



THE FORTINET COOKBOOK

Social Network Authentication

FORTINET DOCUMENT LIBRARY

<https://docs.fortinet.com>

FORTINET VIDEO GUIDE

<https://video.fortinet.com>

FORTINET BLOG

<https://blog.fortinet.com>

CUSTOMER SERVICE & SUPPORT

<https://support.fortinet.com>

FORTINET TRAINING & CERTIFICATION PROGRAM

<https://www.fortinet.com/support-and-training/training.html>

NSE INSTITUTE

<https://training.fortinet.com>

FORTIGUARD CENTER

<https://fortiguard.com/>

END USER LICENSE AGREEMENT

<https://www.fortinet.com/doc/legal/EULA.pdf>

FEEDBACK

Email: techdoc@fortinet.com

FortiPresence supports social network authentication logins with Facebook, Google, Instagram, and LinkedIn. This document describes the configuration of the authentication provider for portal authentication using credentials derived from the Facebook, Google, Instagram, and LinkedIn applications.

- [Creating an Application on Facebook Developers Account](#)
- [Creating an Application on Google Developers Account](#)
- [Creating an Application on Instagram Developers Account](#)
- [Creating an Application on LinkedIn Developers Account](#)
- [Adding Authentication Providers in FortiPresence](#)

Note: Fortinet does not control the requirements imposed by social media platforms, you are required to familiarize yourself with any changes to the policies and update the social media applications accordingly.

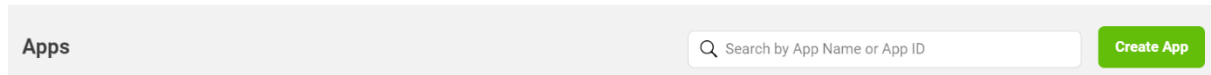
Creating an Application on Facebook Developers Account

Follow this procedure to enable social media authentication with Facebook.

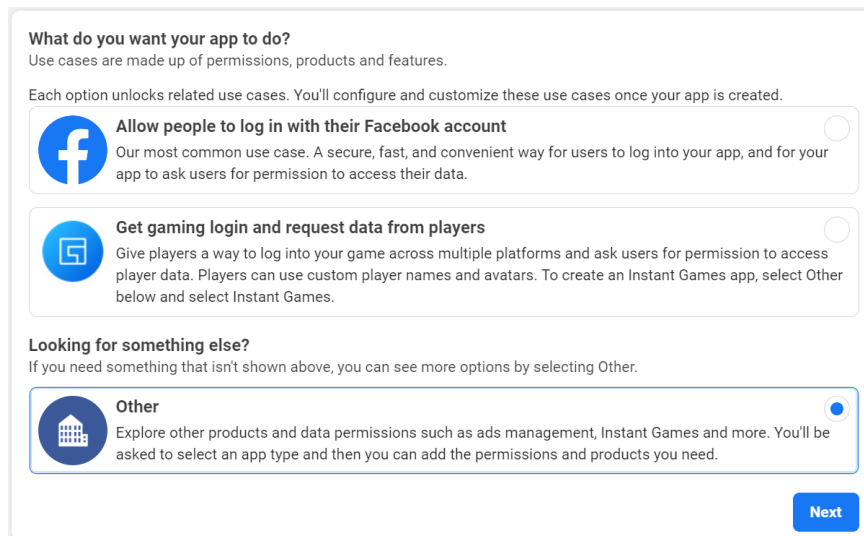
1. Login into the Facebook developers account -

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

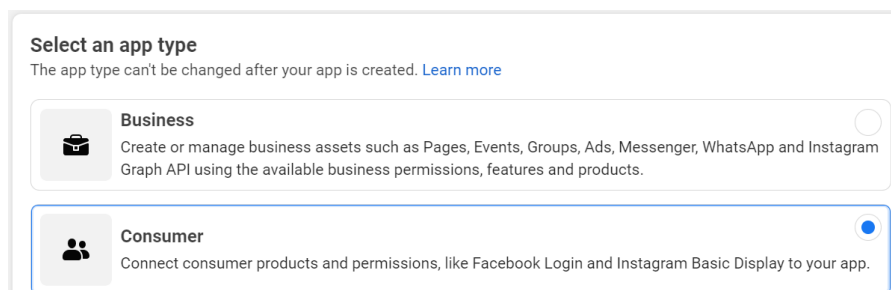
2. In the dashboard, click **My Apps** and then click **Create App**.



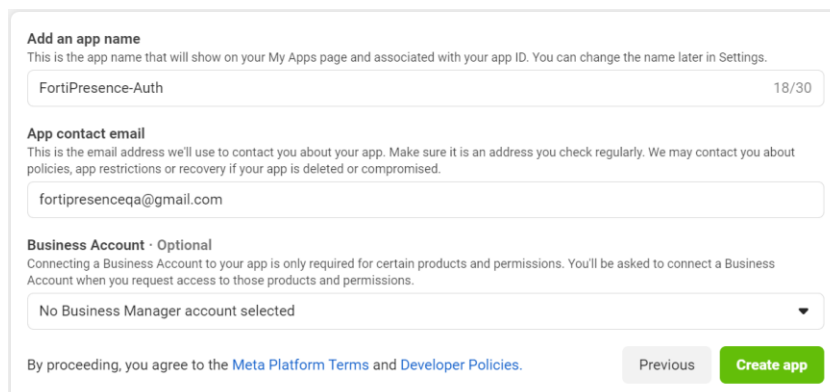
3. Select **Other** and click **Next**.



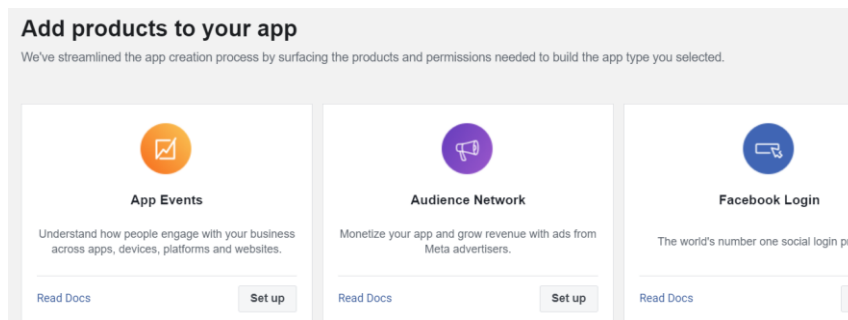
4. Select **Consumer** and click **Next**.



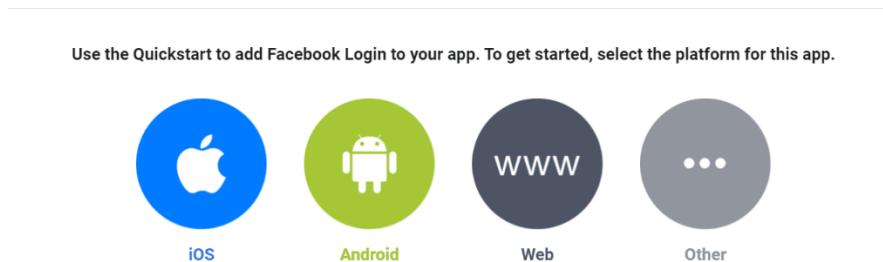
5. Enter a unique application name and your contact email address. Click **Create app**.



6. Select the **Facebook Login** product and click **Set up**.



7. Select the **Web** platform for your application.



8. Enter the FortiPresence FQDN as the **Site URL**. Click **Save**.

The screenshot shows a form titled "1. Tell Us about Your Website". Below the title is a text input field labeled "Site URL" with the value "https://connect.presence.fortinet.com". To the right of the input field is a blue "Save" button.

9. Navigate to **App Settings > Basic**. The generated Facebook **App ID** and the **App Secret** are displayed, copy these credentials. The generated **App ID** and **App Secret** are required to be populated in the FortiPresence Administrative Console.

The screenshot shows a section titled "App Settings > Basic". It contains two fields: "App ID" with the value "274569058865465" and "App secret" with a masked value ".....". To the right of the "App secret" field is a "Show" button.

Some fields in this page are automatically populated, update the required information, for example, **App Domains**, **Contact Email**, **Privacy Policy URL**, and **Terms of Service URL**.

App ID 2464112750285999	App Secret Show
Display Name App for FortiPresence	Namespace
App Domains connect.presence.fortinet.com x presence.fortinet.com x fortinet.com x	Contact Email ⓘ fortipresenceqa@gmail.com
Privacy Policy URL https://www.fortinet.com/corporate/about-us/privacy.html	Terms of Service URL https://www.fortinet.com/corporate/about-us/legal.html

10. Navigate to **Facebook Login > Settings** and enable the following fields for client OAuth settings.

- Client OAuth Login
- Web OAuth Login
- Enforce HTTPS
- Use Strict Mode for Redirect URIs

11. Enter **Valid OAuth Redirect URIs** in the format as depicted in this image.

Client OAuth settings

<input checked="" type="checkbox"/> 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. [?]	<input checked="" type="checkbox"/> Enforce HTTPS Enforce the use of HTTPS for Redirect URIs and the JavaScript SDK. Strongly recommended. [?]
<input checked="" type="checkbox"/> Web OAuth login Enables web-based Client OAuth Login. [?]	<input type="checkbox"/> Force Web OAuth reauthentication When on, prompts people to enter their Facebook password in order to log in on the web. [?]
<input type="checkbox"/> Force Web OAuth reauthentication When on, prompts people to enter their Facebook password in order to log in on the web. [?]	<input type="checkbox"/> Embedded Browser OAuth Login Enable webview Redirect URIs for Client OAuth Login. [?]
<input checked="" type="checkbox"/> Use Strict Mode for redirect URIs Only allow redirects that exactly match the Valid OAuth Redirect URIs. Strongly recommended. [?]	

Valid OAuth Redirect URIs
A manually specified redirect_uri used with Login on the web must exactly match one of the URIs listed here. This list is also used by the JavaScript SDK for in-app browsers that suppress popups. [?]

<https://connect.presence.fortinet.com/portal/oauth/callback/facebook> x

FortiPresence Cloud	https://connect.presence.fortinet.com/portal/oauth/callback/facebook
FortiPresence VM	https://{Application server FQDN}/portal/oauth/callback/facebook

Note: If the captive portal FQDN is created separately then update that URL instead of the application server FQDN.

12. Switch your Facebook application to **Live** mode.

Note: In order to be granted access to certain user information, Facebook requires your application to undergo a review process, click **App Review**. For more information read specific Facebook guidelines and policies on this page.

Creating an Application on Google Developers Account

Follow this procedure to enable social media authentication with Google.

1. Login into Google developers account –
<https://console.developers.google.com>
2. Click **Select a project** and click **New Project**.
3. Enter a unique **Project name** and the **Location** of your organization.

Project name *
FortiPresence

Project ID: fortipresence-399706. It cannot be changed later. [EDIT](#)

Location *
No organization [BROWSE](#)

Parent organization or folder

[CREATE](#) [CANCEL](#)

4. Click **OAuth consent screen** and choose from the following options. Click **Create**.
 1. **Internal** – available only to users within your organization.
 2. **External** – available to any user with a Google Account.

OAuth consent screen

Choose how you want to configure and register your app, including your target users. You can only associate one app with your project.

User Type

☐ Internal

Only available to users within your organization. You will not need to submit your app for verification. [Learn more about user type](#)

☒ External

Available to any test user with a Google Account. Your app will start in testing mode and will only be available to users you add to the list of test users. Once your app is ready to push to production, you may need to verify your app. [Learn more about user type](#)

[CREATE](#)

5. Configure the **App information**, **App logo**, **Authorized domains**, **Application home page**, **Application privacy policy link**, and **Application terms of service link**.
6. Click **Credentials > Create Credentials** and select **OAuth client ID** to create the OAuth 2.0 client ID. Select **Web application** as the application type and add URIs for **Authorized JavaScript origins** and **Authorized redirect URIs**. The following URIs are supported.

FortiPresence Cloud	<ul style="list-style-type: none">• Authorized JavaScript URIs https://connect.presence.fortinet.com• Authorized redirect URIs
---------------------	--

	https://connect.presence.fortinet.com/portal/oauth/callback/google
FortiPresence VM	<ul style="list-style-type: none"> Authorized JavaScript URIs https://{Application server FQDN} Authorized redirect URIs https://{Application server FQDN}/portal/oauth/callback/google

Note: If the captive portal FQDN is created separately then update that URL instead of the application server FQDN.

Authorised JavaScript origins ⓘ

For use with requests from a browser

URIs *

https://connect.presence.fortinet.com

[+ ADD URI](#)

Authorised redirect URIs ⓘ

For use with requests from a web server

URIs *

https://connect.presence.fortinet.com/portal/oauth/callback/google

[+ ADD URI](#)

7. Copy the displayed client ID and Client secret.

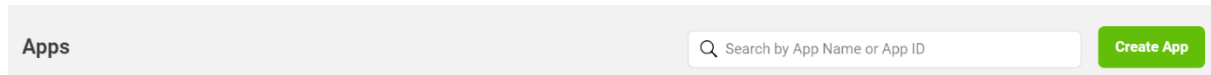
Creating an Application on Instagram Developers Account

Follow this procedure to enable social media authentication with Instagram.

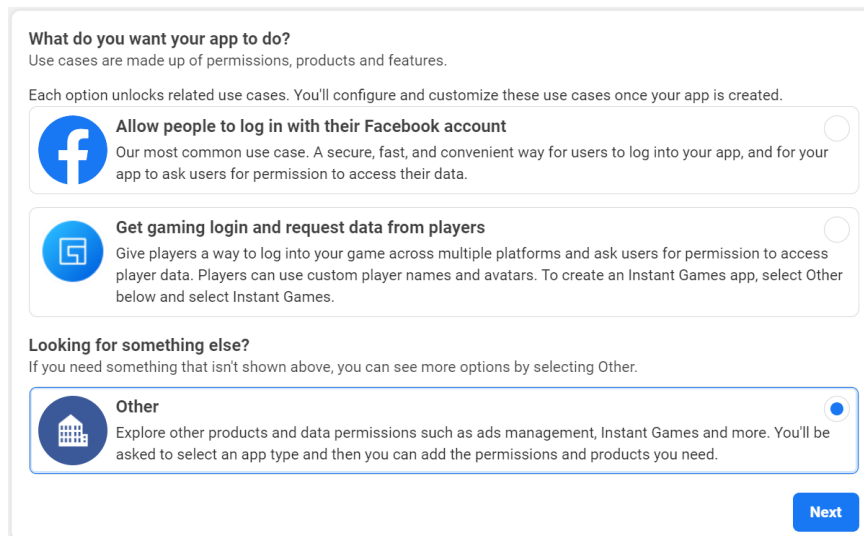
1. Login into the Facebook developers account -

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

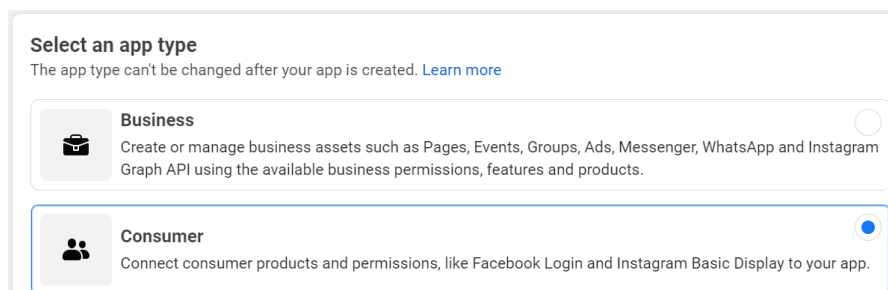
2. In the dashboard, click **My Apps** and then click **Create App**.



3. Select **Other** and click **Next**.

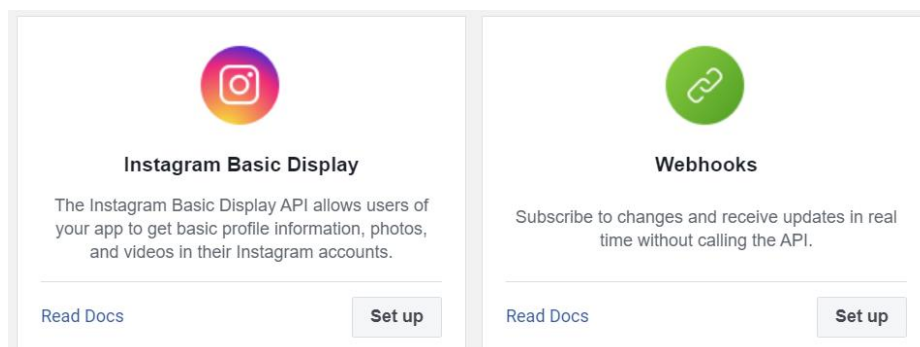


4. Select **Consumer** and click **Next**.



5. Enter a unique application name and your contact email address. Click **Create app**.

6. Select the **Facebook Login** product and click **Set up**.



7. Click **Create New App** and copy the **Instagram App ID** and **App Secret**.
8. Add the following **Valid OAuth Redirect URIs**.

FortiPresence Cloud	https://connect.presence.fortinet.com/portal/oauth/callback/instagram
FortiPresence VM	https://{Application server FQDN}/portal/oauth/callback/instagram

Note: If the captive portal FQDN is created separately then update that URL instead of the application server FQDN.

Instagram App ID: 173206957992793

Instagram App Secret: [Masked] Show

Instagram Display Name: Test-FP-Ins

Client OAuth Settings

Valid OAuth Redirect URIs: https://connect.presence.fortinet.com/portal/oauth/callback/instagram

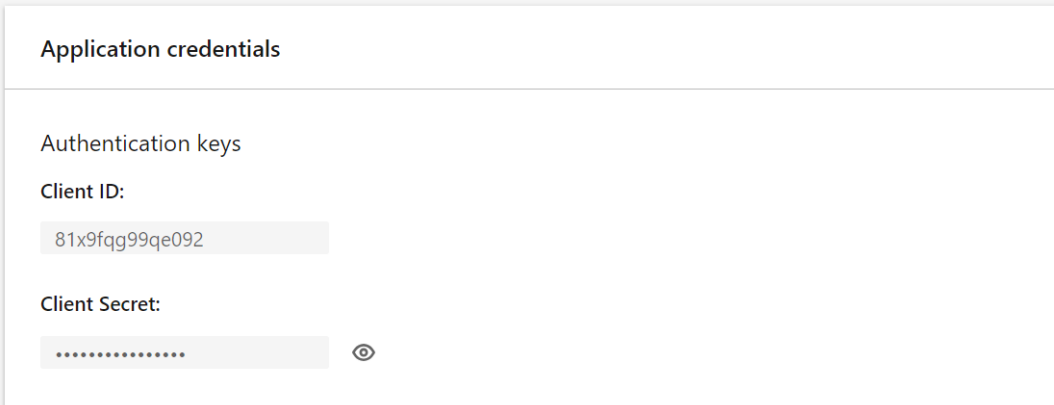
Discard Save Changes

9. Switch your Instagram application to **Live** mode.

Creating an Application on LinkedIn Developers Account

Follow this procedure to enable social media authentication with LinkedIn.

1. Login into the LinkedIn developers account -
<https://www.linkedin.com/developers/>.
2. Click **Create app** or navigate to **My Apps > Create app** to create a new application.
3. Enter the following information and click **Create app**.
 - **App name** - A unique name for your application.
 - **LinkedIn Page** - Your company's name or the URL of the LinkedIn page. (Navigate to <https://www.linkedin.com/company/setup/new/> to create a company page.)
 - **App logo** - Upload a logo for your application that is displayed when the user logs in. The minimum logo size allowed is 100x100.
4. Navigate to **Auth** tab and copy the **Client ID** and **Client Secret** from the **Application Credentials** section.



The screenshot shows the 'Application credentials' section of a LinkedIn developer account. It contains two fields: 'Client ID' with the value '81x9fqg99qe092' and 'Client Secret' which is masked with dots and has an eye icon to toggle visibility.

5. Also in the **Auth** tab, update the **OAuth 2.0 settings** with the following **Redirect URLs**.

FortiPresence Cloud	https://connect.presence.fortinet.com/portal/oauth/callback/linkedin
FortiPresence VM	https://{Application server FQDN}/portal/oauth/callback/linkedin

Note: If the captive portal FQDN is created separately then update that URL instead of the application server FQDN.


OAuth 2.0 settings

Token time to live duration

Access token: **2 months** (5184000 seconds)

Authorized redirect URLs for your app

No redirect URLs added

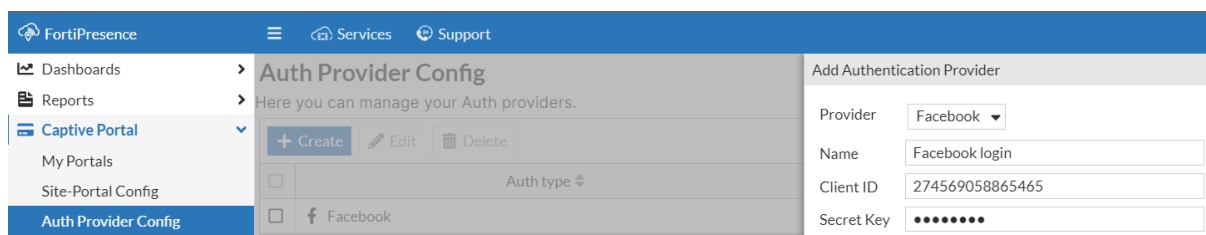


6. Add the products **Sign In with LinkedIn** and **Share on LinkedIn**.

Adding Authentication Providers in FortiPresence

Follow this procedure to add social media authentication providers in FortiPresence.

1. Login into FortiPresence.
2. Navigate to Captive **Portal > Auth Provider config.**
3. Enter the provider name and paste the copied **Client ID** and **Client Secret** (from developers account) and select **Google/Facebook/Instagram/Linkedin** as the **Provider** and save the details.



Auth Provider Config	
Here you can manage your Auth providers.	
+ Create Edit Delete	
<input type="checkbox"/>	
<input type="checkbox"/>	Auth type ↕
<input type="checkbox"/>	f Facebook

Add Authentication Provider
Provider: Facebook ▼
Name:
Client ID:
Secret Key:

Copyright© 2023 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.