SAS® GLOBAL FORUM 2020 #SASGF

Paper SAS4597-2020

Behind the Front Door: Authentication Options with SAS® Viya®

Mike Roda, SAS Institute Inc., Cary, NC

ABSTRACT

If you are tasked with deploying and administering SAS® Viya®, one of your top concerns is how users will be authenticated. Will you use an LDAP directory, or is there a requirement to implement single sign-on with your company's existing security infrastructure? Learn what the authentication options are in SAS Viya 3.5 and what information you need to obtain from your IT security department to configure them. Learn how to limit concurrent logins and see examples of how to customize the login page. If you are administering an existing deployment, find out what new authentication options have been added since SAS Viya 3.4.

INTRODUCTION

One of the first decision a SAS Administrator needs to make is how users should be authenticated. This paper gives an overview of the authentication choices that exist in SAS Viya 3.5. Described in the following sections as identity providers, there are eight options, and often more than one is combined to authenticate different types of users. These are roughly characterized by those that use password-based authentication, and those that implement single sign-on. Some identity providers do both, and one (Guest) does neither since it is basically no authentication.

Table 1 lists the available identity providers for authentication.

Identity Provider	Password-Based	Single Sign-On
Internal (UAA)	Yes	-
LDAP	Yes	-
Kerberos	Yes	Yes
SAS 9.4 / CAS	Yes	Yes
PAM	Yes	-
SAML	-	Yes
OpenID Connect	-	Yes
Guest	-	-

Table 1. Identity providers for authentication

These chapters give a high-level overview of each identity provider and its associated options. This paper is not meant to be used as a configuration guide. Links to more detailed configuration resources are provided at the end. Readers should get a good sense of the different authentication choices they have, what features are supported, and an overview of the information they will need to collect before configuring authentication.

PASSWORD-BASED AUTHENTICATION

When users get the sign-in page and enter their username and password credentials, those credentials are authenticated directly against an identity provider. In a typical scenario, SAS Logon Manager is configured to authenticate users against an LDAP server such as Microsoft Active Directory. However, many other types of identity providers are supported, and more than one can be active at a time. When there are multiple identity providers, SAS Logon Manager will try to authenticate the user credentials against each one until a successful login is made.

INTERNAL USERS

The Cloud Foundry UAA project that SAS Logon Manager in SAS Viya is based on supports internal user accounts via an "uaa" identity provider. The "uaa" identity provider always exists and does not require configuration to enable, but it is used in a very limited capacity. Out of the box, a "sasboot" user account is created for the purpose of completing the initial configuration. Its password is randomized by default, and a link to reset the password is written to the logs.

Error! Reference source not found. shows an example of the reset password link appearing in the saslogon log.

```
2019-11-11 14:46:29.211  INFO 12626 --- [           main]
c.s.l.s.b.PasswordResetScimUserBootstrap : service
[LOGON_INFO_GEN_INITIAL_PASSWORD]
Reset the password for the initial user "sasboot" by using this link:
/SASLogon/reset_password?code=58ha3ycmi2
```

Output 1. Log message will the reset password link

An administrator must copy the link and paste it into his or her web browser. It can only be used once and is valid for 24 hours. A new link is generated each time saslogon is restarted. If there are multiple instances of services running, each one will generate a valid link. Alternatively, the password can be preset by setting the property sas.logon.initial.password. This would typically be done in the sitedefault.yml file but could also be set manually using the sas-bootstrap-config CLI. The property is only evaluated when saslogon starts and if set, it will use the specified password and not write the link to the logs. Aside from the page that comes up when using the reset password link, no other account management pages are surfaced in SAS Viya.

In multi-tenant deployments, the playbook also creates an internal "sasprovider" account in each tenant. This account is meant to be used by the provider administrator to gain access to the tenant for support and administration purposes, thus alleviating the need for a provider account in the tenant's identity and access management system.

LDAP

SAS Viya 3.5 requires access to LDAP to pull user identities and group memberships, so it is only natural that this is also the default identity provider for regular user logins. LDAP configuration is completed in SAS Environment Manager. SAS Logon Manager users the sas.identities.providers.ldap.connection and sas.identities.providers.ldap.user configurations, which are shared with the Identities microservice.

In the connection properties, the protocol, hostname, and port of the LDAP server need to be obtained. Only a single LDAP server can be used per tenant, so this needs to be a server with a global view of the directory. Microsoft Active Directory sites should use the global catalog server; however, LDAP referrals are supported should one need to connect SAS Viya directly with a domain controller. Encryption using LDAPS and startTLS is supported. These may require the server's certificate or certificate authority chain be imported into SAS Viya.

Regular unencrypted LDAP connections can be used but this should only be used in test environments since user passwords will be sent over the network in cleartext.

Also needed in the connection information is a distinguished name (DN) and password for a system account that SAS Logon can use to search the directory. Anonymous connections are also supported. When users are authenticated with LDAP, SAS Logon first binds to the LDAP server using the system account or anonymous connection and searches the LDAP directory using a specified search filter and starting at a specified base DN in the directory. If a directory entry is found, SAS Logon disconnects from the LDAP server and attempts to bind with the user's DN and supplied password.

The username is taken from the LDAP attributes. This allows the username to be consistent between sign-ins, since SAS Viya usernames are case sensitive and LDAP implementations such as Active Directory allow the username to be specified in mixed case.

SAS 9.4 METADATA ONE-TIME PASSWORD

SAS Viya can be configured to consume SAS 9.4 one-time passwords (OTPs) for running SAS Cloud Analytic Services (CAS) code submitted from SAS 9.4 (Stuart, 2018). This feature has been supported since SAS Viya 3.3 and is enabled on the SAS Viya side from within SAS Environment Manager by creating a configuration for sas.logon.sas9.

PLUGGABLE AUTHENTICATION MODULE

On Linux deployments, SAS Logon Manager can be configured to authenticate password credentials against a Pluggable Authentication Module (PAM). When enabled, only the name of the module is required. The "sasauth-viya" module is recommended. PAM support is provided for those customers that want to trigger a PAM login whenever users sign in to SAS Viya with username and password credentials. For example, PAM can be used to facilitate multi-factor authentication with SAS and Symantec VIP (Steadman and Roda, 2018).

KERBEROS

Kerberos authentication is a hybrid. Web logins normally use the SPNEGO protocol, which challenges the web browser to authenticate with a Kerberos ticket, but Kerberos can and is also used to authenticate usernames and passwords. Kerberos authentication has been supported since SAS Viya 3.4 and is required on all Windows deployments (Rogers, 2018). Kerberos authentication is enabled by adding the "kerberos" keyword to profiles.active property in the "spring" configuration for SAS Logon, and by creating a configuration for sas.logon.kerberos.

An Active Directory service account with the HTTP Service Principal Name (SPN) and Kerberos keytab are required as a prerequisite. The Active Directory administrator usually provides these, and the SAS administrator will test the keytab before configuring SAS Viya. Java services must be able to determine the default realm and KDC. A site will usually specify these in a krb5.ini or krb5.conf file on the machine and Java will look in the standard places for this file. Additionally, the location of the Kerberos configuration file, the realm, and the KDC can all be specified using JVM options.

Kerberos can be used only to authenticate users on the front end, but it is often used with delegation to launch backend compute or CAS servers (Rogers, 2018). There are two types of delegation, constrained and unconstrained. With unconstrained delegation, SAS Logon will cache the Kerberos credentials delegated by the web browser by converting the ticket to bytes and saving it to the credentials service. Other services can then retrieve the cached credentials on behalf of the user and use them to initiate a new Kerberos connection to the compute server or CAS server. SAS Viya 3.5 adds support for constrained delegation. Many sites are moving to constrained delegation and this is responsible in part by Windows 10, which comes loaded with Windows Defender Credential Guard, a security package that prevents the client from delegating credentials.

When Kerberos is enabled on the system, web users typically do not see the sign-in page. Their web browser is redirected to SAS Logon from a visual application and performs a Kerberos handshake. Browsers that do not support Kerberos will instead fail to authenticate and land on the login page, where users will have the opportunity to sign in using their username and password. Note that some web browsers will present a login window that the user needs to cancel out of before the SAS Viya login page is displayed (Rogers, 2019).

SINGLE SIGN-ON

SAS Logon Manager supports standardized protocols that can be used to implement single sign-on, and in some cases also single sign-out. There are many advantages of single sign-on, the obvious being that users only need to sign in to their corporate security infrastructure once. This is not only convenient, but it is also more secure. Users don't have to give their password to applications like SAS, and corporate security infrastructure is usually very robust with options like multi-factor authentication.

When single sign-on is enabled in SAS Viya, a link for each authentication provider is displayed on the login page. It can also be configured to automatically redirect users to the provider or use discovery to choose between multiple providers.

Note that command-line tools and other applications that rely on passwords may still authenticate to SAS Viya with a password, so one of the earlier-mentioned providers may still be required.

SECURITY ASSERTION MARKUP LANGUAGE (SAML)

When multiple options exist for single sign-on, SAML remains the recommended choice since the protocol is more standardized and flexible than other options. SAS Logon Manager supports SAML authentication directly, so it does not require additional software to be installed. With the exception of importing certificates, all configuration can be completed in SAS Environment Manager. There are two flows, service provider (SP) initiated and identity provider (IdP) initiated. Both are supported.

In the SP-initiated flow, a user navigates to a SAS Viya web application and is redirected to SAS Logon Manager. SAS Logon Manager saves where the user came from in an HTTP session and redirects the user to the identity provider with a SAML message containing an authentication request. The user authenticates at the identity provider and is sent back to SAS Logon Manager with a SAML message containing the authentication response. SAS Logon Manager processes the authentication, recalls where the user originally came from, and redirects the user back to the SAS Viya web application.

In the IdP-initiated flow, a user that is already signed in to the identity provider selects the SAS Viya application from the identity provider portal. The identity provider sends the user to SAS Logon Manager with the SAML message containing the authentication and includes a RelayState parameter on the request. The RelayState parameter is configured at the identity provider and indicates the URL that the user should be redirected to after processing the authentication. SAS Logon Manager requires that the value provided in the RelayState parameter be a relative URL or it will ignore it.

The May 2019 maintenance update to SAS Viya 3.4 included support for the fore-mentioned RelayState parameter, as well as an optional authnContext configuration option that allows a list of authentication contexts to include in the SAML requests made to the identity provider.

Before configuring SAML authentication, the identity provider's certificate or certificate signing chain need to be imported into the SAS Viya truststore. Always follow the documented steps to update the truststore. SAML authentication is configured in SAS Environment Manager in two steps. The first step involves configuring the service provider information via the sas.logon.saml definition and requires a restart. The SAS Administrator will need an RSA private key and obtain a certificate. It is not necessary that this be the same key and certificate used by the Apache httpd server, but it can be. Self-signed certificates are fine here as well. After the restart, the service provider SAML Metadata can be given to the identity provider. The second step involves configuring information about the identity provider in the sas.logon.saml.providers.external_saml definition. This consists mostly of just entering the URL to the identity provider Metadata, or entering the Metadata XML directly, the latter allowing manual modification. The SAS Administrator may also need to know what NameID format to expect usernames in the SAML assertions, although the default value usually works.

Due to the way the SAML protocol uses POST requests to send users from the identity provider back to the service provider, Cross-Origin Resource Sharing (CORS) comes into play. The best way to handle this is to turn on developer tools in the web browser, go through the login process and examine the Origin header that the browser sends to SASLogon when it makes the POST request at the end of the flow. Then, create a configuration in SAS Environment Manager for sas.commons.web.security.cors and set the allowedOrigins property equal to the value shown in the Origin header. Note that the property can have multiple values separated by commas. The configuration need only be applied to SASLogon.

Another problem exists with SameSite cookies. Beginning in February 2020, a new release of Chrome will change how it handles cookies from sites that don't include a SameSite attribute. Previously, it would default to the most lenient setting, 'None', but now it will default to 'Lax'. This causes the browser to not send the session cookie back to SASLogon when it is coming from the identity provider. An update to SAS Viya 3.5 was shipped in early 2020 to address this issue. Create a configuration for sas.commons.web.security.cookies and set the sameSite property to 'None'. This configuration only needs to be applied to SASLogon. Note that the service must be restarted to pick up these changes.

OPENID CONNECT

An OAuth 2.0 and OpenID Connect (OIDC) server itself, SAS Logon Manager can be configured as a client to another server for the purpose of single sign-on. OIDC is an extension of OAuth 2.0 used for authentication (Roda, 2018). Compared to SAML, it is a relatively simple protocol, but unfortunately significant differences exist between implementations, so compatibility issues exist.

Before configurating SAS Viya, a client ID and secret need to be created in the OIDC server for SAS Viya, and the client must be authorized to use the "authorization_code" grant. The client ID and secret are configured in SAS Viya along with the URLs for the OIDC server's authorization and token endpoints. SAS Logon Manager must be able to validate the digital signature in tokens coming from the other server. There are two ways to do this. Either by entering the public key used to validate the signature, or by entering the URL on the server where the key can be obtained.

SAS 9.4 / CENTRAL AUTHENTICATION SERVICE

The SAS 9.4 middle tier security architecture uses the Central Authentication Service (CAS) single sign-on protocol. The SAS Logon Manager itself is an implementation of the CAS server and SAS 9.4 middle-tier web applications are CAS clients. Since version 3.4, SAS Viya can be configured as a CAS client to facilitate single sign-on and single sign-out between environments (Roda, 2019, Stuart, 2018).

Configuration on SAS Viya is completed in SAS Environment Manager. For CAS in general, there is a configuration definition for sas.logon.jasig.cas, while for SAS 9.4 there is a simplified definition for sas.logon.sas9 that should be used. Some configuration is also required in the SAS 9.4 environment and requires a restart of the SAS 9.4 middle tier.

With the single sign-out option enabled, signing out of either environment will sign 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 will only work for SAS 9.4 user accounts that can be successfully queried by SAS Viya from the configured LDAP provider.

GUEST

Guest access is a feature that allows anonymous public access to a specific and limited set of resources or web applications. When accessing participating applications, a Guest button is displayed on the login page. Users can choose to sign in with credentials or go in as the guest user. Out of the box, guest users cannot access any applications. A default set of rules may be imported into the system using the command line interface (CLI) and enable guest access for viewing reports in SAS Visual Analytics and the SAS Visual Analytics App. Guest access cannot be used in conjunction with Kerberos, and therefore isn't supported on Windows or Kerberized Linux deployments.

LOGIN OPTIONS

CUSTOM CONTENT

Custom content can be placed on the login, logout, and timeout pages by specifying the URL to the custom content. To use this, create a definition in SAS Environment Manager for sas.logon.custom. The custom content is displayed in an iframe.

In some cases, it may be desired to modify the parent window from the custom content. This can be achieved by using javascript and referencing the parent document. For example, the following HTML will hide the iframe and automatically open a new link to initiate a SAML single sign-on login.

```
<!DOCTYPE html>
<html class="bg" lang="en" dir="ltr">
<body>
  <script type="text/javascript">

parent.document.getElementsByClassName("customizations")[0].style.display =
'none';
    window.top.location.href =
'http://sas.example.com/SASLogon/saml/discovery?returnIDParam=idp&entityID=
saml-login&idp=xxx&isPassive=true';
  </script>
</body>
</html>
```

Note that due to the browser same origin policy, javascript from the custom content can only modify the parent document if it was loaded from the same domain. This can be arranged by having the Apache httpd proxy serve up the custom pages by placing them under /var/www/html/ on the machine running the httpd service.

PREVENT CONCURRENT LOGINS

By default, users may sign in an unlimited number of times concurrently from different web browsers or machines, resulting in multiple distinct HTTP sessions for the same user. Concurrency control can be enabled to restrict the number of sessions a user is allowed to have by creating a definition in SAS Environment Manager for sas.logon.sessions. When sessions are limited, the default behavior is to expire an existing session and grant a new session to the user attempting to authenticate. To override this behavior and prevent a new session from being granted, set this property: ejectNewSessionsIfMaxExceeded=true. If you use that approach, be aware that if a user doesn't explicitly log out, they may have to wait for their old session to expire before being able to log back in.

LOGIN HINT

Part of the OpenID Connect specification supported by SASLogon, the login_hint query string parameter is passed in the authorize request, which is /SASLogon/oauth/authorize. SAS Logon expects to receive an email domain in the hint. This value is compared against a list of email domains configured for each SAML or OpenID Connect identity provider. Note that the emailDomain property was added to the configuration definition for SAML in a maintenance update for SAS Viya 3.4 but can still be specified manually in older deployments by using the sas-bootstrap-config CLI.

Currently, there is no configuration support on the client end for passing the login_hint parameter in the authorize requests, but this can still be achieved by adding a RewriteRule to the Apache httpd configuration. For example:

```
RewriteEngine On
RewriteCond "%{QUERY_STRING}" !login_hint
RewriteRule "SASLogon/oauth/authorize"
"/SASLogon/oauth/authorize?login_hint=example.com" [QSA,PT]
```

This example works for a single identity provider. One could craft RewriteCond statements to set the login hint conditionally depending on where the request is coming from. Note that the placement of this rule is important. For deployments that are using HTTPS, this should be placed inside the VirtualHost of the SSL configuration. For example, on RedHat Linux this is the /etc/httpd/conf.d/ssl.conf file. For deployments that are not using HTTPS, this should be placed in a new .conf file. Httpd processes the .conf files in alphabetical order and this configuration needs to occur before the proxy configuration in proxy.conf, so it should be named accordingly, for example, login_hint.conf. Putting the redirect rule in both places is fine too. Httpd must be restarted to pick up changes to the configuration.

IDP DISCOVERY

IdP discovery is a new feature that was shipped as a maintenance update to the SAS Logon Manager in SAS Viya 3.4. When one or more SAML and/or OIDC identity providers are configured, they are listed on the SAS Viya sign-in page under a label that says, "Or sign in with:" and then a hyperlink with configurable text is shown for each one. It may not be desirable for users to have to click on this link for every sign in, especially if there are multiple identity providers to choose from. This is where IdP-discovery comes in. Implementations vary widely but SAS Logon Manager uses the domain of the user's email address to choose which identity provider to use.

The feature is enabled in SAS Environment Manager via the sas.logon.zone configuration and the property on that definition named idpDiscovery.enabled. When enabled, the initial sign-in page users see no longer displays username and password fields. Instead, it displays a field for the user to enter a user Id or email address. Figure 1 shows the user prompt when IdP discovery is enabled.

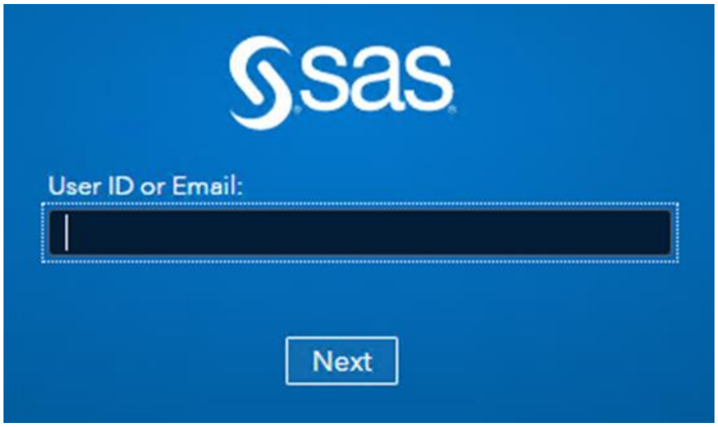

Figure 1. User prompt for IdP Discovery

Note that users need to enter an email address even if they don't use an email address as their username. The domain from the email address is matched against the optional list of email domains configured for each identity provider. If there is a match, the user is automatically redirected to that identity provider, in the same way as if they had clicked the link on the regular sign-in page. If there is no match, username and password fields are displayed as before. If they just type a username, then the username field on the login form is autocompleted for them.

CONCLUSION

SAS Administrators need to understand the authentication choices and login options that exist in SAS Viya 3.5 and be prepared to align that with their IT security policies. Since LDAP is required in all cases, it should be set up as part of the initial configuration and then checked to see that users and groups are populating in SAS Environment Manager. Authentication using LDAP can also be verified at this point, and in many cases this is sufficient.

For those that wish to have single sign-on, the choice will depend on what security infrastructure the company is already using. Sometimes more than one option exists. For example, users in an Active Directory environment may authenticate directly to SAS Viya using Kerberos or can use SAML to authenticate to Active Directory Federation Services (ADFS). Another common scenario is where the customer is using Okta for their identity management. Okta supports SAML as well as OpenID Connect, so either can be used to authenticate with SAS Viya. In some cases, it may be necessary to use both. For example, OpenID Connect could be used to authenticate external users with Google while SAML is used to authenticate internal users with ADFS. Furthermore, IdP-discovery can be set up to determine the correct identity provider for each user by their email address. Just be aware that all user identities need to exist in LDAP.

Those customers that have SAS Viya sitting alongside SAS 9.4 may opt to configure single sign-on directly between those environments. This may be particularly useful for sites that do not have a single sign-on security infrastructure, or are using older technologies like WebSEAL and SiteMinder, or that have already implemented a custom authentication solution with SAS 9.4.

Finally, sites that require guest access to reports can configure that, while allowing regular users to authenticate using LDAP or single sign-on (although not Kerberos).

REFERENCES

Rogers, Stuart. "SAS Viya connecting with SAS 9.4 One-Time-Passwords." Available https://blogs.sas.com/content/sgf/2018/06/21/sas-viya-connecting-with-sas-9-4-one-time-passwords. Last modified June 21, 2018. Accessed on February 5, 2020.

Rogers, Stuart. "SAS Viya 3.4 Kerberos with SAS Logon Manager." Available https://communities.sas.com/t5/SAS-Communities-Library/SAS-Viya-3-4-Kerberos-with-SAS-Logon-Manager/ta-p/523245. Last modified December 22, 2018. Accessed on February 5, 2020.

Rogers, Stuart. "SAS Viya 3.4 Windows with Kerberos." Available https://communities.sas.com/t5/SAS-Communities-Library/SAS-Viya-3-4-Windows-with-Kerberos/ta-p/523254. Last modified December 22, 2018. Accessed on February 5, 2020.

Rogers, Stuart. "SAS Viya 3.4 Kerberos with CAS." Available https://communities.sas.com/t5/SAS-Communities-Library/SAS-Viya-3-4-Kerberos-with-CAS/ta-p/523246. Last modified December 22, 2018. Accessed on February 5, 2020.

Rogers, Stuart. "SAS Viya 3.4 Kerberos with SAS Compute." Available https://communities.sas.com/t5/SAS-Communities-Library/SAS-Viya-3-4-Kerberos-with-SAS-Compute/ta-p/523250. Last modified December 22, 2018. Accessed on February 5, 2020.

Rogers, Stuart. "SAS Viya 3.4 with Fall-back Authentication." Available https://communities.sas.com/t5/SAS-Communities-Library/SAS-Viya-3-4-with-Fall-back-Authentication/ta-p/575810. Last modified July 23, 2019. Accessed on February 5, 2020.

Chrome Platform Status. "Cookies default to SameSite=Lax." Available https://www.chromestatus.com/feature/5088147346030592. Last modified January 28, 2020. Accessed on February 5, 2020.

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

Roda, Mike. 2019. "Under One Umbrella: Single Sign-On with SAS® 9.4 and SAS® Viya®." *Proceedings of the SAS Global Forum 2018 Conference.* Cary, NC: SAS Institute Inc. Available https://www.sas.com/content/dam/SAS/support/en/sas-global-forum-proceedings/2019/3426-2019.pdf

Rogers, Stuart. "SAS Viya 3.4 Single Sign-On & Sign-Out with SAS 9.4." Available https://communities.sas.com/t5/SAS-Communities-Library/SAS-Viya-3-4-Single-Sign-On-amp-Sign-Out-with-SAS-9-4/ta-p/523259. Last modified December 22, 2018. Accessed on February 5, 2020.

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

ACKNOWLEDGMENTS

I would like to thank Stuart Rogers for taking the time to review and contribute to this paper.

RECOMMENDED READING

SAS® Viya® 3.5 Administration: Authentication

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