Sentry SSO with GoogleApps

Contents

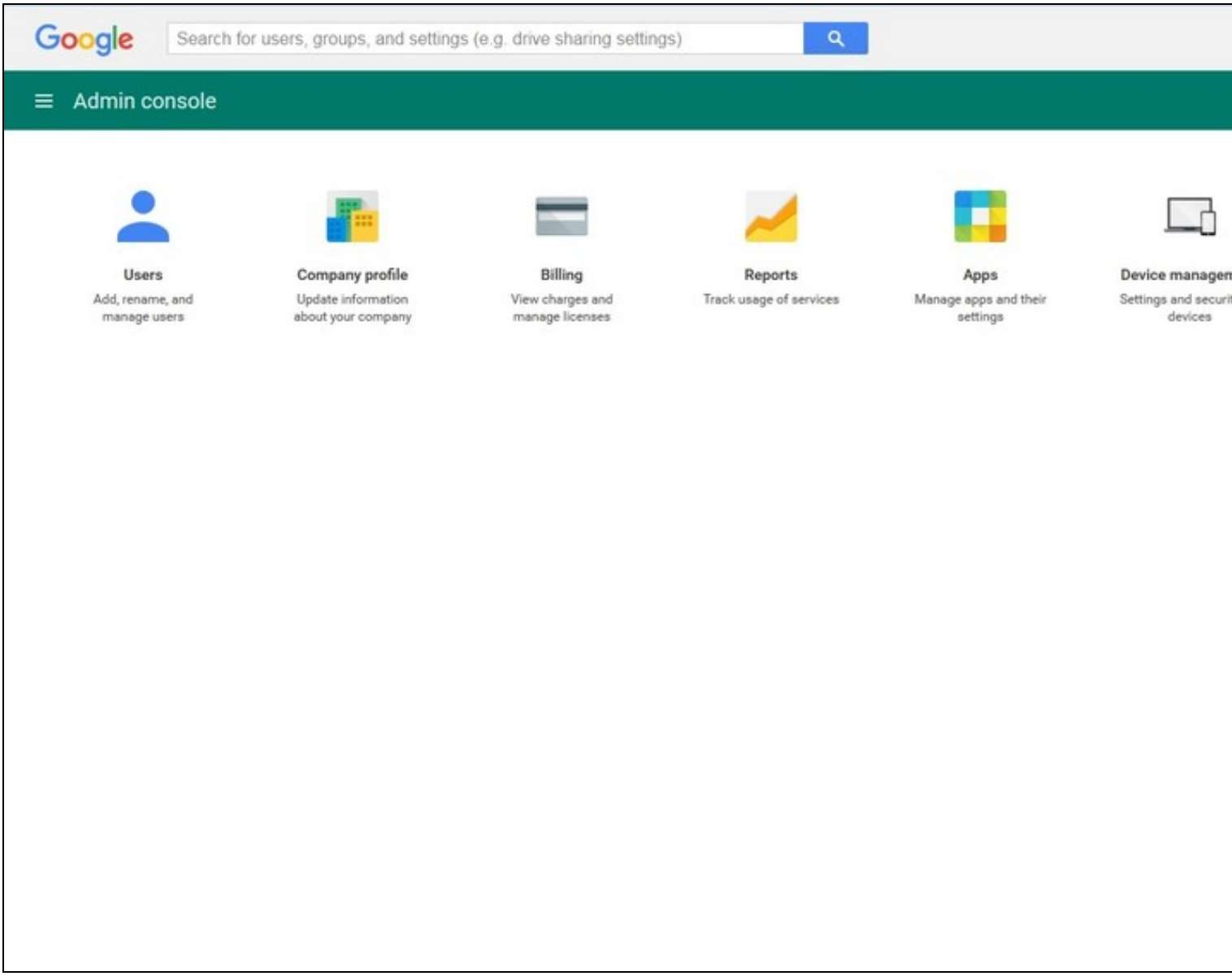
- 1 Setup AuthControl Sentry Keys
- 2 Setup SSO on Google
- 3 Configure Check Password with Repository on the Swivel Core
- 4 Setup AuthControl Sentry Application definition
- 5 Setup AuthControl Sentry Authentication definition
- 6 Testing authentication to Google via Swivel AuthControl Sentry
- 7 Troubleshooting

Setup AuthControl Sentry Keys

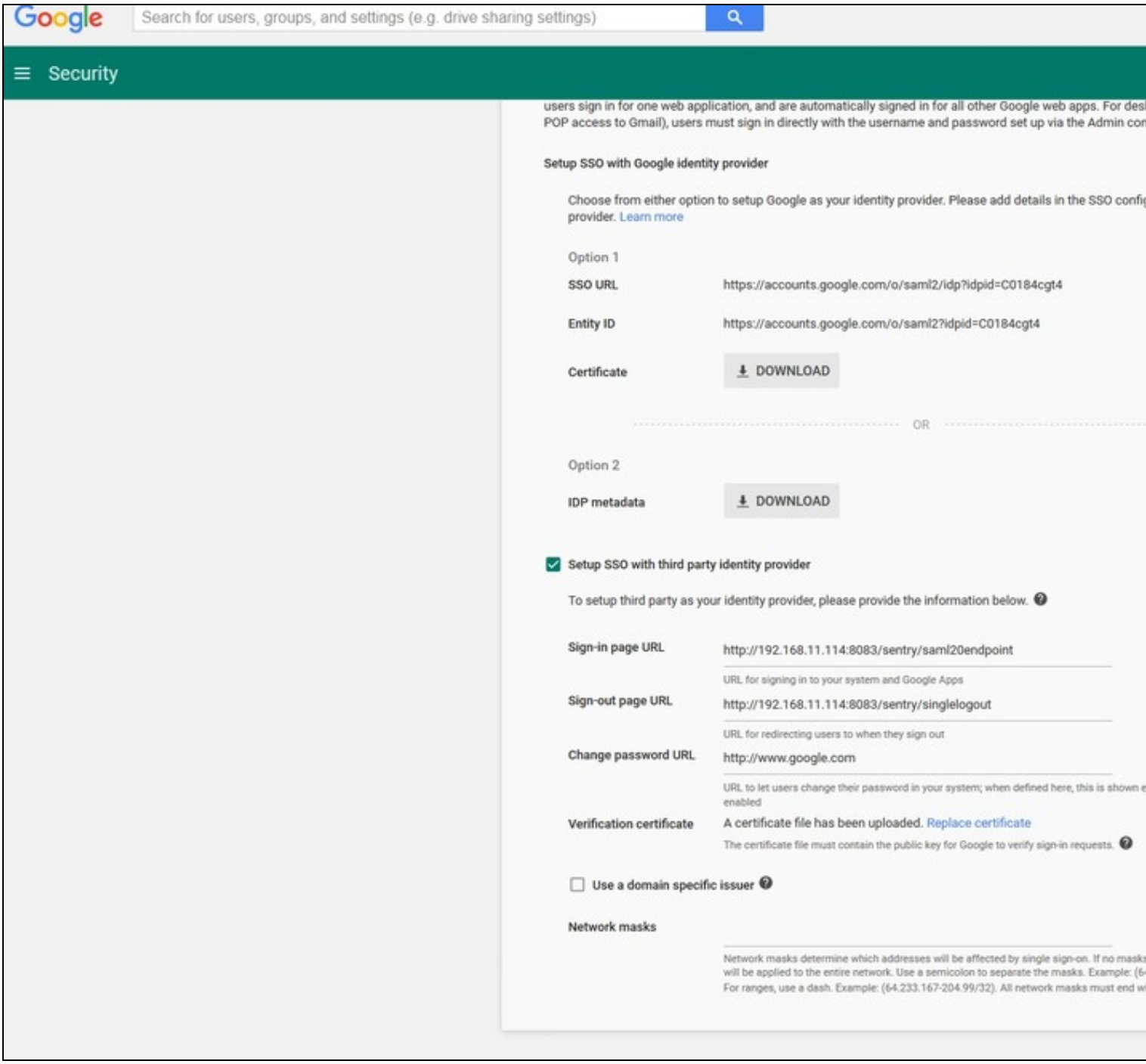
Before you are able to create a Single Sign On configuration on Google.com, you will need to setup some Keys. Please see a separate article: HowToCreateKeysOnCmi. You will need the certificate you generate in a later section of this article. This can be retrieved from the View Keys menu option of Swivel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

Setup SSO on Google

To configure SSO setting on your Google Business account you have to access your Admin console by simply going to **https://admin.google.com/AdminHome** or by following **https://google.co.uk/*Your Company Name*/** You should see an Admin console with an option "Security" similar to the one below:



When you click on the Security you will be shown security options where you have to click on "Set up single sign-on (SSO)".



You will have to click on the checkbox "Setup SSO with third party identity provider" and fill in the details for your AuthControl Sentry such as:

Set the Login, Logout and Change password URLs below, where <FQDN_OF_SENTRY_SERVER> is the public DNS entry of your Swivel AuthControl Sentry server, e.g. swivel.mycompany.com or if you do not have a redirect from port 443 to 8443 in place, you may need to include a port number e.g. swivel.mycompany.com:8443

Sign-in page URL - *https://<FQDN_OF_SENTRY_SERVER>/sentry/saml20endpoint*

Sign-out page URL - *https://<FQDN_OF_SENTRY_SERVER>/sentry/singlelogout*

Change password URL - *http://www.google.com*

Verification certificate - *Browse to the RSA PEM file created earlier to upload the certificate. When you click save, if successfully imported you will see a popup message saying "Your settings have been saved."*

After you have entered all the details as below click Save

Configure Check Password with Repository on the Swivel Core

In order to check the user?s Active Directory password, ensure that the local Agent is configured as explaind here

Setup AuthControl Sentry Application definition

Please note: you must have setup a Google SSO prior to defining this Application entry within AuthControl Sentry. This is so that you are able to populate the Endpoint URL field. Login to the AuthControl Sentry Administration Console. Click Applications in the left hand menu. To add a new Application definition for Google, click the Add Provider button.

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 Consumer Service) is no
SAML (Security Assertion Markup Language) request.

Name: Google Apps Suite

Image: Google.png

Points: 0

Portal URL: https://docs.google.com/a/mycompanyname

Endpoint URL:

Entity ID: google.com

Federated Id: email

- **Name:** Google
- **Image:** Google.png (selected by default)
- **Points:** 100 (the number of points the user needs to score from their Authentication Method in order to successfully authenticate to this Application)
- **Endpoint URL:**N/A
- **Portal URL:** (this Portal URL is your companies google docs URL which you can usually access on: https://docs.google.com/a/mycompanyname)
- **Entity ID:** google.com (at the time of writing this documentation, this settings is always the same when using Google, but may be subject to change by Google.com, so please review the online Google documentation if you find that this Entity ID no longer works)
- **Federated id:** email

Setup AuthControl Sentry Authentication definition

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

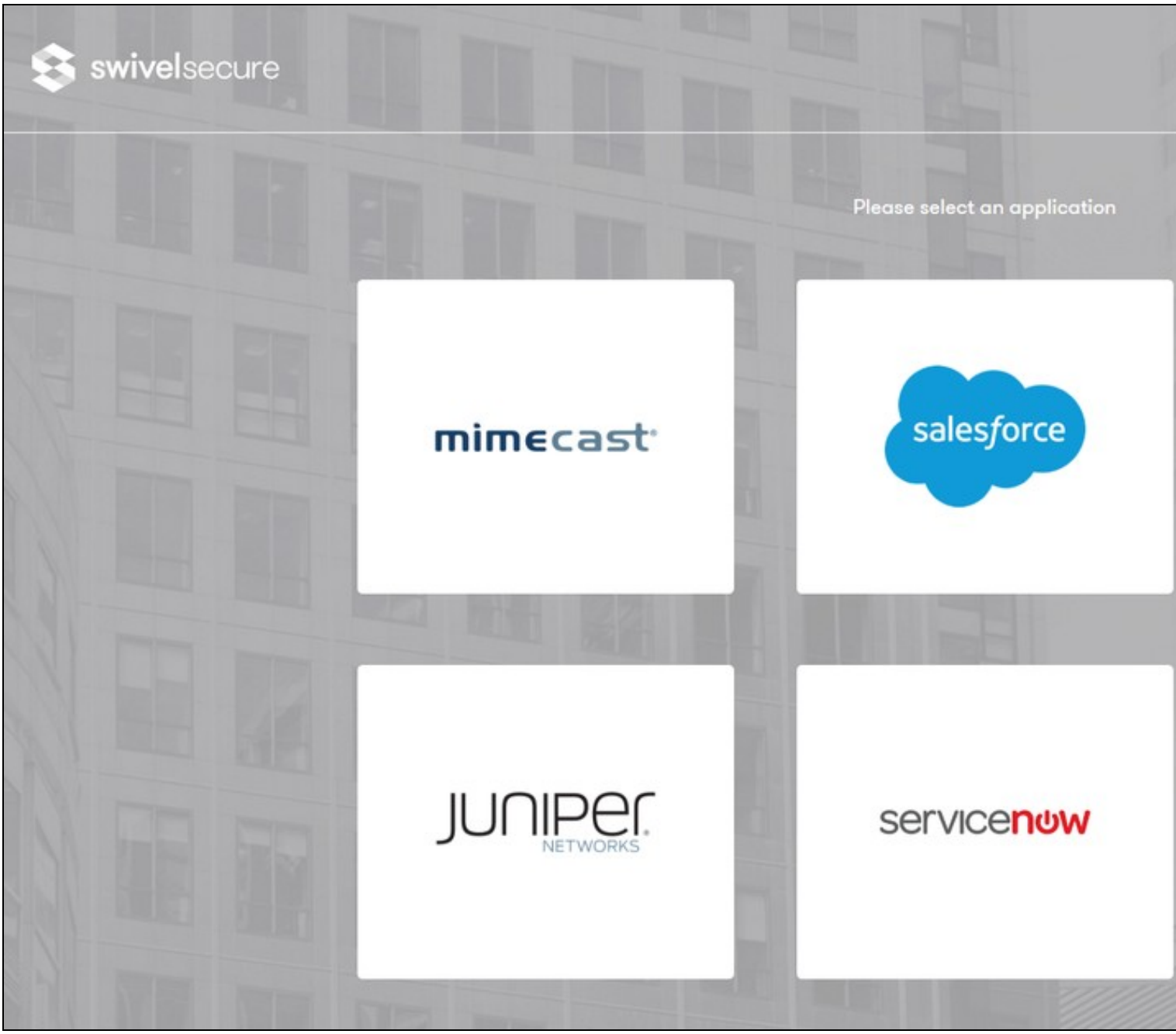
Login to the AuthControl Sentry Administration Console. Click Authentication Methods in the left hand menu. Click the Edit button against the Turing option in the list of Authentication Methods. Give this Authentication Method 100 points. This will mean that when a login attempt is made to the Google 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 Google via Swivel AuthControl Sentry

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

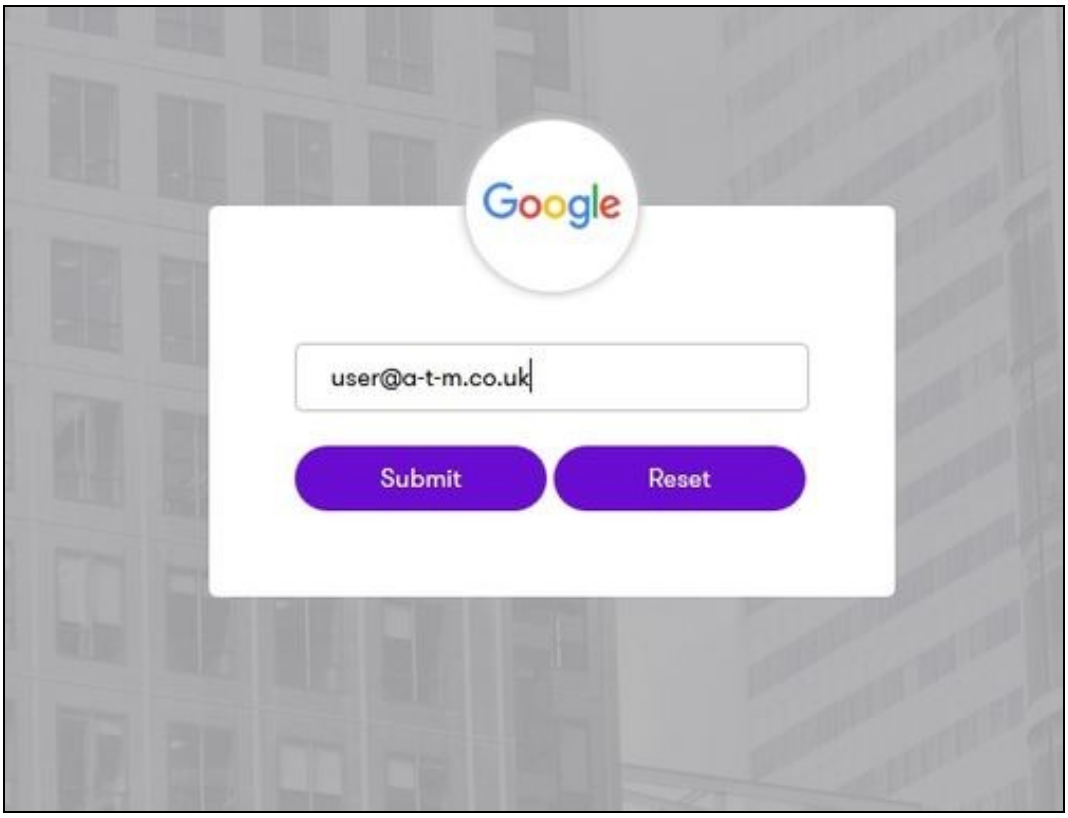
In a web browser, visit the the URL that you setup on AuthControl Sentry as Endpoint URL e.g. **https://docs.google.com/a/mycompanyname**

Alternatively you can 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 Google Icon on which you can click and proceed with authentication (as you would by going straight to the google page)

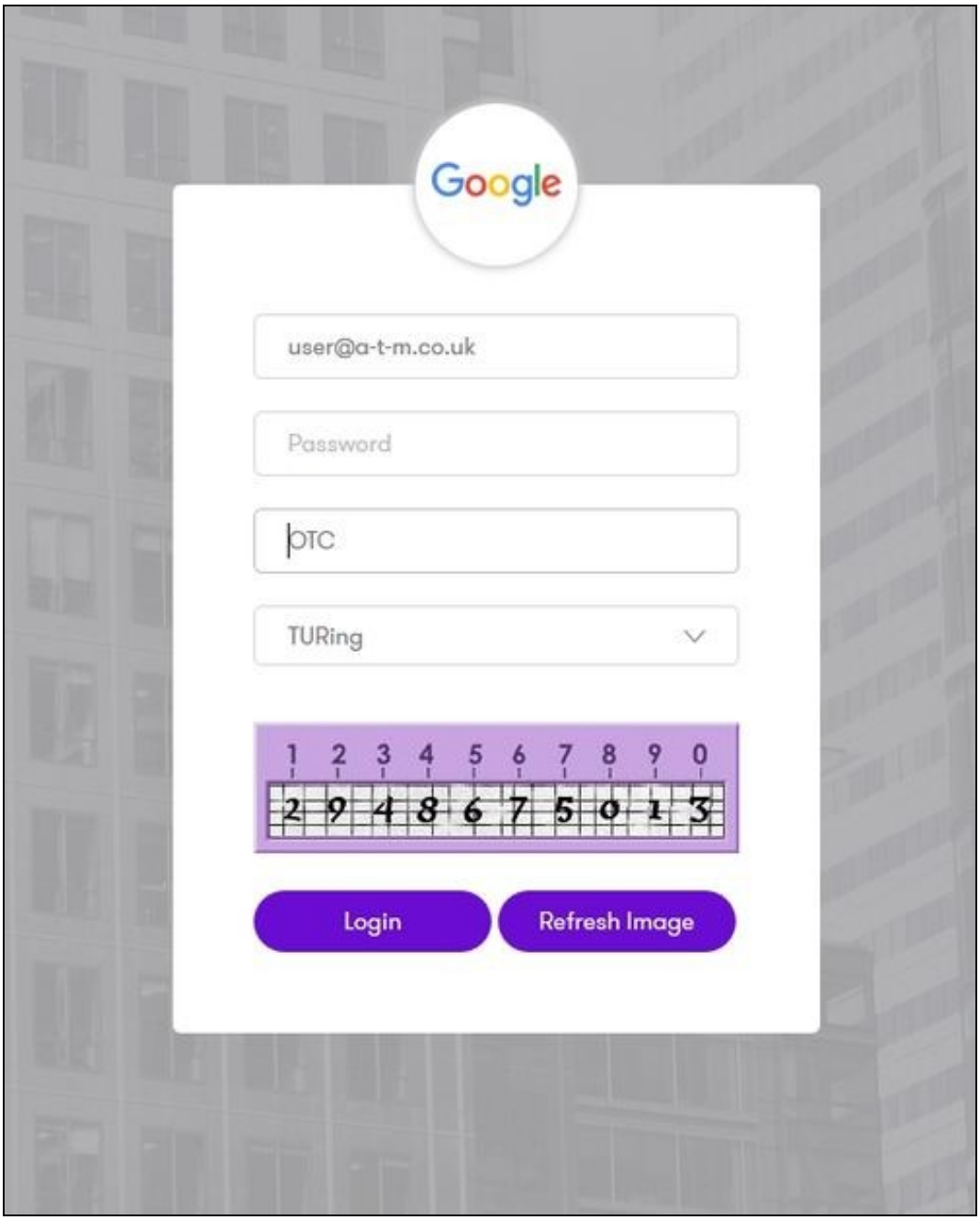


When you visit this URL you will notice that the domain should redirect to the identity provider login URL that you setup, once you have submitted your username. You should be presented with the page of the Authentication Method which can score enough points to match the points required by the Google Application definition.

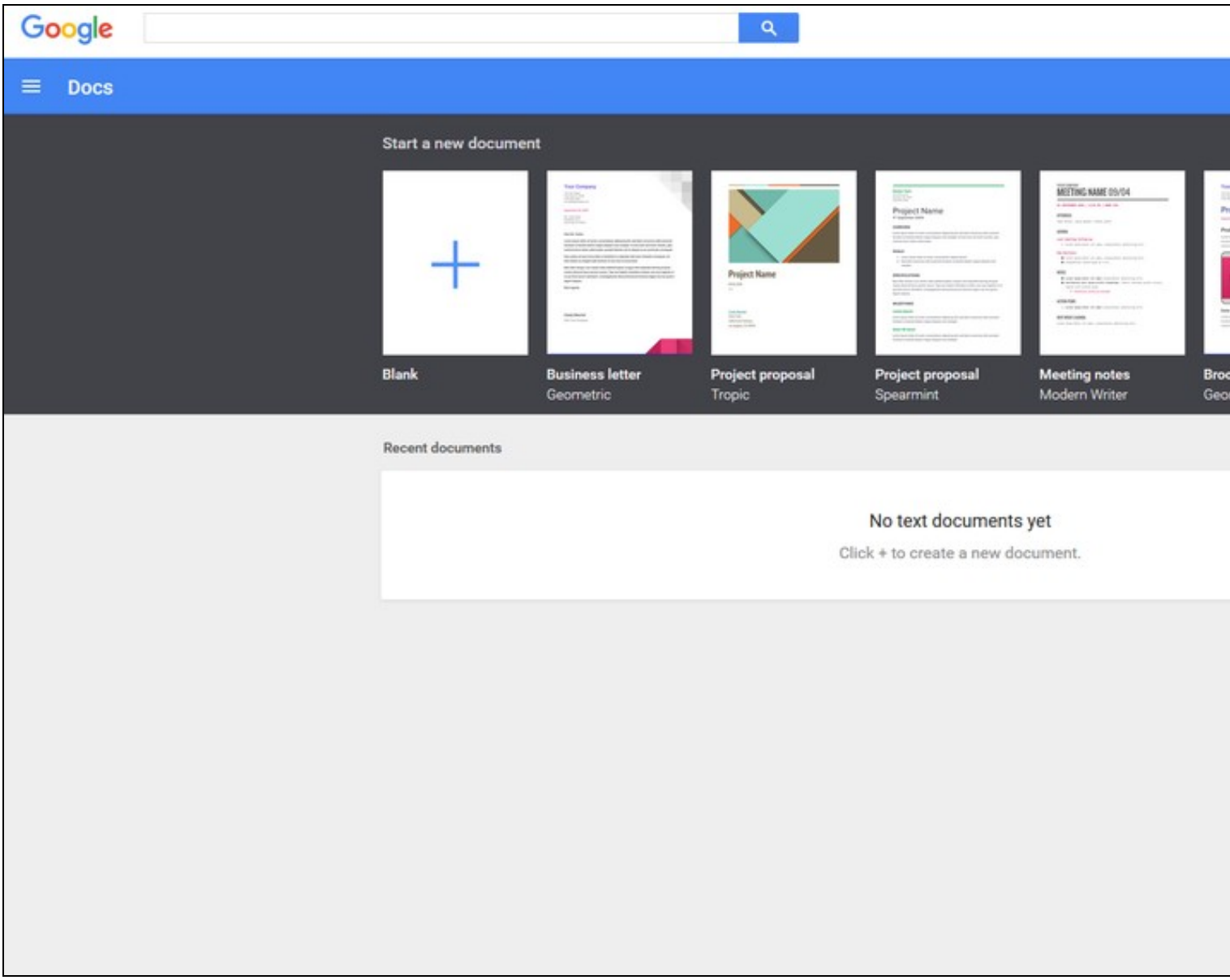
In this login example we are using the email as a username



After we enter the username we are prompted with another authentication method (in this example we use turing)



After we enter our authentication credentials we successfully will see the google docs 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 started for the image request;
- The Swivel AuthControl Sentry has a View Log menu item which provides details about the SAML assertion and response received from Google and can be useful for comparison with the Google SAML Assertion Validator output;

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 Google.com?
    - Does the Repository -> Attribute name being used actually map to a Repository attribute? Has a User Sync occurred in the Swivel Core since modifying this?