Sentry SSO with Citrix Netscaler

Contents

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

Introduction

This article explains how to integrate a Citrix Netscaler with Sentry via SAML.

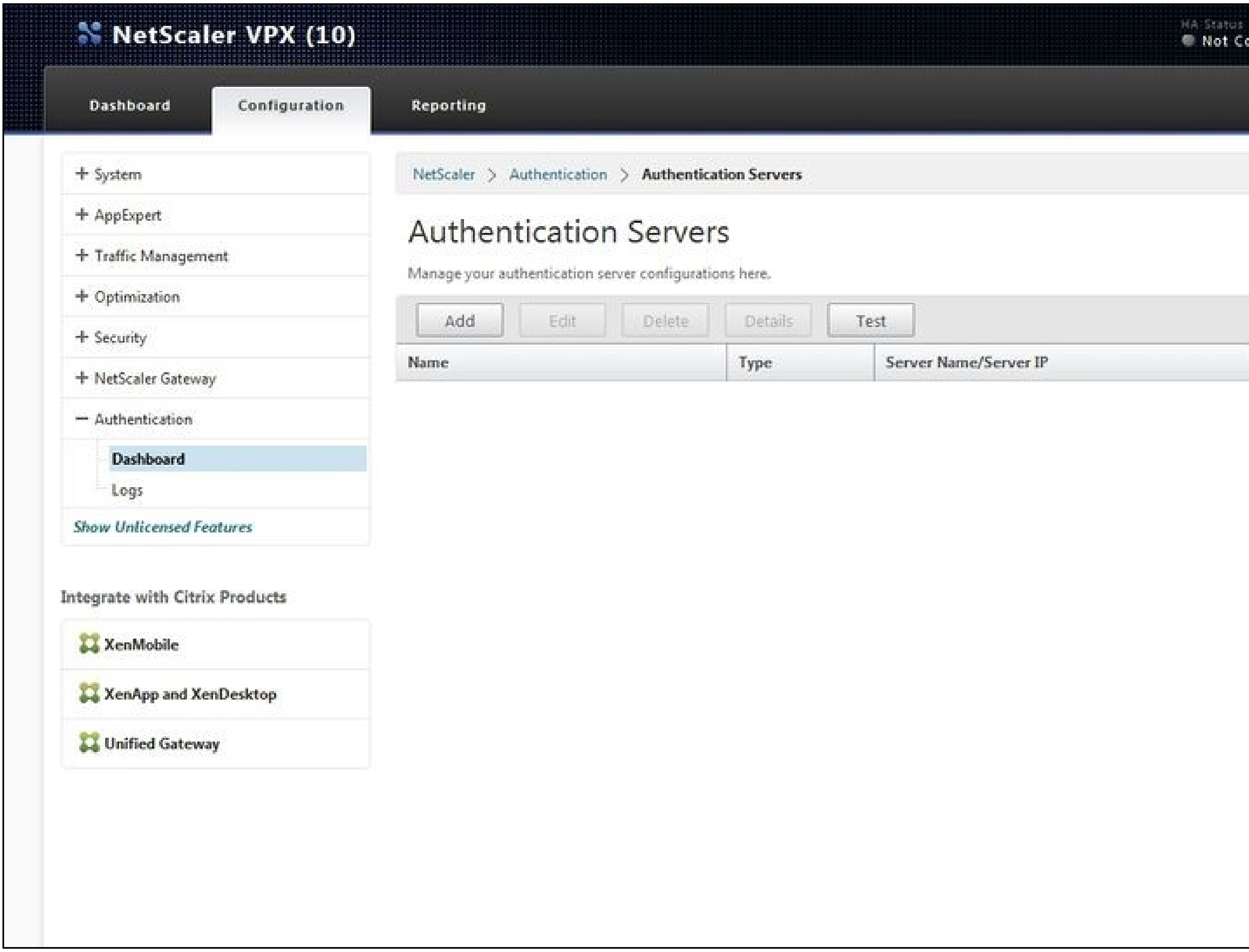
It assumes knowledge of how to configure the Netscaler and that a Virtual Server has been already created, missing just the SAML authentication configuration.

Setup AuthControl Sentry Keys

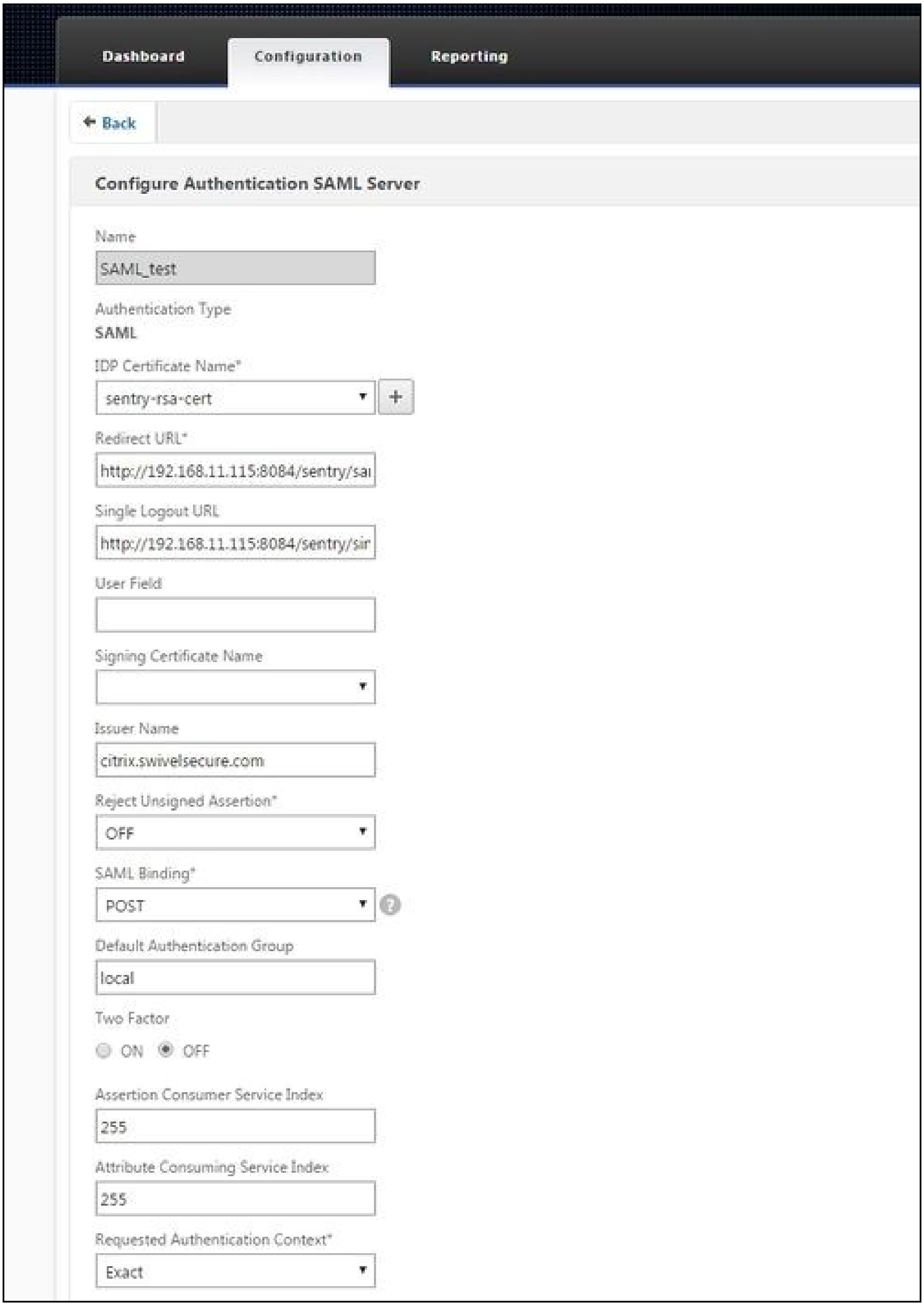
Before you are able to create a Single Sign On configuration on your Netscaler Citrix account, you will need to setup some Keys. Please see a separate article: HowToCreateKeysOnCmi. You will need the certificate you generate in a later section of this article. This can be retrieved from the View Keys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

Setup SAML SSO on Citrix Netscaler

To configure SAML SSO settings on your Citrix Netscaler account you have to access your Admin console. You should see an Admin console with an option "Authentication > Dashboard" similar to the one below:



On the Authentication Servers screen you have to click on the Add button. You will be shown a create authentication server screen with a Choose Server Type options where you have to click on "SAML".



Configure Authentication SAML Server

Name
SAML_test

Authentication Type
SAML

IDP Certificate Name*
sentry-rsa-cert

Redirect URL*
http://192.168.11.115:8084/sentry/sa

Single Logout URL
http://192.168.11.115:8084/sentry/si

User Field

Signing Certificate Name

Issuer Name
citrix.swivelsecure.com

Reject Unsigned Assertion*
OFF

SAML Binding*
POST

Default Authentication Group
local

Two Factor
○ ON ● OFF

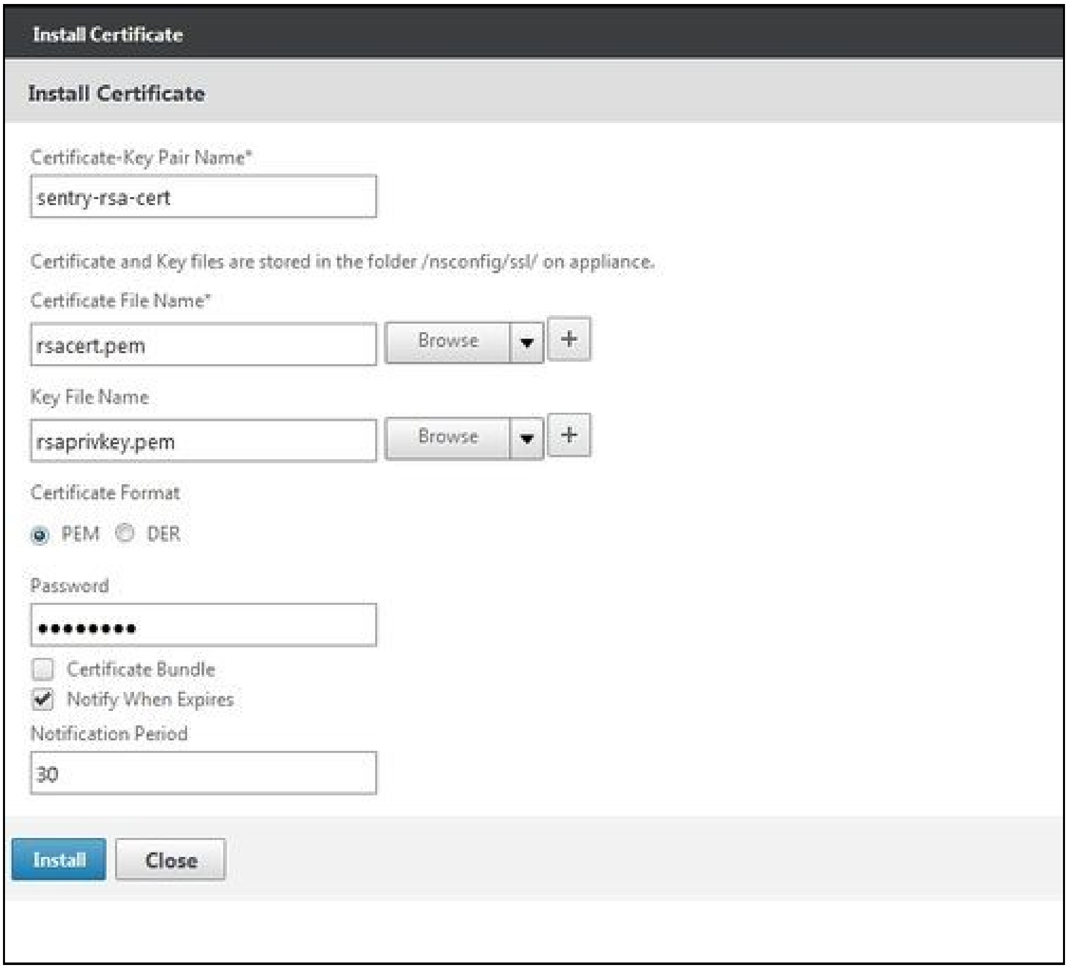
Assertion Consumer Service Index
255

Attribute Consuming Service Index
255

Requested Authentication Context*
Exact

You will have to enter a name for the Authentication SAML Server and fill in the details for your AuthControl Sentry such as:

IDP Certificate Name - *Click on + and a screen like the one displayed below should be displayed. Browse to the RSA PEM files created earlier to upload the certificate and select PEM as a Certificate Format:*



Install Certificate

Install Certificate

Certificate-Key Pair Name*: sentry-rsa-cert

Certificate and Key files are stored in the folder /nsconfig/ssl/ on appliance.

Certificate File Name*: rsacert.pem

Key File Name: rsaprivkey.pem

Certificate Format: ● PEM ○ DER

Password: •••••••••

□ Certificate Bundle

☑ Notify When Expires

Notification Period: 30

After you have entered all the certificate details click Install

Set the Redirect and Single Logout 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

Redirect URL - *https://<FQDN_OF_SENTRY_SERVER>/sentry/saml20endpoint*

Single Logout URL - *https://<FQDN_OF_SENTRY_SERVER>/sentry/singlelogout*

Issuer Name - *E.g. citrix.companyname.com*

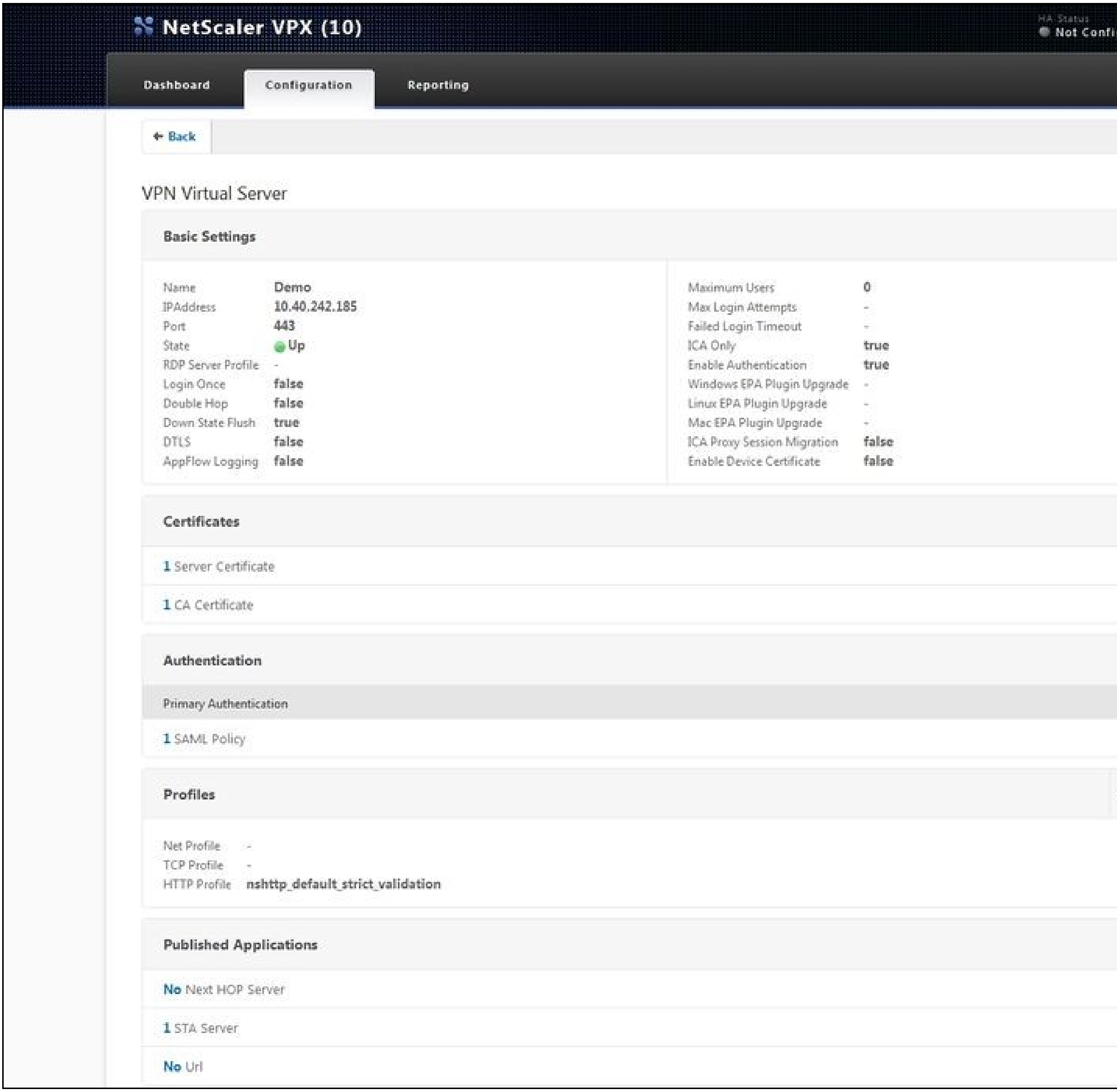
(The value set in here will be used to configure the Citrix Netscaler application on AuthControl Sentry)

Signature Algorithm - RSA-SHA256

Digest Method - SHA1

After you have entered all the details as above click Create

Now the SAML authentication server has been created. To configure the Virtual Server used to log in to use SAML authentication, select Netscaler Gateway > Virtual Servers and click Edit. You should see a screen like the one below:



VPN Virtual Server

Basic Settings

Name	Demo	Maximum Users	0
IPAddress	10.40.242.185	Max Login Attempts	-
Port	443	Failed Login Timeout	-
State	● Up	ICA Only	true
RDP Server Profile	-	Enable Authentication	true
Login Once	false	Windows EPA Plugin Upgrade	-
Double Hop	false	Linux EPA Plugin Upgrade	-
Down State Flush	true	Mac EPA Plugin Upgrade	-
DTLS	false	ICA Proxy Session Migration	false
AppFlow Logging	false	Enable Device Certificate	false

Certificates

1 Server Certificate

1 CA Certificate

Authentication

Primary Authentication

1 SAML Policy

Profiles

Net Profile	-
TCP Profile	-
HTTP Profile	nshttp_default_strict_validation

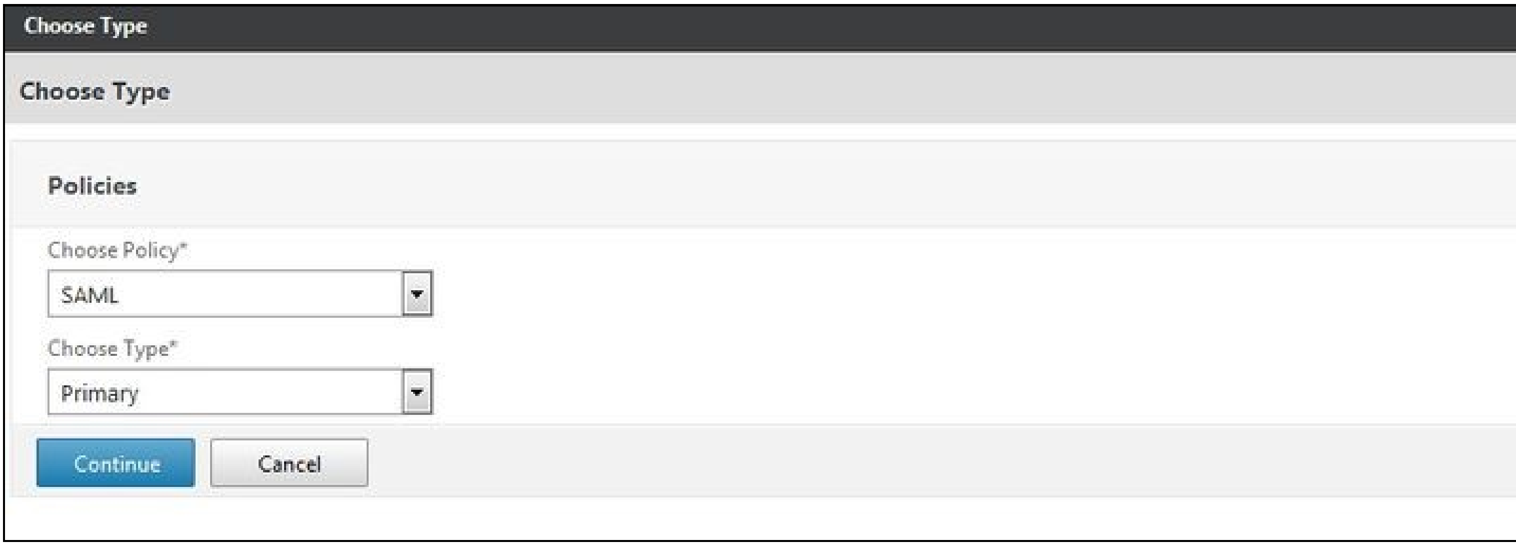
Published Applications

No Next HOP Server

1 STA Server

No Url

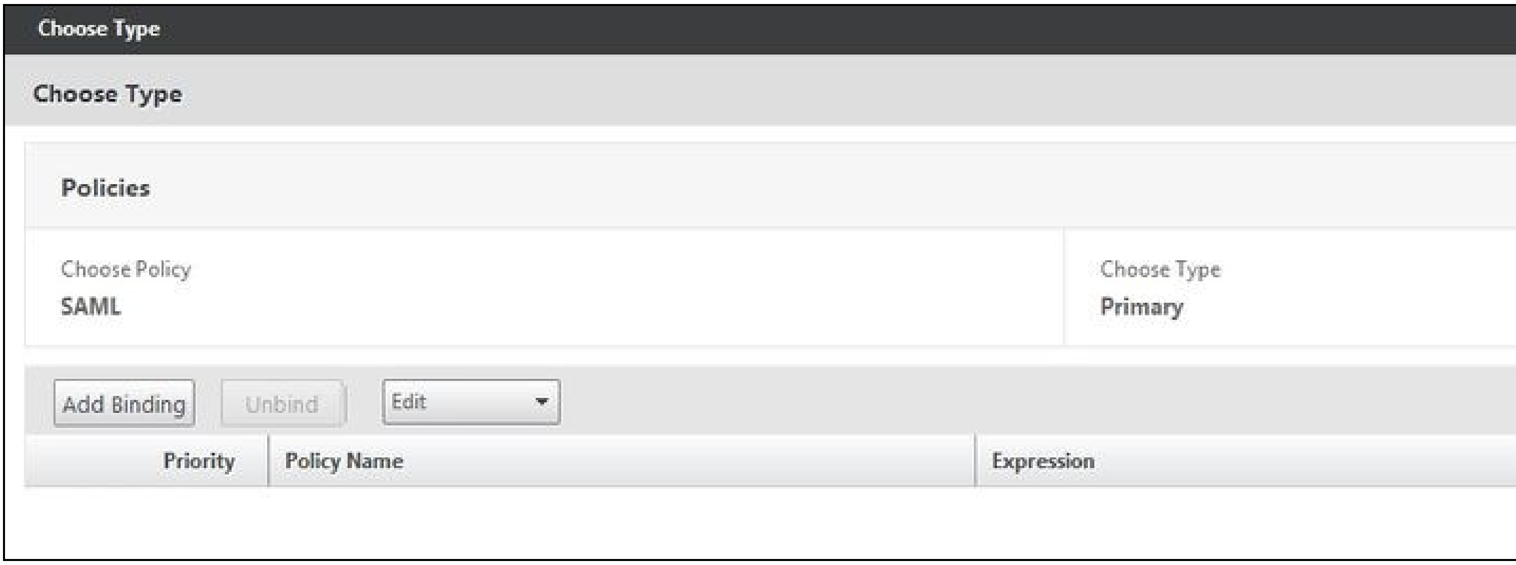
To add the SAML authentication server click + on the Authentication section. Select Policy as SAML and type Primary. Click the Continue button.



Choose Policy*: SAML

Choose Type*: Primary

The below screen will be displayed. Click + to add Add Binding:

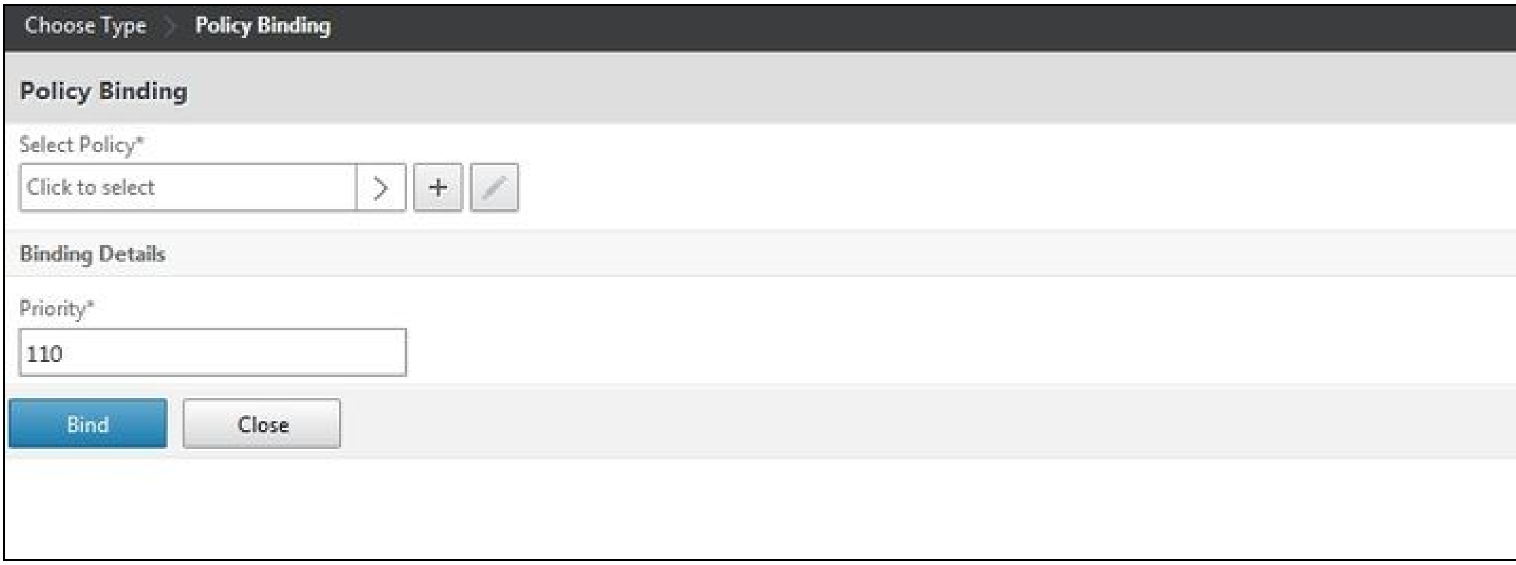


Choose Policy: SAML

Choose Type: Primary

Priority	Policy Name	Expression

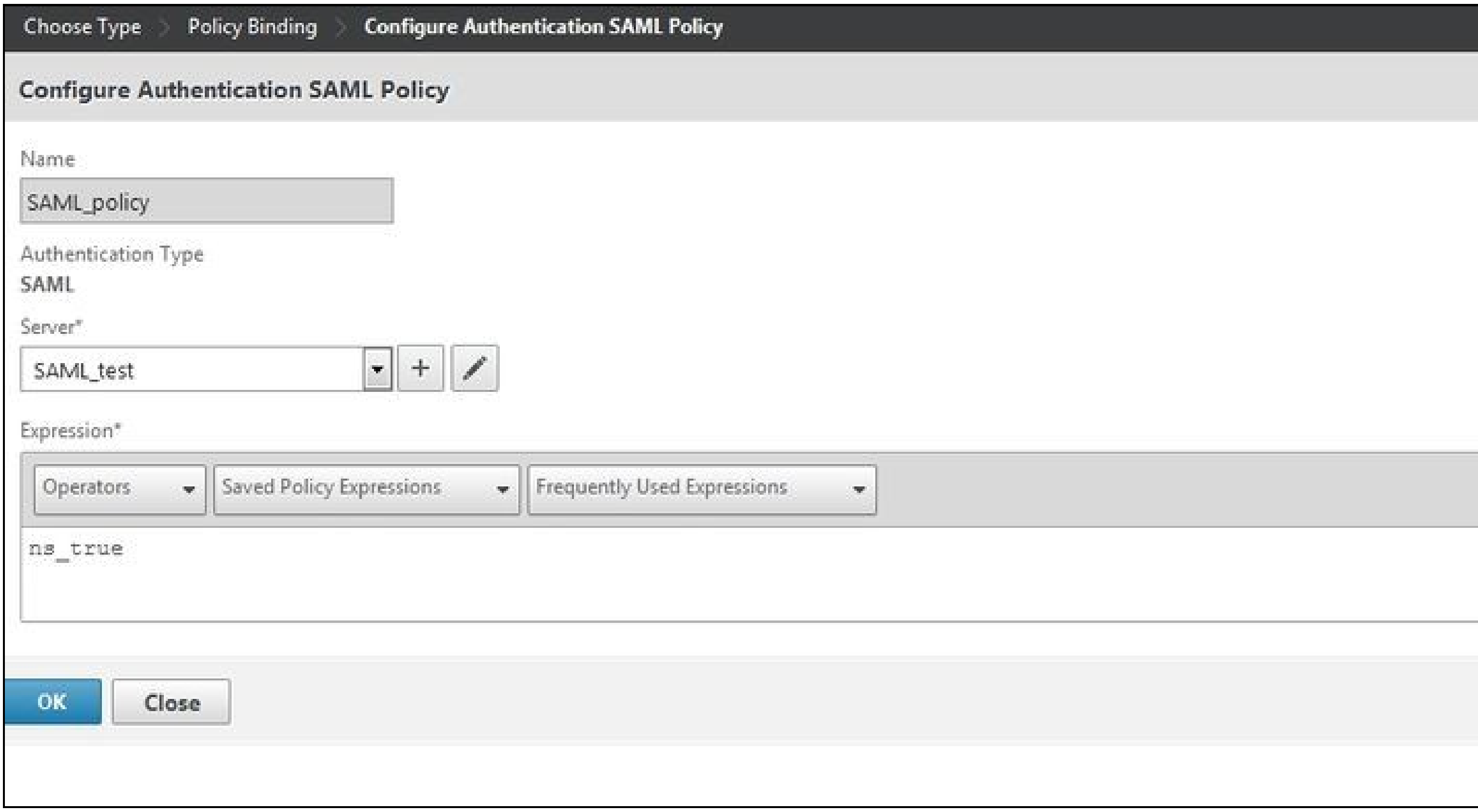
Click + add to add a new Policy Binding:



Select Policy*: Click to select

Priority*: 110

Set a name for the SAML policy, select the SAML server configured before and add on Expression ns_true.



Configure Authentication SAML Policy

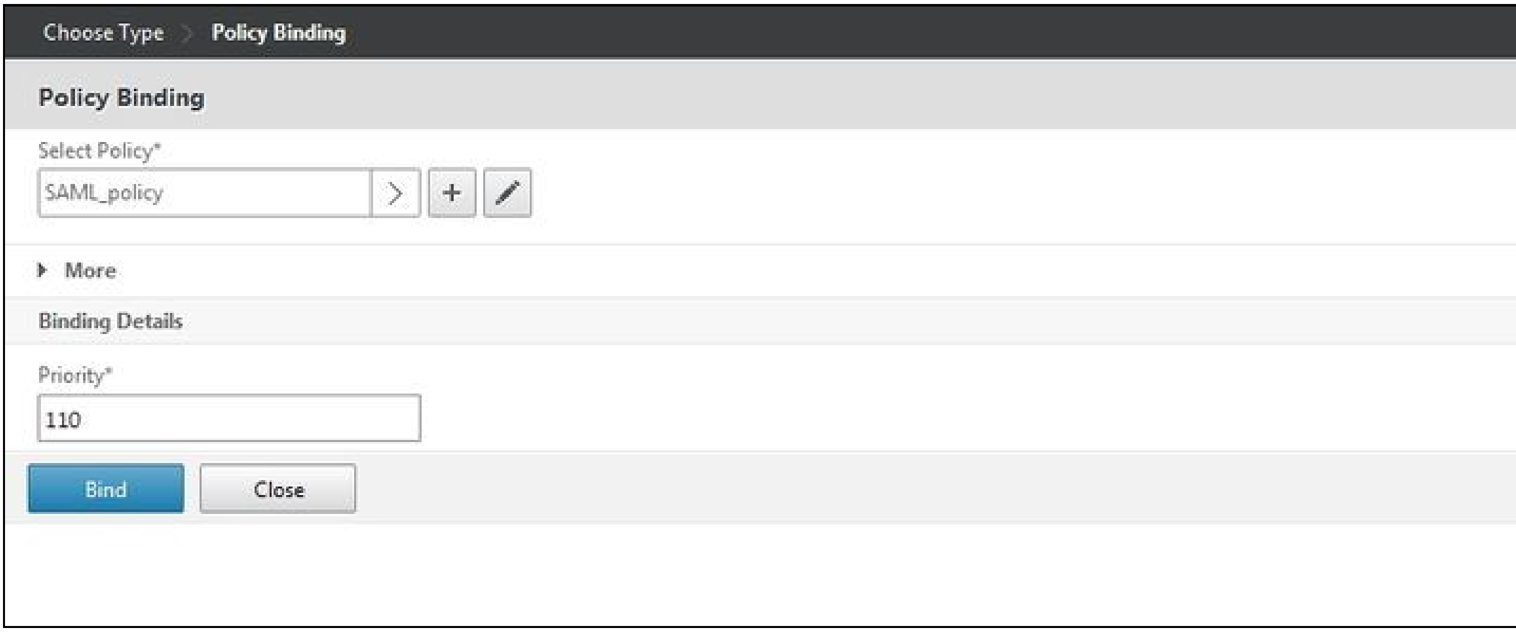
Name: SAML_policy

Authentication Type: SAML

Server*: SAML_test

Expression*: ns_true

After those parameters have been set click the Create button. Then the policy bind screen will be displayed again with the new policy selected.



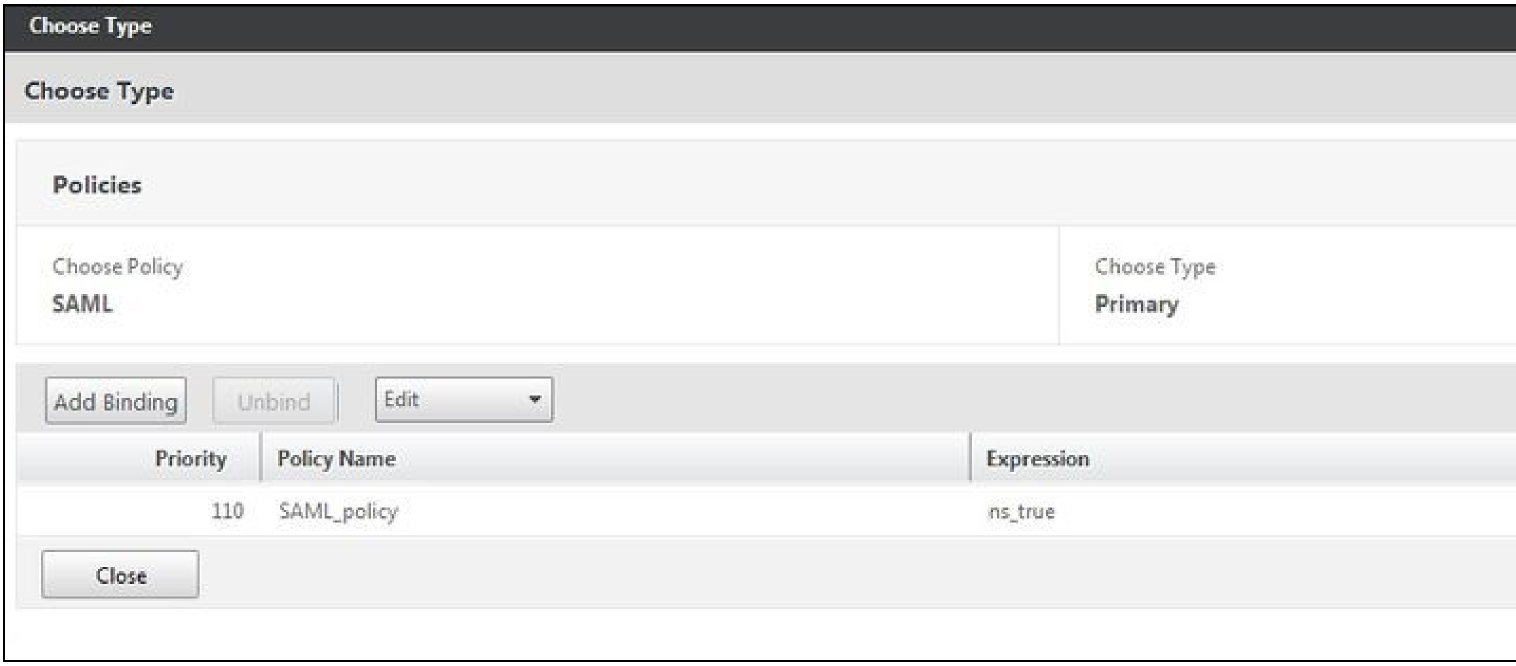
Policy Binding

Select Policy*: SAML_policy

Binding Details

Priority*: 110

Click Bind. The below screen will be displayed.



Choose Policy
SAML

Choose Type
Primary

Priority	Policy Name	Expression
110	SAML_policy	ns_true

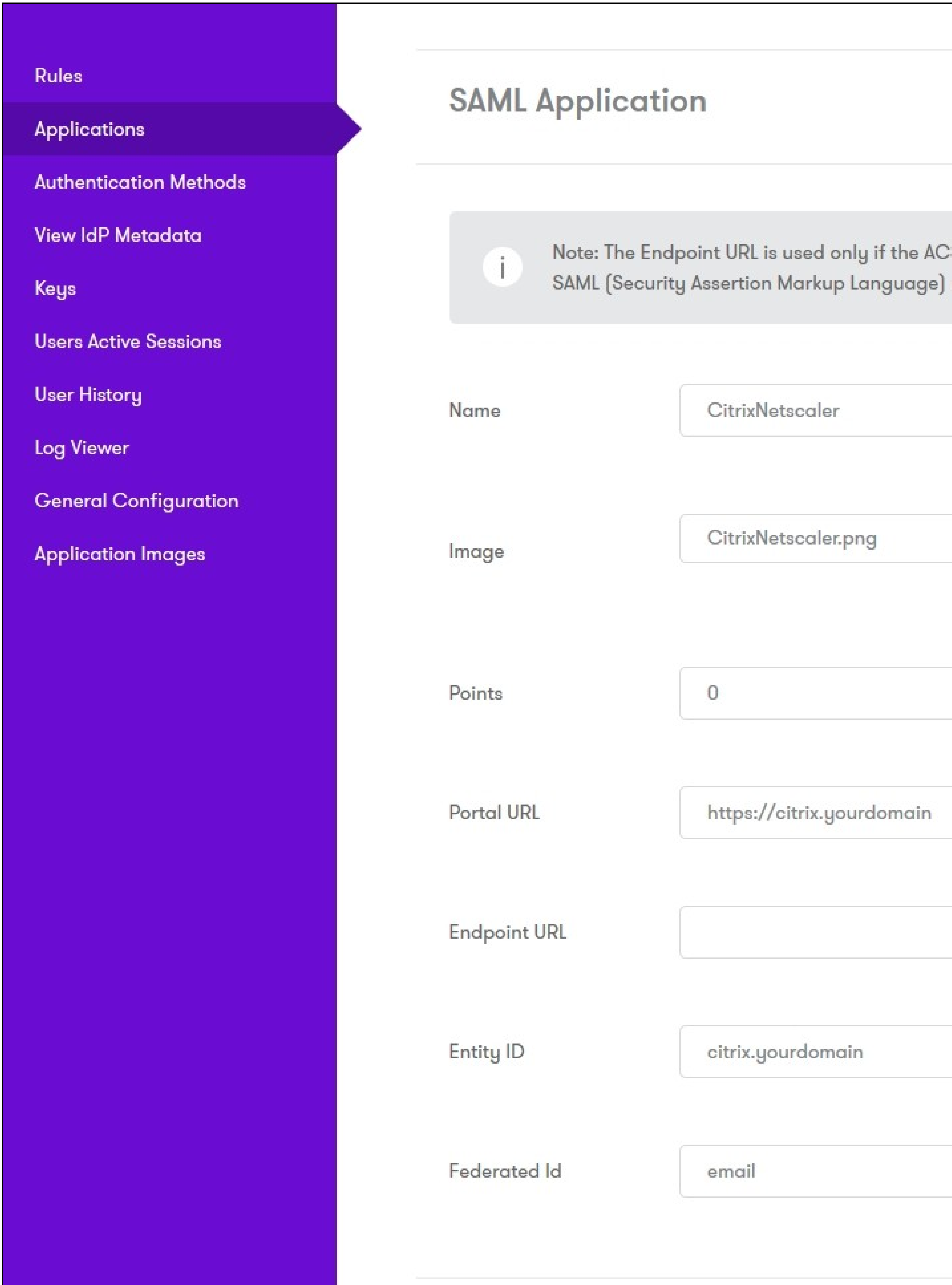
Click the Close button. The virtual server will have now the SAML authentication set. Click the back button and save the current configuration.

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 Citrix Netscaler SAML 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.



SAML Application

Note: The Endpoint URL is used only if the AC
SAML (Security Assertion Markup Language)

Name	CitrixNetscaler
Image	CitrixNetscaler.png
Points	0
Portal URL	https://citrix.yourdomain
Endpoint URL	
Entity ID	citrix.yourdomain
Federated Id	email

- **Name:** Citrix Netscaler(Type an Arbitrary name for this Application)
- **Image:** CitrixNetscaler.png(selected by default)
- **Points:** 100 (the number of the points the user needs to score from their Authentication Method in order to successfully authenticate to this Application)
- **Portal URL:** (this Portal URL is your companies Citrix Netscaler URL which you can usually access on: https://citrix.mycompanyname.com)
- **Endpoint URL:** N/A
- **Entity ID:** citrix.mycompanyname.com (This is the Issuer Name configured on Citrix Netscaler SAML server)

Setup AuthControl Sentry Authentication definition

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

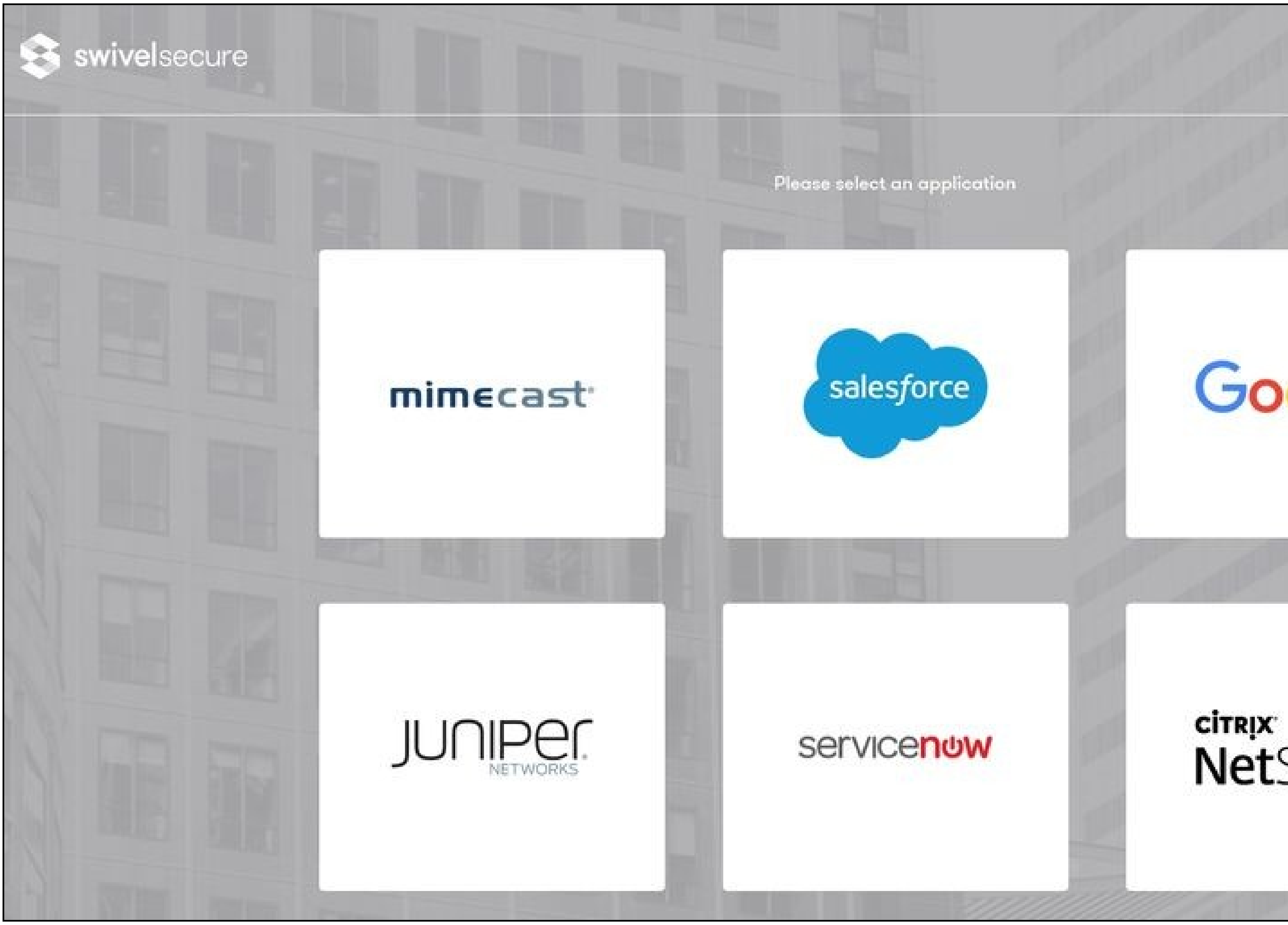
Login to the AuthControl Sentry Administration Console. Click Authentication Methods in the left hand menu. Click the Edit button against the Turing option in the list of Authentication Methods. Give this Authentication Method 100 points. This will mean that when a login attempt is made to the Google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

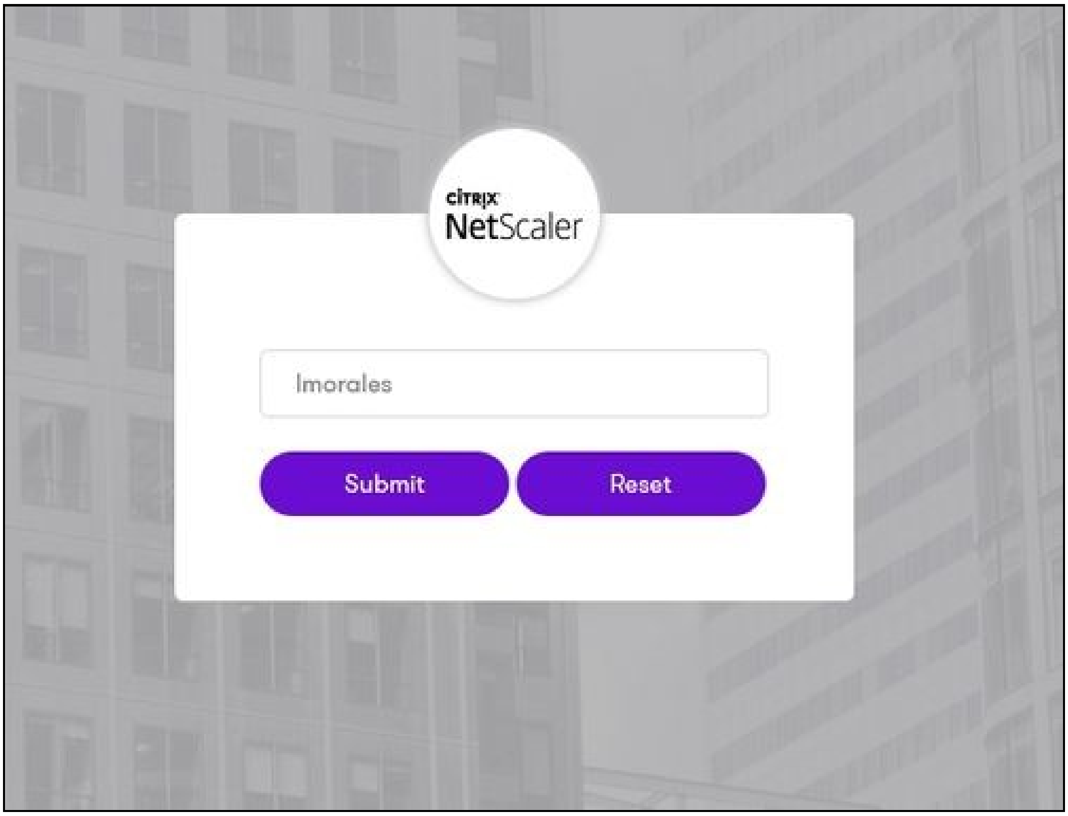
This should be the final step after all previous elements have been configured.

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

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 Citrix Netscaler page)

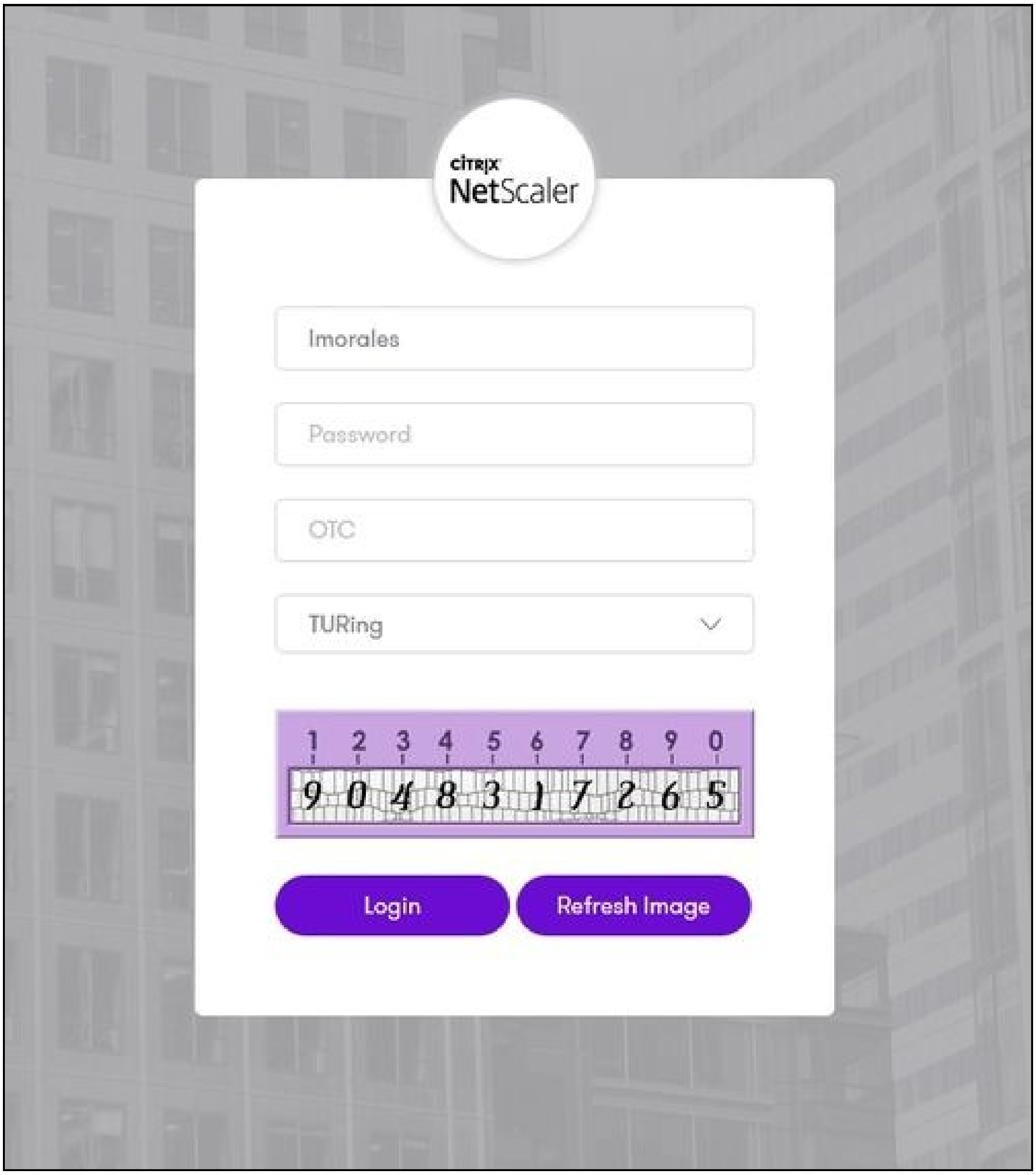


When you visit this URL you will notice that the domain should redirect to the identity provider login URL that you have setup, once you have submitted your username. You should be presented with the page of the Authentication Method which can score enough points to match the points required by the Citrix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



lmorales

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



lmorales

TURing

After we enter our authentication credentials we successfully will see the web app that we have 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 Citrix Netscaler and can be useful for comparison with the Netscaler Citrix 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 Citrix Netscaler?
    - 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?