

Grandstream Networks, Inc.

Captive Portal

Authentication via Facebook



Captive Portal – Authentication via Facebook

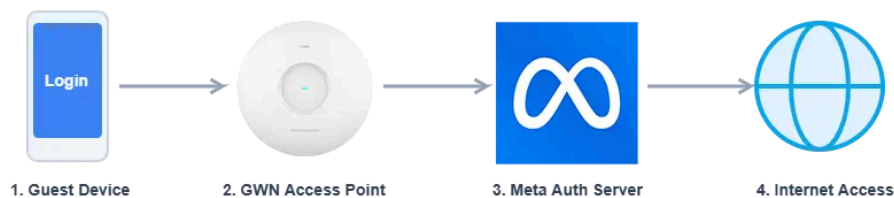
Overview

The Captive Portal feature on Grandstream GWN Networking Solutions allows administrators to define a customized Landing Page (Splash Page) that is displayed on Wi-Fi clients' browsers when attempting to access the internet. Once connected to a GWN Access Point, clients are forced to view and interact with this page before internet access is granted.

By integrating **Facebook Login** (Social Login Authentication), businesses can offer a frictionless, one-click login experience for their guests. Instead of asking users to remember complex passwords or fill out long registration forms, guests can securely authenticate using their existing Meta (Facebook) credentials.

Captive portals with social authentication are highly effective in environments offering free Wi-Fi hotspots, including:

- **Hospitality & Retail:** Hotels, coffee shops, and restaurants.
- **Public Venues:** Airports, shopping malls, and business centers.
- **Marketing:** Businesses looking to increase brand visibility, drive users to their primary website, or collect demographic insights via Facebook Analytics.



Captive Portal Authentication via Facebook

Prerequisites

Before configuring the Captive Portal, ensure you have the following hardware and account requirements ready.

Hardware Requirements

You will need an active internet connection and at least one of the following Grandstream networking setups:

- **Grandstream Access Point:** A standalone GWN series Wi-Fi access point.
- **Grandstream Wireless Router:** A GWN series router with built-in Wi-Fi capabilities.
- **Wired Router + Access Point:** A Grandstream wired router (e.g., GWN70xx series) acting as the controller, paired with at least one GWN Access Point to broadcast the Wi-Fi network.

Account Requirements

- **Meta Developer Account:** An active, verified Meta for Developers account (developers.facebook.com).
- **Meta App Credentials:** You must have already created a Meta App configured for "Facebook Login" and have your **App ID** and **App Secret** ready.

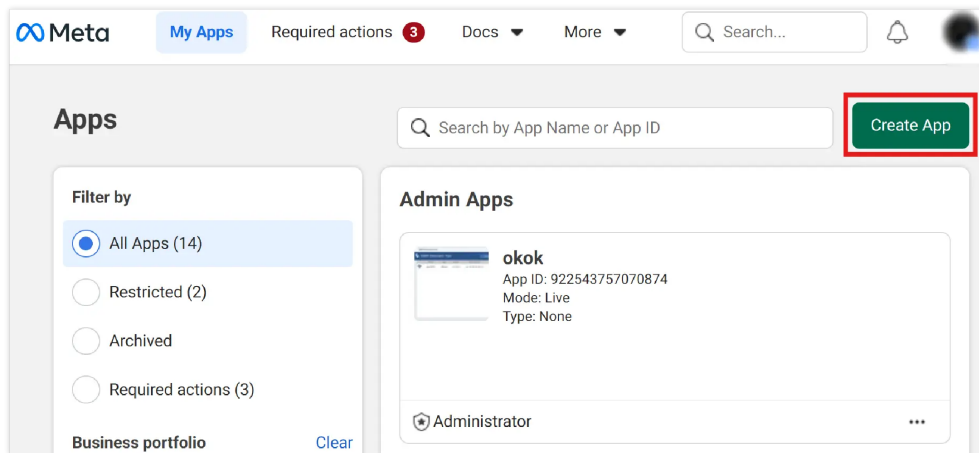
1. Meta App Configuration

Once your Meta Developer account and Business Portfolio are set up, you need to create and configure the specific App that will handle your Wi-Fi portal's authentication requests.

1.1 Create the App

To begin, you need to create a new app container within your Meta Developer workspace.

1. Navigate to your Meta Apps dashboard (developers.facebook.com/apps).
2. Click the green **Create App** button in the top right corner.
3. Follow the on-screen prompts.

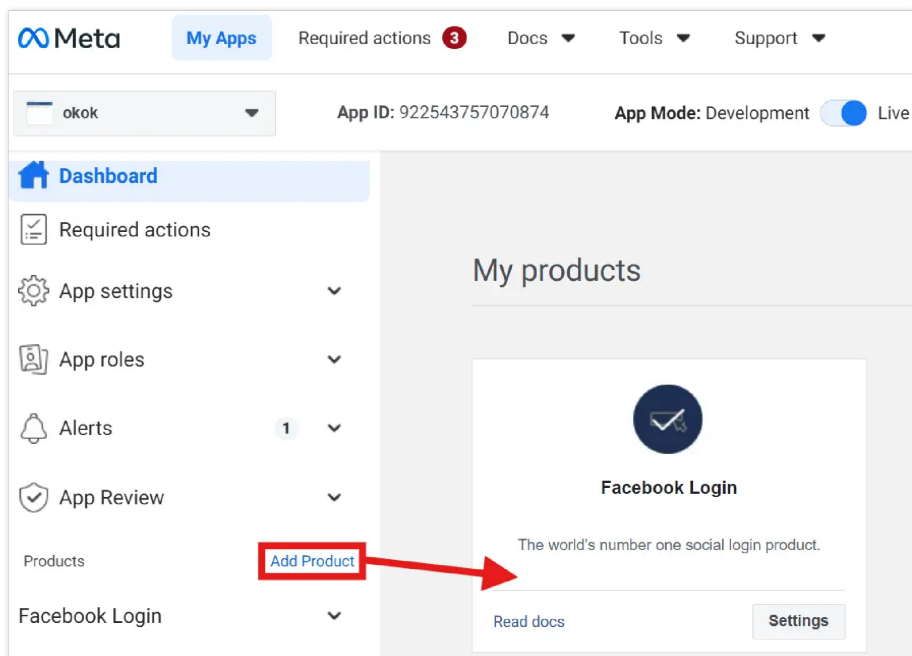


11 Create the App

1.2 Add the Facebook Login Product

Your app needs the specific toolset designed to handle social logins.

1. Once your app is created, you will be taken to the App Dashboard.
2. In the left-hand navigation menu, locate and click **Add Product**.
3. Find the **Facebook Login** card and click **Set Up** to add it to your app.



12 Add the Facebook Login Product

1.3 Configure OAuth Settings (Critical Step)

This is the most important step on the Meta platform. You must tell Facebook exactly which web address (your Grandstream controller) is allowed to request logins.

1. In the left-hand menu, under **Facebook Login**, click **Settings**.

2. Locate the **Valid OAuth Redirect URIs** field.
3. Paste the exact redirect URL provided by your Grandstream controller (<https://cwp.gwnportal.cloud:8443/GsUserAuth.cgi?GsUserAuthMethod=3>).
4. Scroll down to the **Login from devices** setting and toggle it to **Yes**.
5. Click **Save Changes** at the bottom of the page.

The screenshot shows the Meta App settings for an app named 'okok'. The 'Client OAuth settings' section is expanded. The 'Valid OAuth Redirect URIs' field is highlighted with a red box and contains the URL 'https://cwp.gwnportal.cloud:8443/GsUserAuth.cgi?GsUserAuthMethod=3'. The 'Login from devices' toggle is also highlighted with a red box and is set to 'Yes'.

13 Configure OAuth Settings Critical Step

1.4 Retrieve Credentials & Go Live

Finally, you need to gather the unique keys that will connect your Access Point to this app, and publish the app so guests can use it.

1. In the left-hand menu, navigate to **App settings > Basic**.
2. Here, you will find your **App ID** and **App secret** (you may need to re-enter your password to reveal the secret). **Copy both of these down** you will paste them into the Grandstream interface in the next section.
3. Make sure you have entered a valid URL in the **Privacy policy URL** field (Meta requires this for public apps).
4. At the top of the screen, click the toggle to change the **App Mode** from **Development** to **Live**.

The screenshot shows the Meta App settings for an app named 'okok'. The 'App settings' section is expanded, and the 'Basic' tab is selected. The 'App ID' and 'App secret' fields are highlighted with red boxes. The 'App Mode' toggle is also highlighted with a red box and is set to 'Live'.

14 Retrieve Credentials Go Live

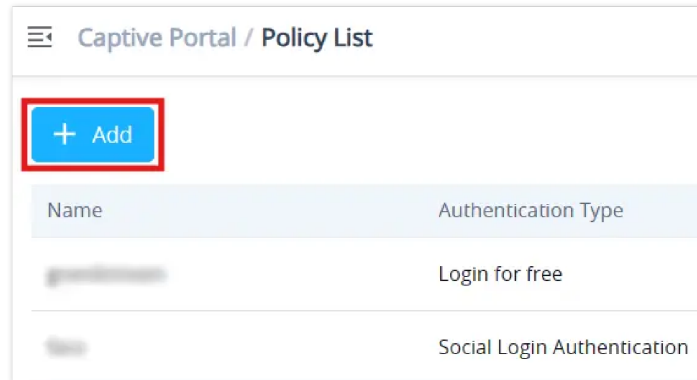
2. Grandstream Access Point Configuration

With your Meta App ready and credentials in hand, it is time to configure your Grandstream GWN Access Point (or Router) to broadcast the network and enforce the Facebook Captive Portal.

2.1 Create a New Captive Portal Policy

First, you need to define the rules for how the splash page will behave.

1. Log in to your Grandstream GWN web interface (or GWN.Cloud / GWN Manager).
2. On the left-hand navigation menu, go to **Captive Portal > Policy List**.
3. Click the blue **+ Add** button to create a new policy.



21 Create a New Captive Portal Policy

2.2 Configure the Policy Settings

In this menu, you will link the Grandstream hardware to your Meta App using the credentials you copied earlier.

1. **Name:** Enter a descriptive name for your policy (e.g., *Facebook Captive Portal*).
2. **Splash Page:** Set this to **Internal**.
3. **Authentication Type:** Select **Social Login Authentication** from the dropdown menu.
4. **Facebook:** Check the box next to Facebook to reveal the credential fields.
5. **App ID & App Secret:** Paste the exact App ID and App Secret you retrieved from the Meta Developer dashboard.
6. **Use Default Portal Page:** Check this box to use Grandstream's built-in, mobile-responsive Facebook login page.
7. Click **Save**.

22 Configure the Policy Settings

Note: When you select Facebook authentication, the GWN system automatically configures the necessary “Pre-Authentication Rules” in the background to allow guest devices to securely reach Facebook’s login servers before they have full internet access.

2.3 Create or Edit an SSID

Next, you need a Wi-Fi network (SSID) to broadcast this new Captive Portal policy to your guests.

1. Navigate to the **SSIDs** menu on the left sidebar.
2. Click the blue + **Add** button to create a new guest network, or edit an existing one.

Name	SSID Band	Wi-Fi	VLAN ID
[Redacted]	2.4GHz & 5GHz	✓	✗
[Redacted]	2.4GHz & 5GHz	✓	✗

23 Create or Edit an SSID

2.4 Apply the Captive Portal to the SSID

Finally, attach the policy you just created to this Wi-Fi network.

1. **SSID:** Name your Wi-Fi network (e.g., *Facebook Wi-Fi*). This is what guests will see on their phones.
2. **Security Mode:** For public captive portals, this is typically set to **Open** (the portal itself acts as the gateway).
3. **Enable Captive Portal:** Check this box to activate the portal on this specific SSID.

4. **Captive Portal Policy:** Click the dropdown menu and select the policy you created in Step 2.2 (e.g., *Facebook Captive Portal*).
5. Click **Save** at the bottom, and don't forget to click **Apply** at the top of the GWN interface to push the changes to your Access Points.

The screenshot shows the 'Edit' configuration page for a Wi-Fi network. The 'Wi-Fi' tab is selected. Under 'Access Security', 'Enable Captive Portal' is checked. The 'Captive Portal Policy' dropdown is open, showing 'Facebook Captive Portal' as the selected option. A red box highlights the 'Captive Portal Policy' dropdown and the 'Facebook Captive Portal' option.

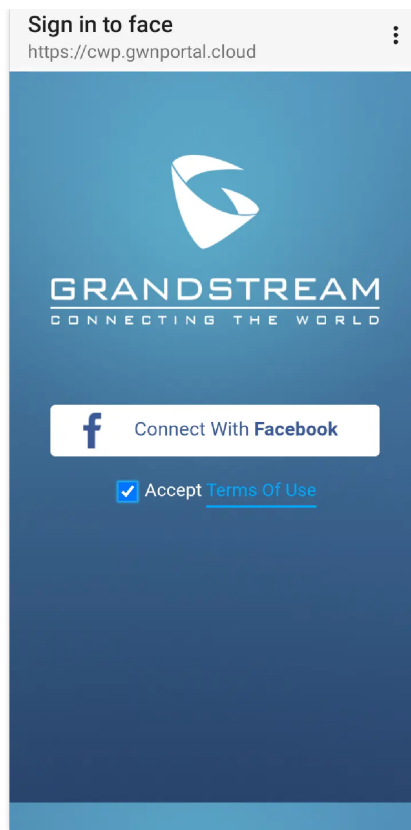
24 Apply the Captive Portal to the SSID

3. Client Verification

Now that the Meta App and Grandstream Access Point configurations are complete, it is highly recommended to verify the user experience by connecting to the newly created guest network using a mobile device.

3.1 Triggering the Captive Portal

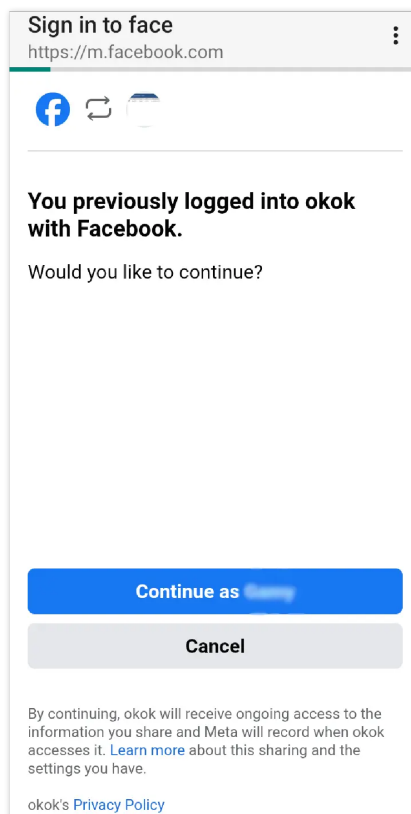
1. On a smartphone or tablet, navigate to the Wi-Fi settings and select the guest SSID you configured (e.g., *Facebook Wi-Fi*).
2. The device should automatically launch its captive portal browser and display the Grandstream Splash Page.
3. Check the **Accept Terms Of Use** box, then tap the **Connect With Facebook** button.



31 Triggering the Captive Portal

3.2 Facebook Authorization

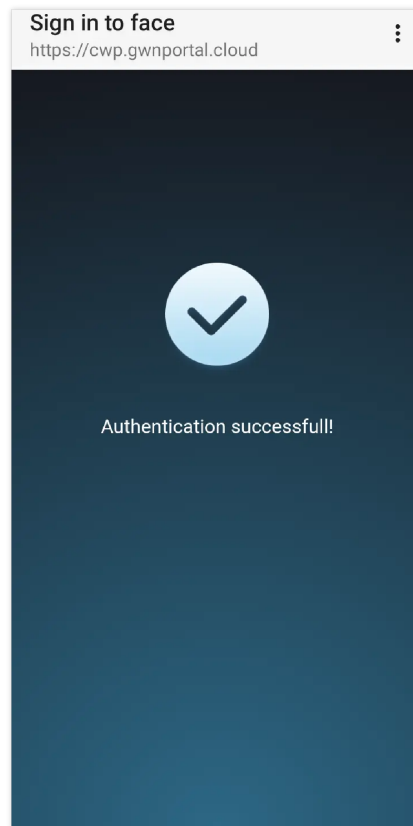
1. The portal will securely redirect the user to Meta's authentication servers.
2. If the user is already logged into the Facebook app or browser on their device, they will see a prompt to continue with their existing profile. (If they are not logged in, they will be asked to enter their Facebook email and password).
3. The user taps **Continue** to grant the portal authentication access.



32 Facebook Authorization

3.3 Successful Connection

1. Once Facebook validates the login, a success token is passed back to the Grandstream Access Point.
2. The portal will display an **"Authentication successful!"** message.
3. The splash page will close, and the guest device is now granted full access to the internet.



33 Successful Connection