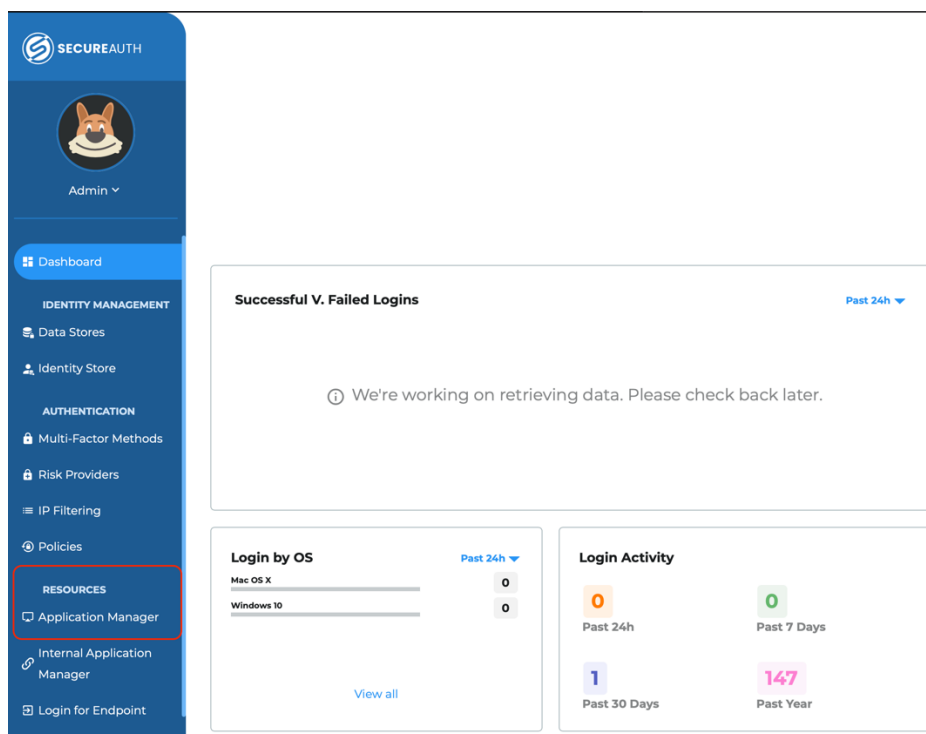


# Secureauth New Client Setup Guide.

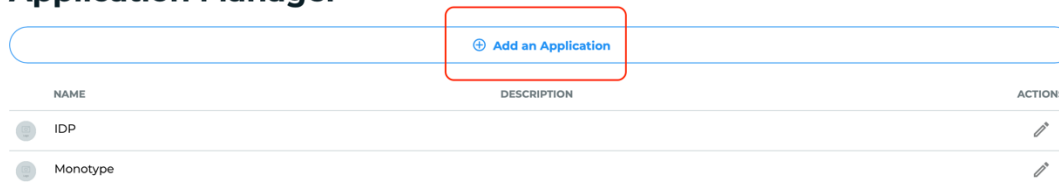
Do the below steps in your Secureauth Admin dashboard so as to provide Single Sign On, password-less authentication resulting in quick and easy access to Monotype Fonts and other Monotype properties

1. Sign into your Secureauth dashboard and select 'Application Manager' under Resources



2. Click 'Add An Application' to create a new application







## Application Manager



3. Select 'SAML Application' from the list of options which open up

[Back to Application Manager](#)

## Add Application (Step 1)

NAME	
 SAML Application	<a href="#">Select...</a>
 10,000ft	<a href="#">Select...</a>
 123ContactForm	<a href="#">Select...</a>
 15Five	<a href="#">Select...</a>
 23Video	<a href="#">Select...</a>
 360 Online	<a href="#">Select...</a>
 / ...	<a href="#">Select...</a>

4. Do the following settings:

a. Give the application a name. – 'Monotype' or 'Monotype Fonts'

b. Monotype logo:

<https://d20o8o00kc97oh.cloudfront.net/assets/images/Monotype.png>

c. Authentication Policy – Default Policy

d. Assign the application to the users you want to give access by choosing the Data Stores as per your Organisation's setup

e. Choose whether you want to give access to every group in selected stores or select the groups as per your need.

Click Continue at the bottom

**SECUREAUTH**

Admin ▾

Dashboard

IDENTITY MANAGEMENT

- Data Stores
- Identity Store

AUTHENTICATION

- Multi-Factor Methods
- Risk Providers
- IP Filtering
- Policies

RESOURCES

- Application Manager**
- Internal Application Manager
- Login for Endpoint

## Application Manager

NAME

- IDP
- Monotype

## Application Details (Step 2)

Logo

Upload

Application Name

Monotype Fonts

Application Description

### AUTHENTICATION AND ACCESS

**Authentication Policy** \*

Select the authentication policy that will apply to this application.

Default Policy ▾

**Data Stores** \*

Select the data stores for this application. Only users in these data stores can access this application.

IDS X

**Groups**

Only these groups will have access to this application.

☒ Allow every group in your selected data stores to access this application.

Continue Go Back

5. Do the following settings in the next step
  - a. Connection Type : SP initiated, By Redirect
  - b. User ID Profile field: Authenticated User ID
  - c. Name ID Format: Unspecified (Default)
  - d. IDP Issuer:
 

urn:auth0:monotypeidp:<Get value from Monotype>
  - e. ACS URL :-
 

https://secure.monotype.com/login/callback?connection=<Get value from Monotype>
  - f. Audience :-
 

urn:auth0:monotypeidp:<Get value from Monotype>

The connection name will be provided by the solution architect. Insert the same above

## Connection Settings (Step 3)

### CONFIGURE CONNECTION

#### Connection Type

SP Initiated

☒ By Redirect ☐ By Post ⓘ

### USER ID MAPPING

#### User ID Profile Field

Select the profile field in your data store that contains your users' IDs.

Authenticated User ID

#### Name ID Format

urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified

### SAML ASSERTION

#### IdP Issuer

Also known as the IdP Entity ID. This is a unique string that identifies the IdP

urn:auth0:monotypeidp:<Get value from Monotype>

#### Assertion Consumer Service (ACS)

This URL, provided by the service provider, is used to accept a SAML assertion

https://secure.monotype.com/login/callback?connection=<Get\_value\_from\_Monotype>

#### Relay State

User will be directed to this URL after authentication

#### Recipient

#### Audience

urn:auth0:monotypeidp:<Get value from Monotype>

## 6. Continue with below:

- a. Choose the IDP Signing Certificate from those available in your organisation
- b. Signing Algorithm: SHA2
- c. Check Sign SAML Assertion and Sign SAML Message

#### Assertion will be valid for:

1 Hours 0 Minutes ⓘ

#### Offset Minutes

Minutes ⓘ

#### IdP Signing Certificate \*

EC2AMAZ-F4N3ISK [Select Certificate](#)

#### IdP Signing Certificate Serial Number

74FEAE495B368ABD42CC1F2E9B98E6CB

[Copy to Clipboard](#)

#### Signing Algorithm

☐ SHA1 ☒ SHA2

☒ Sign SAML Assertion

☒ Sign SAML Message

☐ Encrypt SAML Assertion

## 7. Next add the below 4 attributes

- FirstName – First Name
- LastName – Last Name
- Email – Email 1 (Work)
- Groups – Groups

Click Add Application after adding the attributes

SAML ATTRIBUTES

[Add SAML Attribute](#)

Attribute Name	FirstName	Delete Attribute
Data Store Property	First Name	
Namespace (1:1)		
Filtered Group		
Attribute Name	LastName	Delete Attribute
Data Store Property	Last Name	
Namespace (1:1)		
Filtered Group		
Attribute Name	Email	Delete Attribute
Data Store Property	Email 1 (Work)	
Namespace (1:1)		
Filtered Group		
Attribute Name	Groups	Delete Attribute
Data Store Property	Groups	
Namespace (1:1)		
Filtered Group		

[Add Application](#) [Go Back](#) [Upload Metadata](#)

## 8. In the next step, Copy the Login URL and download the IDP signing Certificate

### Information for Service Providers (Step 4)

Complete the integration and establish a working connection with SecureAuth by using the information below to configure your Service Provider (SP).

#### Login URL

<https://pov9.identity.secureauth.com/SecureAuth4>

[Copy to Clipboard](#)

#### Logout URL

<https://pov9.identity.secureauth.com/SecureAuth4/Logout.aspx>

[Copy to Clipboard](#)

#### IDP Issuer

urn:auth0:monotypeidp:<Get value from Monotype>

[Copy to Clipboard](#)

#### IDP Signing Certificate

74FEAE495B368ABD42CC1F2E9B98E6CB

[Download](#)

9. Send below details to the Monotype Solution Architect or mail to success@monotype.com with Subject line: <Company\_Name SSO setup>
  - a. Initiate Single Sign-on URL
  - b. Signing certificate downloaded
  
10. Once Monotype receives the above details from you, we will set up SSO configuration at our end. Once validated, your SSO access will be all set