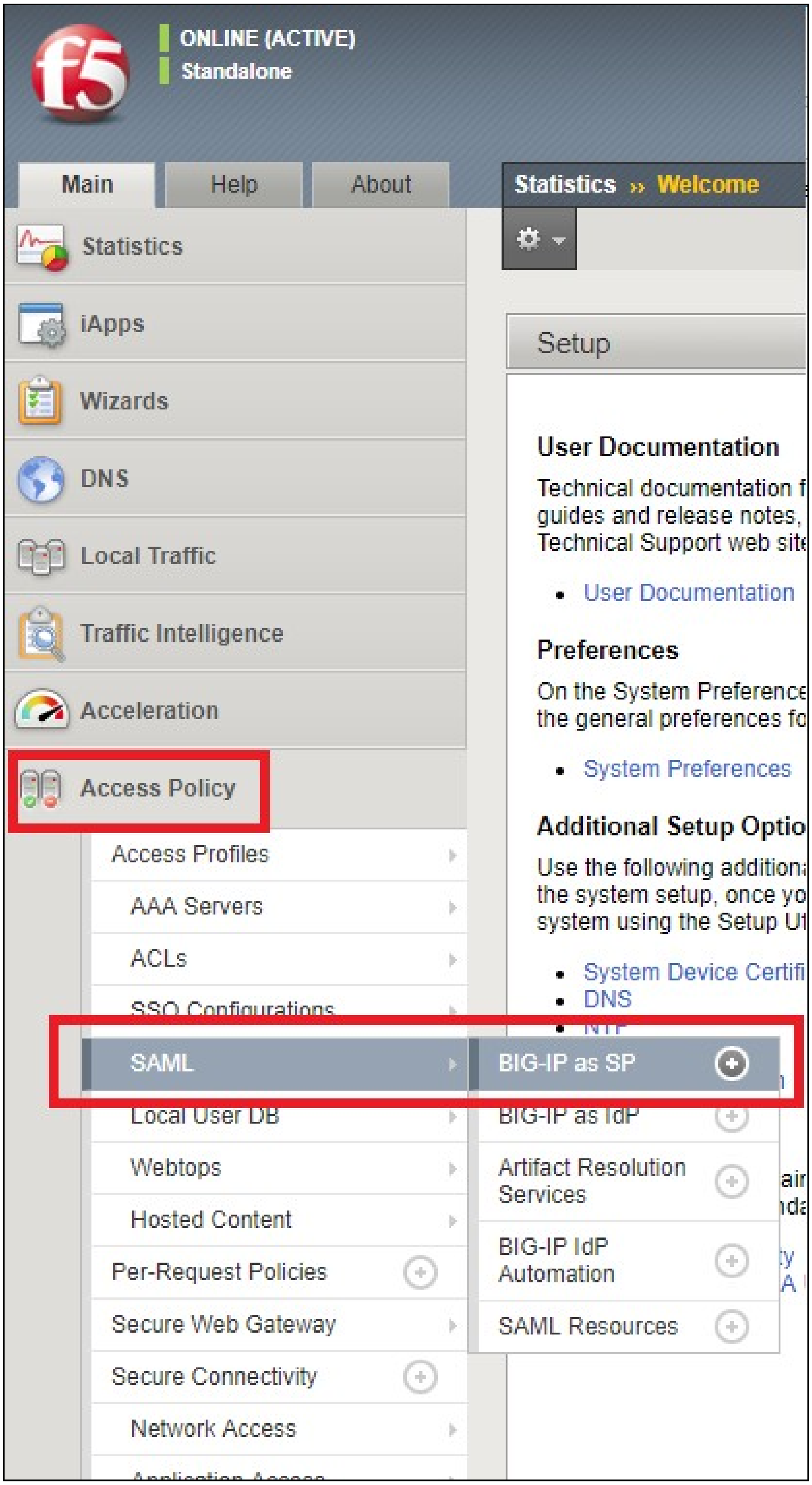
Sentry SSO with F5

Setup SSO on F5

From the F5 BIG-IP Configuration page, select Access Policy -> SAML -> BIG-IP as SP.



User Documentation

Technical documentation f
guides and release notes,
Technical Support web sit

- User Documentation

Preferences

On the System Preference
the general preferences fo

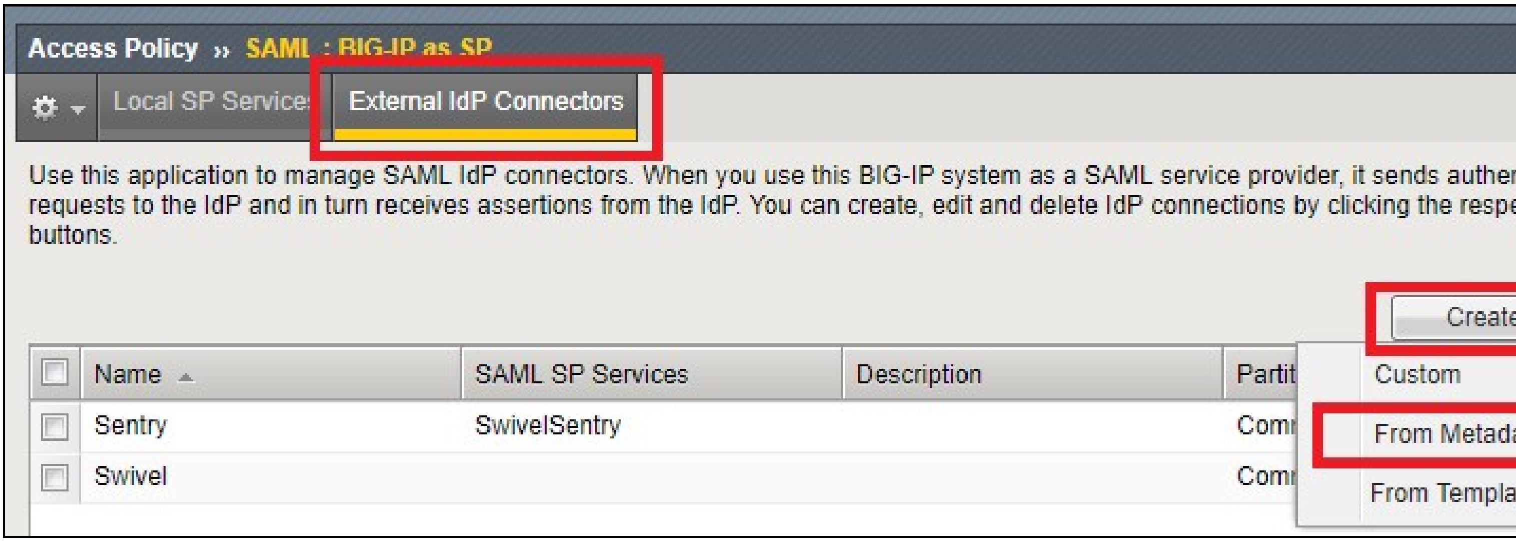
- System Preferences

Additional Setup Optio

Use the following additiona
the system setup, once yo
system using the Setup Ut

- System Device Certifi
- DNS
- NTP

Choose External IdP Connecters and click in Create -> From Metadata

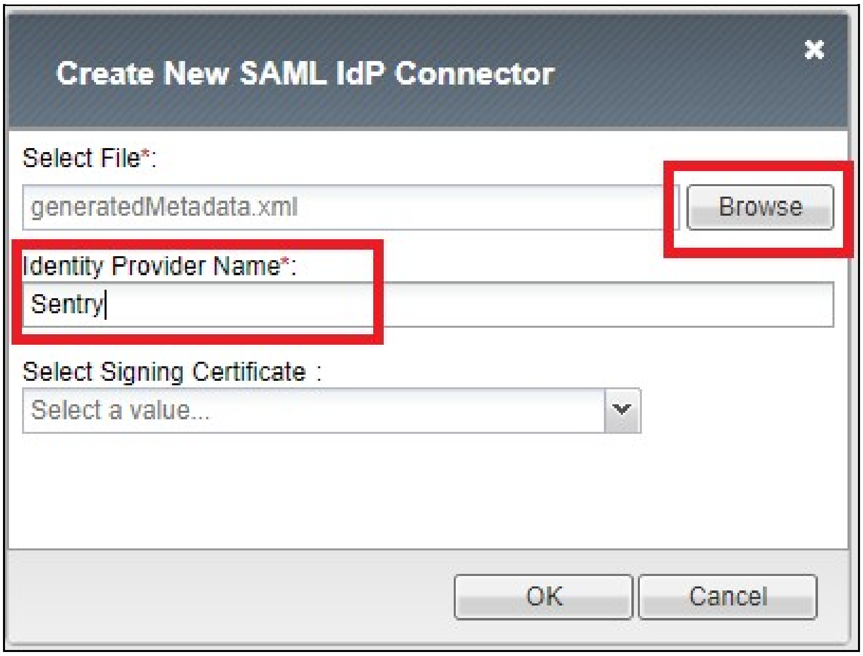


Use this application to manage SAML IdP connectors. When you use this BIG-IP system as a SAML service provider, it sends auther requests to the IdP and in turn receives assertions from the IdP. You can create, edit and delete IdP connections by clicking the respe buttons.

□	Name ▲	SAML SP Services	Description	Partit
□	Sentry	SwivelSentry		Comr
□	Swivel			Comr

Here you will need to import the IdP Metadata file that you can download from Sentry SSO administration console or directly from the url: https://<sentry_URL>/sentry/metadata.

Click browse to upload the file and enter a name for the Identity Provider Name.

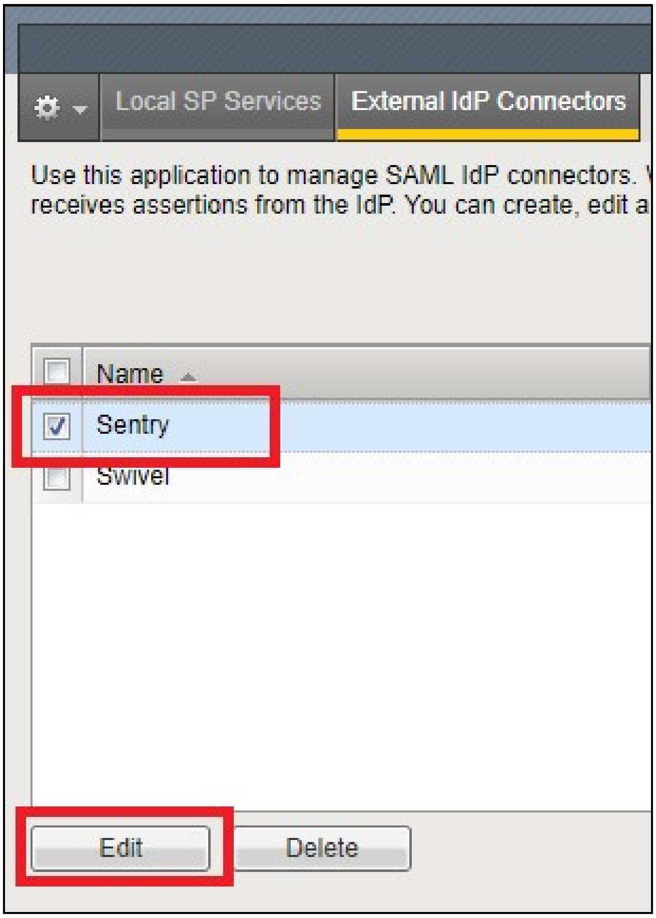


Select File*: generatedMetadata.xml

Identity Provider Name*: Sentry

Select Signing Certificate : Select a value...

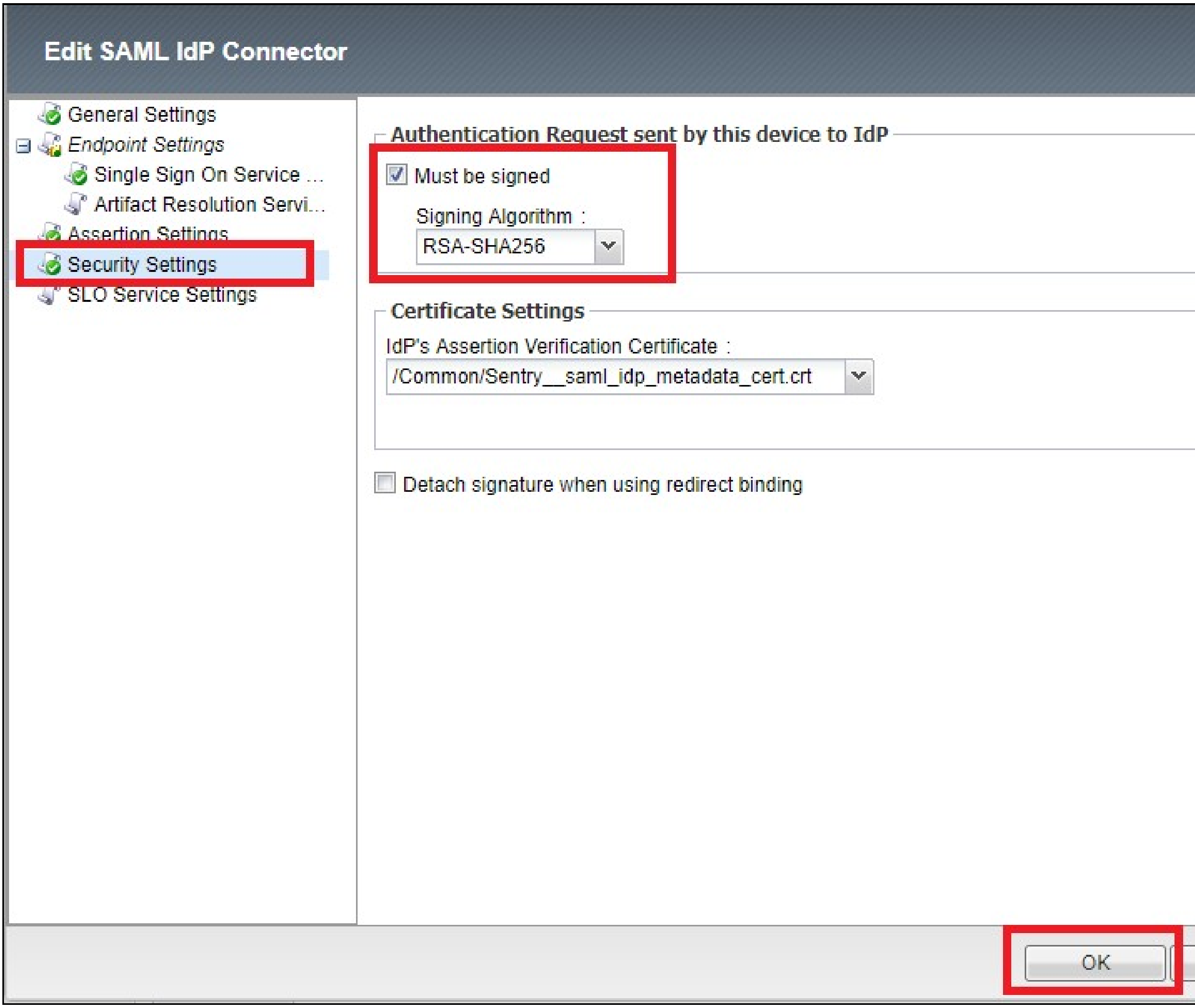
After the connector is created, select it from the list and click Edit.



Use this application to manage SAML IdP connectors. \
receives assertions from the IdP. You can create, edit a

□	Name
☑	Sentry
□	Swivel

Select Security Settings, activate ?Must be signed?, select the Signing Algorithm ?RSA-SHA256? and click OK.



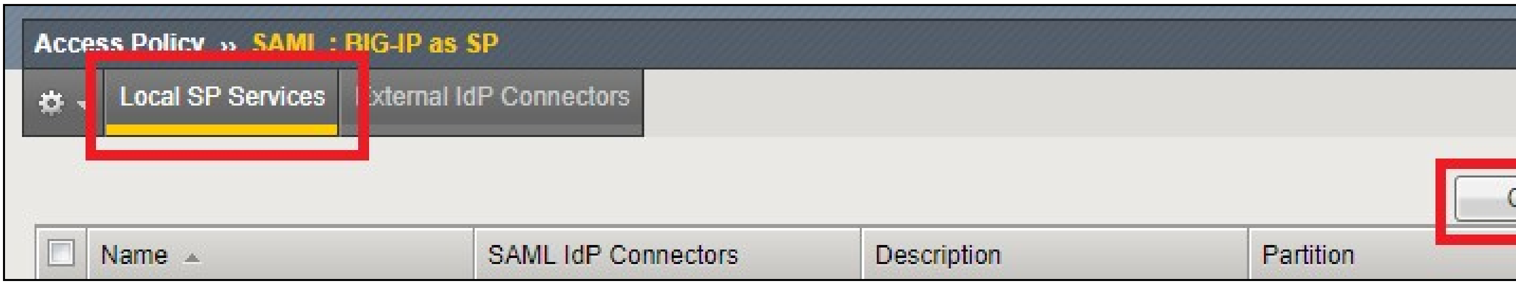
☑ Must be signed

Signing Algorithm : RSA-SHA256

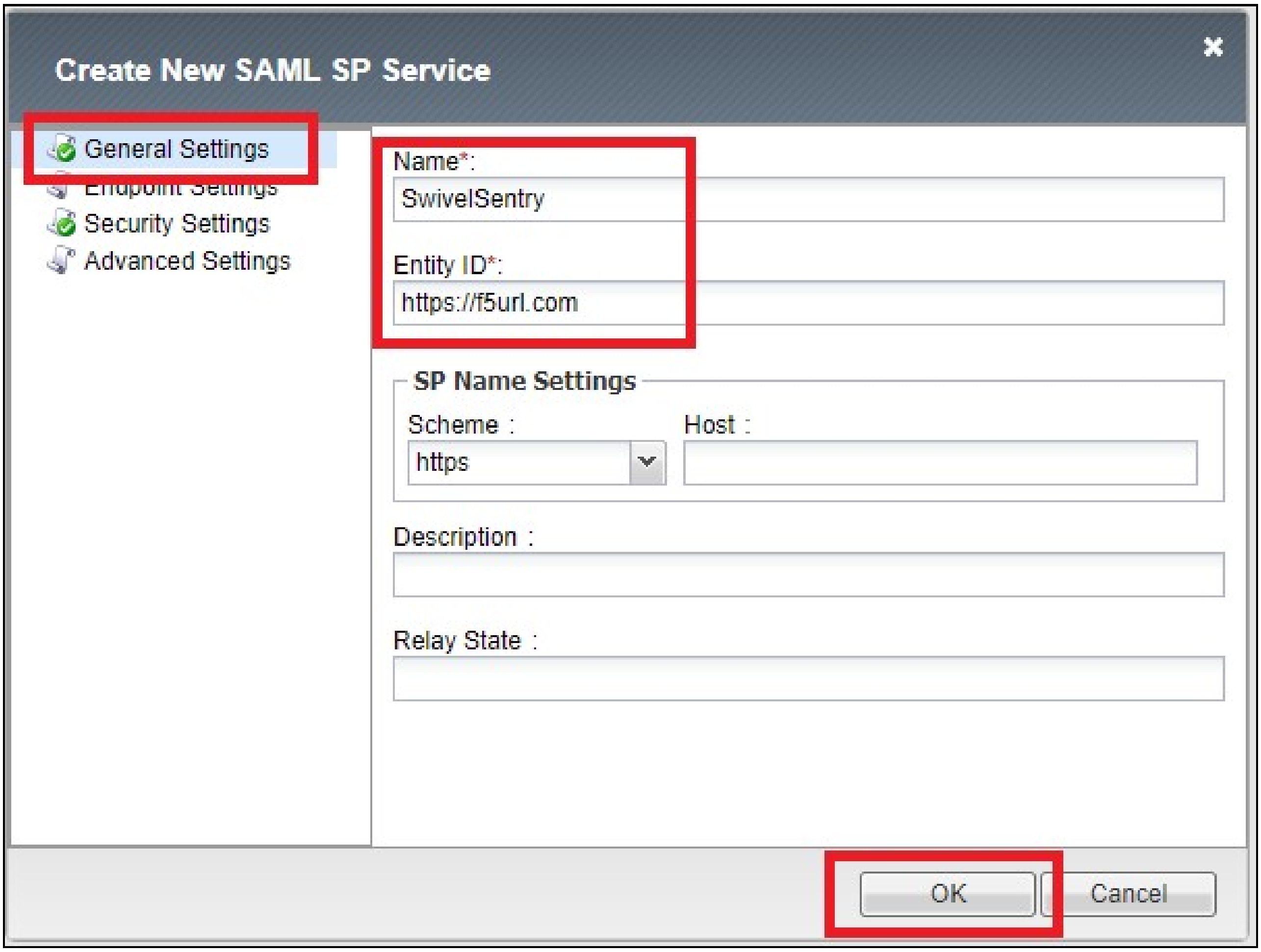
IdP's Assertion Verification Certificate : /Common/Sentry__saml_idp_metadata_cert.crt

□ Detach signature when using redirect binding

Select Local SP Services and click Create



In General Settings, enter a name for the SP service, in the Entity ID enter your F5 URL e.g. https://**F5_HOSTNAME**, and click OK.



Name*: SwivelSentry

Entity ID*: https://f5url.com

SP Name Settings

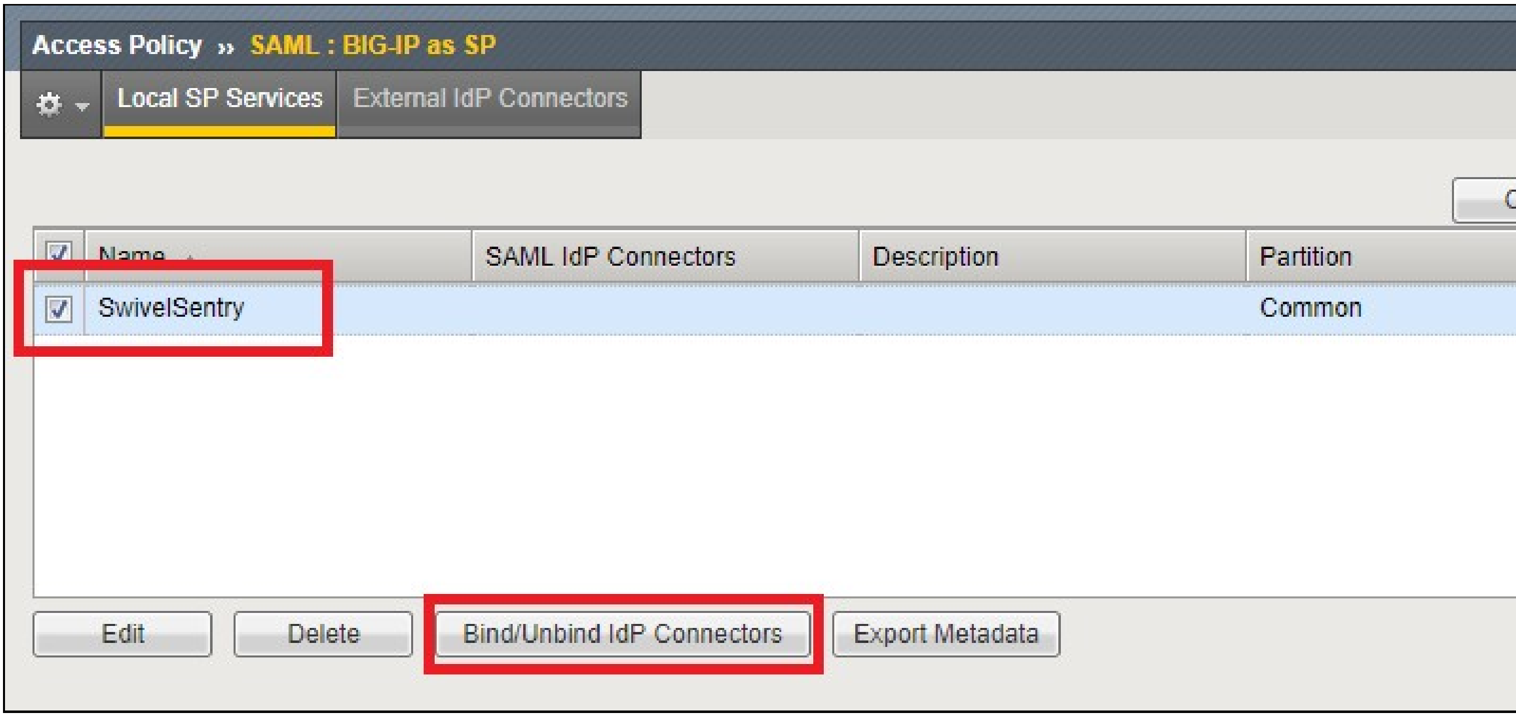
Scheme : https

Host :

Description :

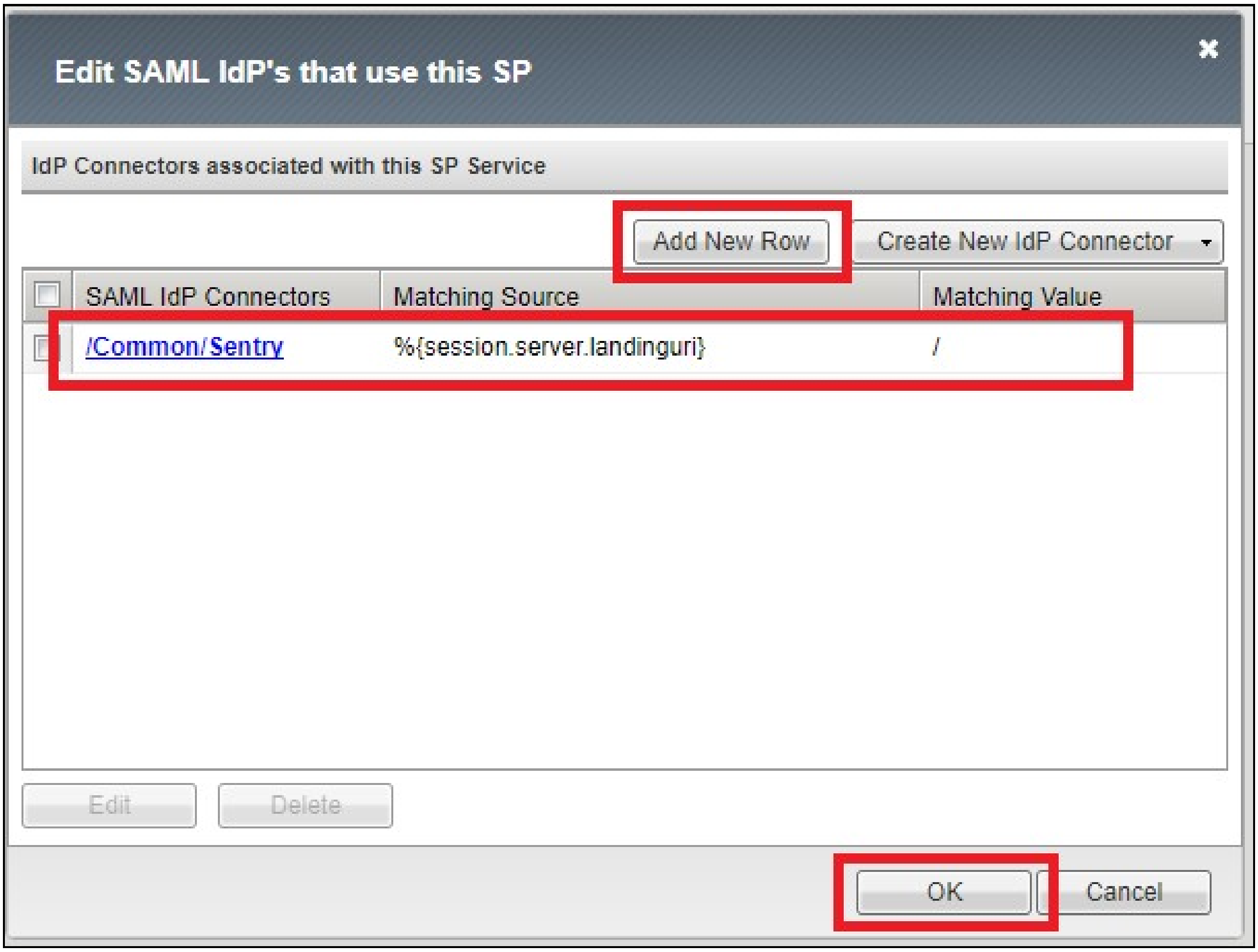
Relay State :

After the SP Service is created, select it and click in Bind/Unbind IdP Connectors.



☑	Name	SAML IdP Connectors	Description	Partition
☑	SwivelSentry			Common

Click ?Add New Row? and select under SAML IdP Connectors, the one that you have previously created. For Matching Source, Select %{session.server.landinguri} and for Matching Value enter a custom path for the login url e.g. / or /PATH. Click Update to save and then click Ok.

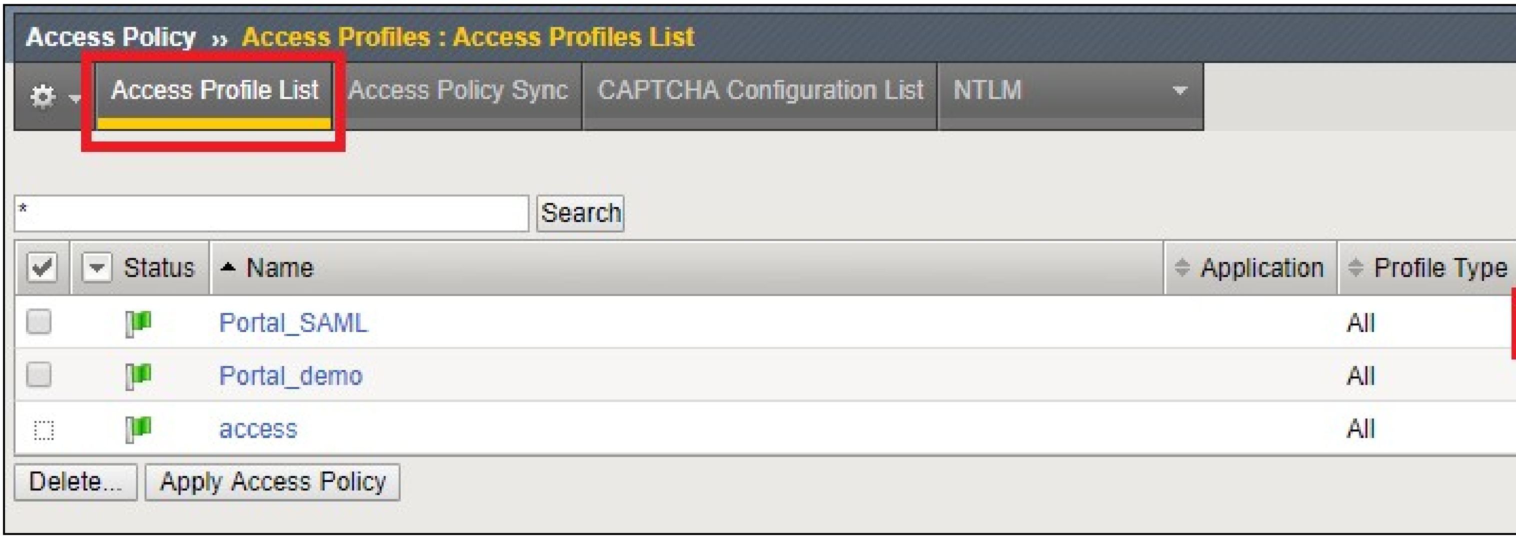


Edit SAML IdP's that use this SP
IdP Connectors associated with this SP Service
Add New Row
Create New IdP Connector
Edit
Delete
OK
Cancel

☐	SAML IdP Connectors	Matching Source	Matching Value
☐	/Common/Sentry	%{session.server.landinguri}	/

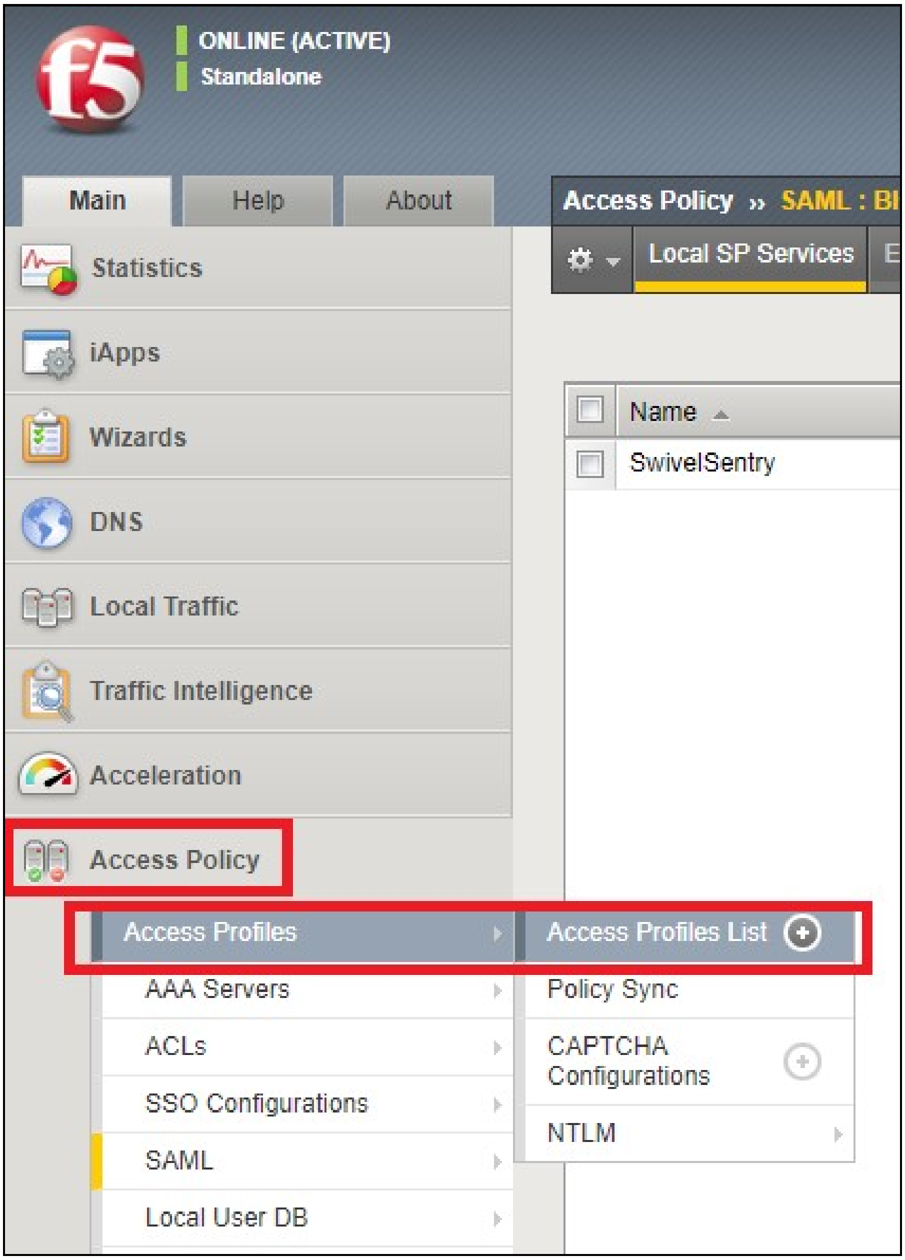
With the External IdP Connector and the Local SP Service configured, you can now change your existing Access Profile.

Go to Access Policy -> Access Profiles -> Access Profiles List and edit the Access Profile that you want to change or create a new one

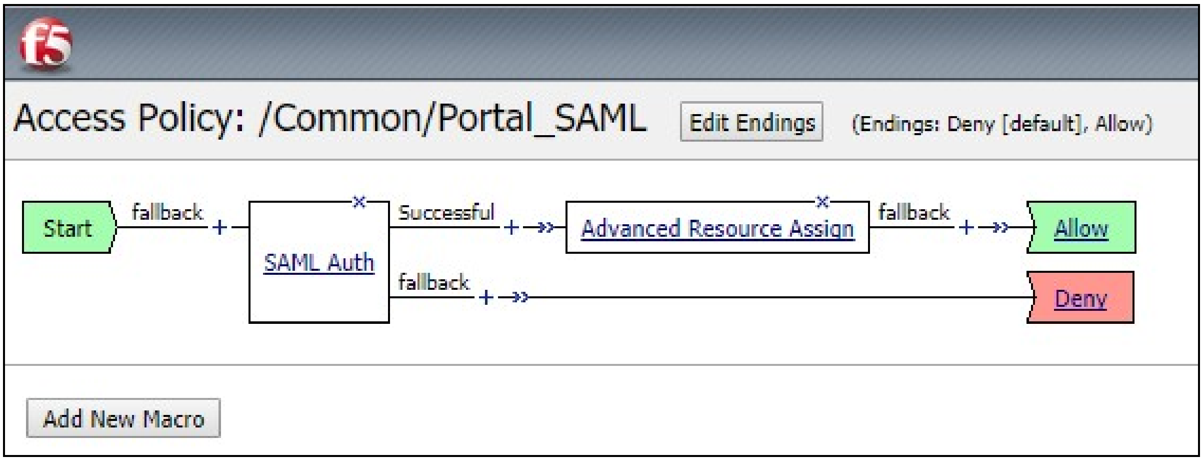


Access Policy » Access Profiles : Access Profiles List
Access Profile List
Access Policy Sync
CAPTCHA Configuration List
NTLM
*
Search
Delete...
Apply Access Policy

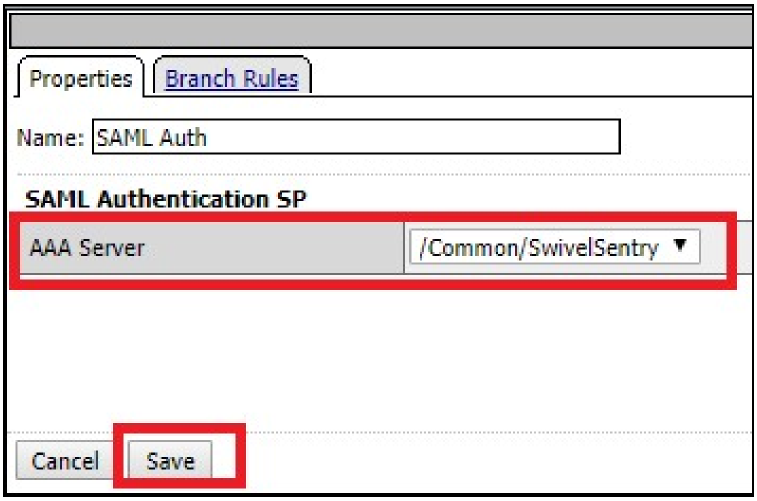
☑	Status	Name	Application	Profile Type
☐	🟩	Portal_SAML		All
☐	🟩	Portal_demo		All
☐	🟩	access		All



You need to configure your Access Policy in order the have the following actions:



Click in the SAML Auth Action to change the properties and change the AAA server to the previously created SP Service.



Name: SAML Auth

SAML Authentication SP

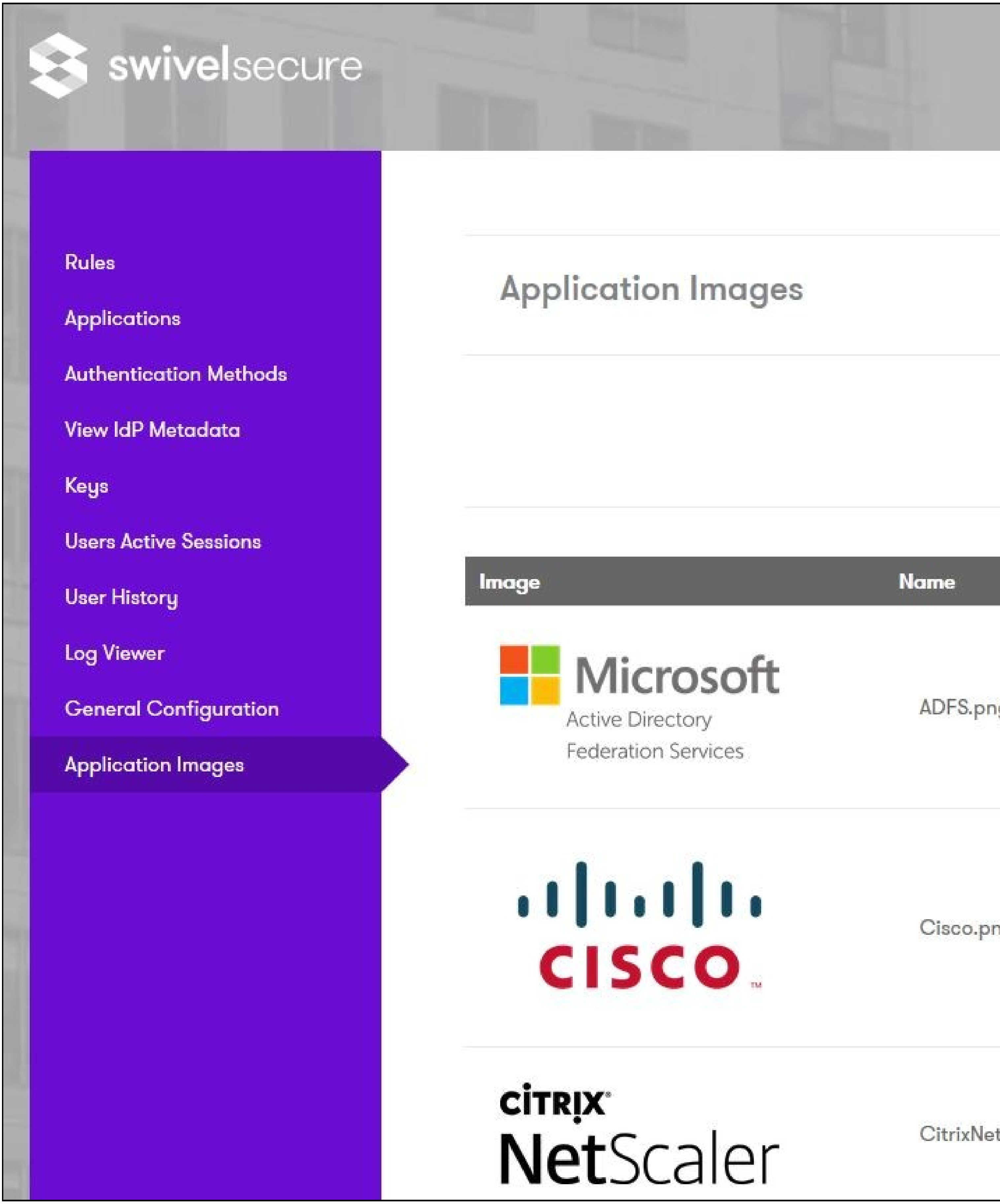
AAA Server: /Common/SwivelSentry

Setup Sentry Application Definition

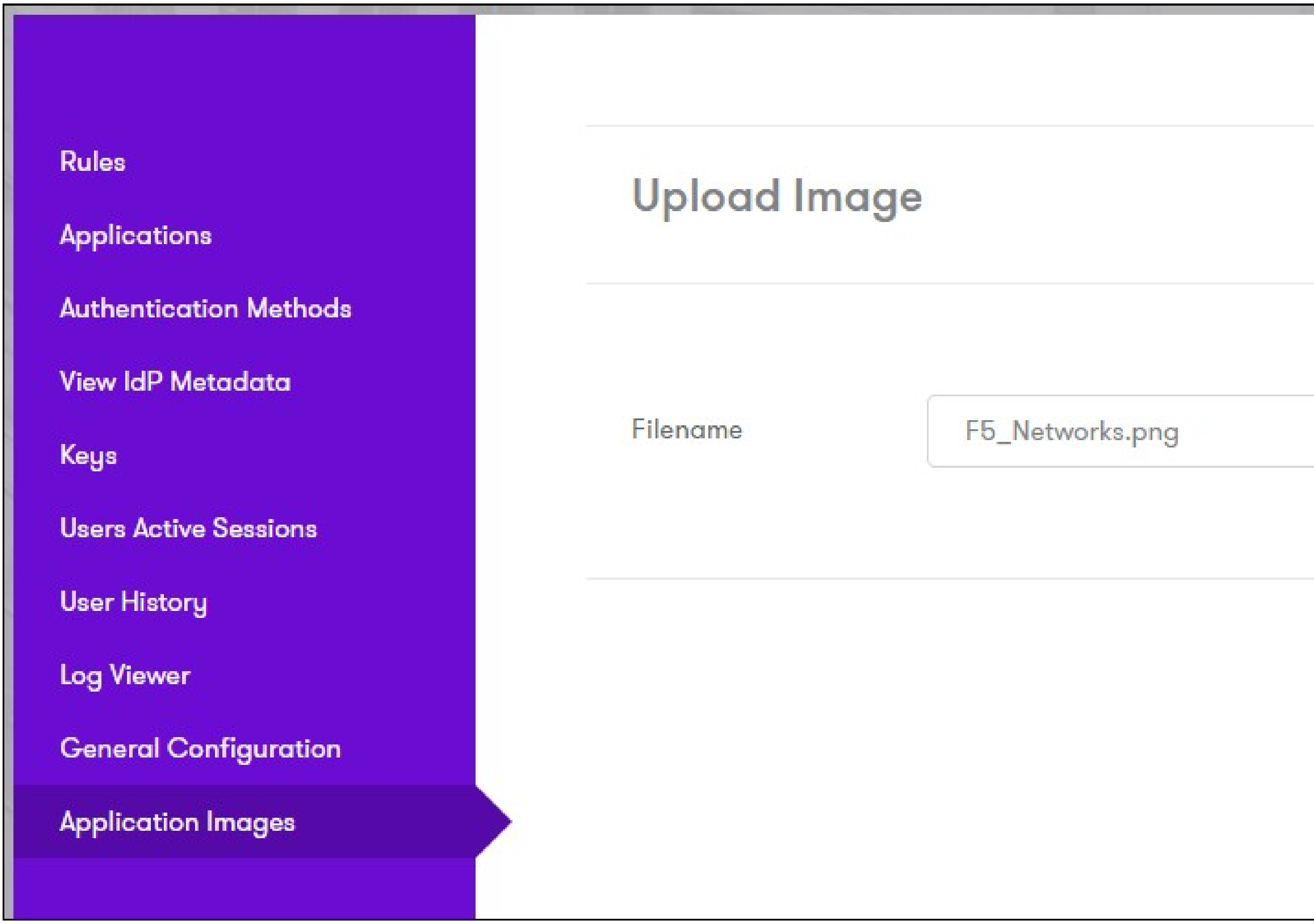
First we should upload the F5 logo. Find it using a Google Images search or copy it from here:

f5

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



Browse to the Logo file you have saved:

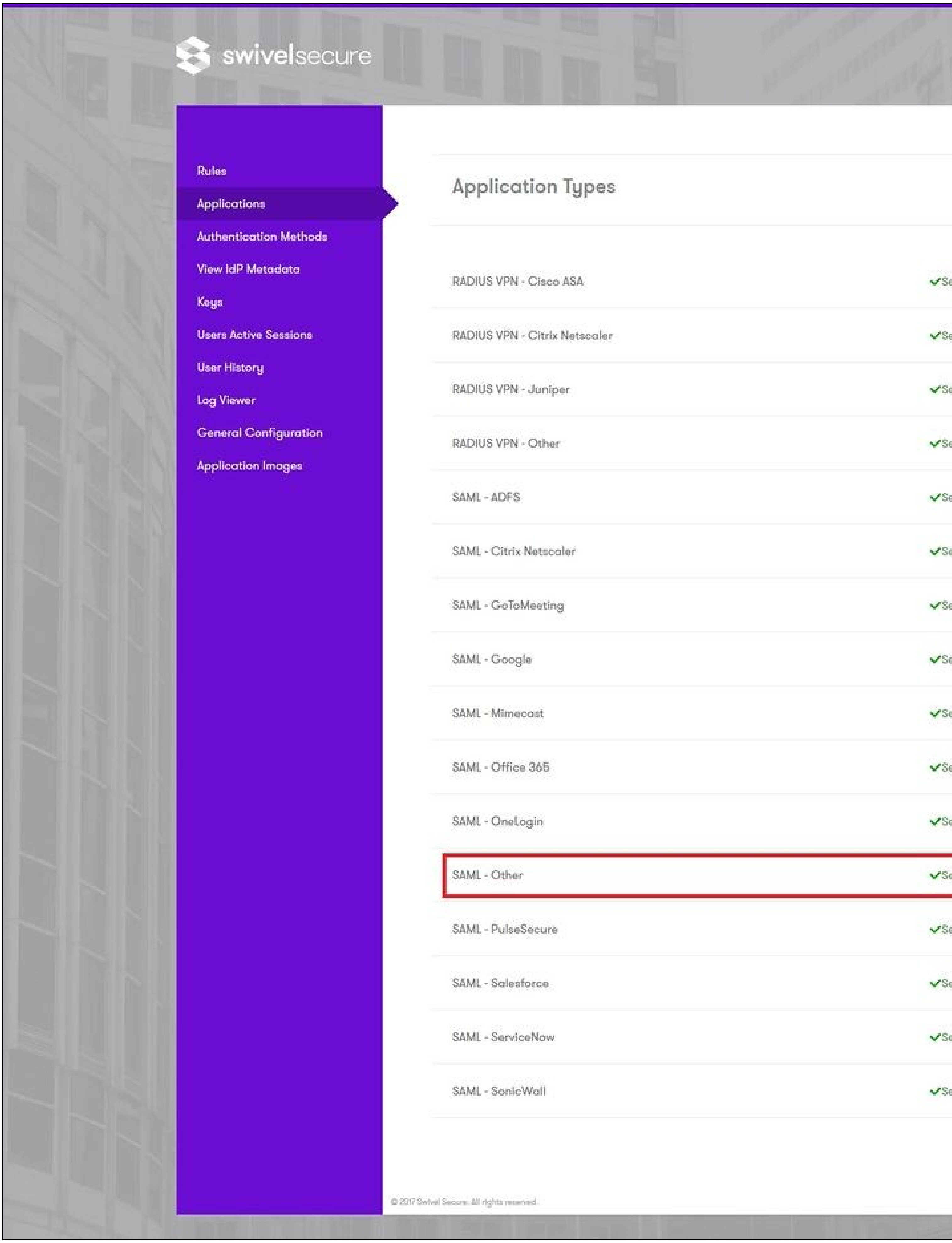


Upload Image

Filename F5_Networks.png

Then upload the image to the Sentry application and the image should now be available to select, when we go to create a new Application definition for JIRA.

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: **F5**

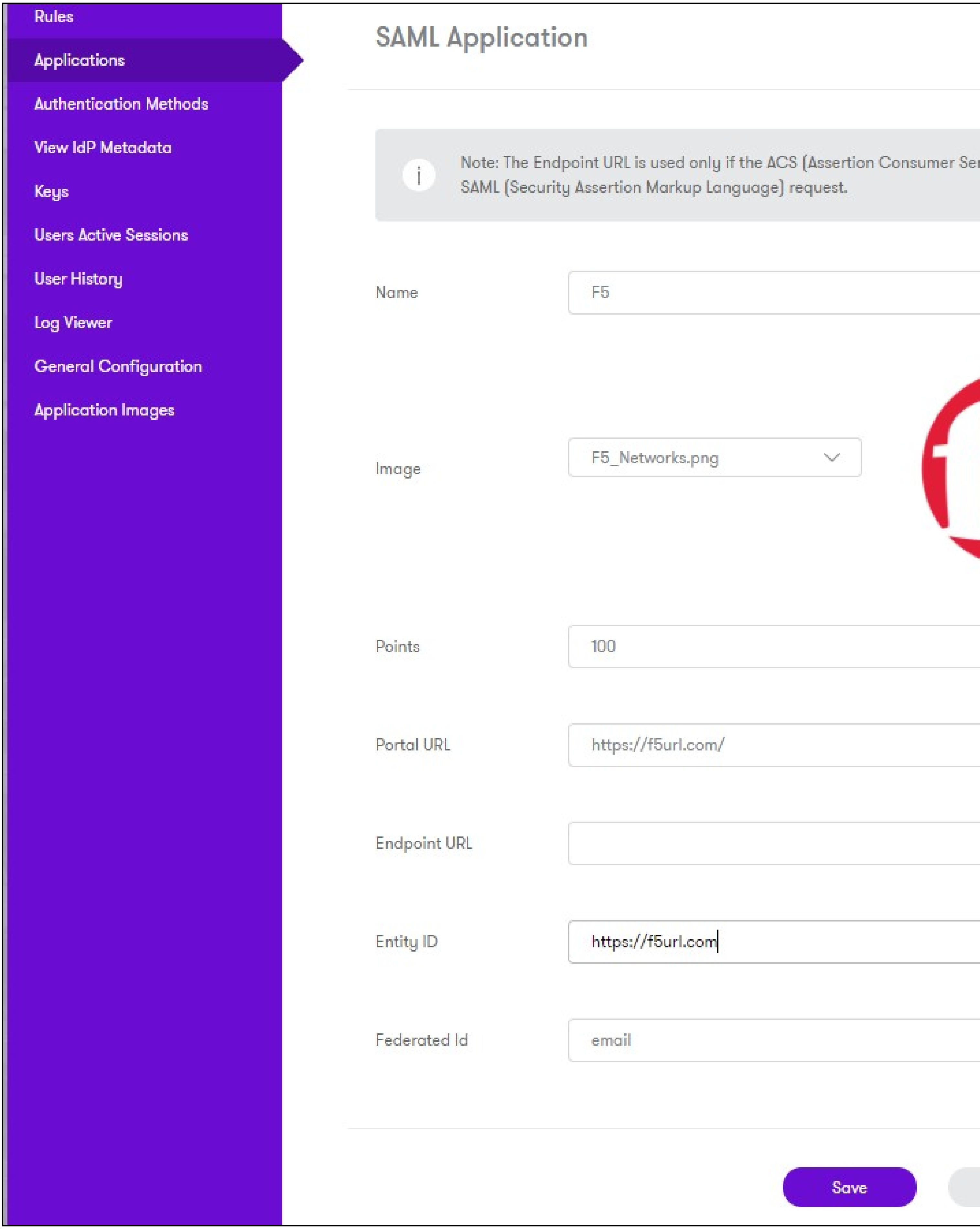
Points: 100 (the number of points the user needs to score from their Authentication Method in order to successfully authenticate to this Application)

Portal URL: URL to access to F5. The PATH needs to match the Matching Value for the previously created SP Service e.g. https://**F5_HOSTNAME**/PATH

Endpoint URL: Leave blank - not required

Entity ID: Identifier of the F5 SAML request. It needs to match the Identifier for the previously created SP Service. e.g. https://**F5_HOSTNAME**

Federated Id: email



SAML Application

Note: The Endpoint URL is used only if the ACS (Assertion Consumer Se
SAML (Security Assertion Markup Language) request.

Name: F5

Image: F5_Networks.png

Points: 100

Portal URL: https://f5url.com/

Endpoint URL:

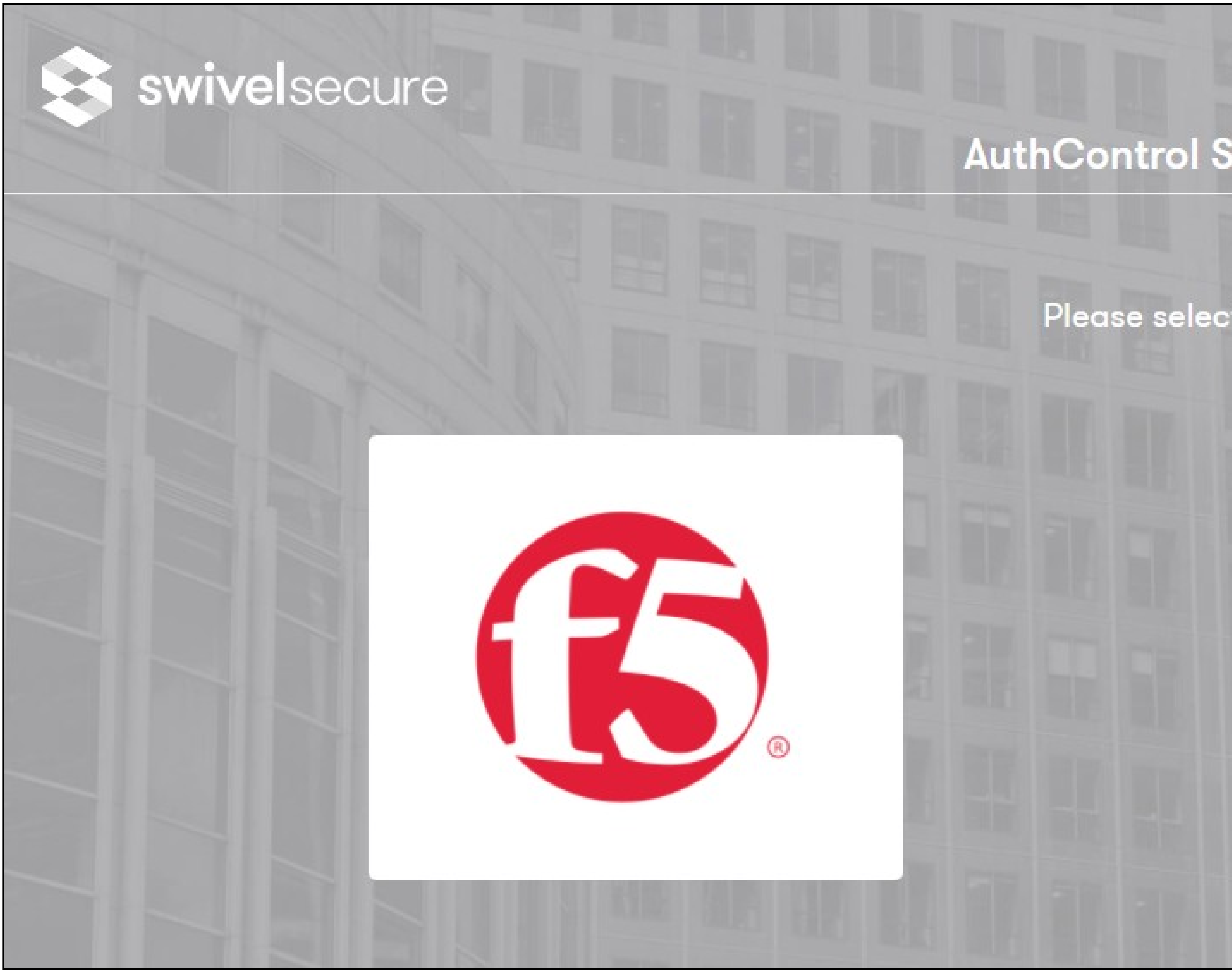
Entity ID: https://f5url.com

Federated Id: email

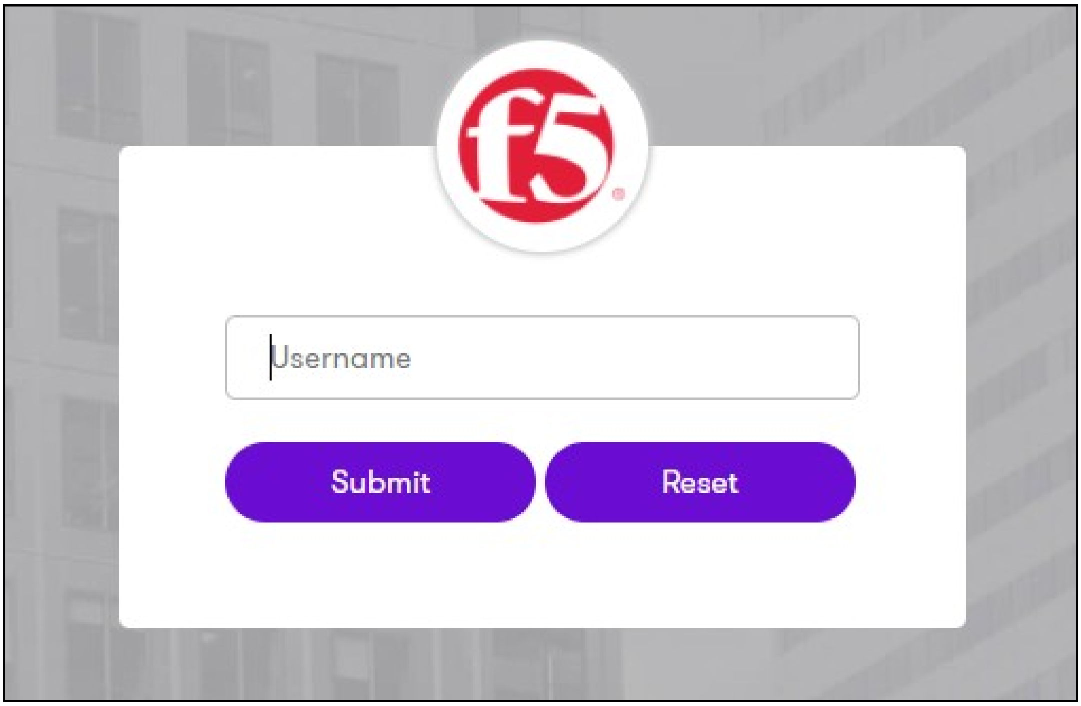
Testing authentication to Salesforce via Swivel Sentry

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 F5 Icon on which you can click and proceed with authentication (as you would by going straight to the F5 page)



When you visit this URL you will notice that the domain should redirect to the identity provider login URL that you setup. You should be presented with the 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 F5 Application definition.

After you enter your authentication credentials you will login into the VPN.