MobileIron Integration

AuthControl Sentry/Cloud to MobileIron

Integration Notes

Contents

Overview

Swivel Secure can provide strong and two factor authentication to the Mobile Iron. AuthControl Sentry is a linux based IdP for SAML federations. It is provided as on-prem or Cloud SaaS flavours, providing an adaptative authentication multifactor, managed by a system of points, depending on the factor used and the target app to access. This document outlines the details required to carry this out.

Prerequisites

Working MobileIron (MobileIron Sentry appliance) MobileIron Core 9.X and Connector 9.X AuthControl Sentry 4.x

How does it work

At App level we use conditional access to Cloud SaaS federated with SAMLv2. The Federated Identity works in 3-way trust with Access between Identity Provider (IDP), Service Provider (SP) and the Access provided by MobileIron AdminPortal/Access Gateway.

SwivelSecure Configuration

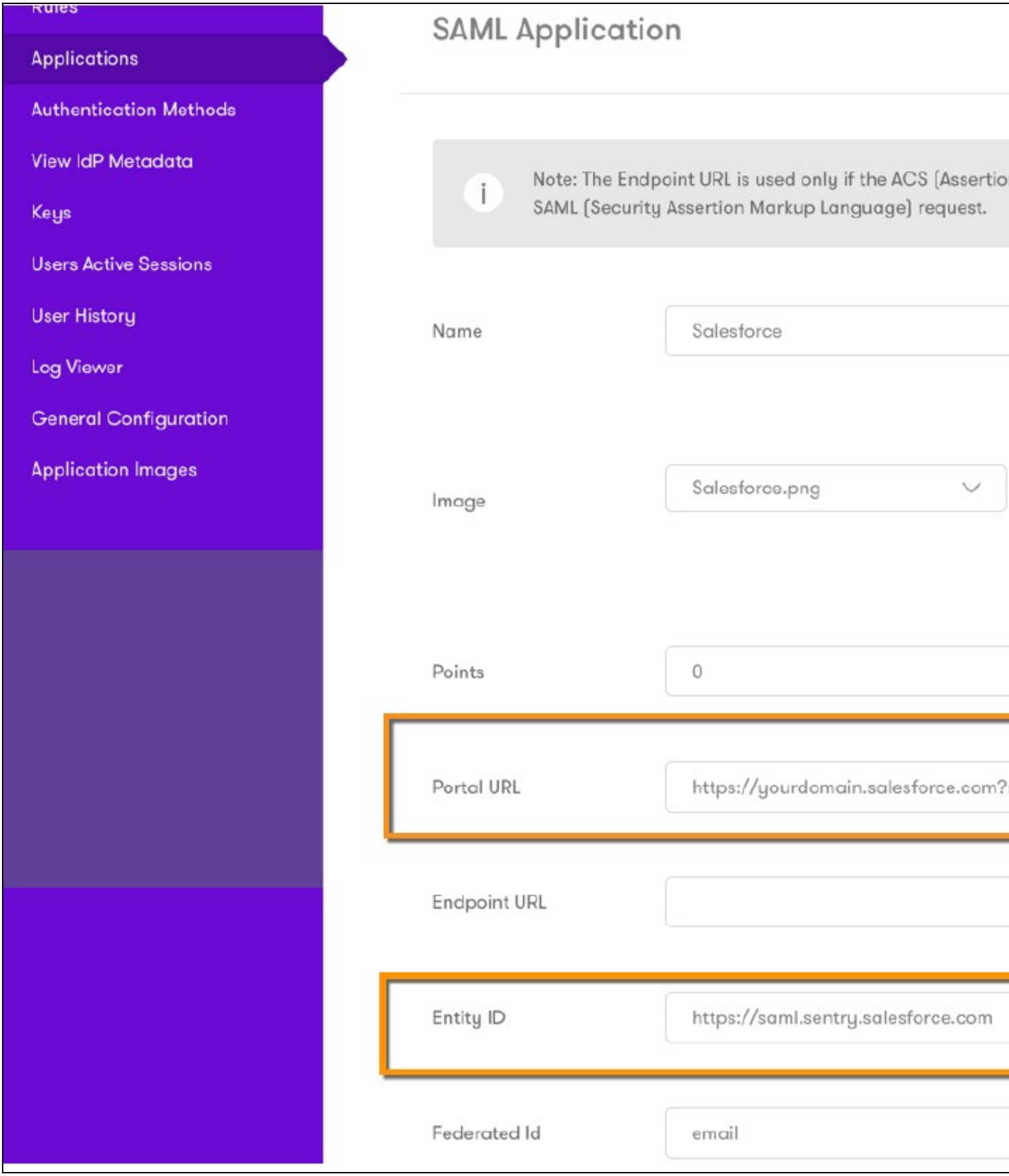
Enabling Standard Federation - Sales Force

The standard federation involves just this 3 fields:

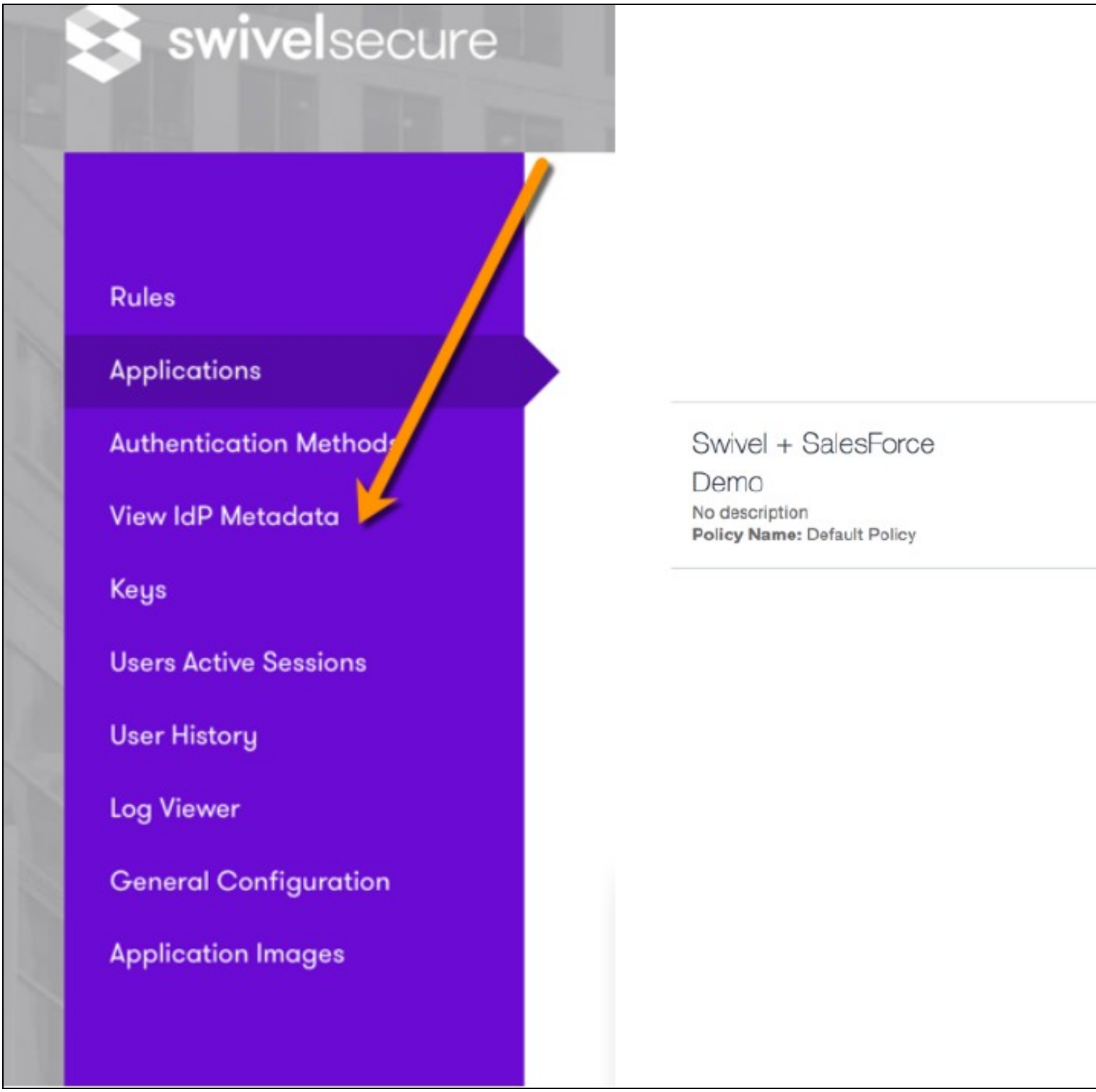
- Portal URL: (this Endpoint URL can be found on the Setup -> Security Controls -> Single Sign-On

Settings page in Salesforce.com, listed as ?Salesforce Login URL? under the Endpoints section. It is unique to your Salesforce.com instance and domain.

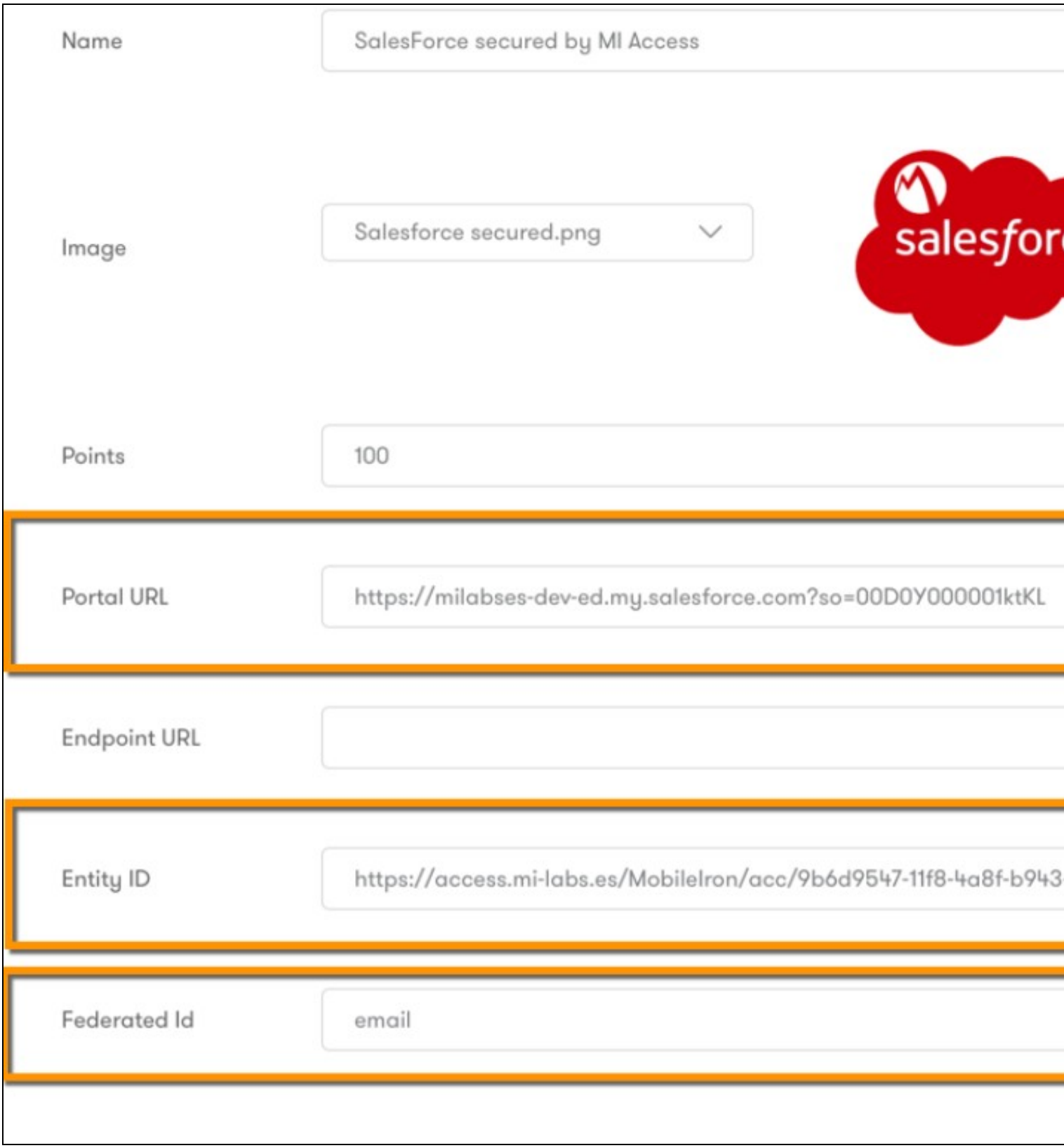
- Entity ID:, Reflected on SalesForce SSO configuration for My Domain
- Federeated id: That needs to match with the attributed defined on Salesforce.com and Swivel



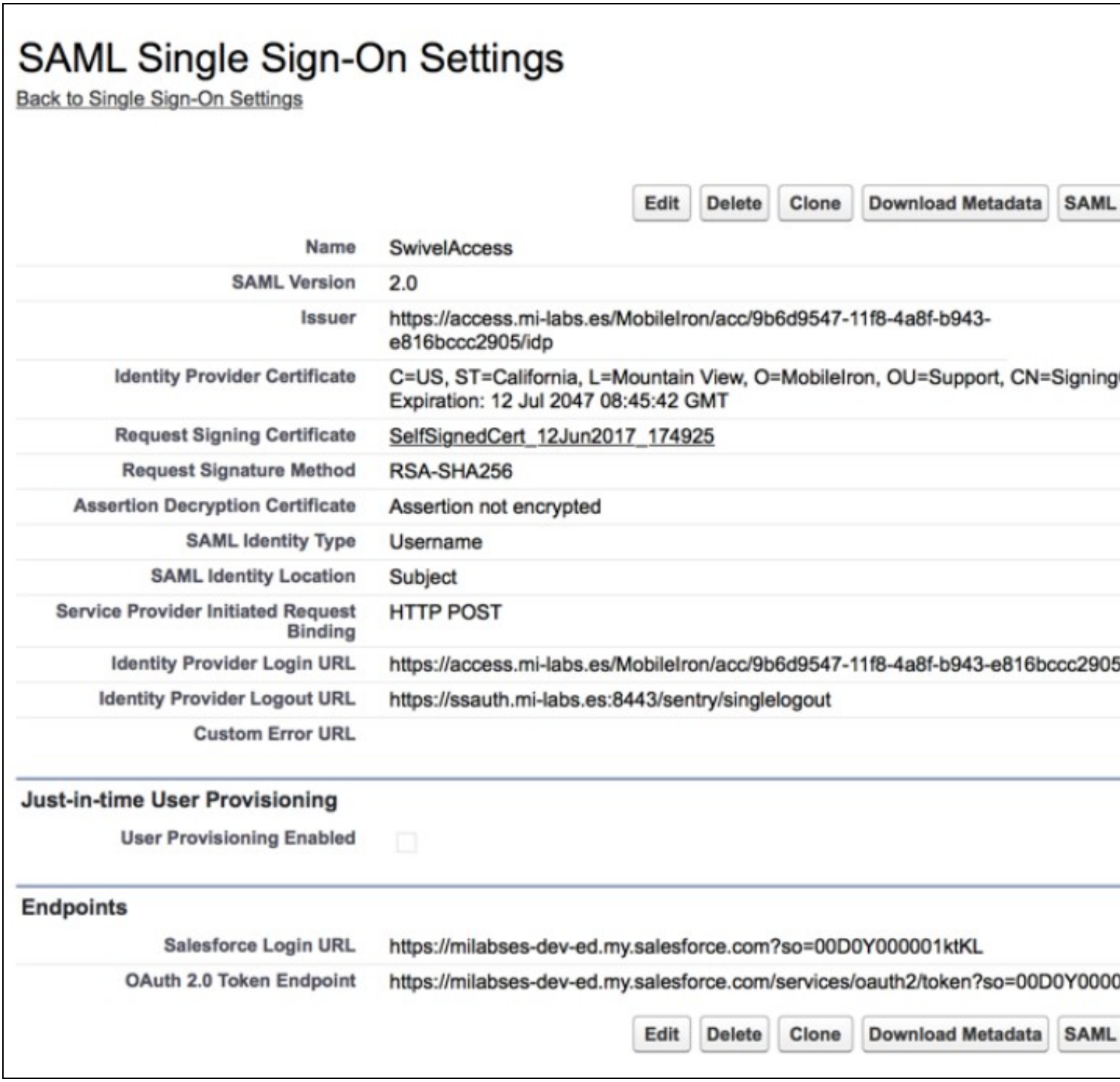
Once that we have a working federation from AuthControl Sentry and the SP, (in the example we will use SalesForce), this is just a standard SalesForce and Custom IdP federation on MI Access console, as the MFA part from Swivel will be triggered once the MI Access has approved the connection. AuthControl Sentry provides a metadata url to quickly get the XML from IdP. It uses POST method for federation.



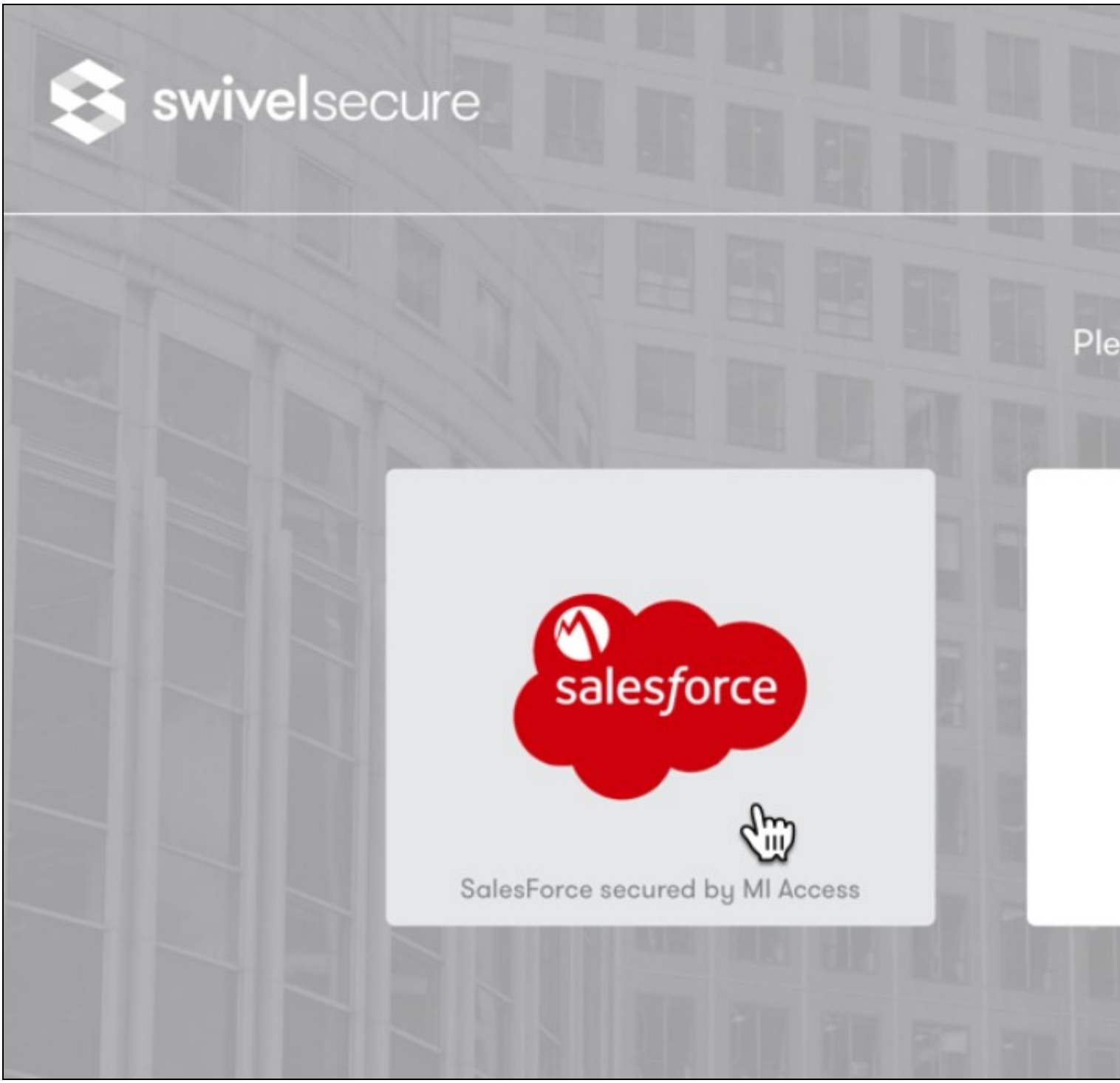
SAML Customization of Mobile Iron settings, Portal URL, Entity ID and Federated ID:



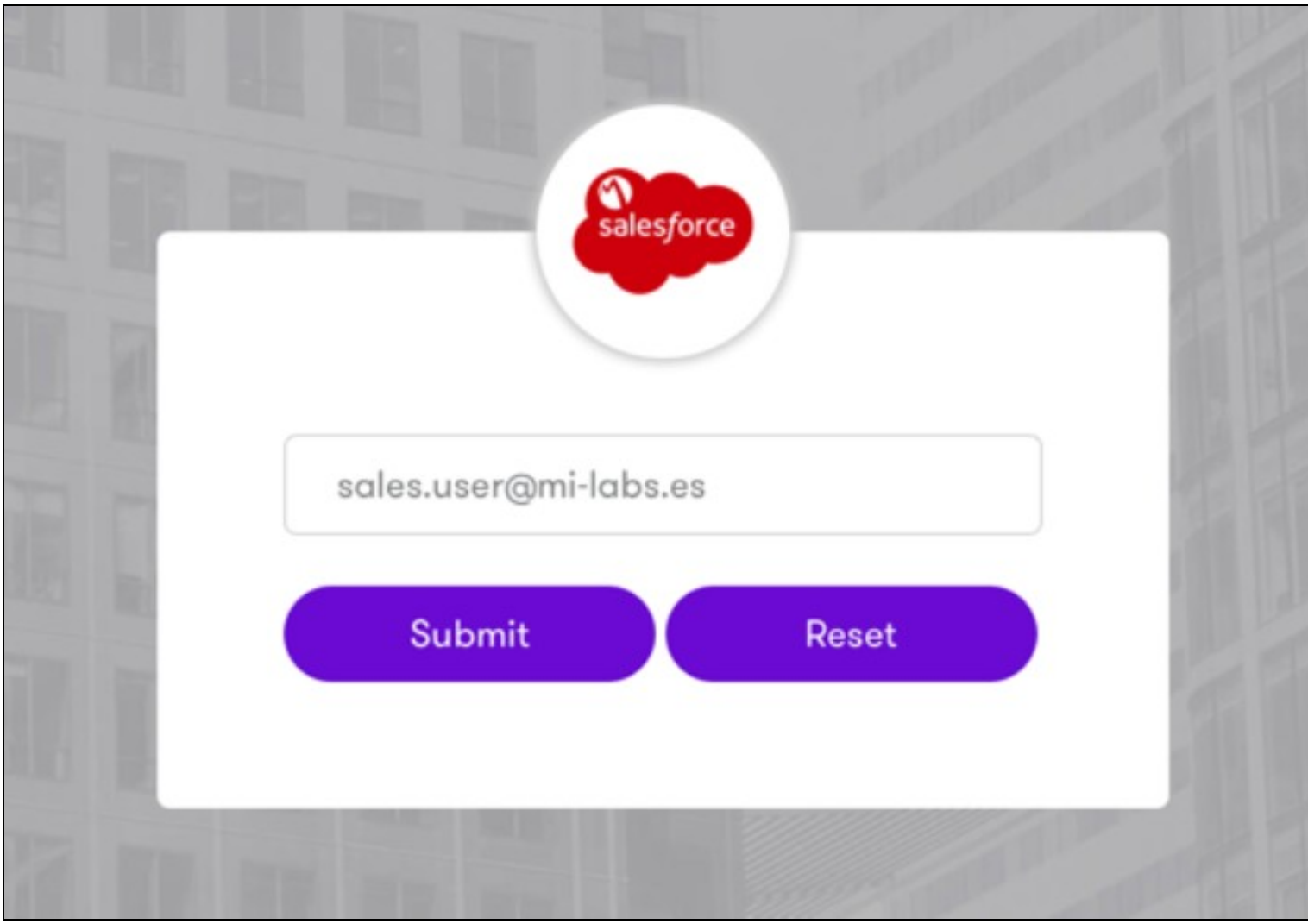
SAML Customization in the Sales Force Side. Settings for Mobile Iron.



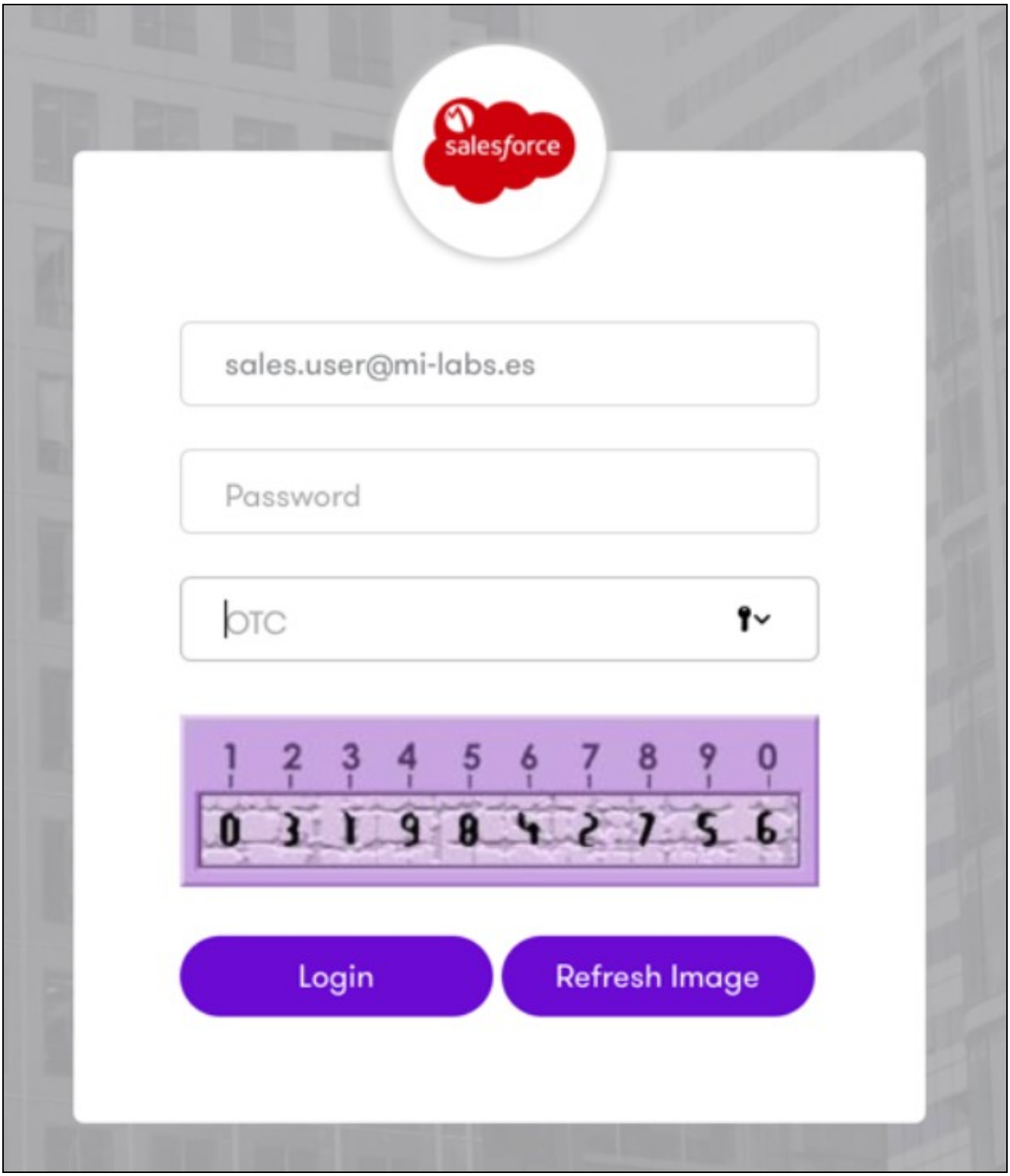
After the application settings definitions have been applied the aplications are available in AuthControl Sentry's web portal.



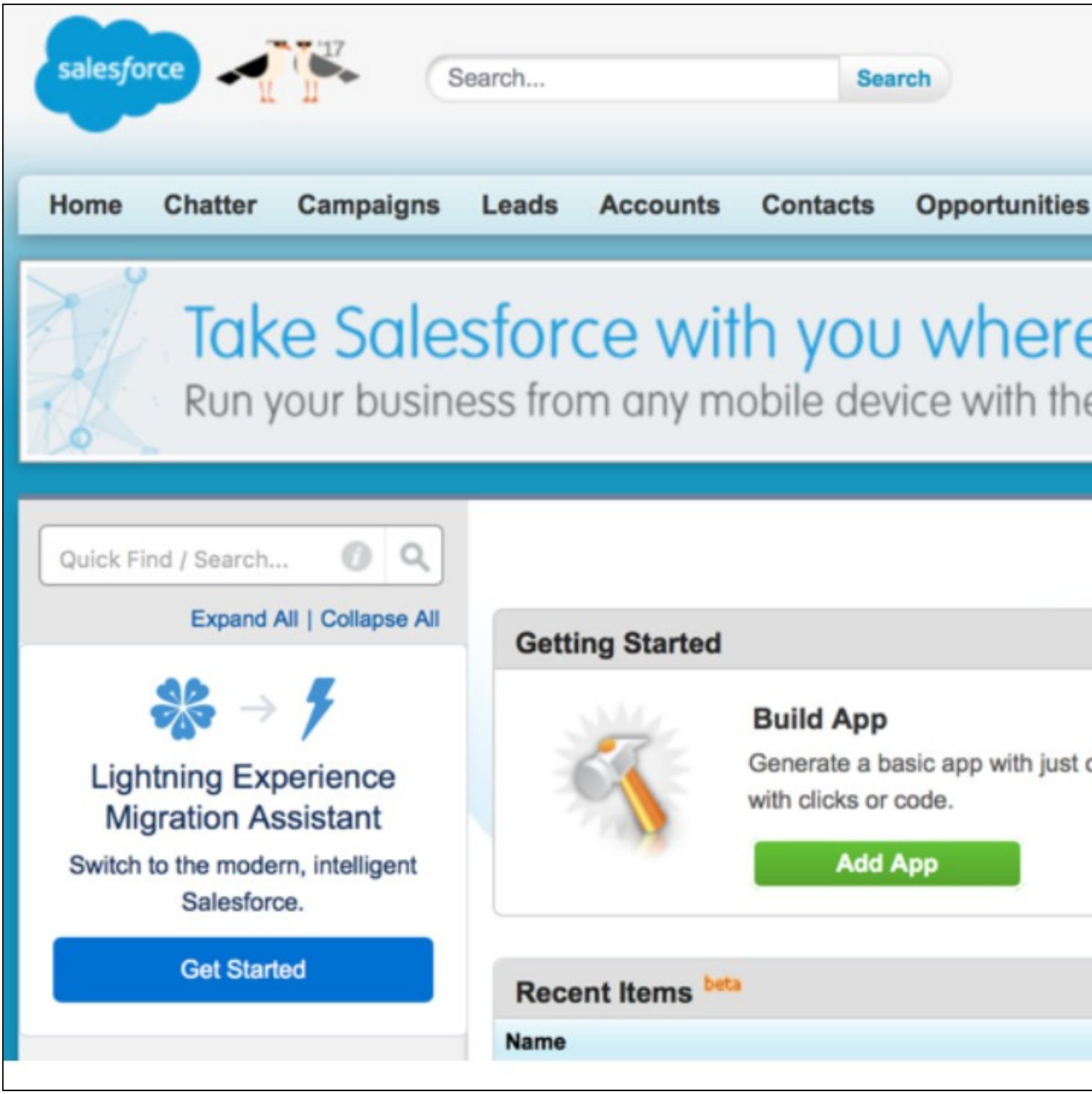
User Login in Authcontrol Sentry with SalesForce using the MI Account



SSO for SalesForce using Mobile Iron and Turing image from SwivelSecure. This means that the user logs in using the Swivel Secure credentials, by the selected method (in this case Turing image) into the Sales Force (without the need of using Sales Force Credentials).

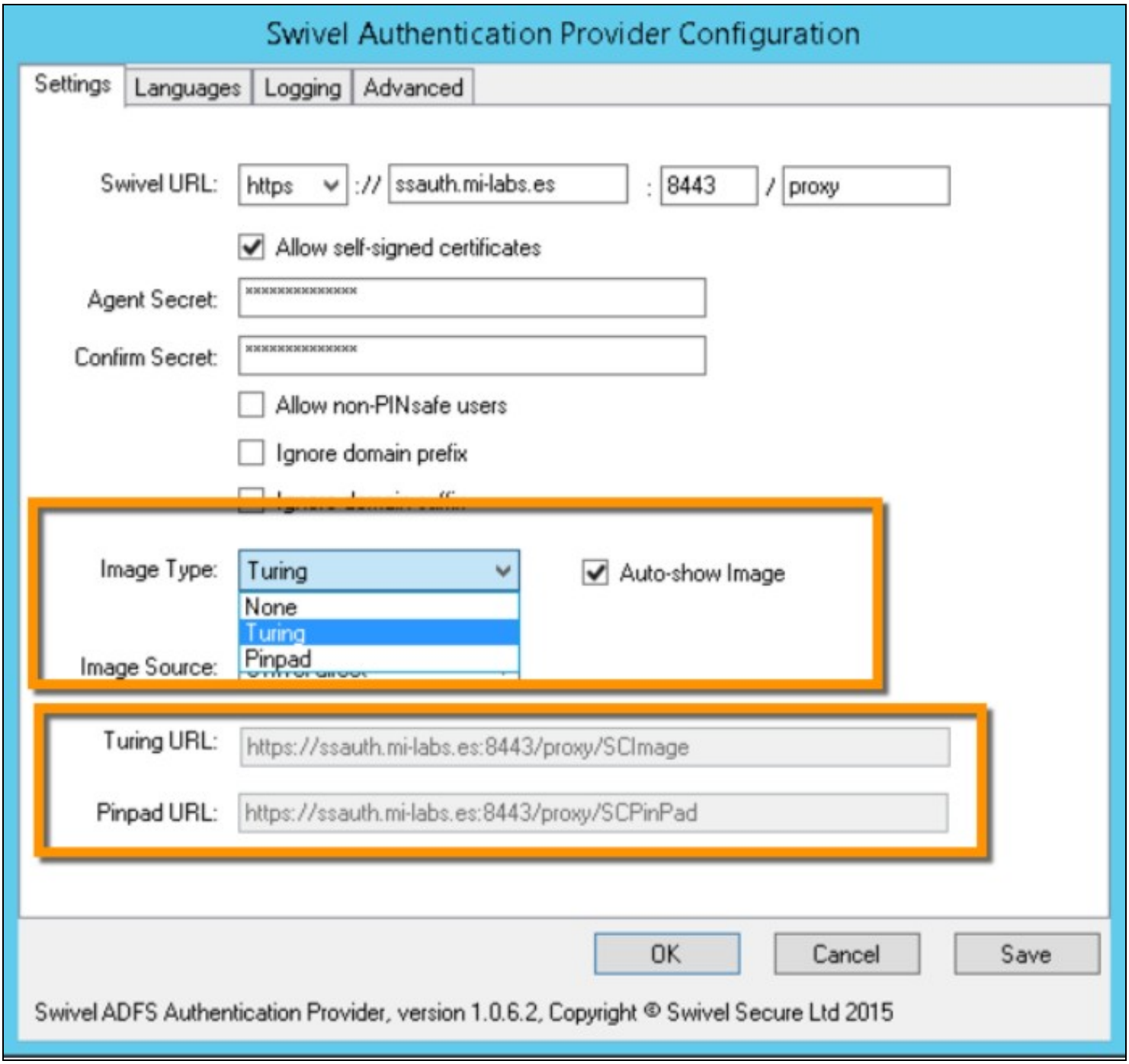


Successfull login in Sales Force.



Enabling Standard Federation - Office 365

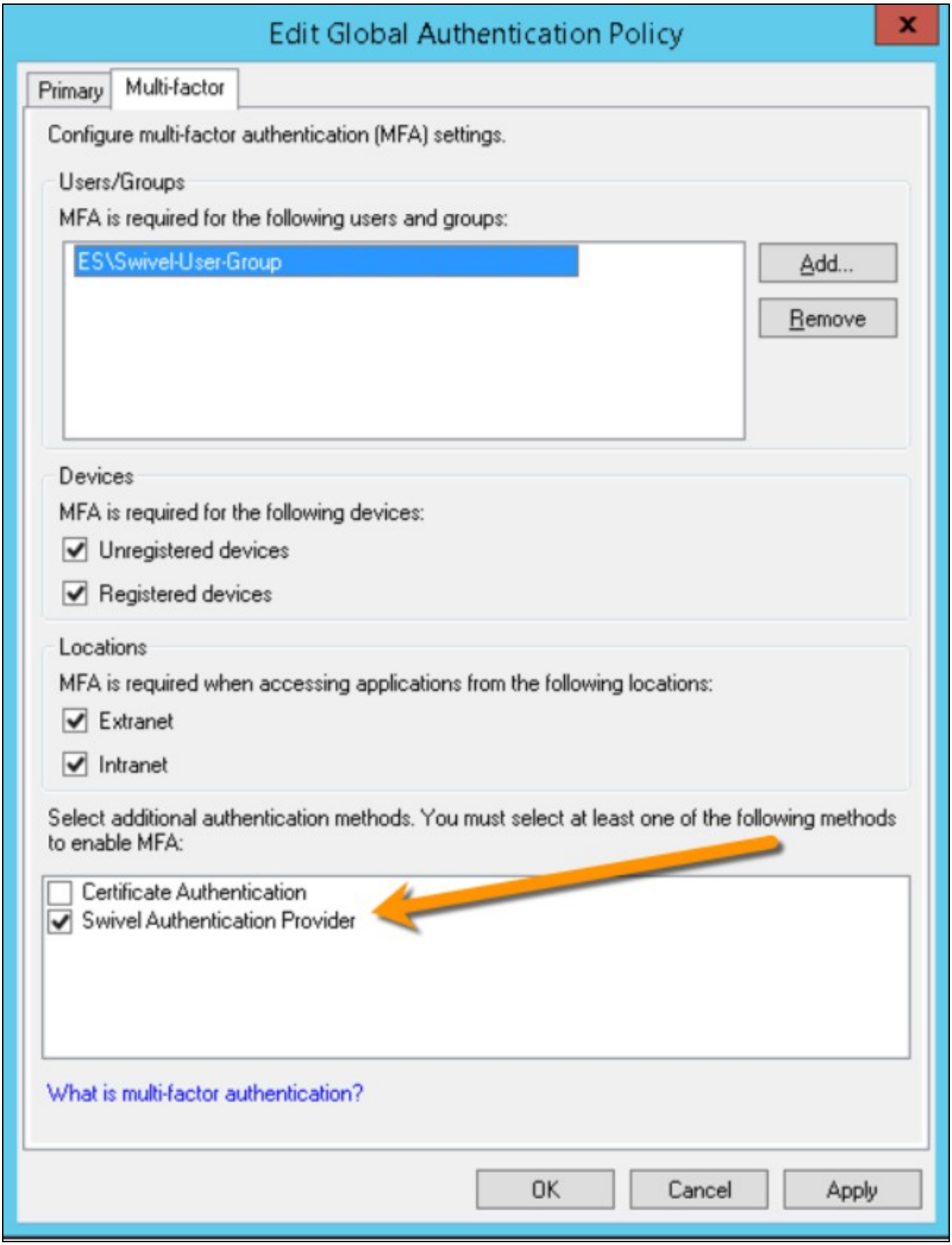
In the case of Office365, AuthControl requires that the main federation must be performed with ADFS. On a working federation, a complement has to be installed on ADFS 3.0 server.



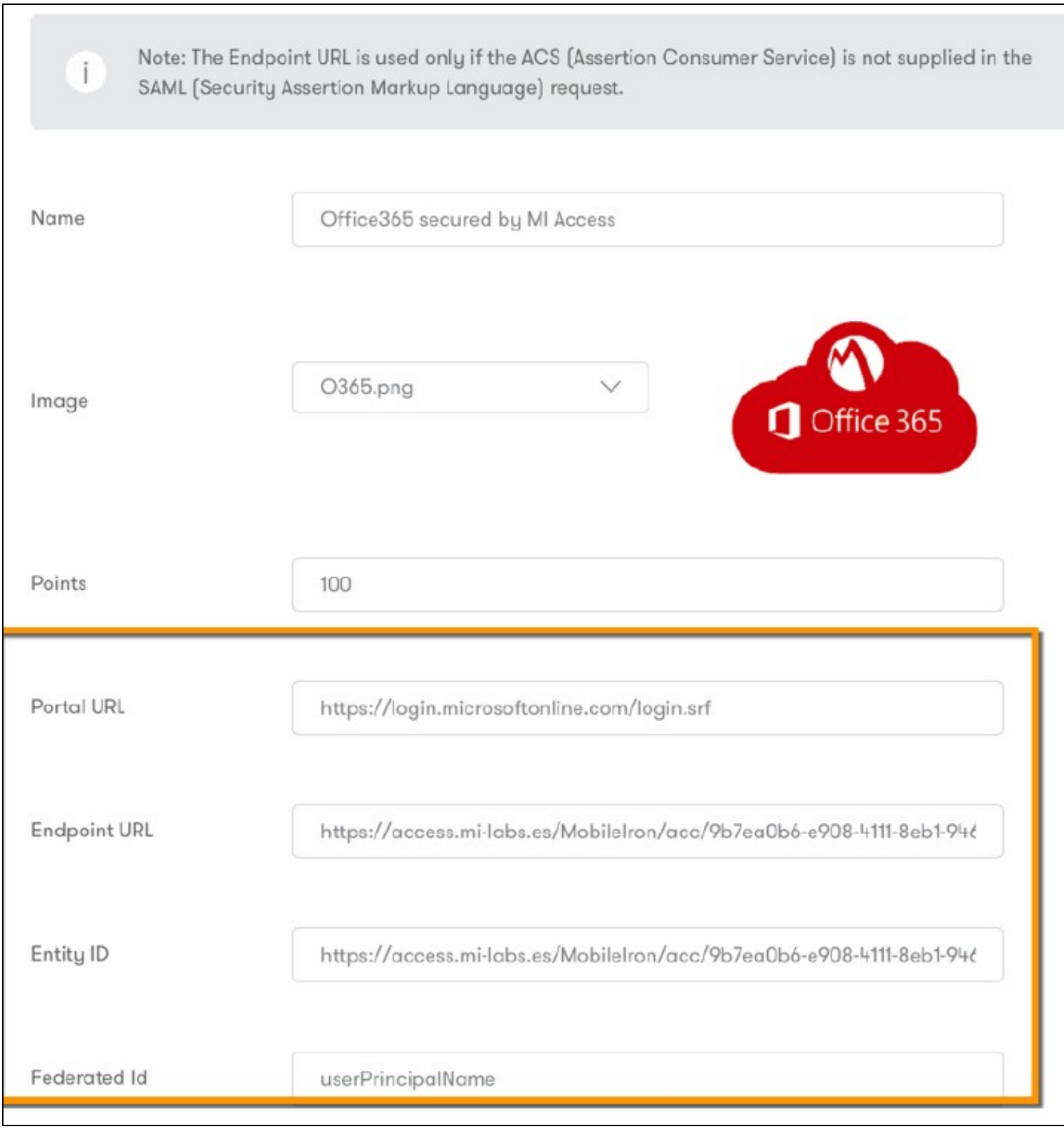
There?s a couple of choices depending if the customer is using ADFS Proxy servers or not.

This plugin installs Swivel Secure product as an MFA to be applied via ADFS Authentication Policy Settings.

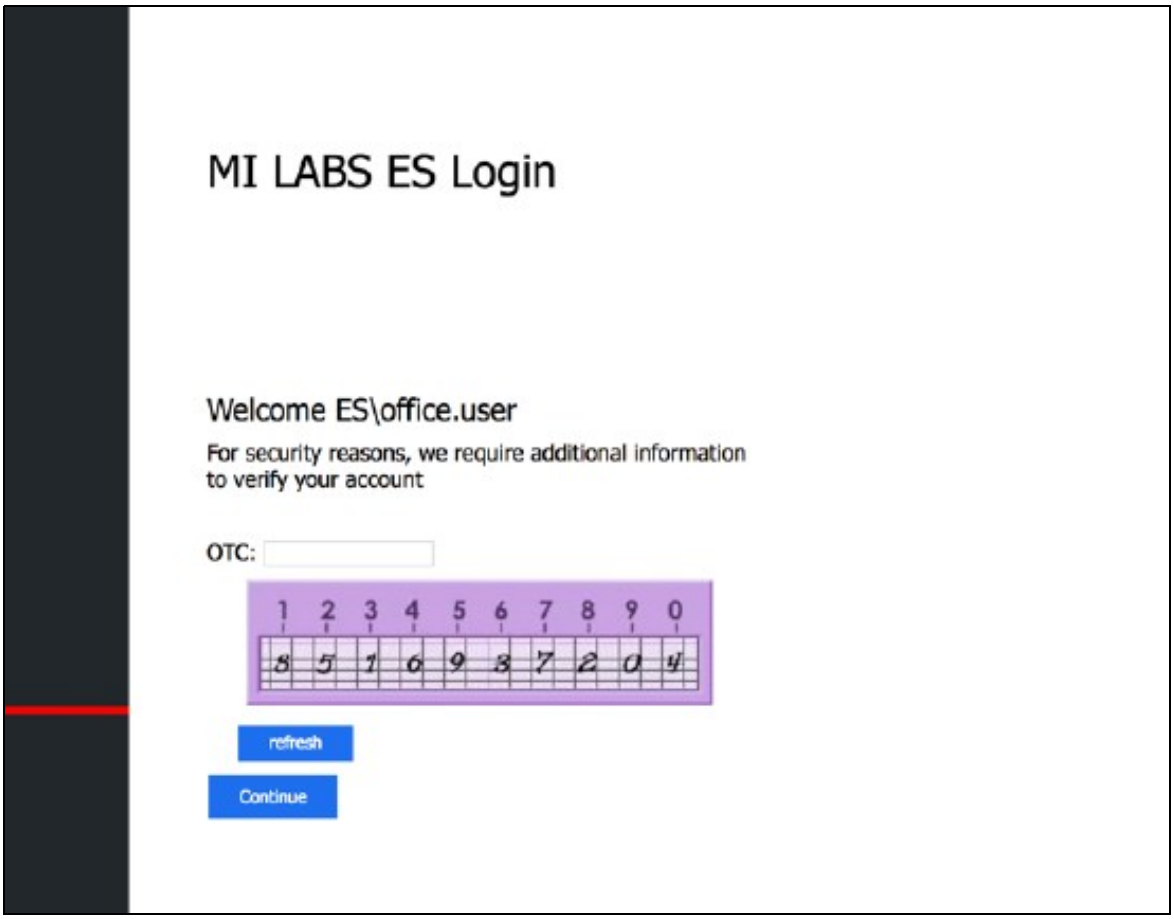
Set AuthControl Sentry / Swivel Secure as Authentication Provider



On AuthControl Sentry side, we will create an Application configuration with MI Access, IdP and Office365 endpoints:



This way, ADFS will require PINPAD or Turing image in order to validate and access Office365, in addition to ADFS primary authentication policy.



Related Articles

- ADFS configuration

https://kb.swivelsecure.com/w/index.php/Microsoft_ADFS_3_Authentication

Additional Information

For assistance in the Swivel Secure installation and configuration please firstly contact your reseller and then email Swivel Secure support at supportdesk@swivelsecure.com