Signicat Documentation

Configure Your Environment with MyConnectis

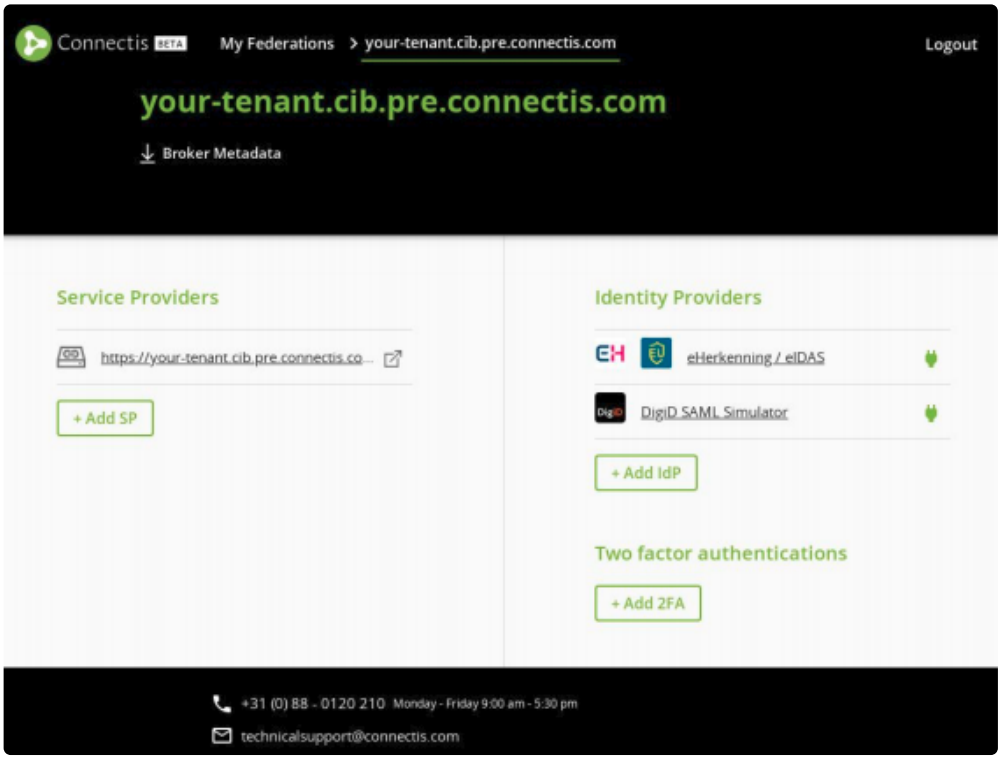
MyConnectis is the self-service portal for configuring your Connectis Identity Broker.

It enables you to configure the Service Provider connections and Identity Provider connections for your own environment.

This section describes everything you need to know to use MyConnectis for configuring and maintaining the configuration of your own environment.

Logging in

1. Go to https://portal.staging.connectis.org
2. Login with the account provided to you
3. Click on the name of the federation you wish to configure to open the dashboard page, from which you can administer your environment.

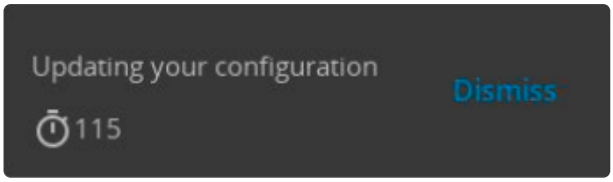


Tenant dashboard page

Depending on the situation, your tenant can run on a connectis.com subdomain or on a custom domain name.

Altering the configuration of your environment

If you alter the configuration in MyConnectis, your Connectis Identity Broker will be updated. A counter will be shown on the page indicating when the new configuration should be effective.



Counter indicating when new configuration will be effective

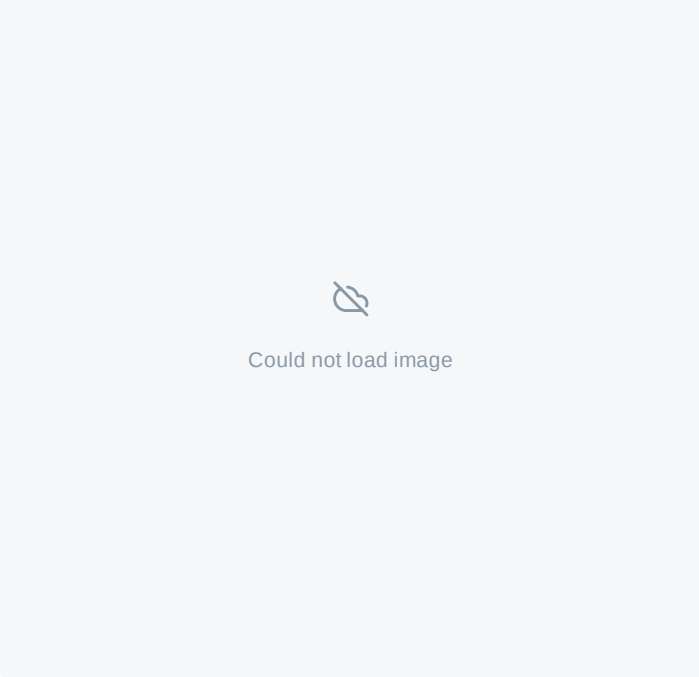
Manual MyConnectis

In this manual we will discuss how to set up the basics. For more information about managing all details in MyConnectis, see the other sections on this site.

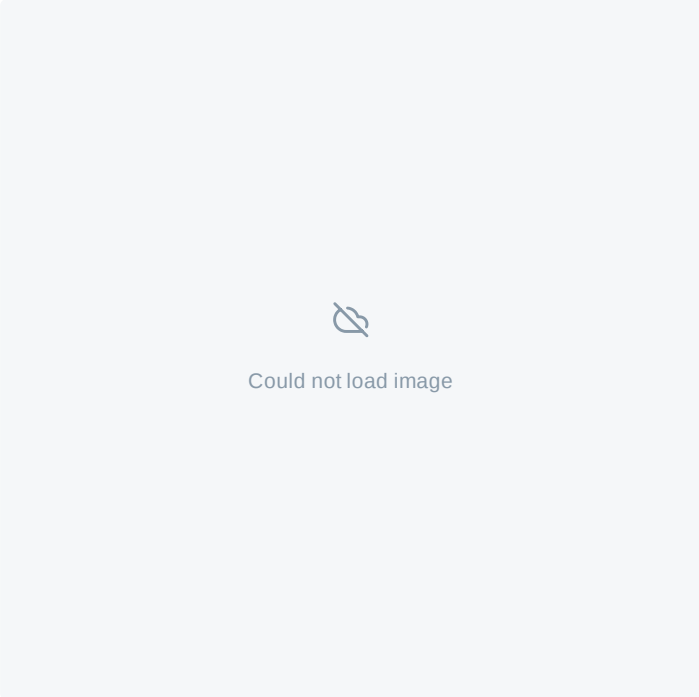
- Activate your account
- Manage Federations
- View configuration
- Add Identity Provider
- Start Service Provider Simulator

Activate your account

1.Click on the link you received via email to set up a password which will activate the account.



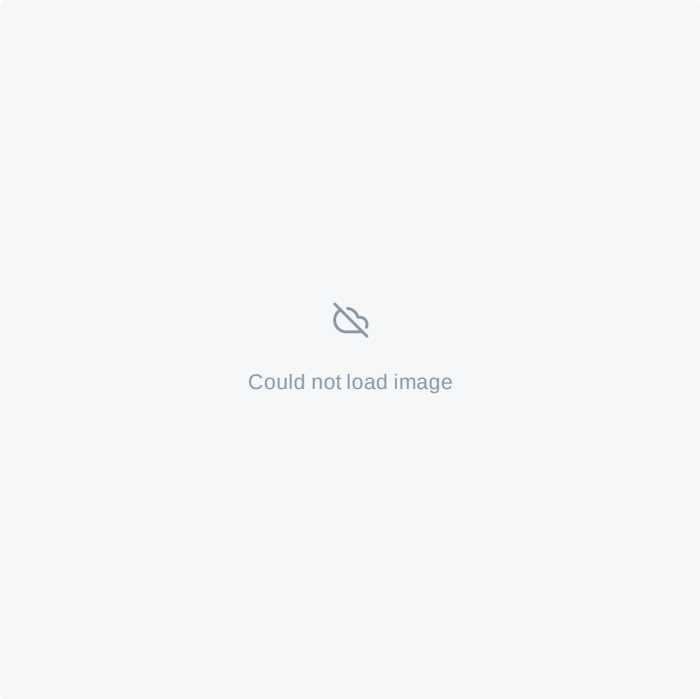
2. After activating your account you can log in with your username (email address) and password. If you want to log in at a later time you can use the link https://portal.staging.connectis.org/.



3. As you first log in, you will have to set up a Two factor authentication.
You can set up your Two factor authentication using an authenticator or mobile app that is used for scanning QR-codes. This can be the following apps or authenticators: Google Authenticator for Andriod, Google Authenticator for Iphone, Authy for Andriod, Authy for Iphone or any authenticator app that supports TOTP protocol.

Scan the QR-code and you will receive a 6-digit code to enter in the ´Confirm TOTP Code´field.

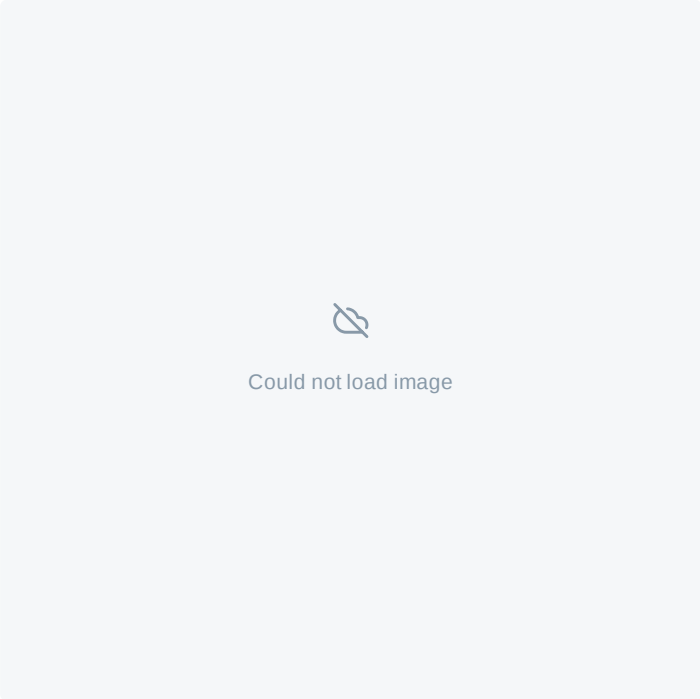
Your Two Factor authentication has now been set.



Manage Federations

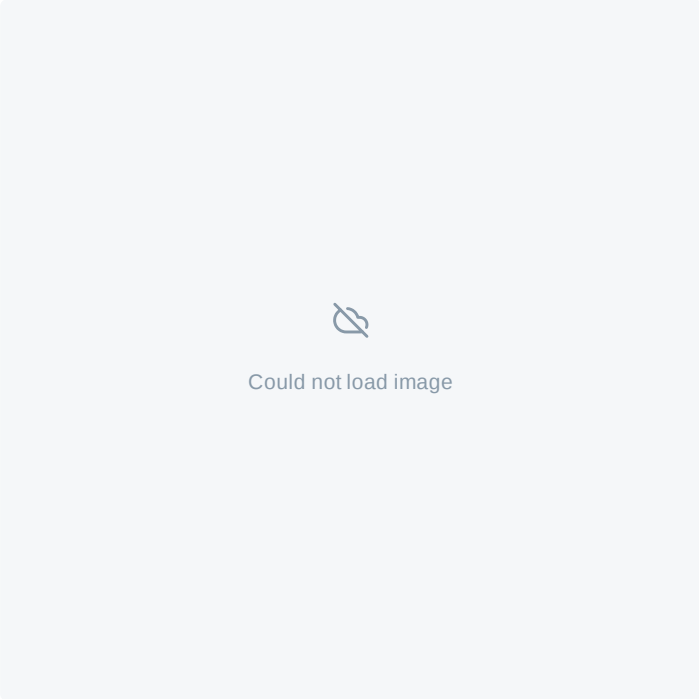
1.After logging in you will find the Federations which you can manage.

Click on the Federation you want to manage. This will open the overview of your Federation.



2. On the left side you can find the configured Service Providers. The right side shows you the configured Identity Providers and the Two factor authentication methods that have been set up.

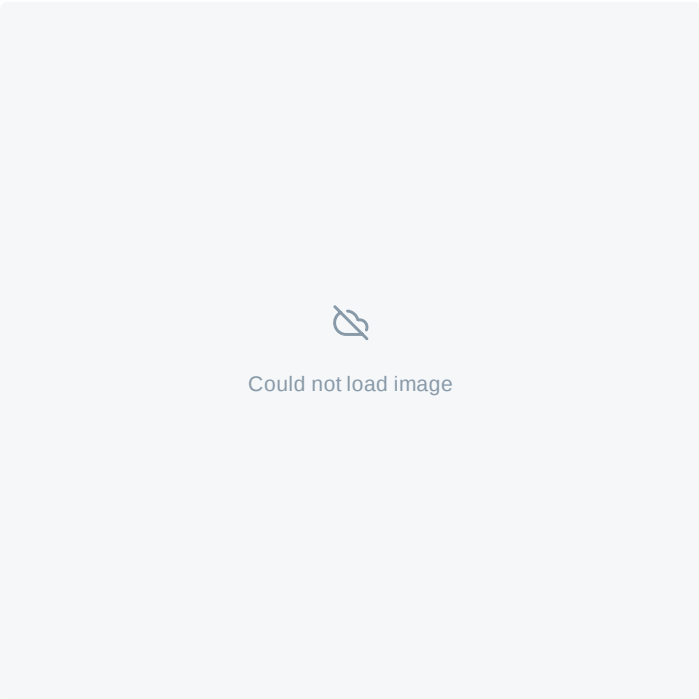
For a new Federation there will be one test Service Provider configured and no Identity Providers or two factor authentication methods.



View configuration

Click on the listed Service Provider to view its configuration.

On this page you can find the Metadata of your Connectis Identity Broker and the Service Provider as well as various other options.

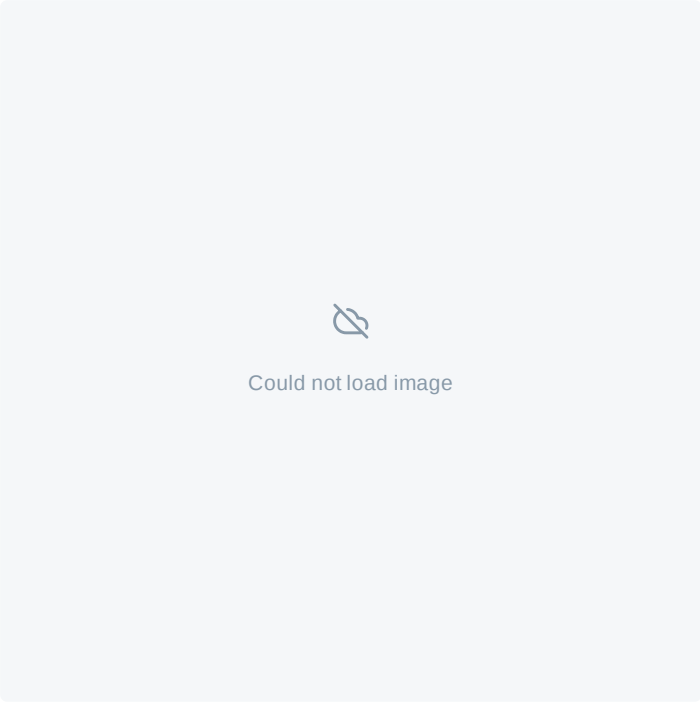


Close the screen to go back to the overview.

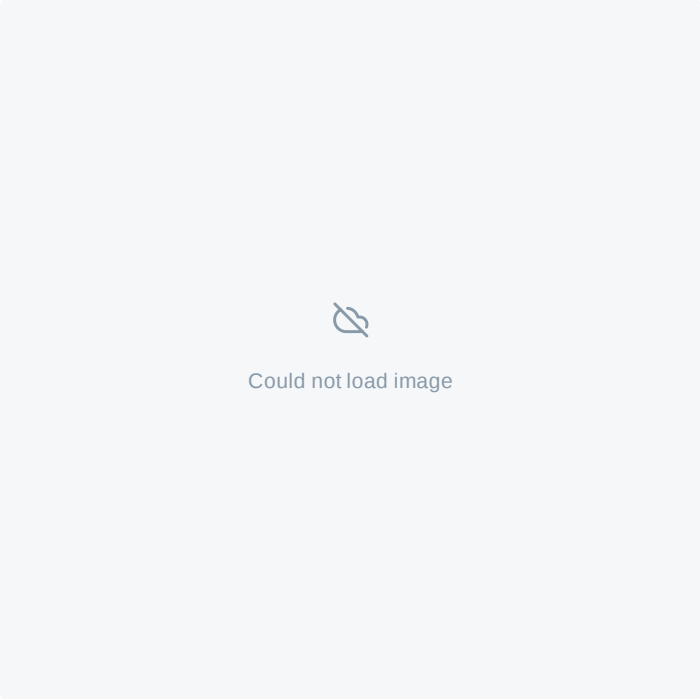
Add Identity Provider

When back in the overview screen, click on Add idP on the right side of the screen.

On the next screen, select the Identity Provider you want to add. For the Trial it is best to start by adding the DigiD SAML Simulator and follow the instructions on the underlying page.



DigiD SAML Simulator has now been added to the Identity Providers



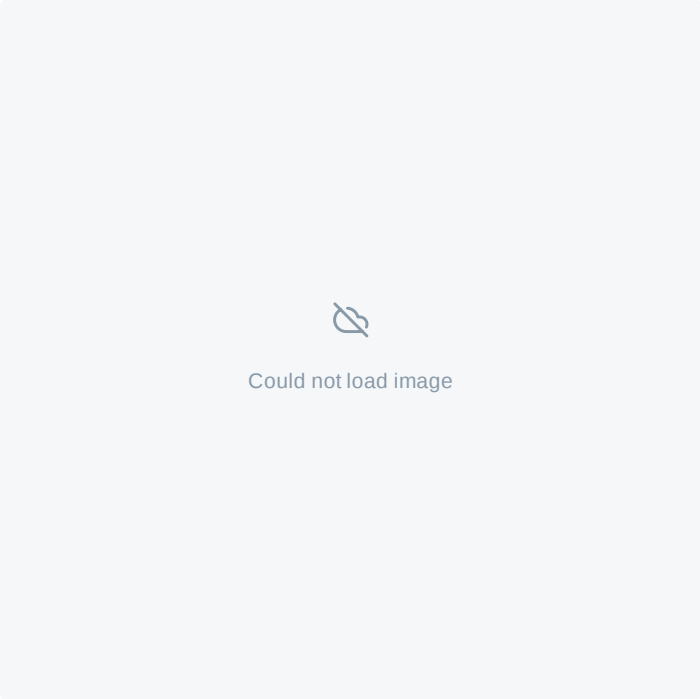
In a similar fashion, you can easily add eH/eIDAS and iDIN. Do not change any of the settings, but just click the Add button.

Start Service Provider Simulator

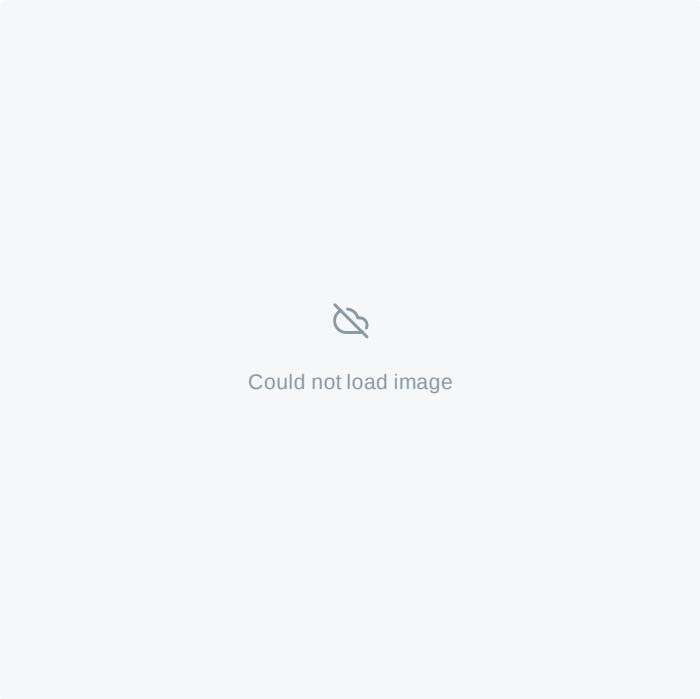
1.To start the Service Provider simulator, copy the Service Provider link in the browser or click on the box with the arrow.

Please note that you will have to add /sp-simulator to the link

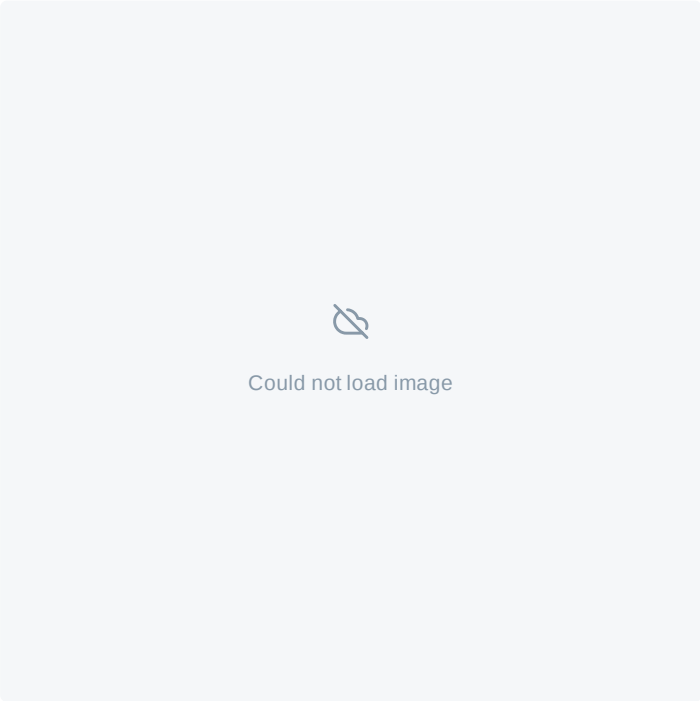
The link will look like this https://(yourfederationname).cib.pre.connectis.com/**sp-simulator**



2. On the next screen you can edit the parameters and click on ´OK´.
For the trial nothing has to be edited.



3. In the next screen you can select the Identity Provider that has been added, in this case: Connectis DigiD Simulator. After clicking the Identity Provider you can now log-in using the DigiD Simulator.

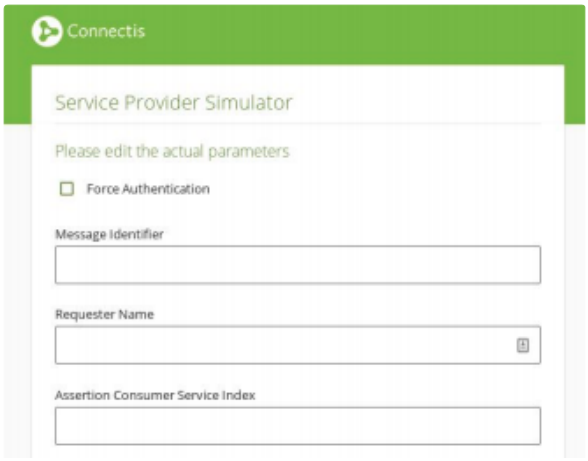


Performing a login flow using the Service Provider Simulator

Your Connectis Identity Broker pre-production environment comes with a Service Provider Simulator that you can use to test before adding your own Service Provider application.

Follow these steps to perform a login flow with the SP Simulator:

1. Login to MyConnectis
2. Note your tenant's URL, e.g. your-tenant.cib.pre.connectis.com in the figure above
3. Browse to url-of-your-tenant**/sp-simulator**, e.g. https://your-tenant.cib.pre.connectis.com**/sp-simulator**
4. The Service Provider Simulator will appear.



Service Provider Simulator

1. Click OK
2. Perform the login flow
3. Inspect the response as received by the Service Provider Simulator

Tip: The default values in the Service Provider Simulator will work to perform a login flow. You can however use the fields in the Service Provider Simulator to send altered requests to test various scenarios. The following additional fields are available in the SP Simulator:

Force Authentication: This option sets the ForceAuthn attribute to true on the SAML AuthnRequest sent to the Connectis Identity Broker (default value: false). This means that users will always have to login at the IdP, even though they still have an active session.

Requester name: Defines the attribute “ProviderName” on the SAML AuthnRequest sent to the Connectis Identity Broker. This appears on the SAML request and has no functional effect.

Protocol Binding: Defines the attribute “ProtocolBinding” on the SAML AuthnRequest. If left blank, the Broker will infer the SAML binding used between the different bindings available (such as POST, Redirect, etc.).

Attribute Consuming Service Index: The Service Index from eHerkenning or eIDAS that you wish to request a login for.

Level of Assurance: The level of assurance that the SP will request from the Connectis Identity Broker.

Configuring Service Providers

A list of coupled Service Providers is provided on your environment's dashboard page. Connectis will preconfigure one Service Provider simulator on pre-production environments, which you can use to simulate logout requests and inspect login responses. See Performing a login flow using the Service Provider Simulator on how to use this.

SAML

To add your own SAML Service Provider application, follow these steps:

1. Download the metadata of your Service Provider application.
2. Click *Add SP* on the dashboard page of your environment.
3. Download the Connectis Identity Broker metadata and upload this to your application. (The Connectis Identity Broker metadata is also available from the Dashboard page.)
4. Upload the metadata of your Service Provider and Save your new Service Provider. The metadata needs to adhere to the following requirements:
    1. Contains at least one signing certificate
    2. Contains at least one Assertion Consuming Service
    3. Contains at least one Country Code in Accepted Countries (each country code is 2 uppercase letters)
    4. Contains at least one Display Name
    5. Contains an Entity Id
    6. Contains an Organization containing at least one Display Name
5. In the Advanced section, select the *Protocol Configuration*, *Attribute Configuration* and *Levels of Assurance* you want to use. Note: the default selected configurations work in most scenarios. You only need to change these if you have specific requirements.
6. Click *Save & Close*.
7. Browse to your Service Provider application and login. You should now be able to login to your Service Provider application using the Connectis Identity Broker.

OpenID Connect

To add your own OpenId Service Provider application, follow these steps:

1. Click Add OpenId SP on the dashboard page of your environment.
2. Complete mandatory fields:
    - Client Id
    - Client Type
    - Client secret (only when Client Type is Server Application)
    - Client Secret Expiry Date (only when Client Type is Server Application)
        - This value is default 1 year in the future
    - JWT Claims Validity (in days)
    - Token expiration (in seconds)
        - Authorization Code (maximum 3 minutes)
        - Access Token (maximum 31 days)
        - Refresh Token
    - Encryption Certificate
    - Redirect Endpoints (redirect endpoint to your application)
3. Click *Save & Close*
4. Browse to your Service Provider application and login. You should now be able to login to your Service

Provider application using the Connectis Identity Broker.

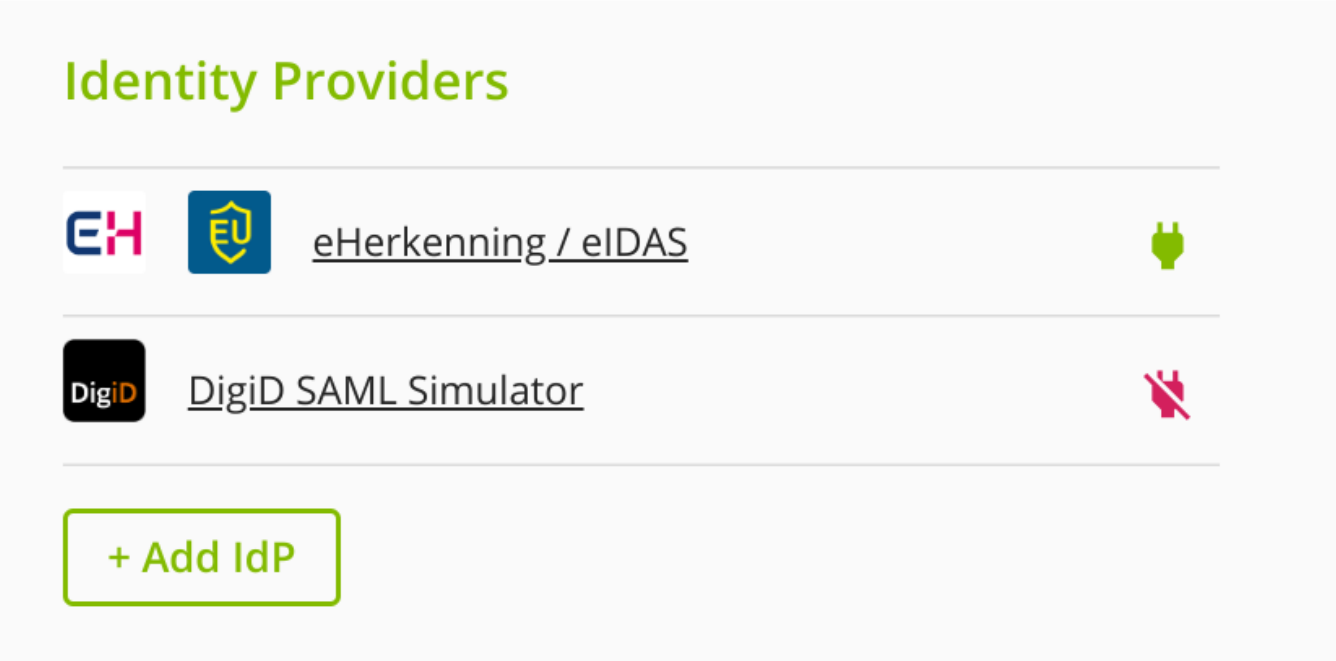
Configuring Identity Providers

A list of coupled Identity Providers is provided on your environment's dashboard page. Identity Providers that are listed here will be available for your users upon activation .

You can add new Identity Providers by clicking *Add IdP* on the dashboard page. On the next screen, select the Identity Provider you want to add and follow the instructions on the underlying page of that specific Identity Provider.

Please contact Connectis Technical Support for assistance if the Identity Provider you wish to add is not on the selection screen.

You can temporarily disable Identity Providers by clicking the connector icon next to the Identity Provider that you want to temporarily disable on the Dashboard page. To re-enable the Identity Provider, simply click on the connector icon again.



Connector icons for enabling & disabling connections

You can permanently delete an Identity Provider connection by opening this Identity Provider and clicking the Delete button on the bottom of the page.

Configuring DigiD SAML Simulator

After selecting the DigiD SAML Simulator Identity Provider on the Choose Identity Provider screen, simply click the "*Add DigiD Simulator Connection*" link on the page. The DigiD SAML Simulator will be configured automatically.

Press the *Close* button on the bottom of the screen to return to the dashboard page.

Enable the connection on the dashboard to make it available for your customers.

See DigiD Simulator on how to use the DigiD SAML Simulator.

Configuring DigiD

After selecting the DigiD SAML Identity Provider on the Choose Identity Provider screen, the page will show you the steps for requesting a DigiD SAML connection at Logius.

See Configuring eIDs - DigiD for more information on the process of getting a DigiD connection.

1. Download the Connectis Identity Broker metadata file.
2. Fill in the request form on the Logius website (see link in step 2 on the page). Use the metadata downloaded in step 1, as well as the public part of the certificate you have received from Connectis when setting up the custom domain name.
    1. If you require assistance in filling in the form on the Logius website, please contact Connectis Technical Support.
    2. Note that for a production connection, Logius will first need to test your pre-production connection. See DigiD SAML 2.0 for more information.
3. Print out the form that you received from Logius via email, sign it, and send it to Logius by regular mail.
4. Logius will send you a confirmation when the connection has been created.
5. Click the "*Add DigiD Connection*" link on the bottom of the page to add the connection.
    1. Note that the connection will not actually work until Logius has confirmed that the connection has been created on their end.
6. Press the *Close* button on the bottom of the screen to return to the dashboard page.
7. Enable the connection on the dashboard after receiving notification from Logius that the connection is created.
8. The connection is now available for your customers.

Configuring eHerkenning / eIDAS

After selecting the eHerkenning / eIDAS Identity Provider on the Choose Identity Provider screen, the page will show you the steps for setting up the eHerkenning or eIDAS connection.

See Configuring eIDs - eHerkenning and/or eIDAS for more information about setting up a eHerkenning and eIDAS connection.

1. Fill in your OIN number. Note that this value might be pre-filled if it could be retrieved from your Service Provider metadata. If you using MyConnectis as a Trial, use the Connectis OIN for this value (00000003244440010000)

2. Click *Save* to save your OIN.
3. Contact Connectis Technical Support to configure your Service Catalog entries. (This functionality will be added to MyConnectis at a later stage.)
4. Click the "*Add Connectis eHerkenning Broker Connection*" link to add the connection.
5. Press the *Close* button on the bottom of the screen to return to the dashboard page.
6. After Connectis Technical Support has informed you that the Service Catalog entries have been created, you can enable the connection on the dashboard.
7. The connection is now available for your customers.

Configuring iDIN

After selecting the iDIN Identity Provider on the Choose Identity Provider screen, the page will show you the steps for setting up the iDIN connection.

See Configuring eIDs - iDIN about more information on setting up an iDIN connection.

1. Fill in your Merchant ID, which you have received from the bank you have signed a contract with. Note that if you want to use the Connectis iDIN Simulator, the Merchant ID does not need to be changed.
2. Fill in your Merchant sub ID if you have one.
3. Select the Acquirer (bank) that you have a contract with. If you want to use the Connectis iDIN Simulator, select it here.
    1. Note, if you bank is not on the list, please contact Connectis Technical Support.
4. Select those attributes you wish to have returned. The Service ID is automatically generated based on the selection. Note that if you deselect BIN, you will receive the *Transient ID* identifier.
5. Click the "*Save & close*" button to save the configuration and add the connection. You will be redirected to the dashboard page.
6. Enable the connection on the dashboard to make the connection available for your customers.

Configuring 2FA Identity Providers

A list of coupled 2-factor authentication (2FA) Identity Providers is provided on your environment's dashboard page. 2FA Identity Providers listed here will be available for your users upon activation.

You can add new Identity Providers by clicking *Add 2FA* on the dashboard page. On the next screen, select the 2FA Identity Provider you want to add and follow the instructions on the underlying page of this 2FA Identity Provider.

If the 2FA Identity Provider you wish to add is not available on the selection screen, please contact Connectis Technical Support for assistance.

You can temporarily disable 2FA Identity Providers by clicking the connector icon next to the 2FA Identity

Provider that you want to temporarily disable. To re-enable the 2FA Identity Provider, simply click the connector icon again.
You can permanently delete a 2FA Identity Provider connection by opening this 2FA Identity Provider and clicking the Delete button on the bottom of the page.

For configuring the 2FA Identity Provider in the login flow, please contact Connectis Technical Support for assistance.

Configuring 2FA SMS

After selecting the SMS 2FA Identity Provider on the Choose A Second Factor screen, the page will show you the steps for setting up the SMS 2FA connection.

1. Select whether or not *Self Registration* is allowed. Self-registration means that the user can register his phone number himself during the login flow, if no 2FA method has yet been registered. If self-registration is not allowed, the Service Provider needs to register the user's phone number.
2. Provide a *Sender*. The Sender data is what the user will see on his phone as sender of the SMS message.
3. Provide a value for the Token *Character Length*. This setting determines how many characters the token sent to the user via SMS has.
4. Provide a value for the *Token Validity Time*. This setting determines how long (in seconds) the user has to enter the token sent via SMS before it becomes invalid.
5. Click the "*Save & Close*" button on the bottom of the page to save the settings and return to the dashboard page.
6. Contact Connectis Technical Support to finalise the configuration in the login flow if you have not already done so. When they inform you that the flow configuration has been finalised, you can enable the connection on the dashboard.
7. The connection is now available for your customers.

How does it work

1. User logs in with first factor (for instance, a username / password combination).
2. User is asked to perform a second factor login.
3. In the case of SMS, a Token is sent to the user's registered phone number via SMS.
4. User fills in the Token received via SMS.
5. User is logged in with a second factor authentication.

Features:

Self-registration

Self-registration means that the user can register his phone number himself during the login flow, if no 2FA method has yet been registered. For example: A user logs in for the first time and does not yet have a 2FA method registered. During the login flow, the user is able to provide his/her phone number to register the 2FA SMS method. The phone number will be verified during this registration flow.

If self-registration is not allowed, the Service Provider needs to register the user's phone number in the database before the user can use the 2FA SMS method during the login flow.

Change phone number (during login flow)

If the user's phone number is already registered, he can change his phone number during the login flow by selecting the option in the login screen. The user will first need to perform the 2FA authentication on his currently registered phone before he can provide a new phone number, which is validated during the same flow.

After the phone has been validated, the user will receive the SMS message on his new phone number during the next login session.

Soft lock

The soft lock setting has been set to 10 tries, which means that a user can get his 2FA option wrong 10 times before his account is temporarily locked. The soft lock is automatically undone after the validation period of the SMS token has ended (approximately 3 minutes). The counter for tracking the number of wrong login attempts is cleared after a successful login for that account.

Configuring 2FA TOTP

After selecting the TOTP (Temporary One Time Password) 2FA Identity Provider on the Choose A Second Factor screen, the page will show you the steps for setting up the TOTP 2FA connection.

1. Select whether or not if *Self Registration* is allowed. Self-registration means that the user can register his Authenticator app on his phone himself during the login flow, if no 2FA method has yet been registered. If self-registration is not allowed, the Service Provider needs to generate the QR code and register the user's shared secret.

2. Provide an *Authentication App Issuer Name*. The issuer data is what the user will see in his authenticator app on his phone as the identifier of the Service Provider.
3. Provide the number of Attempts before *Soft Lock*. This setting indicates how often a user can get his 2FA option wrong before his account is temporarily locked.
4. Click the "*Save & Close*" button on the bottom of the page to save the settings and return to the dashboard page.
5. Contact Connectis Technical Support to finalise the configuration in the login flow if you have not already done so. When they inform you that the flow configuration has been finalised, you can enable the connection on the dashboard.
6. The connection is now available for your customers.

How does it work

1. User logs in with first factor (for instance, a username / password combination).
2. User is asked to perform a second factor login.
3. In the case of TOTP, User fills in the Token generated in his authenticator app on his phone.
4. User is logged in with a second factor authentication.

Features:

Self-registration

Self-registration means that the user can register his authenticator app on his phone number himself during the login flow, if no 2FA method has yet been registered. For example: A user logs in for the first time and does not yet have a 2FA method registered. The user can scan the generated QR code with his authenticator app during the login flow and confirm it by filling in the generated Token.

If self-registration is not allowed, the Service Provider needs to register the shared secret (from the generated QR code) for the user in the database before the user can use the 2FA TOTP method during the login flow.

Change shared secret (during login flow)

If the user suspects that the shared secret might have been compromised, he can change it during the login flow by selecting the option on the screen on which the TOTP token is provided. When this option is selected, the user will, upon successfully providing the TOTP token, see a new QR code that he can scan with his authenticator app. When this is done, and it is validated by providing the TOTP token generated in the authenticator app, the shared secret is changed and the user continues the login flow.

Add extra device (during login flow)

If the user wants to add an extra device for the TOTP 2FA, he can do so by selecting this option in the login screen. After the TOTP has been validated, the user will see the QR code that he can scan with the new device. Upon validating the new device with an additional TOTP token, the new device can also be used for the 2-factor authentication using TOTP.

Soft lock

This setting indicates how often a user can get his 2FA option wrong before his account is temporarily locked. For instance, if the soft lock count has been set to 5, a user will be temporarily blocked after 5 consecutive wrong login attempts. The soft lock is automatically undone after the configured time has expired, which is 30 seconds for TOTP, as the TOTP code is only valid for 30 seconds. The counter for tracking the number of wrong login attempts is cleared after a successful login for that account.

Hard lock

The hard lock is set to 10. This indicates that the user will be indefinitely blocked after 10 consecutive wrong login attempts. The hard lock can only be undone after the Service Provider has re-enabled the account. The counter for tracking the number of wrong login attempts is cleared after a successful login for that account.

Configuring Broker Features

Please contact Connectis Technical Support for assistance with configuring any of the specific Connectis Identity Broker features.

The configuration of the Connectis Identity Broker features will soon become available in MyConnectis.