Paper SAS3426-2019

Under One Umbrella: Single Sign-On with SAS® 9.4 and SAS® Viya®

Mike Roda, SAS Institute Inc.

ABSTRACT

Although organizations are increasingly leveraging SAS® Viya®, many have substantial investment in SAS® 9.4 applications and will for some time. This paper looks at a new feature introduced in SAS Viya 3.4 that provides single sign-on with SAS 9.4, enabling users to move seamlessly between web applications in both environments without having to log on again, and making it possible to use them collaboratively (for example, displaying a SAS® Visual Analytics report from SAS Viya on the SAS® Information Delivery Portal).

INTRODUCTION

Sign-ins to SAS® web applications are handled by the SAS® Logon Manager in both SAS 9.4 and SAS Viya; however, the way those user credentials are authenticated differs substantially. User credentials are authenticated against the Metadata server in SAS 9.4, which by default uses host operating system accounts. In SAS Viya, customers must provide an LDAP directory with user and group membership information. By default, this is also used for authenticating user credentials. However, many customers have existing security infrastructure that support single sign-on.

As a software company that develops enterprise-level web applications, SAS has supported single sign-on, as an optional configuration, with many of the leading technologies used by SAS customers. For SAS 9.4, this includes proprietary vendors such as CA SiteMinder and IBM WebSEAL, as well as open standards such as Kerberos. SAS Viya, perhaps more focused on open standards, also supports Kerberos and directly supports SAML as well as OpenID Connect.

Indeed, a customer with both SAS 9.4 and SAS Viya deployments can effectively use single sign-on between the SAS environments by configuring each with single sign-on to their corporate infrastructure using Kerberos or SAML. However, customers not already using single sign-on with their corporate infrastructure can achieve single sign-on between SAS environments by leveraging a new feature introduced in SAS Viya 3.4.

This paper begins with an overview and comparison of the authentication technology in SAS Viya 3.4 and SAS 9.4. This is orthogonal to the topic of configuring single sign-on between the environments but gives a good background on how things work behind the scenes and what capabilities already exist. Details are provided for configuring single sign-on, and, importantly single sign-out, between SAS Viya 3.4 and SAS 9.4. There are differences in the format of user names between environments, so compatibility of user names is discussed. The conclusion reviews how single sign-on is achieved, what the options are, and limitations to be considered.

OVERVIEW

The SAS Logon Manager authenticates users and facilitates single sign-on between SAS web applications. However, the implementations for this important service are completely different between SAS Viya and SAS 9.4.

AUTHENTICATION IN SAS VIYA

The SAS Viya Logon Manager is based on the open-source Cloud Foundry User Account and Authentication (UAA) Server and modified significantly for the SAS Viya environment. Within the overall SAS Viya architecture, authentication services are provided to SAS Viya microservices and web applications using OAuth 2.0 and OpenID Connect (Roda 2018). These security protocols do not implement single sign-on directly, so this is facilitated using HTTP sessions. For clustered deployments, the SAS Logon Manager relies on an Apache Geode-backed distributed cache server to replicate sessions across all instances in the cluster.

Users can be authenticated in several ways. The UAA software can act as an identity provider itself and manage user accounts locally. However, this is currently used only for the initial "sasboot" account that is created for completing the initial configuration or performing system rescue, and "sasprovider" accounts used to administer tenants in a multi-tenant deployment. Regular user sign-ins must leverage one or more external identity providers supplied by the customer. LDAP is the default identity provider. Other options are Kerberos, PAM, SAML, OpenID Connect, or SAS 9.4, which is the subject of this paper.

These providers can be grouped into two categories:

- direct authentication: The first category includes providers such as LDAP that can be called on directly to authenticate password credentials. When a user name and password have been entered on the sign-in page, SAS Logon Manager goes through each of these providers and attempts to authenticate the credentials until one of them is successful. For LDAP, which is the default identity provider in SAS Viya, SAS Logon Manager searches the LDAP directory for the account that matches the user name, obtains the DN for the account, and then attempts to bind to the LDAP server with that DN and the supplied password. The Pluggable Authentication Module (PAM) architecture is another example of a provider that can be used to authenticate credentials directly. In SAS Viya, PAM can be used to support multi-factor authentication (Steadman and Roda, 2018).
- remote authentication: The other category of identity providers authenticates users remotely and pass back some type of assertion, token, or ticket that is processed by the SAS Logon Manager. This can be used to support enterprise single sign-on. SAML and OpenID Connect fall into this category. They are presented on the sign-in page with an optional link or setup to automatically redirect to the provider. Kerberos is a unique case that overlaps both categories. Typically, the sign-in page is not displayed, and the browser performs a Kerberos handshake that results in a ticket being sent to the server. However, it is used to authenticate user name and password credentials sent to the SAS Logon Manager API by non-browser clients.

MIDDLE-TIER AUTHENTICATION IN SAS 9.4

The SAS 9.4 Logon Manager is based on the open-source Central Authentication Service project. This protocol is designed to support single sign-on. Instead of HTTP sessions, it issues a ticket granting cookie (TGC) to the web browser. In a clustered environment, all instances of the SAS Logon Manager share a Gemfire-backed distributed cache of tickets so that any instance will accept the TGC sent by the web browser and issue service tickets for applications accordingly.

As mentioned in the introduction, user logins are authenticated by the metadata server by default, and this authenticates the credentials against the host operating system. However, numerous other mechanisms can be configured for authentication and grouped under a common umbrella referred to as web authentication. In this mode, the CAS software is

configured (by default since 9.4M2) to trust the authentication performed by the web application container. The container, Pivotal tc Server (Apache Tomcat), directly supports security protocols such as SPNEGO (Kerberos), LDAP, and several other methods of authenticating credentials. In addition, the container can be extended with "valves" to support CA SiteMinder, IBM WebSEAL, client certificate authentication, and even authentication performed upstream in the reverse proxy server. For the latter, numerous options are possible. For example, customers can install the native Shibboleth SP software for the Apache web server and use it to authenticate with SAML (Roda 2015).

COMPARISON

Table 1 below gives a quick comparison between the middle-tier authentication architecture used in SAS Viya and SAS 9.4.

Concept	SAS 9.4	SAS Viya
Security Protocol	Central Authentication Service	OAuth 2.0 and OpenID Connect
To access service you need	Service or proxy ticket, 1 min lifetime	Access token, 12-hour lifetime
Browser is redirected to	/SASLogon/login	/SASLogon/oauth/authorize, then /SASLogon/login if necessary
Browser used for single sign-on	Ticket Granting Cookie, 12-hour lifetime	HTTP Session Cookie, 30-minute lifetime
For a service to call another service	Use Proxy Granting Ticket to get Proxy Ticket	Reuse access token
After expiration	not applicable	Use Refresh Token (30-day lifetime) to get a new access token
API	/SASLogon/v1/tickets	/SASLogon/oauth/token
Security payload	None, tickets are opaque	Yes, JSON Web Token (JWT)
Validation	Service must make callback to SASLogon	Digital signature with optional remote validation
Ticket/token includes group membership information	No	Yes (as scopes)

Table 1. Comparison of SAS 9.4 and SAS Viya Middle-Tier Authentication Architecture

SINGLE SIGN-ON AND SINGLE SIGN-OUT

While the underlying authentication architecture differs significantly, SAS Viya can be configured to integrate with SAS 9.4. SAS Viya 3.3 added support for authenticating credentials against SAS 9.4, and SAS Viya 3.4 further extended this to support single sign-on and single sign-out. Single sign-on and single sign-out affects only the SAS Viya 3.4 visual interfaces that use SAS Logon Manager, so SAS Studio® 4.4 is not affected. Figure 1 below describes the single sign-on flow starting from SAS Viya.

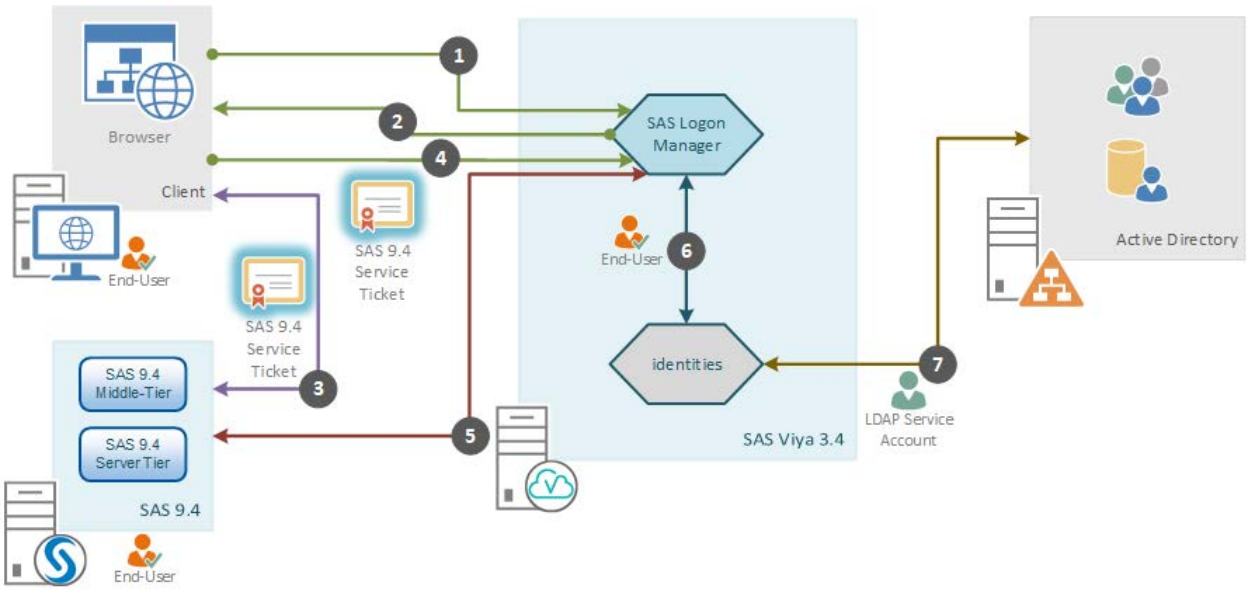


Figure 1. Single Sign-On Flow from SAS Viya

1. The client web browser connects to the SAS Logon Manager in SAS Viya after being redirected from a visual interface.
2. If the request to SAS Logon does not have an existing session, the SAS Logon Manager on SAS Viya displays the sign-in page, giving the end user a choice between entering credentials on the form or clicking a hyperlink to sign on using SAS 9.4. The hyperlink contains the service URL that the SAS Logon Manager on SAS Viya wants the browser to be redirected back to with a service ticket.
3. The client web browser connects to the SAS Logon Manager on SAS 9.4 when the end user clicks the hyperlink. After authenticating the end user, the browser is redirected back to the SAS Logon Manager on SAS Viya with a service ticket.
4. The browser calls the SAS Logon Manager on SAS Viya and passes the service ticket.
5. The SAS Logon Manager on SAS Viya makes an out-of-band request to the SAS Logon Manager on SAS 9.4 to validate the service ticket and obtain the user name of the end user. Note that the domain is stripped off the user name by the SAS Logon Manager on SAS Viya.
6. The SAS Logon Manager on SAS Viya connects to the identities microservice to fetch the end user's custom and LDAP group memberships.
7. The identities microservice connects to the LDAP server using the LDAP Service Account to look up the group memberships assigned to the user name.

In single sign-out, signing out of one environment signs the user out of both environments. No change is noticeable when signing out of a SAS 9.4 web application. Behind the scenes, the SAS Logon Manager on SAS 9.4 makes requests to all the URLs for which the user has obtained service tickets, notifying them that the user associated with the service ticket has signed out. These requests are made out-of-band, so they are transparent to the user. The SAS Logon Manager on SAS Viya receives the notification and invalidates the user's HTTP session, which it has previously associated with the service ticket. This causes events to be sent out to all the SAS Viya web applications and microservices, notifying them of the logout, so they might terminate any HTTP session associated with the user and invalidate tokens as well. When a user signs out of SAS Viya, the user is redirected to the logout endpoint of the SAS Logon Manager on SAS 9.4. This facilitates the sign-out on that

environment. However, the user's web browser is left on the sign-out page on SAS 9.4. Unfortunately, there is no Sign In button to take the user all the way back to SAS Viya.

CONFIGURATION

SAS 9.4 CONFIGURATION

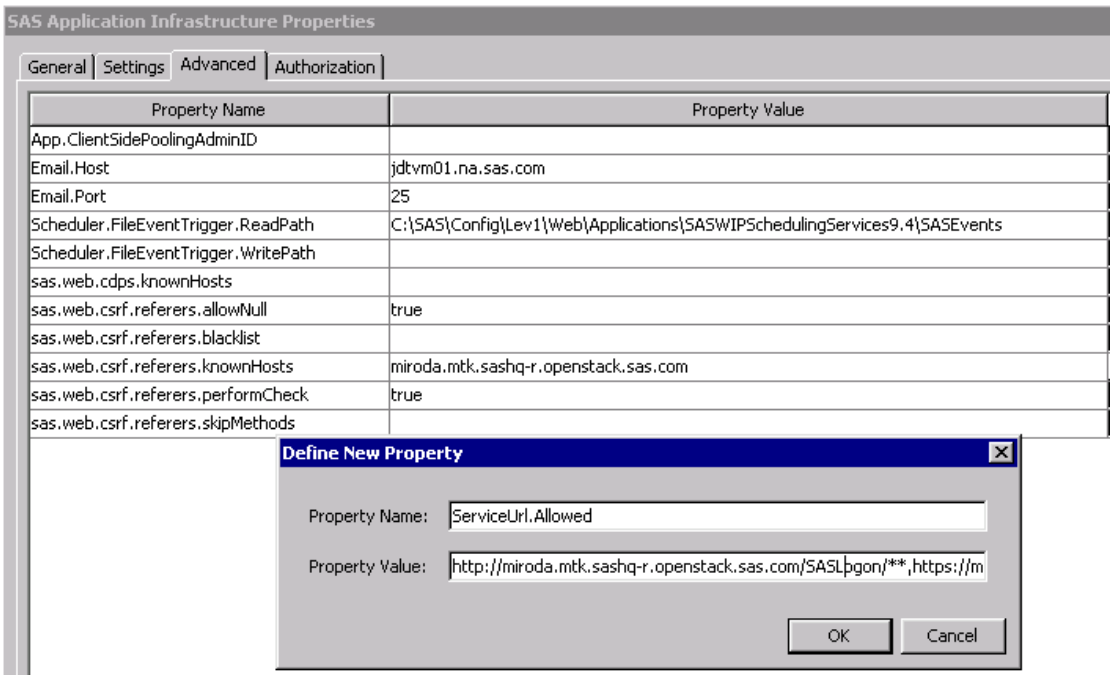
The SAS 9.4 middle-tier security properties must be updated about the SAS Viya deployment. Those configuration changes are described below. A restart of SASServer1 is necessary, at a minimum, after making these changes.

Allowed Service URLs

In a single sign-on setup with SAS Viya, the SAS Logon Manager on SAS 9.4 acts as the identity provider and issues service tickets to the SAS Logon Manager on SAS Viya. As a security measure, the SAS Logon Manager on SAS 9.4 issues tickets only to services it knows about. By default, it builds a list of application URLs from the metadata connection properties and other sources it knows about, but the SAS Viya URL needs to be added. This is done in SAS® Management Console.

1. In SAS Management Console, expand Application Management and then Configuration Manager.
2. Right-click SAS Application Infrastructure, select Properties, and open the Advanced tab.
3. If there is already a property listed for ServiceUrl.Allowed, edit it. If not, click the Add button and create it.
4. For the value, enter the top-level URL to the SAS Viya Logon Manager with /** at the end. The full URL needed here is actually /SASLogon/login/j_spring_cas_security_check, but /** is easier to enter and less error prone. Most likely the URL will be using https, but if http is being used, enter that. It can be entered both ways to be safe.

Display 1 is a screen capture of SAS Management Console where ServiceUrl.Allowed is set.



Display 1. Setting ServiceUrl.Allowed in SAS Management Console

Cross-Site Request Forgery

Another security feature involved here is Cross Site Request Forgery (CSRF). SAS 9.4 enforces restrictions on the Referer header for websites that link directly to it. Again, a default list of URLs is built automatically, but the SAS Viya host name needs to be added. On the Advanced tab, there should be an existing entry for sas.web.csrf.referers.knownHosts. To unlock this property, click on the lock icon to the right and enter the host name for the SAS Viya machine in the value.

Certificate Trust

The SAS 9.4 middle tier must be configured to trust the certificate presented by the SAS Viya environment by adding that certificate, or the Certificate Authority chain that signed it, to the SAS Private JRE truststore on the SAS 9.4 environment. If the Apache HTTP Server (httpd) on SAS Viya is using the default self-signed certificate, the certificate can simply be copied from the machine running the httpd server and imported into the SAS 9.4 environment.

For example, on RedHat Linux, the default self-signed certificate is /etc/pki/tls/certs/localhost.crt. If the certificate used by the httpd server was signed by a Certificate Authority (CA), the best practice is to import the CA chain instead.

In either case, the mechanism by which certificates are imported into the SAS 9.4 environment depends on the maintenance level of the environment:

- SAS 9.4M3 and later: You can import certificates by using the SAS® Deployment Manager.
- SAS 9.4M2 and earlier: You can import certificates by using the Java keytool command directly into the truststore of the SAS Private JRE. For consistency, the truststores on multi-machine deployments should be kept synchronized, so this should be done on all the server hosts, but technically only required on the hosts running SASServer1.

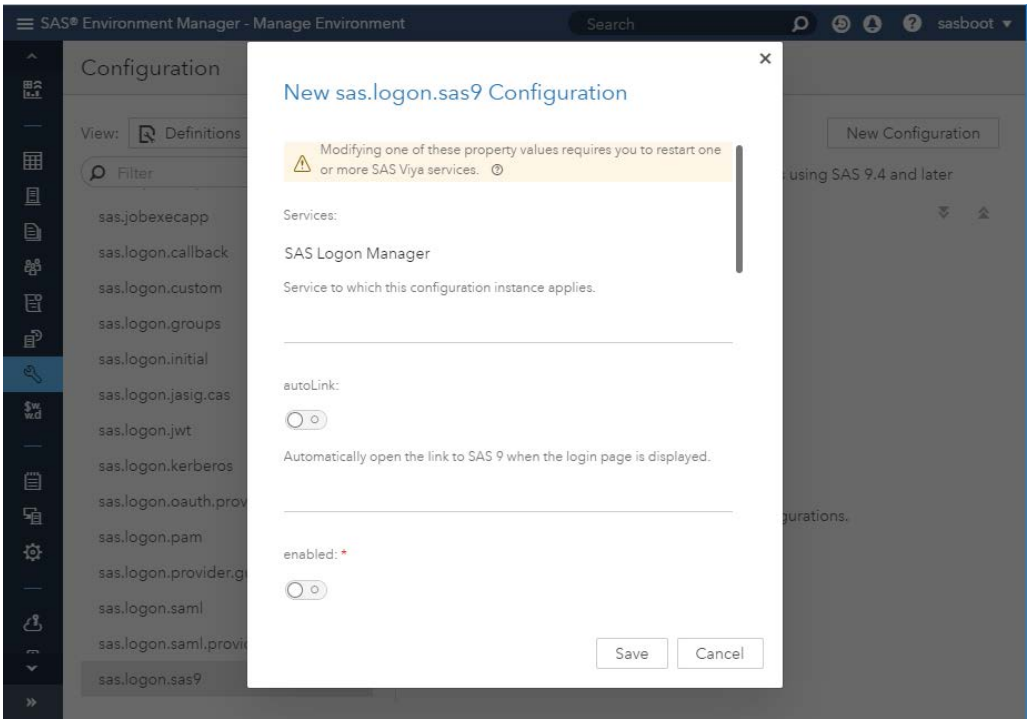
SAS VIYA CONFIGURATION

Configuring SAS Viya for single sign-on with SAS 9.4 involves adding Central Authentication Service (CAS) used by SAS 9.4 as an external identity provider to the SAS Logon Manager in SAS Viya. SAS Viya maintains a list of external identity providers that it uses to authenticate credentials, such as with the LDAP, and/or redirect users to for authentication. The configuration to add and enable this identity provider in SAS Viya is done in SAS® Environment Manager.

1. Log on with an administrator account, and click on the wrench icon to go into the configuration area.
2. Select Definitions from the picklist at the top to see a list of all configuration definitions.
3. Scroll down the list, select sas.logon.sas9, and click the New Configuration button on the right.
4. If there is an existing configuration already, click on the icon to edit it rather than creating another one.
5. In the dialog box, make selections. After you save the changes, the sas-viya-saslogon-default service should be restarted.

Note: The properties for sas.logon.sas9 are internally mapped to another configuration, sas.logon.jasig.cas. This other definition exists for customers who want to configure SAS Viya to authentication with a CAS provider other than SAS. This definition provides more granular options that are not needed when using SAS 9.4.

Display 2 shows the SAS 9.4 properties in SAS Environment Manager.



Display 2. Configuring SAS 9.4 Properties in SAS Environment Manager

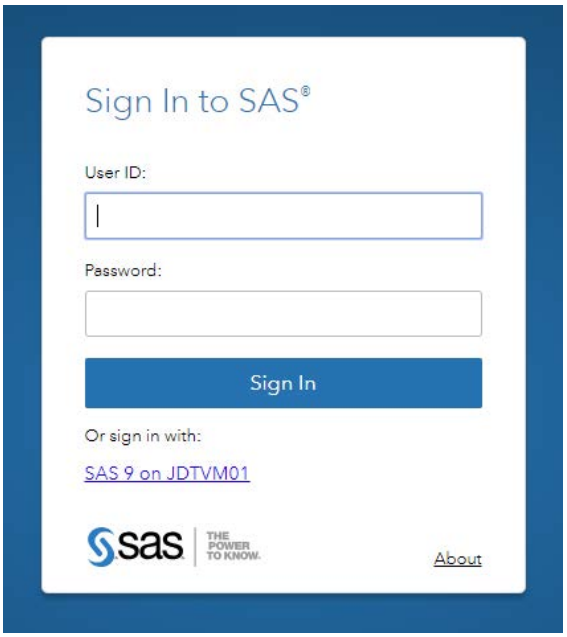
The fields from the sas.logon.sas9 configuration definition are described in Table 2 below.

Field	Default	Description
autoLink	Off	Automatically open the link to SAS 9 when the login page is displayed.
enabled	Off	The main switch for enabling sign-ins using SAS 9 credentials. It must be enabled for single sign-on, but it also enables SAS Viya to consume SAS 9.4 one-time passwords (OTPs) for running SAS Cloud Analytic Services code submitted from SAS 9.4.
linkText	Use your corporate credentials	The hyperlink to display on the sign-in page. Users can choose to enter credentials on the sign-in page or click this link to be redirected to SAS 9.4 for authentication.
sas9LogonUrl		The URL of the SAS 9 Logon Manager. The URL should end with /SASLogon.
showLinkText	Off	Show the link text on the sign-in page. Used with the linkText option above.
single.signOn.enabled	Off	Redirect to SAS 9 for single sign-on. This is the main option used to enable single sign-on.
single.signOut.enabled	Off	Local sign-out should sign user out of SAS 9 also. When enabled, users signing out of SAS Viya will end up on the SAS 9.4 signed out page. Note that no Sign In button will be displayed to return to SAS Viya.
viyaLogonUrl		The URL of the SAS Viya Logon Manager. The URL should end with /SASLogon.

Table 2. Properties for the sas.logon.sas9 Configuration Definition

With showLinkText turned on and autoLink left off, the link to SAS 9.4 is displayed on the SAS Viya sign-in page. When users access the sign-in page, they can choose to enter credentials directly on the page or click on the hyperlink to sign on with the SAS 9.4 system. If the user is already signed on to SAS 9.4, the browser is automatically redirected back to SAS Viya and the application from which the user started. Otherwise, the user must sign on using the SAS 9.4 sign-in page.

Display 3 shows the Sign-In page with link to SAS 9.4.



Display 3. Sign-In Page with Link to SAS 9.4

Certificate Trust

If the SAS Web Server on SAS 9.4 has been configured for HTTPS, the SAS Viya environment will need to be configured to trust the certificate presented to it by adding the certificate or CA chain to the truststore on the SAS Viya environment. This can be completed using Ansible (Linux Full Deployment) or manually using the Java keytool command to import the certificate or CA chain directly into the truststore. Restart the sas-viya-saslogon-default service to pick up changes to the truststore.

Auto Redirect

Once single sign-on is working using the hyperlink on the sign-in page, automatic redirection can be enabled. Note that sign-ins using LDAP or internal accounts such as sasboot or sasprovider are not possible once this is configured. Therefore, it is critical that administrators can sign on using the hyperlink and opt in to their administrator privileges. Edit the sas.logon.sas9 configuration again, and turn on the autoLink option. It might take up to a minute for the change to take effect, but a restart is not necessary. Users will automatically be redirected to SAS 9.4 for sign-in once this option is enabled.

Reverting Changes

Changes can be made to the configuration for sas.logon.sas9 by going back into SAS Environment Manager as an administrator and finding the existing configuration, making the necessary changes, and saving the changes. This might require a restart of saslogon to take effect. If you are unable to sign on as an administrator, the SAS configuration command-line interface (CLI) can be used to update the configuration. The following example is for Linux.

1. Initialize the CLI and login:

```
. /opt/sas/viya/config/consul.conf && /opt/sas/viya/home/bin/sas-admin
profile init && /opt/sas/viya/home/bin/sas-admin auth login
```

2. Get the existing configuration for sas.logon.sas9 and save it to a file:

```
/opt/sas/viya/home/bin/sas-admin configuration configurations download -d
sas.logon.sas9 --target filename
```

The output will be written to the file specified. From that file, the ID and existing values can be obtained.

3. Create a new file in the format shown below, substituting the ID and values from the existing configuration.

```
{
   "version":2,
   "count":1,
   "name":"configurations",
   "items":[
      {
         "version":1,
         "id":"b2877cd5-7c6e-4cdf-8ca7-f26d3ccabc68",
         "metadata":{
            "isDefault":false,
            "services":[
               "SASLogon"
            ],

"mediaType":"application/vnd.sas.configuration.config.sas.logon.sas9+json;v
ersion=2",
            "createdBy":"sasboot",
            "modifiedBy":"sasboot",
            "creationTimeStamp":"2018-11-26T15:14:52.235Z",
            "modifiedTimeStamp":"2018-11-26T15:14:52.235Z"
         },
         "showLinkText":true,
         "single.signOn.enabled":true,
         "single.signOut.enabled":false,
         "autoLink":false,
         "viyaLogonUrl":"http://miroda.mtk.sashq-
r.openstack.sas.com/SASLogon",
         "linkText":"SAS 9 on JDTVM01",
         "enabled":true,
         "sas9LogonUrl":"http://jdtvm01.na.sas.com/SASLogon"
      }
   ]
}
```

4. Update the configuration by passing the new file created in the last step.

```
./sas-admin --output json configuration configurations update --file
newfile
```

COMPATIBILITY OF USER NAMES

While there are many options to use for authentication with an external identity provider, group memberships in SAS Viya must always be obtained from LDAP. This means that the user name supplied by the authentication provider must be compatible with the LDAP search criteria configured on the Identities microservice. Internal SAS 9.4 "@saspw" accounts will not work unless some effort has been made to create these accounts in the LDAP directory. Furthermore, SAS Viya strips the domain qualifier from user names coming from SAS 9.4, so "sasadm@saspw" becomes just "sasadm" to SAS Viya. This can be overridden in Consul by adding a Key/Value property config/SASLogon/sas.logon.jasig.cas.stripDomain=false. For

example, this might be useful if SAS 9.4 were configured so that users entered an email address to sign on. Of course, the Identities microservice on SAS Viya would need to be configured to look up users by email address then as well.

CONCLUSION

In this paper we've seen how both SAS 9.4 and SAS Viya support several options for enabling single sign-on with a customer's corporate security infrastructure, and now with SAS Viya 3.4, single sign-on can be achieved between SAS environments. With the single sign-out option enabled, signing out of either environment signs the user out of both environments. However, this does have the limitation that users signing out of SAS Viya will land on the SAS 9.4 signed-out screen, without an option to return to their SAS Viya application. Another limitation is that single sign-on works only for SAS 9.4 user accounts that can be successfully queried by SAS Viya from LDAP. In most cases, this should be manageable, and customers who are leveraging both SAS 9.4 and SAS Viya should consider enabling this integration.

REFERENCES

Roda, Mike. 2015. "Federated Security Domains with SAS® and SAML." *Proceedings of the SAS Global Forum 2015.* Cary, NC: SAS Institute Inc. Available at https://support.sas.com/resources/papers/proceedings15/SAS1385-2015.pdf.

Roda, Mike. 2018. "OpenID Connect Opens the Door to SAS® Viya® APIs." *Proceedings of the SAS Global Forum 2018.* Cary, NC: SAS Institute Inc. Available at https://www.sas.com/content/dam/SAS/support/en/sas-global-forum-proceedings/2018/1737-2018.pdf.

SAS Institute Inc. 2018. "Add Your Certificates to the SAS Private JRE." In *Encryption in SAS® 9.4.* 6th ed. Cary, NC: SAS Institute Inc. Available at https://go.documentation.sas.com/api/docsets/secref/9.4/content/secref.pdf?locale=en#nameddest=n12033intelplatform00install.

SAS Institute Inc. 2018. "Manage Truststores." In *Encryption in SAS® Viya® 3.4: Data in Motion*. Cary, NC: SAS Institute Inc. Available at https://go.documentation.sas.com/api/collections/calcdc/3.4/docsets/calencryptmotion/content/calencryptmotion.pdf?locale=en#nameddest=n1xdqv1sezyrahn17erzcunxwix9.

SAS Institute Inc. 2018. "Whitelist of Websites and Methods Allowed to Link to SAS Web Application." In *SAS® 9.4 Intelligence Platform: Middle-Tier Administration Guide*. 4th ed. Cary, NC: SAS Institute Inc. Available at https://go.documentation.sas.com/api/collections/bicdc/9.4/docsets/bimtag/content/bimtag.pdf?locale=en#nameddest=p1xtsni38p58t3n1ljd2fy4c3joz.

Steadman, Jody, and Mike Roda. 2018. "Multi-Factor Authentication with SAS® and Symantec VIP." *Proceedings of the SAS Global Forum 2018,* Cary, NC: SAS Institute Inc. Available at https://www.sas.com/content/dam/SAS/support/en/sas-global-forum-proceedings/2018/2142-2018.pdf.

ACKNOWLEDGMENTS

Stuart Rogers from SAS has written about this feature in an internal company blog. In many ways, that work paved the way for this paper, and the single sign-on flow depicted in Figure 1 originated from his work. I am extremely grateful for his contribution.

CONTACT INFORMATION

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

Mike Roda
SAS Institute Inc.
100 SAS Campus Drive
Cary, NC 27513
mike.roda@sas.com