Sentry SSO with Thycotic Secret Server

Contents

Introduction

This document describes how to configure Thycotic Secret Server to work with AuthControl Sentry SSO. Before following these instructions, you should be familiar with using Sentry - see the Sentry User Guide for more information.

Also refer to the official Thycotic SAML integration guide for Secret Server version 10.5+:
https://thycotic.force.com/support/s/article/SS-SAML-Config-Guide

Setup AuthControl Sentry Keys

Before you are able to create a SAML configuration in Thycotic Secret Server, you will need to setup some Keys. Please see a separate article: HowToCreateKeysOnCmi. You will need the certificate you generate in a later section of this article. This can be retrieved from the View Keys menu option of Swivel AuthControl Sentry.

Convert Sentry Keys to PFX

You will need to retrieve the keys generated above from the /home/swivel/.swivel/sentry/keys folder so that you are able to convert from PEM format to a PFX file containing the private key.

The openssl command to achieve a PEM to PFX conversion is as follows:

```
openssl pkcs12 -export -out Cert.pfx -in cert.pem -inkey key.pem
```

You will be prompted for a password for the private key and a password for the PFX you are creating This command assumes:

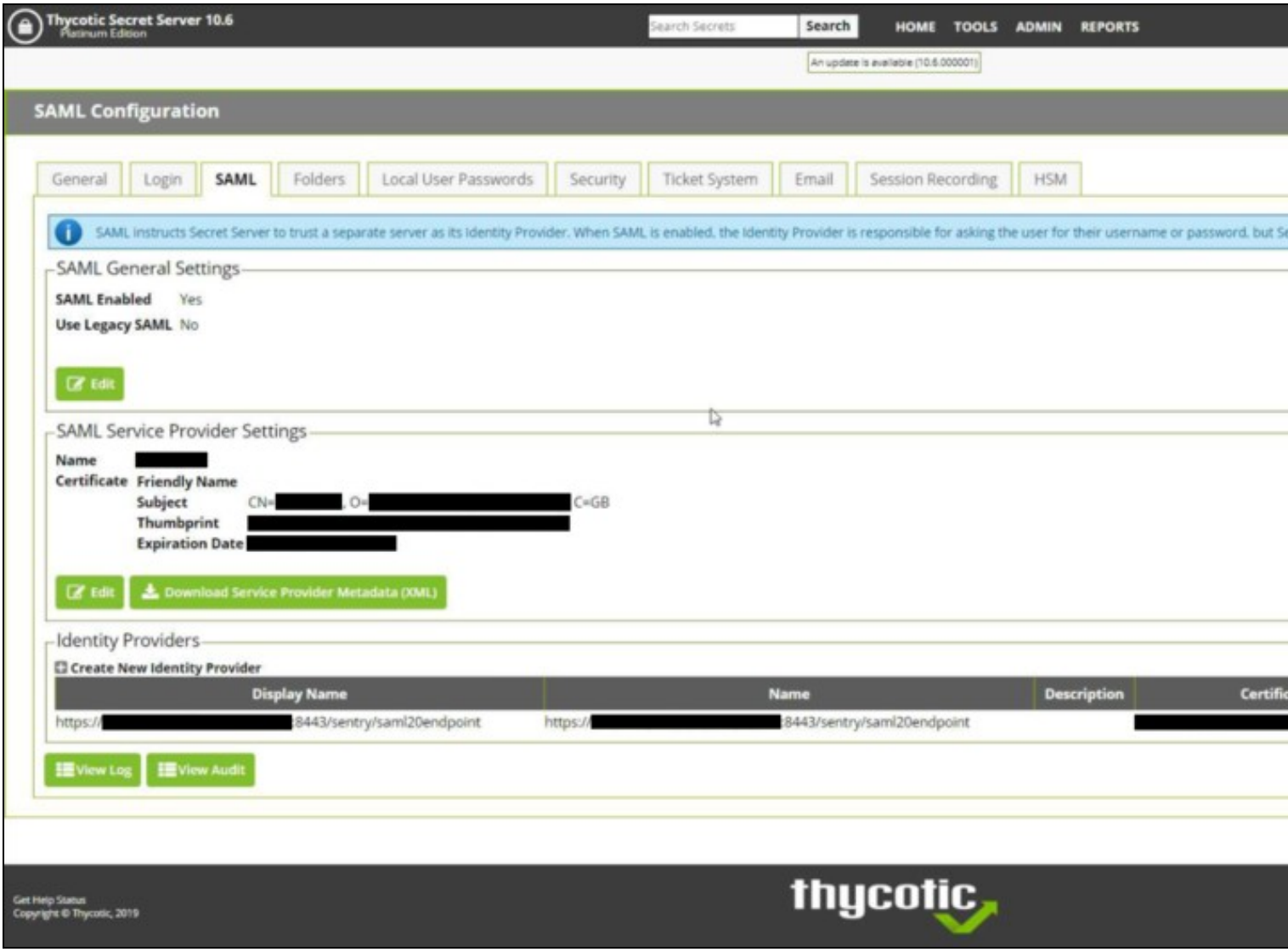
- Cert.pfx is the file being created
- cert.pem is the cert file downloadable from the AuthControl keys GUI
- key.pem is the private key you download from the /home/swivel/.swivel/sentry/keys folder using WinSCP

Download the Sentry SSO IdP metadata

In the Sentry SSO Web GUI (running on port 8443), right click on the 'View IdP Metadata' left hand menu option and 'Save As' an xml file e.g. SwivelIdPMetadata.xml. We will upload this to the Thycotic Secret Server in a moment.

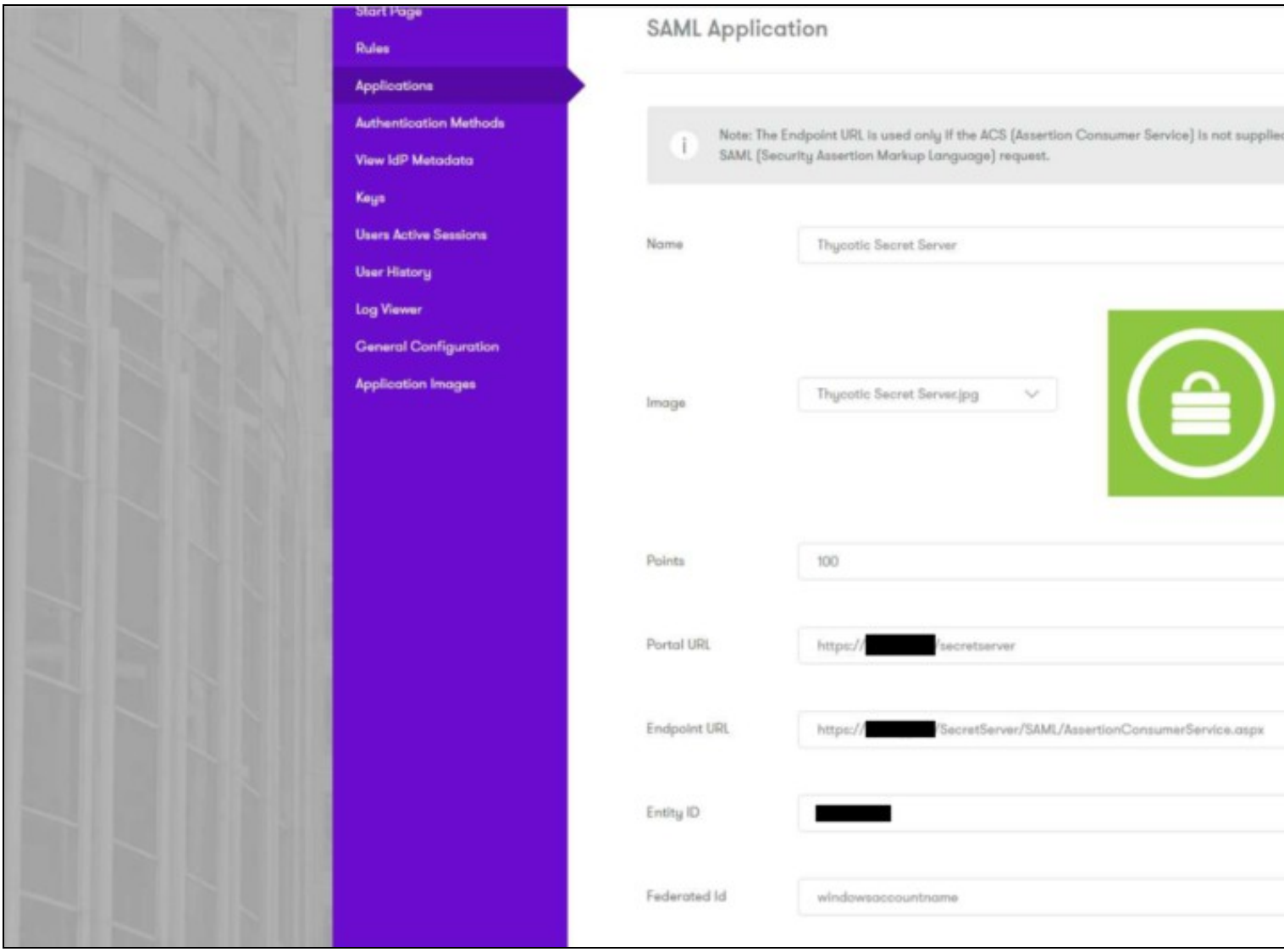
Setup SAML on Thycotic Secret Server

Login to Thycotic Secret Server as an administrator. You should see a SAML tab where you can perform the SAML configuration:



- Enable SAML by checking the checkbox. Note: it's worth noting that there is a URL to facilitate a local login in the event that SAML is not configured correctly. We recommend you read the Thycotic user manual to have this as a backup option prior to your SAML implementation attempt.
- Under SAML -> Service Provider settings, select a certificate and browse to the PFX certificate created earlier.
- Under Identity Providers, select 'Create New Identity Provider'. This is where you will upload the IdP metadata file from earlier (e.g. SwivelIdPMetadata.xml that you saved from the 'View IdP Metadata' menu option in the Sentry SSO Web GUI). This should import successfully and populate all the endpoint URLs. The FQDN of these URLs should be valid. If not, login to the Swivel Secure CMI -> Main Menu -> Appliance -> Sentry and set the Base URL to be correct. Then export the IdP metadata again and repeat these steps to attempt to create a new identity provider.
- Download the Service Provider metadata and open this in a text editor such as Notepad. Locate the entityID. This will be used in the Sentry SSO Application definition in a moment.

Setup Thycotic Secret Server as a Sentry SSO Application definition



In the Sentry SSO Web GUI (running on port 8443):

- Locate a Thycotic logo online and upload this via the Application Images option
- Create a new Application definition using the SAML -> Other option
    - Name: Thycotic Secret Server
    - Image: (select the image you just uploaded)
    - Points: 100 - or whatever fits your risk profile if you have already deployed Sentry session
    - Portal URL: https://<thycoticsecretserverhostname>/secretserver
    - Endpoint URL: https://<thycoticsecretserverhostname>/SecretServer/SAML/AssertionConsumerService.aspx
    - Entity ID: enter the EntityID you copied from the Service Provider metadata (just the value from the XML without quotes)
    - FederatedID: (this will vary according to your installation) windowsusername
        - windowsusername will need to be setup as a username attribute in the Sentry Core GUI running on port 8080 under Repository -> Attributes if it does not exist already. See section below.

Configure windowsusername attribute

In Swivel Core

Thycotic Secret Server requires the username to be in the format domain\username if integrated with AD. To do this, you need to create a Swivel attribute that includes the prefix.

In the Swivel admin console, under the repository details for the relevant AD repository, set the domain qualifier to be the short-form domain name, followed by "\" - don't forget the backslash at the end.

swivelsecure

- Status
- Log Viewer
- ⊞ Server
- ⊞ Policy
- ⊞ Logging
- ⊞ Transport
- ⊞ Database
- ⊞ Mode
- ⊟ Repository
  - Servers
  - Types
  - Groups
  - Attributes
  - Repos Admin
  - AD
- ⊞ RADIUS
- ⊞ Migration
- ⊞ Windows GINA
- ⊞ Appliance
- ⊞ OATH
- ⊞ Config Sync
- ⊞ Reporting
- User Administration
- Save Configuration
- Administration Guide
- Logout

Repository>AD

Please enter the details for accessing Active Directo

Hostname/IP:

Username:

Password:

Port:

Allow self-signed certificates:

Synchronization schedule:

Username attribute:

Mark missing users as deleted:

Initial PIN attribute:

Initial password attribute:

Import disabled users:

Import disabled state:

Ignore FQ name changes:

Reformat Phone Number:

Prefix to remove:

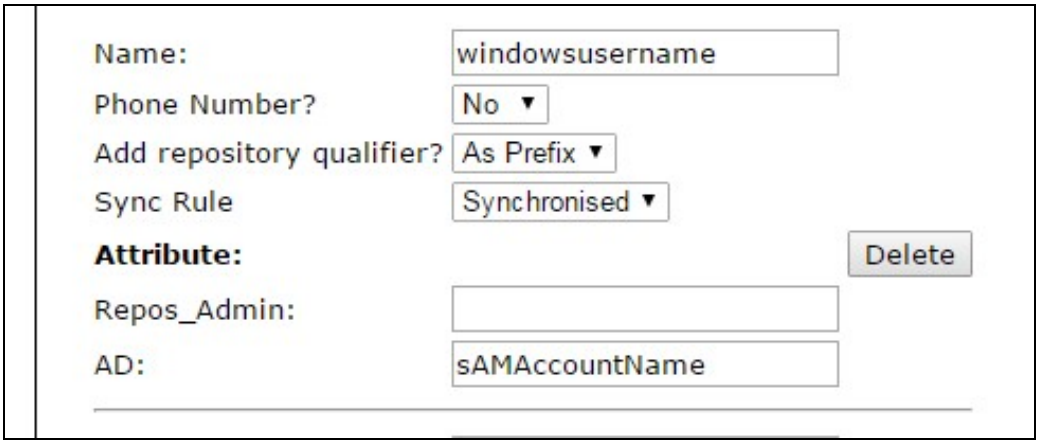
Prefix to add:

Add domain qualifier:

Repository Domain Qualifier:

Allow expired passwords:

Under Repository -> Attributes, create an attribute - for example, call it "windowsaccountname". In the definition for the AD repository, put the AD attribute name "sAMAccountName", and under domain qualifier, select "As Prefix".



Finally, synchronise the AD repository, to ensure that all users have an attribute in the form domain\username.

Click save. You will see something like the below. Click save again.

Login Example

As an example here we will be using OATH authentication as the Primary method required for Thycotic Secret Server authentication.

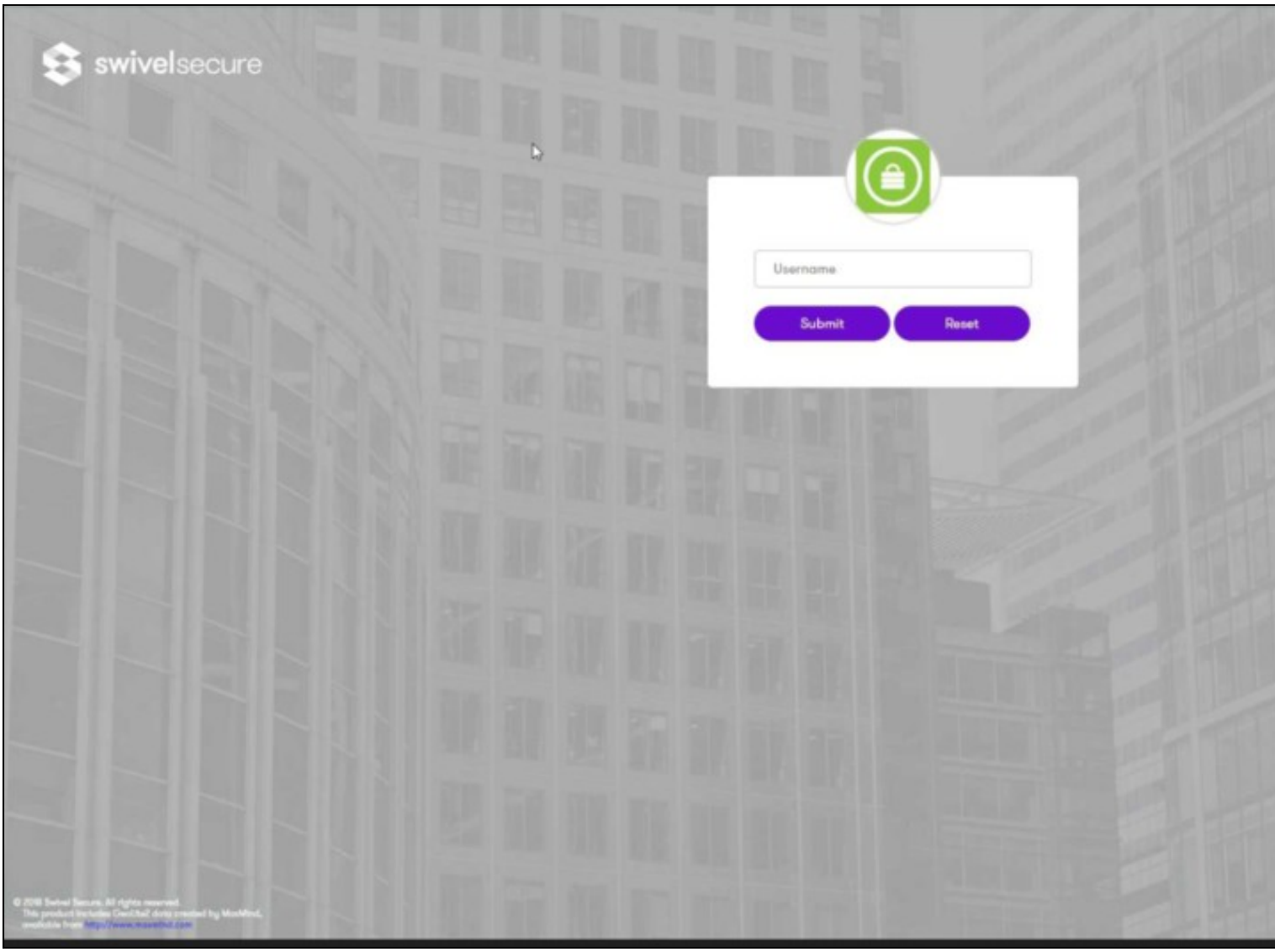
Login to the AuthControl Sentry Administration Console. Click Authentication Methods in the left hand menu. Click the Edit button against the OATH option in the list of Authentication Methods. Give this Authentication Method 100 points. This will mean that when a login attempt is made to the Thycotic Secret Server Application, this Authentication Method will be offered during login. (Please read about AuthControl Sentry Rules and familiarize your self with AuthControl Sentry here)

Testing authentication to Thycotic Secret Server via Swivel AuthControl Sentry

This should be the final step after all previous elements have been configured.

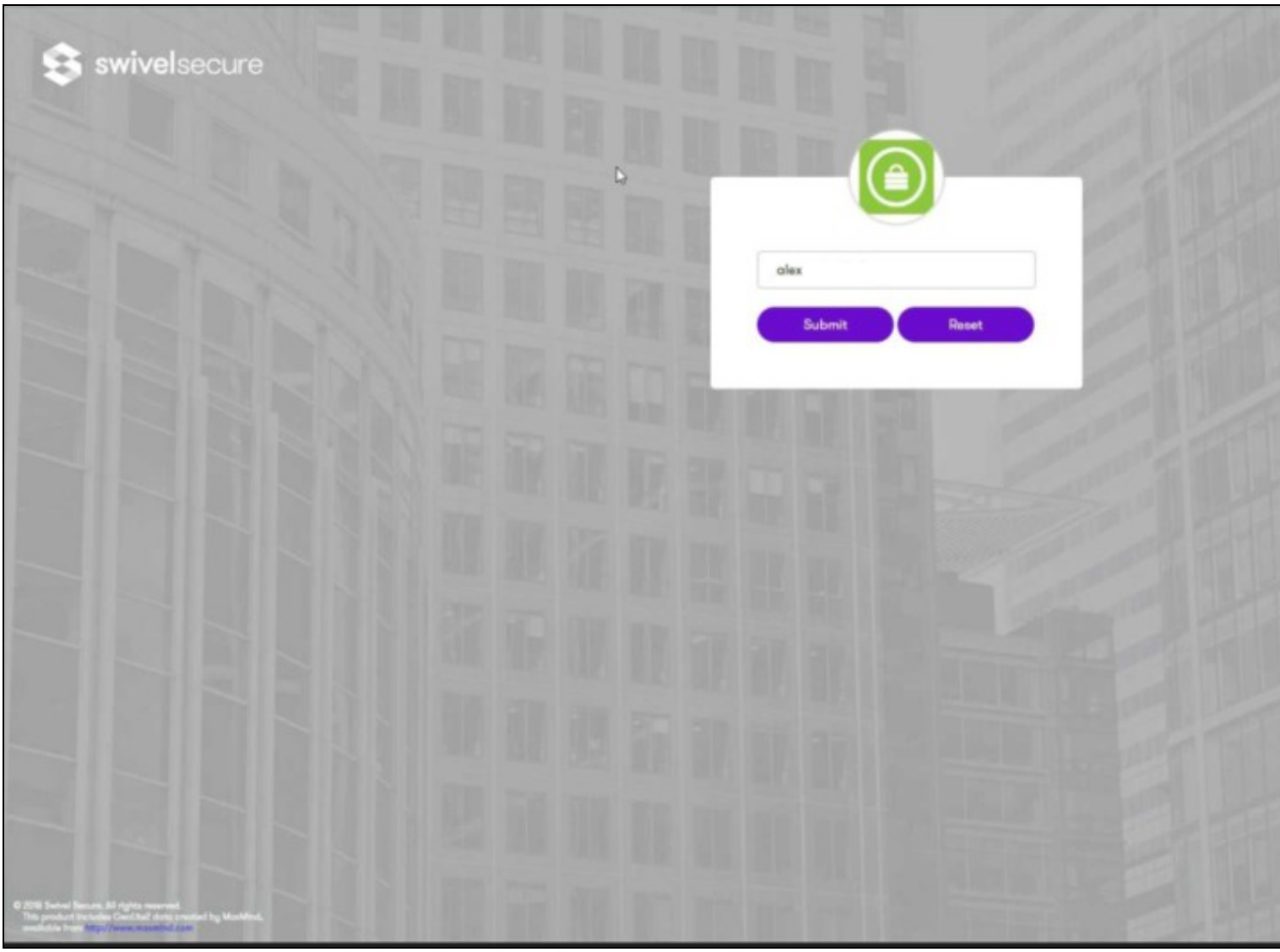
Visit your AuthControl Sentry Page with your public DNS entry of your Swivel AuthControl Sentry server, e.g. https://mycompanysentrydomain/sentry/startPage. On a Start Page you will be able to see a new Thycotic Secret Server Icon on which you can click and proceed with authentication (as you would by going straight to the Thycotic Secret Server page)

When you visit this URL you will notice that the domain should redirect to the identity provider login URL that you setup.

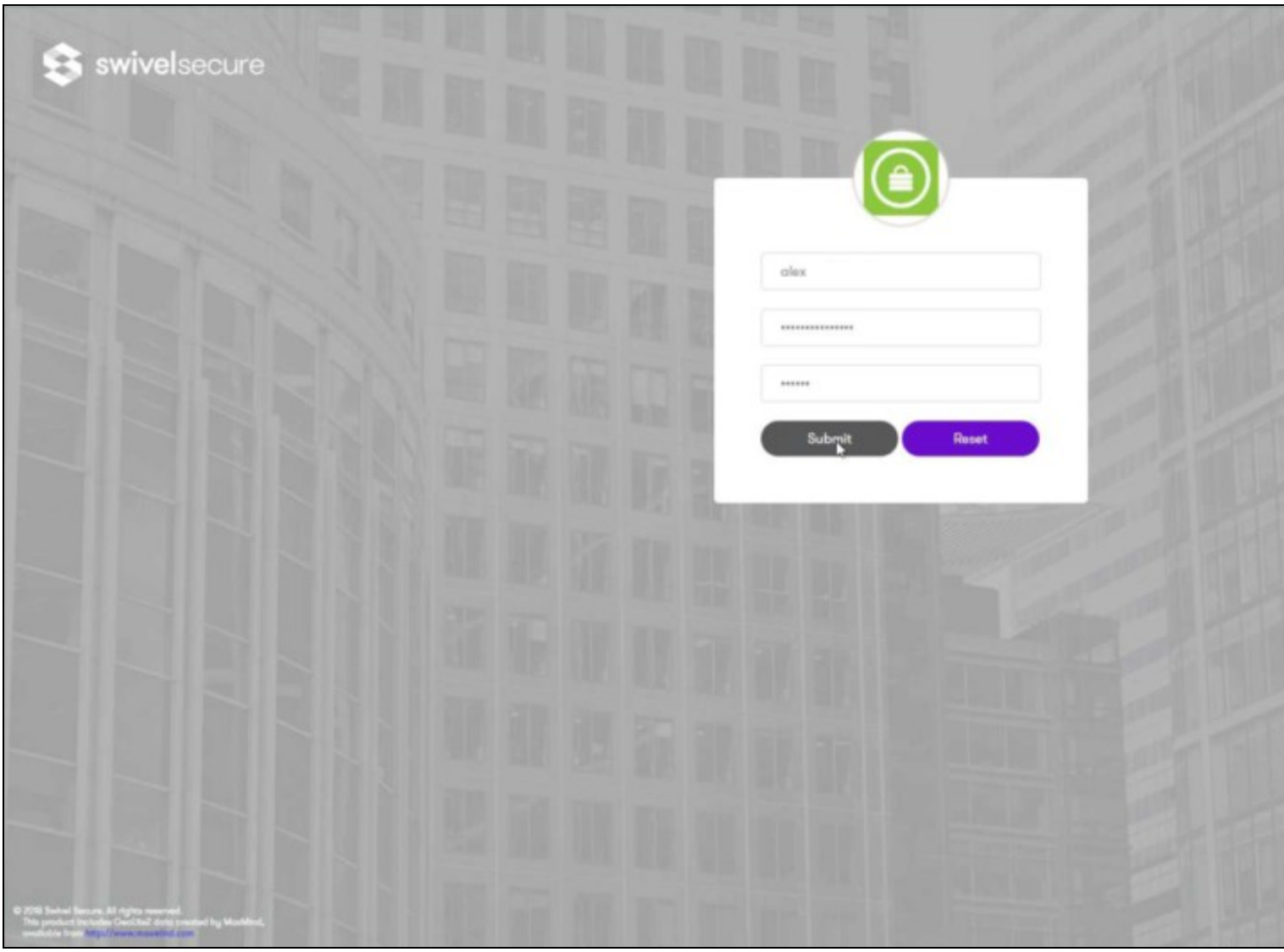


Once you have submitted your username. You should be presented with the Sentry authentication page.

In this login example we are using the sAMAccountName as a username and the fully qualified domain\username is being passed at the back end.



Once you have submitted your username. You should be presented with the page of the Authentication Method which can score enough points to match the points required by the Thycotic Secret Server Application definition.



After we enter our authentication credentials we successfully will see the Thycotic Secret Server account that we tried to access.

Troubleshooting

There are various logging components available for this particular integration which can aid in diagnosis at different points during authentication.

```
The Swivel Core has a Log Viewer menu item which can reveal information concerning user status e.g. is the user locked, has a session been
The Swivel AuthControl Sentry has a View Log menu item which provides details about the SAML assertion and response received from Thycotic
```

It is crucial when troubleshooting, to pinpoint where the authentication is failing. For example, you may find that the Swivel Core logs show a successful authentication (which would indicate that the user has entered their Password and OTC correctly), but the AuthControl Sentry logging shows that there is a problem with the SAML assertion.

Two common issues which can be diagnosed with the validator are:

```
Certificate or decryption issues;
    Can AuthControl Sentry find the Certificate locally, is it the correct one?
    Has the correct Certificate been uploaded to Thycotic Secret Server?
    Does the Repository -> Attribute name being used actually map to a Repository attribute? Has a User Sync occurred in the Swivel Core s
```