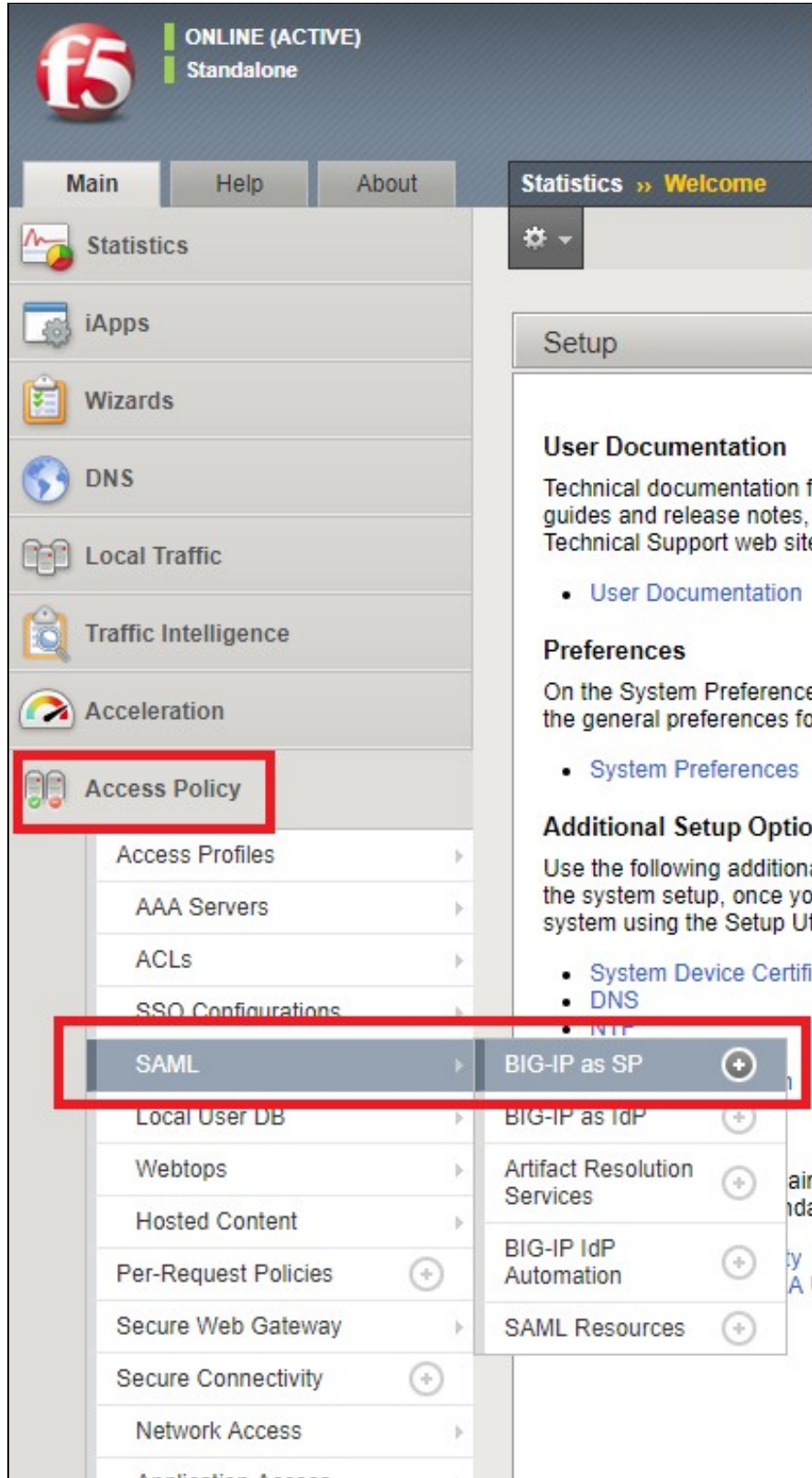


Sentry SSO with F5

Setup SSO on F5

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



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

Access Policy >> SAML : BIG-IP as SP

Local SP Services **External IdP Connectors**

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

<input type="checkbox"/>	Name ▲	SAML SP Services	Description	Partitions
<input type="checkbox"/>	Sentry	SwivelSentry		Common
<input type="checkbox"/>	Swivel			Common

Create
Custom
From Metadata
From Template

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.

Create New SAML IdP Connector [X]

Select File*:

generatedMetadata.xml **Browse**

Identity Provider Name*:

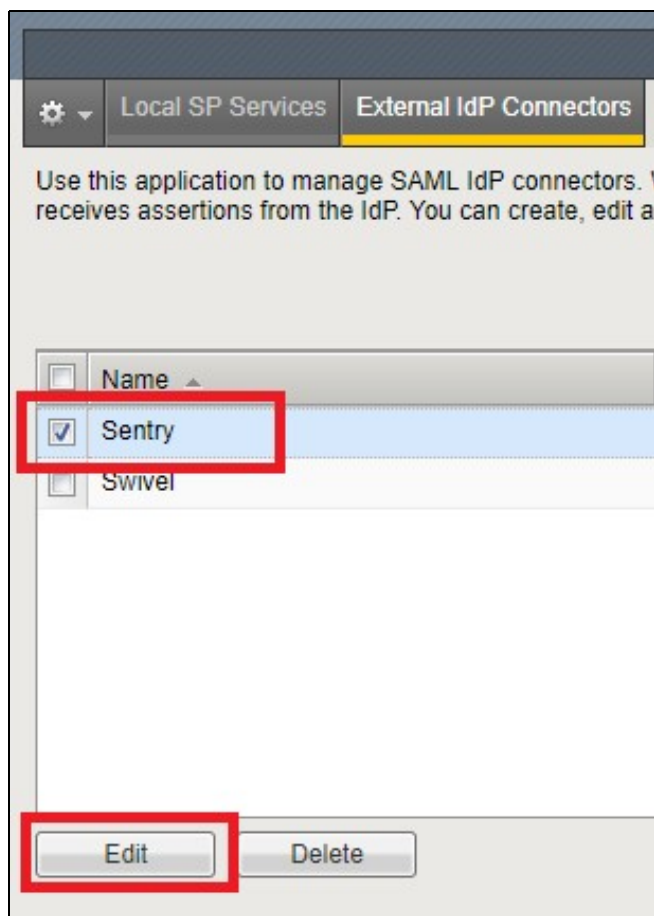
Sentry

Select Signing Certificate :

Select a value... [v]

OK Cancel

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



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

Edit SAML IdP Connector

- General Settings
- Endpoint Settings
- Single Sign On Service ...
- Artifact Resolution Servi...
- Assertion Settings
- Security Settings**
- SLO Service Settings

Authentication Request sent by this device to IdP

☒ Must be signed
Signing Algorithm :
RSA-SHA256

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

☐ Detach signature when using redirect binding

OK

Select Local SP Services and click Create

Access Policy >> SAML : BIG-IP as SP

Local SP Services

External IdP Connectors

☐

Name ▲

SAML IdP Connectors

Description

Partition

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.

Create New SAML SP Service

☒ General Settings
 ☐ Endpoint Settings
 ☒ Security Settings
 ☐ Advanced Settings

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.

Access Policy » SAML : BIG-IP as SP

☒ Local SP Services
 ☐ External IdP Connectors

<input checked="" type="checkbox"/>	Name	SAML IdP Connectors	Description	Partition
<input checked="" type="checkbox"/>	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.landingurl}` 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

<input type="checkbox"/>	SAML IdP Connectors	Matching Source	Matching Value
<input type="checkbox"/>	/Common/Sentry	<code>%{session.server.landinguri}</code>	/

Edit

Delete

OK

Cancel

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

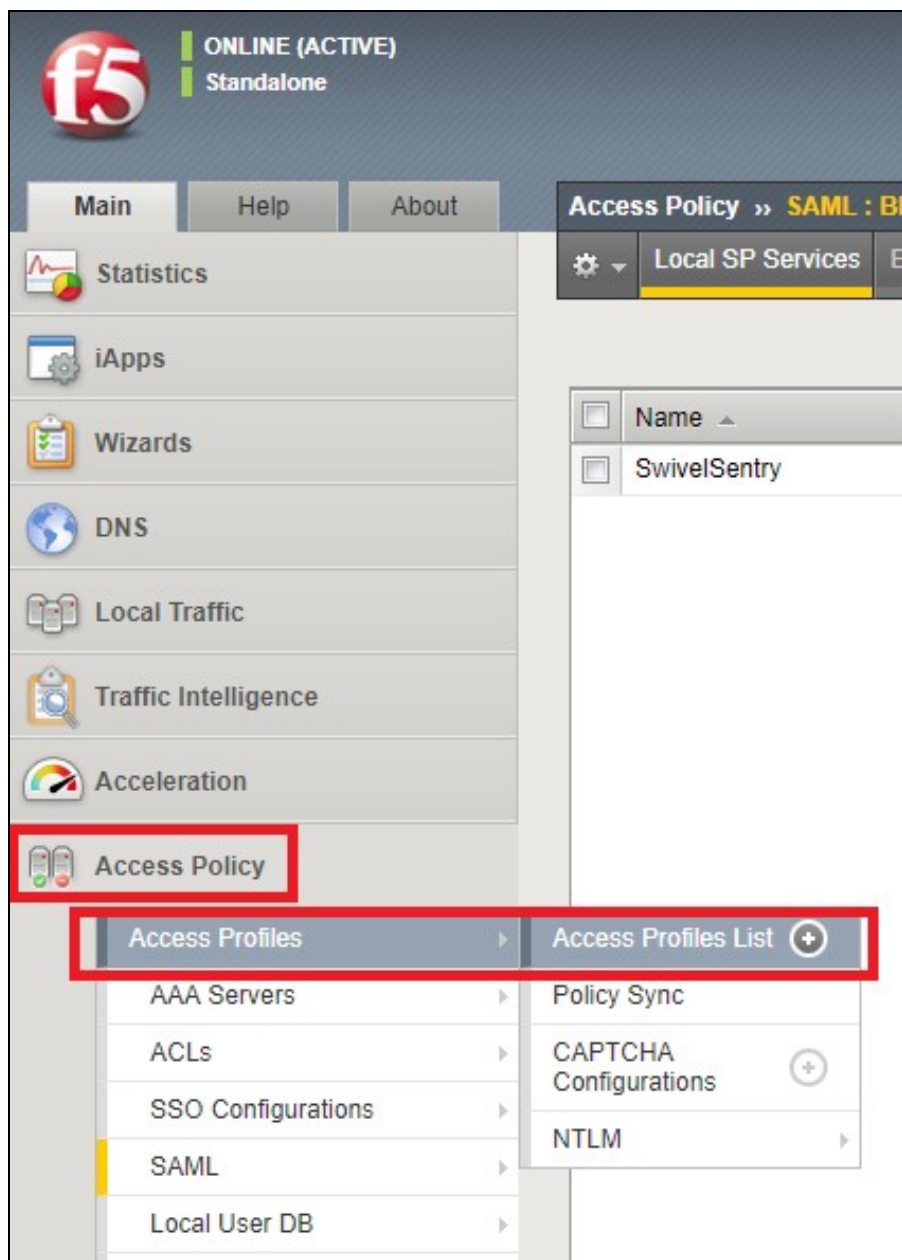
NTLM

Search

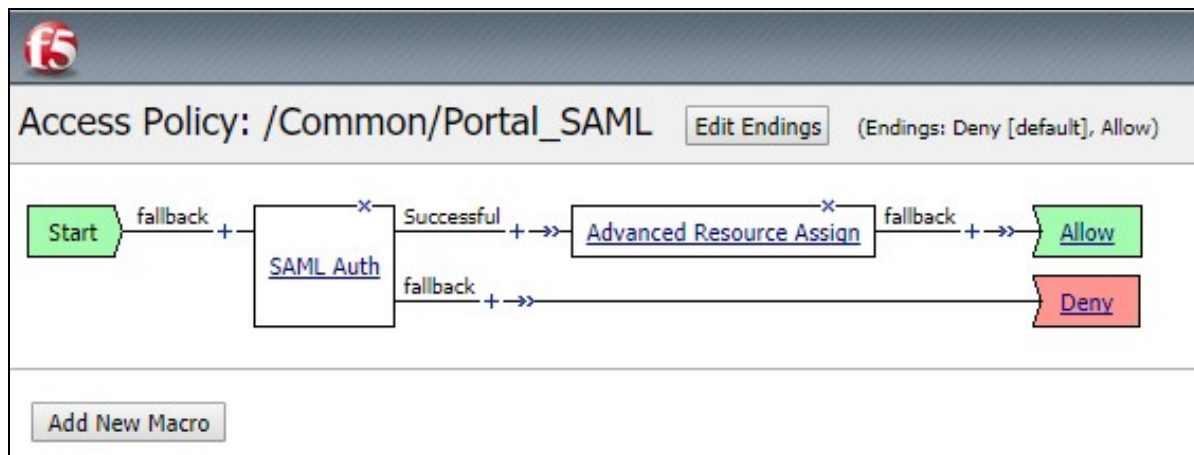
<input checked="" type="checkbox"/>	Status	Name	Application	Profile Type
<input type="checkbox"/>		Portal_SAML		All
<input type="checkbox"/>		Portal_demo		All
<input type="checkbox"/>		access		All

Delete...

Apply Access Policy



You need to configure your Access Policy in order to 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.

Properties Branch Rules

Name: SAML Auth

SAML Authentication SP


AAA Server /Common/SwivelSentry ▼

Cancel Save

Setup Sentry Application Definition

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



 swivelsecure

Rules

Applications

Authentication Methods

View IdP Metadata

Keys

Users Active Sessions




User History

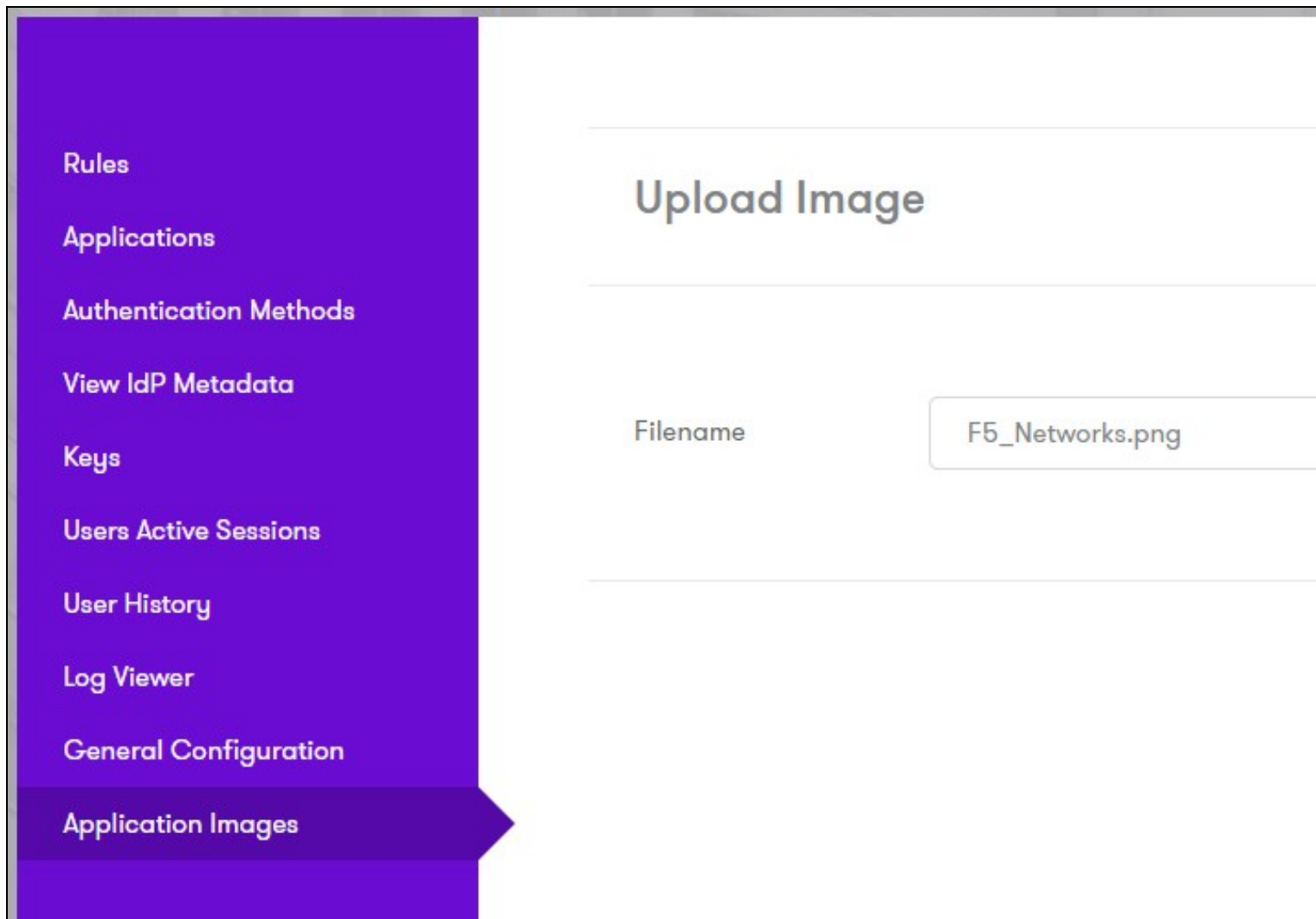
Log Viewer

General Configuration

Application Images

Application Images

Image	Name
 <div>Microsoft Active Directory Federation Services</div>	ADFS.png
	Cisco.png
	CitrixNetScaler.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.

[Rules](#)[Applications](#)[Authentication Methods](#)[View IdP Metadata](#)[Keys](#)[Users Active Sessions](#)[User History](#)[Log Viewer](#)[General Configuration](#)[Application Images](#)

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

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) 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

Save


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.



A login form for F5. At the top center is the F5 logo, which consists of a red circle containing the white text 'f5'. Below the logo is a white rectangular box with rounded corners. Inside this box, there is a text input field with the placeholder text 'Username'. Below the input field are two purple buttons with rounded corners. The left button is labeled 'Submit' and the right button is labeled 'Reset' in white text.

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.