



# Federated SSO Quick Start Guide Okta

Concord Technologies

2025 First Avenue Suite 800

Seattle, WA, 98121, USA

Call Us: +1 206-441-3346

[Concord.net](http://Concord.net)

## Contents

Overview .....	2
Okta Application Registration.....	3
Section 1: Concord Portal Federation Configuration – Phase 1 .....	3
Section 2: Okta Application Creation.....	6
Section 3: Concord Portal Federation Configuration – Phase 2.....	12
Best Practices.....	14
Getting Help .....	16
Appendices .....	17
Appendix A – Custom Claims .....	17

## Overview

This document is intended to provide information on setting up federation in your Okta and Concord environments. The process of creating a federated relationship between Okta and Concord consists of registering an application on the Okta portal and copying bits of information between the Okta portal and the Federation tab on the Concord admin portal.

This document will provide a basic set of instructions for registering the application on the Okta portal as well as what information needs to be copied from the Okta portal to the Concord portal and vice versa.

**Note** that Concord does not control or maintain the configuration settings within Okta. While the steps depicted in the following document have been used to successfully configure Federation in Okta, these may be subject to change and additional configuration may be needed to achieve your own desired results. You are advised to consult Okta's OpenID Connect documentation for further assistance as needed.

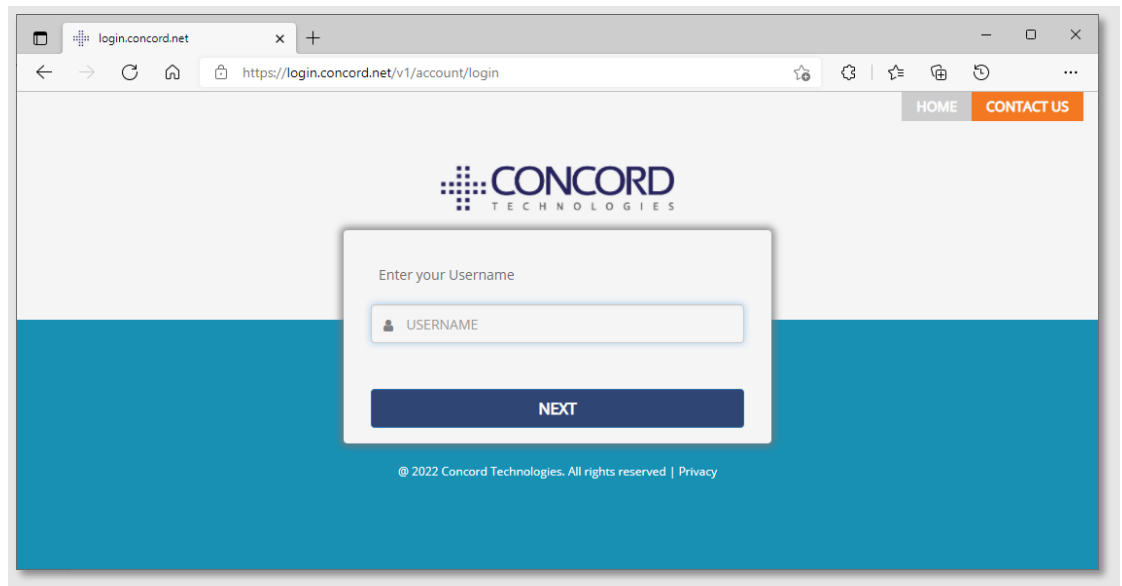
Concord is not responsible for any issues or service interruptions resulting from configuration steps taken in Okta or the Concord Admin Portal to configure or enable federated access to Concord services.

For more detailed information on this integration, or for integrating other federation providers, please see the more comprehensive Concord Federation Admin & User Guide.

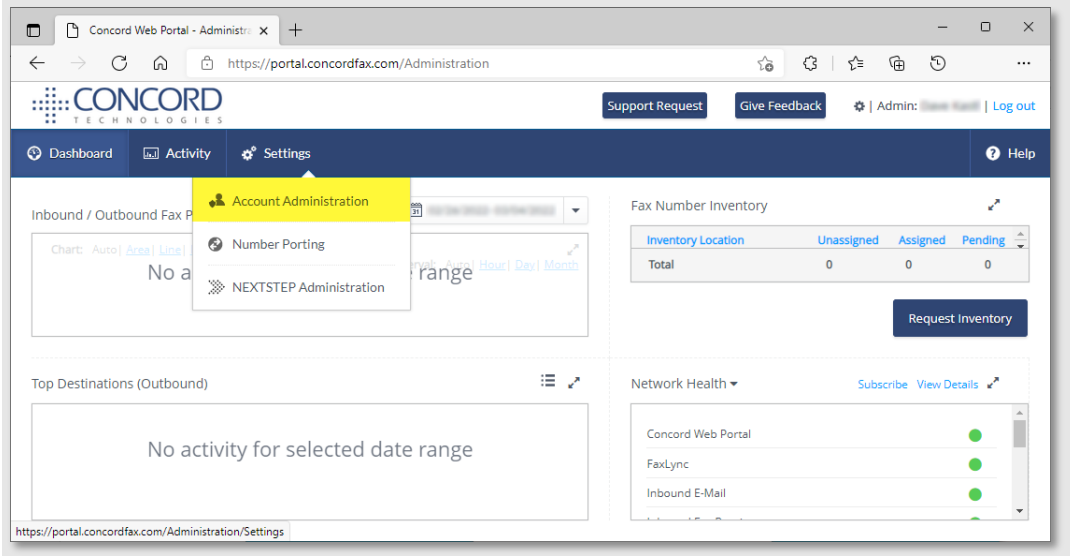
# Okta Application Registration

## Section 1: Concord Portal Federation Configuration – Phase 1

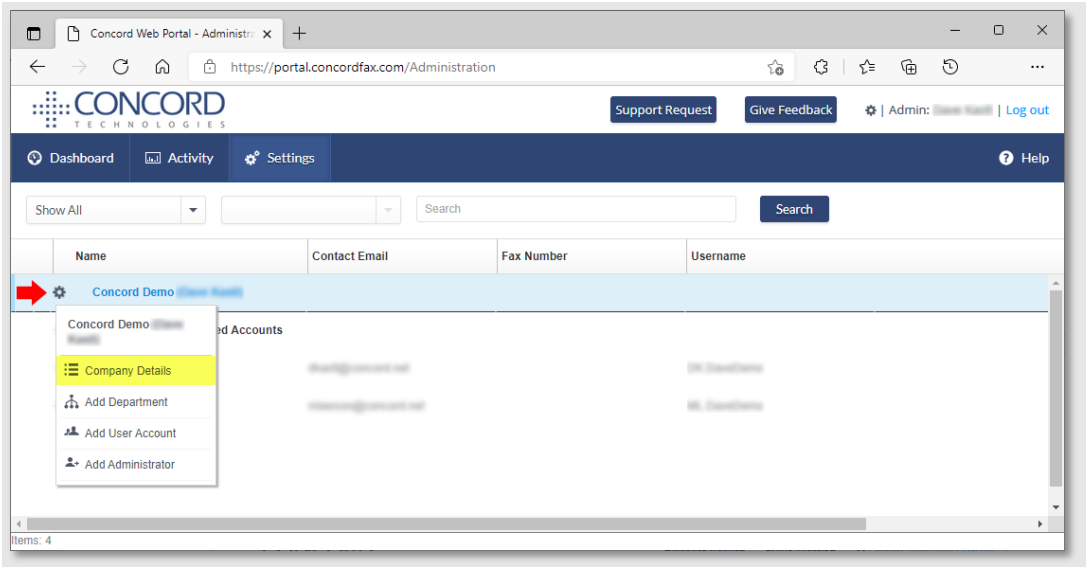
1. Login to the Concord portal using an administrative account with permissions to access the Federated tab.



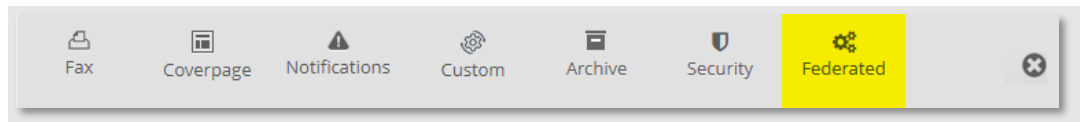
2. Click Setting->Account Administration.



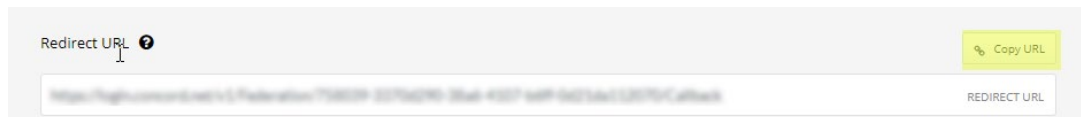
3. On the Account Administration page, click the gear icon next to the company account name and select **Company Details**.



4. On the **Company Details** page, select the **Federated** tab. **NOTE:** If you do not see the Federated tab, ensure you are logged in with an administrative account and that account has been granted access to the federation tab. You may need to contact Concord Premium Support to have your account enabled for federation access.



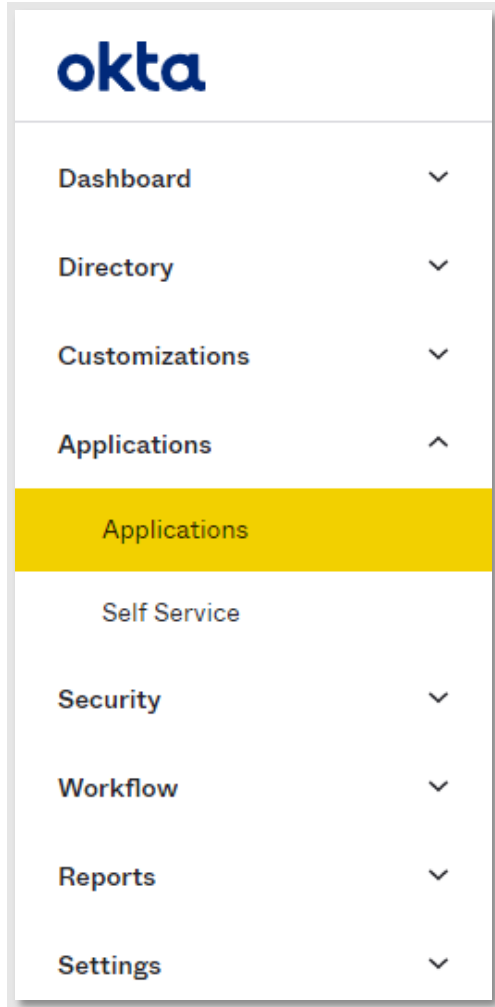
5. On the **Federated** tab, click the **Copy URL** button to copy the **Redirect URL**. It is recommended to copy and save this value as it will be used when we create the Okta application later in Section 2.



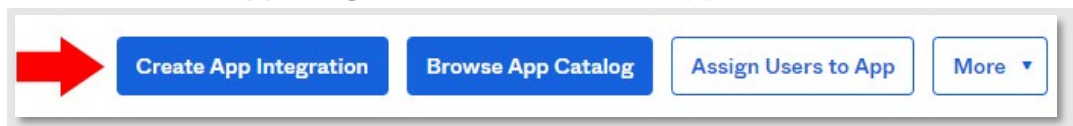
This completes the first stage of configuration within the Concord admin portal. The next stage is to create and configure the Okta application that will be used to enable federation.

## Section 2: Okta Application Creation

1. Connect to the Okta administrative portal.
2. Expand **Applications** from the left menu and select **Applications**:



3. Click the **Create App Integration** to create a new application instance:



4. On the **Create a new app integration** dialog, select **OIDC – OpenID Connect**: as the sign-in method and **Web Application** as the application type and click the **Next** button:

### Create a new app integration ✕

**Sign-in method**  
[Learn More](#)

- OIDC - OpenID Connect**  
Token-based OAuth 2.0 authentication for Single Sign-On (SSO) through API endpoints. Recommended if you intend to build a custom app integration with the Okta Sign-In Widget.
- SAML 2.0**  
XML-based open standard for SSO. Use if the Identity Provider for your application only supports SAML.
- SWA - Secure Web Authentication**  
Okta-specific SSO method. Use if your application doesn't support OIDC or SAML.
- API Services**  
Interact with Okta APIs using the scoped OAuth 2.0 access tokens for machine-to-machine authentication.

---

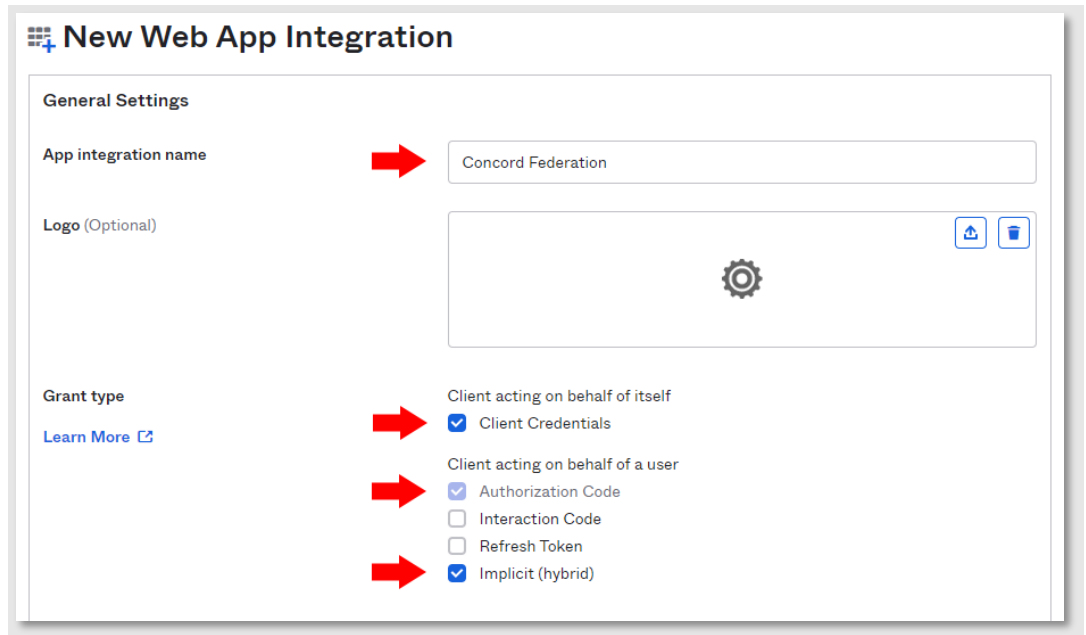
**Application type**  
What kind of application are you trying to integrate with Okta?  
Specifying an application type customizes your experience and provides the best configuration, SDK, and sample recommendations.

- Web Application**  
Server-side applications where authentication and tokens are handled on the server (for example, Go, Java, ASP.Net, Node.js, PHP)
- Single-Page Application**  
Single-page web applications that run in the browser where the client receives tokens (for example, Javascript, Angular, React, Vue)
- Native Application**  
Desktop or mobile applications that run natively on a device and redirect users to a non-HTTP callback (for example, iOS, Android, React Native)

[Cancel](#) [Next](#)







5. On the **New Web App Integration** page, enter an **App integration name** value (the value is arbitrary) and specify the following **Grant types** in the top portion of the page:







**New Web App Integration**

**General Settings**

App integration name  Concord Federation

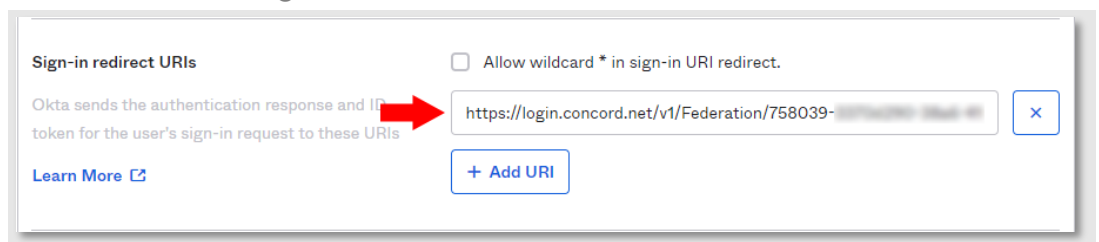
Logo (Optional)   

Grant type   



[Learn More](#) 


- Client acting on behalf of itself
- Client Credentials
- Client acting on behalf of a user
- Authorization Code
- Interaction Code
- Refresh Token
- Implicit (hybrid)

6. Paste the redirect URL copied from the previous section (Step #5 in Section 1) into the **Sign-in redirect URIs** section:

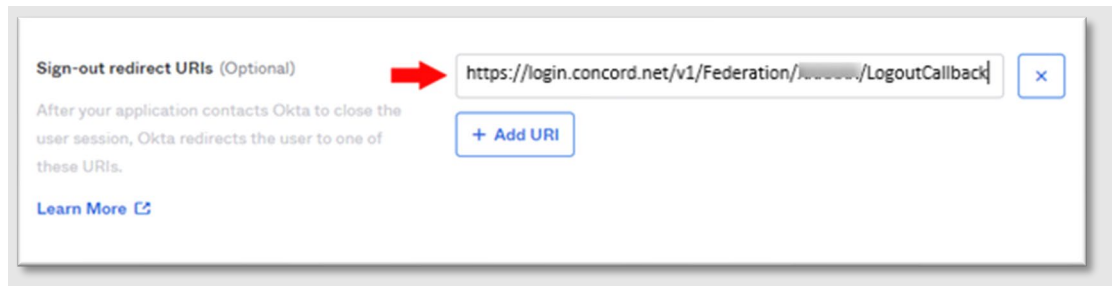


**Sign-in redirect URIs**  Allow wildcard \* in sign-in URI redirect.

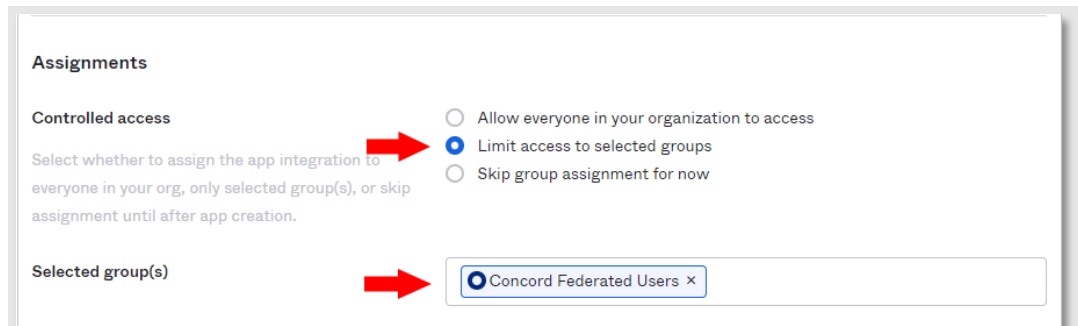
Okta sends the authentication response and ID token for the user's sign-in request to these URIs   

[Learn More](#) 

- OKTA requires a very specific URL format to construct the **Sign-out redirect URL**. To create this, you will use the redirect URL from Step #6 and replace the **Callback** value at the end with **LogoutCallback** instead. Make sure you do not modify the URL in any other way and that you add the value “**LogoutCallback**” with that specific capitalization, as the requirements for this URL are very syntactically and structurally specific:





- Select the access you wish to grant your users. **Allow everyone in your organization to access** will grant access to all your Okta users whereas **Limit access to selected groups** (recommended) will allow you to specify which groups of users will have access to the Okta application:



- Click **Save** to create the Okta application.
- Copy the **Client ID** and **Client Secret** values as these values will be copied to the Concord portal. **NOTE:** The client secret is a sensitive value and should not be shared:

### Client Credentials Edit

Client ID   




Public identifier for the client that is required for all OAuth flows.

Client authentication  Client secret  Public key / Private key

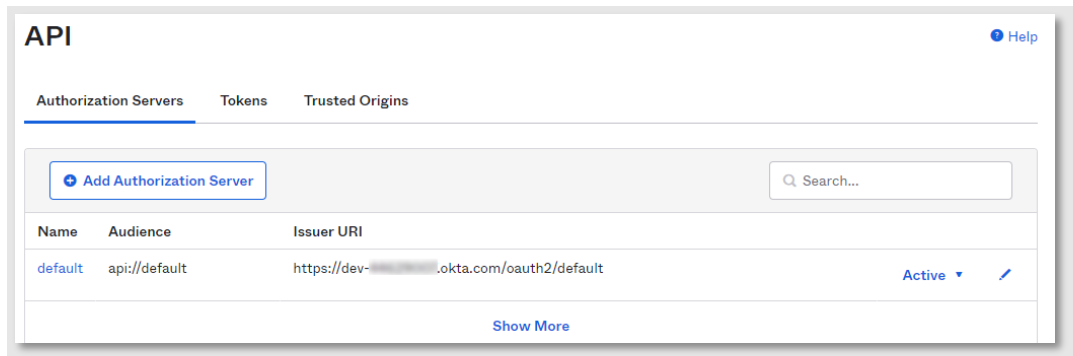
---

### CLIENT SECRETS

[Generate new secret](#)

Creation date	Secret	Status
 Mar 29, 2022	.....  	Active ▾

11. The last piece of information needed from the Okta configuration is the OpenID Connect metadata address. This is a combination of the base Okta address appended with the value **.well-known/openid-configuration**. To find the Okta base URL, select **Security->API**. On the API page, select the Authorization Server used for this instance:

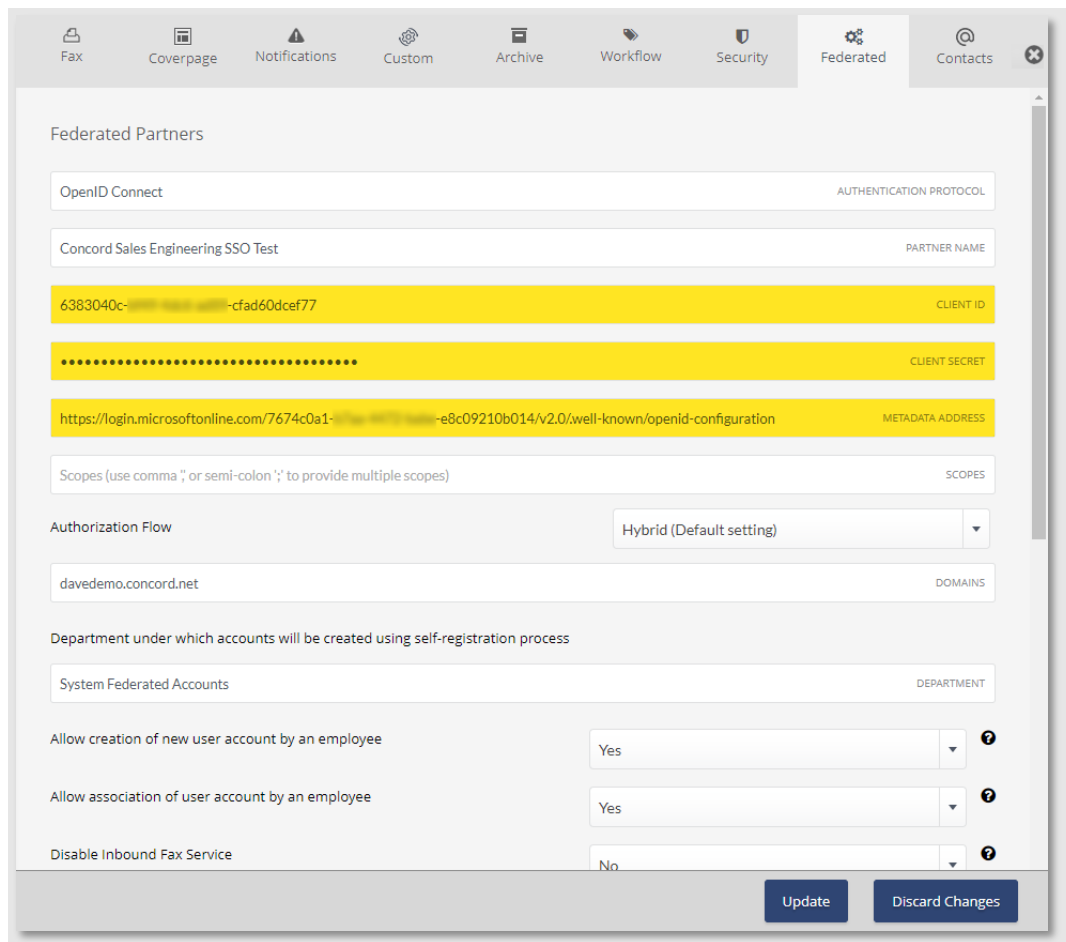


12. Copy the **Issuer URI** value and append the value **/.well-known/openid-configuration** to this URL as this will be used as the OpenID Connect metadata address.

This completes the Okta configuration stage. We will now take the values created and copied from the Okta application and apply them to the Concord Federated tab.

## Section 3: Concord Portal Federation Configuration – Phase 2

1. In a browser, navigate to the Federated tab on the Concord admin portal as described in Phase 1 of this process.
2. Paste the following values retrieved from the Okta configuration into the Federated tab:
  - Client ID
  - Client Secret
  - OpenID Connect Metadata Address

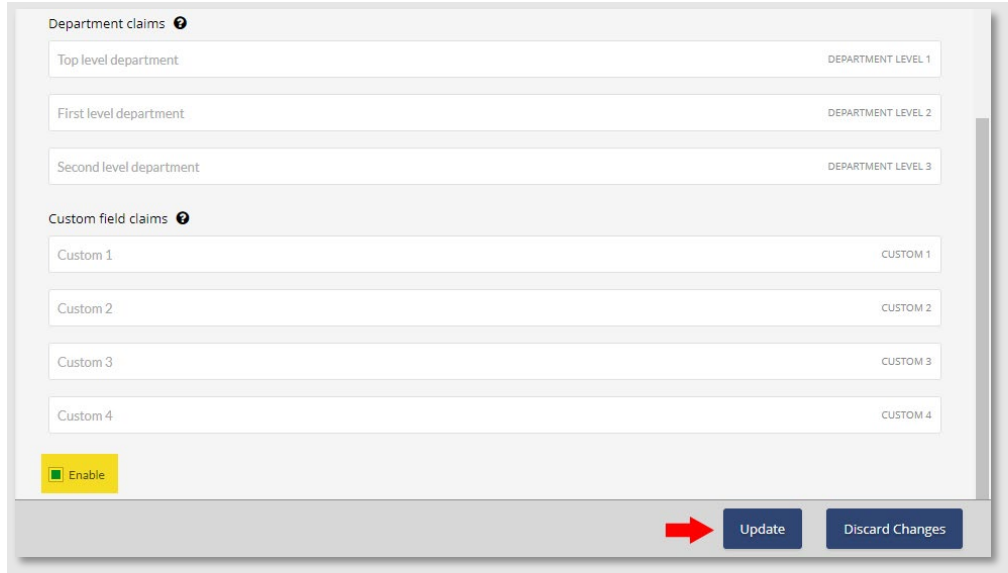


The screenshot displays the 'Federated Partners' configuration page in the Concord admin portal. The 'Federated' tab is selected in the top navigation bar. The configuration includes the following fields and values:

- Authentication Protocol:** OpenID Connect
- Partner Name:** Concord Sales Engineering SSO Test
- Client ID:** 6383040c-...-cfad60dcef77
- Client Secret:** (masked with dots)
- Metadata Address:** https://login.microsoftonline.com/7674c0a1-...-e8c09210b014/v2.0/well-known/openid-configuration
- Scopes:** (empty field)
- Authorization Flow:** Hybrid (Default setting)
- Domains:** davedemo.concord.net
- Department:** System Federated Accounts
- Allow creation of new user account by an employee:** Yes
- Allow association of user account by an employee:** Yes
- Disable Inbound Fax Service:** No

Buttons for 'Update' and 'Discard Changes' are located at the bottom right of the form.

3. Ensure the **Enable** checkbox is checked and click the **Update** button to enable federation:



The screenshot shows a configuration interface with two main sections: 'Department claims' and 'Custom field claims'. Each section has three input fields. The 'Department claims' section has fields for 'Top level department', 'First level department', and 'Second level department', each with a corresponding label on the right: 'DEPARTMENT LEVEL 1', 'DEPARTMENT LEVEL 2', and 'DEPARTMENT LEVEL 3'. The 'Custom field claims' section has four input fields labeled 'Custom 1' through 'Custom 4', each with a corresponding label on the right: 'CUSTOM 1', 'CUSTOM 2', 'CUSTOM 3', and 'CUSTOM 4'. At the bottom left, there is a yellow 'Enable' checkbox. At the bottom right, there are two buttons: 'Update' and 'Discard Changes'. A red arrow points to the 'Update' button.

This completes the second phase of the federation configuration in the Concord admin portal. At this point, any user who attempts to login to the Concord portal with a username containing the redirect domain will be redirected to the configured identity management endpoint.

This may complete all the requirements you have for federation. If you are interested in using custom claims to create users in specific Concord departments, see **Appendix A** which describes the process of creating and assigning custom claims.

## Best Practices

- It is highly recommended that you create an administrative account that has access to the federated tab but that itself does not use federation. The reason being is that if, for some reason, you enable federation and there is an issue, this admin account can easily login to the Concord portal and disable federation.

Without this non-federated admin account, it is possible that you could lock all users out of the Concord portal with no ability to disable federation.

An example of a non-federated admin account would be to create an admin with the username of “FirstName.LastName” rather than user@domain.com where “domain.com” is the federated domain.

- Related to the first bullet point, if you create admin and user accounts for the same person, we recommend that the admin account use this “FirstName.LastName” convention and the user account uses the e-mail address for that user.

This is to ensure that if you choose to use any of the Concord client utilities, which require a user account to authenticate to the Concord platform, that you can use federation for that user account.

- Ensure the correct Grant Type settings are enabled:

**APPLICATION**

App integration name	Concord Federation
Application type	Web
Grant type	<p>Client acting on behalf of itself</p> <ul style="list-style-type: none"><li><input checked="" type="checkbox"/> Client Credentials</li></ul> <p>Client acting on behalf of a user</p> <ul style="list-style-type: none"><li><input checked="" type="checkbox"/> Authorization Code</li><li><input type="checkbox"/> Interaction Code</li><li><input type="checkbox"/> Refresh Token</li><li><input checked="" type="checkbox"/> Implicit (hybrid)</li></ul> <ul style="list-style-type: none"><li><input checked="" type="checkbox"/> Allow ID Token with implicit grant type</li><li><input checked="" type="checkbox"/> Allow Access Token with implicit grant type</li></ul>



## Getting Help

Concord's customer service team is available Monday–Friday from 6:00 AM to 6:00 PM (Pacific Time).

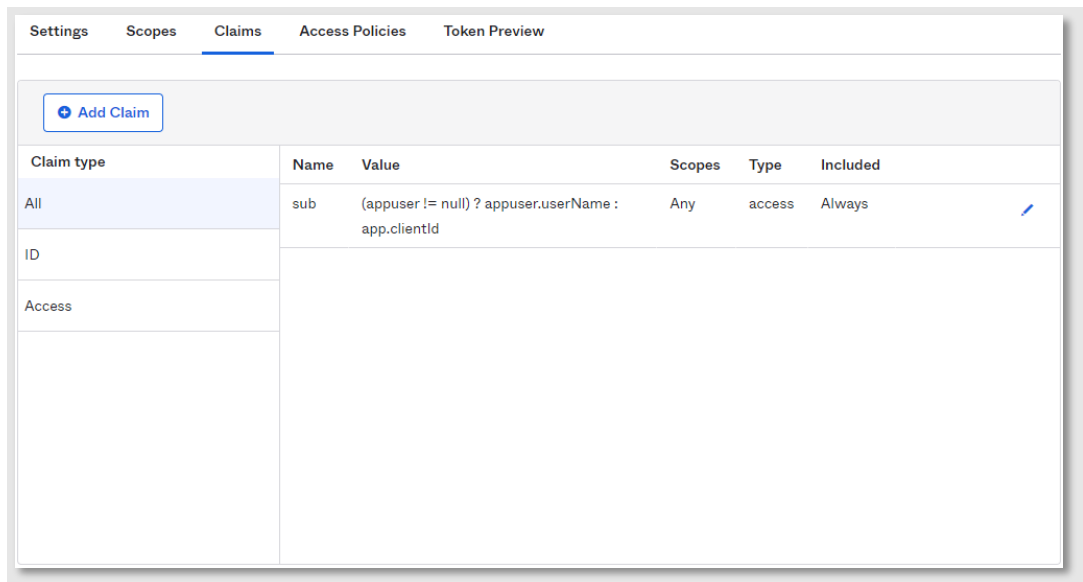
- Phone: +1 (206) 441-3346
- Email: [premiumsupport@concord.net](mailto:premiumsupport@concord.net)
- Web: <https://concord.net/about/contact-us/>

## Appendices

### Appendix A – Custom Claims

Custom claims can be created and associated with a registered Okta application. These claims can then be used to specify additional user properties such as the department to create the Concord user in (when auto-creating federated users), or to specify custom user fields that can be used for cover sheets or reporting.

1. To create a new claim, select **Security->API** in the Okta administration portal.
2. On the **API** page, select **Claims**:




Claim type	Name	Value	Scopes	Type	Included
All	sub	(appuser != null) ? appuser.userName : app.clientId	Any	access	Always
ID					
Access					

3. Click the **Add Claim** button to create a new claim.

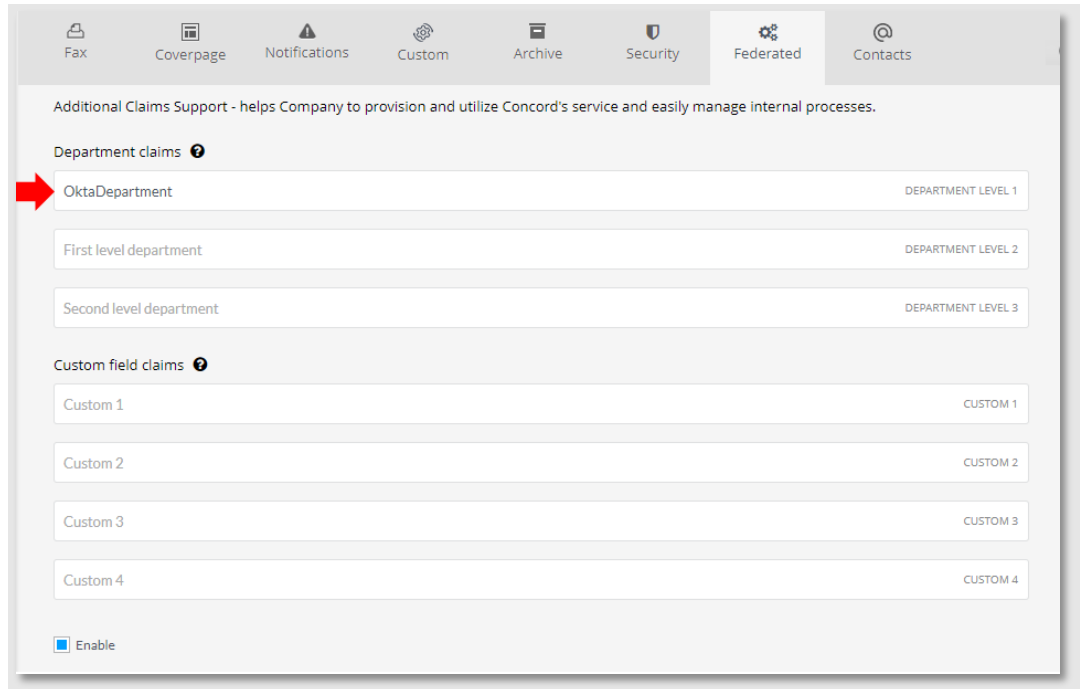
4. Enter in the name of the new claim, specify “ID Token” and add the value you want to be passed as part of the claim:

### Add Claim

Name	<input type="text" value="OktaDepartment"/>
Include in token type	<input type="text" value="ID Token"/> <input type="text" value="Always"/>
Value type	<input type="text" value="Expression"/>
Value 	<input type="text" value="user.department"/> <a href="#">Expression Language Reference</a>
Disable claim	<input type="checkbox"/> Disable claim
Include in	<input checked="" type="radio"/> Any scope <input type="radio"/> The following scopes:

5. Click the Create button to save the new claim.

6. In the Concord Admin Portal, browse to the **Federated** tab and enter the newly created claim as a department claim:



7. Save the changes.

This completes the federated SSO configuration. You should now be able to test associating or creating users via the federated SSO process.