Signicat Documentation

Configuring eIDs

In this section, you can find information on enabling Electronic Identities (eIDs) in the Connectis Identity Broker. For different options and questions about enabling eIDs, please contact us via sales@connectis.com.

- DigiD
- eHerkenning and/or eIDAS
- iDIN
- Google SAML
- Google GSuite
- Facebook
- Connecting a SAML 2.0 compatible eID
- Enabling your private authentication means via MyOwnIdP

DigiD

Please follow these steps to enable DigiD.

You can connect DigiD via SAML or the (legacy) DigiD CGI protocol. Connectis supports both protocols.

▭ DigiD SAML 2.0

▭ DigiD CGI

DigiD SAML 2.0

Please follow these steps to enable DigiD SAML 2.0:

- Download the DigiD Checklist published by Logius on their website.
- Make sure you familiarise yourself with the testing criteria that Logius maintains for using DigiD in your service, and use this information to prepare your service for DigiD. Logius will test compliance after the connection is established.
- Dutch law requires you to sign a *Verwerkersovereenkomst* (Processor Agreement) with Connectis. You can contact sales@connectis.com to receive a default template.

Connecting to pre-production

- Connectis Identity Broker must be configured on a domain name that is controlled by the organization that requests the DigiD connection. This has the be the organization that is allowed to process BSN. Follow *Setting up a domain name* to change the domain name of your Connectis Identity Broker if required.
- Contact Logius and request a pre-production connection. You can use this connection to test your pre-production environment. Logius will need up to 5 working days to process your request.
- Logius will provide you with metadata. Send this metadata file to technicalsupport@connectis.com.
- Run through the *Logius checklist* to prepare to test your DigiD connection on pre-production.
- Logius must perform tests on your pre-production connection. This will take up to 5 working days. When the tests are done, you will receive their findings. When your connection is approved, you can continue to connect to production.

Connecting to production

- As described in the Logius DigiD Checklist, the Connectis Identity Broker must be configured on a domain name that is controlled by the organization that requests the DigiD connection. This has the be the organization that is allowed to process BSN. Follow *Setting up a domain name* to change the domain name of your Connectis Identity Broker if required.

- Logius requires you to use a PKI Overheid (Government) CA 2020 certificate.
- Contact Logius and request a production connection. Logius will need up to 5 working days to process your request.
- Send the metadata of the connection to Connectis, please see steps required for pre-production.
- Logius will activate your connection for DigiD SAML.

Audit your DigiD connection within 2 months

- Within 2 months after going live, execute a DigiD assessment via a Registered ETP Auditor and send the report with findings to Logius. *More information*

If you have also enabled other authentication methods than just DigiD you can use the NameQualifier attribute in SAML responses to your Service to detect in your application that DigiD was used to log in for this request:

```
<saml:Subject>
  <saml:NameID
    Format="urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified"
    NameQualifier="https://was-preprod1.digid.nl/saml/idp/metadata">
      sector number:bsn
  </saml:NameID>
  <saml:SubjectConfirmation Method="urn:oasis:names:tc:SAML:2.0:cm:bearer">
    <saml:SubjectConfirmationData
      InResponseTo="..." NotOnOrAfter="..." Recipient=".../>
  </saml:SubjectConfirmation>
</saml:Subject>
```

Attention points DigiD SAML

Keep the following attention points in mind when setting up a DigiD SAML connection:

1. In the request form from Logius for the connection, use the URL of the Connectis Identity Broker in the field "URL aansluiting (pre)productieomgeving".
2. Make sure your website contains a PKIO certificate (see DigiD Checklist Testen, T2).
3. Adhere to the error page requirements of DigiD (see DigiD Checklist Testen, T6).

4. Adhere to the cancel requirements of DigiD (see DigiD Checklist Testen, T7).
5. When using a session on your website, adhere to the session requirements of DigiD (see DigiD Checklist Testen, T14 & T15).
    1. When not using a session, for instance when using the DigiD connection for signing, notify Logius of this during the pre-production test.
6. Don't forget to activate your connection on production. This requires an extra email to the service desk of Logius after your production connection has been created.
7. With regard to planning, keep in mind the processing time of Logius (maximum of 5 working days per request, 4 requests in the entire flow to production).

DigiD CGI

Please follow these steps to enable DigiD CGI:

- Download the DigiD Checklist published by Logius.
- Make sure you familiarise yourself with the testing criteria that Logius maintains for using DigiD in your service, and use this information to prepare your service for DigiD. Logius will test compliance after the connection is established.
- Dutch law requires you to sign a *Verwerkersovereenkomst* (Processor Agreement) with Connectis. You can contact sales@connectis.com to receive a default template.

Connecting to pre-production

- Connectis Identity Broker must be configured on a domain name that is controlled by the organization that requests the DigiD connection. This has the be the organization that is allowed to process BSN. Follow *Setting up a domain name* to change the domain name of your Connectis Identity Broker if required.
- Contact Logius and request a pre-production connection. You can use this connection to test your pre-production environment. Logius will need up to 5 working days to process your request.
- Logius will provide you with details on your connection.
- Send these details to technicalsupport@connectis.com using a password-protected zip file. Call Connectis by phone to transfer the password, using phone number 088-012 02 10.
- Run through the *Logius checklist* to prepare to test your DigiD connection on pre-production.
- Logius must perform tests on your pre-production connection. This will take up to 5 working days. When the tests are done, you will receive their findings. When your connection is approved, you can continue

to connect to production.

Connecting to production

- As described in the Logius DigiD Checklist, the Connectis Identity Broker must be configured on a domain name that is controlled by the organization that requests the DigiD connection. This has the be the organization that is allowed to process BSN. Follow *Setting up a domain name* to change the domain name of your Connectis Identity Broker if required.
- Logius requires you to use a PKI Overheid (Government) CA 2020 certificate.
- Contact Logius and request a production connection. Logius will need up to 5 working days to process your request.
- Send the metadata of the connection to Connectis, please see steps required for pre-production.
- You must activate your credentials at Logius.

Audit your DigiD connection within 2 months

- Within 2 months after going live, execute a DigiD assessment via a Registered ETP Auditor and send the report with findings to Logius. *More information*

If you have also enabled other authentication methods than just DigiD you can use the NameQualifier attribute in SAML responses to your Service to detect in your application that DigiD was used to log in for this request:

```
<saml:Subject>
  <saml:NameID
    Format="urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified"
    NameQualifier="https://was-preprod1.digid.nl/saml/idp/metadata">
      sector number:bsn
  </saml:NameID>
  <saml:SubjectConfirmation Method="urn:oasis:names:tc:SAML:2.0:cm:bearer">
    <saml:SubjectConfirmationData
      InResponseTo="..." NotOnOrAfter="..." Recipient=".../>
  </saml:SubjectConfirmation>
</saml:Subject>
```

eHerkenning and/or eIDAS

Please follow these steps to enable eHerkenning/eIDAS

Getting started

- Familiarise yourself with eHerkenning/eIDAS
- Sign Self-Declaration (Zelfverklaring) and send this signed self-declaration, in which you indicate to agree to the demands and agreements in the eHerkenning federation (https://afsprakenstelsel.etoegang.nl), to technicalsupport@connectis.com. Perform this step for each service that you want to publish in the eHerkenning and/or eIDAS service catalogue.
- The Connectis Identity Broker must be configured on a domain name that is controlled by your organisation. Follow Setting up a domain name to change the domain name of your Connectis Identity Broker if required.
- The Connectis Identity Broker must be configured with two certificates, one for pre-production and one for production, which will be used to cryptographically sign the messages between the Connectis Identity Broker and the eHerkenning/eIDAS network.
  These certificates must be CA 2020 certificates with at least 2048 bit encryption. Connectis prefers to use EV (extended validation) SSL SHA2 certificates with 4096 bits encryption.
  You can choose to reuse an existing PKIO certificate.
- Determine which services you want to connect to eIDAS/eHerkenning. Please provide the following information for each service:
  - Name
  - Description
  - Web page
  - Level of Assurance

  Connectis can support you in determining the necessary Level of Assurance for a service, the naming of that service, and in setting up an authorisation model for that service with the right granularity.

- A variety of identifying attributes (EntityConcernedTypes) can be returned in the responses in eIDAS / eHerkenning. Choose an EntityConcernedTypesAllowed for your service.
- Your service can request attributes as specified in the eIDAS & eHerkenning attribute catalogue.

- However, it is not guaranteed that attributes will actually be delivered to all users in eIDAS & eHerkenning: users to whom attributes are not returned should also be able to log in. See RequestedAttributes for more information on which attributes you can request.

Connecting to pre-production

- Prepare and send your eHerkenning/eIDAS Service Catalogue to Connectis. In this XML file, you will define what service you want to make available in the eHerkenning/eIDAS network. Connectis will process your Service Catalogue and publish it on the testing network of eHerkenning/eIDAS.
-

Request pre-production accounts so that you can test your connection on pre-production. A pre-production can be requested via https://connectis.com/nl/testmiddel-aanvragen/.

- It is not necessary to run tests using multiple identity providers (authentication services): Connectis ensures that eHerkenning works correctly with all different identity providers in the network.
- If you require an account to test eIDAS, please contact technicalsupport@connectis.com.
- Test your connection by logging into your pre-production service via eHerkenning, using your pre-production test accounts.

Preparing your connection to production

- Give Connectis your permission to distribute your service catalogue into the eHerkenning/eIDAS network. This will make your service available. Only after this step can users be authorised for your service!

Going to production

- When your connection is active, it can be used by end users immediately. Send your planned date of going to production to technicalsupport@connectis.com. This allows Connectis to be on standby in case of any problems.

Communication eHerkenning

It is important to prepare your users in time, in order to allow them to prepare for logging into your services with eHerkenning. As it takes some time to request and receive the eHerkenning login means, they will need a timely notice. So it is important to ensure effective internal and external communication.

eHerkenning provides a manual with several steps explaining how to best communicate the upcoming switch to eHerkenning for your service, see https://www.eherkenning.nl/communicatie.

Required graphics (the logo, login buttons, and Levels of Assurances) for eHerkenning can also be downloaded.

eIDAS communication

Communication eIDAS

To ensure a uniform appearance for European users, you can use text elements and visual elements designed for eIDAS.

Communication checklist: setting up your website for eIDAS

1. **Texts:** provide a clear explanation about eIDAS on your website. Use text elements and visual elements, such as the logo, for this.
2. **Images:** use the EU flag as a visual marker for European login, at the login button for European login. As a result, European citizens and companies know that they can log in to your service via this button.

Text elements eIDAS

From September 29, 2018, your organisation must be able to grant holders of eIDAS-recognised login means access to your digital services. In due course, even more recognised login tools will be added. This means that a multitude of users can come to your organisation.

The eIDAS regulation does not oblige organisations to translate the service into multiple European languages. However, your organisation can use a number of standard text elements in English.

Word of welcome

Make it clear to European users that they can log in with their European login. If you want to indicate that the service is only for citizens or companies, you can add '(for businesses)' or '(for citizens)'. You can use the following options:

1. Here you can log in with a European-recognised login means
2. Do you have a European approved digital identity? Please login here.
3. Login with your European digital identity.

Key messages

If you want to provide European users with more information about the possibilities of eIDAS, you can use an in-depth text. Keep in mind that the term eIDAS is often still unknown to a European user.

Take your European digital identity with you, everywhere you go in Europe

Are you in the possession of an eIDAS-approved digital identity? That means that you can take advantage of the eIDAS-regulation that becomes effective on the 29th of September. Accessing online public services like filing your income taxes at the Dutch Tax Authority or registering for courses at a Dutch university are made accessible to you without physically having to cross the border. This applies to all online public services that are already available to local citizens in possession of a digital identity, in all of the European Union.

EU flag as a visual marker at the login button

EU flag and files application

The EU flag is available in various formats to use on your website as a visual marker at the login button for European login. You can find these files in the communication toolkit. Requirements:

- The EU flag itself should not be used as a login button
- Application examples of how to use the EU flag next to the login button can be found in the communication toolkit.

The logo is also well scalable. In the communication toolkit you can find both logos in different formats (150, 300, 500 px) and formats (CMYK and RGB, PNG, EPS, AI). Contact our technical support team to receive the toolkit.

eHerkenning/eIDAS Info

Service providers in the Netherlands can use eHerkenning to allow users to log in on behalf of their organisations. Service providers in the Netherlands can allow users of (non-Dutch) European eIDs to log into their services by using the eHerkenning network. More information on eHerkenning is available via https://www.eherkenning.nl/.

Service catalogues

In order to publish a service in the eHerkenning network so that organisations can authorise their members to log into those services, data on the service must be published to eHerkenning. This data is published through so-called *service catalogues*. A service catalogue can contain information for multiple services.

Service catalogues define information about your services. Services are indicated through a ServiceID, which contains an *Overheids Identificatie Number* (OIN, or Government Identification Number). More information about OINs can be found *here*. The Service ID format is:

```
urn:etoegang:DV:oin:services:service index
```

The required Level of Assurance for each of your services is listed in the service catalogue. Each service can have its own Level Of Assurance. It also indicates what kind of identifying attribute (EntityConcernedTypesAllowed) you want to receive in your application, and whether or not you wish to enable eIDAS (Classifier). More detailed information on service catalogues.

To create a service catalogue, copy the following information into a text file and fill it out. Send this file to technicalsupport@connectis.com. Connectis will ensure the eHerkenning / eIDAS network will subsequently be updated with your changes.

```
<?xml version="1.0" encoding="UTF-8"?>
<esc:ServiceCatalogue xmlns:esc="urn:etoegang:1.13:service-catalog" xmlns:md="urn:oasis:na
                      xmlns:ds="http://www.w3.org/2000/09/xmldsig#" xmlns:saml="urn:oasis:
                      esc:IssueInstant="2019-12-28T10:19:57Z" esc:Version="urn:etoegang:1.
                      ID="198d678c-239e-43c4-acf7-b4f6f1f6d8c0">
```

```
    <esc:ServiceProvider esc:IsPublic="true">
        <esc:ServiceProviderID><!--OIN van organistatie--></esc:ServiceProviderID>
        <esc:OrganizationDisplayName xml:lang="nl"><!--Naam van organistatie--></esc:Organ
        <esc:ServiceDefinition esc:IsPublic="true">
            <esc:ServiceUUID><!--unieke ID genereren via uuidgenerator.net--></esc:Service
            <esc:ServiceName xml:lang="nl"><!--Naam van de Service--></esc:ServiceName>
            <esc:ServiceName xml:lang="en"><!--Naam van de Service--></esc:ServiceName>
            <esc:ServiceDescription xml:lang="nl"><!--Beschrijving van de Service--></esc:
            <esc:ServiceDescription xml:lang="en"><!--Beschrijving van de Service--></esc:
            <esc:ServiceDescriptionURL xml:lang="nl">http://example.etoegang.nl</esc:Servi
            <saml:AuthnContextClassRef>urn:etoegang:core:assurance-class:<!--Loa van de Se
            <esc:HerkenningsmakelaarId>00000003244440010000</esc:HerkenningsmakelaarId>
            <esc:EntityConcernedTypesAllowed>urn:etoegang:1.9:EntityConcernedID:KvKnr</esc
              <esc:ServiceRestrictionsAllowed>urn:etoegang:1.9:ServiceRestriction:Vestigin
        </esc:ServiceDefinition>
        <esc:ServiceInstance esc:IsPublic="true">
            <esc:ServiceID>urn:etoegang:DV:<!--OIN -->:services:<!--Service Index--></esc:
            <esc:ServiceUUID><!--unieke ID genereren via uuidgenerator.net--></esc:Service
            <esc:InstanceOfService><!-- UUID of service definition--></esc:InstanceOfServi
            <esc:ServiceURL xml:lang="nl">vul hier een service url in</esc:ServiceURL>
            <esc:ServiceURL xml:lang="en">vul hier een service url in</esc:ServiceURL>
            <esc:PrivacyPolicyURL xml:lang="nl">vul hier een privacy url in</esc:PrivacyPo
            <esc:PrivacyPolicyURL xml:lang="en">vul hier een privacy url in</esc:PrivacyPo
            <esc:HerkenningsmakelaarId>00000003244440010000</esc:HerkenningsmakelaarId>
            <esc:SSOSupport><!-- a boolean that indicates if the service supports SingleSi
            <esc:ServiceCertificate>
        <md:KeyDescriptor use="encryption">
          <ds:KeyInfo>
            <ds:KeyName>.............</ds:KeyName>
            <ds:X509Data>
              <ds:X509Certificate>.............</ds:X509Certificate>
            </ds:X509Data>
          </ds:KeyInfo>
        </md:KeyDescriptor>
      </esc:ServiceCertificate>
        </esc:ServiceInstance>
    </esc:ServiceProvider>
</esc:ServiceCatalogue>
```

Classifier

By specifying a Classifier element, you can couple your service to eIDAS, instead of eHerkenning. Please use one of these options:

Omit the <Classifier> element	The service is coupled to eHerkenning
Specify a <Classifier> element as shown in the	

example, i.e. *<Classifier>eIDAS-inbound<Classifier>*	The service is coupled to eIDAS

EntityConcernedTypesAllowed - eHerkenning

By setting a value for *EntityConcernedTypesAllowed*, you determine which types of identifying attributes (in other words, which kinds of users) are allowed to log into your service. Different values can be used, depending on whether your service is coupled to eHerkenning or eIDAS.

eHerkenning

The following values for EntityConcernedTypesAllowed are available for eHerkenning:

EntityConcernedID:RSIN	Used to identify a user through the RSIN (Rechtspersonen en Samenwerkingsverbanden Identificatienummer) (Legal persons and Partnerships Identification Number) of the represented organisation.
EntityConcernedID:KvKnr	The KvK number (Dutch Chamber of Commerce number) of the represented organisation.
ServiceRestriction:Vestigingsnr	Can only be used together with EntityConcernedID:KvKnr. The field “vestigingsnummer (nieuwe formaat)” (“branch number (new format)”) as available in the Chamber of Commerce will be included in the response.

If you include *ServiceRestriction:Vestigingsnr* in the EntityConcernedTypesAllowed field, then users can also log in if they are only authorised to represent a particular branch (vestiging) of the organisation. **You must include this restriction in your service.** This means that you should craft your application so that the user can only act on behalf of this branch, and not on behalf of the entire organisation.

EntityConcernedTypesAllowed - eIDAS

By setting a value for *EntityConcernedTypesAllowed*, you determine which types of identifying attributes (in other words, which kinds of users) are allowed to log into your service. Different values can be used, depending on whether your service is coupled to eHerkenning or eIDAS

EntityConcernedID:eIDASLegalIdentifier	Identifying attribute to allow a non-legal person (Niet Natuurlijk Persoon) to log into eHerkenning and eIDAS.
EntityConcernedID:Pseudo	Identifying attribute for a consumer in eIDAS.

RequestedAttributes

RequestedAttributes allow you to request additional data on the users using your service. The use of RequestedAttributes is optional. Please take note, however, that the eHerkenning specifications do not guarantee that the extra RequestedAttributes are known for each user, and can thus be returned in the response. When logging in via eIDAS, the delivery of attributes is guaranteed for so-called *required attributes* (verplichte attributen). The *optional attributes* will only be delivered in eIDAS when they are known to the user that is logging in.

Please see the attribute catalogue for more information:

- Attributencatalogus natuurlijke personen (Attribute catalogue for legal persons)
- Attributencatalogus niet-natuurlijke personen (Attribute catalogue for non-legal persons)
- Attributencatalogus generiek (Attribute catalogue generic)

```
<esc:EntityConcernedTypesAllowed>urn:etoegang:1.9:EntityConcernedID:Pseudo</esc:EntityConc
  <esc:RequestedAttribute Name="urn:etoegang:1.9:attribute:FirstName" isRequired="true">
     <esc:PurposeStatement xml:lang="en">For testing purposes.</esc:PurposeStatement>
     <esc:PurposeStatement xml:lang="nl">Voor testdoeleinden.</esc:PurposeStatement>
  </esc:RequestedAttribute>
  <esc:RequestedAttribute Name="urn:etoegang:1.9:attribute:FamilyName" isRequired="true">
     <esc:PurposeStatement xml:lang="en">For testing purposes.</esc:PurposeStatement>
     <esc:PurposeStatement xml:lang="nl">Voor testdoeleinden.</esc:PurposeStatement>
  </esc:RequestedAttribute>
  <esc:RequestedAttribute Name="urn:etoegang:1.9:attribute:DateOfBirth" isRequired="true">
     <esc:PurposeStatement xml:lang="en">For testing purposes.</esc:PurposeStatement>
     <esc:PurposeStatement xml:lang="nl">Voor testdoeleinden.</esc:PurposeStatement>
  </esc:RequestedAttribute>
```

Example of an eIDAS service with Requested Attributes

BSNk Polymorhic Decryption Keys

How to find out which key you received using MyConnectis BSNk Key retrieval

When you have received BSNk key material from Connectis Technical Support or via the automatic Connectis Identity Broker endpoint, it is not directly clear which keys are for which purpose. There are three possible keys that are obtained from BSNk that are used in polymorphic decryption of pseudo ids and identifiers. These are:

- The closing key (EC)
- Pseudo Id key (EP)
- Identity key (EI)

Here are steps to identify which keys you receive from BSNk:

1.From BSNk you will receive a Base64 encoded stream of keys. For each Base64 encoded string first save it in a file. Then base64 decode the contents using:

```
base64 -d {file} > out.p7
```

The base64 decoded output is the p7 file which contains an encrypted key in binary format.

2. Have your private key ready. The file should begin with

```
-----BEGIN RSA PRIVATE KEY-----
```

with the base64 encoded private key contents and end with

```
-----END RSA PRIVATE KEY-----
```

Let's name this file dv-private-key.pem.

3. Decrypt the encrypted key using

```
openssl cms -decrypt -in out.p7 -inkey dv-private-key.pem -inform DER -out key-file.pem
```

4. Open the output key-file.pem. The contents will look like

```
-----BEGIN EC PRIVATE KEY-----
SchemeVersion: 1
SchemeKeyVersion: 1
Type: EP Closing
Recipient: OIN of the customer
RecipientKeySetVersion: Version identifying the recipient and their active key set.

Base64 encoded private key
-----END EC PRIVATE KEY-----
```

Here in the metadata section you can see what type of key it is. The types are

- EP Closing --> closing key
- EP Decryption --> Pseudo Id key
- EI Decryption --> Identity key

iDIN

Please follow these steps to enable iDIN

- Familiarise yourself with iDIN by reading the online documentation.

Getting started

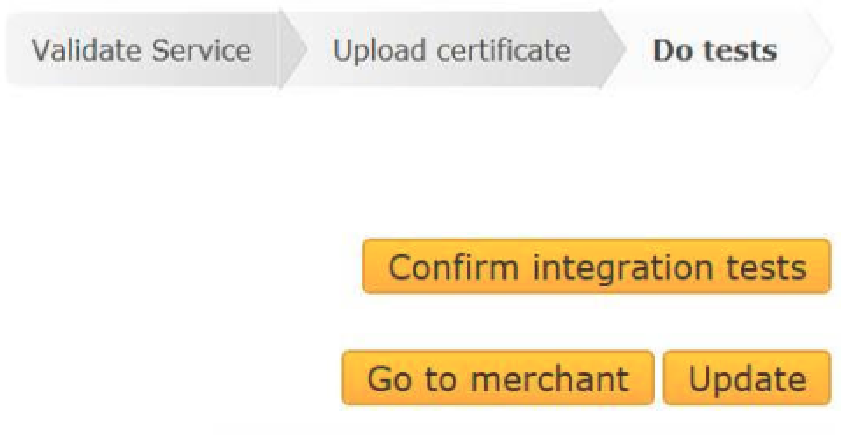
- Choose which attributes you want to receive in your iDIN response. You can also use this spreadsheet to help you choose which attributes to request and calculate the corresponding iDIN ServiceID.
- Choose a Dutch bank from which you want to buy your iDIN connection and sign a contract with them. The bank will fulfill the role of Acquirer for your iDIN connection.

Connecting to pre-production

- Go to pre-production portal of the chosen Acquirer**.**
- Contact technicalsupport@connectis.com to receive your signing certificate.
- Log in with the credentials provided by the bank, and go to Merchants → Services.
- Upload the signing certificate at the bottom part of the page.
- Send the following information to technicalsupport@connectis.com: Acquirer, MerchantID, Routing Service URL, and ServiceID

Going to production

- Follow the same steps as mentioned above to set up the production connection.
- You have to enable your iDIN production connection in the portal of your Acquirer. Log in to your Acquirer’s production portal and go to Merchants → Services.
- In the “Do tests” step, click “Confirm integration tests”. Check all the boxes to finish the process.



iDIN dialogues

Google SAML

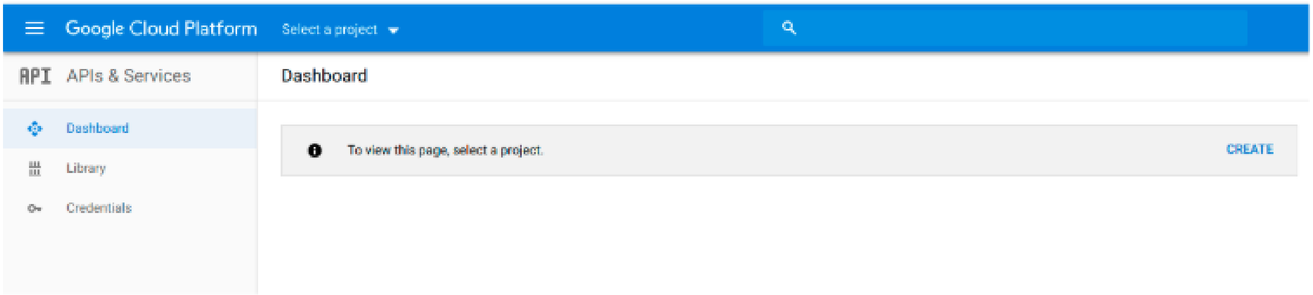
Please follow these steps to enable Google SAML IdP

- Log in to G Suite Admin Panel.
- Go to SAML App in Apps Section.
- Click on plus sign to add new application.
- Click on Setup my own custom app.
- Click on Option 2 Download to download the Google metadata.
- Enter the application name and description.
  This will be shown to the application's end-users. It can be the name of your application you wish to connect to the Connectis Identity Broker.
- Enter the following:
  - ACS
  - url
  - Entity ID Start url - This is the url that the user can click on to start the login process.
    You can find this information in the metadata of the Connectis Identity Broker.
- Select *Primary Email* as Name ID.
- Select email as Name ID format.
- Send the downloaded metadata from step 5 to technicalsupport@connectis.nl.
- When the metadata is processed, edit the new service by clicking on *Editing Service* to enable this application for the desired organisational units.

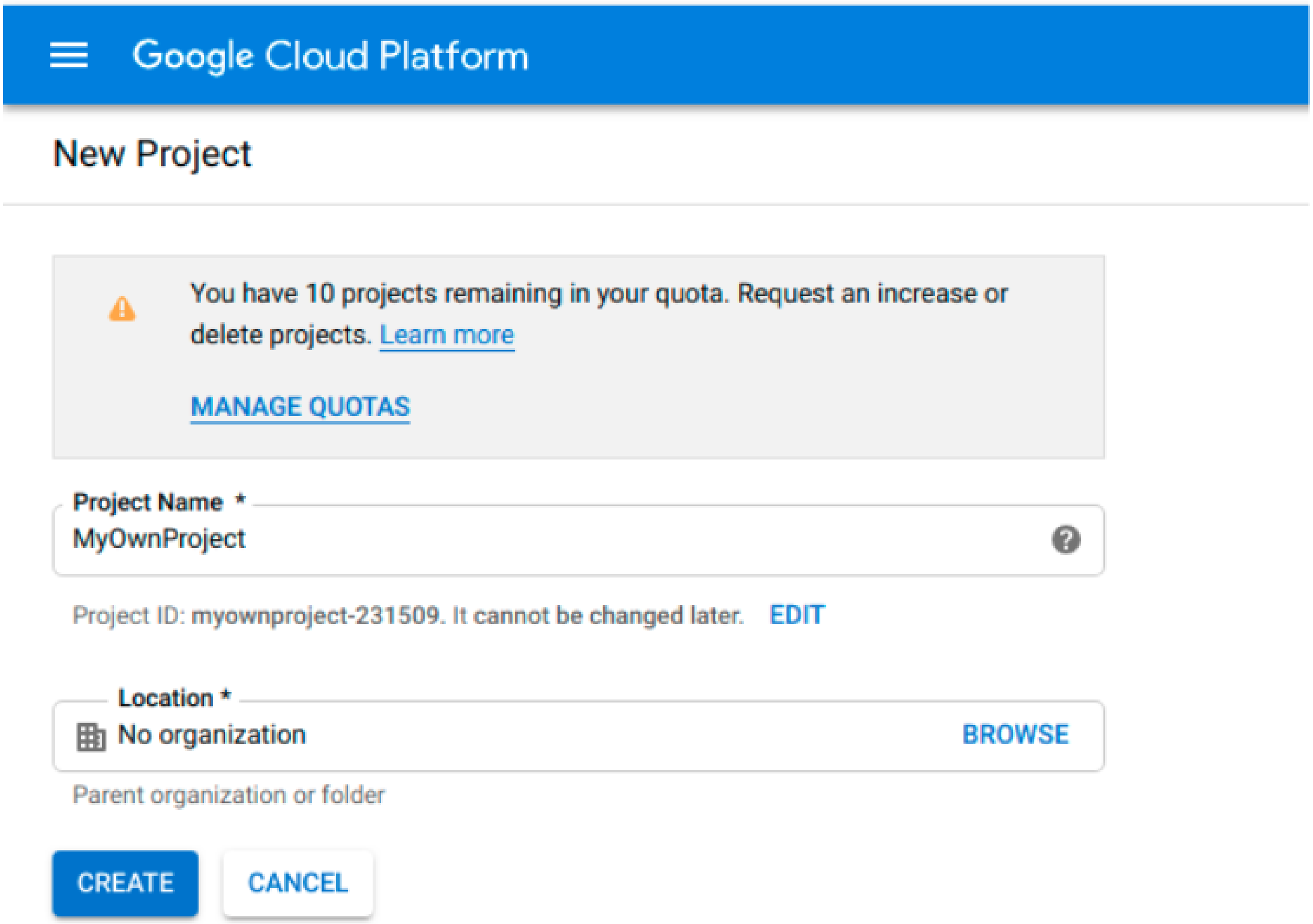
Google GSuite

Please follow these steps to connect Google as an eID

- Go to https://console.cloud.google.com/apis/
- Click on *Create* and create a new project



To view this page, select a project.



New Project

You have 10 projects remaining in your quota. Request an increase or delete projects. Learn more

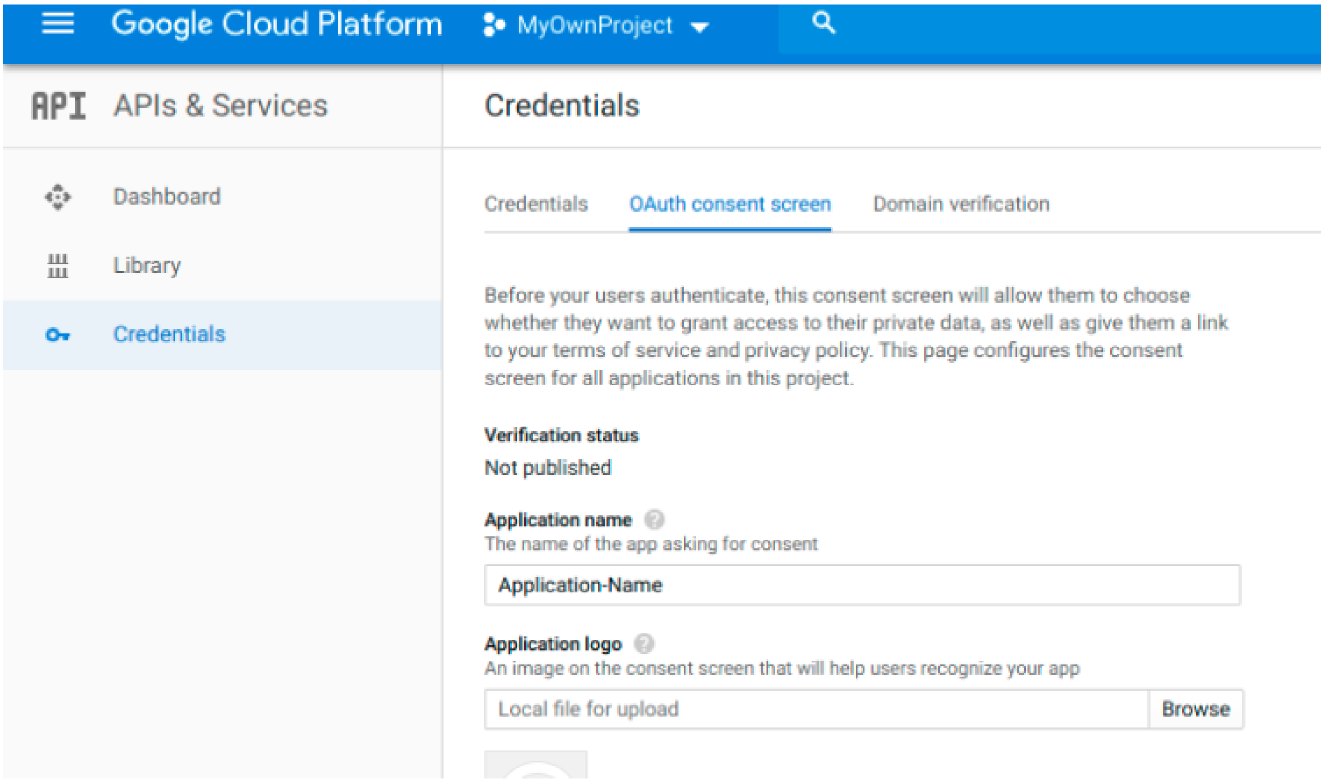
Project Name * MyOwnProject

Project ID: myownproject-231509. It cannot be changed later.

Location * No organization

Parent organization or folder

- Under Credentials -> OAuth Consent Screen setup:
  - Application name.
  - In authorised domains, enter your domain and the domain provided by Connectis.

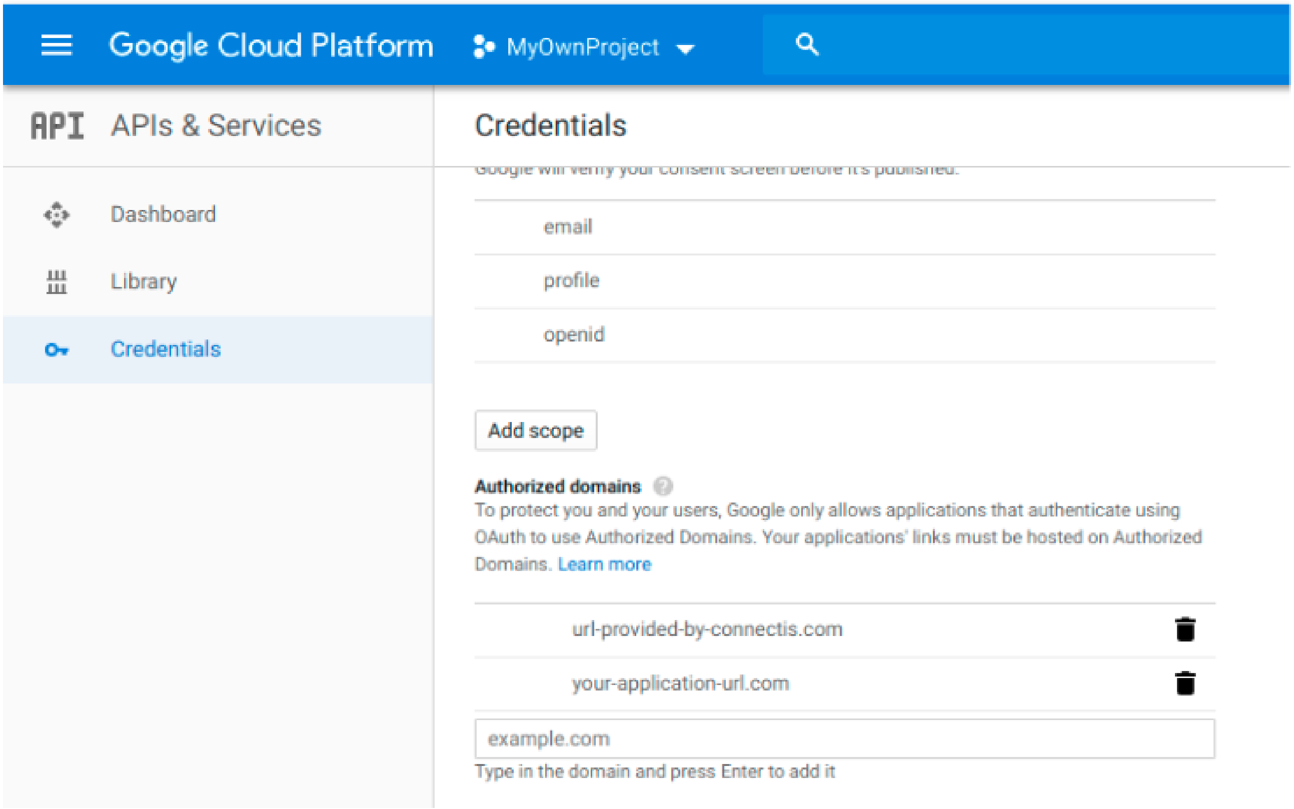


Before your users authenticate, this consent screen will allow them to choose whether they want to grant access to their private data, as well as give them a link to your terms of service and privacy policy. This page configures the consent screen for all applications in this project.

Verification status
Not published

Application name
The name of the app asking for consent
Application-Name

Application logo
An image on the consent screen that will help users recognize your app
Local file for upload



Google will verify your consent screen before it's published.

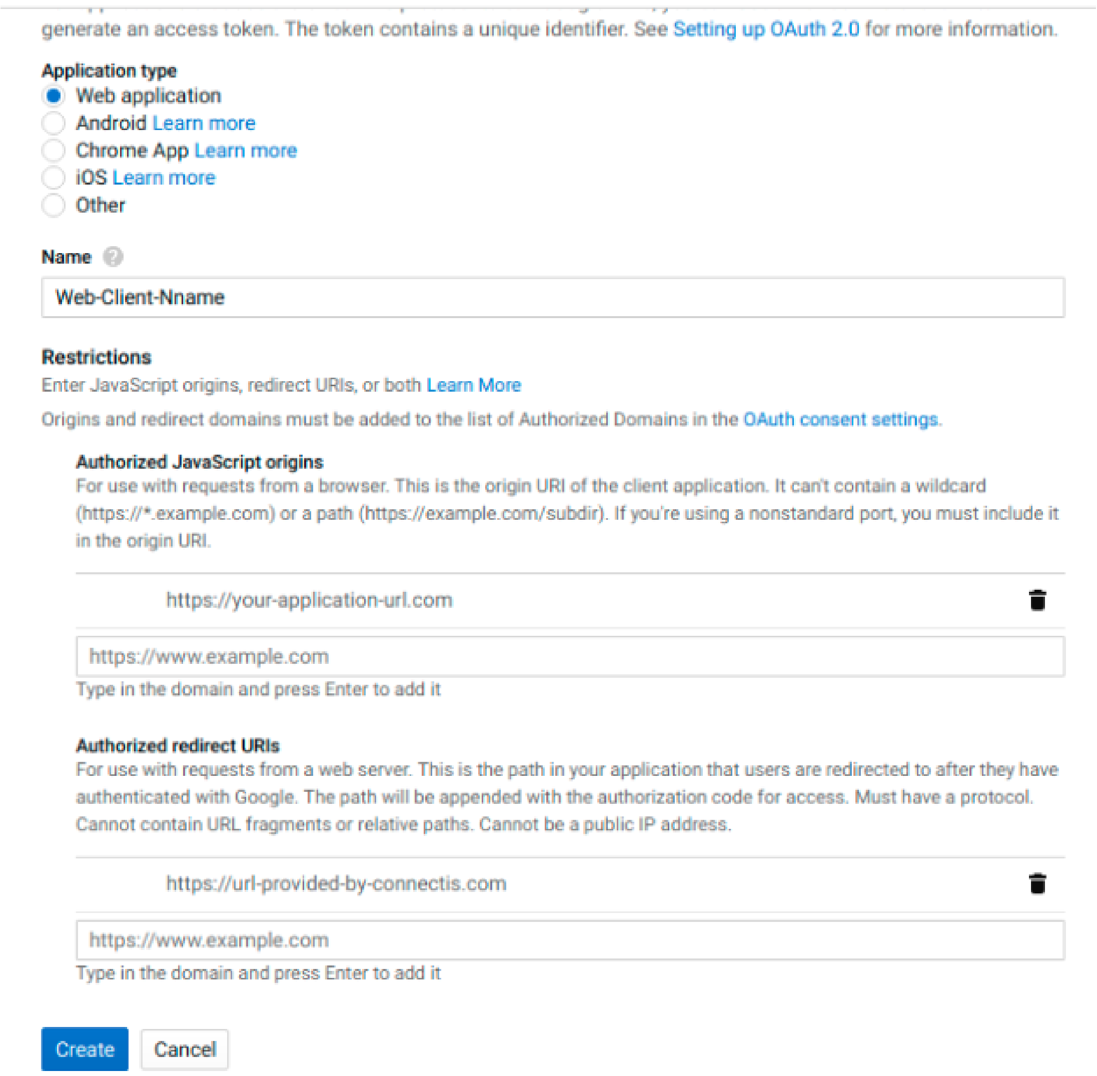
email
profile
openid

Authorized domains
To protect you and your users, Google only allows applications that authenticate using OAuth to use Authorized Domains. Your applications' links must be hosted on Authorized Domains. Learn more

url-provided-by-connectis.com
your-application-url.com
example.com
Type in the domain and press Enter to add it

- Create a new *OAuth eID* as *Web application* and enter values for:
  - Name.
  - Under *Authorised redirect URIs*, enter the url provided by Connectis.

Create OAuth client ID



generate an access token. The token contains a unique identifier. See Setting up OAuth 2.0 for more information.

Application type

● Web application
○ Android Learn more
○ Chrome App Learn more
○ iOS Learn more
○ Other

Name

Web-Client-Nname

Restrictions

Enter JavaScript origins, redirect URIs, or both Learn More

Origins and redirect domains must be added to the list of Authorized Domains in the OAuth consent settings.

Authorized JavaScript origins

For use with requests from a browser. This is the origin URI of the client application. It can't contain a wildcard (https://*.example.com) or a path (https://example.com/subdir). If you're using a nonstandard port, you must include it in the origin URI.

https://your-application-url.com

https://www.example.com

Type in the domain and press Enter to add it

Authorized redirect URIs

For use with requests from a web server. This is the path in your application that users are redirected to after they have authenticated with Google. The path will be appended with the authorization code for access. Must have a protocol. Cannot contain URL fragments or relative paths. Cannot be a public IP address.

https://url-provided-by-connectis.com

https://www.example.com

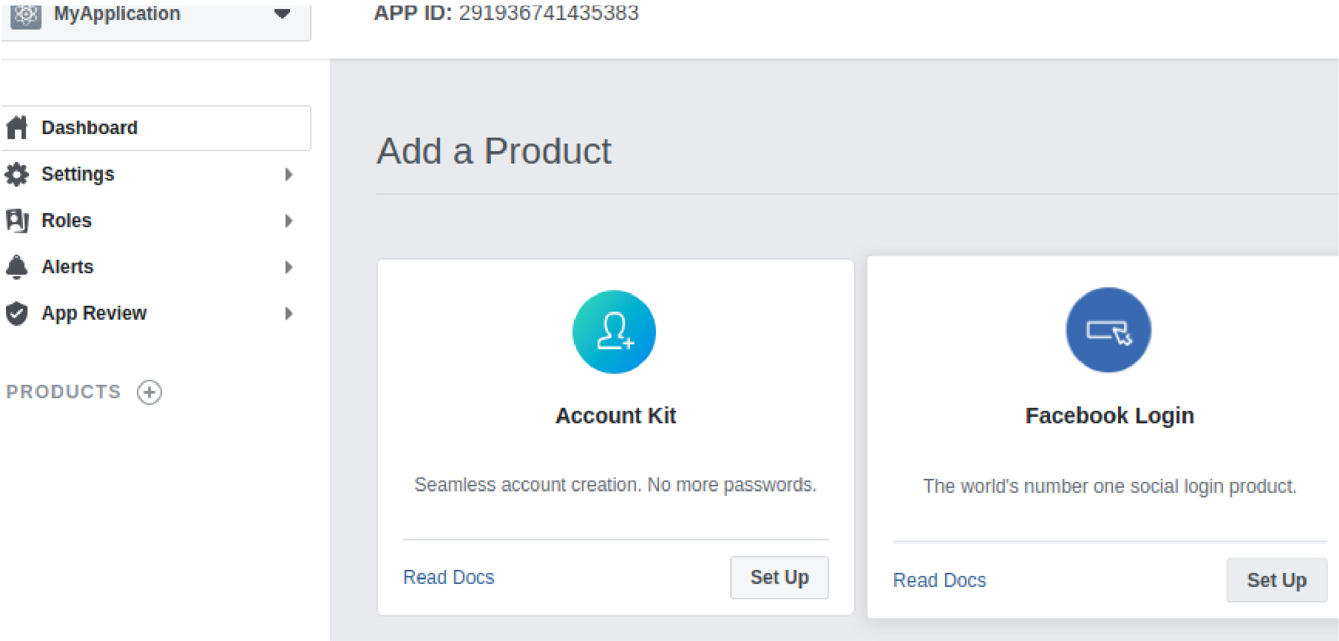
Type in the domain and press Enter to add it

- email the following information to technicalsupport@connectis.com:
  - Client ID
  - Client secret
  - Token endpoint
  - Discovery endpoint

Facebook

Please follow these steps to connect Facebook as an eID

- Go to https://developers.facebook.com/
- Click on *MyApp->Add a new App* and create a new application
- Click on *Products -> Facebook Login*, select *Web*, and complete your *Site url*.



APP ID: 291936741435383

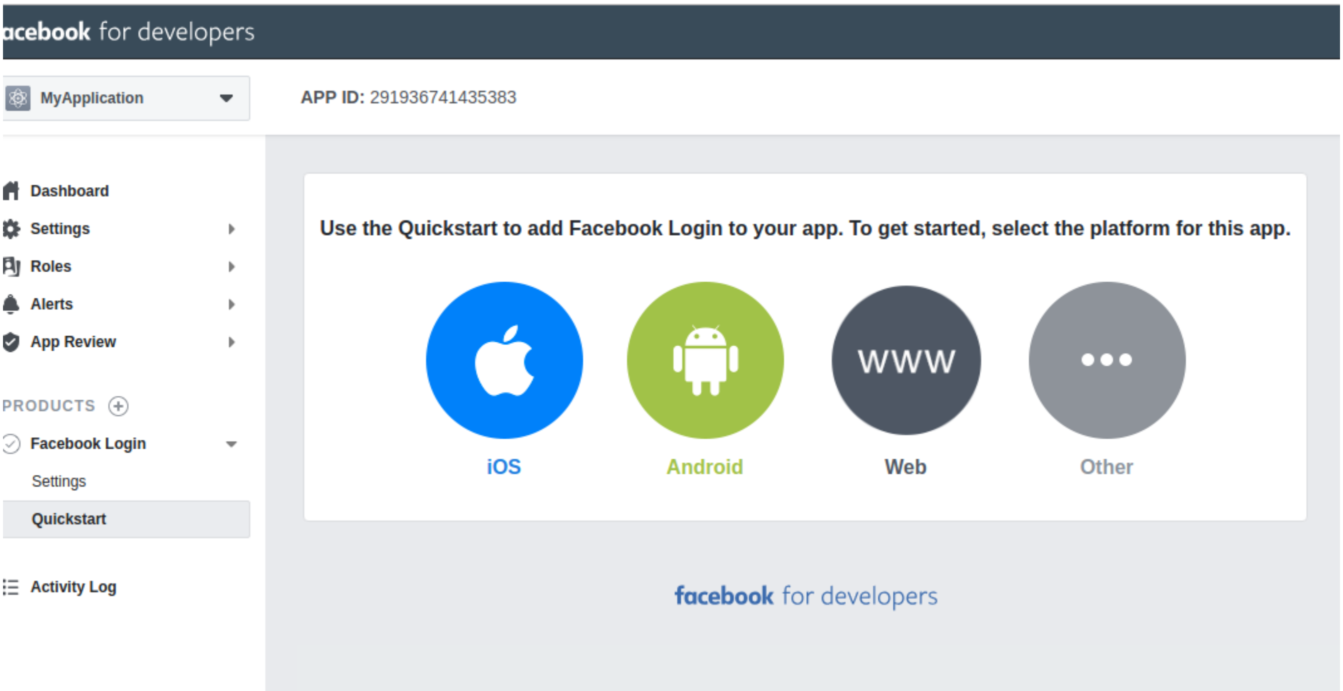
Add a Product

Account Kit

Seamless account creation. No more passwords.

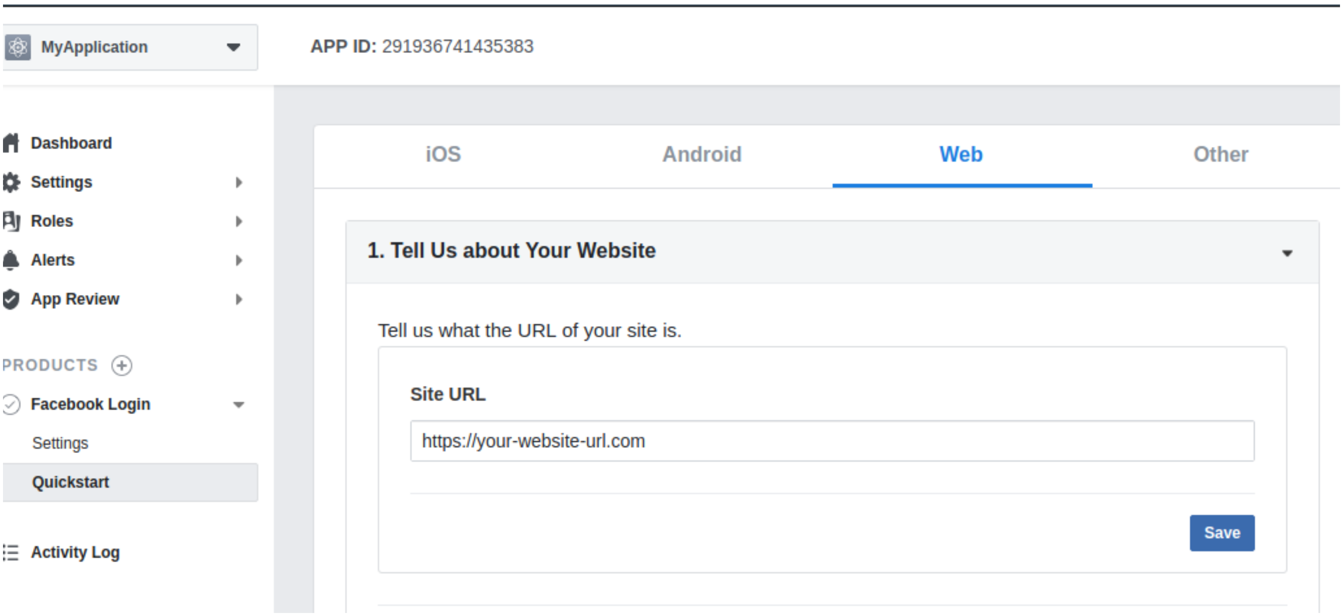
Facebook Login

The world's number one social login product.



APP ID: 291936741435383

Use the Quickstart to add Facebook Login to your app. To get started, select the platform for this app.

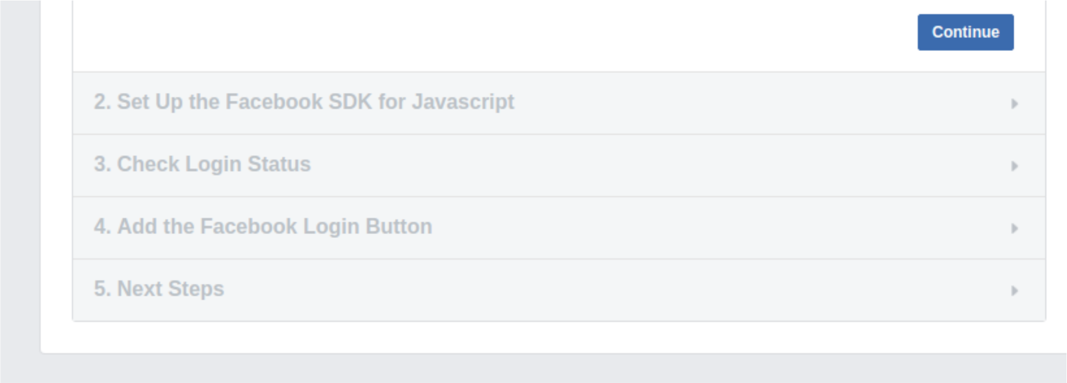


APP ID: 291936741435383

1. Tell Us about Your Website

Tell us what the URL of your site is.

Site URL: https://your-website-url.com



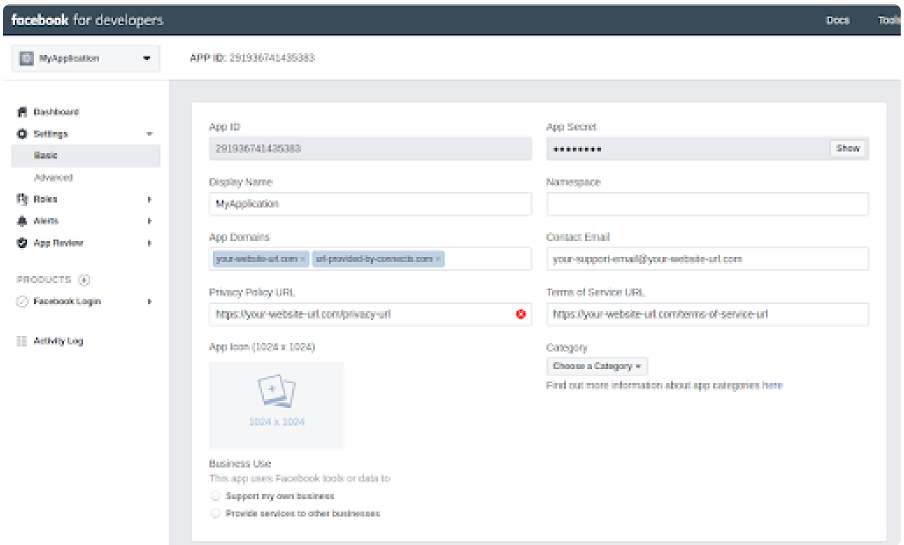
2. Set Up the Facebook SDK for Javascript

3. Check Login Status

4. Add the Facebook Login Button

5. Next Steps

- Please complete the following fields under *Settings -> Basic*:
  - *Display name*
  - *App domains* (both your domain and the domain provided by Connectis)
  - *Contact email*
  - *Privacy Policy url*
  - *Terms of Service url*



APP ID: 291936741435383

App ID: 291936741435383

App Secret: ••••••••

Display Name: MyApplication

Namespace:

App Domains: your-website-url.com × url-provided-by-connectis.com ×

Contact Email: your-support-email@your-website-url.com

Privacy Policy URL: https://your-website-url.com/privacy-url

Terms of Service URL: https://your-website-url.com/terms-of-service-url

App Icon (1024 x 1024)

Category

Find out more information about app categories here

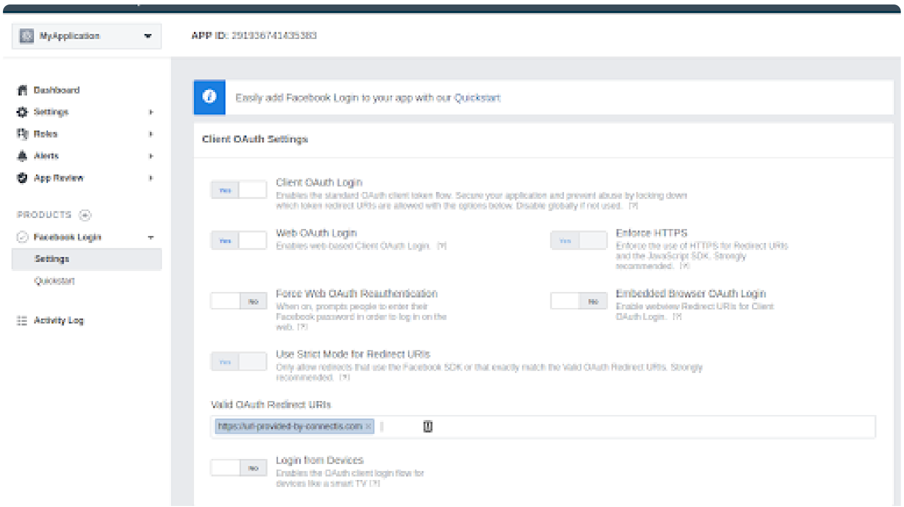
Business Use

This app uses Facebook tools or data to

○ Support my own business

○ Provide services to other businesses

- Under *Facebook login -> Settings*, please complete *Valid OAuth Redirect URIs* with the url provided by Connectis.



APP ID: 291936741435383

Easily add Facebook Login to your app with our Quickstart

Client OAuth Settings

Yes — 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 Client OAuth Login. [?]

Yes — Enforce HTTPS
Enforce the use of HTTPS for Redirect URIs and the JavaScript SDK. Strongly recommended. [?]

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
Enable webview Redirect URIs for Client OAuth Login. [?]

Yes — Use Strict Mode for Redirect URIs
Only allow redirects that use the Facebook SDK or that exactly match the Valid OAuth Redirect URIs. Strongly recommended. [?]

Valid OAuth Redirect URIs
https://url-provided-by-connectis.com ×

No — Login from Devices
Enables the OAuth client login flow for devices like a smart TV [?]

- Email the following information to technicalsupport@connectis.com:
  - Client ID
  - Client secret
  - Refresh Token endpoint
  - Authorization Token endpoint

Connecting a SAML 2.0 compatible eID

You can enable an eID via the Connectis Identity Broker if it supports SAML 2.0. Please follow these steps:

- Familiarise yourself with the SAML 2.0 protocol
- Identify which SAML 2.0 binding you want to use to receive SAML Requests from the Connectis Identity Broker, and to send SAML Responses back to the Connectis Identity Broker.
- Obtain SAML 2.0 metadata from your identity provider and send it to technicalsupport@connectis.com. Contact the supplier of the identity provider if you need additional help obtaining metadata.
- Contact technicalsupport@connectis.com to receive metadata of the Connectis Identity Broker and configure it on your identity provider.

Contact the supplier of your identity provider if you need additional help in configuring SAML 2.0 connections in your identity provider. Contact technicalsupport@connectis.com if you need to troubleshoot your connection.

Enabling your private authentication means via MyOwnIdP

By enabling MyOwnIdP, you can enable your own private authentication means. MyOwnIdP supports both usernames/passwords and X509 certificates as login tokens. If you have an existing system with usernames and passwords, you can import these accounts into MyOwnIdP. Like with any login method, you can configure a second factor.

Enabling username/password

Please follow these steps to enable MyOwnIdP in the Connectis Identity Broker for Username/Password:

- Choose which identifier you want to use for your users, for instance a username or an email address.
- Choose which user attributes you want to store in the user profile and receive in the login response.
- Choose a password policy. You can set up a minimal password length, forbid the user to select a password that has been used as the last X passwords, and set up a character set policy (e.g. demand request digits, capitalised and non-capitalised letters and symbols).

- Choose an account locking policy.
  We support two levels of account locking: Soft lock (which will be lifted after some time) and hard lock (which can only be lifted by support employees).
  - Incorrect password attempts for soft lock: Number of times a user can use an incorrect password before being soft-locked.
  - Number of soft lock before hard lock.
  - Soft lock duration in minutes.
- Choose if you want the passwords to expire after a given number of days, or whether you want them to be perpetual.
- Choose if you want to enable the password reset flow for forgotten passwords. This functionality requires that the users' email addresses are stored in the user profiles. If you want to enable this, send an email to technicalsupport@connectis.com with message, subject, and address. The email will be text-only.

Account registration functionality (optional)

When email addresses are used as login tokens, you can optionally enable Account Registration. Send an email to technicalsupport@connectis.com if you want to enable Account Registration. Please include the following information:

- Whether you want to enable pre-registration. Without pre-registration, every user that provides a valid email address can create an account. With pre-registration enabled, you control who can make accounts, because only users who are pre-registered in the Attribute Provider can create accounts.
- This involves two emails. Please provide the text you want to register for both emails:
  - Account successfully registered: It includes a link that, once clicked, allows the user to set up a password for his/her account.
  - Account already registered/cannot register: Error message.

MyOwnIdP migration/provisioning

We provide a REST API to provision new users and facilitate migration of user accounts. Contact technicalsupport@connectis.com to receive a copy.

User attributes

You can create user accounts in the attribute provider by creating resources with either one of these attributes filled. These attributes will be used by the user as the login field: Username login: urn:myownidp:authenticate:Username:username email address / X509 Login: urn:myownidp:authenticate:EmailAddress:emailAddress BSN Login: urn:digid:BSN:bsn

Important: The forgotten password functionality or account creation requires that an email is sent to the end user’s email address. As a consequence, urn:myownidp:authenticate:EmailAddress:emailAddress needs to be available for that specific user if you want to use the forgotten password functionality.

If you want to allow your end users to log in with username, you can provision the attribute "urn:myownidp:authenticate:Username:username", but if you also want them to be able to reset their password using the forgotten password functionality, then you need to provision "urn:myownidp:authenticate:EmailAddress:emailAddress" as well.

To provision attributes to the attribute provider, you can ask for the attribute provider API documentation with examples via technicalsupport@connectis.com.

Password manager

We provide another REST API to allow you to manage the passwords of your users. You can request the full API documentation with examples via technicalsupport@connectis.com.

You can either use the migration endpoint (allowing you to set the passwords with their current hashed version) or the manage endpoint, which allows you to set the password from a plain text. You can also perform password management operations by using that API and force a password change after the next login.

Enabling X509

Please consider that we log in users via this method by reading the EMAILADDRESS field on the certificate. Every user that wants to log in should be registered on the attribute provider with the “urn:myownidp:authenticate:EmailAddress:emailAddress” attribute set.

To enable X509 Login:

- Deliver the CA public certificate, which signs the client certificates used by users to log in, to technicalsupport@connectis.com.