App onboarding

Introduction

SecureAuth IdP integrates with your company's applications to provide Single sign-on (SSO) access via a Security Assertion Markup Language (SAML) assertion to all applications the authorized end-user is allowed to access. Each SAML application integration configured on the SecureAuth IdP Web Admin results in the creation of an XML metadata file to be uploaded to your application (service provider). This metadata file contains information to identify and assert the end-user during the authentication login process in which digitally-signed XML documents are exchanged between SecureAuth IdP and the application over a secure connection.

You create and manage SAML application integrations using the app onboarding tool on the New Experience user interface. Select a SAML application template from the library, then use common components to customize each new application integration you create. Provide a name for the app, associate a data store with it, and specify which group(s) can access the app. Upload a logo to quickly find the completed app in the Application Manager list.

Define how the connection will be initiated – by service provider (SP-initiated) or by SecureAuth IdP (IdP-initiated) – and configure user ID mapping criteria, user attributes, and information about the SAML assertion.

> The SP-initiated SAML application integration starts the login process at the service provider / application, then redirects the end-user to SecureAuth IdP for authentication, and finally asserts the end-user back to the application once successfully authenticated.
>
> The IdP-initiated SAML application integration starts the login process at SecureAuth IdP and asserts the end-user to the application once successfully authenticated.

Use the Classic Experience user interface to configure the end-user's authentication Workflow, and enable Two-Factor Authentication methods and Adaptive Authentication modules. Return to the New Experience user interface to make any modifications to data stores associated with the app.

NOTE: An application integration created on the New Experience user interface is stored in the cloud as well as in the web.config file on the SecureAuth IdP appliance, making many configured elements of the application accessible on the Classic Experience user interface.

Prerequisites

- SecureAuth IdP version 9.3 installed and running.
- On-premises Active Directory / SQL Server (membership directory / profile directory) integrated with SecureAuth IdP which can be used in the application integration.
- Service provider administrator account to configure the application to be integrated with SecureAuth IdP.

Select the application integration

SAML Application integration

Salesforce app integration

See Application template library master list for the current list of available application templates