Sentry SSO with JIRA

Contents

Introduction

This document describes how to configure on-premise Atlassian JIRA to work with Sentry SSO. Before following these instructions, you should be familiar with using Sentry - see the Sentry User Guide for more information.

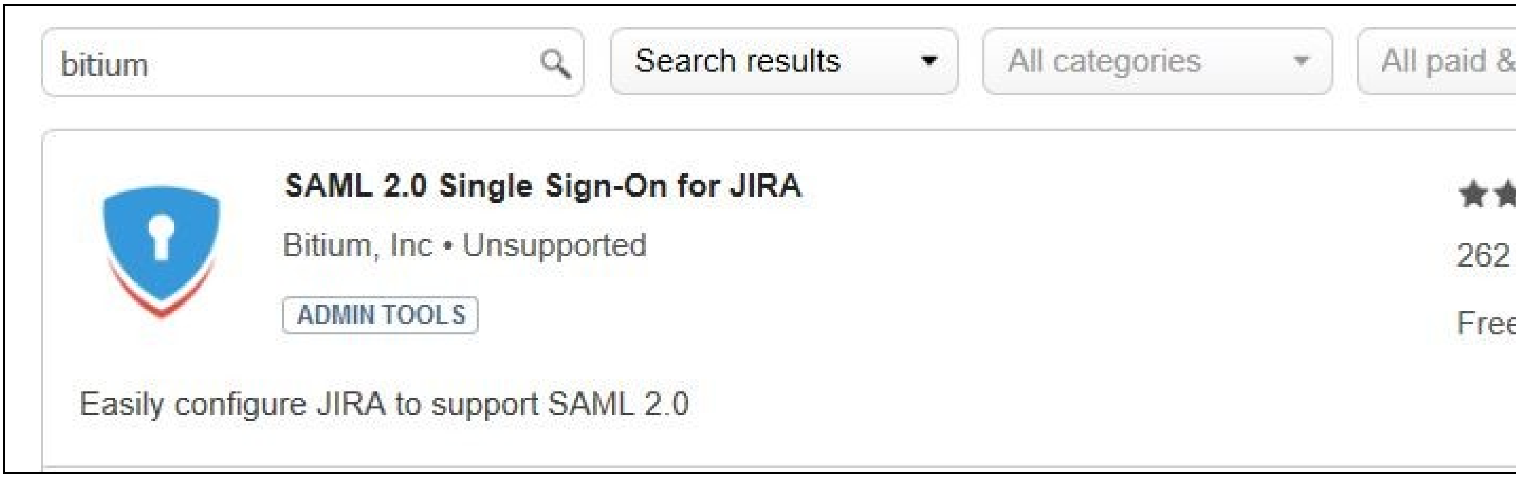
Setup AuthControl Sentry Keys

Before you are able to create a Single Sign On configuration on your JIRA site, 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.

Setup SSO on JIRA

To configure SSO on JIRA a third party add-on is required. There are many SAML plugins available but the plugin that has been used by one of our partners and integrated successfully is the "SAML 2.0 Single Sign-On for JIRA" plugin by Bitium, Inc.

Goto the AddOns configuration page in JIRA. Search for Bitium and install the "SAML 2.0 Single Sign-On for JIRA" addon:



bitium

Search results

All categories

All paid &

SAML 2.0 Single Sign-On for JIRA

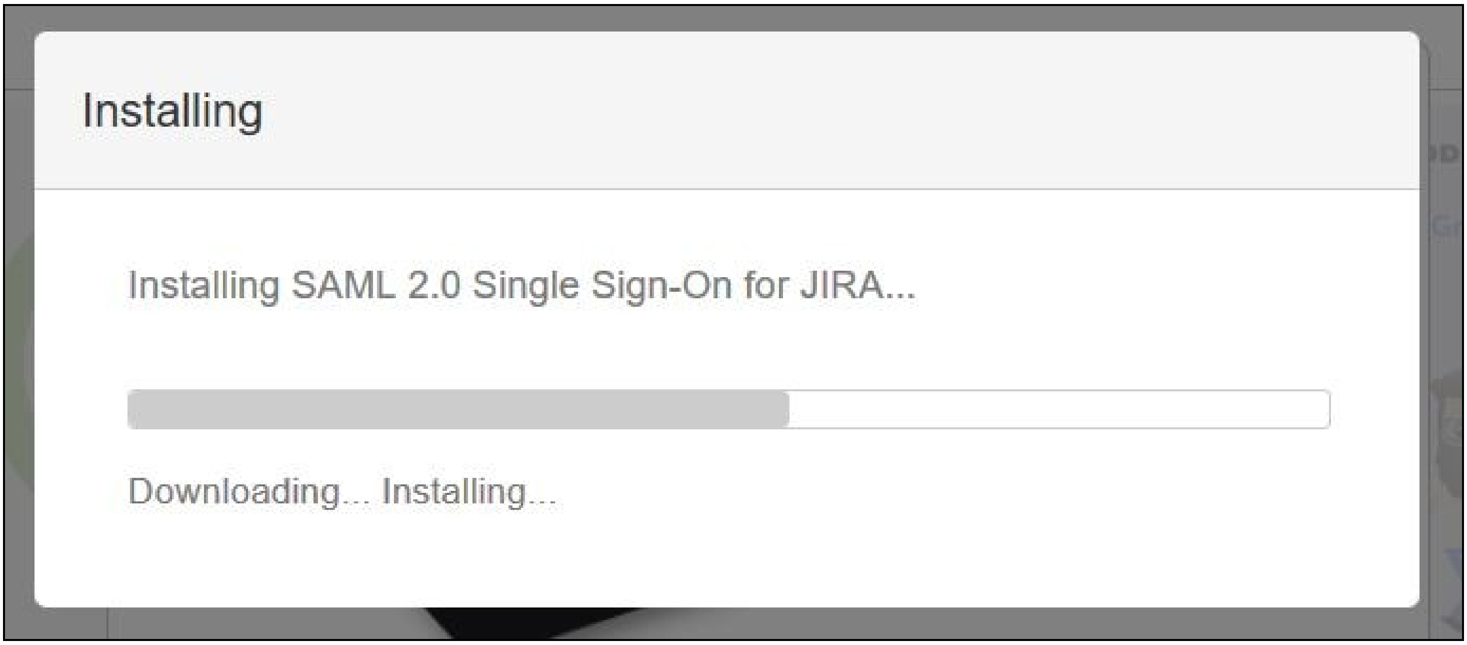
Bitium, Inc • Unsupported

ADMIN TOOLS

262

Free

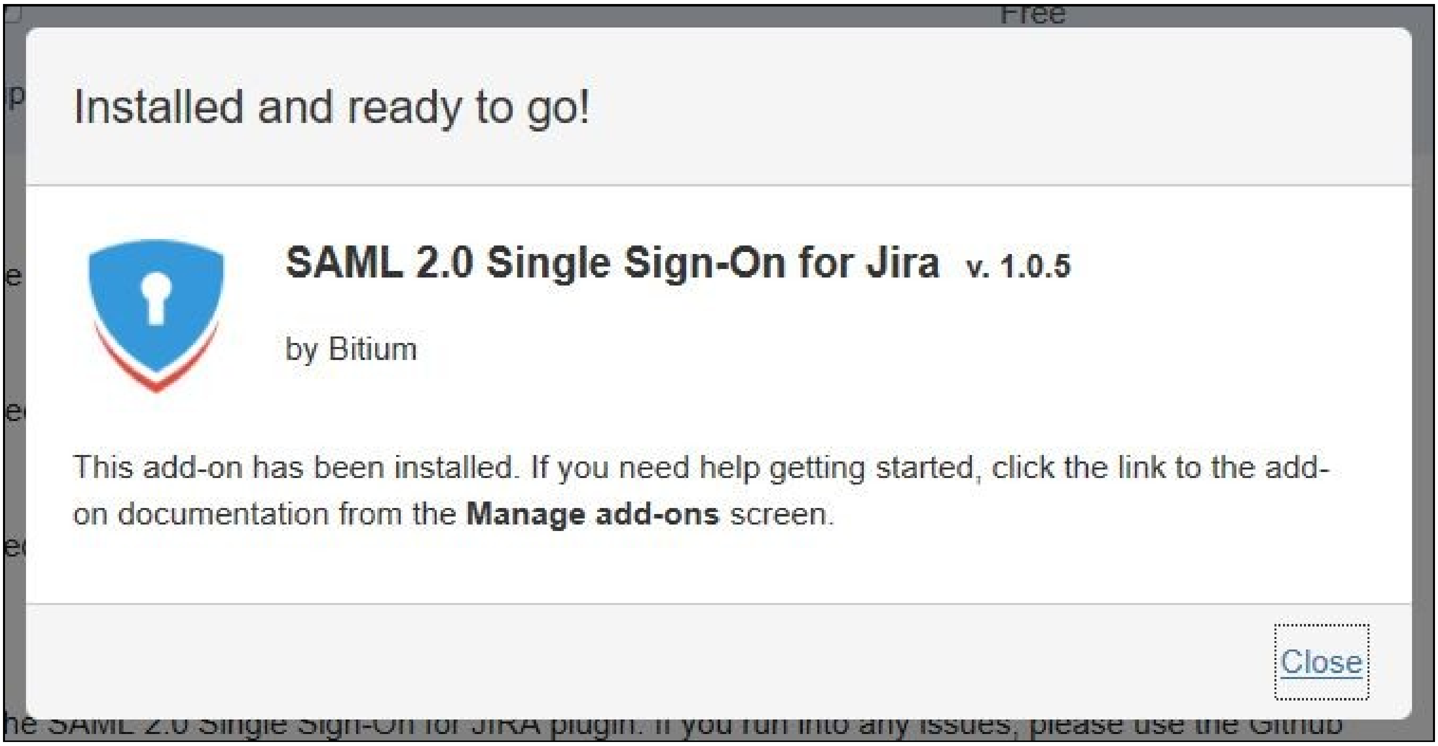
Easily configure JIRA to support SAML 2.0



Installing

Installing SAML 2.0 Single Sign-On for JIRA...

Downloading... Installing...



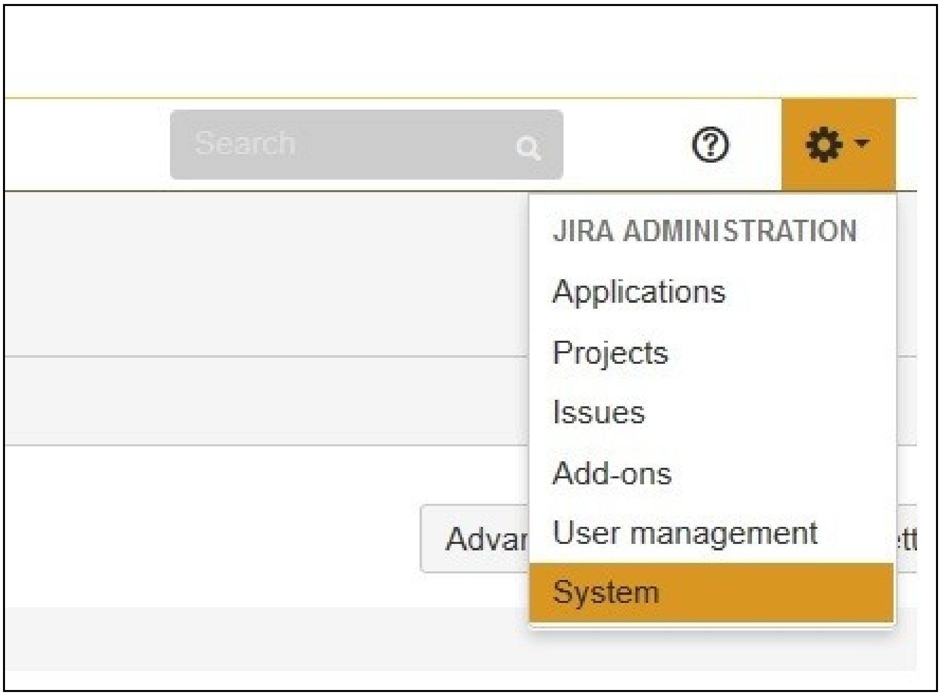
Installed and ready to go!

SAML 2.0 Single Sign-On for Jira v. 1.0.5

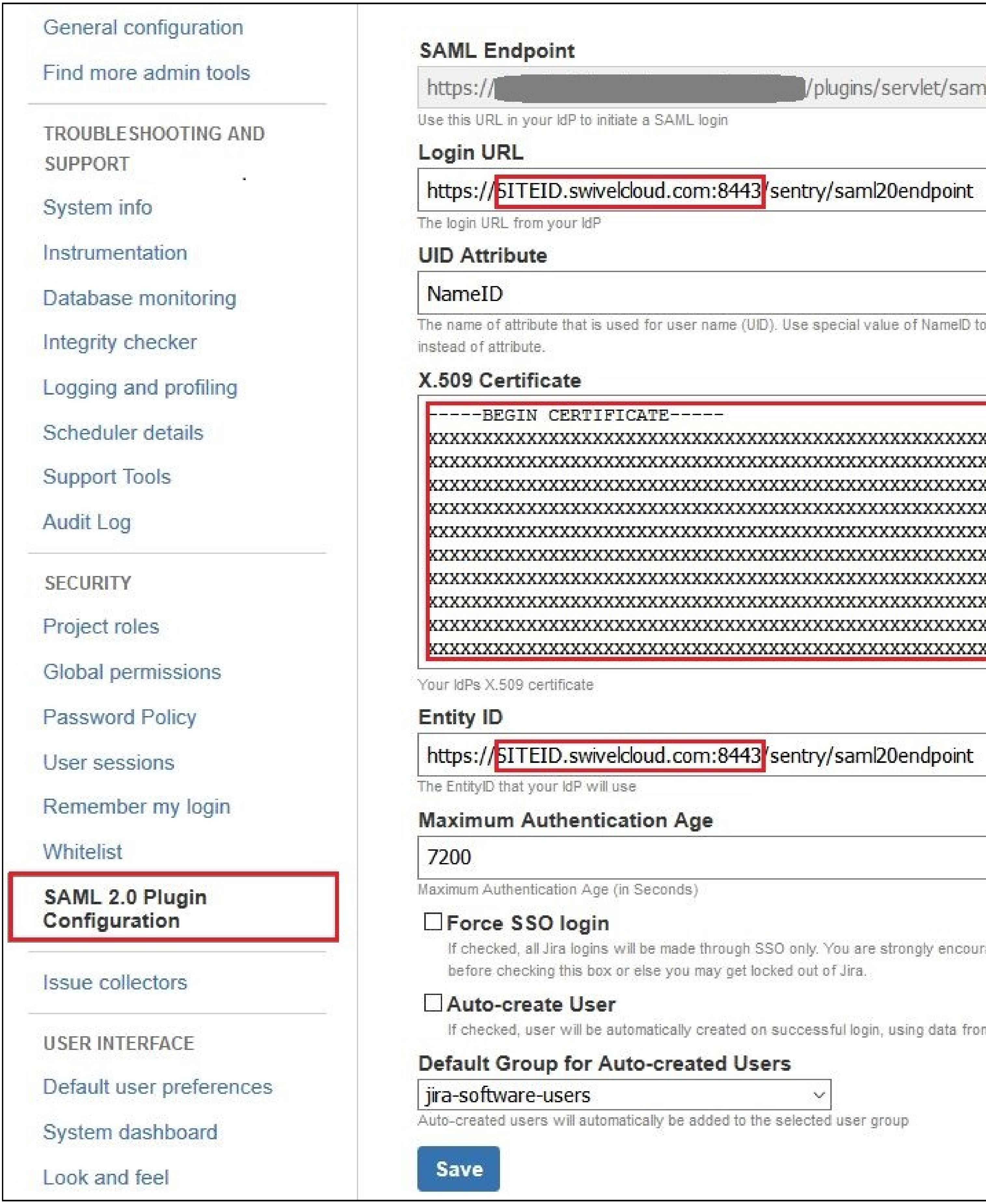
by Bitium

This add-on has been installed. If you need help getting started, click the link to the add-on documentation from the **Manage add-ons** screen.

Once installed, goto the System settings screen in JIRA, to begin the SAML configuration:



The plugin configuration screen is located on the left hand menu under Security:



SAML Endpoint

https://[redacted]/plugins/servlet/sam

Use this URL in your IdP to initiate a SAML login

Login URL

https://SITEID.swivelcloud.com:8443/sentry/saml20endpoint

The login URL from your IdP

UID Attribute

NameID

The name of attribute that is used for user name (UID). Use special value of NameID to instead of attribute.

X.509 Certificate

```
-----BEGIN CERTIFICATE-----
xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
```

Your IdPs X.509 certificate

Entity ID

https://SITEID.swivelcloud.com:8443/sentry/saml20endpoint

The EntityID that your IdP will use

Maximum Authentication Age

7200

Maximum Authentication Age (in Seconds)

☐ **Force SSO login**

If checked, all Jira logins will be made through SSO only. You are strongly encour before checking this box or else you may get locked out of Jira.

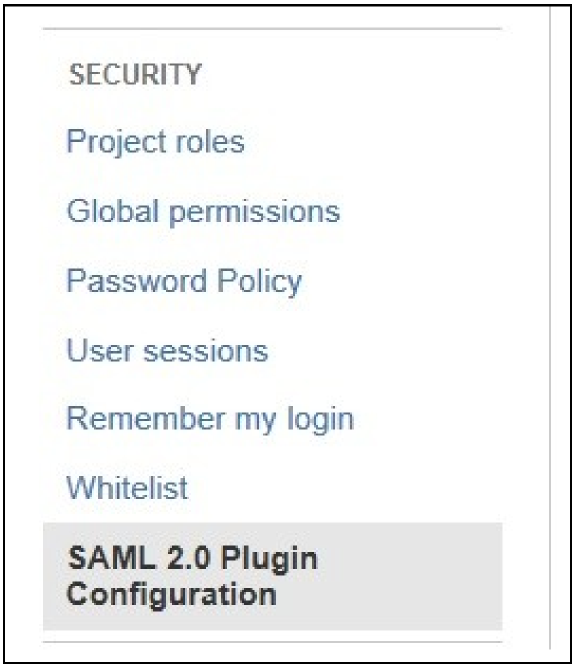
☐ **Auto-create User**

If checked, user will be automatically created on successful login, using data fron

Default Group for Auto-created Users

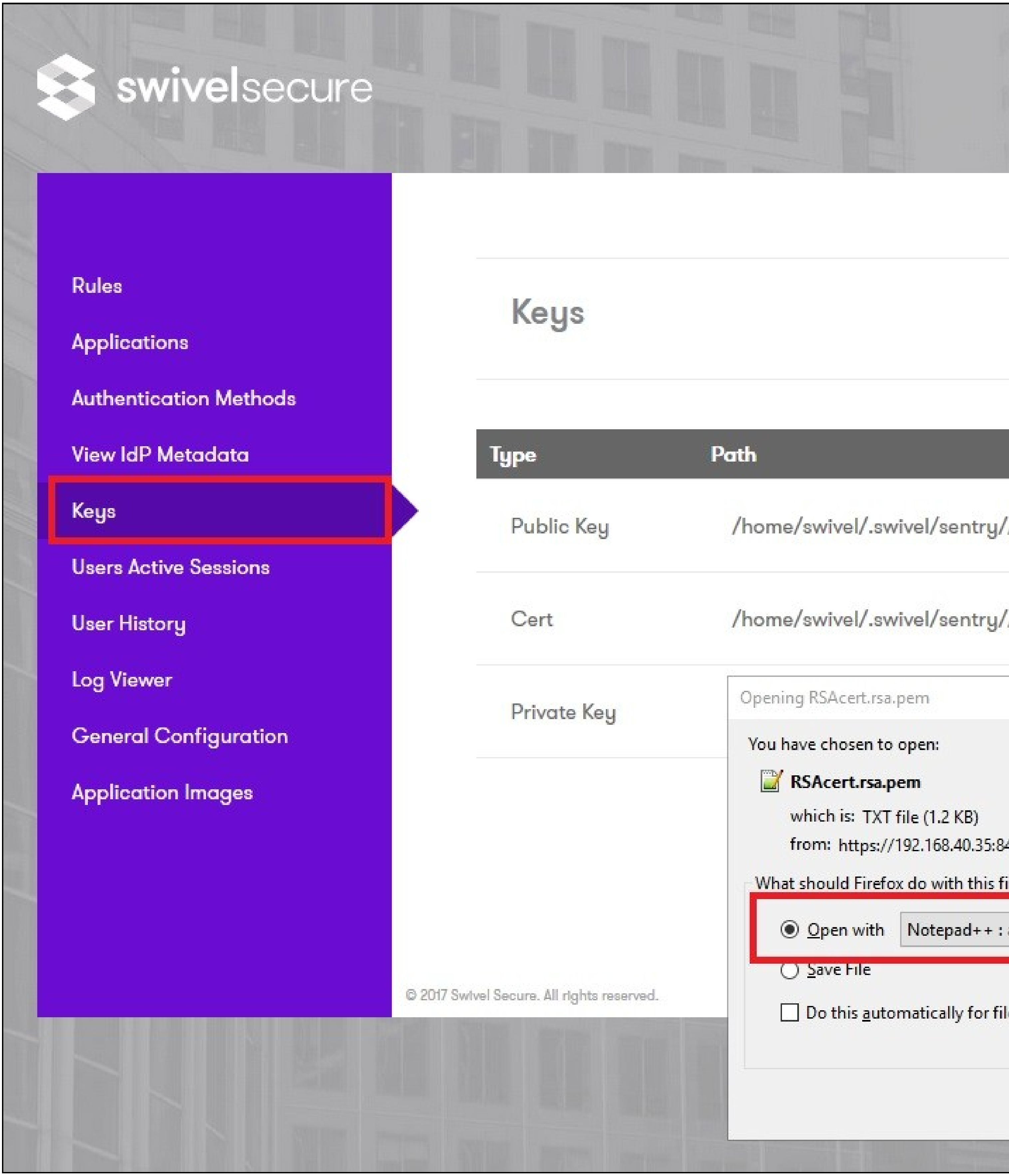
jira-software-users

Auto-created users will automatically be added to the selected user group



Configure the settings as shown in the screenshot, being careful to replace your hostname in the highlighted areas. Leave NameID as it is.

In the X.509 Certificate field, you will need to paste the Key from Swivel AuthControl Sentry. Navigate to your AuthControl Sentry Keys page and copy the certificate text into the SAML plugin in JIRA.



Keys

Type	Path
Public Key	/home/swivel/.swivel/sentry/
Cert	/home/swivel/.swivel/sentry/
Private Key	

You have chosen to open:

RSAcert.rsa.pem

which is: TXT file (1.2 KB)

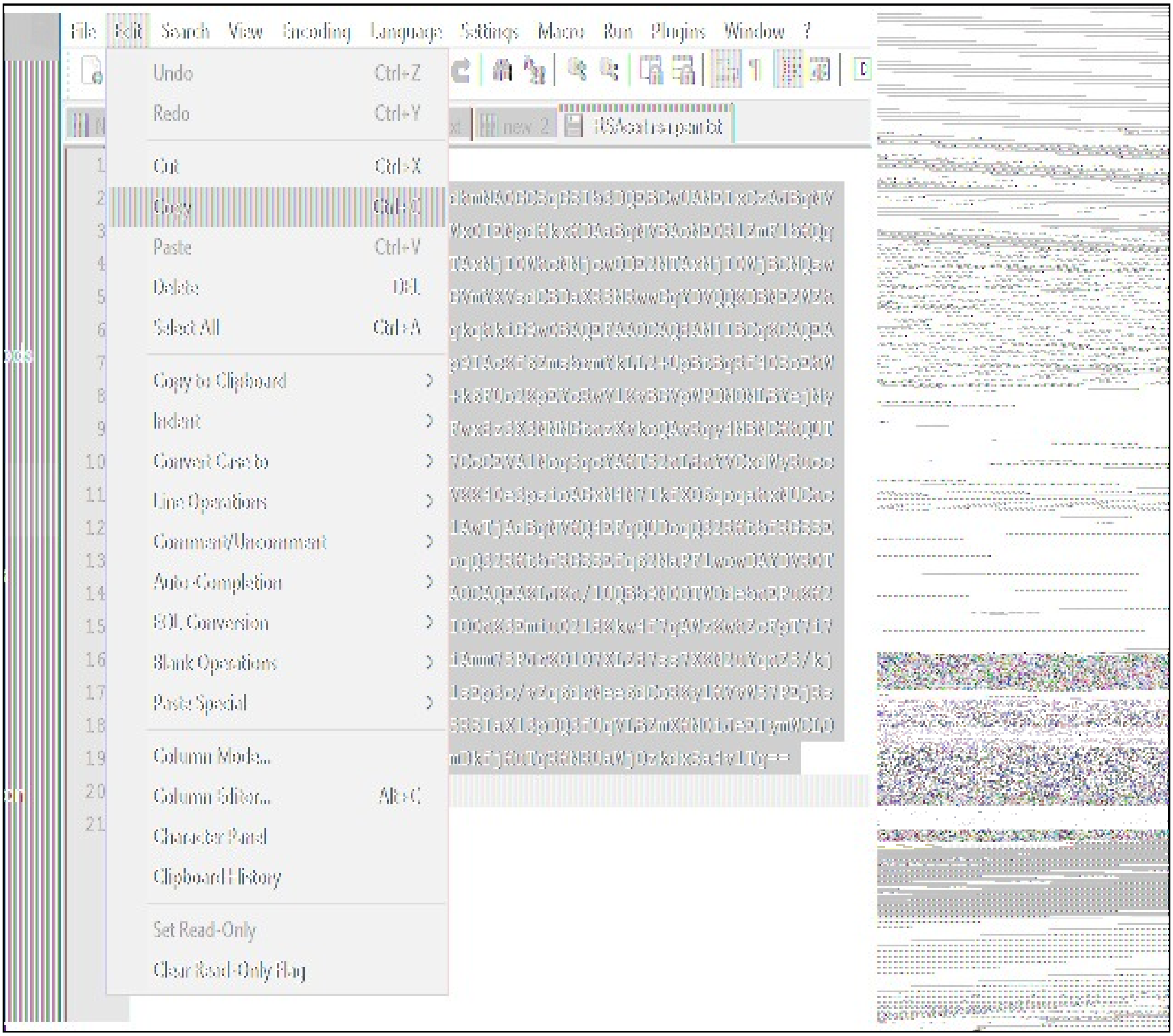
from: https://192.168.40.35:84

What should Firefox do with this fi

● Open with Notepad++ :

○ Save File

□ Do this automatically for fil

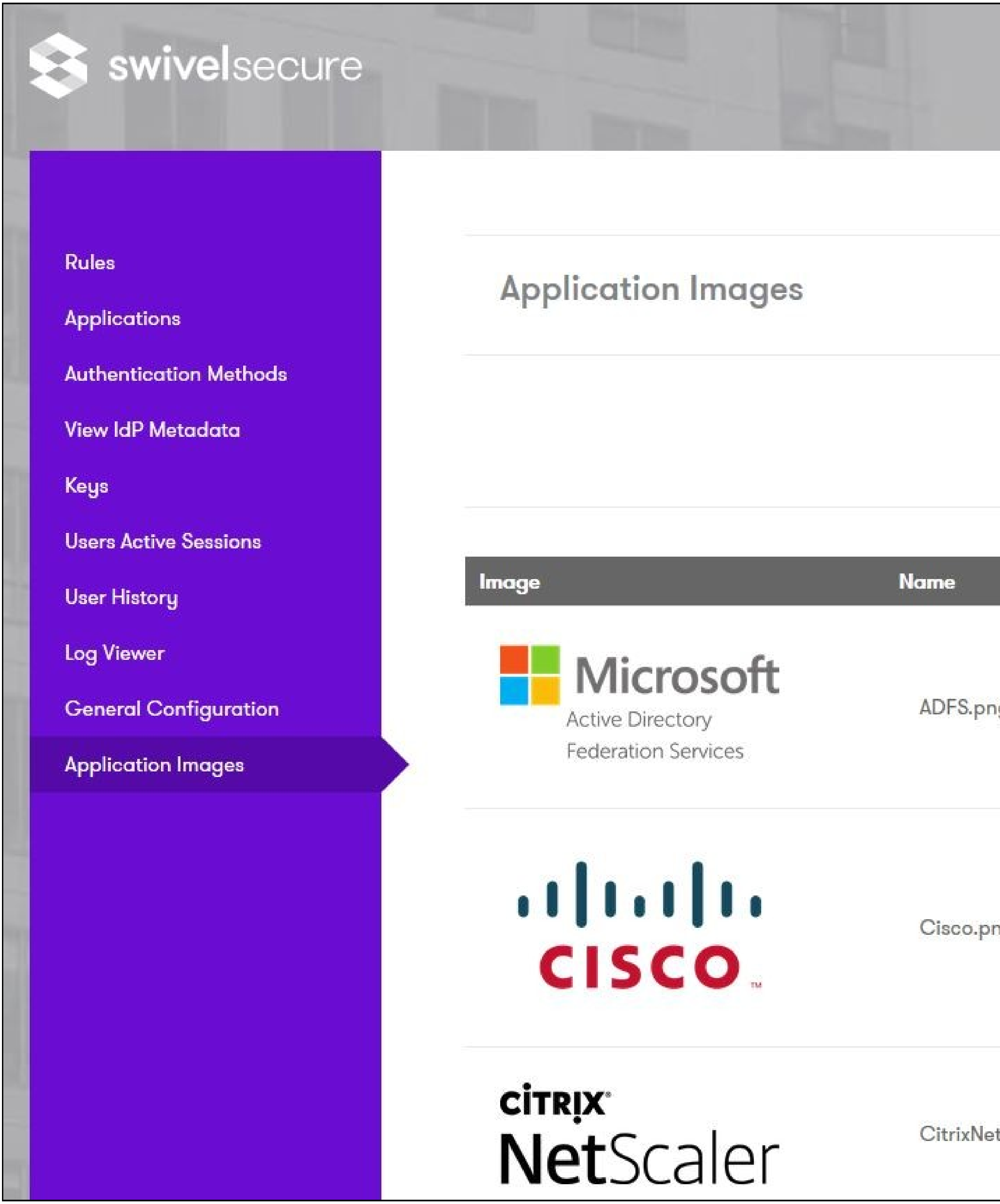


Once all the settings have been configured in the JIRA SAML plugin, save and apply the changes.

Setup AuthControl Sentry Application definition

First we should upload the JIRA logo. Find it using a Google Images search or copy it from here:

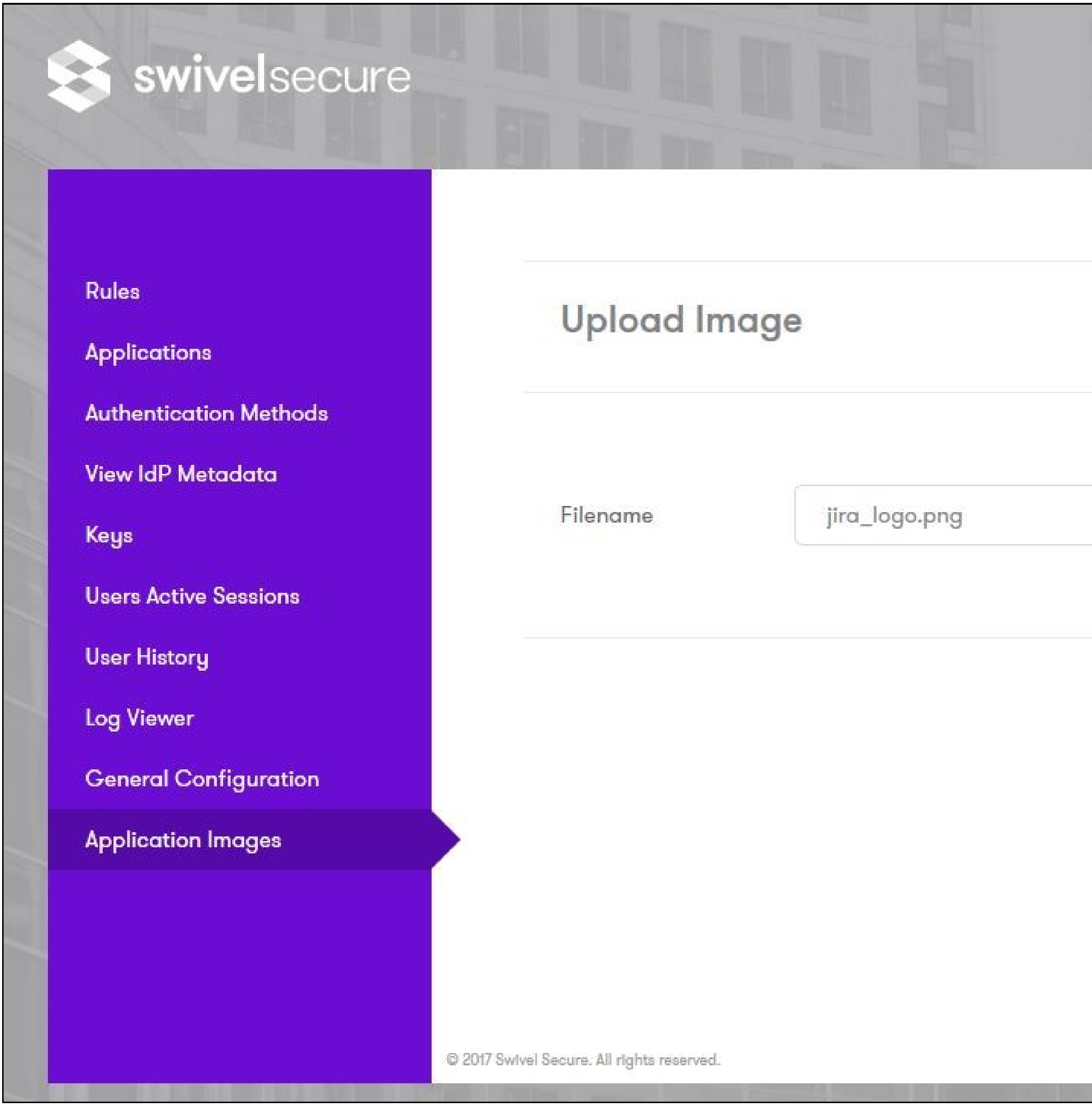
Login to the AuthControl Sentry Administration Console. Click Application Images in the left hand menu. Click the Upload Image button on the top right.



Application Images

Image	Name
Microsoft Active Directory Federation Services	ADFS.pn
CISCO	Cisco.pn
CiTRIX NetScaler	CitrixNet

Browse to the Logo file you have saved:

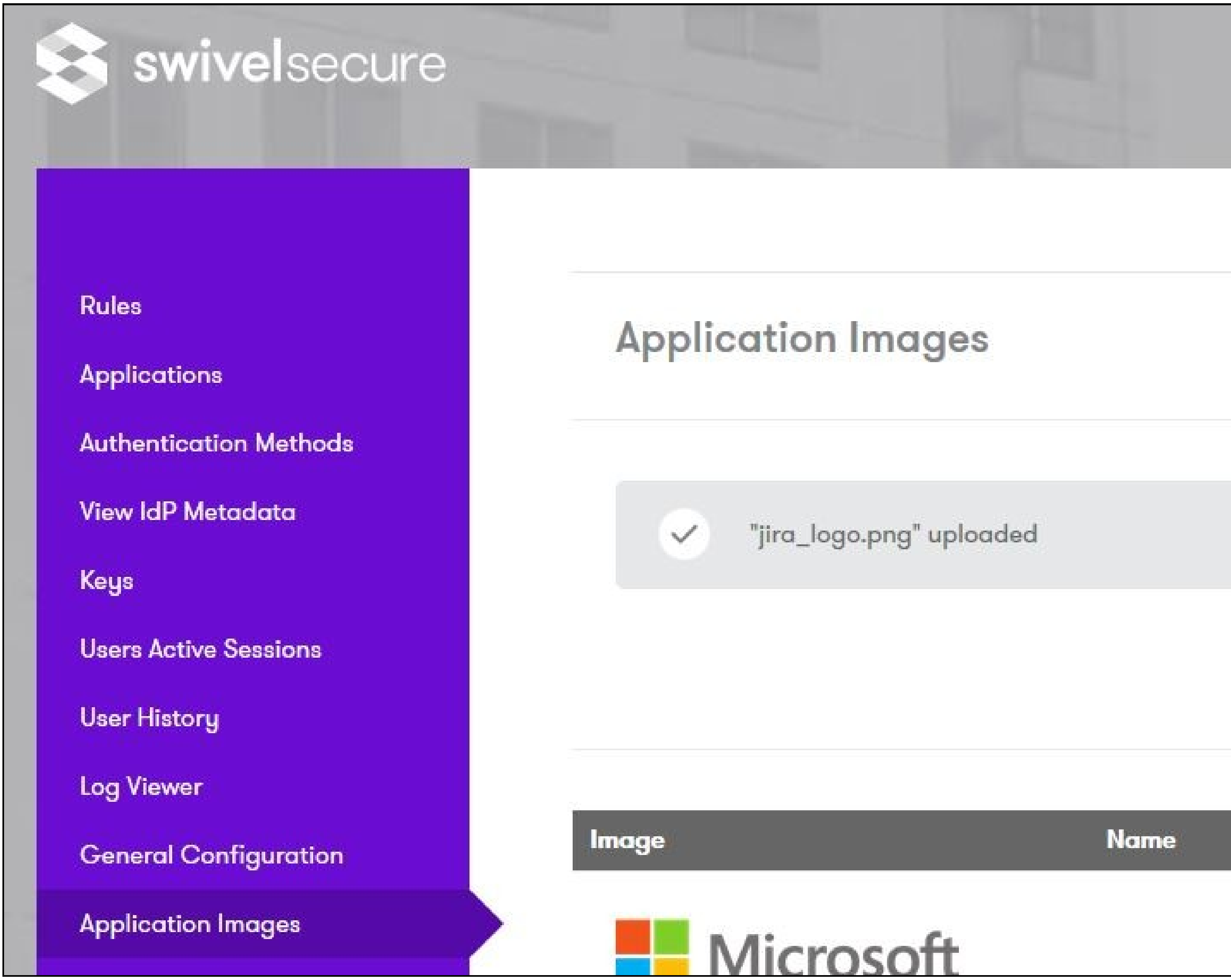


Upload Image

Filename: jira_logo.png

© 2017 Swivel Secure. All rights reserved.

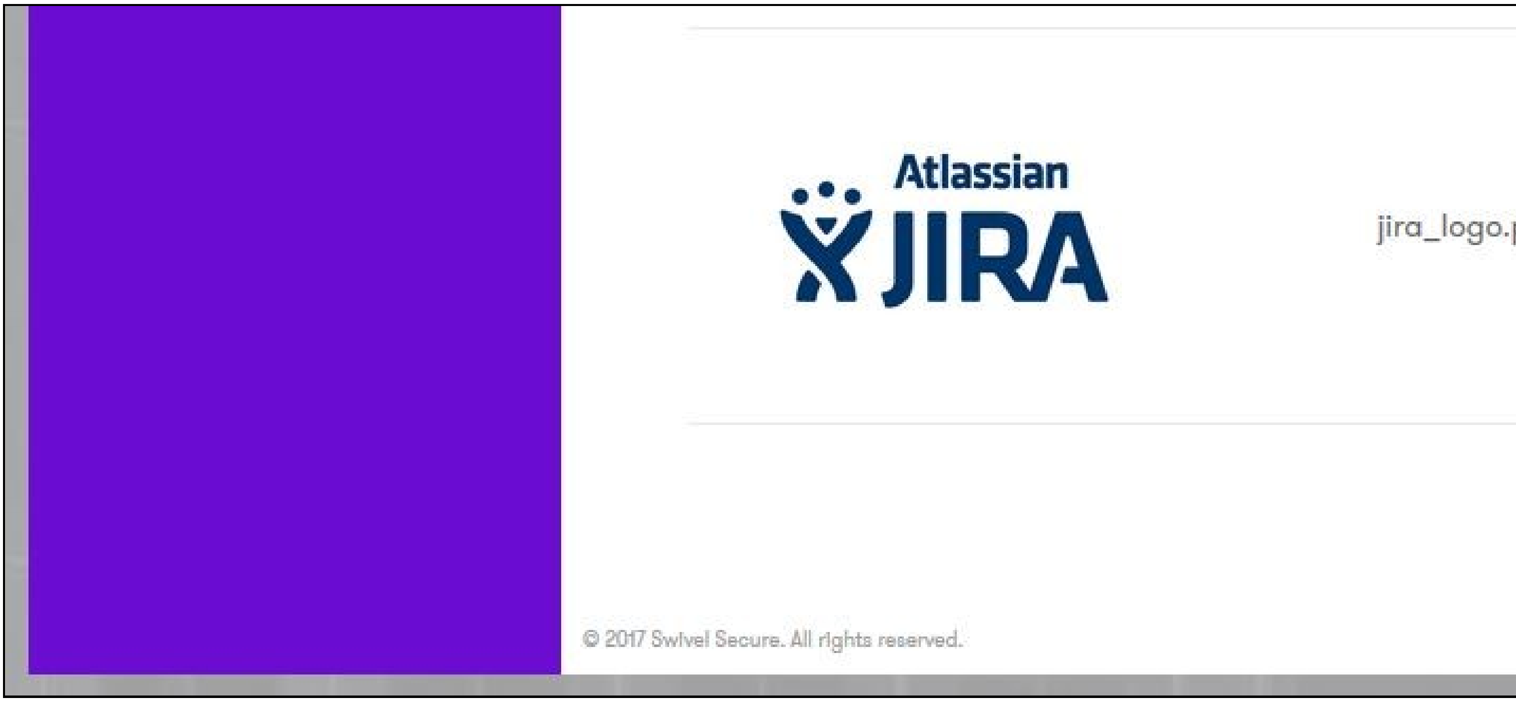
Then upload the image to the Sentry application:



Application Images

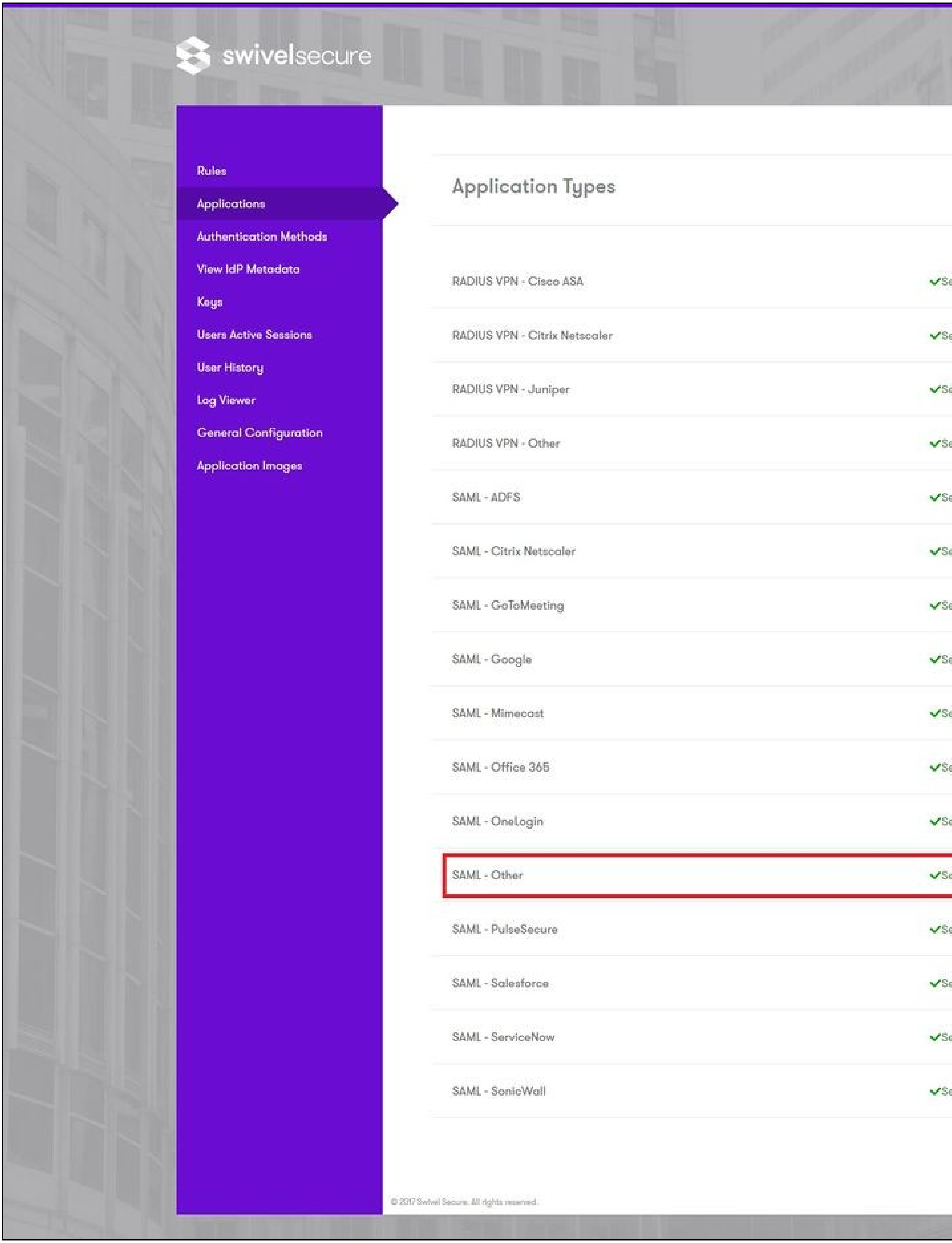
"jira_logo.png" uploaded

The image should now be available to select, when we go to create a new Application definition for JIRA:



© 2017 Swivel Secure. All rights reserved.

Login to the AuthControl Sentry Administration Console. Click Applications in the left hand menu. To add a new Application definition for JIRA, click the Add Application button and select SAML - Other type.



Application Types

RADIUS VPN - Cisco ASA	✓Se
RADIUS VPN - Citrix Netscaler	✓Se
RADIUS VPN - Juniper	✓Se
RADIUS VPN - Other	✓Se
SAML - ADFS	✓Se
SAML - Citrix Netscaler	✓Se
SAML - GoToMeeting	✓Se
SAML - Google	✓Se
SAML - Mimecast	✓Se
SAML - Office 365	✓Se
SAML - OneLogin	✓Se
SAML - Other	✓Se
SAML - PulseSecure	✓Se
SAML - Salesforce	✓Se
SAML - ServiceNow	✓Se
SAML - SonicWall	✓Se

Name: **JIRA**

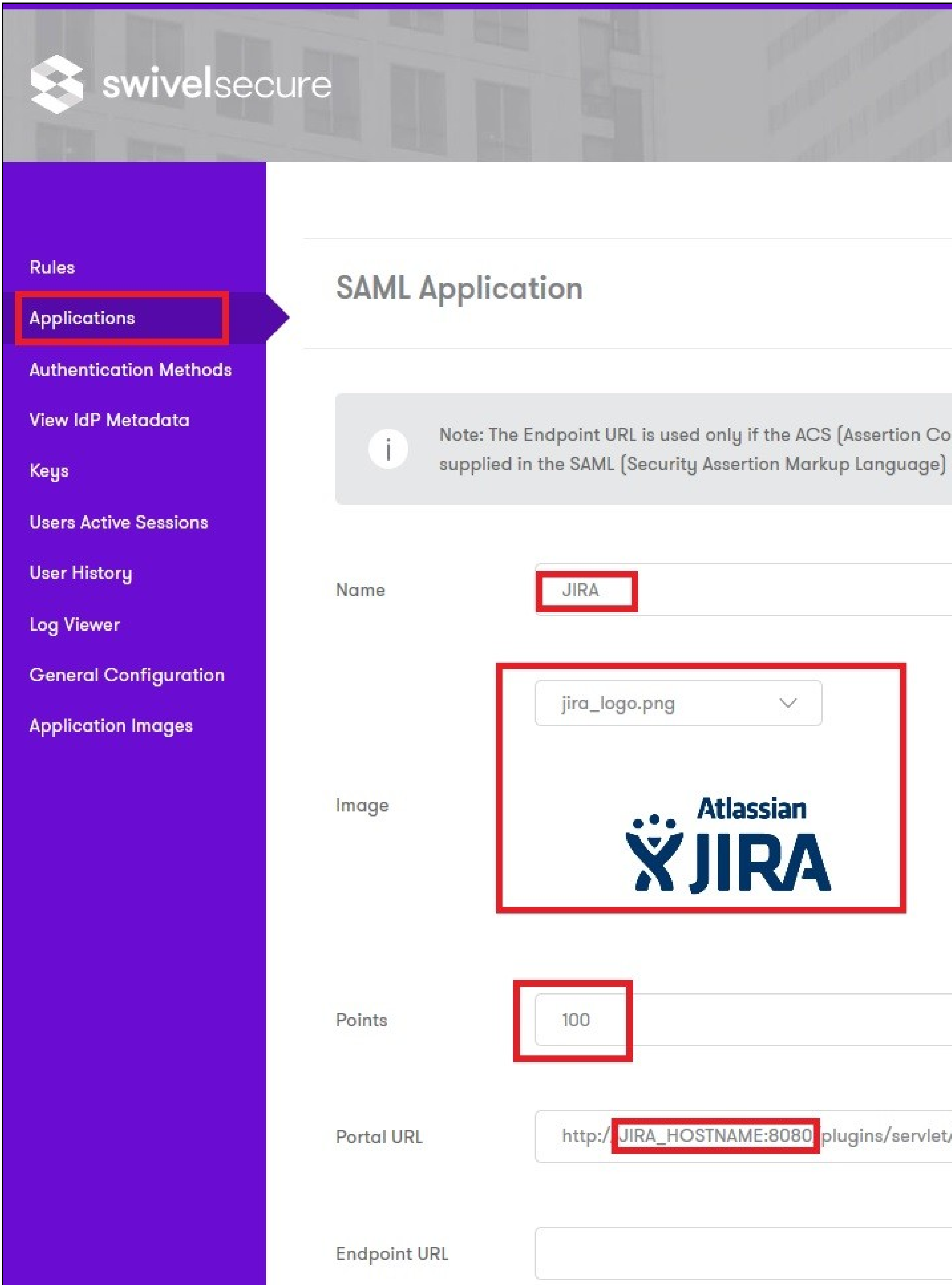
Points: 100 (the number of points the user needs to score from their Authentication Method in order to successfully authenticate to this Application)

Portal URL: URL to access to JIRA e.g. http://**JIRA_HOSTNAME:8080**/plugins/servlet/saml/auth

Endpoint URL: Leave blank - not required

Entity ID: Identifier of the JIRA SAML request e.g. http://**JIRA_HOSTNAME:8080**/jiraSAML

Federated Id: email



SAML Application

Note: The Endpoint URL is used only if the ACS (Assertion Co
supplied in the SAML (Security Assertion Markup Language)

Name	JIRA
Image	jira_logo.png
Points	100
Portal URL	http://JIRA_HOSTNAME:8080/plugins/servlet/
Endpoint URL	

Setup AuthControl Sentry Authentication definition

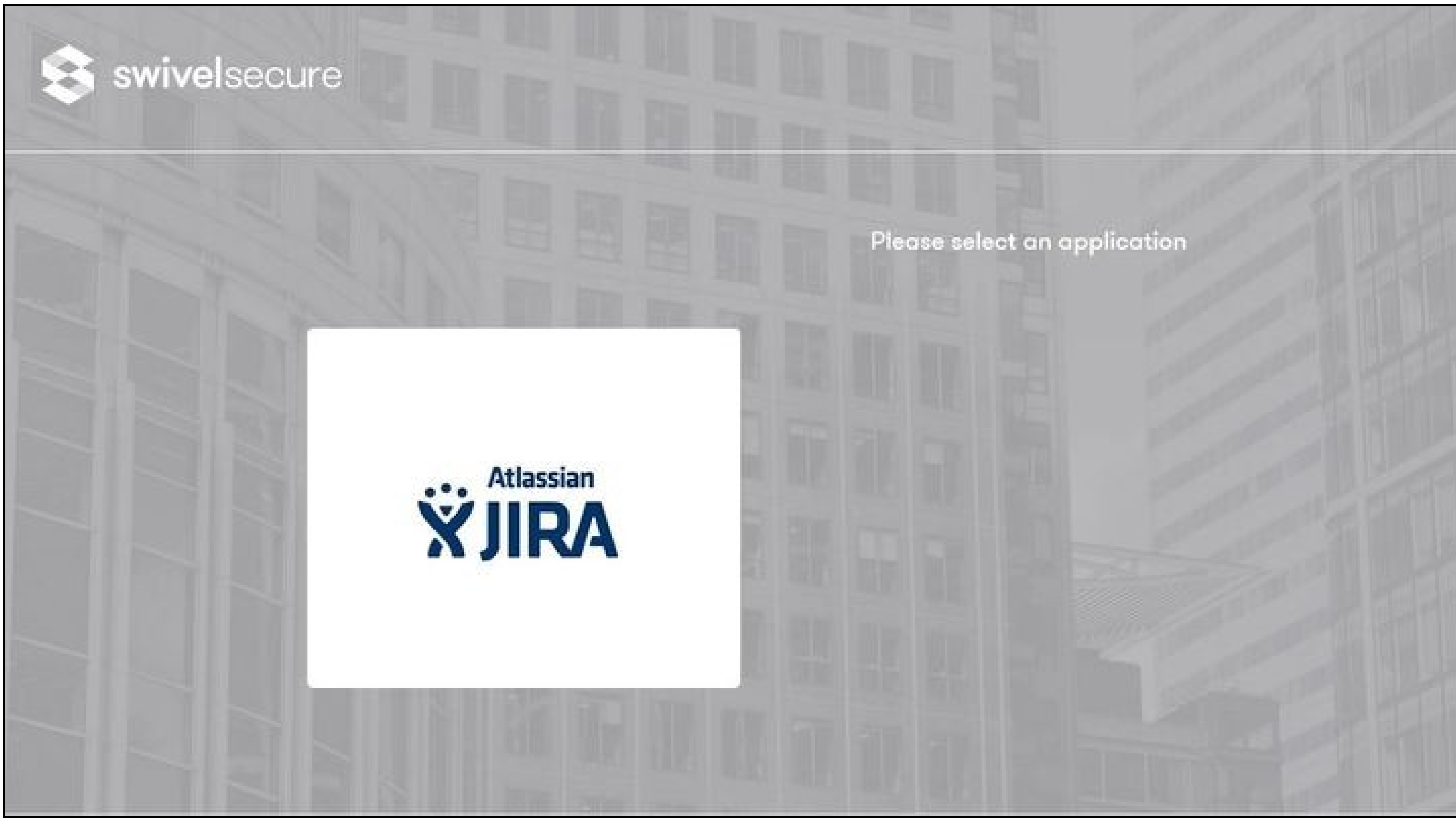
As an example here we will be using Turing authentication as the Primary method required for JIRA authentication.

Login to the AuthControl Sentry Administration Console. Click Authentication Methods in the left hand menu. Click the Edit button against the Turing 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 JIRA 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 JIRA via Swivel AuthControl Sentry

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

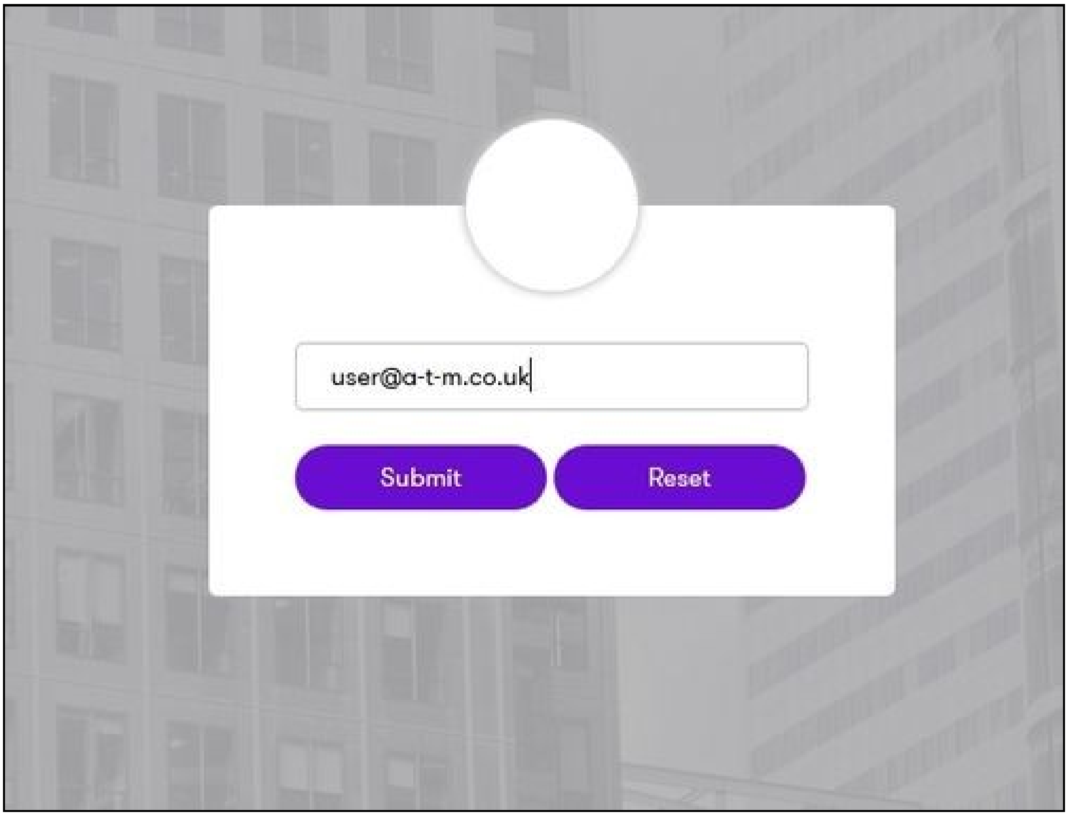
Visit your AuthControl Sentry Page with your public DNS entry of your Swivel AuthControl Sentry server, e.g. https://mycompanysentrydomain/sentry/startPage. On a Start Page you will be able to see a new JIRA Icon on which you can click and proceed with authentication (as you would by going straight to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



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

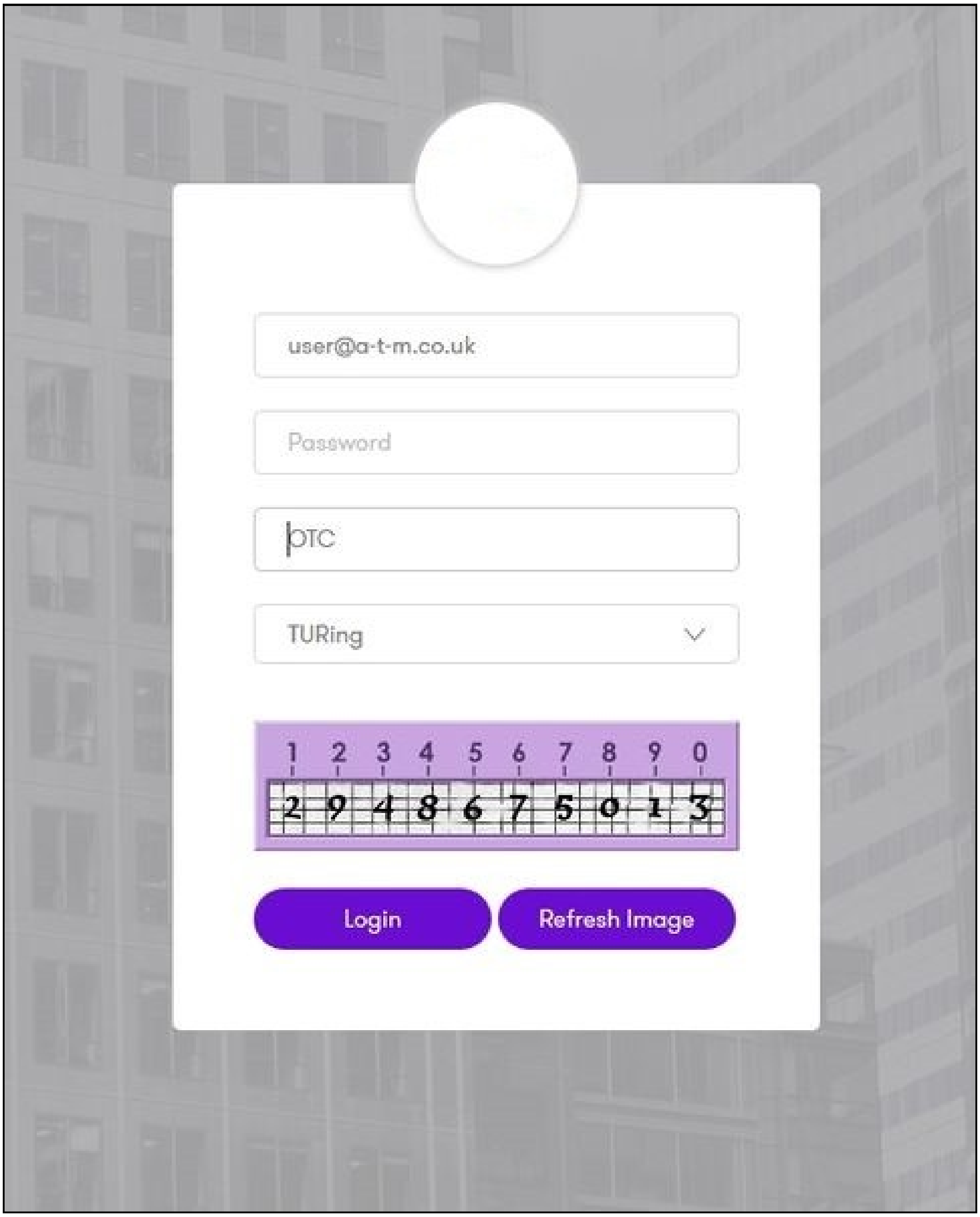
Once you have submitted your username. You should be presented with the Sentry username page.

In this login example we are using the email as a username.



user@a-t-m.co.uk

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 JIRA Application definition.



user@a-t-m.co.uk

Password

OTC

TURing

After we enter our authentication credentials we successfully will see the JIRA 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 JIRA and
```

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 JIRA?
    Does the Repository -> Attribute name being used actually map to a Repository attribute? Has a User Sync occurred in the Swivel Core s
```