



Concord Federated SSO

Admin and User Guide

Concord Technologies

2025 First Avenue Suite 800

Seattle, WA, 98121, USA

Call Us: +1 206-441-3346

Concord.net

Contents

Introduction to Federation	5
What is Federated SSO?	5
What is a Claim?	5
Federated Partners.....	7
Who are the players in a Federated Partnership?.....	7
Resource Partner (Concord).....	7
Account Partner (Customer)	7
Configuring Federation.....	8
What steps are required to Set-Up a Federated Partnership?	8
Concord to Enable Federation	9
Client to Register Concord as Federated Partner	9
Client to Configure Federated Partner.....	16
Federated SSO – Account Creation and Association	21
Create Account (User).....	23
Associate With Credentials (User Account).....	30
Associate With Token (User Account).....	34
Associate With Credentials (Administrator Profile)	40
Associate With Token (Administrator Profile).....	45
Federated SSO User Experience	51



Now that Concord is a Federated Partner, what is the User Experience?.....	51
Best Practices.....	52
Federated SSO - Glossary of Terms.....	53
Getting Help	55



Copyright © 2022 CONCORD Technologies. All Rights Reserved.

The material in this guide is for informational purposes only. The products and specifications it describes are subject to change without prior notice. Concord is not responsible for any damages of any nature whatsoever related to or arising from reliance on the information contained herein.

More Information

Additional support can be provided through:

Email: premiumsupport@concord.net

Telephone: +1 (206) 441-3346

Fax: +1 (206) 441-7965

Website: <https://concord.net/>

Introduction to Federation

What is Federated SSO?

Federation is a relationship maintained between organizations, enabling users from one organization to access another's web properties and applications. Federated Single Sign-On (SSO) provides an authentication token to a user, in lieu of a new set of username and password credentials. This eliminates the need for the user to create a unique user or admin account to access web properties and applications.

In a Federated model, when a user from an organization requests authentication to Concord's web services or portal applications, they will be redirected to their home organization for authentication and, if successful, will be redirected back to the application with a token confirming the authentication. This is managed by the customer organization's Identity Provider, with whom a Federated integration is built.

What is a Claim?

A claim is a statement about a user that is used for authorization purposes in an application. Federation brokers trust between customers and Concord by allowing the trusted exchange of arbitrary claims that contain arbitrary values. The receiving party uses these claims to make authorization decisions.



To date Concord supports the receipt of the following claims:

Claim	Concord Usage
Email Address	Contact email address If unique, also used as sending email address
Display Name	Currently not used
Given Name	First name
Surname	Last name
User Principal Name	Used as a unique identifier, may vary between providers.

Concord provides support for an admin to configure which claim will be used for the User ID. The admin can do this in the portal via a dropdown to select UserId based on ObjectIdentifier, NameIdentifier or UPN.

If a customer has set up a custom User Id claim, then the Portal does not allow this to be changed and would display this as "read-only."

Federated Partners

Who are the players in a Federated Partnership?

There are two main entities in a Federated Partnership: the Resource Partner and the Account Partner.

Resource Partner (Concord)

As the [Resource Partner](#) organization in a federated partnership, Concord represents the organization in the federated trust relationship whose Web servers are protected by a resource-side identity server. The identity server at the resource partner uses the security tokens produced by the account partner to provide claims to the Web servers located at the resource partner.

Account Partner (Customer)

As the [Account Partner](#) in a Federated Partnership, the customer represents the organization in the federation trust relationship that physically stores user accounts in a supported attribute store and provides authentication services.

The federation server in the account partner organization authenticates local users and creates security tokens that are used by the resource partner (Concord) in making authorization decisions, such as allowing access to a portal or to submit a message.

Configuring Federation

What steps are required to Set-Up a Federated Partnership?

Both the Resource Partner (Concord) and the Account Partner (Customer) have responsibilities in configuring the Federated Partnership. To ensure the customer's federated application is correctly configured, Concord recommends customers use a test domain, e.g. "test.company.com" rather than "company.com," to test and verify Federation is working as expected.

Once correct functionality has been determined, the test domain can be replaced with the correct, production domain. This allows Account Partners to test and verify Federation is working without impacting existing users.

Test Domain Acceptance Criteria	Ability to log in with <u>user@testdomain.com</u> , and self-register
	Ability to log in with <u>user@testdomain.com</u> , authenticate using customer's UPN domain/user, and self-register
	Ability to log in with <u>user@testdomain.com</u> , and using a token associate with an existing account.
	Ability to log in with <u>user@testdomain.com</u> , and using Concord credentials associate with an existing account.

Note> You will need to collect the Redirect URL from the Concord admin portal once Federation has been enabled. This data is needed to begin the registration process configuration inside your Identity Provider.



Redirect URL format:

<https://logintest.concord.net/v1/Federation/{AuthenticationScheme}/Callback>

Concord to Enable Federation

The first order of business for Concord is to enable Federation on the customer's Company account, which then allows the customer to configure partnership settings in Concord's Admin Portal.

Client to Register Concord as Federated Partner

The Client Administrator is responsible for registering Concord as a federated partner. This process varies between login providers.

Concord has dedicated documentation for **Okta** and **Microsoft Azure AD**. For the purpose of demonstration in this document, ADFS 2016 will be used, and we have provided an example set-up with step-by-step instructions.

AD FS On-Premise Registration Process Example

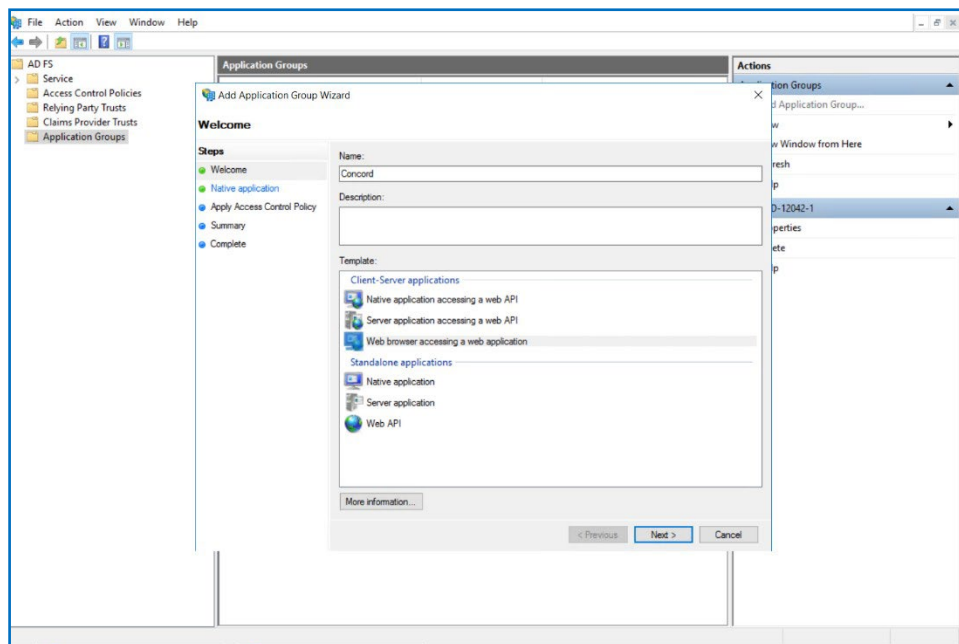
When using AD FS 2016, the Client Administrator will need to capture the following information as they are required to configure the Federated Partner on the Concord Portal:

- Application Client ID
- Metadata Address

AD FS 2016 Step 1> Register the Application / Capture Client ID and Metadata Address

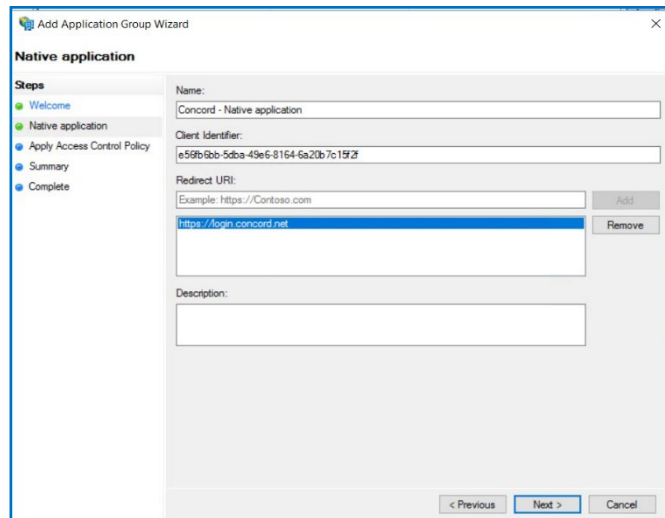
Using the AD FS Management tool, select Application Groups from the left navigation, and click "Add Application Group" to set up an Open ID AD FS Client.

Provide the name of the client and choose "Web browser accessing a web application" under "Client-Server applications" and click **Next**.



Important> The next window will display the Client Identifier, copy this value as it will be required when configuring the Federated Partner in the Concord Portal.

Provide the Redirect URL as <https://login.concord.net/> click Add, and then click **Next**.

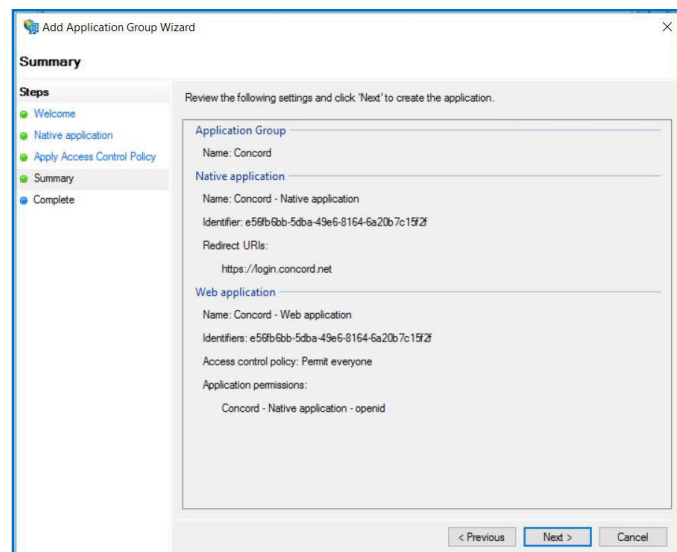


The screenshot shows the 'Add Application Group Wizard' window, specifically the 'Native application' step. The 'Steps' pane on the left shows 'Native application' as the current step. The main area contains the following fields:

- Name:** Concord - Native application
- Client Identifier:** e59fb6bb-5dba-49e6-8164-6a20b7c19f2f
- Redirect URI:** Example: https://Contoso.com. A list of URIs is shown below, with 'https://login.concord.net' selected. There are 'Add' and 'Remove' buttons next to the list.
- Description:** (Empty text box)

Navigation buttons at the bottom include '< Previous', 'Next >', and 'Cancel'.

Click **Next** again on the following window and a Summary of the configuration will be displayed.



The screenshot shows the 'Add Application Group Wizard' window, specifically the 'Summary' step. The 'Steps' pane on the left shows 'Summary' as the current step. The main area contains the following information:

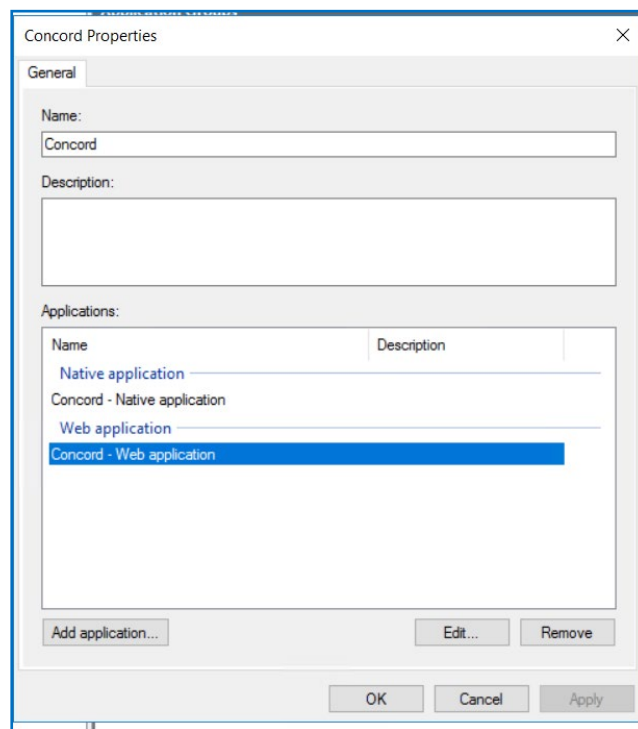
- Application Group:** Name: Concord
- Native application:** Name: Concord - Native application; Identifier: e59fb6bb-5dba-49e6-8164-6a20b7c19f2f; Redirect URIs: https://login.concord.net
- Web application:** Name: Concord - Web application; Identifiers: e59fb6bb-5dba-49e6-8164-6a20b7c19f2f; Access control policy: Permit everyone
- Application permissions:** Concord - Native application - openid

Navigation buttons at the bottom include '< Previous', 'Next >', and 'Cancel'.

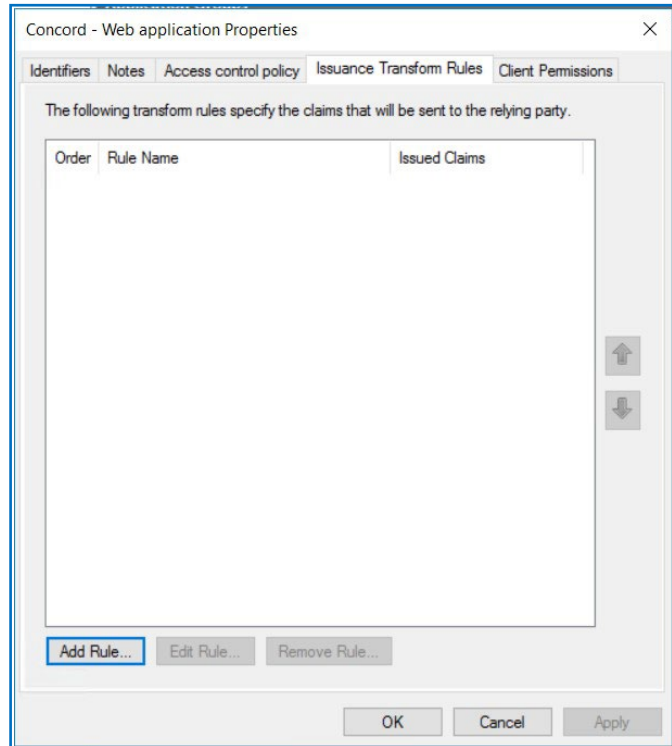
AD FS 2016 Step 2> Add Claims

To add claims to be returned to Concord on a successful login:

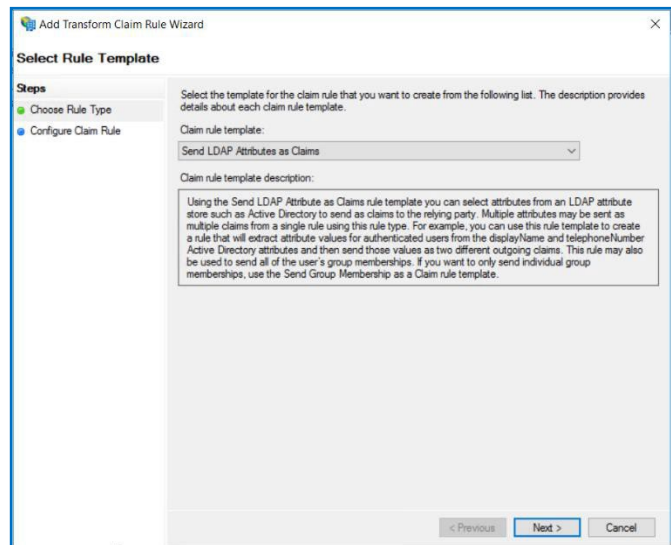
- Right click on the newly created Application Group and select Properties
- Select "<ClientName> - Web application" under Web application and click **Edit**



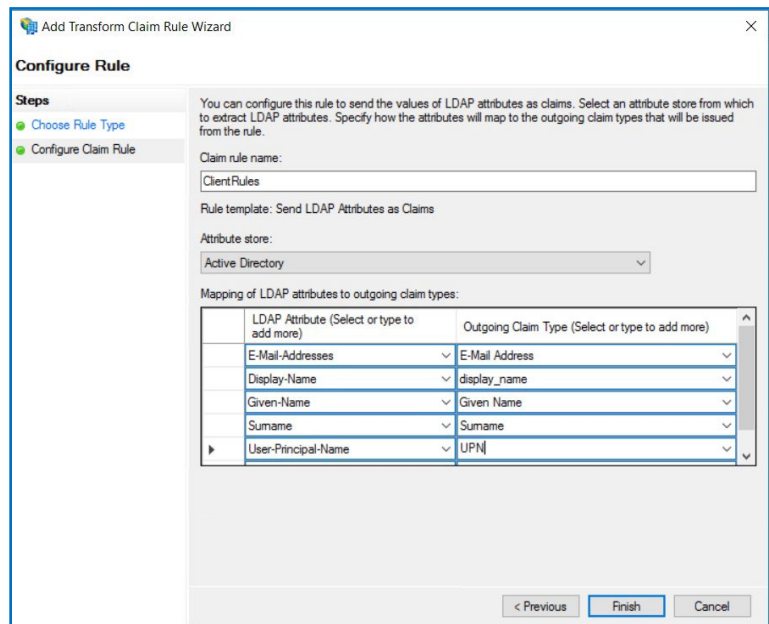
Choose the “Issuance Transform Rules” tab and click “**Add Rule**”



Choose “Send LDAP Attributes as Claims” from the Claim rule template and click **Next**



- Provide the Claim rule name
- Select “Active Directory” from the Attribute store drop-down list and provide claims that should be returned after a successful user login
- To complete, click the **Finish** button



Add Transform Claim Rule Wizard

Configure Rule

You can configure this rule to send the values of LDAP attributes as claims. Select an attribute store from which to extract LDAP attributes. Specify how the attributes will map to the outgoing claim types that will be issued from the rule.

Claim rule name:
ClientRules

Rule template: Send LDAP Attributes as Claims

Attribute store:
Active Directory

Mapping of LDAP attributes to outgoing claim types:

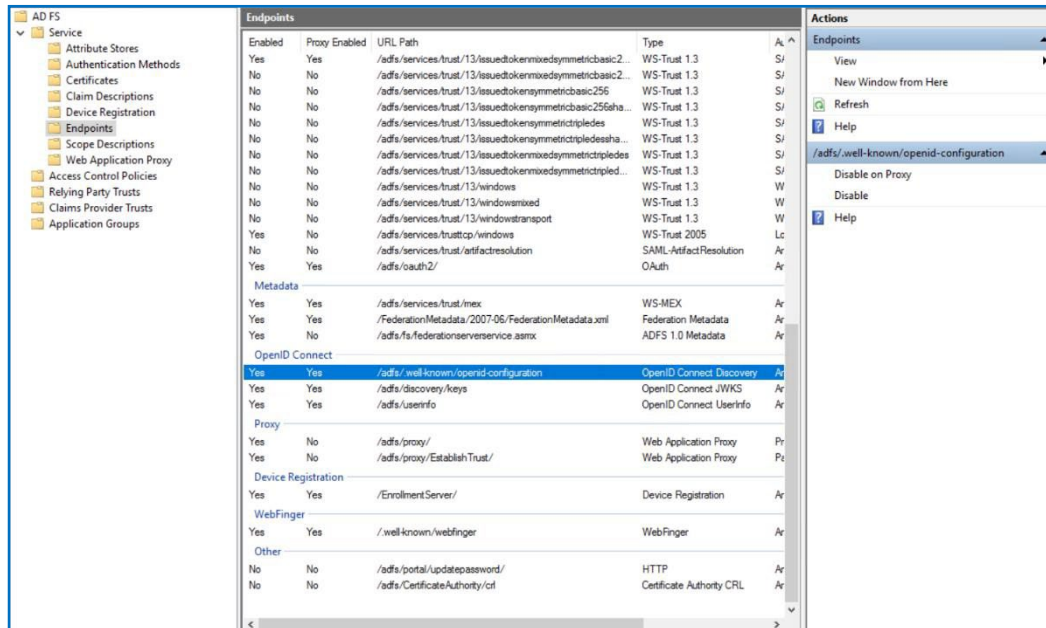
LDAP Attribute (Select or type to add more)	Outgoing Claim Type (Select or type to add more)
E-Mail-Addresses	E-Mail Address
Display-Name	display_name
Given-Name	Given Name
Surname	Surname
User-Principal-Name	UPN

< Previous **Finish** Cancel

AD FS 2016 Step 3> Capture Metadata Address

To capture the metadata address, select Endpoints from Service Node and under the OpenID Connect section, capture the URL for Type “OpenID Connect Discovery”. As this is a relative address, append this value to the base URL AD FS instance.

Important> This Metadata Address will be required when configuring the Federated Partner in the Concord Portal.



The screenshot shows the AD FS configuration console with the 'Endpoints' section expanded. The 'OpenID Connect' section is visible, and the 'OpenID Connect Discovery' endpoint is highlighted. The URL path for this endpoint is '/adsf/.well-known/openid-configuration'.

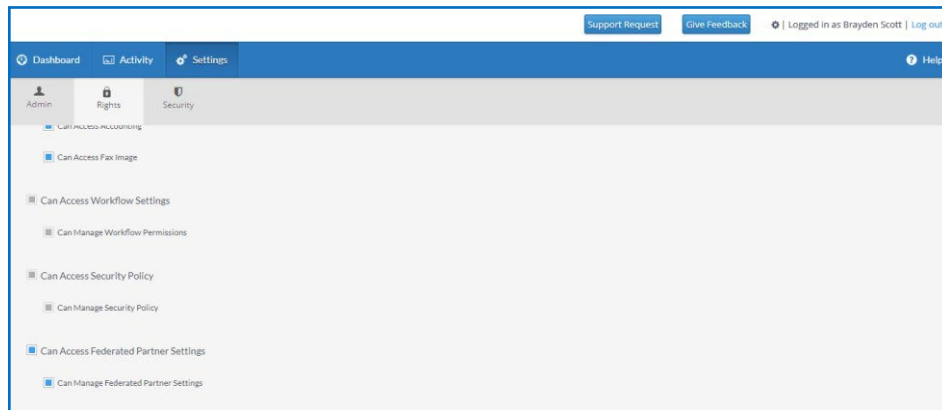
Enabled	Proxy Enabled	URL Path	Type	Actions
Yes	Yes	/adsf/services/trust/13/issuedtokenmixedsymmetricbasic2...	WS-Trust 1.3	Ar
No	No	/adsf/services/trust/13/issuedtokenmixedsymmetricbasic2...	WS-Trust 1.3	Ar
No	No	/adsf/services/trust/13/issuedtokenmixedsymmetricbasic256...	WS-Trust 1.3	Ar
No	No	/adsf/services/trust/13/issuedtokenmixedsymmetricbasic256ha...	WS-Trust 1.3	Ar
No	No	/adsf/services/trust/13/issuedtokenmixedsymmetrictripledesha...	WS-Trust 1.3	Ar
No	No	/adsf/services/trust/13/issuedtokenmixedsymmetrictripledes...	WS-Trust 1.3	Ar
No	No	/adsf/services/trust/13/issuedtokenmixedsymmetrictripledes...	WS-Trust 1.3	Ar
No	No	/adsf/services/trust/13/windows	WS-Trust 1.3	W
No	No	/adsf/services/trust/13/windowmixed	WS-Trust 1.3	W
No	No	/adsf/services/trust/13/windowtransport	WS-Trust 1.3	W
Yes	No	/adsf/services/trustcp/windows	WS-Trust 2005	Lc
No	No	/adsf/services/trust/artifactresolution	SAML-ArtifactResolution	Ar
Yes	Yes	/adsf/oauth2/	OAuth	Ar
Metadata				
Yes	Yes	/adsf/services/trust/mex	WS-MEX	Ar
Yes	Yes	/FederationMetadata/2007-06/FederationMetadata.xml	Federation Metadata	Ar
Yes	No	/adsf/fs.federationsevervice.asmx	ADFS 1.0 Metadata	Ar
OpenID Connect				
Yes	Yes	/adsf/.well-known/openid-configuration	OpenID Connect Discovery	Ar
Yes	Yes	/adsf/.discovery/keys	OpenID Connect JWKS	Ar
Yes	Yes	/adsf/.userinfo	OpenID Connect UserInfo	Ar
Proxy				
Yes	No	/adsf/proxy/	Web Application Proxy	Pr
Yes	No	/adsf/proxy/EstablishTrust/	Web Application Proxy	Pr
Device Registration				
Yes	Yes	/EnrollmentServer/	Device Registration	Ar
WebFinger				
Yes	Yes	/well-known/webfinger	WebFinger	Ar
Other				
No	No	/adsf/portal/Updatepassword/	HTTP	Ar
No	No	/adsf/CertificateAuthority/crl	Certificate Authority CRL	Ar

Client to Configure Federated Partner

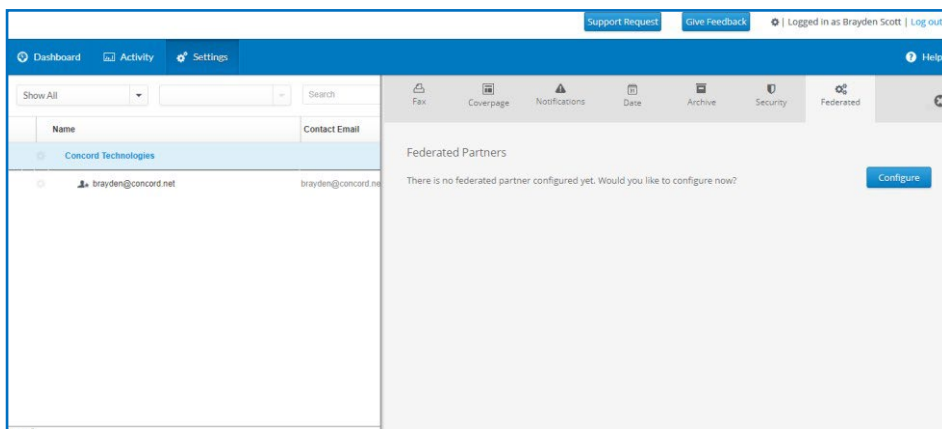
Listed below are the steps for configuring the federated partner from within the Concord Admin Portal.

Important> The portal is the only place where this configuration is done.

Once Federation has been enabled by Concord, then Access Rights for managing the Federated Partner will be available and the Federated Tab will be visible to administrator(s) who have rights for Federation.



If the company does not have a Federated Partner configured, they can do so by selecting **Configure** button under Federated Tab under Company.



It is important to set all the mandatory values in configuring a Federated Partner. Requirements for mandatory values may vary according to Identity Provider.

Authentication Protocol: Currently **OpenID Connect** is the only supported method and will be pre-populated (field not currently editable)

Partner Name: Customer provided, display name for the configured partner.

****mandatory field**

Redirect URL: Your identity server will use this redirect URL to redirect back to Concord after successful login. Depending on your Identity Server requirements, update the Return URL under your Federated Partner settings with either the entire URL or the base URL "https://login.concord.net/"

Client ID: Customer provided, Client ID of the Federated Partner that customer has created to federate with Concord. This is required in order for Concord's Identity Server to communicate with Customer's Identity Provider.

****mandatory field**

Client Secret: Customer provided and associated with Client ID (similar to a password) if available. (Note: mandatory for Microsoft Azure AD, Okta and other Identity Providers)

Metadata Address: Customer provided, URL for the discovery document for the Client identity server. ****mandatory field**

Federated ID Claim Type: The claim type that will be passed when users authenticate to Concord in a Federated configuration: NameIdentifier, Smart Detect, ObjectIdentifier or SID.

Scopes: Customer provided, pre-defined elements that a Customer's Identity Provider will expect to receive from Concord during the authentication process.

Authorization Flow: The flow of data between Concord and a customer's Identity Provider: Hybrid, Auth Code Flow or Auth Code Flow with PKCE.

Domains: This field will be pre-populated with the domain(s) provided by a Customer and entered by Concord when enabling Federation.

Department: This field defines the Default department where to place new users, if a specific department was not defined during the registration process. Note: If no department is provided a department will be created by default called *System Federated Accounts*

New User Creation: Default setting is Yes. If this setting is set to “Yes”, User will be allowed to create a new account if the Federated User account is not already existent in Concord.

Associate Existing User: Default setting is Yes. If this setting is set to “Yes”, user can associate an existing account in Concord System.

Disable Inbound Fax Service: Default setting is No. If this setting is set to “Yes”, User will be allowed to create a new account for outbound Fax Service only.

Include Login Hint: Setting to include login hint parameter as part of Federation login request while redirecting to login provider.

Allow Admin to Remove Account Association: Allows and admin to undo an existing Federated Association for a User.

Enable Silent User Creation Path: Setting to allow a customer employee to create a User account without entering any additional information.

Department Claims: You can define up to 3 levels of departments (claims). The value of these claims retrieved during the registration process will be used to select the department under which the user account will be created.

Note: if these claims are not provided then the user will be created within the System Defined Department.

- **Department Level 1:** This provides the top-level department in the account hierarchy.
- **Department Level 2:** This defines the second level department. In the account hierarchy. Note: The **Department Level 1** claims must be provided if a Level 2 claim is provided.

- **Department Level 3:** This defines the third level department in the account hierarchy. **Note:** Department Level 2 claims must be provided if a Level 3 claim is provided.

Custom Field Claims: These 4 optional claims can be defined to support passing during registration and will then be associated with the user account.

Enable: When the customer is ready to allow their users to use the Federated Login, this check box should be checked, and details should be saved.

Important>

- If the Enable checkbox is de- selected, users will no longer be able to authenticate with their standard organizational credentials
- Once federated is enabled any valid user can create an account

Fax
Coverage
Notifications
Custom
Archive
Security
Federated
Contacts
X

Federated Partners

AUTHENTICATION PROTOCOL

PARTNER NAME

REDIRECT URL Copy URL

CLIENT ID

CLIENT SECRET

METADATA ADDRESS

Federated ID Claim Type NameIdentifier

Scopes (use comma ',' or semi-colon ';' to provide multiple scopes) SCOPES

Authorization Flow Hybrid (Default setting)

DOMAIN

Department under which accounts will be created using self-registration process

DEPARTMENT

Allow creation of new user account by an employee	Yes
Allow association of user account by an employee	No
Disable Inbound Fax Service	Yes
Include Login hint	Yes
Allow admin to remove account association	Yes
Enable Silent User Creation Path	No

Additional Claims Support - helps Company to provision and utilize Concord's service and easily manage internal processes.

Department claims

DEPARTMENT LEVEL 1

DEPARTMENT LEVEL 2

DEPARTMENT LEVEL 3

Custom field claims

CUSTOM 1

CUSTOM 2

CUSTOM 3

CUSTOM 4

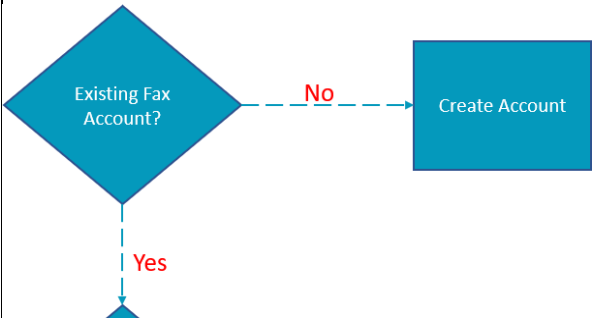
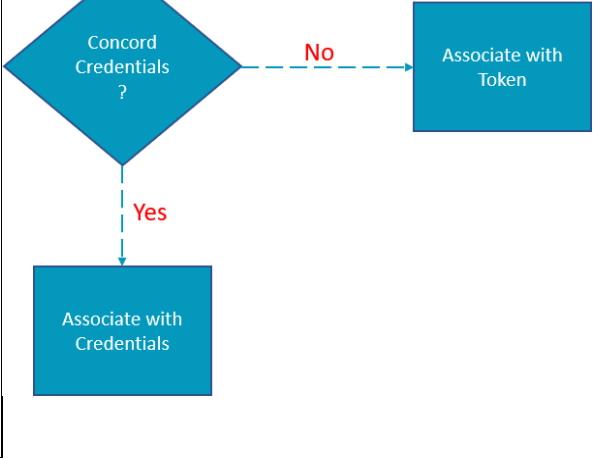
Enable

Please ensure that the details you have provided above are correct before enabling this partner. Incorrect details may lead to the user's inability to login.

Federated SSO – Account Creation and Association

How does a user, or Administrator, get configured to use Concord with their standard credentials?

Depending on the settings configured by the Client Administrator, the following flows allow a user and/or administrator to gain access to Concord's Web applications with their organizational credentials.

Flow	Use Case / Description	Flow Decision Diagram
Create Account	<p>When a user does not have an existing Fax account with Concord, they will need to follow the Create New User flow.</p> <p>**Note: Available if permitted by the Client Administrator</p>	 <pre> graph TD D1{Existing Fax Account?} -- No --> R1[Create Account] D1 -- Yes --> D2{Concord Credentials?} </pre>
Associate with Credentials	<p>When a user has an existing Fax account with Concord, and they know their Concord credentials, they can follow the Associate with Credentials flow to associate with the existing account.</p> <p>**Note: Also applicable for an administrator</p>	 <pre> graph TD D2{Concord Credentials?} -- No --> R2[Associate with Token] D2 -- Yes --> R3[Associate with Credentials] </pre>
Associate with Token	<p>When a user has an existing Fax account with Concord, but does NOT know their Concord credentials, their Admin will need to provide a Token so they can follow the <i>Associate with Token</i> flow to associate with the existing account.</p> <p>**Note: Also applicable for an administrator.</p>	

Create Account (User)

If enabled by the Client Administrator, the Create Account flow is for users who do not yet have a Concord Fax account.

Important> Based on the permissions selected by the Client Administrator, some of the steps in the Create Account flow may be omitted.

Steps to Create User Account

Persona: User

Step 1. In a web browser, enter the URL <https://portal.concordfax.com/> and you will be directed to Concord's login server.

Step 2. You will be prompted to enter your email address. Assuming your domain is a federated domain, you will be directed to your local identity server for authentication.

Step 3. Once authenticated by your local identity server, you will then be directed back to Concord to complete the Creation process.

Step 4. You will first need to choose the Create User option, as you do not currently have a Concord fax account.

Step 5. You will then need to enter your account details: first and last name

Step 6. Following, you will then be prompted to enter your contact information: street address and phone number.

Step 7. If your Client Administrator has enabled Inbound Faxing, you will be prompted to select a fax number. As this is optional, you may bypass selecting a fax number.

Note> It is important to note that if a fax number is chosen, it will come from Concord's inventory pool, and **not** from the customer's private inventory. Once added to the customer's inventory, the fax number will be subject to the applicable monthly charge per fax number.

Step 8. Based on certain conditions, you may be prompted to enter your sending email address and / or where you want to receive your inbound fax documents. Those conditions are noted below.

- If your email address is not unique within the Concord system, then you will be prompted to provide another email address that will be used for sending faxes.
- If your Client Administrator has disabled Inbound Faxing or if you have chosen not to select a fax number, you will not be prompted to provide how and where you want to receive inbound faxes.
- If your account is configured for NEXTSTEP, you will not be prompted to provide an address for receiving faxes.

Step 9. Once you have completed the creation process, a summary of your account information will be displayed.

Note> You must capture the API Service User ID and Password if you will be using Web Services or Print2Fax.

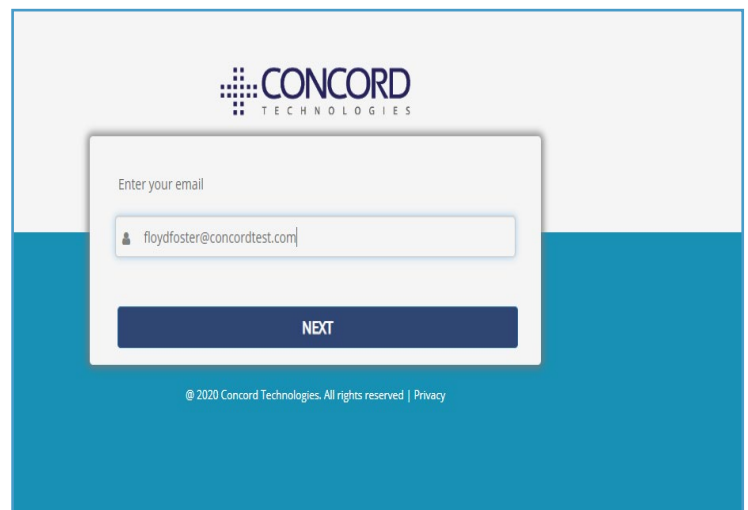
Step 10. From here, you can go directly to the Concord Web Portal by clicking on the Go To Dashboard button.

Steps to Create User Account with Images in an AD FS Federated scenario

Persona: User

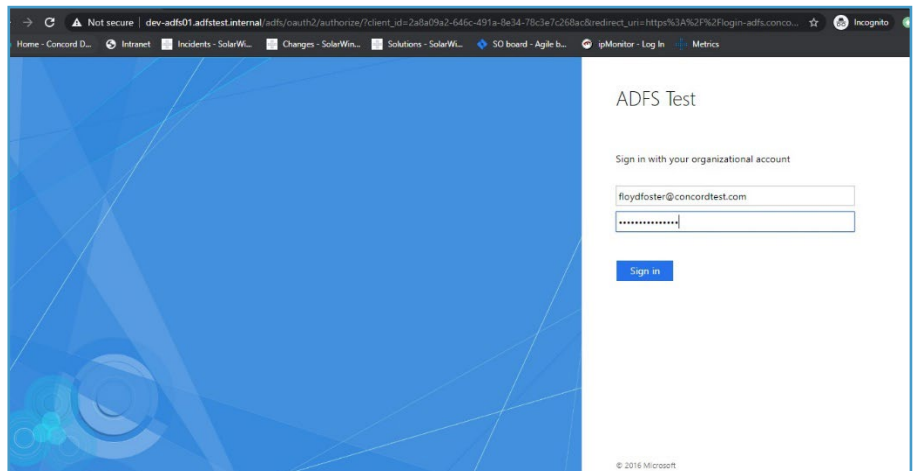
Step 1.

In a web browser, enter the URL <https://portal.concordfax.com/> and you will be directed to Concord's login server.



Step 2.

Enter your email address. Assuming your domain is a federated domain, you will be directed to your local identity server for authentication.

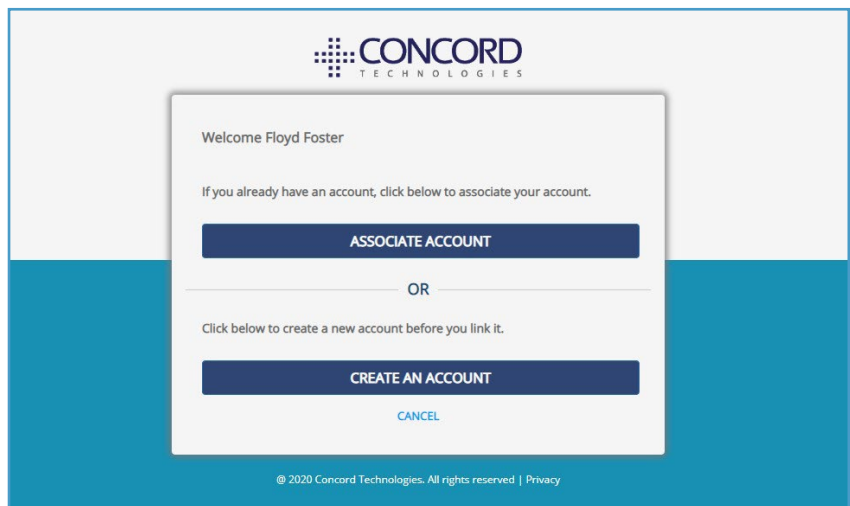


Step 3.

Once authenticated by your local identity server, you will then be directed back to Concord to complete the Creation process.

Step 4.

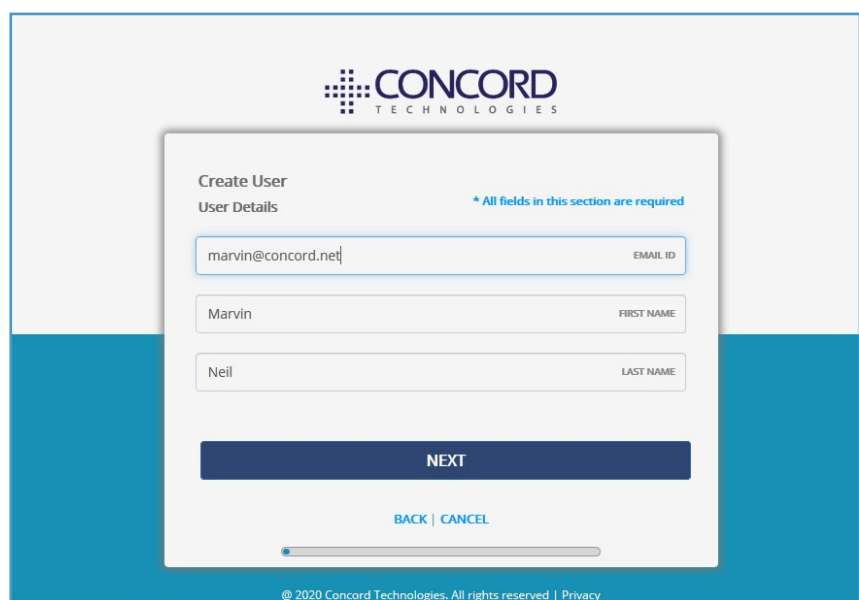
You will first need to choose the Create User options, as you do not currently have a Concord fax account.



Step 5.

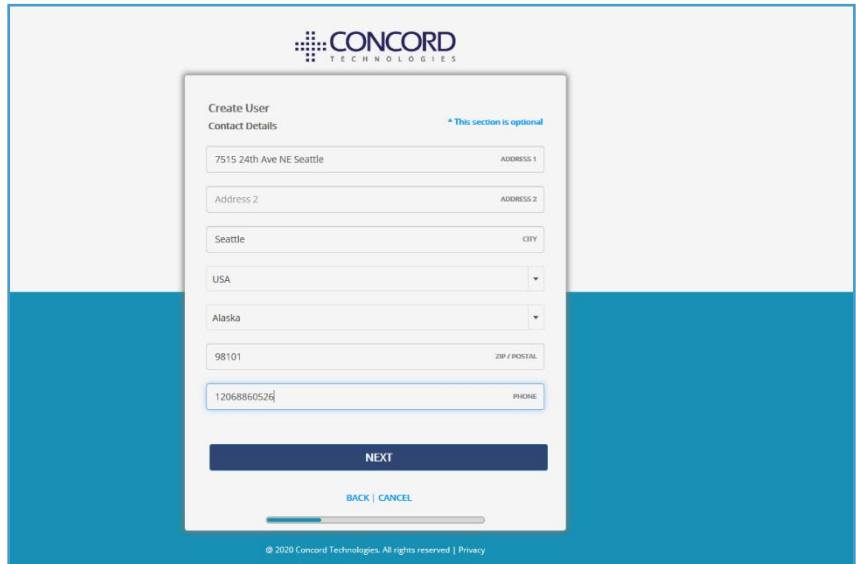
In the next screen, enter your account details as prompted, and click NEXT.

Note: your email address will be pre-populated.



Step 6.

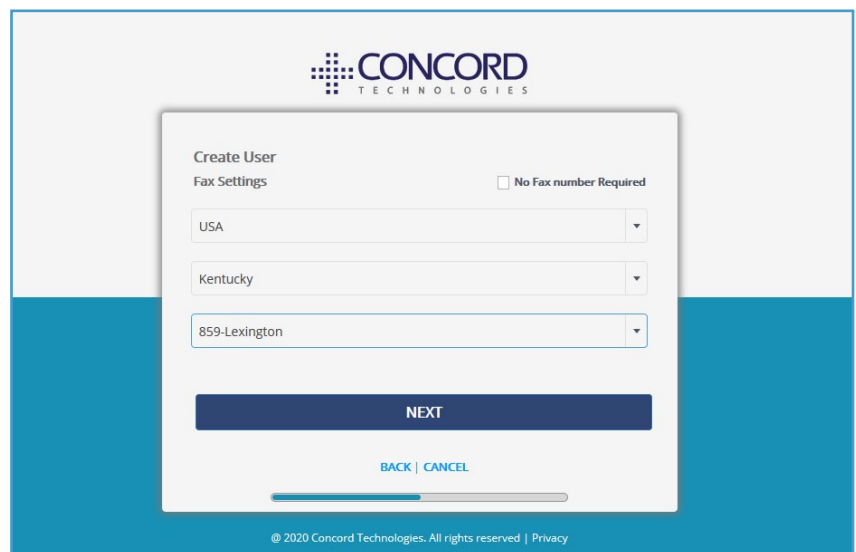
In the next screen, you will be prompted to enter your contact information.



© 2020 Concord Technologies. All rights reserved | Privacy

Step 7.

In the next step enter your Fax Settings. An inbound fax number is not required, and you may bypass this screen by selecting the “No Fax number Required” checkbox.



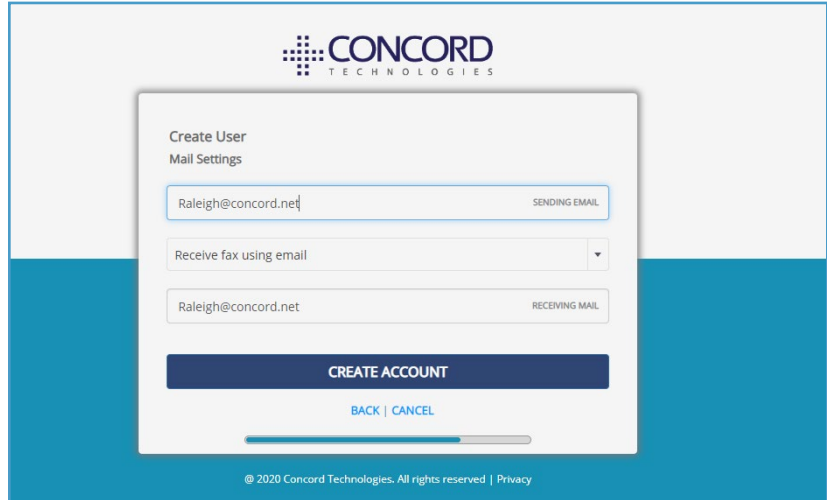
© 2020 Concord Technologies. All rights reserved | Privacy

Note: This step may be omitted, if the Client Administrator disabled Inbound Faxing for new users

Note: It is important to note that if a fax number is chosen, it will come from Concord’s inventory pool, and **not** from the customer’s private inventory. Once added to the customer’s inventory, the fax number will be subject to the applicable monthly charge per fax number.

Step 8.

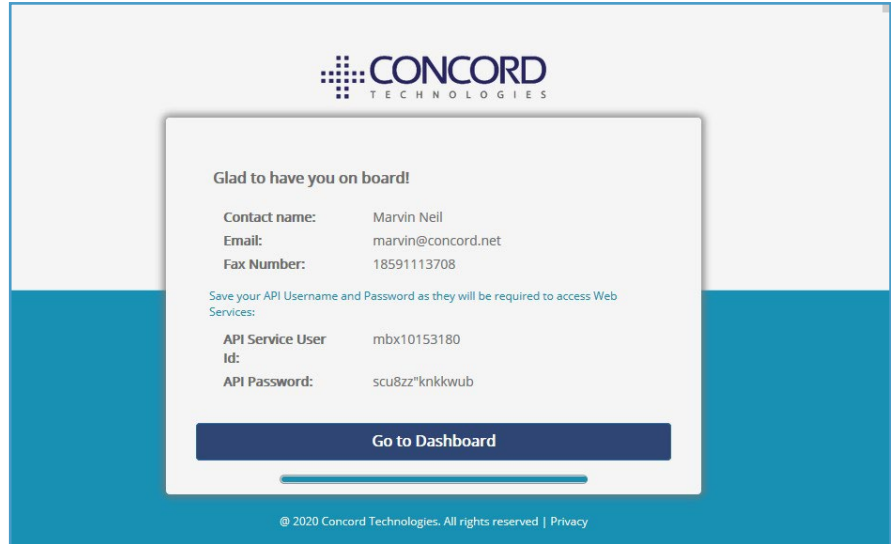
You may be prompted to enter your sending email address and / or where you want to receive your inbound fax documents. This step may appear slightly different, or may not appear at all, based on the following conditions:



- If your email address is not unique within the Concord system, then you will be prompted to provide another email address that will be used for sending faxes.
- If your Client Administrator has disabled Inbound Faxing or if you have chosen not to select a fax number, you will not be prompted to provide how and where you want to receive inbound faxes.
- If your account is configured for NEXTSTEP, you will not be prompted to provide an address for receiving faxes.

Step 9.

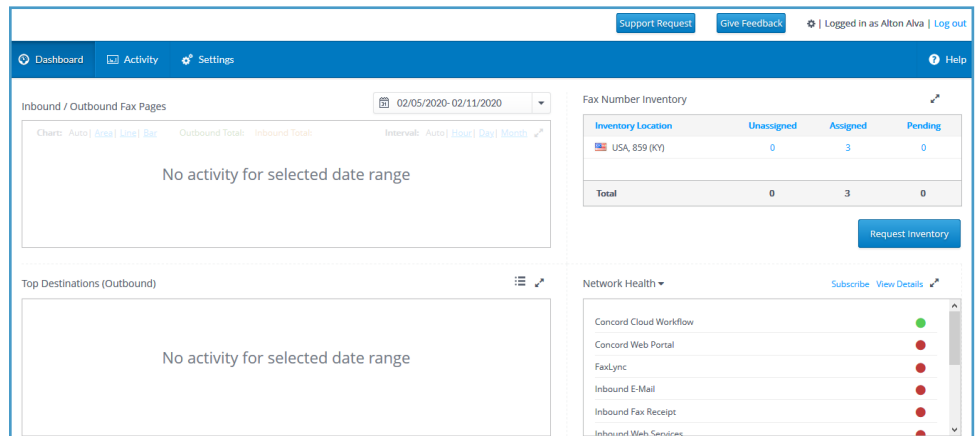
Once you have clicked on the **CREATE ACCOUNT** button, your account has been created and the following message will be displayed.



Note: You must capture the API Service User ID and Password if you will be using Web Services or Print2Fax.

Step 10.

From here, you can go directly to the Concord Web Portal by clicking on the **Go To Dashboard** button.



Associate With Credentials (User Account)

For users who have a Concord fax account, and know their Concord username and password, they will follow the Associate with Credentials flow to link their accounts.

Important> Based on the permissions selected by the Client Administrator, some of the steps in the Create Account flow may be omitted.

Steps to Associate a User Account with Credentials

Persona: User

Step 1. In a web browser, enter the URL <https://portal.concordfax.com/> and you will be directed to Concord's login server.

Step 2. You will be prompted to enter your email address. Assuming your domain is a federated domain, you will be directed to your local identity server for authentication.

Step 3. Once authenticated by your local identity server, you will then be directed back to Concord to complete the Association process.

Step 4. At this time, you may choose to either associate the account with your Concord credentials or create a new account (if your Client Administrator has enabled the Create User feature).

Step 5. Assuming you have chosen to associate the account with your Concord credentials, enter your Concord username and password.

Step 6. You will then be presented with information from your Concord account for verification. From here you may choose to complete the association process, cancel, or back up to the previous step to take another path.

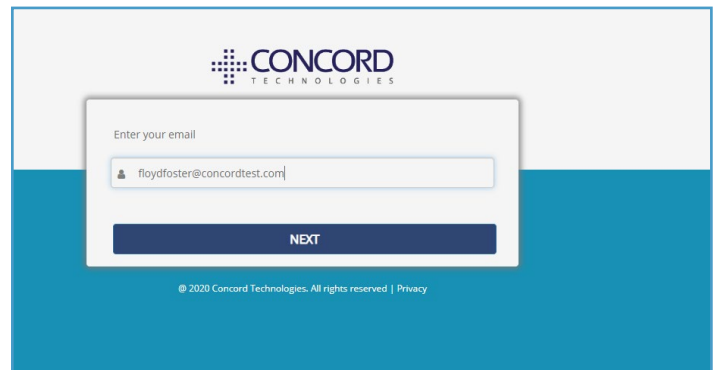
Note: This is the final screen before association of user account using Concord credentials.

Step 7. Once the association is complete, you will be presented with the following welcome message.

Steps to Associate a User Account with Credentials with Images

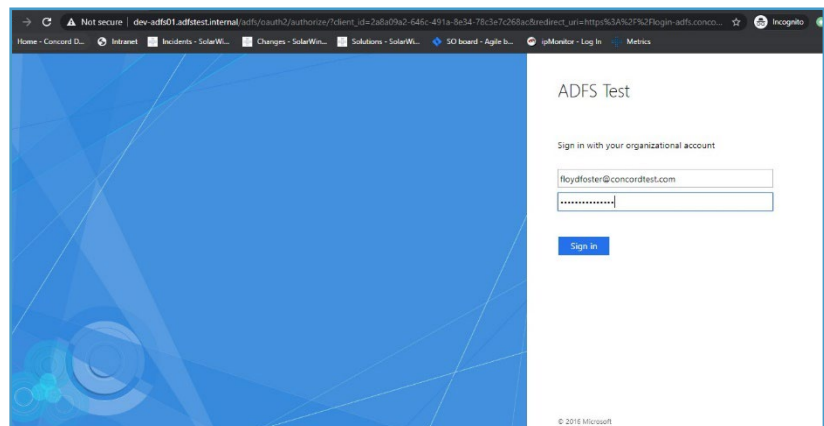
Step 1.

In a web browser, enter the URL <https://portal.concordfax.com/> and you will be directed to Concord's login server.



Step 2.

Enter your email address. Assuming your domain is a federated domain, you will be directed to your local identity server for authentication.



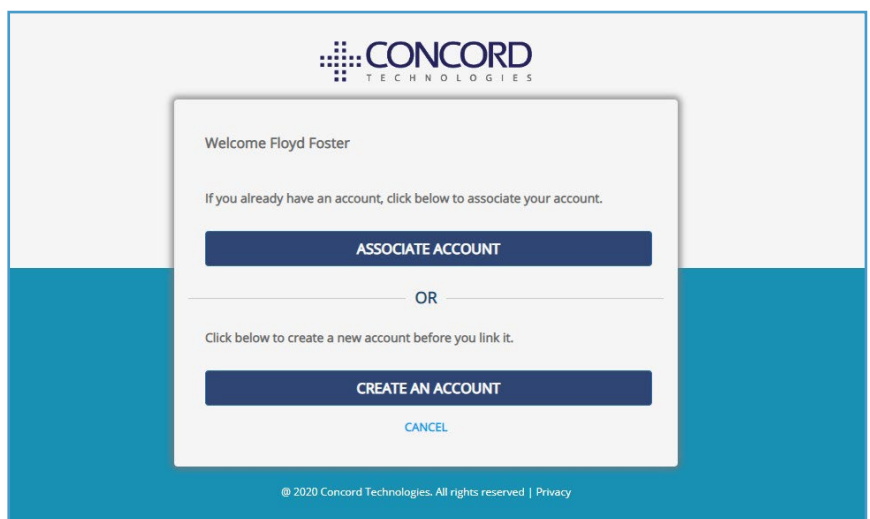
Step 3.

Once authenticated by your local identity server, you will then be directed back to Concord to complete the Association process.

Step 4.

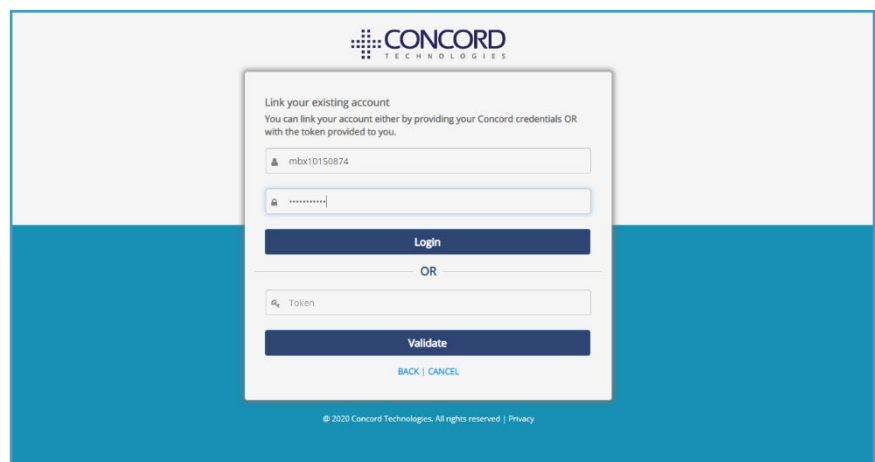
In the first screen, you may choose to either associate the account with your Concord credentials or create a new account.

Note: This step may be omitted if the Client Administrator has disabled the Create User feature.



Step 5.

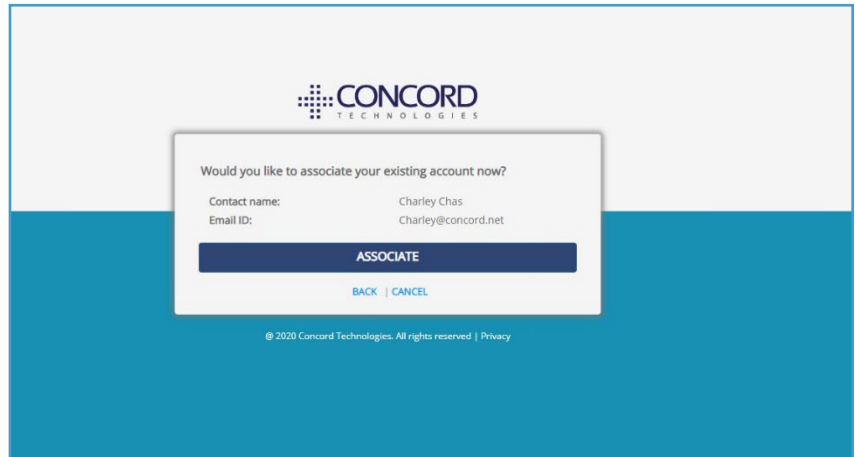
In this scenario, it is assumed you have chosen to associate the account with your Concord credentials and have entered your Concord username and password.



Note: For more information regarding token association, please see the section [Associate with Token](#).

Step 6.

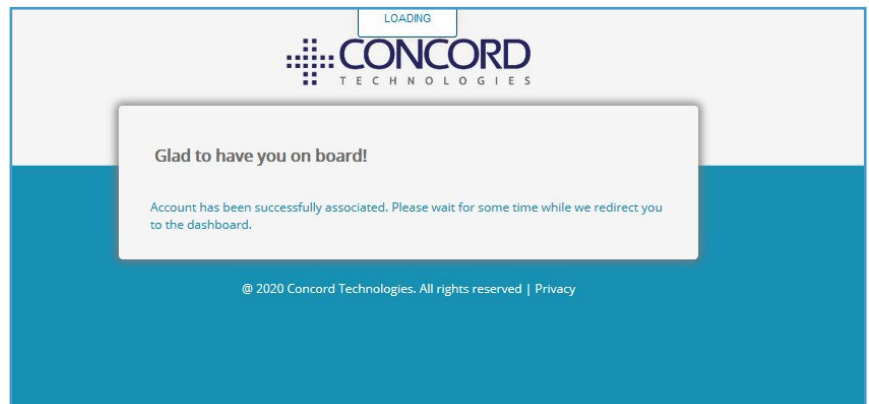
You then be presented with information from your Concord account for verification. From here you may choose to complete the association process, cancel, or back up to the previous step to take another path.



Note: This is the final screen before association of user account using Concord credentials.

Step 7.

Select ASSOCIATE to continue with the process. Once the association is complete, you will be presented with the following welcome message:



Associate With Token (User Account)

For users who have a Concord fax account, but do not know their Concord credentials, the Client Administrator will need to provide them a secure token to enable them to associate with their account.

Important> Based on the permissions selected by the Client Administrator, some of the steps in the Create Account flow may be omitted.

Steps to Associate a User Account with Token

Persona: Administrator

Step 1. First, the Administrator must create a token for the user in the Concord Portal. To do so, the administrator will navigate to the User tab for that user and select “Generate Federated Account Token to link the existing account”.

Note: Once generated, the Administrator **must** provide the token to the user, for Concord does **not** distribute tokens.

Persona: User

Step 2. In a web browser, enter the URL <https://portal.concordfax.com/> and you will be directed to Concord’s login server.

Step 3. You will be prompted to enter your email address. Assuming your domain is a federated domain, you will be directed to your local identity server for authentication.

Step 4. Once authenticated by your local identity server, you will then be directed back to Concord to complete the Association process.

Step 5. At this time, you may choose to either associate the account with the provided token or create a new account.

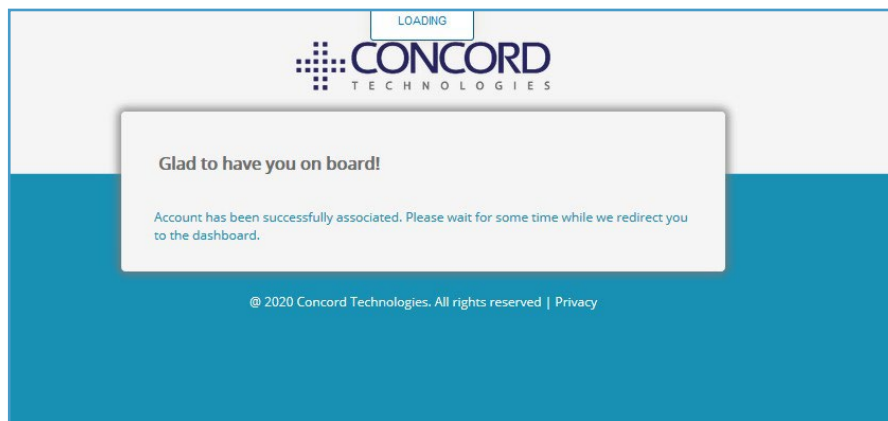
Note: This step may be omitted if the Client Administrator has disabled the Create User feature.

Step 6. At this point enter the token supplied by your administrator and click the Validate button

Step 7. You will then be presented with information from your Concord account for verification. From here you may choose to complete the association process, cancel, or back up to the previous step to take another path.

Note: This is the final screen before association of user account using Concord credentials.

Step 8. Once the association is complete, you will be presented with the following welcome message:

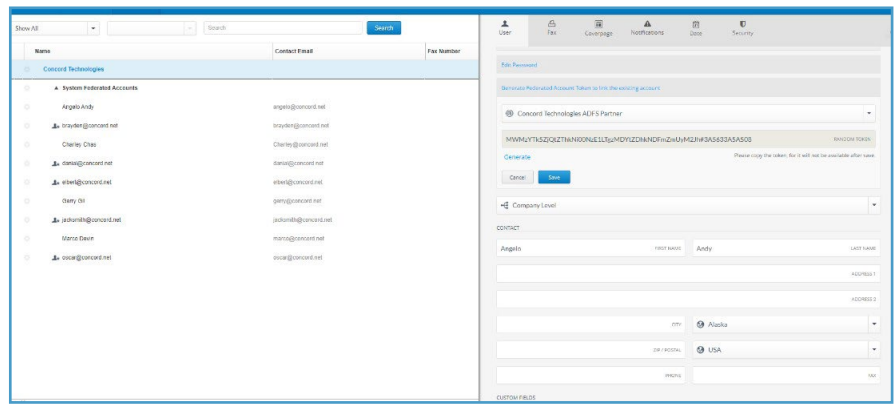


Steps to Associate a User Account with Token with Images

Persona: Administrator

Step 1.

The first step of this process is for the Administrator to create a token for the user in the Concord Portal. To do so, the administrator will navigate to the User tab for that user and select “Generate



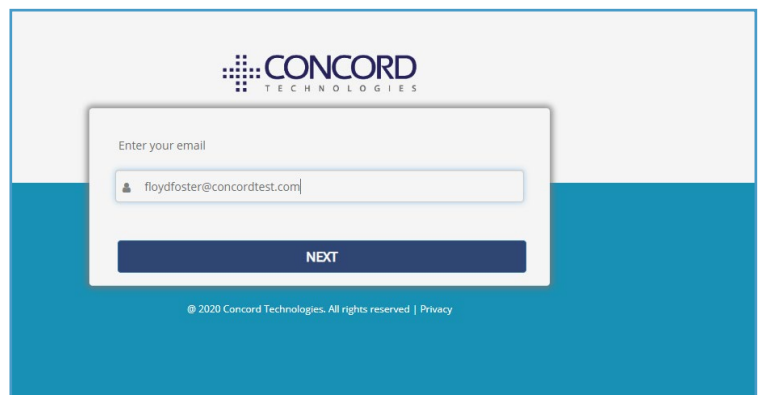
Federated Account Token to link the existing account”.

Note: Once generated, the Administrator **must** provide the token to the user, for Concord does **not** distribute tokens.

Persona: User

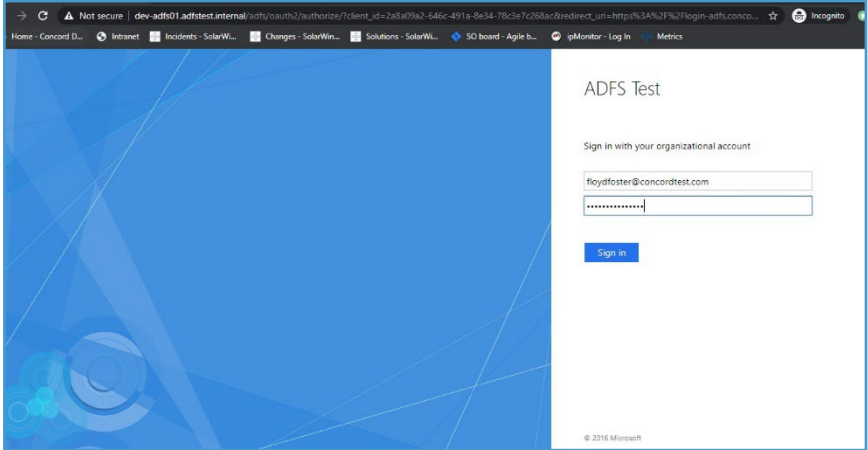
Step 2.

In a web browser, you, the user, will enter the URL <https://portal.concordfax.com/> and you will be directed to Concord’s login server.



Step 3.

Enter your email address. Assuming your domain is a federated domain, you will be directed to your local identity server for authentication.



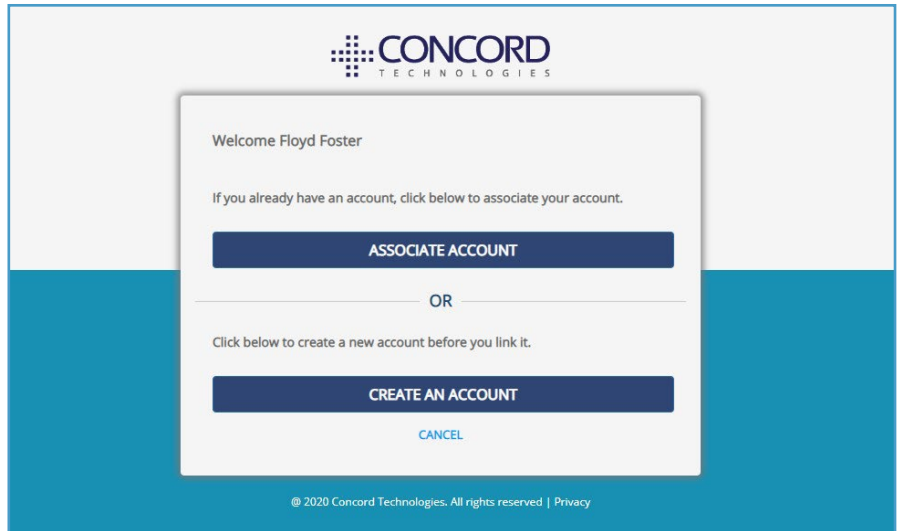
Step 4.

Once authenticated by your local identity server, you will then be directed back to Concord to complete the Association process.

Step 5.

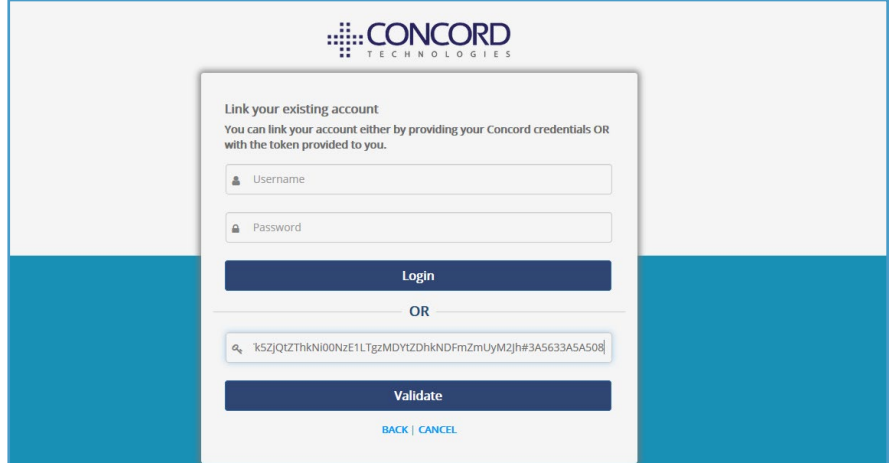
In the first screen, you may choose to either associate the account with the provided token or create a new account.

Note: This step may be omitted if the Client Administrator has disabled the Create User feature.



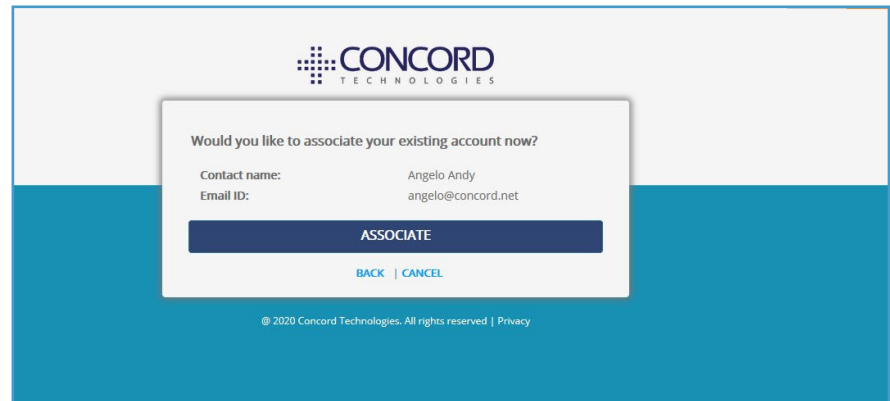
Step 6.

At this point enter the token supplied by your administrator and click the Validate button.



Step 7.

You will then be presented with information from your Concord account for verification. From here you may choose to complete the association process,

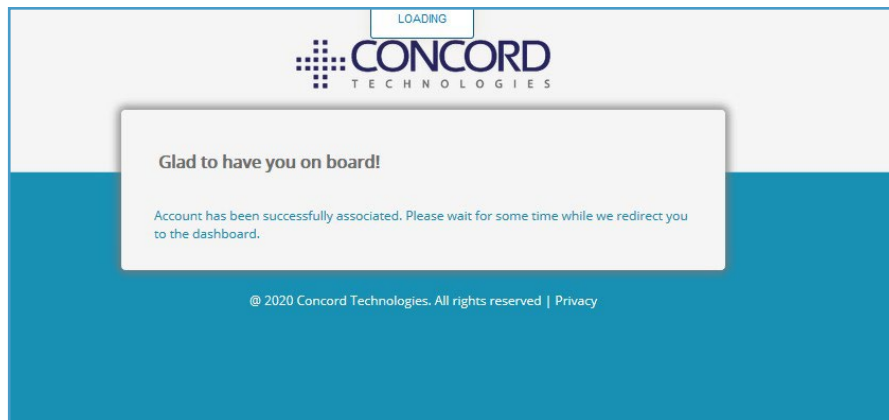


cancel, or back up to the previous step to take another path.

Note: This is the final screen before association of user account using Concord credentials.

Step 8.

Select ASSOCIATE to continue with the process. Once the association is complete, you will be presented with the following welcome message:



Associate With Credentials (Administrator Profile)

For administrators who know their Concord username and password, they will follow the Associate with Credentials flow to link their accounts.

Important> It is important to note, that an Administrator Profile must first be created through the Concord Portal, or through Concord's Account Management API.

Steps to Associate an Administrator Profile with Credentials

Persona: Administrator

Step 1. In a web browser, enter the URL <https://portal.concordfax.com/> and you will be directed to Concord's login server.

Step 2. You will be prompted to enter your email address. Assuming your domain is a federated domain, you will be directed to your local identity server for authentication.

Step 3. Once authenticated by your local identity server, you will then be directed back to Concord to complete the Association process. At this time, you will choose to associate with your Administrative profile using your Concord credentials.

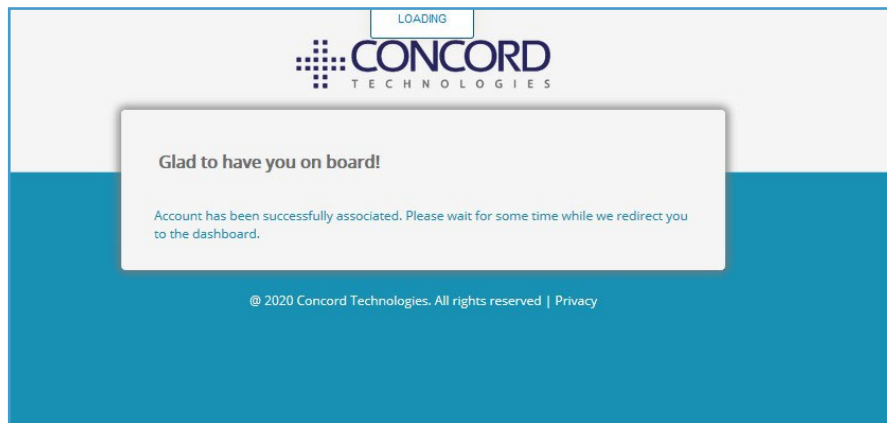
Note: Although the Create Account option is displayed it does not support creating Administrative accounts and should be disregarded.

Step 4. Enter your Concord username and password to associate with your Concord Administrator Profile.

Step 5. You will then be presented with information from your Concord account for verification. From here you may choose to complete the association process, cancel, or back up to the previous step to take another path.

Note: This is the final screen before the association of the administrative profile will be processed.

Step 6. Once the association is complete, you will be presented with the following welcome message:

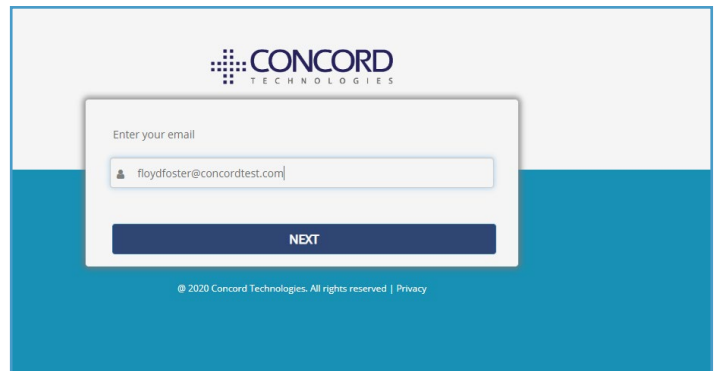


Steps to Associate an Administrator Profile with Credentials with Images

Persona: Administrator

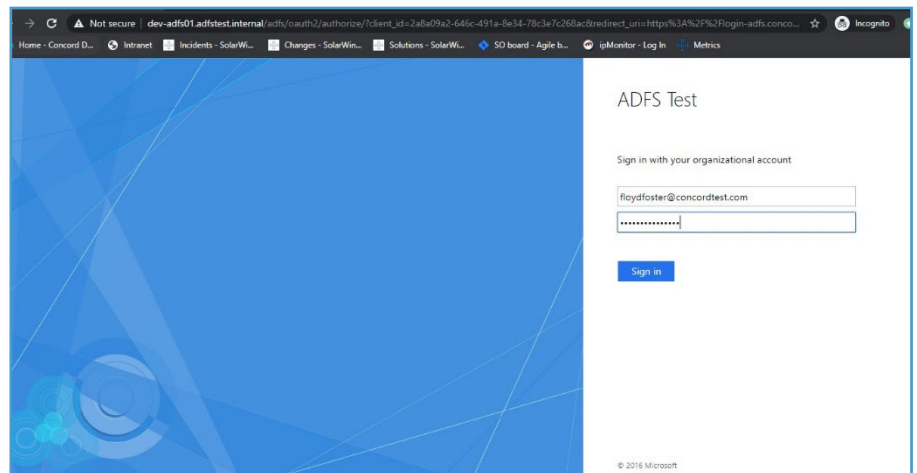
Step 1.

In a web browser, enter the URL <https://portal.concordfax.com/> and you will be directed to Concord's login server.



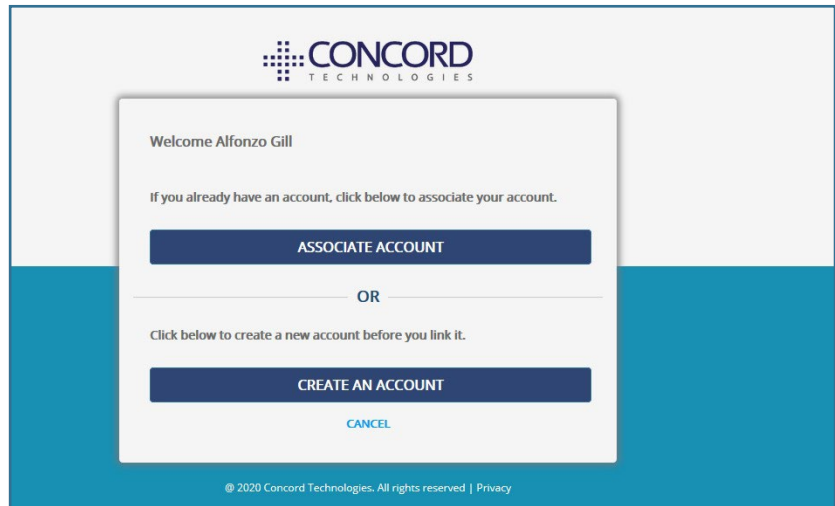
Step 2.

You will be prompted to enter your email address. Assuming your domain is a federated domain, you will be directed to your local identity server for authentication.



Step 3.

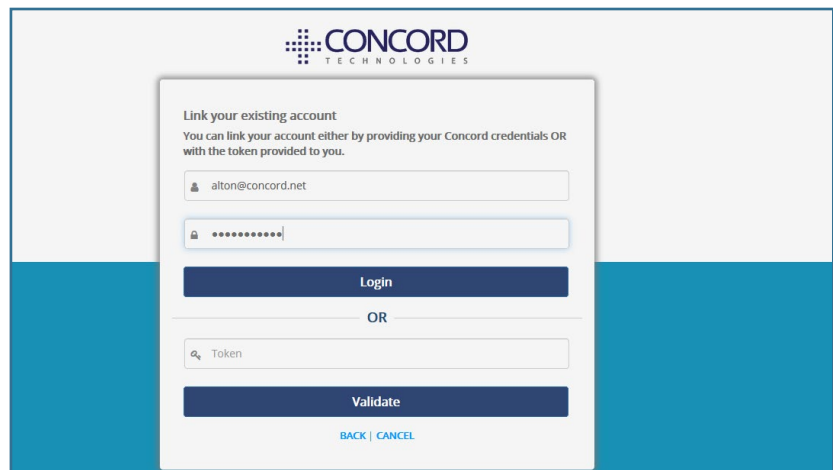
Once authenticated by your local identity server, you will then be directed back to Concord to complete the Association process. At this time, you will choose to associate with your Administrative profile using your Concord credentials.



Note: Although the Create Account option is displayed it does not support creating Administrative accounts and should be disregarded.

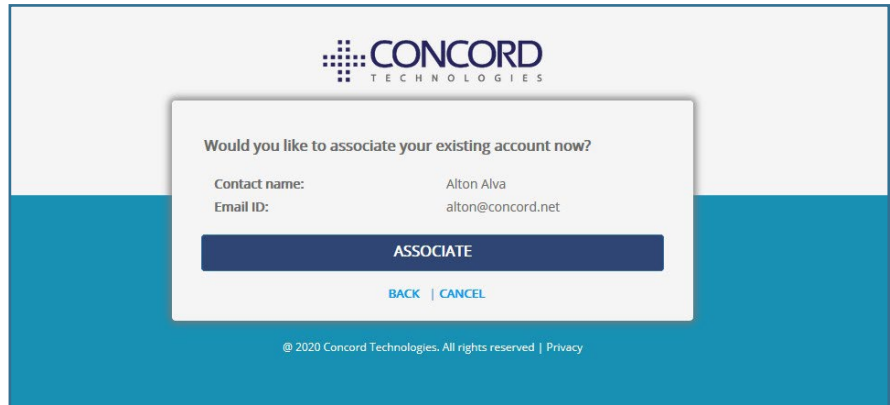
Step 4.

Enter your Concord username and password to associate with your Concord Administrator Profile.



Step 5.

You will then be presented with information from your Concord account for verification. From here you may choose to complete the association

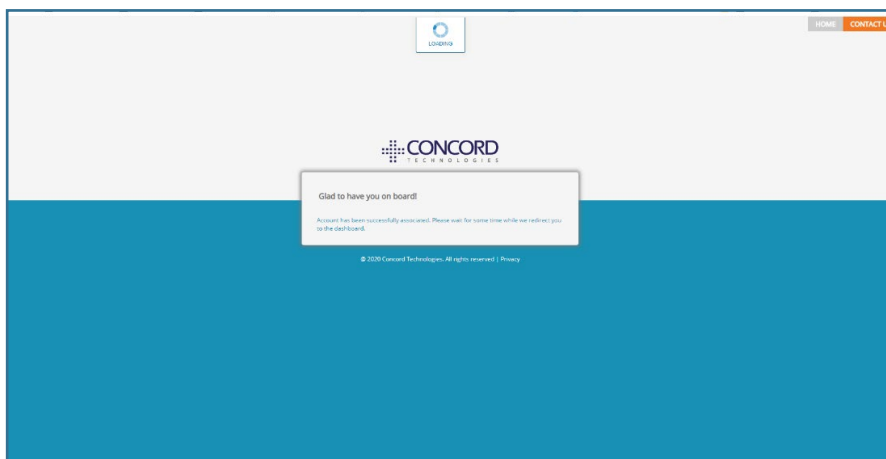


process, cancel, or back up to the previous step to take another path.

Note: This is the final screen before the association of the administrative profile will be processed.

Step 6.

Once the association is complete, you will be presented with the following welcome message:



Associate With Token (Administrator Profile)

For administrators (admins) who have a Concord Administrative Profile but do not know their Concord credentials, their Company Administrator will need to provide them a secure token to enable them to associate with their account.

Important>

- The Company Administrator has additional privileges and will create a token for the Administrator attempting to associate with their account.
- It is important to note, that an Administrator Profile must first be created through the Concord Portal, or through Concord's Account Management API.

Steps to Associate an Administrator Profile with Token

Persona: Company Administrator

Step 1. First, the Company Administrator must create a token for the admin in the Concord Portal. To do so, the Company Administrator will navigate to the Administrator Details tab (Admin) and select "Generate Federated Account Token to link the existing account".

Note: Once generated, the Company Administrator must provide the token to the admin, for Concord does not distribute tokens.

Persona: Admin

Step 2. In a web browser, enter the URL <https://portal.concordfax.com/> and you will be directed to Concord's login server.

Step 3. You will be prompted to enter your email address. Assuming your domain is a federated domain, you will be directed to your local identity server for authentication.

Step 4. Once authenticated by your local identity server, you will then be directed back to Concord to complete the Association process. At this time, you will choose to associate with your Administrative profile using the provided token.

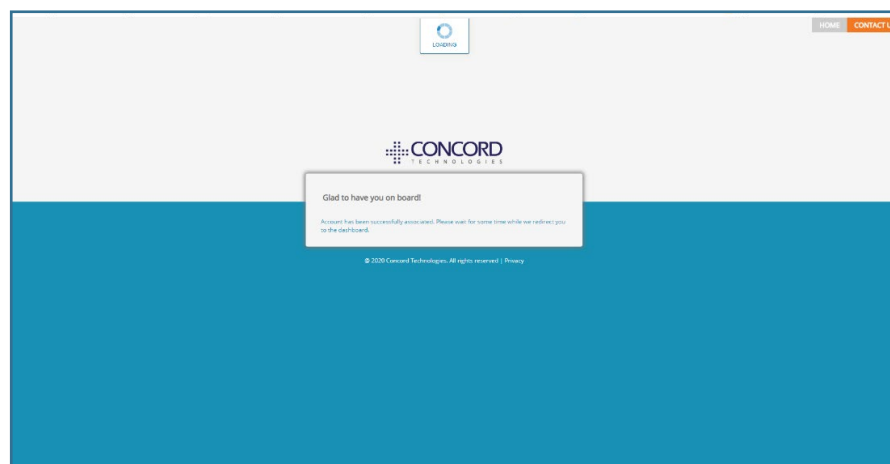
Note: Although the Create Account option is displayed, it does not support creating Administrative accounts and should be disregarded.

Step 5. At this point enter the token supplied by your administrator and click the Validate button

Step 6. You will then be presented with information from your Concord account for verification. From here you may choose to complete the association process, cancel, or back up to the previous step to take another path.

Note: This is the final screen before association of user account using Concord credentials.

Step 7. Once the association is complete, you will be presented with a welcome message:

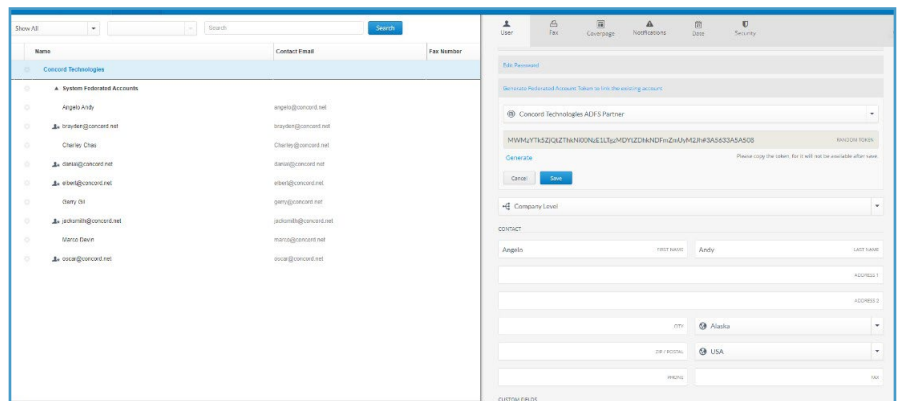


Steps to Associate an Administrator Profile with Token with Images

Persona: Company Administrator

Step 1.

To create a token, the **Company Administrator** will navigate to the Administrator Details tab (Admin) and select “Generate Federated Account Token to link the existing account”.

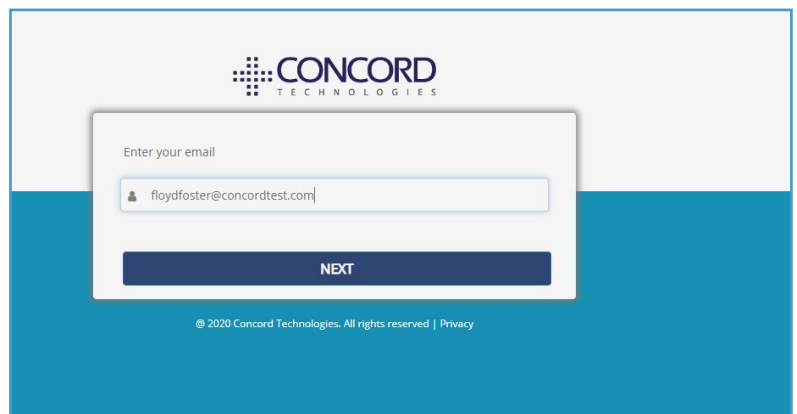


Note: Once generated, the Company Administrator **must** provide the token to the admin, for Concord does **not** distribute tokens.

Persona: Admin

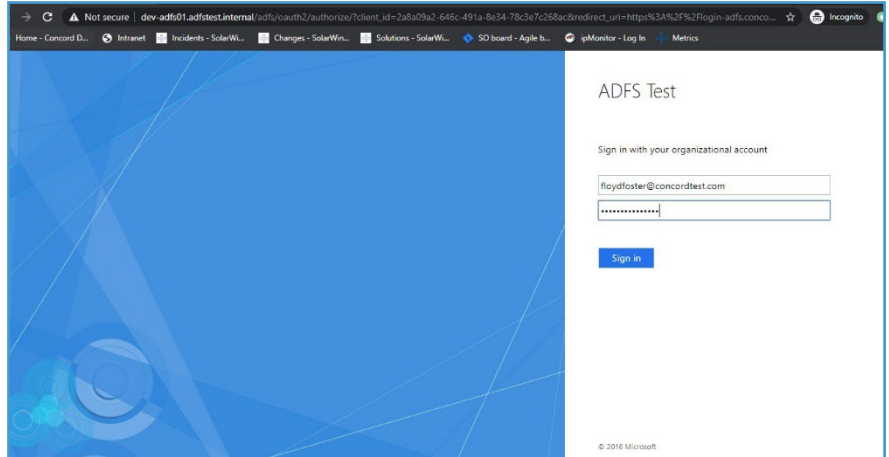
Step 2.

In a web browser, enter the URL <https://portal.concordfax.com/> and you will be directed to Concord’s login server.



Step 3.

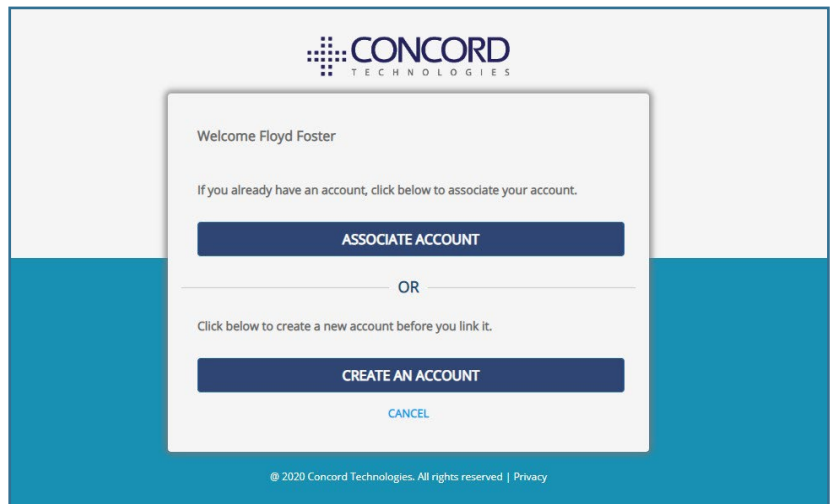
You will be prompted to enter your email address. Assuming your domain is a federated domain, you will be directed to your local identity server for authentication.



Step 4.

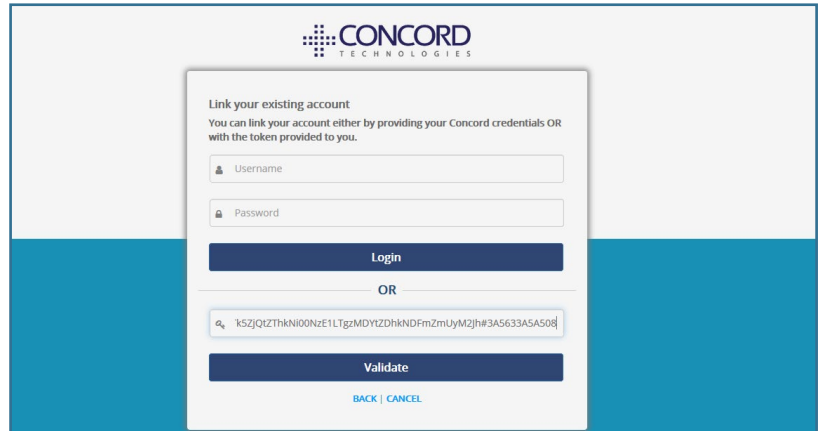
Once authenticated by your local identity server, you will then be directed back to Concord to complete the Association process. At this time, you will choose to associate with your Administrative profile using the provided token.

Note: Although the Create Account option is displayed, it does not support creating Administrative accounts and should be disregarded.



Step 5.

At this point enter the token supplied by your administrator and click the Validate button.



CONCORD TECHNOLOGIES

Link your existing account
You can link your account either by providing your Concord credentials OR with the token provided to you.

Username

Password

Login

OR

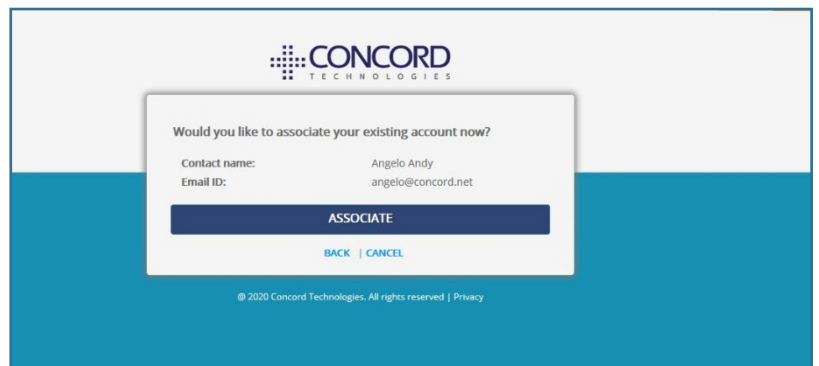
TKSZjQtZThkNi00Nze1LTgrMDYtZDhkNDFmZmUyM2Jh#3A5633A5A508

Validate

BACK | CANCEL

Step 6.

You will then be presented with information from your Concord account for verification. From here you may choose to complete the association process, cancel, or back up to the previous step to take another path.



CONCORD TECHNOLOGIES

Would you like to associate your existing account now?

Contact name: Angelo Andy
Email ID: angelo@concord.net

ASSOCIATE

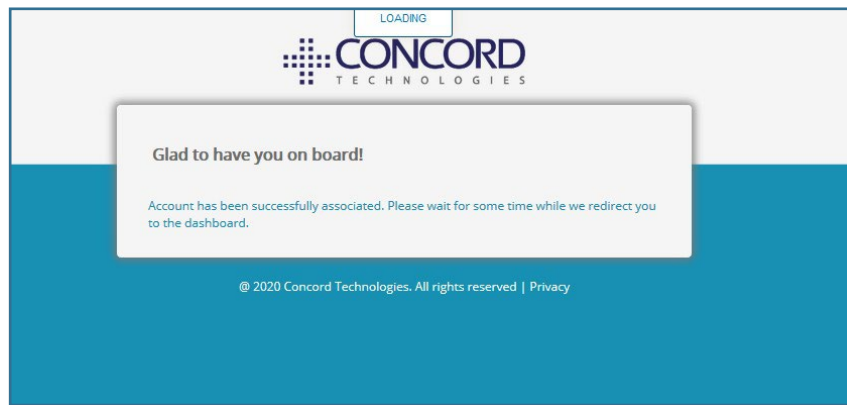
BACK | CANCEL

© 2020 Concord Technologies. All rights reserved | Privacy

Note: This is the final screen before association of user account using Concord credentials.

Step 7.

Once the association is complete, you will be presented with the following welcome message:



Federated SSO User Experience

Now that Concord is a Federated Partner, what is the User Experience?

Once a customer has configured and enabled Federated Services, and their users and administrators alike have associated existing accounts, they will follow a federated authentication flow when accessing Concord's web-based applications. The steps could not be simpler.

Step 1. In a web browser, enter the URL <https://portal.concordfax.com/> and you will be directed to Concord's login server.

Step 2. Enter your email address, and you will be directed to your local Identity Server for authentication

Step 3. Once authenticated you will be directed to the Concord portal.

There will no longer be a need to know your Concord credentials.

Important>

The process will be identical for access to NEXTSTEP or Fax Inbox.

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.

Federated SSO - Glossary of Terms

Term	Definition
Account Partner	<p>The Account Partner is the organization in the federation trust relationship that physically stores user accounts in a Federated Identity attribute store.</p> <p>The Concord Customer is the Account Partner</p>
AD FS	<p>Active Directory Federation Services (AD FS) is a feature of the Windows Server operating system (OS) that extends end users' single sign-on (SSO) access to applications and systems outside the corporate firewall and reach of the Active Directory.</p>
Claim	<p>A claim is a piece of information asserted about an Entity. Federation brokers trust between disparate entities by allowing the trusted exchange of claims that contain values that may be used to make authorization decisions. In Concord terms, claims may be used to set specific configurations for users such as department.</p>
Client ID	<p>The Client Identifier is a public identifier for an application leveraging federation.</p>
Client Secret	<p>A client secret is a secret known only to the application and the authorization server. It protects your resources by only granting tokens to authorized requestors.</p>
Federated Application	<p>A web-based application that is Federated SSO enabled, which means that federated users can access it via their Identity Provider.</p>

Term	Definition
Federated User	A user whose account resides in an account partner organization, who can access federated applications that reside in a resource partner organization. This would constitute a Concord user or administrator that is enabled for Federated access.
Metadata Address	The metadata address is a customer provided URL endpoint for the discovery document to use to reference the Client's identity server.
Resource Partner	<p>The Resource Partner is the organization that contains the Web servers hosting the Web-based applications that will be accessed by users in the account partner.</p> <p>Concord is the Resource Partner</p>
Security Token	A cryptographically signed data unit that expresses one or more claims. In a federated partnership, a signed security token indicates that the federation server that issues the token has successfully verified the authenticity of the federated user.
Scopes	User information that defines the specific actions applications can be allowed to do on a user's behalf
Single Sign on	An optimization of the authentication sequence to remove the burden of repeated logon actions by an end user. Also known as SSO.

Getting Help

Concord Technologies Premium Support

Customer service hours are Monday – Friday from 9:00 AM to 9:00 PM EST.

Contact Information (Technical Support):

Email: premiumsupport@concord.net

Phone: +1 (206) 441-3346

Fax: +1 (206) 441-7965

After-hours Emergency Support (For critical issues only): +1 (206) 467-4068