Paper SAS4360-2016

By the Docs: Securing SAS® Software

Robin Crumpton, Qiana Eaglin, and Donna Bennett, SAS Institute Inc., Cary, NC

ABSTRACT

Have you ever wondered the best way to secure SAS® software? Many pieces need to be secured–from passwords and authentication to encryption of data at rest and in transit. In this paper we discuss several security tasks that are important when setting up SAS, and we provide some tips for finding the information that you need in the mountains of SAS documentation. The tasks include 1) enabling basic network security (TLS) using the automation options in the latest release of SAS® 9.4; 2) configuring HTTPS for the SAS middle tier (once the TLS connection is established); 3) setting up user accounts and IDs with an eye toward auditing user activity. Whether you are an IT expert who is concerned about corporate security policies, a SAS Administrator who needs to be able to describe SAS capabilities and configure SAS software to work with corporate IT standards, or an auditor who needs to review specific questions about security vulnerabilities, this paper is for you.

INTRODUCTION

What comes to mind when you hear the term “security”? Are there categories that come to mind, such as authentication, authorization, encryption, or audits? Are there other terms that come to mind? Perhaps Transport Layer Security (TLS), Secure Socket Layer (SSL), HTTPS, certificates, tokens, Kerberos, SAML, single sign-on, SAS Anonymous Web User, guest logon, time-outs, Integrated Web Authentication (IWA), WebSEAL, lockdown, metadata-bound libraries, credentials, permissions, roles, users, identities, and the list goes on and on.

We recognize that security does not fit neatly into a few categories. Security spans roles, such as IT administrator, Security Administrator, application specialist, and end user. Security also spans tasks that you have to perform, and platforms, machines, technologies, and services that you have to administer. Security is a complex issue, as is the documentation written about this expansive topic.

First, we recognize that you might wear many hats (system administrator, SAS administrator, end user, SAS programmer, auditor, or tester). This paper highlights where most of our documentation is located, and then provides a shortened list of the most used security documents. We provide a general roadmap of SAS documentation that will help you locate and address topics related to your security needs.

Second, we illustrate how you can use our documentation by reviewing three general scenarios and example tasks:

- The first two scenarios focus on infrastructure security. After we provide an overview of certificates used for TLS and HTTPS, we explain how to use those certificates to set up TLS on the server tier, followed by how to use certificates to set up HTTPS security on the middle tier for web services.
- The third scenario highlights tasks associated with auditing user actions within the SAS environment. We provide an overview of how users are defined in SAS options for collecting data and creating audit reports.

This paper is not meant to provide extensive technical detail, but rather identify a few common security scenarios, and then point you to the SAS documentation that provides more information.

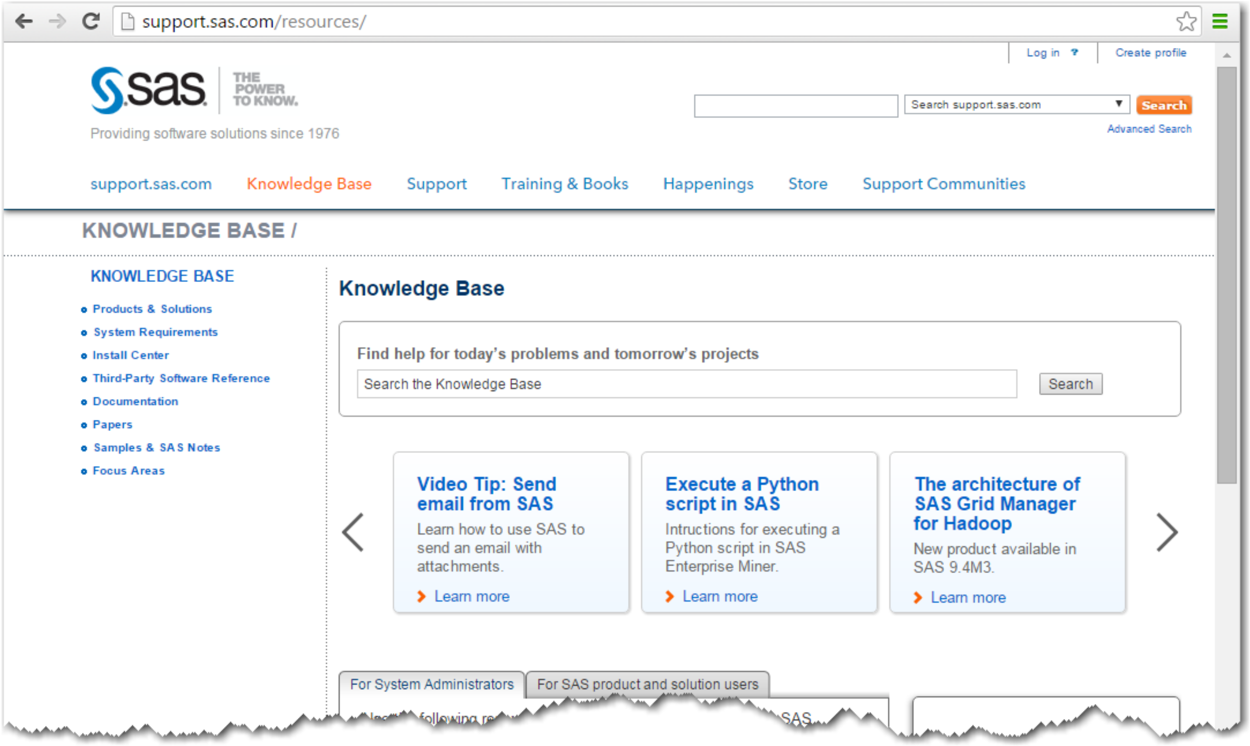
OVERVIEW

Where do I find information about how to secure data when using SAS? We document how to secure your network communications, your web applications, your services, your data (SAS or other databases), and your deployment. We document securing your deployment on various platforms (Windows, Linux, UNIX, z/OS). We write about using third-party software (TLS/SSL, Kerberos, LDAP, JAVA, and so on) to secure your deployment.

We write documentation that is customer facing for administrators, end users (programmers or other users of SAS), and installers. White papers and SAS Global Forum papers address very specific security scenarios. Security bulletins highlight important security issues. The SAS Software Security Framework paper describes the development and testing processes that SAS follows. User Communities provide a forum where you can ask specific questions and share examples with your peers.

That is a lot of documentation to read through! To help you navigate security-related documentation, we created a roadmap that provides a list of collateral. For each entry, there is a short description of the type of security information, and there are links to key security topics.

The roadmap for security documentation is located at http://support.sas.com/documentation/onlinedoc/secure/index.html. Most of the documentation listed in the roadmap can be found at support.sas.com/resources in the Knowledge Base.



Knowledge Base

Find help for today's problems and tomorrow's projects

Search the Knowledge Base

Video Tip: Send email from SAS
Learn how to use SAS to send an email with attachments.
Learn more

Execute a Python script in SAS
Intructions for executing a Python script in SAS Enterprise Miner.
Learn more

The architecture of SAS Grid Manager for Hadoop
New product available in SAS 9.4M3.
Learn more

Figure 1 Knowledge Base of SAS Documentation

ENABLING BASIC NETWORK SECURITY (TLS) USING THE AUTOMATION OPTIONS IN THE LATEST RELEASE OF SAS® 9.4

TLS uses versioned protocols that are updated frequently. You can find information about the versions of TLS that SAS supports, the cipher suites supported, and how SAS supports TLS on each platform at:

- "TLS Software Availability" in *Encryption in SAS® 9.4*: http://support.sas.com/documentation/cdl/en/secref/68007/HTML/default/viewer.htm#n0gzdro5ac3enzn18qbmaqy4liz3.htm
- "Cipher Suites Supported by SAS" in *Encryption in SAS® 9.4*: http://support.sas.com/documentation/cdl/en/secref/68007/HTML/default/viewer.htm#p1or8wckslb1jgn1ugaqc2be53yu.htm

- *Mapping Between SAS Version and OpenSSL Version*: http://support.sas.com/documentation/onlinedoc/secure/index.html

Transport Layer Security (TLS) and its predecessor, Secure Sockets Layer (SSL), are cryptographic protocols that are designed to provide communication security. TLS and SSL are protocols that provide network data privacy, data integrity, and authentication.

Note: All discussion of TLS is also applicable to the predecessor protocol, Secure Sockets Layer (SSL). While there are technical differences, the terms TLS, SSL, and HTTPS are sometimes used interchangeably.

Adding TLS on top of Hyper Text Transfer Protocol (HTTP) provides you with the HTTPS protocol. HTTPS is used to provide encrypted communication with a Web server.

Certificates Are the Cornerstone of TLS

Certificates are the cornerstone of using TLS and HTTPS. Certificates communicate the identity of the server to its visitors (clients, services, servers, and so on). The mechanism to distribute the public key used for the TLS Handshake is the X.509 certificate.

The TLS Handshake Protocol is responsible for the authentication and key exchange necessary to establish or resume secure sessions. It also secures application data by using the symmetric keys created during the Handshake. To understand the specifics and details of the TLS Handshake, how certificates are signed, the certificate chain, and how the X.509 certificate is validated, see Rogers (2016). RFC 5280 (Cooper, et al. 2008) defines the version 3 structure of a TLS certificate.

- Rogers, Stuart J. 2016. “Tips and Techniques for Using Site-Signed HTTPS with SAS® 9.4. *Proceedings of the SAS Global Forum 2016 Conference*. Cary, NC: SAS Institute Inc.
- Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile RFC 5280 (Cooper, et al. 2008)

Certificate Authority (CA) and the Public Key

When messages are exchanged between entities, there is a risk that a message can be intercepted and that a process or a user can become impersonated. Certificate Authorities (CAs) are trusted parties that provide confidence that a public key truly belongs to an entity.

As part of the process for setting up a secure connection, the administrator needs to create a certificate that is in the appropriate format, and that is signed by a third party or within your organization. One way to get the certificate is to request that a Certificate Authority (CA) issue a certificate that contains your public key. You can also request that the CA digitally sign the certificate. This is referred to as a signed certificate. The entity that receives your message acknowledges that your signed certificate is issued by a CA that it recognizes. If it recognizes the CA, the entity is able to substantiate your identity.

Authenticating entities is accomplished through certificates issued by self-signed, site-signed, or third-party-signed CAs.

Specifics about CA signed certificates, how they are used, and when to use them can be found in:

- “Certificates Explained” in *Encryption in SAS® 9.4* http://support.sas.com/documentation/cdl/en/secref/68007/HTML/default/viewer.htm#p1jf3or94q48y9n1om73rtgo0bct.htm
- “Setting Up Certificates for SAS Deployment” in *SAS® 9.4 Intelligence Platform: Installation and Configuration Guide* http://support.sas.com/documentation/cdl/en/biig/69172/HTML/default/viewer.htm#p12intellplatform00installgd.htm
- Rogers, Stuart J. 2016. “Tips and Techniques for Using Site-Signed HTTPS with SAS® 9.4.” *Proceedings of the SAS Global Forum 2016 Conference*. Cary, NC: SAS Institute Inc.

In our examples, we will assume that most of the certificates that you create are site-signed certificates. You will also have the Third-Party-signed certificates in the Mozilla CA bundle that is delivered as part of the SAS deployment. A common practice of many organizations is to use site-signed certificates, or to setup a CA solely for their internal use.

Providers of Trust

For the TLS Handshake to successfully validate the X.509 Certificate, either the X.509 Certificate (in the case of self-signed certificates), or the Root CA Certificate (in the case of site-signed or third-party signed certificates) must be trusted. As part of the TLS Handshake the X.509 Certificate is validated. The validation algorithm checks to see whether the certificate of the issuing CA was issued by a trusted CA, and so on, until a trusted CA is found. A secure connection is established when a trusted CA is found.

The client holds the list of trusted CAs or the list is held by the operating system of the client.

Different types of clients have different providers of trust. In the third maintenance release of SAS® 9.4, the SAS® Security Certificate Framework is a new provider of trust. Clients that use the SAS Security Certificate Framework include the Java Desktop Client, the SAS® Server Process for UNIX, and the SAS® Web Application Server.

To be able to establish trust for a site-signed X.509 Certificate, the Root CA Certificate must be added to the provider of trust. Different providers can participate in a SAS deployment, including Windows, Mozilla Firefox, and mobile operating systems, as well as the SAS Security Certificate Framework. Each of these "truststores" has a different mechanism for adding the Root CA Certificate.

In the third maintenance release of SAS 9.4, when you install SAS® software on the host, you can then use the SAS® Deployment Manager to add your site-signed Root CA Certificate to the SAS Security Certificate Framework.

To see a list of clients, their providers of trust, and the mechanism used to add a Root CA Certificate, refer to Rogers (2016).

The SAS Security Certificate Framework

Introduced with the third maintenance release of SAS 9.4, the SAS Security Certificate Framework enables SAS to provide the Mozilla bundle of trusted CA Certificates (Mozilla Wiki. 2015). Starting with the third maintenance release of SAS 9.4, any installation that includes the SAS® Private Java Runtime Environment also includes the SAS Security Certificate Framework. Therefore, any SAS® installed Java process uses the SAS Security Certificate Framework as its provider of trust. SAS no longer uses the default JSSE truststore (cacerts) that is delivered with Java. In the SAS Private JRE, the SAS-delivered CA certificates take precedence when a client application establishes trust using the JRE truststore.

The SAS Security Certificate Framework is also included with SAS® Foundation installations on UNIX platforms. This provides SAS® Foundation processes on UNIX platforms with a standard provider for trust. This standard provider was not available in previous releases of SAS.

The following figure is taken from the *SAS® 9.4 Intelligence Platform: Installation and Configuration Guide, Second Edition*. This figure summarizes the process of installing the SAS Security Certificate Framework, as well as adding a CA certificate to the trusted bundle of CA certificates.

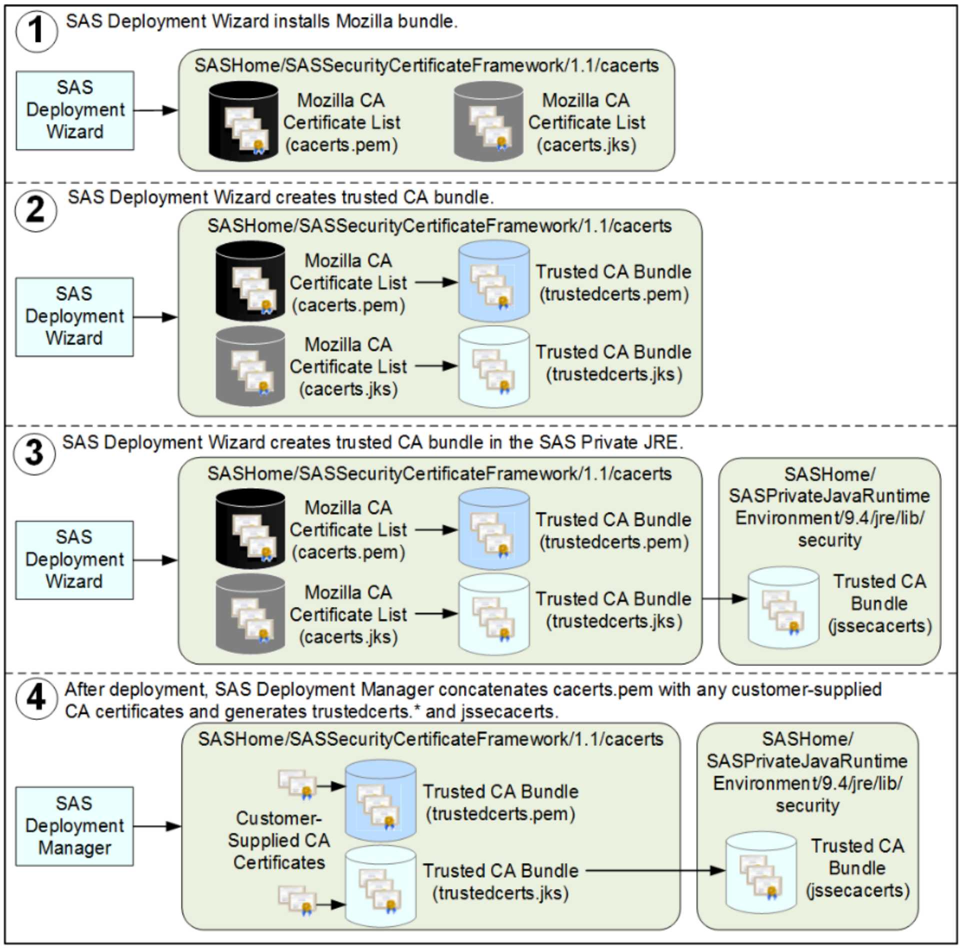

1
SAS Deployment Wizard installs Mozilla bundle.
SAS Deployment Wizard
SASHome/SASSecurityCertificateFramework/1.1/cacerts
Mozilla CA Certificate List (cacerts.pem)
Mozilla CA Certificate List (cacerts.jks)
2
SAS Deployment Wizard creates trusted CA bundle.
SAS Deployment Wizard
SASHome/SASSecurityCertificateFramework/1.1/cacerts
Mozilla CA Certificate List (cacerts.pem)
Trusted CA Bundle (trustedcerts.pem)
Mozilla CA Certificate List (cacerts.jks)
Trusted CA Bundle (trustedcerts.jks)
3
SAS Deployment Wizard creates trusted CA bundle in the SAS Private JRE.
SAS Deployment Wizard
SASHome/SASSecurityCertificateFramework/1.1/cacerts
Mozilla CA Certificate List (cacerts.pem)
Trusted CA Bundle (trustedcerts.pem)
Mozilla CA Certificate List (cacerts.jks)
Trusted CA Bundle (trustedcerts.jks)
SASHome/ SASPrivateJavaRuntime Environment/9.4/jre/lib/ security
Trusted CA Bundle (jssecacerts)
4
After deployment, SAS Deployment Manager concatenates cacerts.pem with any customer-supplied CA certificates and generates trustedcerts.* and jssecacerts.
SAS Deployment Manager
SASHome/SASSecurityCertificateFramework/1.1/cacerts
Customer-Supplied CA Certificates
Trusted CA Bundle (trustedcerts.pem)
Trusted CA Bundle (trustedcerts.jks)
SASHome/ SASPrivateJavaRuntime Environment/9.4/jre/lib/ security
Trusted CA Bundle (jssecacerts)

Figure 2 How SAS® Deployment Wizard Installs the Trusted CA Bundle

A Summary of What is New in SAS 9.4M3 about Managing TLS Certificates

The following list provides a summary of the changes that were made to TLS and HTTPS security in the third maintenance release for SAS 9.4:

- The SAS Deployment Wizard is now used to lay down the bundle of certificates by Mozilla at Installation or Migration.
  - Mozilla Included CA Certificate List: https://wiki.mozilla.org/CA:IncludedCAs
  - *SAS® Deployment Wizard and SAS® Deployment Manager 9.4: User's Guide*: http://support.sas.com/documentation/installcenter/en/ikdeploywizug/66034/PDF/default/user.pdf

- Certificate bundle management has been added to SAS Deployment Manager. Using SAS Deployment Manager, you can add and remove certificates to and from the trusted CA bundle.
  - "Manage Trusted CA Bundle" in *SAS® Deployment Wizard and SAS® Deployment Manager 9.4: User's Guide*: http://support.sas.com/documentation/installcenter/en/ikdeploywizug/66034/PDF/default/user.pdf

- SAS provides a default truststore (the jssecacerts file) that takes precedence over the previous truststore (the cacerts file) in the SAS Private JRE.

  The trusted Certificate Authority (CA) bundle distributed by SAS is a copy of the list of Third-Party signed certificates that are distributed with Mozilla software products.
  - Mozilla Included CA Certificate List: https://wiki.mozilla.org/CA:IncludedCAs

- On UNIX, trusted certificates are now located in the trusted CA bundle in *SAS-installation-directory*/SASSecurityCertificateFramework/1.1/cacerts/trustedcerts.pem. During installation, SAS Deployment Wizard sets the SSLCALISTLOC system option in the SAS-installation-directory/SASFoundation/9.4/sasv9.cfg file to point to the trustedcerts.pem file by default.

- If certificates are not used, SAS ignores the SSLCALISTLOC system option. The order that SAS uses when searching for certificates can be found at:
  - "SSLCALISTLOC = System Option" in Encryption in SAS 9.4 http://support.sas.com/documentation/cdl/en/secref/68007/HTML/default/viewer.htm#p0pul4j64w0mg0n1h1k6z8zhfvaf.htm

HTTPS FOR THE MIDDLE TIER

Why are we talking about security in the middle tier?

The middle tier of the SAS Intelligence Platform enables you to access data and perform various tasks using a web browser. This tier provides web-based interfaces for report creation and information distribution, while passing analysis and processing requests to the SAS servers.

The components of the middle tier environment that might require network security and privacy are SAS Web Server and SAS Web Application Server. SAS Web Server is a Hypertext Transfer Protocol (HTTP) server that is configured as a single connection point to the network for SAS web applications. In most cases, you will want to enable TLS security and configure SAS Web Server to support HTTPS connections. The SAS Deployment Wizard is designed to automate this secure setup.

The SAS web applications that run in the SAS middle tier are processed in SAS Web Application Server, and SAS Web Application Server, in turn, communicates with the external network via SAS Web Server. Some companies choose to configure both SAS Web Server and SAS Web Application Server to support HTTPS. The SAS web applications communicate with the user's web browser. HTTPS consists of communication over HTTP within a connection encrypted by TLS using certificates. Configuring HTTPS for both servers ensures that all communications with SAS web applications run in a secure environment.

SAS Environment Manager is another tool that is designed to allow HTTPS connections; discussion of SAS Environment Manager configuration is outside the scope of this paper.

For more information about the middle-tier environment, see the following books:

- "Middle-Tier Components of the SAS Intelligence Platform" in *SAS® 9.4 Intelligence Platform: Overview* http://support.sas.com/documentation/cdl/en/biov/69018/HTML/default/viewer.htm#p091iagmsk7kmen0zeg409unmpkb.htm

- "Middle-Tier Security" in *SAS® 9.4 Intelligence Platform: Middle-Tier Administration Guide* http://support.sas.com/documentation/cdl/en/bimtag/68217/HTML/default/viewer.htm#n1q28511wr19k2n1t2q852eayc8z.htm

- “Working With Web Applications in the Middle Tier Environment” in *SAS® 9.4 Intelligence Platform: Web Application Administration Guide*
  http://support.sas.com/documentation/cdl/en/biwaag/68048/HTML/default/viewer.htm#n0h9o3hbwmrason1lc1osvrzouvi.htm

Configuring SAS Web Server and SAS Web Application Server for HTTPS

SAS is moving toward fully automating the process of configuring HTTPS. SAS Web Server can be configured by SAS Deployment Wizard either during or after the initial deployment, but SAS Web Application Server must be manually configured for HTTPS. It is recommended that you allow SAS Deployment Wizard to configure SAS Web Server for HTTPS. The configuration process for SAS Web Server is complex and inaccuracies could lead to an environment that does not work. In addition, if you are required to apply maintenance or upgrades to your system, you first have to revert the manual changes that you made for HTTPS. Once your environment has been upgraded, you then have to reconfigure HTTPS.

Starting in January 2016, warning and error messages are displayed while upgrading your system or installing maintenance if any manual changes were made to SAS Web Server and SAS Web Application Server for HTTPS. The messages warn you to revert your system to the original non-HTTPS values before making updates to your system. The warning and error messages that you might see while applying maintenance releases or upgrades to your system are:

-
  ```
  Error Message: The SAS Deployment Wizard has detected that SSL
  encryption was manually added to the following:
    <ServerNames>

  The manual TLS configuration changes must be reverted to the original
  non-TLS values before applying any maintenance releases or upgrades to
  the system. Then the manual TLS configuration steps can be reapplied to
  the upgraded system.
  ```

-
  ```
  Warning Message:  The SAS Deployment Wizard has detected that SSL
  encryption was manually added to the following:
    <ServerNames>

  The manual TLS configuration changes must be reverted to the original
  non-TLS values before applying any maintenance releases or upgrades to
  the system. Then the manual TLS configuration steps can be reapplied to
  the upgraded system.
  ```

For the error message, you must click OK, and then revert your changes before you can continue. For the warning message, you are prompted whether you want to ignore the warning message and continue upgrading your system. It is recommended that you discontinue the process and revert the HTTPS changes you made to the SAS Web Server and/or the SAS Web Application Server. If you ignore the warning message during an update or application of maintenance, automatic configuration will overwrite your changes, causing you to lose them and possibly corrupting the installation.

For more information about configuring SAS Web Server for HTTPS using SAS Deployment Wizard, see:

- “Install and Configure SAS Interactively” in *SAS® 9.4 Intelligence Platform: Installation and Configuration Guide*
  http://support.sas.com/documentation/cdl/en/biig/69172/HTML/default/viewer.htm#n05020intelplatform00install.htm

For more information about manually configuring SAS Web Server for HTTPS using your own certificates, see:

- "Provide Your Own Certificates" in *SAS® 9.4 Intelligence Platform: Installation and Configuration Guide*
  http://support.sas.com/documentation/cdl/en/biig/69172/HTML/default/viewer.htm#n12035intelplatform00install.htm#n12008intelplatform00install

- "Post-Deployment Tasks for SAS Web Server" in *SAS® 9.4 Intelligence Platform: Installation and Configuration Guide*
  http://support.sas.com/documentation/cdl/en/biig/69172/HTML/default/viewer.htm#n12025intelplatform00install.htm#n12024intelplatform00install

- "Configuring SAS Web Server Manually for HTTPS" in *SAS® 9.4 Intelligence Platform: Middle-Tier Administration Guide*
  http://support.sas.com/documentation/cdl/en/bimtag/68217/HTML/default/viewer.htm#n0nakjyj6hlqmvn11p9p04l25j9n.htm

For more information about manually configuring SAS Web Application Server for HTTPS, see:

- "Configuring SAS Web Application Server to Use HTTPS" in *SAS® 9.4 Intelligence Platform: Middle-Tier Administration Guide*
  http://support.sas.com/documentation/cdl/en/bimtag/68217/HTML/default/viewer.htm#n1enfdk7f1fjcqn1ggbrx79lm9i0.htm

Assess and Document Your Current Environment

Any manual changes to the HTTPS configuration of SAS Web Server and SAS Web Application Server must be reverted to the original non-HTTPS values before applying a maintenance release or upgrading any software. These manual changes to the TLS configuration will need to be reapplied to the upgraded system. We encourage you to keep a copy of your changed configuration files before reverting the changes.

Manual versus Automatic Configuration of HTTPS

The SAS Deployment Wizard and the SAS Deployment Manager provide an option for automatically configuring TLS to enable HTTPS connections for the SAS Web Server. Because of some improvements in the configuration process that were introduced after SAS 9.4M2 was released, customers who have manually configured TLS need to remove those changes from the configuration files before updating the deployment. We encourage you to use the automated deployment options going forward. When you use the automated SAS Deployment Wizard tool to configure HTTPS for SAS Web Server, you do not need to revert configuration changes. If you choose to configure SAS Web Application Server, then you will be performing a manual deployment, and you will need to manage those changes.

The following sections highlight the steps for reverting the changes. During an update or application of maintenance, automatic configuration will overwrite your changes, causing you to lose them. We recommend that you back up the files before reverting changes as described below. That will give you a reference of your previous settings, and enable you to restore these files if you encounter problems while editing. You will need to shut down the SAS middle tier while making some changes.

Reverting Manual Changes to SAS Web Server

If you manually configured SAS Web Server to use HTTPS and want to apply maintenance or upgrades to your system, you *must* first complete the following brief list of the steps. The steps are required to revert manual HTTPS changes that were made to SAS Web Server. For a more detailed description of the procedure, see *SAS® 9.4 Intelligence Platform: Middle-Tier Administration Guide*.

1. Comment out the INCLUDE statement that references the httpd-ssl.conf file.
2. For each instance of SAS Web Application Server, change the Connector element proxyPort and scheme to specify HTTP.
3. In SAS Management Console, for each SAS web application, change the protocol and port number.
4. Use SAS Management Console to update the SAS Content Server connection information.
5. For SAS Visual Analytics deployments, confirm that the SAS LASR Authorization Service URI is updated.
6. Depending on which products you have installed, you might have to update the SAS environment file.
7. To access SAS Environment Manager Console with TLS enabled on SAS Web Server, specify the information for your environment.
8. Update the SAS Content Server JVM options.
9. Verify that the reversion to non-TLS is complete by restarting the SAS Web Server and accessing it from your web browser.

Reverting Manual Changes to SAS Web Application Server

If you manually configured SAS Web Application Server to use HTTPS and want to apply maintenance or upgrades to your system, you *must* first complete the following brief list of the steps. The steps are required to revert manual HTTPS changes that were made to SAS Web Application Server. For a more detailed description of the procedure, see *SAS® 9.4 Intelligence Platform: Middle-Tier Administration Guide*.

1. For each server that was configured to use HTTPS, modify the Connector element.
2. For each SAS Web Application Server, set or add JVM options specifying the HTTP port that SAS Web Application Server is listening on.
3. For SAS Web Server, change the BalancerMember directives to use HTTP as the protocol, change the HTTP port that SAS Web Application Server is listening on, and remove the SSL* directives.
4. Verify that the reversion to non-TLS is complete by restarting the SAS Web Application Server.
5. Modify SAS Web Application Server to stop returning the session ID with the secure attribute.

Overlay That Information onto the Automated Processes

After you have completed the steps to revert your previous manual configurations, you can now upgrade your software. During the upgrade process, we encourage you to use the options in the SAS Deployment Wizard to automatically configure HTTPS for the SAS Web Server. Once you have successfully used the automated tools to configure SAS Web Server for HTTPS, you will not have to revert the changes for future upgrades. If you want to enable HTTPS for SAS Web Application Server, then you will need to perform a manual configuration, and reapply your customizations.

SETTING UP USER ACCOUNTS/IDS WITH AN EYE TOWARD AUDITING USER ACTIVITY

We are shifting topics now, and talking about users and auditing. Why? Because security is about more than infrastructure and encryption. Running audit reports about system usage has become a required task in many IT organizations. Some internal audits are designed to monitor general use of the system and software. Other audits are driven by external requirements, such as the need to prove to internal or external auditors that IT follows internal policies, or to provide reports that demonstrate compliance to regulations such as SOX, GLBA, PCI-DSS, and HIPAA. Many compliance and auditing reviews focus on user activities and on who has access to what information.

It is helpful to understand how users are defined to SAS as a baseline for responding to audit requests about user access and activities.

- Authentication by external provider. SAS relies on its various server machines to authenticate external user accounts. The authentication provider might be local to the machine, or might use a directory service such as Active Directory or LDAP, which means you have a choice of creating local or directory accounts for users. See:

  - "Local or Directory Service Accounts?" in *SAS® 9.4 Intelligence Platform: Installation and Configuration Guide*

    http://support.sas.com/documentation/cdl/en/biig/69172/HTML/default/viewer.htm#n02002intelplatform00install.htm

- Authorization within SAS metadata. SAS solutions rely on SAS metadata to control authorization - who can access what SAS data and applications. For accountability, SAS recommends that you create an individual SAS metadata identity for each person who uses the SAS environment, and associate that identity with the authentication identity. This enables you to make access distinctions and audit individual actions in the metadata layer.
  - "Create Metadata User Definitions" in *SAS® 9.4 Intelligence Platform: Security Administration Guide*

    http://support.sas.com/documentation/cdl/en/bisecag/67045/HTML/default/viewer.htm#n0wmklmi4n49o6n1pzeikk6tqucm.htm
  - "Managing User Access" in *SAS® Environment Manager 2.5 Administration: User's Guide* http://support.sas.com/documentation/cdl/en/evadmug/68379/HTML/default/viewer.htm#p1oo51oqq6tuchn1si35myscl4x4.htm
- Synchronizing processes. SAS provides sample macros that simplify the process of creating SAS metadata identities by synchronizing user definitions in metadata with account ID information from the authentication provider.
  - "User Import Macros" in *SAS® 9.4 Intelligence Platform: Security Administration Guide*

    http://support.sas.com/documentation/cdl/en/bisecag/67045/HTML/default/viewer.htm#p1ar98lajfgm4jn1wa1h6e19jjre.htm
- Special cases. SAS recommends that a small number of accounts be designated as "internal user accounts": these accounts are known only to SAS and are typically used for Administrative tasks and to support special connections. These internal accounts do not have an external user ID, and cannot be used to access any capabilities outside of SAS software. Examples include sasadm@sas.com and sastrust@sas.com.
  - "SAS Internal Authentication" in *SAS® 9.4 Intelligence Platform: Security Administration Guide*

    http://support.sas.com/documentation/cdl/en/bisecag/67045/HTML/default/viewer.htm#p1cjwe7ruon8p4n1hkekbza7prrr.htm

NOTE: SAS Environment Manager, a web-based administration tool, is the preferred administrative interface, replacing SAS Management Console for most user management tasks.

The bottom line: "User activity" is a broad topic, and you might need several reports to answer audit questions about user activity.

Administrative Tools Provide Reporting Options

Two SAS administrative tools - SAS Environment Manager, and SAS Visual Analytics Administration - include pre-defined templates for creating reports about user activity within the SAS environment. System administrators can use the pre-defined reports, or extend these templates to create custom reports that meet specific needs. Moreover, a system administrator can leverage operating system and database tools to collect and analyze user-related activities at the system level.

- SAS Environment Manager
  - Auditing and the Service Architecture Framework: three types of data:

        - Audit and Performance Metrics (was previously SAS APM)
        - Metric data collected by SAS Environment Manager Agents
        - Solution data - often requires special configuration of solution “kits”
    - Report Center
        - More than 130 standard reports (including 15 audit-specific reports) with 9.4M3
        - Nightly summary reports
        - Ad hoc reports
        - Extendable - administrators can add their own reports

- SAS Visual Analytics Administration
    - Provides reports focused on Visual Analytics activity
    - User Actions logging
        - All logon and logoff activity by SAS web applications is recorded
        - Initially stored in SharedServices database (WIP Data Server)
        - New data added to SAS Visual Analytics reporting database every 15 minutes
            - “Manage audit” in SAS Communities https://communities.sas.com/t5/forums/searchpage/tab/message?filter=labels&q=manage+audits
            - “Key Actions Auditing” in *SAS® Visual Analytics: Administration Guide* http://support.sas.com/documentation/onlinedoc/va/index.html
    - Enabling data sources
        - Data feed from SAS Environment Manager Data Mart via Autoload
        - Enable Middle-tier auditing to capture basic web activity
        - Enable Visual Analytics auditing to capture additional tasks
    - Pre-defined Reports
        - Visual Analytics Administrator interface lets you access pre-defined reports here **View > Usage Reports > Other reporting options**
        - Extendable - administrators can add and customize reports
- Produce data, create your own reports. For information about authorization reporting, and tools that help create a snapshot of metadata layer access control settings, see:
    - “Security Report Macros” in *SAS® 9.4 Intelligence Platform: Security Administration Guide* http://support.sas.com/documentation/cdl/en/bisecag/67045/HTML/default/viewer.htm#p1h2c11fxfn6xcn1gq9adnt7yhrb.htm

Collecting Data

Before you can create an audit report, you need to collect data. By determining what information you want in a report, you can refine the information that you want to collect. SAS solutions offer a great deal of configuration flexibility that can define the types and amount of data collected. The process of collecting data is sometimes referred to as “logging” when the data is written to a log file and at other times it is referred to as “auditing.” While “logging” and “auditing” are not fully interchangeable concepts or processes, the end result of collecting data overlaps. When auditing or logging is enabled and data records are generated, the data size increases according to two factors:

- the number actions that are enabled for auditing
- how frequently the audited actions are performed

That means that you need to consider the physical resources needed to capture and retain audit records and other raw data. You might want to implement some of the archiving and purging options defined the documents and blogs referenced in this paper.

The location of the log files and audit records can vary, based on which tools you are using and how you have configured your deployment. The SAS Environment Manager ETL processes scan the directory structure of the SAS deployment to find log files and to add information to the data mart.

Summary of Options, tasks, and tools for creating audit reports about user activity

For VA, the process of collecting and analyzing data about user activity builds on the data that is collected by the SAS Middle Tier. Pre-defined ETL tasks make that data available for access by a SAS Visual Analytics administrator. SAS Environment Manager administrators have access to additional data that is mined from SAS logs and that includes metrics generated by the Deployment Agents. Pre-defined ETL tasks make that data available for access by a SAS Visual Analytics administrator, and by administrators who run SAS Environment Manager.

The SAS Middle Tier and the role of Web Administration Console

- The middle tier administration guide defines the setup needed to collect audit information for specific middle tier activities. Setting up this information is a prerequisite for feeding information to the SAS Visual Analytics EVDMLA library.
    - "Configuring Auditing for SAS Web Applications" in *SAS® 9.4 Intelligence Platform: Middle-Tier Administration Guide*

      http://support.sas.com/documentation/cdl/en/bimtag/68217/HTML/default/viewer.htm#n06skrc2rtwecsn14vi4qtfl54kx.htm
- The Web Administration Console provides the ability to view simple audit reports that show user logon and logoff activity and failed logon attempts. The Web Administration Console can perform other tasks that are sometimes associated with auditing, including:
    - monitoring information about users who are currently logged on to SAS web applications
    - viewing the current configuration for web applications that have been deployed at your site.

SAS Visual Analytics administrators work within the SAS Visual Analytics framework to analyze data and produce reports.

- When you enable auditing for the SAS middle tier, user activity is recorded in the audit tables of the shared services database. You can check the table content with pgAdmin tool to confirm that auditing is active.
    - *Using pgAdmin III*
      http://www.pgadmin.org/docs/dev/using.html
- Data is extracted from the shared services database and written to the SAS Visual Analytics autoload location. You can specify the timeframes for updating the data; by default, the data is extracted every 30 minutes.
- To manage data sizes, review the archive settings for the middle tier shared services database.
- By enabling autoload for the EVDMLA library, data is loaded into SAS Visual Analytics memory. The default refresh cycle is every 30 minutes.
- System Administrators can access a panel of pre-defined standard reports, and can use the reporting and analysis tools within SAS Visual Analytics to customize the standard reports and to create new reports.

SAS Environment Manager provides extended monitoring and auditing options

- An administrator must initialize and enable the Service Architecture, which initializes the SAS Environment Manager Data Mart and loads the data used by the Report Center. In addition, the APM and ACM ETL processes must be enabled and initialized. APM ETL extracts data from SAS logs when the logs roll over (usually after midnight). ACM ETL extracts metric data generated by SAS Environment Manager agents.

- The Report Center tab within SAS Environment Manager includes Metadata Audit Reports built on data from the logs, which is loaded nightly to the SAS Environment Manager data mart. Examples of reports in the Audit Reports folder include: “Metadata Group Changes”, “Access Control Changes”, “User Accounts Added” and “User Accounts Removed.”
    - SAS Environment Manager Service Architecture Framework: http://support.sas.com/rnd/emi/SASEnvMgr/EVSAF/index.html
- SAS Environment Manager functionality has been enhanced several times during the SAS 9.4 release cycle. The *SAS Environment Manager User’s Guide* describes the function and setup of the Service Architecture and Data Mart, and describes Report Center options. The *SAS Environment Manager Administration User’s Guide* focuses on administration tasks including creating and managing users, managing metadata access, and managing backups.
    - *SAS Environment Manager: User’s Guide*: http://support.sas.com/documentation/cdl/en/evug/68091/HTML/default/viewer.htm#titlepage.htm

Start with Overviews Available in SAS Blogs

Several blogs from SAS voices provide a great place to start your journey toward establishing an ongoing auditing process. These blogs provide an overview of the capabilities and processes. For specific implementation and usage details, refer to the SAS documentation. The documentation provides details about how to set up auditing for specific SAS components and activities, and describes reports available from specific tools.

- Auditing data access: Who did what and when, by Gerry Nelson http://blogs.sas.com/content/sgf/2015/09/30/part-1-auditing-data-access-who-did-what-and-when/
- Part 2: Auditing data access: Who did what and when, by Gerry Nelson http://blogs.sas.com/content/sgf/2015/10/07/part-2-auditing-data-access-who-did-what-and-when/
- What is going on with my Visual Analytics data archiving? by Gerry Nelson http://blogs.sas.com/content/sgf/2016/01/26/going-visual-analytics-audit-data-archiving/
- What is going on with my Visual Analytics data collection? by Gerry Nelson http://blogs.sas.com/content/sgf/2015/12/29/what-is-going-on-with-my-visual-analytics-audit-data-collection/
- SAS Environment Manager Data Mart - the heart of the Service Management Architecture, by Gilles Chrzaszcz http://blogs.sas.com/content/sgf/2014/11/26/sas-environment-manager-data-mart-the-heart-of-the-service-management-architecture/

USEFUL SECURITY DOCUMENTATION LINKS

SAS documentation provides information about security tasks. Topics include how to enable HTTPS for the SAS middle tier, how to choose and enable encryption algorithms, and how to create audit reports. User blogs provide additional insight about how to use the available tools to accomplish IT and business tasks. You can access the full series of SAS Blogs at blogs.sas.com, and you can use the search option to find blog entries related to administration and auditing and to topics such as Kerberos and security. SAS Communities enable you to share tips and questions with your peers.

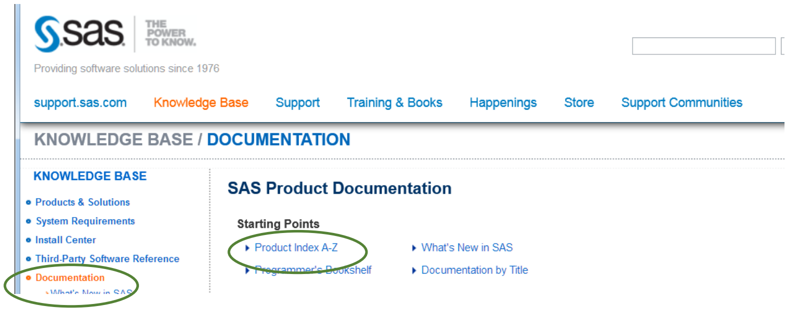
If you haven’t already reviewed the ***Checklist for a More Secure Deployment*** in the *SAS® 9.4 Intelligence Platform: Security Administration Guide*, it is a great place to see an overview of the breadth of security capabilities and controls that are available for SAS administrators.

Security topics such as setting up encryption options for TLS and HTTPS (secure HTTP) are covered in the Intelligence Platform collection of documents. Information about auditing and user management is also covered in several of the administration guides. Additional details about encryption options are provided in the SAS/SECURE document collection. Some solutions, such as SAS Visual Analytics, provide additional information in application-specific Administration Guides.

Find the document collections via the support.sas.com web page. Some documents, such as SAS Environment Manager, are referenced as part of a collection (Intelligence Platform) and via their own collection page.

Here is a brief example of navigating the Documentation Knowledge Base.

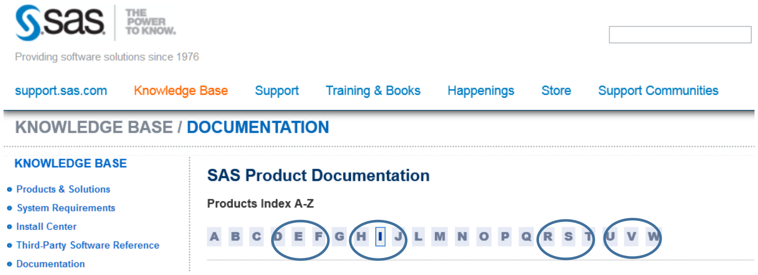
https://support.sas.com/documentation/index.html



Choose **Documentation** on the left menu.

Click the alphabetical list **Product Index A-Z**

https://support.sas.com/documentation/productaz/index.html

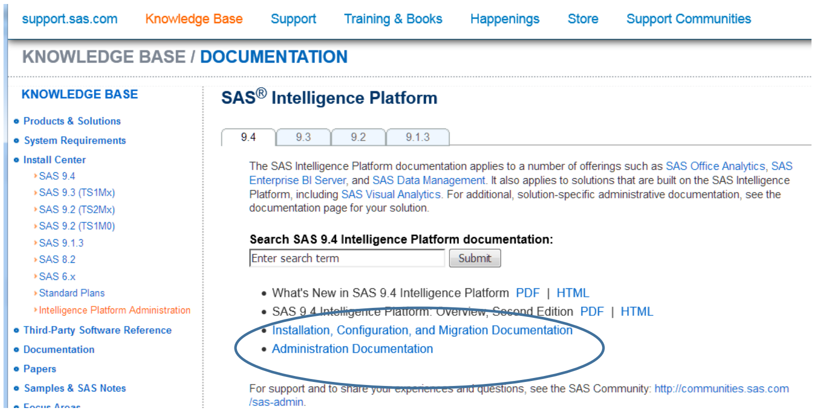


Select…

- ***E*** for **SAS Environment Manager**
- ***I*** for SAS **Intelligence Platform**
- ***S*** for **SAS/SECURE**
- ***V*** for SAS **Visual Analytics**

https://support.sas.com/documentation/onlinedoc/intellplatform/index.html

(or the shortcut format: http://support.sas.com/94administration)



The SAS Intelligence Platform documentation applies to a number of offerings such as SAS Office Analytics, SAS Enterprise BI Server, and SAS Data Management. It also applies to solutions that are built on the SAS Intelligence Platform, including SAS Visual Analytics. For additional, solution-specific administrative documentation, see the documentation page for your solution.

Search SAS 9.4 Intelligence Platform documentation:

- What's New in SAS 9.4 Intelligence Platform PDF | HTML
- SAS 9.4 Intelligence Platform: Overview, Second Edition PDF | HTML
- Installation, Configuration, and Migration Documentation
- Administration Documentation

For support and to share your experiences and questions, see the SAS Community: http://communities.sas.com/sas-admin.

Expand the **Administration Documentation** link to see the list of document titles, including

- **Security Administration Guide**
- **Middle-Tier Administration Guide**
- **System Administration Guide**
- **Encryption Guide**

Choose **Installation…** for information about new or upgraded deployments.

The following table highlights links to security-related documentation. These links are available at www.sas.com and support.sas.com.

Knowledge Base category	Starting link for the resource	Titles and comments
Products & Solutions	http://support.sas.com/software/94/index.html	SAS 9.4 Software for Security Administrators
Security Bulletin	http://support.sas.com/security/alerts.html	SAS Security Bulletins and Alerts
Install Center	http://support.sas.com/documentation/installcenter/en/ikdeploywizug/66034/PDF/default/user.pdf	SAS Deployment Wizard and SAS Deployment Manager 9.4: User's Guide (Contains information about installing certificates OOTB for TLS and HTTPS)
	http://support.sas.com/documentation/cdl/en/bisecag/67045/PDF/default/bisecag.pdf	SAS 9.4 Intelligence Platform: Security Administration Guide
	http://support.sas.com/downloads/package.htm?pid=1212	SAS 9.4 Pre-Installation Checklist Installation and Configuration Service Select your product deployment. Then find a ZIP file that best matches your deployment. See the "Standard Deployment Plans for 9.4"
	http://support.sas.com/documentation/cdl/en/fndigwin/68208/PDF/default/fndigwin.pdf	SAS 9.4 Foundation and Related Software: Installation Guide for Windows
	http://support.sas.com/documentation/cdl/en/fndigunx/68209/PDF/default/fndigunx.pdf	SAS 9.4 Foundation and Related Software: Installation Guide for UNIX
Documentation	http://support.sas.com/documentation/cdl/en/whatsnew/64788/PDF/default/whatsnew.pdf	What's New for SAS 9.4
	http://support.sas.com/documentation/cdl/en/whatsdiff/66129/PDF/default/whatsdiff.pdf	SAS Guide to Software Updates
	http://support.sas.com/documentation/cdl/en/secref/68007/HTML/default/viewer.htm#titlepage.htm	Encryption in SAS 9.4 (SAS/SECURE)
	http://support.sas.com/documentation/onlinedoc/secure/index.html	Roadmap for Security
	http://support.sas.com/documentation/onlinedoc/secure/openssl/SAStoOpenSSLVersionTable.pdf	OpenSSL Version and Library Files Available for Each Version of SAS
Third-Party Software Reference	http://support.sas.com/resources/thirdpartysupport/index.html	Third-Party Software Requirements and License Information for Hadoop, Java Runtime Environments, Java Development Kits, Web Application Servers, and so on.

Knowledge Base category	Starting link for the resource	Titles and comments
	http://support.sas.com/resources/thirdpartysupport/Java7Updates.html	Java Updates
Papers	http://support.sas.com/resources/papers/index.html	SAS Technical Papers
	http://www.sas.com/content/dam/SAS/en_us/doc/whitepaper1/sas-software-security-framework-107607.pdf	SAS Software Security Framework White Paper
	http://www.sas.com/en_us/whitepapers.html	White Papers
Samples & SAS Notes	http://support.sas.com/notes/index.html	Search for samples and SAS Notes using security-related keywords
SAS Blogs	http://blogs.sas.com/content/	Search for blogs using security-related keywords
SAS Support Communities	https://communities.sas.com/	Search communities using security-related keywords
Reference	http://www.sas.com/en_us/company-information/security.html	SAS Security Assurance

CONCLUSION

Security is a complex issue. We highlighted a few new and different examples for handling encryption using HTTPS and TLS. We also highlighted some of the auditing techniques that build on pre-defined reports. These topics are just the tip of the security iceberg.

SAS takes software security seriously. SAS will continue to evolve its security capabilities.

Whether you are an IT expert who is concerned about corporate security policies, an Administrator who needs to describe SAS capabilities and configure SAS software to work with corporate IT standards, or an auditor who needs to review specific questions about security vulnerabilities, we hope that this paper helps you with your security efforts.

There is a lot of documentation written about this expansive software security topic. Use the security roadmap to help you find the information that you need for the security task that you are tackling.

REFERENCES

In addition to the SAS documents referenced in this paper, here are some additional papers. A more complete list is included in the Security Documentation Roadmap at: http://support.sas.com/documentation/onlinedoc/secure/index.html

Cooper, et al. May 2008. "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile". RFC 5280. Available at https://tools.ietf.org/html/rfc5280.

Rogers, Stuart J. 2016. "Tips and Techniques for Using Site-Signed HTTPS with SAS® 9.4." *Proceedings of the SAS Global Forum 2016 Conference*. Cary, NC: SAS Institute Inc.

Rogers, Stuart J. "Managing TLS Certificates in SAS 9.4". YouTube. Published September 2015. Available at: https://www.youtube.com/watch?v=eWfHhZxqogQ.

Mozilla Wiki. 2015. “Mozilla Included CA Certificate List”. Accessed January 6, 2016. https://wiki.mozilla.org/CA:IncludedCAs.

Using pgAdmin III
Available at: http://www.pgadmin.org/docs/dev/using.html

ACKNOWLEDGMENTS

Many colleagues around SAS provided comments and content to improve this paper, including Stuart Rogers, Gerry Nelson, Bob Bonham, Merri Jensen, and Steve Holzworth.

RECOMMENDED READING

In the rapidly evolving world of security, our goal is to provide current and accurate information. These papers and documents provide a baseline as of early 2016. Please refer to the online roadmap for additional references and pointers.

Customer Experience Testing team 2016. “Helpful Hints for SAS®9.4.” *Proceedings of the SAS Global Forum 2016 Conference*. Cary, NC: SAS Institute Inc.

Langston, Richard D. 2016. “Implementing Hashing Techniques in SAS®.” *Proceedings of the SAS Global Forum 2016 Conference*. Cary, NC: SAS Institute Inc.

Park, Heesun. 2014. “Advanced Security Configuration Best Practices for SAS® 9.4 Web Applications and Mobile Devices”. Proceedings of the SAS Global Forum 2014. Available at http://support.sas.com/resources/papers/proceedings14/SAS054-2014.pdf.

Park, Heesun & Hughes Jerome. 2015. “SSL Configuration Best Practices for SAS® Visual Analytics 7.1 Web Applications and SAS® LASR™ Authorization Service”. Proceedings of the SAS Global Forum 2015. Available at http://support.sas.com/resources/papers/proceedings15/SAS1541-2015.pdf.

Park, Heesun. 2016. “How to Make Your SAS® Web Applications More Secure: Top Ten Tips.” *Proceedings of the SAS Global Forum 2016 Conference*. Cary, NC: SAS Institute Inc.

Roda, Mike. 2016. “Tips and Best Practices for Configuring Integrated Windows Authentication.” *Proceedings of the SAS Global Forum 2016 Conference*. Cary, NC: SAS Institute Inc.

Rogers, Stuart J. 2016. “Kerberos Delegation with SAS® 9.4” *Proceedings of the SAS Global Forum 2016 Conference*. Cary, NC: SAS Institute Inc.

CONTACT INFORMATION

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

Robin Crumpton
Base SAS Documentation
Robin.crumpton@sas.com

Qiana Eaglin
Enterprise Administration Documentation
Qiana.Eaglin@sas.com

Donna Bennett
Product Manager, Cloud and Platform Technologies
Donna.Bennett@sas.com