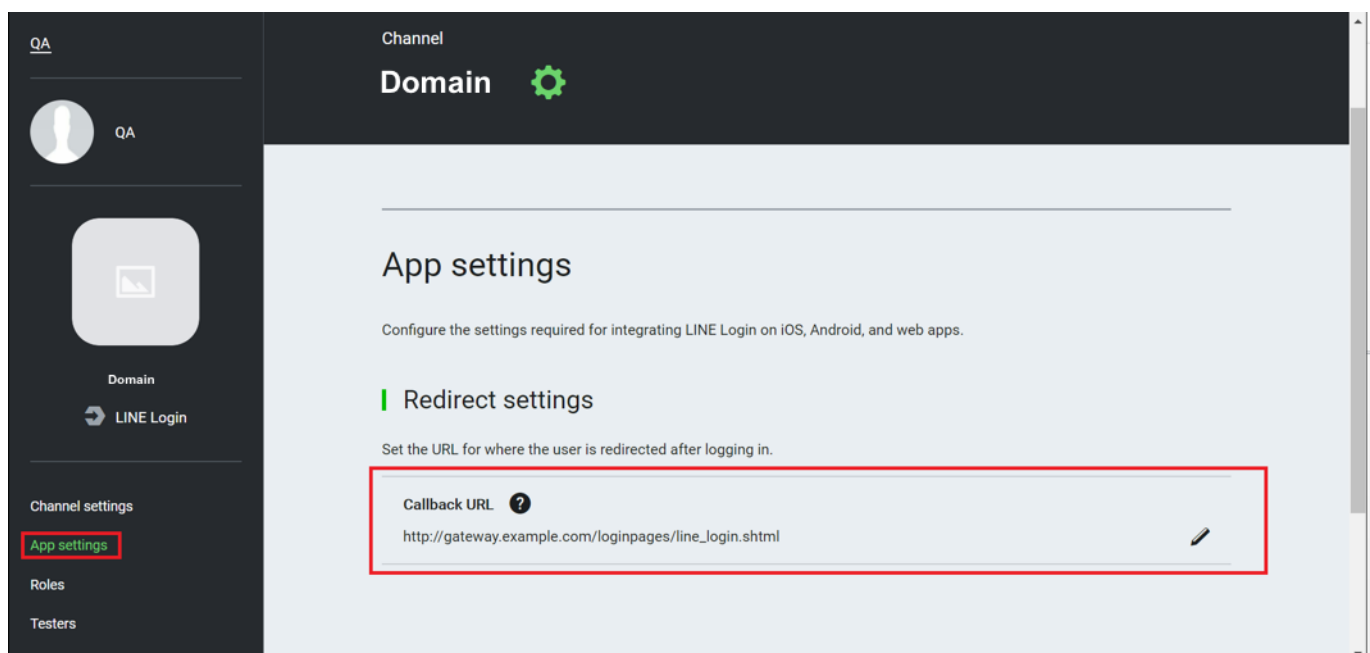
Facebook App Secret

\*

13. Make sure to enable Facebook Login in the appropriate Service Zones.

## 3.2 Sign in with LINE Account

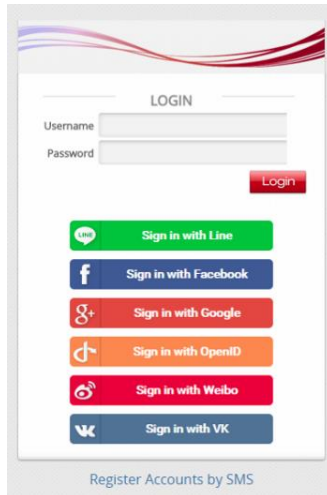
Administrators are to visit the LINE developers website (<https://developers.line.me/>) to create a “LINE Login” product. Administrators should first login with their registered LINE account, and they can start to create a “LINE Login” product. Please refer to the instructions provided on the website (<https://developers.line.me/en/docs/line-login/getting-started/>) for the setup. Note that in App settings, please set the Callback URL to [http://gateway.example.com/loginpages/line\\_login.shtml](http://gateway.example.com/loginpages/line_login.shtml) if the Internal Domain Name on the Controller is left at default. If the Internal Domain Name has been changed, please set the Callback URL to [http://your internal domain name/loginpages/line\\_login.shtml](http://your internal domain name/loginpages/line_login.shtml).



## 3.3 Verification

As mentioned previously, when a user chooses a specific social media for login on the login page, he/she will be redirected to the login page of that social media. After logging in with their social media account, the user will be asked to give permission to the App to collect certain account information. The user has to agree for successful login.

## Facebook Login flow



LOGIN

Username

Password

Login

Sign in with Line

Sign in with Facebook

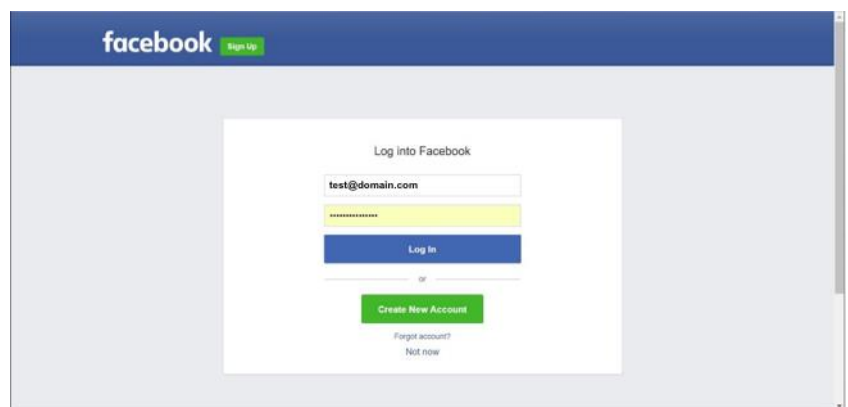
Sign in with Google

Sign in with OpenID

Sign in with Weibo

Sign in with VK

Register Accounts by SMS



facebook Sign Up

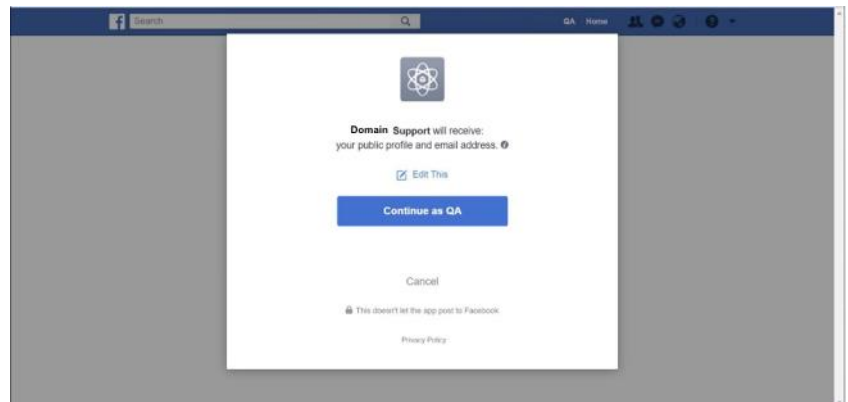
Log into Facebook

test@domain.com

Log In

Create New Account

Forgot account? Not now



Domain Support will receive:  
your public profile and email address.

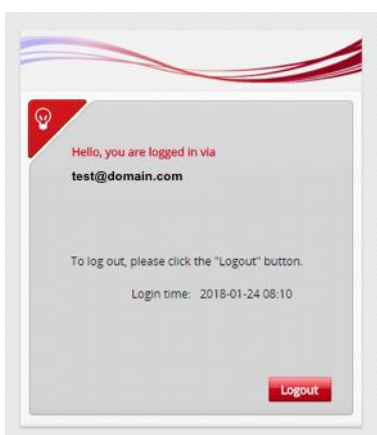
☒ Edit This

Continue as QA

Cancel

This doesn't let the app post to Facebook

Privacy Policy



Hello, you are logged in via  
test@domain.com

To log out, please click the "Logout" button.

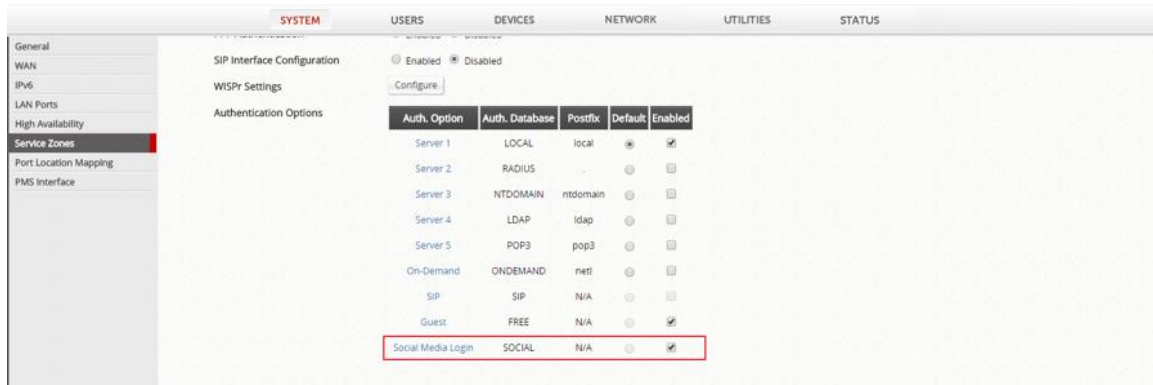
Login time: 2018-01-24 08:10

Logout

## 4. Controller Configuration

### 4.1 Service Zone Configuration

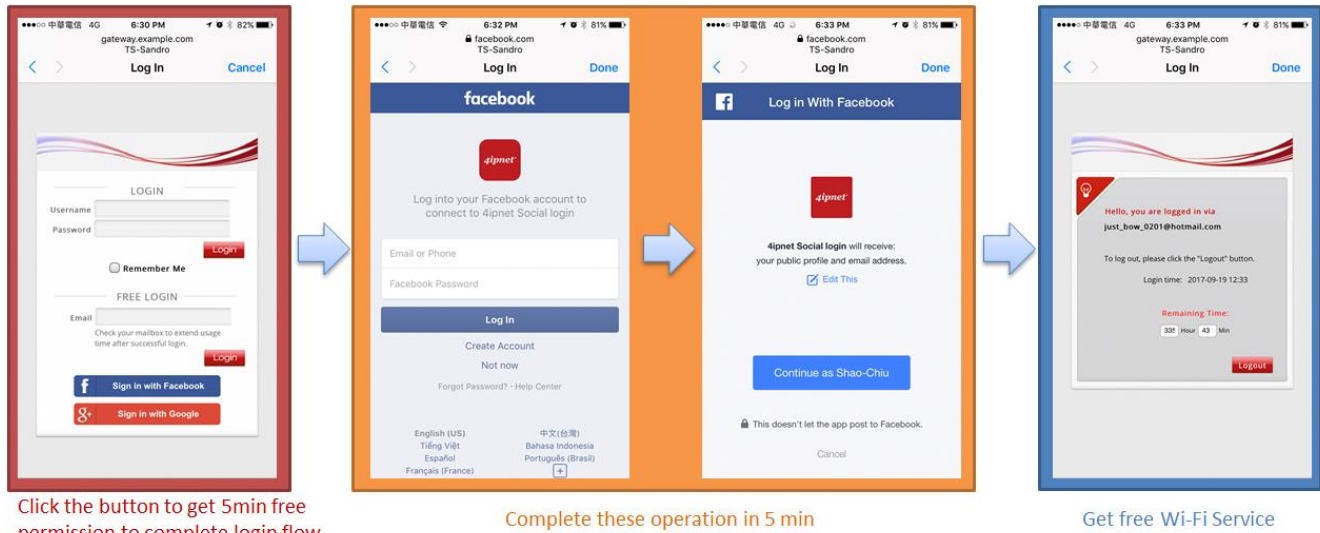
To enable Social Media Authentication, go to **System > Service Zone > Configuration**, and enable Social Media Login under “Authentication Options”.



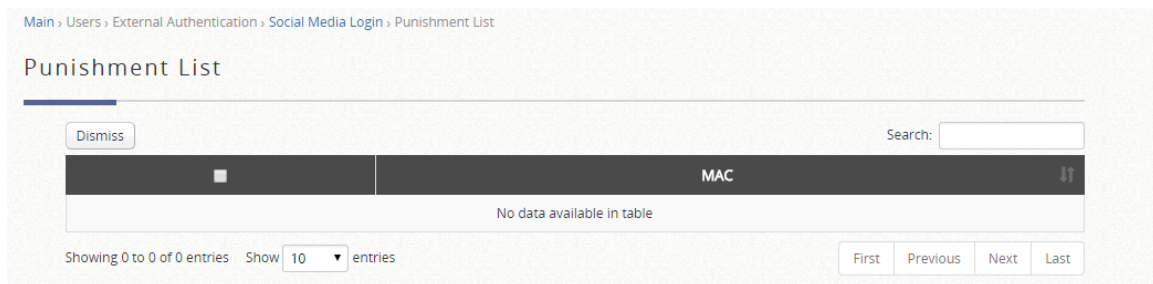
Consequently, when users connect to the Service Zone, the corresponding Login Page will display Social Media Login options. In Controller, MAC addresses will be checked to avoid malicious use of free access.

## 4.2 Social Media Login Mechanism and Limitation

In firmware version v3.42.00 or later versions, when a user clicks on any of the social media sign-in buttons, he/she will be given 5 minutes of free Internet access.



If the user clicked on the sign-in button for one of the social media but did not complete the login process three times, the user will be blocked for 15 minutes as punishment, during which he/she will not be able to login using the same option. Administrators can check user status from WMI (**Users > External Authentication > Social Media Login > Punishment List**) and dismiss the punishment manually.





## 5. Social Account Log

### 5.1 User Events

Logs on User Events can be saved for up to 30 days. Administrators can select the begin and end dates from the calendar to filter User Events, and they can click on the Download button to download the displayed User Events into a comma separated .txt file. Besides user events for social media accounts, user events for other accounts such as Local, On-Demand and Guest can also be displayed in User Events with user related information such as Event, Email address, IP address, MAC address and etc.

Main > Status > Logs and Reports > User Events

### User Events

Display Mode Configure

From 2017-09-19 Display

To 2017-09-21

User Type ☐ Local ☐ On-Demand ☐ Guest ☐ Roaming Out ☐ Roaming In ☐ External ☒ Social

Download Type Search

Type	Date	Name	IP	MAC	Event	Remark
SOCIAL	2017-09-19 12:15:00 +0200	70:70:0D:B4:EB:84@SOCIAL	192.168.30.13	70:70:0D:B4:EB:84	Initiate	facebook
SOCIAL	2017-09-19 12:15:49 +0200	john.jones_1234@facebook.com	192.168.30.13	70:70:0D:B4:EB:84	Login	facebook
SOCIAL	2017-09-19 12:28:04 +0200	john.jones_1234@facebook.com	192.168.30.13	70:70:0D:B4:EB:84	Admin-Reset	facebook
SOCIAL	2017-09-19 12:31:58 +0200	70:70:0D:B4:EB:84@SOCIAL	192.168.30.13	70:70:0D:B4:EB:84	Initiate	facebook
SOCIAL	2017-09-19 12:32:56 +0200	70:28:8B:46:6C:6A@SOCIAL	192.168.30.76	70:28:8B:46:6C:6A	Initiate	facebook
SOCIAL	2017-09-19 12:33:21 +0200	john.jones_1234@facebook.com	192.168.30.13	70:70:0D:B4:EB:84	Login	facebook
SOCIAL	2017-09-19 12:37:58 +0200	70:28:8B:46:6C:6A@SOCIAL	192.168.30.76	70:28:8B:46:6C:6A	Session-Timeout	facebook

(Total:7) First Prev Next Last Go to Page 1 (Page:1/1) Row per Page: 20

### 5.2 Social Media Account Quota List

The Social Media Account Quota List displays the status for online social users who are logged in by their own social media accounts (Email Address or Unique ID), along with clients' MAC Addresses, Valid Time and corresponding Allowance. Administrators can delete entries from this list if necessary.



Main » Users » External Authentication » Social Media Login » Social Media Account Quota List

### Social Media Account List

Delete

	Status	MAC Address	Email Address / Unique ID	Time	Allowance
<input type="checkbox"/>	Valid	70:70:0D:B4:EB:84	<a href="#">[Redacted]</a>	Valid before 2017/10/05 03:41	Unlimited

(Total: 1/10000) [First](#) [Prev](#) [Next](#) [Last](#) Go to Page  (Page: 1/1) Row per Page:

## 5.3 Social Media Account Information

The Controller is capable of collecting valuable customer information from Guest Email Login clients and/or Social Media Login clients for further analysis or marketing purposes. Administrators can download Social Account Names and Account Emails/Unique ID on the Social Media Account List. Besides, the last login field indicates when the client has logged in to the system and the logins field shows how many times the social account user appears in the system. This information can be helpful for tracking client royalty of stores, for example.

Main » Users » External Authentication » Social Media Login » Social Media Account Information

### Social Media Account information

Download Delete All

Type	Name	Email Address / Unique ID	Last Login	Logins
facebook	Mirco Fulminis	<a href="#">[Redacted]</a>	2017-07-13 17:31:34	0
facebook	<a href="#">[Redacted]</a>	<a href="#">[Redacted]</a>	2017-09-21 03:41:26	3

(Total: 2/12000) [First](#) [Prev](#) [Next](#) [Last](#) Go to Page  (Page: 1/1) Row per Page:

## 6. Conclusion

This solution is capable of performing flexible guest authentication such as email verification or social media account login. Social media supported for login includes Facebook, Line, Weibo, and OpenID. Along with the robust authentication features, the WLAN Controller is able to consolidate valuable information collected from guests for future marketing purposes. With this solutions, administrators can easily and efficiently provide guest Wi-Fi service to users.

## ***7. Remarks***

For more information, please contact your local system integrator or our Technical Support team.