Sentry SSO with Palo Alto

Contents

- 1 Setup AuthControl Sentry Keys
- 2 Setup SSO on Palo Alto
- 3 Sentry
- 4 Login Steps

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 Palo Alto

SAML IDENTITY PROVIDER SERVER PROFILE IMPORT

- Profile Name: Swivel_sentry (example)

Identity Provider Configuration

- Identity Provider Metadata : Copy the Metadata from Sentry and import it to Palo Alto

After this you should get :

SAML IDENTITY PROVIDER SERVER PROFILE

- Profile Name: Swivel_sentry

Identity Provider Configuration

- Identity Provider ID : https://demo.swivelcloud.com/sentry/saml20endpoint
- Identity Provider Certificate :
- Identity Provider SSO URL : https://demo.swivelcloud.com/sentry/saml20endpoint
- Identity Provider SLO URL : https://demo.swivelcloud.com/sentry/singlelogout
- SAML HTTP Binding for SSO Requests to IDP : Select Post
- SAML HTTP Binding for SLO Requests to IDP : Select Post

- Maximum Clock Skew (seconds) : 60

AUTHENTICATION PROFILE

- Name : SAML

TAB : Authentication

- Type : SAML
- IdP Server Profile : Swivel_sentry
- Certificate for Signing Requests :

```
Check : "Enamble Single Logout"
```

- Certificate Profile : Swivel

User Attributes in SAML Messages from IDP

- Username Attribute : username

Sentry

- Name : Palo Alto VM
- Image : Palo Alto logo (png)
- Poits : 100 (example)
- Portal URL :
- Endpoint URL :
- Entity ID :
- Federated Id : username

Login Steps

Click : User Single Sign-On

Swivel username then click continue...

Insert username then click submit

Authenticate with Swivel authentication method (Turing / PINPad...)