Sentry SSO with ServiceNow

Contents

Introduction

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

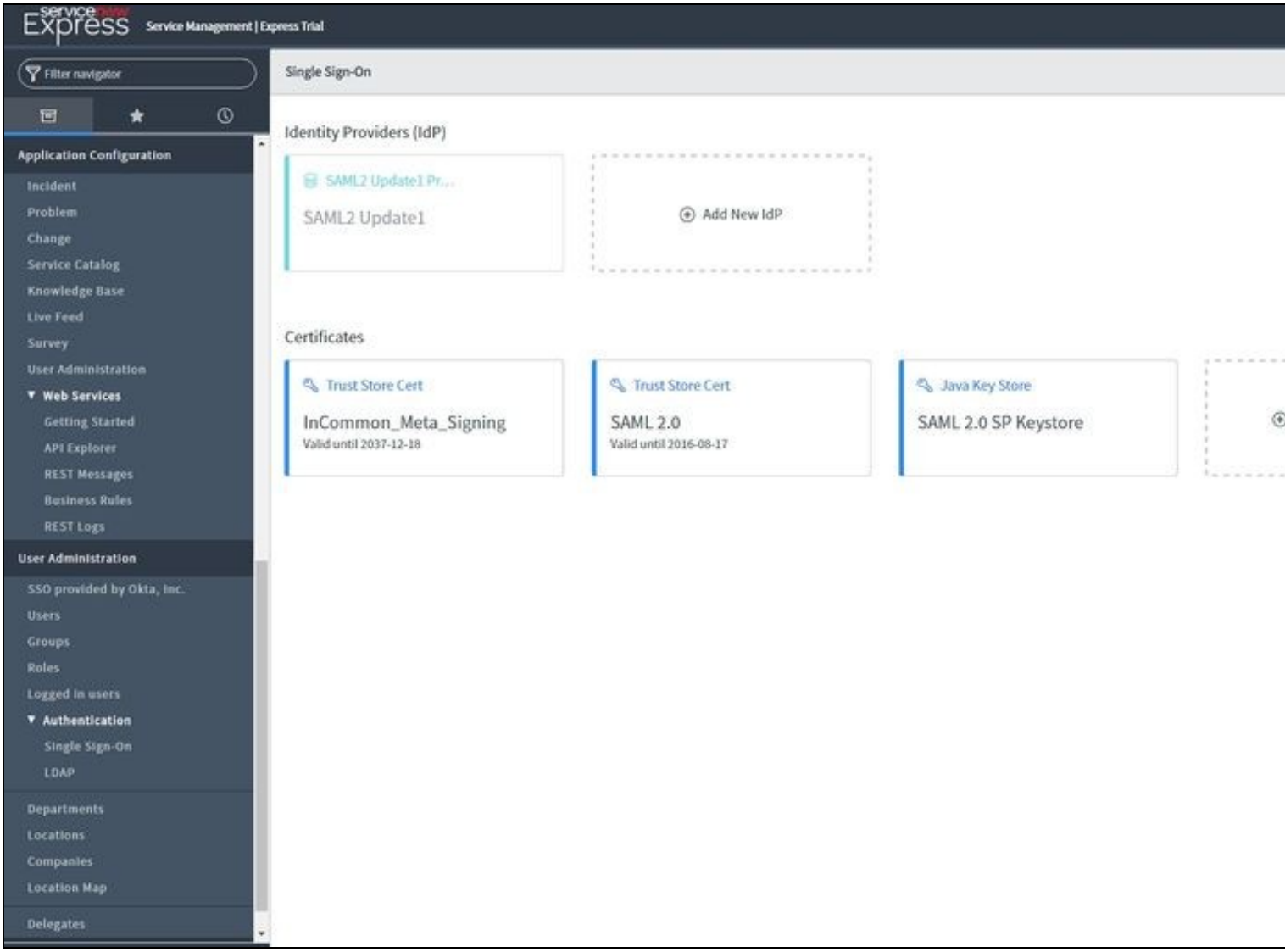
Setup AuthControl Sentry Keys

Before you are able to create a Single Sign On configuration on yourdomain.service-now.com, you will need to setup some Keys if they were not set up already. 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.

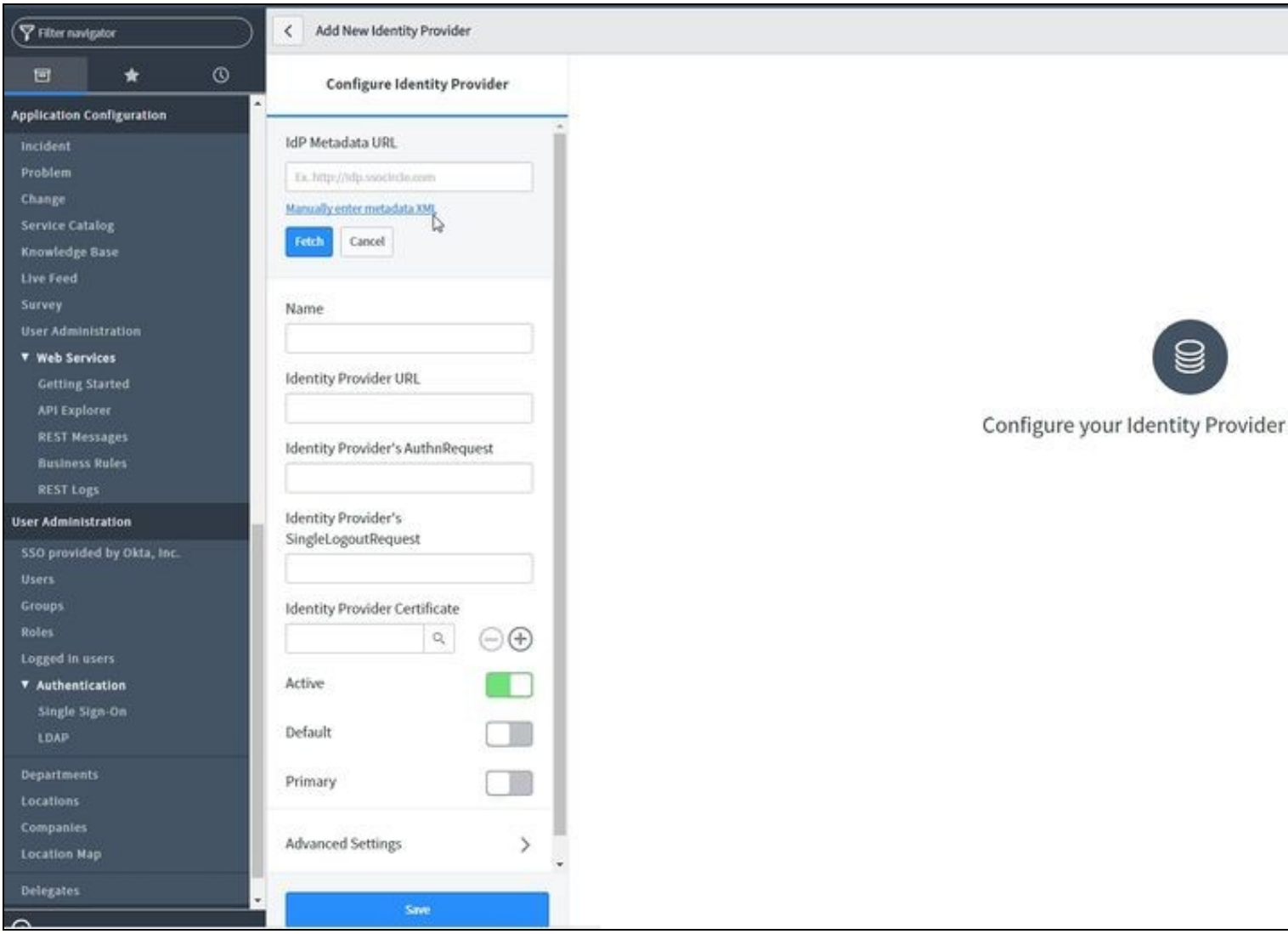
Setup SSO on ServiceNow

To configure SSO setting on your ServiceNow accounts you have to access your Admin console by simply going to **https://yourdomain.servicenow.com** You should see an Admin console.

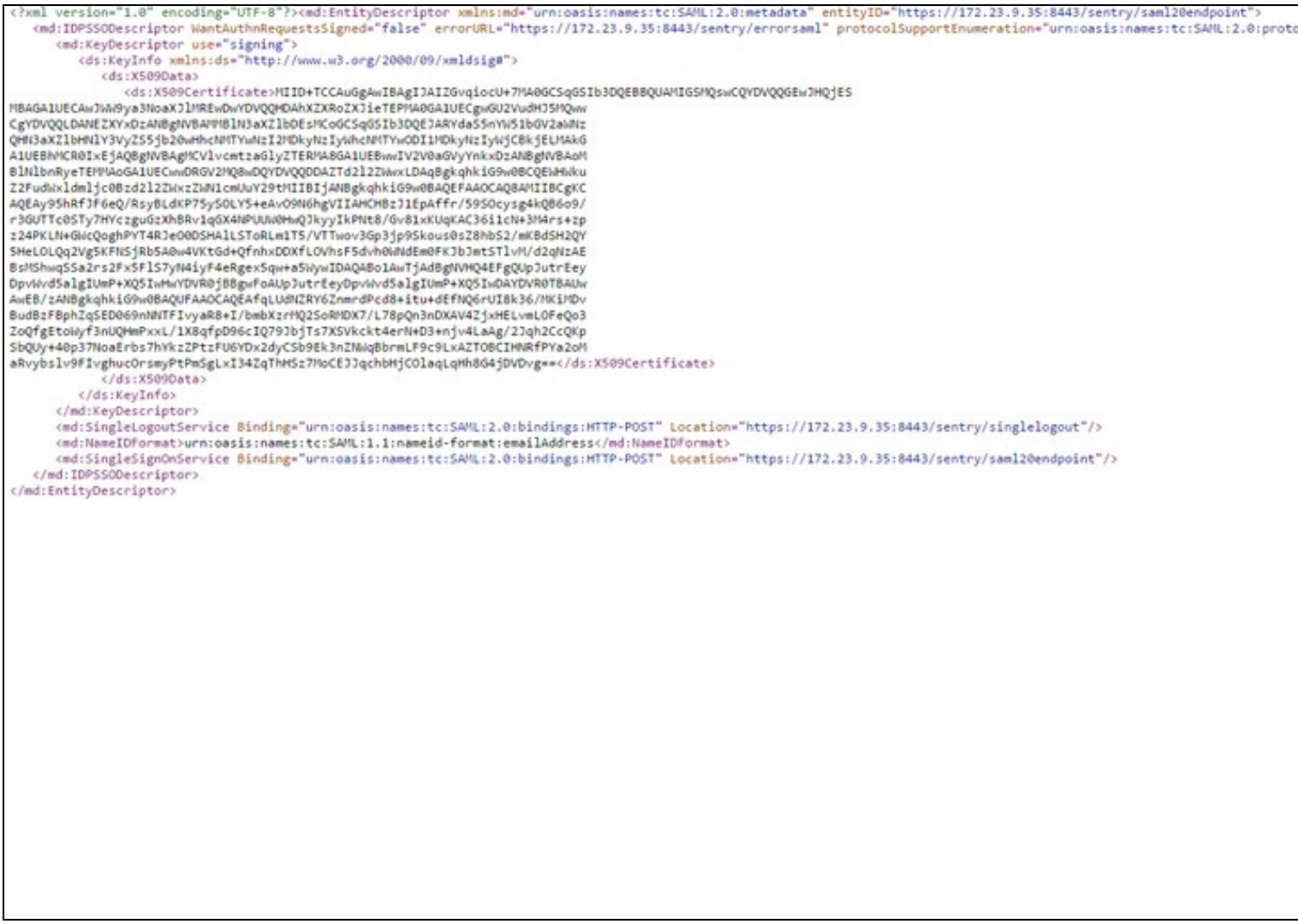
On the left menu you will see a User Administration section. When you click on the Single Sign-On you will be see the following screen. You have to enable the options displayed on the right, which are: "Enable multiple provider SSO" and "Enable Auto Importing of users from all identity providers into the user table" . Click on the button "Add New IdP" and select the User group for which to use SSO. For this example we are using "Swivel Users".



Click on the button "Add New IdP" and click "Manually enter metadata XML".



Now navigate to your AuthControl Sentry metadata page as below(*https://<FQDN_OF_SENTRY_SERVER>/sentry/metadata/generatedMetadata.xml*) and copy the content of this page.



```
<?xml version="1.0" encoding="UTF-8"?><md:EntityDescriptor xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata" entityID="https://172.23.9.35:8443/sentry/saml20endpoint">
   <md:IDPSSODescriptor WantAuthnRequestsSigned="false" errorURL="https://172.23.9.35:8443/sentry/errorsaml" protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:proto
      <md:KeyDescriptor use="signing">
         <ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
            <ds:X509Data>
               <ds:X509Certificate>MIID+TCCAuGgAwIBAgIJAIZGvqiocU+7MA0GCSqGSIb3DQEBBQUAMIGSMQswCQYDVQQGEwJHQjES
MBAGA1UECAwJWW9ya3NoaXJlMREwDwYDVQQHDAhXZXRoZXJieTEPMA0GA1UECgwGU2VudHJ5MQww
CgYDVQQLDANEZXYxDzANBgNVBAMMBlNJaXZlbDEsMCoGCSqGSIb3DQEJARYdaS5nYW51bGV2aWNz
QHN3aXZlbHNlY3VyZS5jb20wHhcNMTYwNzI2MDkyNzIyWhcNMTYwODI1MDkyNzIyWjCBkjELMAkG
A1UEBhMCR0IxEjAQBgNVBAgMCVlvcmtzaGlyZTERMA8GA1UEBwwIV2V0aGVyYnkxDzANBgNVBAoM
BlNlbnRyeTEMMAoGA1UECwwDRGV2MQ8wDQYDVQQDDAZTd2l2ZWwxLDAqBgkqhkiG9w0BCQEWHWku
Z2FudWxldmljc0Bzd2l2ZWxzZWN1cmUuY29tMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKC
AQEAy95hRfJf6eQ/RsyBLdKP75ySOLY5+eAvO9N6hgVIIAHCHBzJ1EpAffr/59SOcysg4kQB6o9/
r3GUTTc0STy7HYczguGzXhBRv1qGX4NPUUW0HwQJkyyIkPNt8/Gv81xKUqKAC36i1cN+3M4rs+zp
z24PKLN+GWcQoghPYT4RJeO0DSHAlLSToRLm1T5/VTTwov3Gp3jp9Skous0sZ8hbS2/mKBdSH2QY
5HeLOLQq2Vg5KFNSjRb5A0w4VKtGd+QfnhxDDXfLOVhsF5dvh0WNdEm0FKJbJmtSTlvM/d2qNzAE
BsMShwqSSa2rs2Fx5FlS7yN4iyF4eRgex5qw+a5WywIDAQABo1AwTjAdBgNVHQ4EFgQUpJutrEey
DpvWvd5algIUmP+XQ5IwHwYDVR0jBBgwFoAUpJutrEeyDpvWvd5algIUmP+XQ5IwDAYDVR0TBAUw
AwEB/zANBgkqhkiG9w0BAQUFAAOCAQEAfqLUdNZRY6ZnmrdPcd8+itu+dEfNQ6rUI8k36/MKiMDv
BudBzFBphZqSED069nNNTFIvyaR8+I/bmbXzrMQ2SoRMDX7/L78pQn3nDXAV4ZjxHELvmLOFeQo3
ZoQfgEtoWyf3nUQHmPxxL/1X8qfpD96cIQ79jbjTs7XSVkckt4erN+D3+njv4LaAg/2Jqh2CcQKp
SbQUy+40p37NoaErbs7hYkzZPtzFU6YDx2dyCSb9Ek3nZNWqBbrmLF9c9LxAZTOBCIHNRfPYa2oM
aRvybslv9fIvghucOrsmyPtPmSgLxI34ZqThHSz7MoCEJJqchbHjCOlaqLqHh8G4jDVDvg==</ds:X509Certificate>
            </ds:X509Data>
         </ds:KeyInfo>
      </md:KeyDescriptor>
      <md:SingleLogoutService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST" Location="https://172.23.9.35:8443/sentry/singlelogout"/>
      <md:NameIDFormat>urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress</md:NameIDFormat>
      <md:SingleSignOnService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST" Location="https://172.23.9.35:8443/sentry/saml20endpoint"/>
   </md:IDPSSODescriptor>
</md:EntityDescriptor>
```


Return back on the ServiceNow setup

IdP Metadata XML - *Paste copied metadata from your AuthControl Sentry* and click Fetch. After that the following fields will be set automatically

Identity Provider URL

Identity Provider's SingleLogoutRequest

Identity Provider Certificate

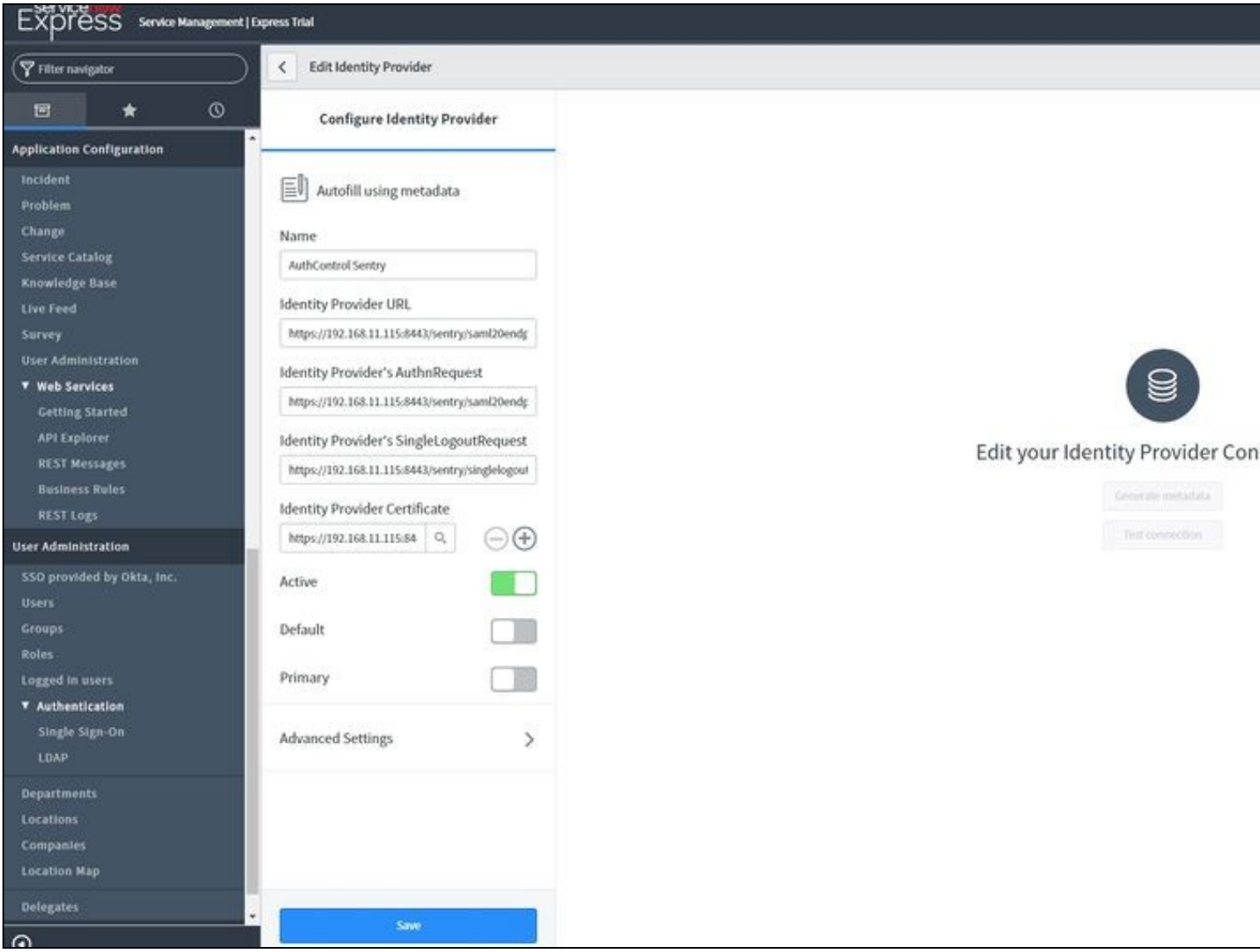
You will have to fill the following ones for your AuthControl Sentry such as:

Identity Provider's AuthnRequest - *Copy and paste the value set on "Identity Provider URL"*

Active - Enabled

Default - Enabled

Primary - Enabled



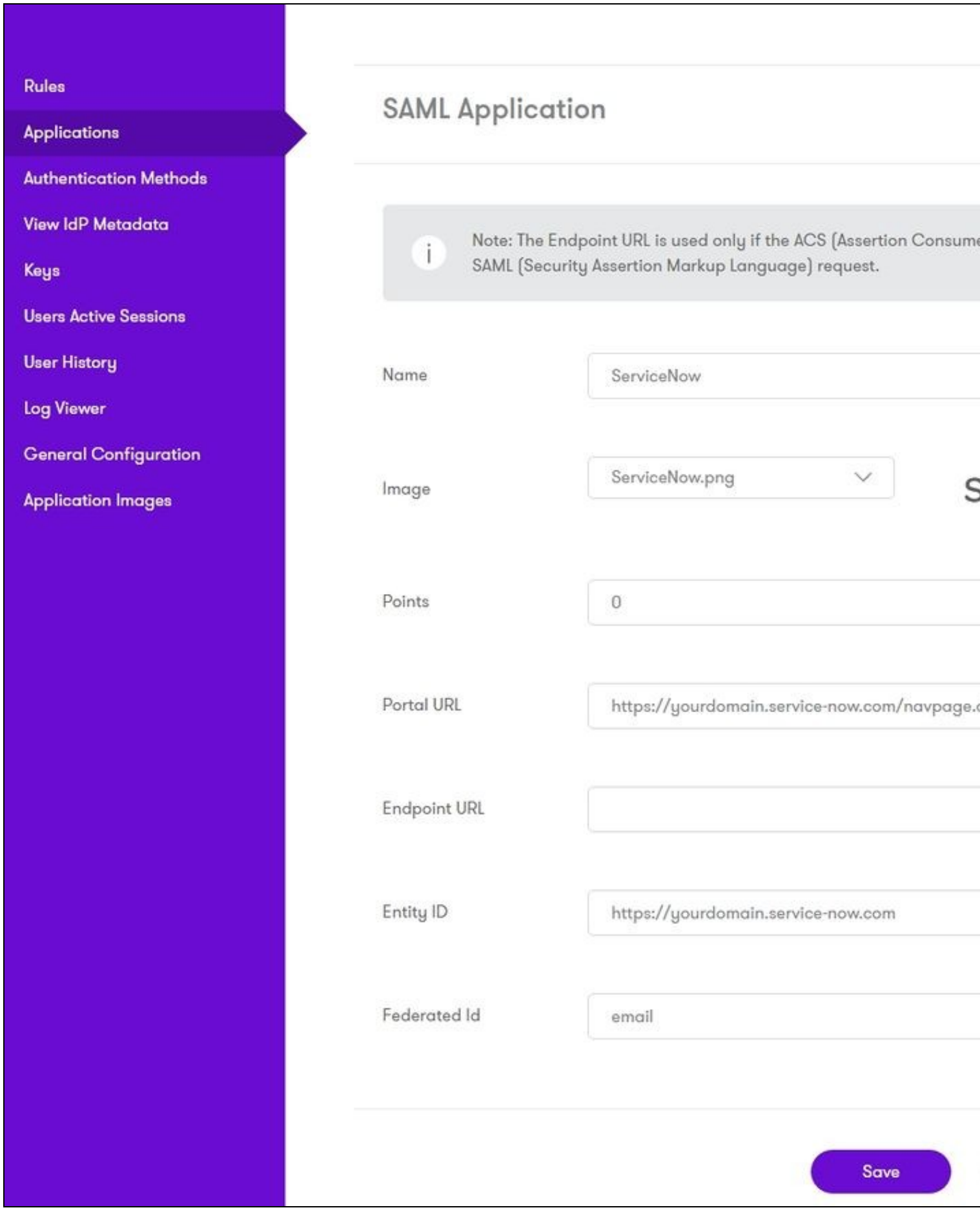
After you have entered all the details as above click Save. You can test the connection after setting up Auth Control Sentry

Configure Check Password with Repository on the Swivel Core

In order to check the user?s Active Directory password, ensure that the local Agent defined under Server -> Agents has got the Check Password with repository checkbox enabled. When an authentication occurs in AuthControl Sentry, the Active Directory password will then be passed to Active Directory for verification.

Setup AuthControl Sentry Application definition

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



Name: ServiceNow(Type an Arbitrary name for this Application)

Image: ServiceNow.jpg(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)

Portal URL: (this Portal URL is ServiceNow login URL which you can usually access on: https://yourdomain.service-now.com/navpage.do

Endpoint URL: N/A

Entity ID: https://yourdomain.service-now.com (Entity ID is the one defined on ServiceNow > User Administration > Single Sign-On > AuthControl Sentry Idp > Advanced Settings: Entity ID)

Federated Id: email

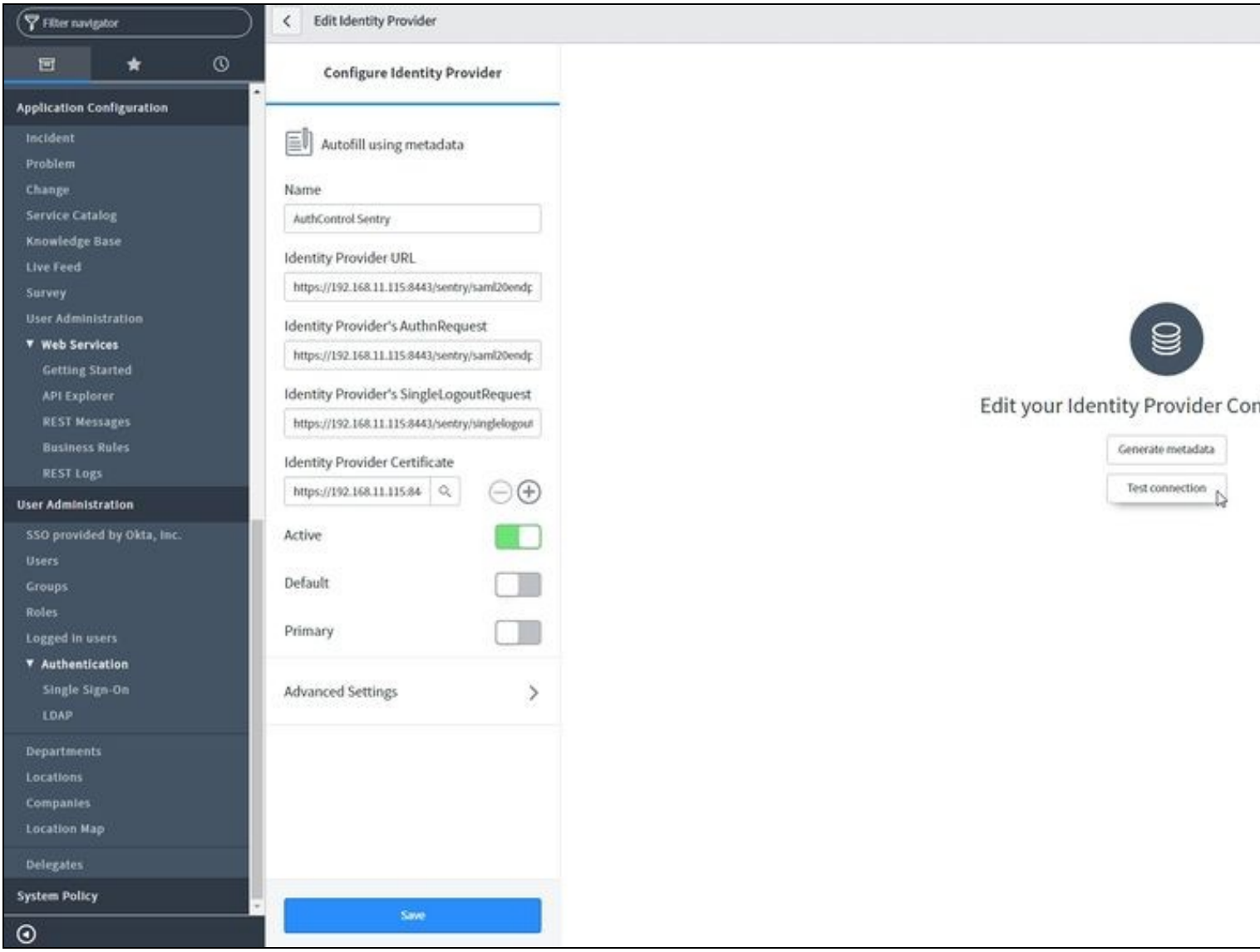
Setup AuthControl Sentry Authentication definition

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

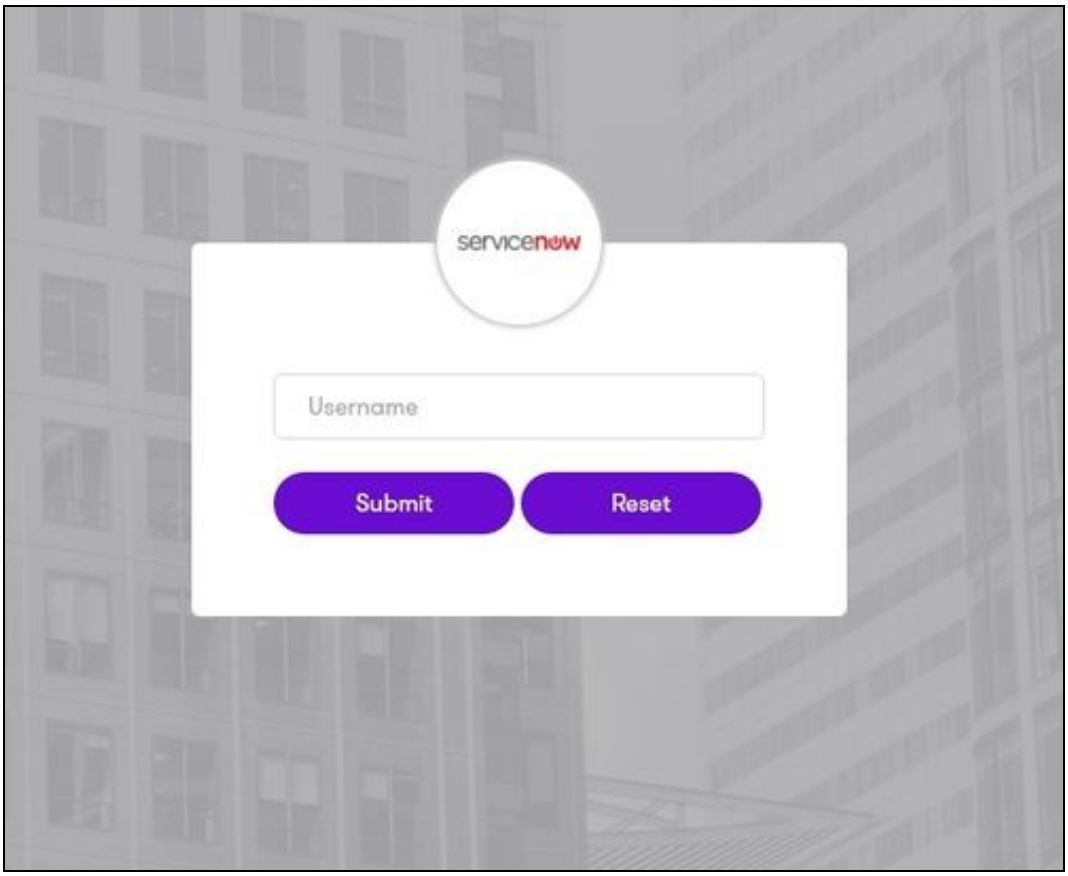
Login to the AuthControl Sentry Administration Console. Click Authentication Methods in the left hand menu. Click the Edit button against the Turing option in the list of Authentication Methods. Give this Authentication Method 100 points. This will mean that when a login attempt is made to the ServieNow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

Testing connection with ServiceNow tool

ServiceNow provides a tool to test the connection. Go to User Administration > Single Sign-On and click AuthControl Sentry Idp. After that click Test connection.

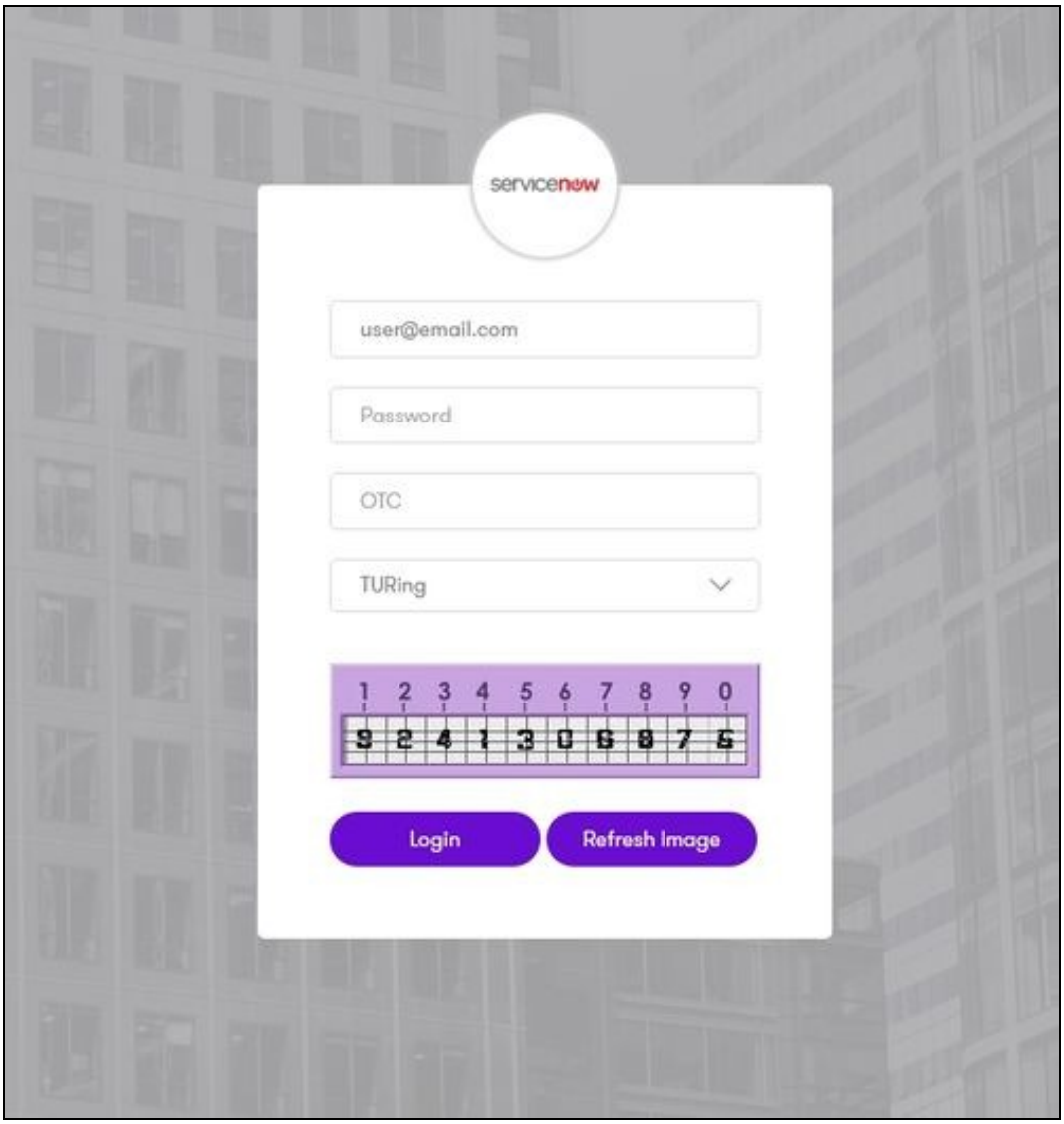


A new window will be displayed that will redirect to AuthControl sentry username page.



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 ServiceNow Application definition.

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



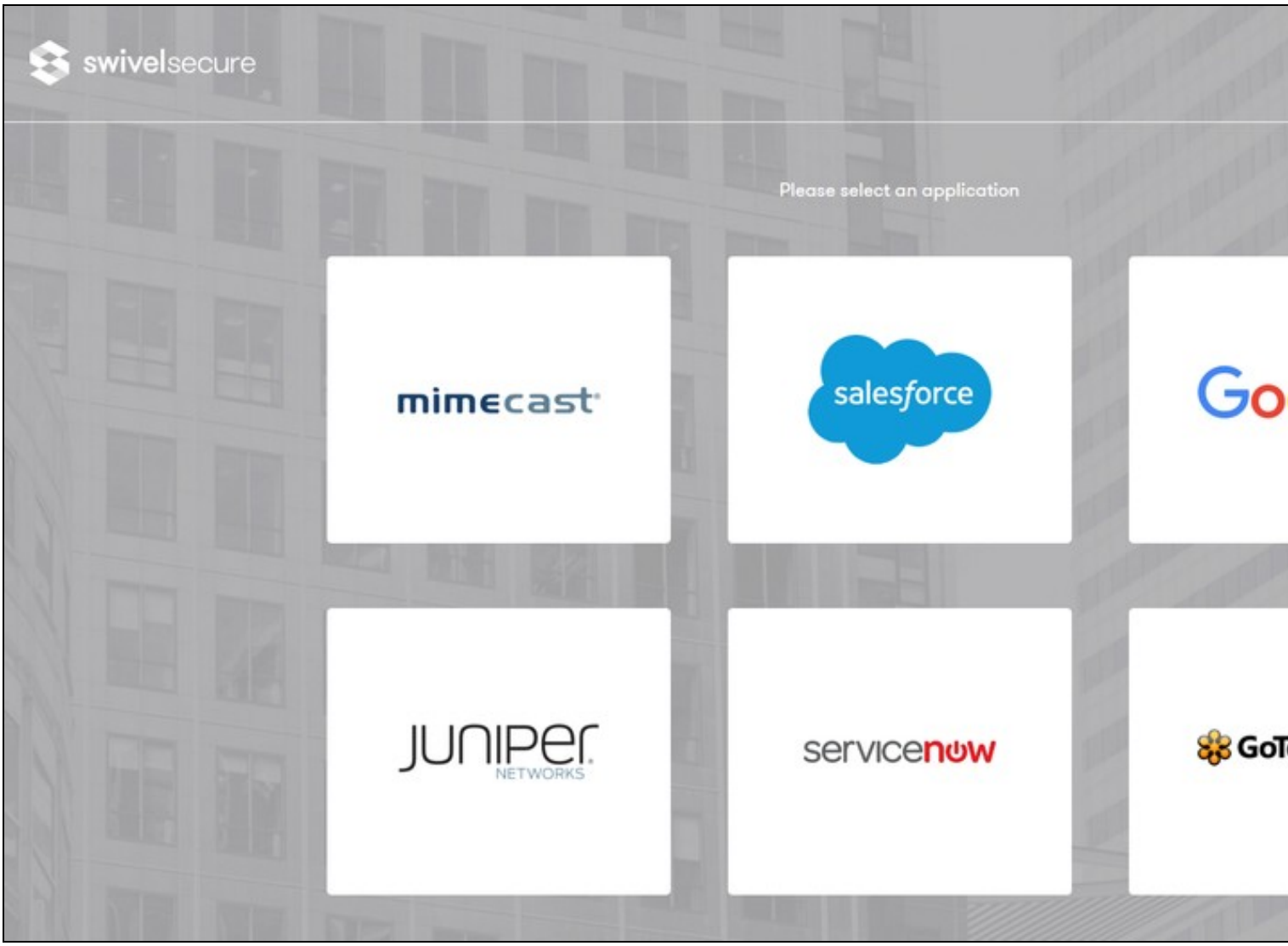
After we enter our authentication credentials we will see a logout screen. Close that window and on the ServiceNow page click View Log. Check that the logs indicate that the SAML authentication was successful.

Testing authentication to ServiceNow via Swivel AuthControl Sentry

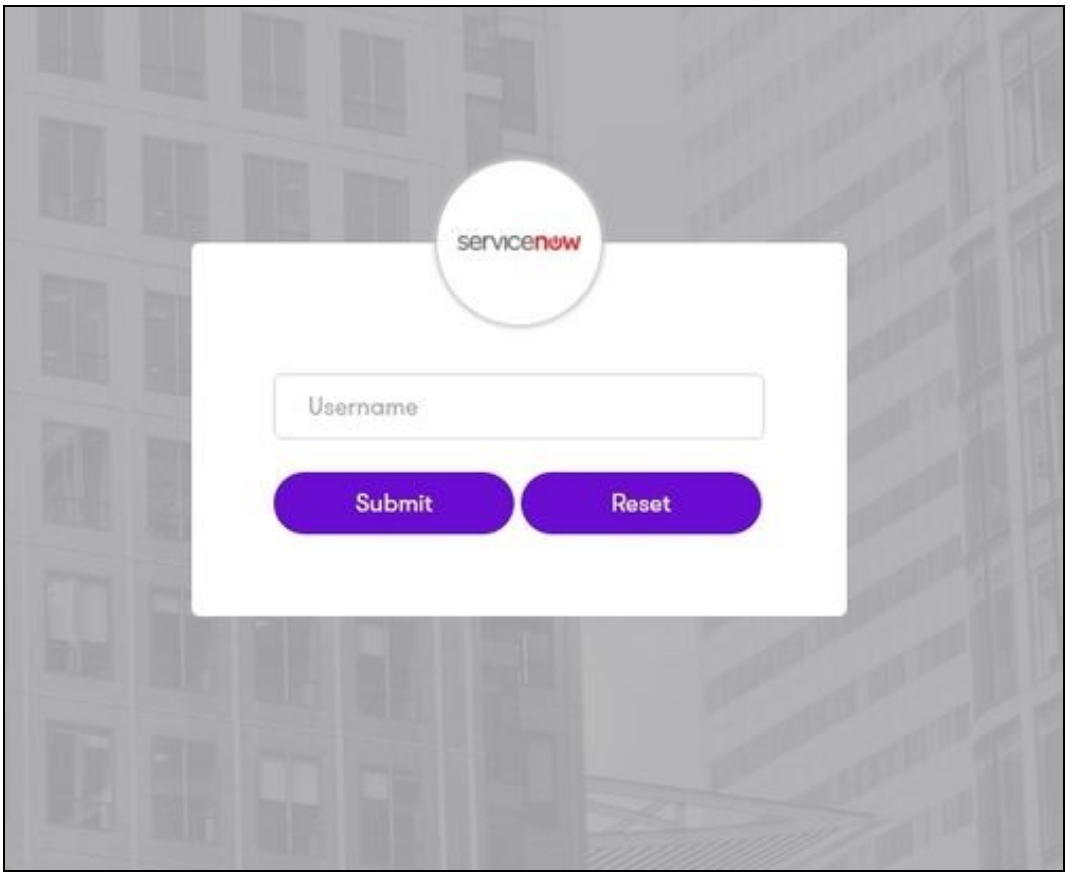
This should be the final step after all previous elements have been configured.

In a web browser, visit the the URL that you setup on AuthControl Sentry as Endpoint URL e.g. **https://yourdomain.service-now.com/navpage.do**

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

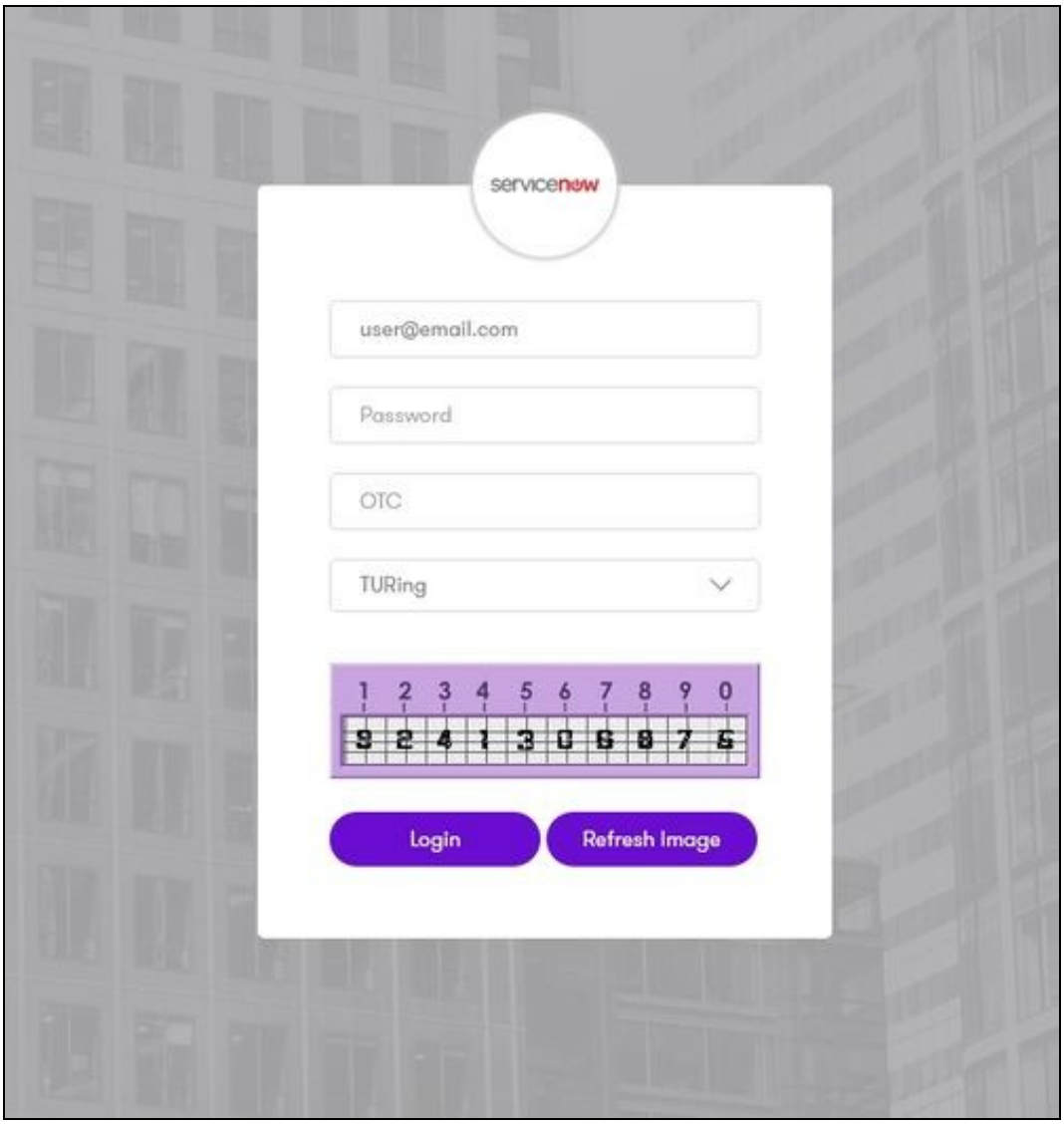


When you visit this URL you will notice that the domain should redirect to the identity provider login URL that you setup.



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 ServiceNow Application definition.

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



After we enter our authentication credentials we successfully will see the ServiceNow 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 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 ServiceNow
- The ServiceNow has a Test Connection feature that provides details about the SAML response received from AuthControl Sentry

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.

If you have issues login in with then SAML authentication to the admin console you can always access by https://yourdomain.service-now.com/side_door.do

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 Metadata been uploaded to the ServiceNow?
    - 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?