Paper SAS299-2014

Secure Your Analytical Insights on the Plane, in the Café and on the Train with SAS® Mobile BI

Christopher Redpath and Meera Venkataramani, SAS Institute Inc., Cary, NC

ABSTRACT

Security-conscious organizations have rigorous IT regulations, especially when company data is available on the move. This paper explores the options available to secure a deployment of SAS® Mobile BI with SAS® Visual Analytics. The setup ensures encrypted communication from remote mobile clients all the way to back-end servers. In addition, the integration of SAS Mobile BI with third-party Mobile Device Management software and Virtual Private Network technology allow you to place several layers of security and access control to your data. The paper also covers the out-of-the-box security features of the SAS Mobile BI and SAS Visual Analytics administration applications to help you close the loop on all possible areas of exploitation.

INTRODUCTION

The world is more mobile than ever. The widespread consumer popularity of tablets and smartphones has created the demand on businesses and organizations to adopt them. This has fueled the growing popularity of mobile technology as an integral part of working life and has increased pressure on IT to facilitate the technology's exploitation. IT is now tasked with the need to supply employees and executives current and relevant business information while on the move.

IT, therefore, has to deal with many difficult questions in regards to its mobile strategy, one of the most important being - "How do you protect valuable corporate data?"

SAS MOBILE BI

SAS® Mobile BI is an application available for Apple® iPad® or Android™ Tablets and a critical component of the powerful SAS Visual Analytics solution. SAS Visual Analytics is an easy to use, web-based solution that leverages the SAS® LASR Analytic Server, and empowers organizations to explore small to huge volumes of data very quickly. A major cornerstone of SAS Visual Analytics is the framework of "build once, consume anywhere". Reports built through the SAS Visual Analytics Designer web interface can be consumed directly through SAS Mobile BI thanks to the adaptive presentation layer within the SAS Visual Analytics solution. This adaptive layer eliminates the need to create separate reports specific for the Visual Analytics Viewer web client or SAS Mobile BI. In particular, SAS Mobile BI enables IT to provide synchronized, up-to-date information for analysis and reporting on mobile devices. The application is free and can be downloaded from the respective application stores for the type of tablet. This makes the process of distribution easy and less expensive for IT. Business users can download the application anytime, anywhere with no cost and dependency to IT.

SECURITY SUMMARY

While information is quickly and easily delivered to mobile devices, IT still maintains control of the underlying data and security – overcoming one of the main concerns with providing organizational information via mobile devices.

In summary, below is a list of the security features that are available out of the box in SAS Visual Analytics 6.3 and SAS Mobile BI 6.3.x

- **Secure server:** Data and reports reside on a secure server. Users must log on with a user name and password combination in SAS Mobile BI to subscribe to any reports and access their data.
- **Security model:** The data and reports fall under the SAS Metadata security model. Identity-driven access controls to SAS content can be configured.
- **Encryption:** When a report is subscribed to by the end user, the offline report and the data behind it are encrypted on the local tablet.
- **Tethered only mode**: If this feature is enabled, users can view the reports only when connected to the server. The data from the device is erased once the user closes the report. Therefore, no data, even if encrypted, is saved on the device.
- **Black listing:** Once an administrator adds a device to this list, this device will not be able to connect to the server.
- **White listing:** Only devices added to this list will be able to access the server. (This feature is mutually exclusive with Black Listing.)

- **Data wipe out:** Users who are blacklisted will have any local data associated with that server erased when they try to reconnect to that server.
- **Application passcode:** Apart from the device passcode login, if enabled, an application passcode adds another layer to prevent unauthorized use of SAS Mobile BI application.
- **Application time out:** Administrators can set a time in days. If the user is inactive and did not connect to the server in the specified time frame, SAS Mobile BI application will freeze the content and not allow the user to access the content offline until the user logs in and is validated. (This feature is mutually exclusive with Tethered only mode.)

In addition, the out-of-the-box features can be supplemented with some additional security layers depending on your mobile device security strategy:

- **Secure Sockets Layer (SSL):** Protects communication between server and remote client to ensure encryption of communication.
- **Intranet wireless networks:** If a corporate tablet has access to intranet wireless networks, this means that the client-to-server communication happens within the organization's firewalls and is secured from the wider web.
- **Virtual Private Networks (VPN):** Many vendors now offer VPN software compatible with mobile devices. This enables secure communication between the SAS Mobile BI application and the back-end services across shared or public networks as if SAS Mobile BI were directly connected to the server private network.
- **Mobile Device Management (MDM):** With MDM, IT can easily control device settings on any managed device – corporate liable, BYO, or COPE – and ensure safe access to proprietary business information.
- **MDM application wrappers:** SAS Mobile BI supports some leading third-party MDM software packages for securely wrapping applications.

The next sections look at some of the above supplemental layers of security in more detail.

JUST LIKE MAKING A CAKE

We make an analogy between configuring the desired setup and the process of making a cake. Just like a cake, IT is free to pick and choose the majority of the layers to use in the final solution. Based on their specific requirement and the way they deliver content to the user base, the IT people can go for a low-fat, quick and simple cake or the rich full-fat cake.

FROM SERVER TO MOBILE DEVICE

An important factor in deciding your desired mobile device strategy is understanding the flow of data and information between the device and the back-end SAS Visual Analytics server. Here is a high-level summary for a vanilla (non-customized) deployment of SAS Visual Analytics.

SAS VISUAL ANALYTICS TRANSPORT SERVICES

The SAS Visual Analytic Transport Services component of the SAS Visual Analytics web tier is used to handle all authentication and communication between the tablet and the back-end SAS Visual Analytics server.

At a high level, the way the SAS Visual Analytics Transport Services facilitates this communication is outlined as follows:

1. An end user defines a connection in the application to the back-end server. This communication occurs through the Transport Services.
2. A valid user name and password must be provided on the connection setup to connect to SAS Metadata. A SAS user metadata profile must exist for the user name supplied.
3. Once SAS Metadata has authenticated the user, the user can navigate the SAS Metadata Folder structure that the SAS Metadata security model grants authorization rights to see.
4. Once the user finds a desired report, the user can select it and "Subscribe" to it.
5. From the tablet, a request is made to the Transport Service for the selected report.
6. The corresponding metadata definition of the report contains information about the associated LASR Analytic Server and table name.
7. The Transport Service passes this request to the SAS LASR Analytic Server.
8. The SAS LASR Analytic Server queries the source data before passing it back to the Transport Services for packaging.

9. The service then passes a final results package (that is, containing the resulting data and XML language describing the visuals) down to the tablet.
10. The report and data package is encrypted on the local tablet for offline use.
11. Now the user can interact with the report and native objects to explore and interact with the data. This interaction happens offline on the encrypted report and data package (**Note:** For large data reports, there might be calls back through the Transport Service with more data queries during interaction if the volume of data required to drive the report is above certain customer configurable thresholds.)

You will notice in the above there is no mention of encrypted communication between the tablet and the server. This is because there is none in such a vanilla deployment of SAS Visual Analytics. HTTP will be the primary communication protocol configured for the web tier that contains the SAS Visual Analytics Transport Service. This might be acceptable to you if the communication is happening within an internal intranet network, but is definitely not recommended when dealing with sensitive corporate data when SAS Mobile BI communicates from outside the organization inside, especially via potentially unsecured external networks.

SUPPLEMENTAL LAYERS OF THE CAKE

SSL AND SAS 9.4

With SAS 9.4 there is an increase in scope of SSL for the candidate application, the scope is now beyond simply securing the JEE container where the SAS web applications live but also authenticate endpoints and encrypt traffic. SAS Deployment Wizard (SDW) and SAS Deployment Manager (SDM) have been improved to handle most of the SSL configuration in an automated manner.

If you plan to use HTTPS, then it is best to enable this feature during the installation and configuration time frame with the SAS Deployment Wizard. The SAS Deployment Wizard prompts the user for the required SSL collateral during installation.

The new SAS 9.4 architecture includes the following components that can be configured for SSL:

1. SAS Web Server (an HTTP server used for reverse proxy)
2. SAS Web Application Server (lightweight web application server that runs the SAS web applications)
3. SAS Environment Manager (systems and application management for the SAS servers in your deployment)
4. SAS Deployment Agents (facilitate software deployment and system administration activities)

For the purposes of this paper, we will focus only on the SAS Web Server and SAS Web Application Server as they are generally directly involved in SAS Mobile BI communication with the back-end SAS Servers.

Transport layer security - Secure Sockets Layer

The Transport Layer Security (TLS) protocol allows client/server applications to communicate across a network in a way designed to prevent eavesdropping and tampering. Secure Sockets Layer (SSL), which is now formally known as TLS, is a protocol to establish a private and confidential conversation between two endpoints over an insecure network.

SSL uses:

1. Digital Identity Certificates, signed by a Trusted Authority, for authentication to ensure confidentiality, that is, to prevent eavesdropping.
2. Public/Private Key Crypto to secretly exchange a symmetric key (SSL Handshake).
3. Messages encrypted by strong algorithms (for example, AES), seeded with the shared symmetric key, to keep entire conversations private.
4. Message authentication codes for integrity.

Without digital certificates and a trusted authority, you can't achieve the initial authentication. Without authentication, you can't guarantee a private and confidential conversation.

The best practice is to acquire Certificate Authority (CA) signed certificates before you install and configure SAS software.

One-Way or Two-Way

The most popular SSL mechanism is one-way SSL. In this scenario, the server sends its certificate to the client application (SAS Mobile BI), and the client validates the server certificate using the CA public key. The handshake process then establishes a secure communication channel using a particular encryption algorithm.

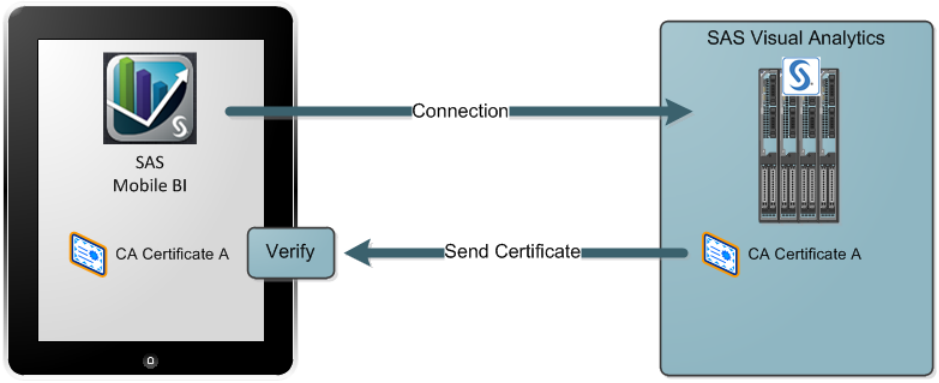

Figure 1. One Way SSL and SAS Mobile BI

In two-way SSL authentication, in addition to the above, during the SSL handshake not only does the client application verify the identity of the server application, but the server application verifies the identity of the client application. Two-way SSL authentication is also known as client authentication due to the fact that the client certificate is an important part of the process.

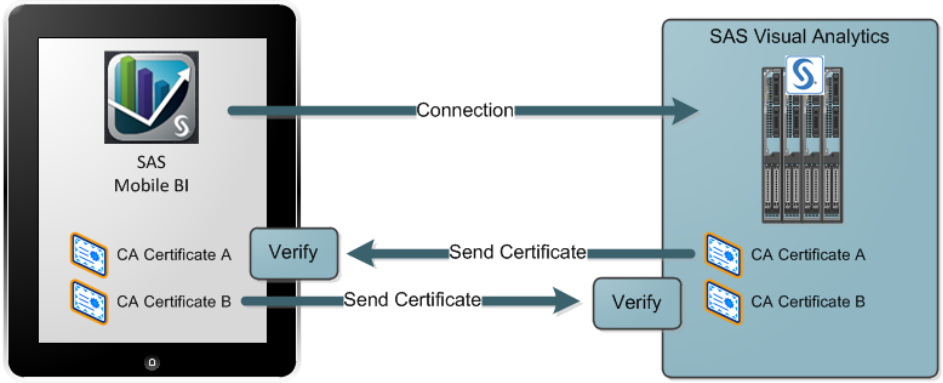

Figure 2. Two Way SSL and SAS Mobile BI

SSL CONFIGURATION

SDW during Configuration time

Discovering your specific needs and pre-planning deployments appropriately is part of the SAS pre-installation requirements process. One of the steps is to identify the requirement for SSL. The SAS Deployment Wizard (SDW) now includes options to do a lot of the complex configuration automatically, that is, SSL is no longer just a post deployment advanced configuration activity.

However, it is good to be aware that the automatic configuration configures SSL in specific ways. For example, in deployments that use the SAS Web Server, the SDW does not include an option to configure the SAS Web Application Server for HTTPS. The communication path between the SAS Web Server and the SAS Web Application Server uses HTTP, whereas the communication path between the clients and the SAS Web Server is over HTTPS.

This setup is generally enough for most customers looking to implement some form of SSL. The end-point, in this case the SAS Web Server, probably already resides in the internal network. However, many of you might require the downstream link to be SSL as a matter of policy, and thus it still is an important component for the overall configuration of SSL. For example, you might choose to house the SAS Web Server in a Demilitarized Zone (DMZ), which is not quite fully inside the corporate intranet. Therefore, to configure HTTPS between the SAS Web Server and the SAS Web Application Server, there are specific steps to follow in the *SAS® 9.4 Intelligence Platform: Middle-Tier Administration Guide*. Figure 3 below illustrates such a setup that houses the SAS Web Server in a DMZ to act as a reverse proxy to the back-end SAS Visual Analytics server.

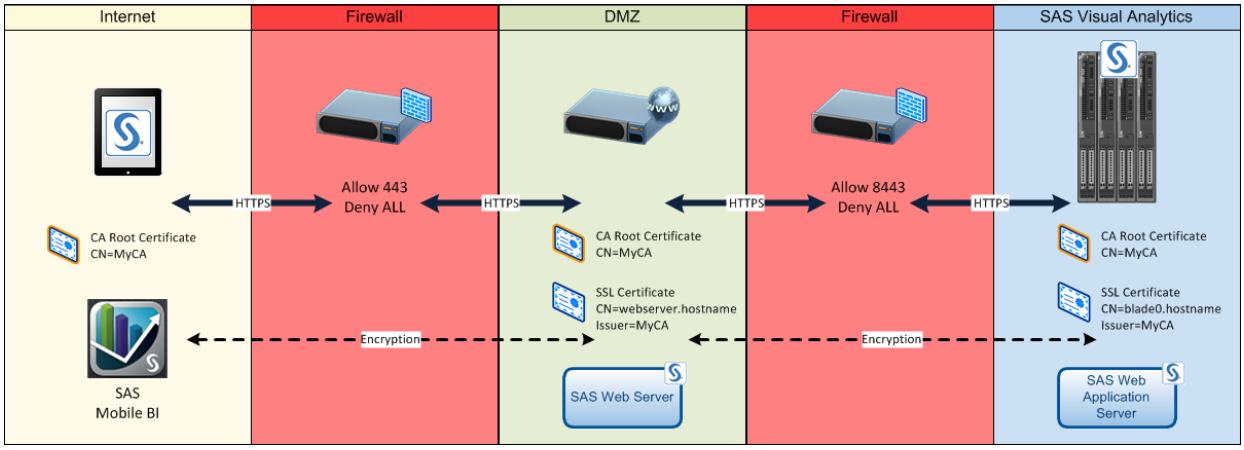

Figure 3. Example Setup Using HTTPS and the SAS Web Server in a DMZ

Manual Reconfiguring to Use HTTPS

If you have already deployed a SAS 9.4 environment and did not choose to configure with SSL during the initial installation and configuration with the SDW, you can manually configure the SAS Web Server to use HTTPS. All manual steps are captured in the *SAS® 9.4 Intelligence Platform: Middle-Tier Administration Guide*.

SSL with Client Certificate Authentication

To configure two-way SSL, first one-way SSL has to be configured. Then this can be converted to a two-way SSL.

There are two possible configurations: SSL for SAS Web Server and SAS Web Application Server, and SSL for a stand-alone SAS Web Application Server. Some sites prefer to authenticate directly to the SAS Web Application Server instead of the SAS Web Server.

In this configuration, the SAS Web Server is installed in front of the SAS Web Application Server. The client performs the SSL handshake and exchanges certificates with the SAS Web Server. The client certificate is passed directly through to the SAS Web Application Server via HTTP headers or HTTPS, depending on what is configured.

Configuring the Middle Tier to Use an Existing Reverse Proxy

Some network topologies already have an HTTP Web Server that is used to proxy connections. In these deployments, you can reconfigure the SAS middle tier so that it interacts with the existing HTTP Web Server. Even in this case, it is still simplest to keep the SAS Web Server in the deployment so that it can continue to load balance connections to a SAS Web Application Server cluster.

Closing the LOOP ON HTTP

When the SAS Web Server is configured by the SAS Deployment Wizard to support the HTTPS protocol, the port that handles unsecured HTTP requests is left open. All traffic containing sensitive information will be redirected through the secured HTTPS port. As an additional level of security, the HTTP port can either be closed or all HTTP traffic can be redirected to the secured port. One possible solution is to deny access through the firewall. If you configure the SAS Web Server not to listen on the HTTP port, any requests to that port will return an error message. You can also have any requests from browsers redirect the request rather than report failure, keeping the unsecured port open.

VPN

With Virtual Private Networks, you can extend the reach of your internal networks across public networks, thus enabling secure and encrypted communication to happen between an external unsecured network and the internal networks of the organization. Many VPN vendors offer support for VPN connectivity over mobile tablet devices, and in addition to this, there are also application-specific VPN solutions available. (See the next section.)

MOBILE DEVICE MANAGEMENT

Many organizations use Mobile Device Management (MDM) technology such as Good, Mocana, Airwatch and MobileIron to support the complete device lifecycle. IT can easily control device settings on any managed device – corporate liable, BYO or COPE – and ensure safe access to proprietary business information. The policies covered by MDM software usually include passcode, device restrictions, version restrictions, provisioning profile expiration, and so on.

Wrapping It Up

Some MDM vendors offer mobile application security by wrapping the application with a shield that isolates the application from others and directs the communications through the wrapper layers. In this approach, the users are provided a private tunnel to the app, from the server. So the communication is channeled.

Application wrappers are:

- Easy for IT to install and manage. The configuration requires an agreement between the company using SAS and the MDM vendor.
- Faster in performance. There is no additional server through which the traffic needs to flow through. There is no latency in the communication. Hence, it is faster.
- Secure. Application data coming to and from the mobile device is secure and encrypted through private application VPN, providing end-to-end security from the device to behind the firewall. On the application itself, you can set secure policies on access without having to re-wrap. These policies include passcode, device restrictions, version restrictions, provisioning profile expiration, and so on.
- Light on the client-side. The technology allows a direct connection between the application and the server, so there is no client-side agent on the device.
- Faster availability of new SAS Mobile BI versions. No re-write of the source code is required. Since the wrapper is used, there is no need to change the source code of the mobile app. This makes releasing new versions of the application faster, easier and qualitatively better.
- No additional SAS Mobile BI maintenance cost. Since the application is wrapped with no change to the source code, it is less intrusive and needs no new code maintenance. Hence, there will be no additional cost for SAS or for you.

CUSTOMER SCENARIOS – MAKING THE CAKE

So far in this paper, we have discussed the various security layers available to your IT to adequately protect corporate data. Now we will look at how all these could be brought together with real-world implementations based on two customer scenarios.

Here are the scenarios:

1. **Company A** is looking to roll out SAS Mobile BI to the business. Their IT has a BYOD policy; the user base is mostly planning to use their own tablet devices to access the environment from inside the various offices of the company – mostly for going through data visuals in meetings and workshops. There is no immediate need for them to access up-to-date information from outside the company's offices, and the users are happy with just an offline copy of the reports available to view. In all of their offices, there is an internal wireless network available that connects devices to the corporate intranet (provided the connection to the wireless is set up with a valid corporate ID and password).
2. **Company B** is looking to roll out SAS Mobile BI to their executive management. Their IT has issued all executives tablet devices that also include a cellular connection. These devices are configured by IT with Mobile Device Management as standard. The executive management is a highly mobile group of individuals, and requires access while on the move to up-to-date visuals on corporate data to make business decisions. This access is both inside and outside corporate offices on unsecured wireless networks or cellular networks. Any exposure or loss of certain data being viewed by the executives could lead to both reputational and financial losses for the organization.

COMPANY A

Table 1 captures the choices made by Company A in their configuration of their SAS Visual Analytics with SAS Mobile BI environment.

Non-optional layers	Additional Layers used	Layers not used
Secure Server	Application passcode	Tethered only mode
Security Model	Application time out	Secure Sockets Layer (SSL)
Encryption	Black listing	White listing (mutually exclusive with black listing)
Data wipe out	Intranet wireless networks	Virtual Private Networks
		Mobile Device Management
		MDM application wrappers

Table 1. Security Choices Made by Company A

Company A has decided to forgo VPN and SSL because the access is required only within the organization's offices over an already secure internal wireless network. Communication over this wireless network is already encrypted and ring-fenced through firewall infrastructure from the wider Internet. This network enables their user base to securely reach and communicate with the SAS Visual Analytics back-end server while in the corporate offices. Because of their BYOD policy and lack of MDM software to enforce per device passcode policies, they have enabled the application pass code that requires a PIN when the SAS Mobile BI application is launched. In addition, they have decided to manage access via a black list. This saves time during initial setup for the end users because the unique device ID is not required to be known upfront. The administrators have set an application time out of seven days. This means that offline data on the device will be automatically frozen after this time and inaccessible until the device reconnects through the internal wireless network.

COMPANY B

Table 2 captures the choices made by Company B in their configuration of their SAS Visual Analytics with SAS Mobile BI environment.

Non-optional layers	Additional Layers used	Layers not used
Secure Server	Application passcode	Intranet wireless networks
Security Model	White listing	Black listing (mutually exclusive with white listing)
Encryption	Tethered only mode	Application time out (mutually exclusive with Tethered only mode)
Data wipe out	Secure Sockets Layer (SSL)	
	Virtual Private Networks	
	Mobile Device Management	
	MDM application wrappers	

Table 2. Security Choices Made by Company B

Company B has stacked its security cake with several layers between SAS Mobile BI and the back-end SAS Visual Analytics server. When the IT people provision tablets for their executive users or on-board existing tablet users, they also make sure that the device unique ID is added to the SAS Visual Analytics environment white list. This guarantees that devices must go through the onboarding/provisioning process in order to connect to the back-end SAS Visual Analytics environment. Mobile Device Management is configured on the devices as a standard that enforces a device entry passcode of a minimum complexity. They still enable the application passcode as well to access the SAS Mobile BI application on launch, just in case a tablet is left unattended but unlocked (although the MDM software does automatically lock the tablet after 60 seconds of inactivity). The SAS Mobile BI application has been wrapped with an MDM application wrapper, which in turn provides a private application VPN that launches and connects when the application is used. This is further coupled with one-way SSL being the primary communication protocol all the way from the device, through the VPN, to inside the organization through their internal maze of firewalls and DMZs. Along with the VPN, this is effectively communication encryption on communication encryption. Finally, no data is ever left on the device even if it is locally encrypted. With tethered only mode, all local offline data is purged when the report is closed. An active and valid connection through the whole infrastructure is needed to be able to view the report again.

CONCLUSION

This paper has outlined the options available to your organization to securely move beyond the desktop workplace and into the mobile world while bringing the powerful analytical insight along with you. Although no single "recipe" applies to all organizations, a wealth of available choices enables you to customize your security "cake" and match your specific requirements.

REFERENCES

Chitale, Anand, and Redpath, Christopher. 2013. "Whirlwind Tour Around SAS® Visual Analytics." *Proceedings of the SAS Global Forum 2013 Conference*. Cary, NC: SAS Institute Inc. Available at http://support.sas.com/resources/papers/proceedings13/

Nori, Murali. 2013. "How Mobile Changes the BI Experience." *Proceedings of the SAS Global Forum 2013 Conference*. Cary, NC: SAS Institute Inc. Available at http://support.sas.com/resources/papers/proceedings13/

Park, Heesun. 2014. "Advanced Security Configuration Options for SAS® 9.4 Web Applications and Mobile Devices." *Proceedings of the SAS Global Forum 2014 Conference*. Cary, NC: SAS Institute Inc.

SAS® 9.4 Intelligence Platform: Middle-Tier Administration Guide. Available at http://support.sas.com/documentation/cdl/en/bimtag/66823/HTML/default/viewer.htm#titlepage.htm

SAS® Mobile BI Fact Sheet. Available at http://www.sas.com/content/dam/SAS/en_us/doc/factsheet/sas-mobile-bi-106141.pdf

ACKNOWLEDGMENTS

We would like to acknowledge the great work and contributions by all members of SAS Mobile BI and SAS Visual Analytics teams at SAS. In addition, we would like to acknowledge the direct contribution to the paper from Jim Adams, Kenny Lui and Stuart Rogers.

CONTACT INFORMATION

Your comments and questions are valued and encouraged. Contact the authors:

Christopher Redpath
SAS Institute Inc.
100 SAS Campus Drive
Cary, NC 27513
christopher.redpath@sas.com

Meera Venkataramani
SAS Institute Inc.
100 SAS Campus Drive
Cary, NC 27513
meera.venkataramani@sas.com