

MobileIron Integration

AuthControl Sentry/Cloud to MobileIron

Integration Notes

Contents

- 1 Overview
- 2 Prerequisites
- 3 How does it work
- 4 SwivelSecure Configuration
 - ◆ 4.1 Enabling Standard Federation - Sales Force
 - ◆ 4.2 Enabling Standard Federation - Office 365
- 5 Related Articles
- 6 Additional Information

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

- Rules
- Applications**
- Authentication Methods
- View IdP Metadata
- Keys
- Users Active Sessions
- User History
- Log Viewer
- General Configuration
- Application Images

SAML Application



Note: The Endpoint URL is used only if the ACS (Assertion SAML [Security Assertion Markup Language] request.

Name

Salesforce

Image

Salesforce.png

Points

0

Portal URL

https://yourdomain.salesforce.com?

Endpoint URL

Entity ID

https://saml.sentry.salesforce.com

Federated Id

email

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.

Rules

Applications

Authentication Methods

View IdP Metadata

Keys

Users Active Sessions

User History

Log Viewer

General Configuration


Application Images

Swivel + Salesforce

Demo

No description

Policy Name: Default Policy

Name	SalesForce secured by MI Access
Image	Salesforce secured.png 
Points	100
Portal URL	https://milabses-dev-ed.my.salesforce.com?so=00D0Y000001ktKL
Endpoint URL	
Entity ID	https://access.mi-labs.es/MobileIron/acc/9b6d9547-11f8-4a8f-b943
Federated Id	email

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

SAML Single Sign-On Settings

[Back to Single Sign-On Settings](#)

[Edit](#) [Delete](#) [Clone](#) [Download Metadata](#) [SAML](#)

Name	SwivelAccess
SAML Version	2.0
Issuer	https://access.mi-labs.es/MobileIron/acc/9b6d9547-11f8-4a8f-b943-e816bccc2905/idp
Identity Provider Certificate	C=US, ST=California, L=Mountain View, O=MobileIron, OU=Support, CN=Signing Expiration: 12 Jul 2047 08:45:42 GMT
Request Signing Certificate	SelfSignedCert_12Jun2017_174925
Request Signature Method	RSA-SHA256
Assertion Decryption Certificate	Assertion not encrypted
SAML Identity Type	Username
SAML Identity Location	Subject
Service Provider Initiated Request Binding	HTTP POST
Identity Provider Login URL	https://access.mi-labs.es/MobileIron/acc/9b6d9547-11f8-4a8f-b943-e816bccc2905
Identity Provider Logout URL	https://ssauth.mi-labs.es:8443/sentry/singlelogout
Custom Error URL	

Just-in-time User Provisioning

User Provisioning Enabled

Endpoints

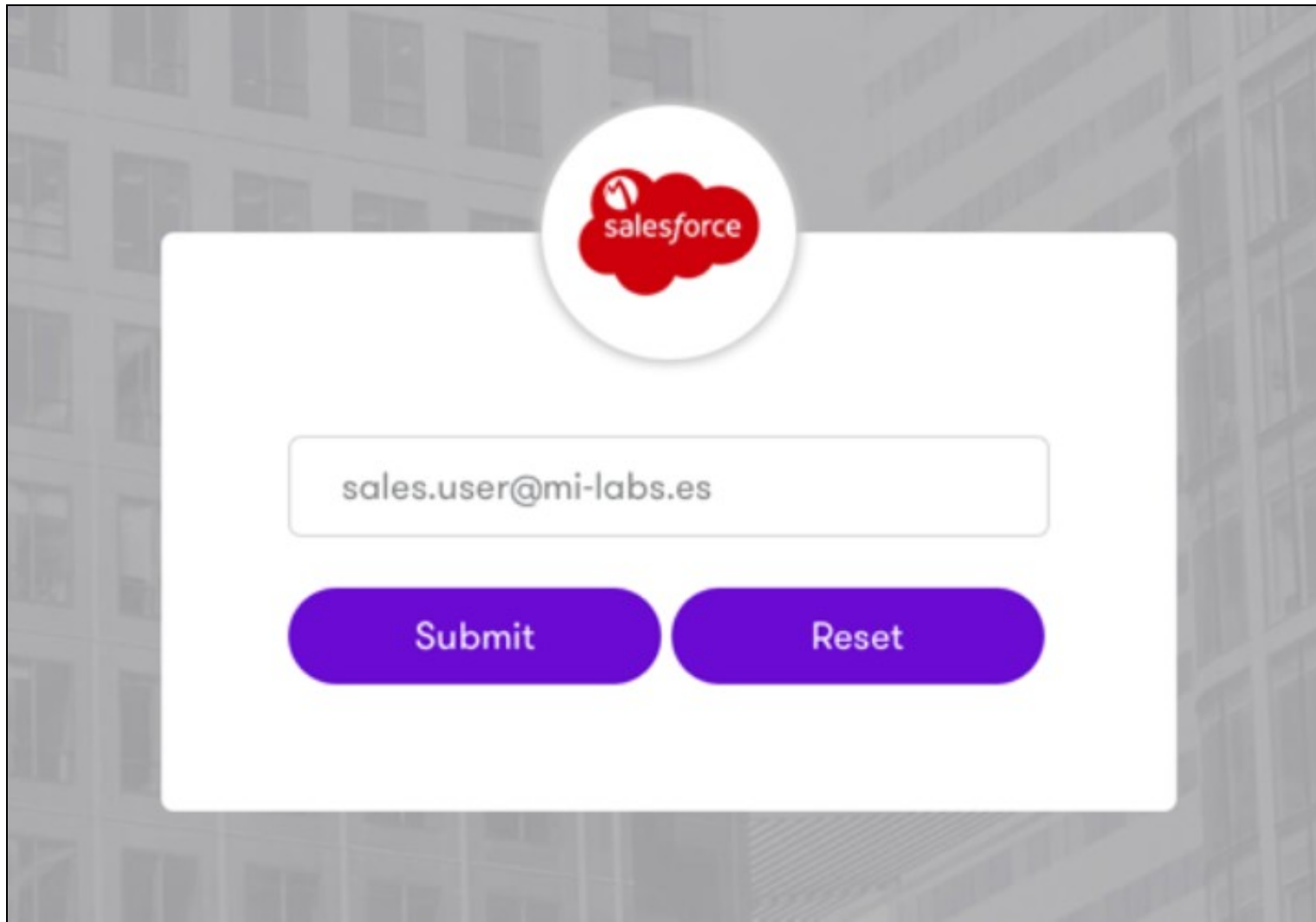
Salesforce Login URL	https://milabses-dev-ed.my.salesforce.com?so=00D0Y000001ktKL
OAuth 2.0 Token Endpoint	https://milabses-dev-ed.my.salesforce.com/services/oauth2/token?so=00D0Y0000

[Edit](#) [Delete](#) [Clone](#) [Download Metadata](#) [SAML](#)

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



SalesForce secured by MI Access



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).



sales.user@mi-labs.es

Password

l0TC 



Login

Refresh Image

Successfull login in Sales Force.

 [Search](#)

[Home](#) [Chatter](#) [Campaigns](#) [Leads](#) [Accounts](#) [Contacts](#) [Opportunities](#)



Take Salesforce with you where

Run your business from any mobile device with the

 [i](#) [Q](#)

[Expand All](#) | [Collapse All](#)



Lightning Experience Migration Assistant

Switch to the modern, intelligent Salesforce.

[Get Started](#)

Getting Started



Build App

Generate a basic app with just clicks or code.

[Add App](#)

Recent Items beta

Name

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.

Swivel Authentication Provider Configuration

Settings Languages Logging Advanced

Swivel URL: :// : /

Allow self-signed certificates

Agent Secret:

Confirm Secret:

Allow non-PINsafe users

Ignore domain prefix

Image Type: Auto-show Image

Image Source:

Turing URL:

Pinpad URL:

OK

Cancel

Save

Swivel ADFS Authentication Provider, version 1.0.6.2, Copyright © Swivel Secure Ltd 2015

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

Edit Global Authentication Policy

Primary Multi-factor

Configure multi-factor authentication (MFA) settings.

Users/Groups

MFA is required for the following users and groups:

- ES\Swivel-User-Group

Add...
Remove

Devices

MFA is required for the following devices:

- Unregistered devices
- Registered devices

Locations

MFA is required when accessing applications from the following locations:

- Extranet
- Intranet

Select additional authentication methods. You must select at least one of the following methods to enable MFA:

- Certificate Authentication
- Swivel Authentication Provider

[What is multi-factor authentication?](#)

OK Cancel Apply

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



Note: The Endpoint URL is used only if the ACS (Assertion Consumer Service) is not supplied in the SAML (Security Assertion Markup Language) request.

Name

Office365 secured by MI Access

Image

O365.png



Points

100

Portal URL

<https://login.microsoftonline.com/login.srf>

Endpoint URL

<https://access.mi-labs.es/MobileIron/acc/9b7ea0b6-e908-4111-8eb1-94c>

Entity ID

<https://access.mi-labs.es/MobileIron/acc/9b7ea0b6-e908-4111-8eb1-94c>

Federated Id

userPrincipalName

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

MI LABS ES Login

Welcome ES\office.user

For security reasons, we require additional information to verify your account

OTC:

1	2	3	4	5	6	7	8	9	0
8	5	1	0	9	3	7	2	0	4

refresh

Continue

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