TAP TO GO BACK TO KIOSK MENU

SAS® GLOBAL FORUM 2020

MARCH 29 - APRIL 1
WASHINGTON, DC

USERS PROGRAM

Securing SAS® Viya® Access with Single Sign-on and 2FA

Sandeep Grande, Senior SAS Administrator

CORE COMPETE INC

Index

Please use the headings above to navigate through the different sections of the poster

Sandeep Grande

- A quick look at data breach trends shows that most of the security breaches involved weak, default or stolen passwords. Two-factor authentication (2FA) strengthens access security by requiring two methods (also referred to as factors) to verify your identity. These factors can include something you know - like a username and password, plus something you have - like a smartphone app to approve authentication requests. 2FA protects against phishing, social engineering and password brute-force attacks and secures your logins from attackers exploiting weak or stolen credentials. Single sign-on (SSO) is a session and user authentication service that permits an end user to enter one set of login credentials (such as a name and password) and be able to access multiple applications.
- In this e-poster, we want to share our experience in securing SAS® Viya® access by implementing single sign-on and 2 Factor Authentication with Duo Security, a vendor of cloud-based two-factor authentication services and SSO.

Access Flow:

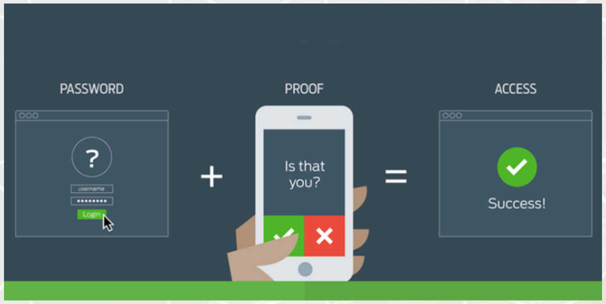


Image : Duo Security

CORECOMPETE

Securing SAS® Viya® Access with Single Sign-on and 2FA

Sandeep Grande, Senior SAS Administrator

CORE COMPETE INC

Index

Please use the headings above to navigate through the different sections of the poster

Intro

- SAS Viya Logon Manager supports authenticating users against an external identity provider via SAML. The Security Assertion Markup Language (SAML) 2.0 standard defines a framework for exchanging security information between relying partners in a federation

Term: Concept

Federation: Two or more security domains with trust established between them.

Assertion: XML document that is created and sent during a federated access request and contains claims about a user.

Claims: Information of a federated member is asserting to be true.

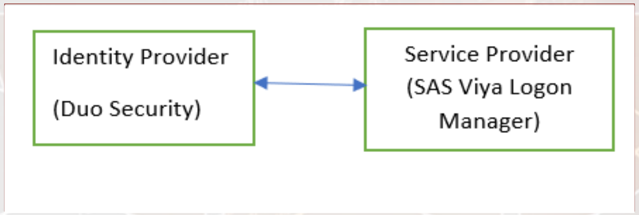
Identity provider: A federation member that creates assertions for its users. Also referred to as the asserting party.

Service provider: A federation member that consumes assertions to make access control decisions for its applications. Also referred to as a relying party.

Metadata: XML document produced by a SAML provider to describe its service endpoint URLs, x.509 certificate and other information in a standard way for consumption by partners in the federation

Objective

- The objective here is to establish SAML Communication between Identity Provider (Duo Security) which authenticates the users and Service Provider (SAS® Viya® Logon Manager) which provides access to application for successfully authenticated users.



CORECOMPETE

Securing SAS® Viya® Access with Single Sign-on and 2FA

Sandeep Grande, Senior SAS Administrator

CORE COMPETE INC

Please use the headings above to navigate through the different sections of the poster

Pre-Requisites:

Before configuring SAS Viya, we need to obtain Identity Provider Metadata. Configuring Duo Security requires configuring Duo Access Gateway at your site. The SAML Provider should send a link that provides metadata about SAML Provider. Example: https://<hostname>/metadata.php

Steps :

These are the high-level steps to be performed to secure SAS Viya with single sign-on and 2FA:

1. Configure the Service Provider in SAS Environment Manager
2. Configure the Identity Provider properties in SAS Environment Manager
3. Restart Logon manager microservice to generate Service Provider Metadata at SASLogon/saml/metadata
4. Configure the Identity Provider (Third-Party) – Duo Security

CORECOMPETE

Securing SAS® Viya® Access with Single Sign-on and 2FA

Sandeep Grande, Senior SAS Administrator

CORE COMPETE INC

Index

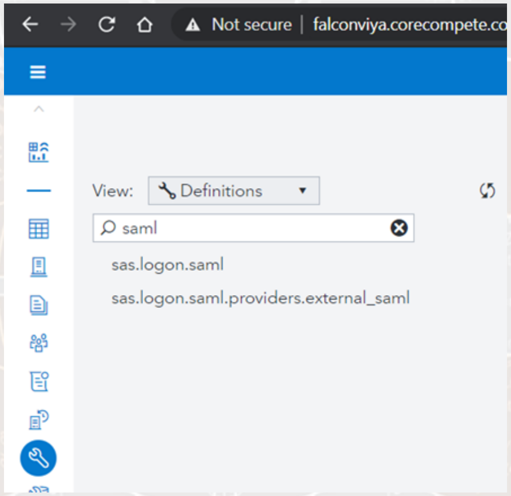
Please use the headings above to navigate through the different sections of the poster

Configuration

Configuring SAML Authentication requires exchanging Metadata information between Identity Provider and Service Provider.

Step 1: Configure the Service Provider in SAS Environment Manager

Go to SAS Environment Manager > Configuration > Definitions > search SAML. Create new configuration for sas.logon.saml. This definition has set of SAML service provider properties that are used to enable sign-ins using an external provider. Modifying one of these property values requires you to restart SAS Logon Manager



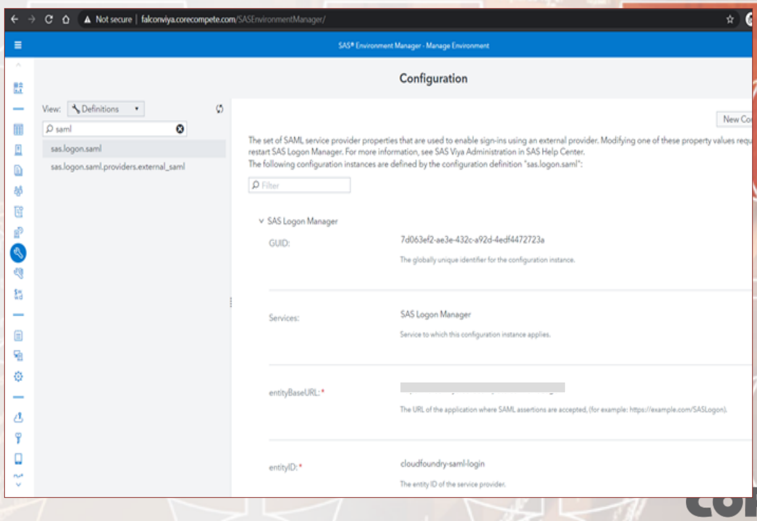
Not secure | falconviya.corecompete.co

View: Definitions

saml

sas.logon.saml

sas.logon.saml.providers.external_saml



Not secure | falconviya.corecompete.com/SASEnvironmentManager/

SAS® Environment Manager - Manage Environment

Configuration

View: Definitions

saml

sas.logon.saml

sas.logon.saml.providers.external_saml

The set of SAML service provider properties that are used to enable sign-ins using an external provider. Modifying one of these property values requ restart SAS Logon Manager. For more information, see SAS Viya Administration in SAS Help Center.

The following configuration instances are defined by the configuration definition "sas.logon.saml":

SAS Logon Manager

GUID: 7d063ef2-ae3e-432c-a92d-4edf4472723a

The globally unique identifier for the configuration instance.

Services: SAS Logon Manager

Service to which this configuration instance applies.

entityBaseURL:* [redacted]

The URL of the application where SAML assertions are accepted, (for example: https://example.com/SASLogon).

entityID:* cloudfoundry-saml-login

The entity ID of the service provider.

Securing SAS® Viya® Access with Single Sign-on and 2FA

Sandeep Grande, Senior SAS Administrator

CORE COMPETE INC

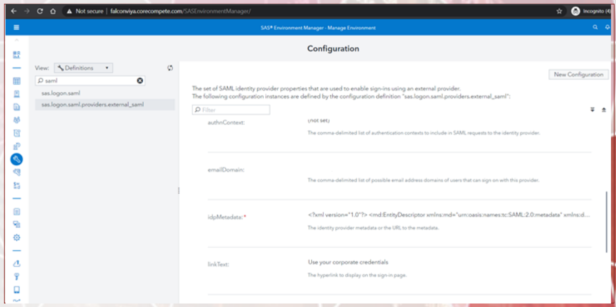
Index

Please use the headings above to navigate through the different sections of the poster

Step 2: Configure the Identity Provider properties in SAS Environment Manager

Go to SAS Environment Manager > Configuration > Definitions > search SAML. Create new configuration for sas.logon.saml.providers.external_saml. This definition has set of SAML identity provider properties that are used to enable sign-in using an external provider.

idpMetadata : The URL to the identity provider metadata. This definition requires SAML Identity Provider Metadata obtained as part of pre-requisites.


Not secure | falconviya.corecompete.com/SASEnvironmentManager/
Incognito (4)
SAS® Environment Manager - Manage Environment
View: Definitions
saml
New Configuration
Filter

Configuration

sas.logon.saml
sas.logon.saml.providers.external_saml

The set of SAML identity provider properties that are used to enable sign-ins using an external provider.
The following configuration instances are defined by the configuration definition "sas.logon.saml.providers.external_saml":

authnContext: (not set)
The comma-delimited list of authentication contexts to include in SAML requests to the identity provider.

emailDomain:
The comma-delimited list of possible email address domains of users that can sign on with this provider.

idpMetadata: * <?xml version="1.0"?> <md:EntityDescriptor xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata" xmlns:d...
The identity provider metadata or the URL to the metadata.

linkText: Use your corporate credentials
The hyperlink to display on the sign-in page.

Step 3: Restart SAS Viya Logon Manager

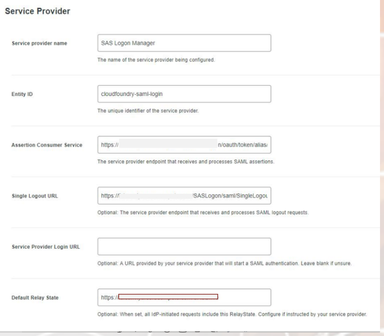
We need to restart SAS Viya Logon Manager to generate service provider's metadata at /SASLogon/saml/metadata. Below is the command to restart SAS Logon manager

```
systemctl restart sas-viya-saslogon-default
```

Step 4 : Configure the Identity Provider (Third-Party) – Duo Security

In this final step, we provide the SAML Identity provider with Service Provider's metadata generated in step 3 and below are the Duo specific properties that's are configured.

Name	Description
Service Provider Name	The name of the service provider.
Entity ID	The service provider identifier.
Assertion Consumer Service	The URL where your service provider receives SAML assertions.
Single Logout URL	Optional: The URL where your service provider receives SAML logout asser
Service Provider Login URL	Optional: Enter the URL for IdP-initiated logins if your service provider spec
Default Relay State	Optional: If your service provider requires a specific RelayState parameter, here.



Service Provider

Service provider name: SAS Logon Manager
The name of the service provider being configured.

Entity ID: cloudfoundry-saml-login
The unique identifier of the service provider.

Assertion Consumer Service: https://[redacted]n/oauth/token/alias/
The service provider endpoint that receives and processes SAML assertions.

Single Logout URL: https://[redacted]/SASLogon/saml/SingleLogou
Optional: The service provider endpoint that receives and processes SAML logout requests.

Service Provider Login URL:
Optional: A URL provided by your service provider that will start a SAML authentication. Leave blank if unsure.

Default Relay State: https://[redacted]
Optional: When set, all IdP-initiated requests include this RelayState. Configure if instructed by your service provider.

CORECOMPETE

Securing SAS® Viya® Access with Single Sign-on and 2FA

Sandeep Grande, Senior SAS Administrator

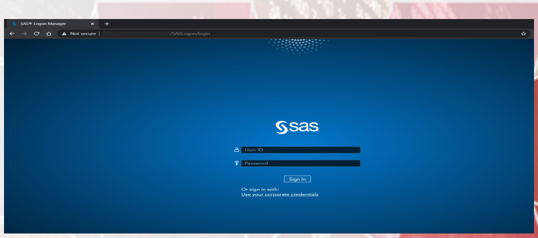
CORE COMPETE INC

Index

Please use the headings above to navigate through the different sections of the poster

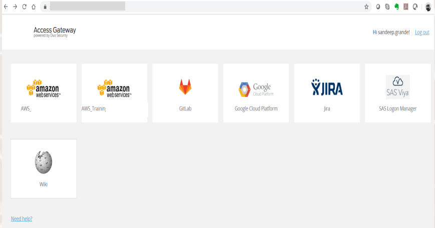
Results

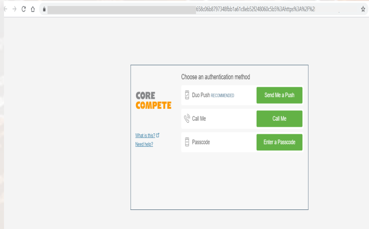
Once step 4 is configured they are generally two ways in accessing SAS Viya. One is using the SAS Logon page and is called as Service Provider Initiated login. In this login, user gets to choose to enter his corporate credentials using a link provided on SAS Logon Webpage as shown in below screen shot.

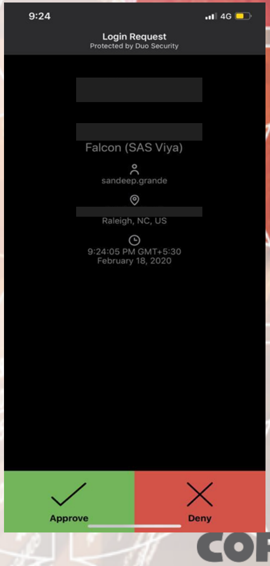


Or sign in with:
Use your corporate credentials

The other is IdP-Initiated SAML Authentication. The Identity Provider Initiated flow starts from the Identity Provider, typically a portal application, and users click a link to SAS Viya. SAML has a solution for the IdP-Initiated flow called the **RelayState** parameter. The RelayState was designed to be a state that the SP could pass to the IdP with the authentication request and get back in the subsequent response. In the IdP-initiated flow, the SAML RelayState has taken on a de facto use whereby the IdP can specify a URL to redirect the user to after authentication. Duo supports Relaystate parameter.







[redacted]

[redacted]

[redacted]

CORECOMPETE

Securing SAS® Viya® Access with Single Sign-on and 2FA

Sandeep Grande, Senior SAS Administrator
CORE COMPETE INC

Index

Abstract
Introduction
Steps
SP Config
IDP Config
Results
Conclusion

Thank you …

By implementing single sign-on and MFA , SAS Admin's can secure their SAS Viya environment against phishing, social engineering and password brute-force attacks and secured our logins from attackers.

Your comments and questions are valued and encouraged. Contact the author at:

Sandeep.Grande@corecompete.com
Technical Consultant
CORE COMPETE INC
Durham, NC

References

SAS® Viya® 3.5 Administration: Authentication – Available at https://documentation.sas.com/api/docsets/calauthmdl/3.4/content/calauthmdl.pdf?locale=en

SAML2.0 Wikipedia – Available at https://en.wikipedia.org/wiki/SAML_2.0

Duo Two factor authentication: Available at https://guide.duo.com/

SAS Viya 3.4 Simplified SAML or OpenID Connect Integration – Available at https://communities.sas.com/t5/SAS-Communities-Library/SAS-Viya-3-4-Simplified-SAML-or-OpenID-Connect-Integration/ta-p/575811

Please use the headings above to navigate through the different sections of the poster

CORECOMPETE

SAS® GLOBAL FORUM 2020

USERS PROGRAM

MARCH 29 – APRIL 1 | WASHINGTON, DC | #SASGF