Single Sign-On for SureTrend Cloud

Enable Federation in SureTrend Cloud

1. Log in into SureTrend Cloud
   Note: You must be the owner of the account to enable federation for Single Sign-On (SSO).
2. Click **Settings** and select Account Management.
3. Click **Enable Federation.**
4. Enter the Company Name, Client ID, Client Secret, Metadata Address, and Identity Provider.
   See below for a description of each field.

Identity Provider Options

Company Name – This is your company name, it needs to be a unique name. If the name already exists, then it has been used to set up Single Sign-On in another account.

ClientId – Client ID or consumer key, is the identity provider key that is connecting with SureTrend Cloud. This is usually provided with the registered app in the service (Azure, AWS Cognito, Salesforce, etc.). For details on how to set up an app in your identity provider service, please refer to your administrator or your identity provider's documentation.

Client Secret – A secret key for the registered app in identity provider service.

Metadata Address – This address refers to metadata document from the identity provider and is mostly formatted like ***https://{domain}/.well-known/openid-configuration***. This can be found in the registered app settings from your identity provider service.

Identity Provider – The schema used by your identity provider service to establish the identity of a user. Currently, **OpenIdConnect** is the only schema

supported by SureTrend Cloud.

Additional Options

All additional options are optional. See below for a description of these options.

Callback Path – This field is prepopulated with the Callback URL. The Callback Path is needed for the registered app on identity provider service side, usually called Callback URL. This information should be entered into the app settings for the app registered with your identity provider service. The complete Callback URL is: https://suretrend.hygiena.com/FederationLoginCallback

Logging into SureTrend Cloud with Single Sign-On

To log in into SureTrend Cloud using configured SSO, you can use SureTrend login page or navigate directly to the federation link. Both options explained below.

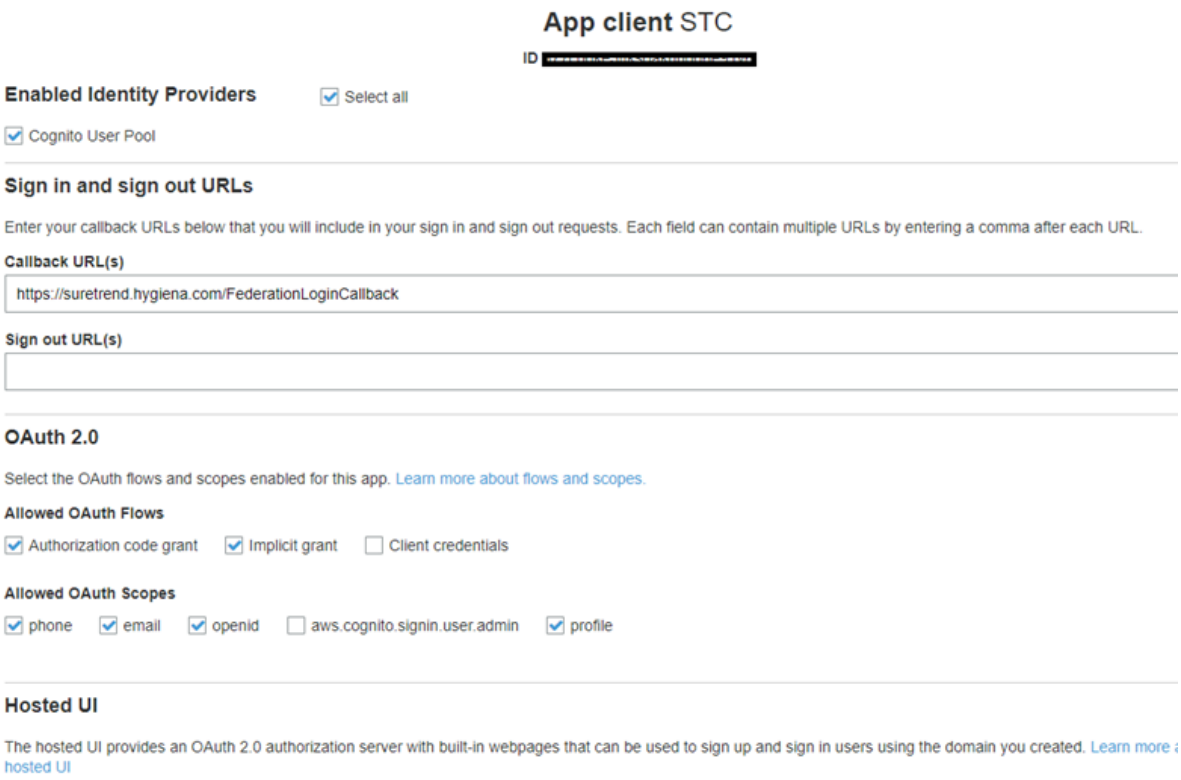
Logging into SureTrend Cloud Using Single Sign-On

1. Click on the Single Sign-On link on the SureTrend Cloud login page.
   Note: You may also use the direct SSO link for your account. The direct link is https://suretrend.hygiena.com/FederationLogin/{companyName}, where {companyName} is the name provided in your Identity provider options in SureTrend Cloud.
2. Enter your email address and complete the CAPTCHA, then click **Log In**.
3. You will be redirected to your identity provider. Complete the login process from your identity provider.
4. Once you have finished logging in, you will be redirected to your SureTrend Cloud account.

App Registrations for Identity Provider Services

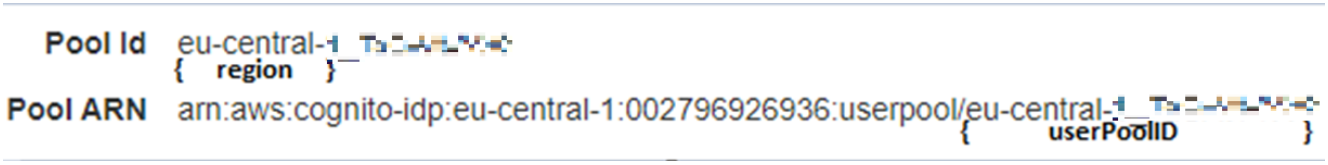
Amazon – OpenIdConnect setup

1. Navigate to Cognito AWS service and click on Manage User Pools.
2. If there is no user pools created, you can create new one. Details about how to create and manage user pools can be found here.
3. Check **Cognito User Pool**.
4. Enter https://suretrend.hygiena.com/FederationLoginCallback for the Callback URL(s).
5. Check **Implicit Grant**.
6. Uncheck **aws.cognito.signin.user.admin**.



The metadata address is in a format like this: https://cognito-idp.{region}.amazonaws.com/{userPoolId}/.well-known/openid-configuration

Replace {region} with user pool region and {userPoolId} with userpool.



Azure OpenIdConnect setup

OpenIdConnect can be configured in Azure following the steps below.

1. Log into Azure portal (portal.azure.com)
2. Navigate to Azure Active Directory.
3. From the left pane, select **App registrations**.
4. Click **New registration**.
5. Enter name for your application then click **Register**.
6. On the left pane, click**Authentication**.
7. Click A**dd a platform**.
8. Set the Redirect URI to https://suretrend.hygiena.com/FederationLoginCallback and ensure ID tokens is selected.

The Client ID is Application (client) ID from Overview section. The Client secret needs to be generated following the steps below.

1. On the left pane, under newly registered app, click **Certificates & secrets**.
2. Under Client secrets, click **New client secret**.
3. Use value from client secret to set up Client Secret field in STC.

Metadata address can be found under Overview -> Endpoints. Copy value from **OpenID Connect metadata document.**