Circle Security

Circle for SailPoint

Implementation Guide

Context

This guide helps you to plan the implementation of Circle Access for Credential-free access to the SailPoint environment. It is written for SailPoint administrators who **build, deploy, and maintain** the Circle Access service and features for their organizations.

About Circle Access

Circle Access serves as the basis for our **uncompromising Authentication solution** through a simple to use **API**. It provides cryptographic authentication that **eliminates all cloud vulnerabilities** with a frictionless **U**ser E**X**perience. For more information about Circle Access and about the platform, see https://www.circlesecurity.ai

Circle Access for SailPoint

Prerequisites before starting the setup and implementation of Circle for SailPoint:

1. You should be the SailPoint Administrator
2. You will be using the same computer for the entire process
3. Ensure that Circle Service is installed on this computer

Overall summary

Implementation of Circle Access for SailPoint is just a few steps.

The result of this guide is that SailPoint users will be redirected to Circle Access when they try to login.

Step 1. Install Circle Service

If you haven't done this already, download and install Circle Service for your operating system.

You can find it on https://circlesecurity.ai under the downloads link in the upper right of the home page.

Step 2. Install Circle Access App

Open the AppStore on your phone and search for 'Circle Access'; install and open it.

When prompted, select 'Start fresh' and wait for it to finish. This can take a minute or so (it's creating 4k RSA encryption keys which can take a while on some devices)

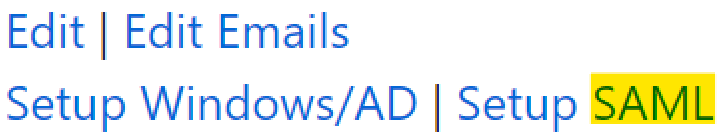
Step 3. Create a Circle Access Tenant

Navigate to https://adsso.circlesecurity.ai and click the 'Login with Circle' button.

Open Circle Access on your mobile device and scan the QR code.

The website will do some stuff then prompt you to scan one more QR code. Scan the code and the website will automatically create a tenant for you, create license keys, app keys, and more encryption keys and store it all in a secure Circle capsule on your computer and **Redirects** you to Auto Provisioning Done page, just renavigate to https://adsso.circlesecurity.ai and login once again by scanning if prompted.

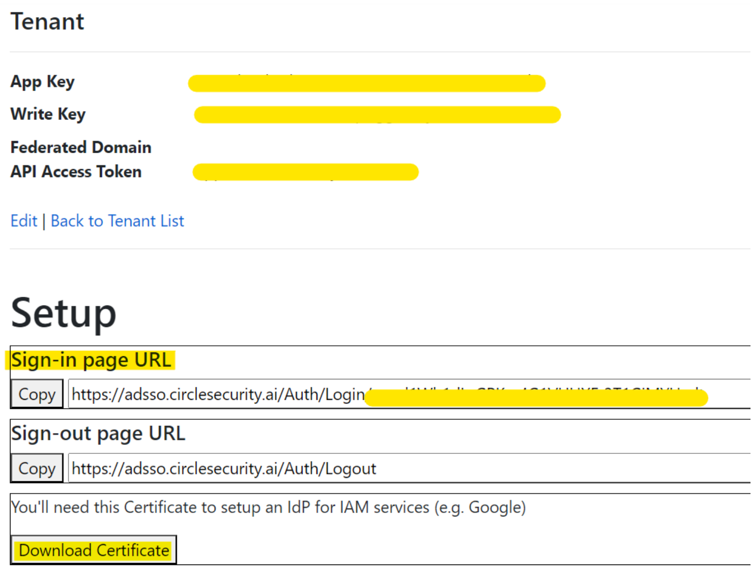
You should now see a tenant created for you with some options to it, click on Setup SAML.



Edit | Edit Emails

Setup Windows/AD | Setup SAML

After this the user should see a tenant page with setup information.



Tenant

App Key	[redacted]
Write Key	[redacted]
Federated Domain	
API Access Token	[redacted]

Edit | Back to Tenant List

Setup

Sign-in page URL

Copy https://adsso.circlesecurity.ai/Auth/Login[redacted]

Sign-out page URL

Copy https://adsso.circlesecurity.ai/Auth/Logout

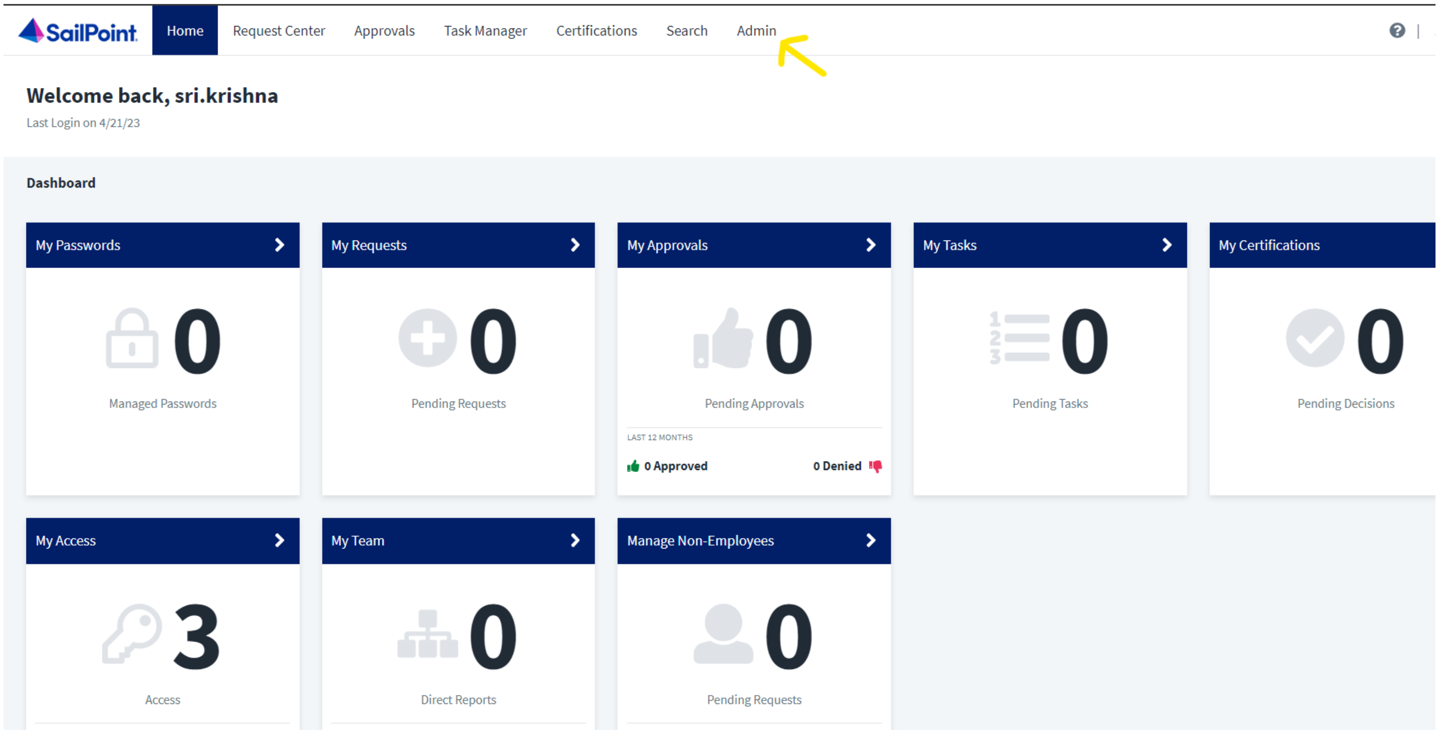
You'll need this Certificate to setup an IdP for IAM services (e.g. Google)

Download Certificate

Here download the certificate also copy over App Key(this will be Entity ID), Sign-in page URL and Sign-out page URL, we will need these for service provider setup in sailpoint in the next step. Preferably you could keep this tab open and then follow the next steps.

Step 4. Setting up Circle Access as Service Provider for SailPoint

For this step, you'll need to be a SailPoint administrator. Now, head over to your **SailPoint Website** eg: https://dummyTenant.identitynow.com and log into your SailPoint admin console.



Welcome back, sri.krishna

Last Login on 4/21/23

Dashboard

My Passwords 0 Managed Passwords

My Requests 0 Pending Requests

My Approvals 0 Pending Approvals

LAST 12 MONTHS 0 Approved 0 Denied

My Tasks 0 Pending Tasks

My Certifications 0 Pending Decisions

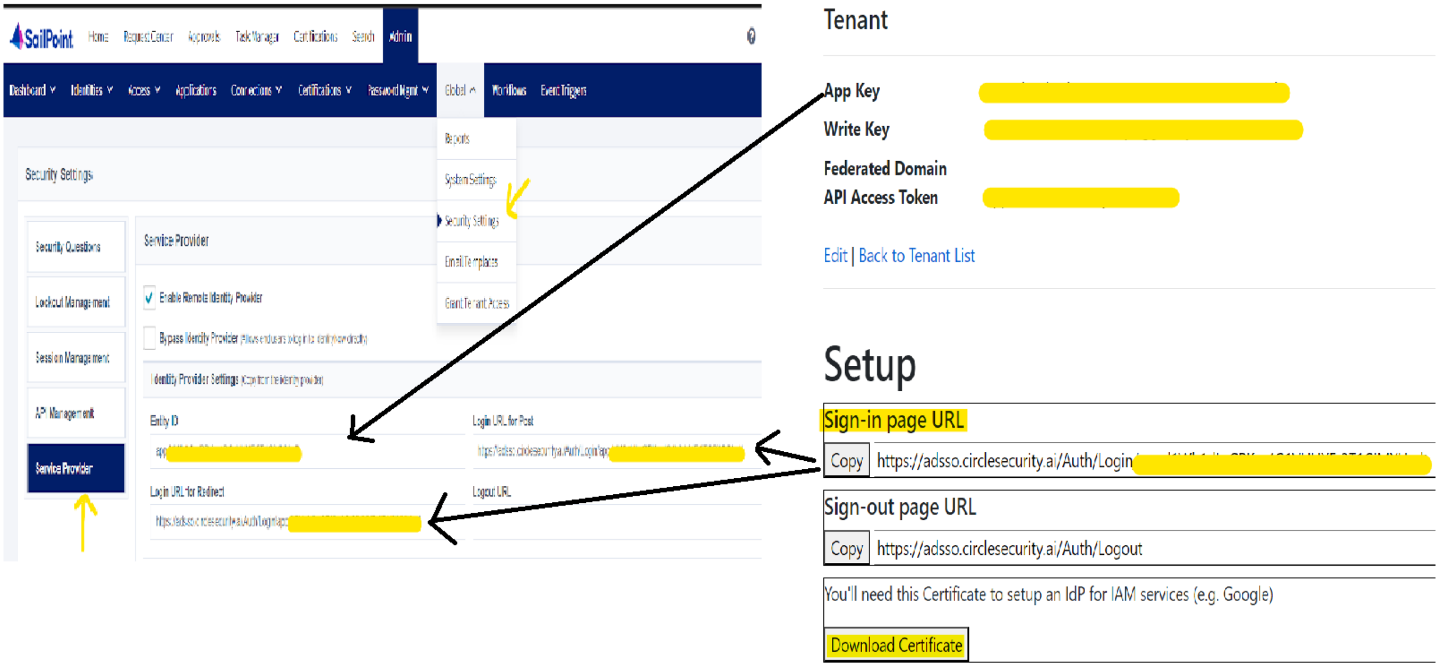
My Access 3 Access

My Team 0 Direct Reports

Manage Non-Employees 0 Pending Requests

Once logged in head over to

Global->Security->Service Provider



Service Provider

☑ Enable Remote Identity Provider

□ Bypass Identity Provider (allows end users to login to identity now directly)

Identity Provider Settings (configure the identity provider)

Entity ID: app[redacted]

Login URL for Post: https://adsso.circlesecurity.ai/Auth/Login?app[redacted]

Login URL for Redirect: https://adsso.circlesecurity.ai/Auth/Login?app[redacted]

Logout URL

Tenant

App Key [redacted]

Write Key [redacted]

Federated Domain

API Access Token [redacted]

Setup

Sign-in page URL

https://adsso.circlesecurity.ai/Auth/Login[redacted]

Sign-out page URL

https://adsso.circlesecurity.ai/Auth/Logout

You'll need this Certificate to setup an IdP for IAM services (e.g. Google)

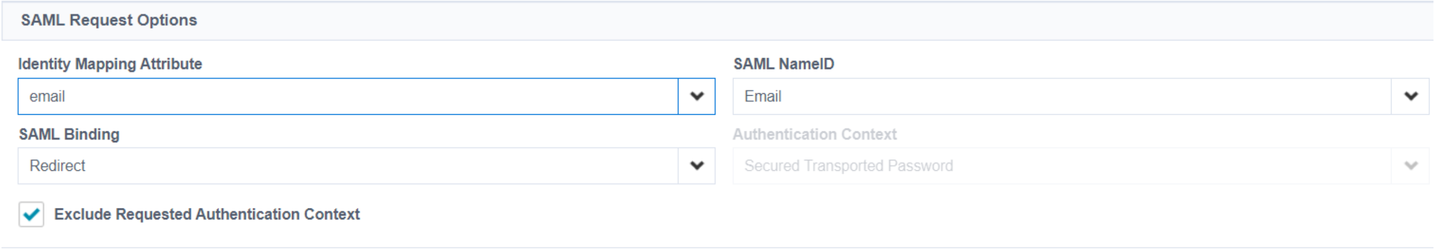
First let's configure the provider settings, as a reference you can take a look at the highlighted fields in the above image. The first is your sailpoint tenant website and the second is your circle tenant from step 3.

- Entity ID - Paste the app key shown in Step 3 and he

- Login URL for Post/Redirect - Both values will be the same like this https://adsso.circlesecurity.ai/Auth/Login/YourAppKeyHere You can also copy this from SAML Details page in circle sso tenant
- we will select whether to use Redirect/Post in the next step.

(not recommended) **Optionally you can enable Bypass Identity Provider if you want to ALLOW users to login with sailpoint's inherent username password login.(Admins can bypass using ?prompt=true query param irrespective)**

Next we will configure SAML Request Options



SAML Request Options

Identity Mapping Attribute: email

SAML NameID: Email

SAML Binding: Redirect

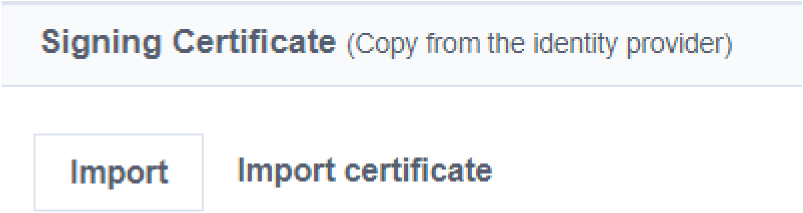
Authentication Context: Secured Transported Password

☑ Exclude Requested Authentication Context

This is the exact configuration you need to use so make sure all fields match the same.

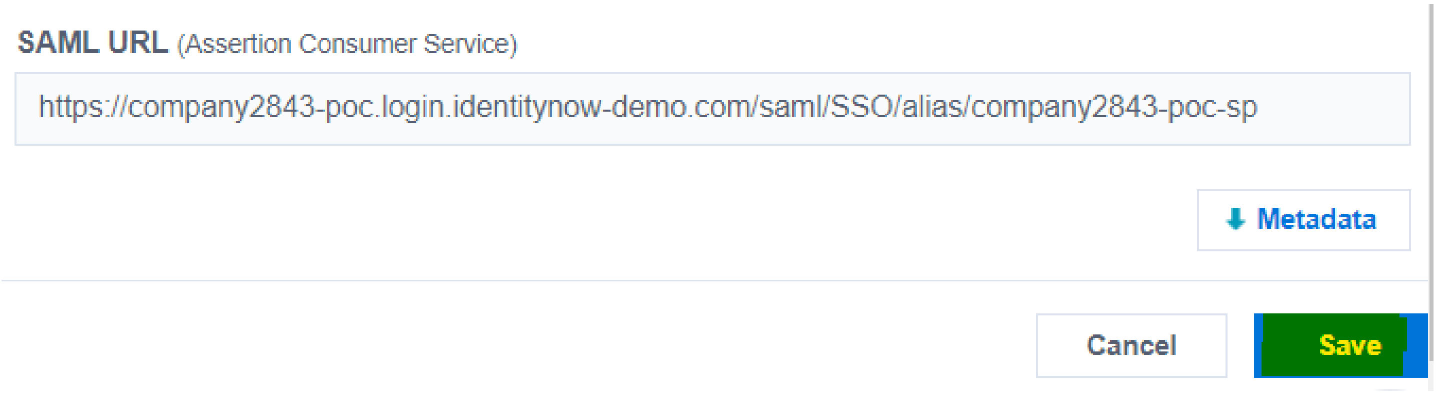
Note: Identity Mapping Attribute is what sailpoint uses to identify a user, we use Email SAML NameID attribute to authenticate the user so if your user groups have emails mapped to a different attribute then you can use that.

The next step is just uploading the public key we downloaded previously at the end of step 2a



Signing Certificate (Copy from the identity provider)

Finally DO NOT FORGET to click on **SAVE.**



SAML URL (Assertion Consumer Service)

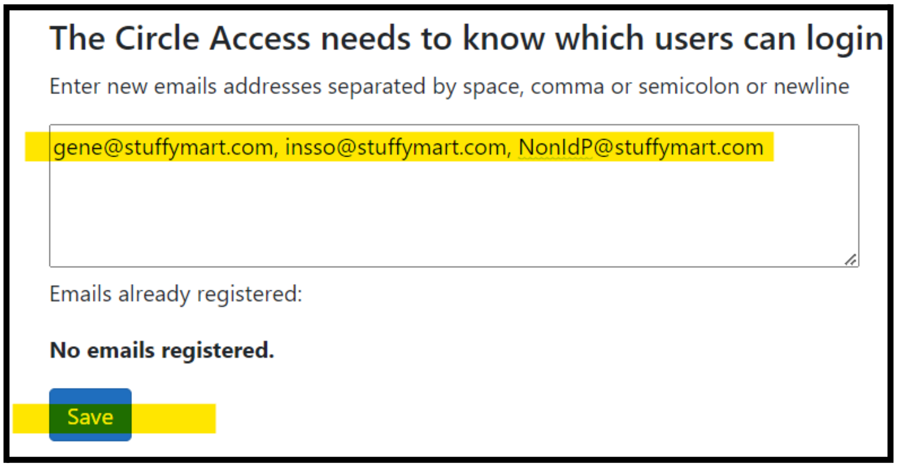
https://company2843-poc.login.identitynow-demo.com/saml/SSO/alias/company2843-poc-sp

Make sure you finish step 5 BEFORE trying to LOG IN.

Step 5. Adding emails to your Circle Access tenant

To enable Circle Access the email ids of the users should be added to the Tenant SAML page. SailPoint relies on email addresses to indicate identity. Enter them separated by comma and click the save button at the bottom.

Here's an example.



The Circle Access needs to know which users can login

Enter new emails addresses separated by space, comma or semicolon or newline

gene@stuffymart.com, insso@stuffymart.com, NonIdP@stuffymart.com

Emails already registered:

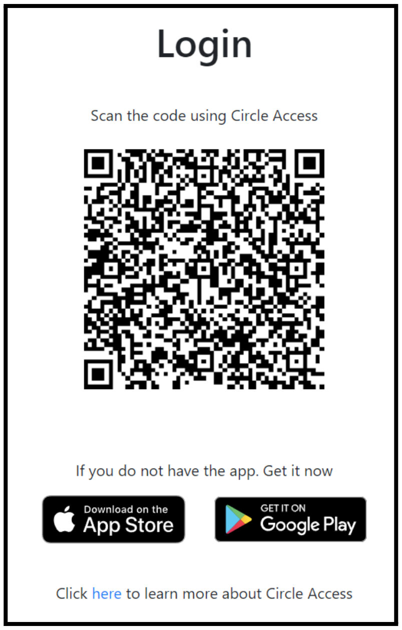
No emails registered.

Step 6. Let's give it a test

Note: Users will have to have configured Circle Access on their devices BEFORE you turn on Circle Access as the IdP otherwise they will not be able to access SailPoint.

Let's test the SSO flow now.

Open an Incognito window and navigate to your identity now domain eg: https://dummyTenant.identitynow.com and if you get redirected and see a nice pretty QR code, we set up the SSO correctly



Login

Scan the code using Circle Access

If you do not have the app. Get it now

Click here to learn more about Circle Access

.

If you scan this code with a device that has an email that was added in the previous step, you'll be logging in successfully.

Appendix

Adding another SSO administrator.

When your Circle Access tenant was created on the website, it was tied to the mobile device used to log in. If you want to add another user or device to this tenant, you can use the ‘Add New Administrator’ button on the main tenant list page.

Here are the steps:

1. Click the ‘Add New Administrator’ button
2. Read the short description and instructions and click the ‘Add New Administrator’ button
3. Scan the QR Code with the NEW device
4. All done.

You can now log into Circle Access Tenant (https://adsso.circlesecurity.ai) with the new device.