Introduction to Security Information

Securing SAS Software

How you approach the task of securing SAS Viya or SAS software is not straightforward, and the strategy or strategies that you use depend on several factors. To apply security can depend on your job in the organization and the SAS products, the third-party products, and the open-source software that you use. Other dependencies are the platform that you support and the components (the hardware and software services) in your environment. Consider these factors in more detail:

- Your role in the SAS Viya or SAS environment. Here are selected roles with an emphasis on security issues:
  - the IT expert who is concerned about corporate security policies
  - the network administrator who applies user access and authentication policies, configures SAS authentication components, maintains firewalls and proxy servers, and modifies LDAP settings as needed
  - the database administrator who executes restricted commands and installs and configures required DBMS or supporting software. The database administrator might also modify database user account privileges to enable the installation of required functions, libraries, or extensions by the SAS administrator
  - the SAS administrator who must be able to describe SAS capabilities and configure SAS software to work with corporate IT standards
  - the SAS auditor who must review specific questions about security vulnerabilities
  - the SAS programmer who connects to external sources and accesses data or creates new data
the SAS installer (deployment specialist) who must apply appropriate security features to new or upgraded deployments

the SAS applications developer who must apply security details to end-user applications

Typical security tasks that are performed in an organization. Examples are managing external and logon credentials, authenticating users and services, authorizing users who access data, and encryption of data at rest and in motion. This category of tasks requires knowledge about these topics: certificates, tokens, single sign-on, SAS Anonymous Web User, guest logon, time-outs, lockdown, metadata-bound libraries, credentials, permissions, roles, users, and identities.

SAS products that contain configurable security features.

Third-party and open-source products that SAS has optimized to secure your deployment. Examples of third-party software are Transport Layer Security (TLS), Secure Socket Layer (SSL), Kerberos, LDAP, Java, HTTPS, Integrated Web Authentication (IWA), WebSEAL, OpenID Connect, and Security Assertion Markup Language (SAML).

Security strategies include support for these platforms: Linux, UNIX, Windows, and z/OS.

Components of the business environment that require security. Examples are network communications, web applications, mobile devices, services, data (SAS or external data sources), deployment, and programming connections.

Navigating Security Information in SAS Documentation

The details that you need in order to apply security are not scoped to a specific SAS document. Instead, security details extend across the entire SAS documentation set according to these factors: your role in the SAS environment, the particular security task, the product, the platform, and the component.

All the SAS documents that contain security information are presented in two comprehensive lists: SAS Viya documents and SAS 9.4 documents. Scan the document titles and the associated brief descriptions to locate the information that relates to your interest. To explore the chosen topic, click the link to the document title. The link takes you directly to the topic within the document.

Additional Security Information

In addition to the SAS customer documentation, various supplementary sources also contain security information.

Security Assurance

You can read Security Assurance From SAS to learn about the SAS Software Security Framework and how it incorporates industry best practices and defines the guiding principles for the secure product development life cycle. You can also learn about SAS’ commitment to quality and its implementation of a full General Data Protection Regulation (GDPR) compliance program.

You can find white papers and technical documents about security by searching the SAS Resource Center.

Security Bulletins and SAS Technical Support Security Hot Fixes

SAS Security Bulletins highlight important security issues.
SAS Security Updates and Hot Fixes provide the latest security updates from SAS.

SAS Viya Documents: Security-Related Information

Here is a list of SAS Viya documents that contain security-related information:

Client Authentication Using an Authinfo File
   Provides information about using and formatting an authinfo file for client authentication.

Cloud Data Exchange and SAS Data Agent
   Cloud Data Exchange (CDE) is a data connection capability for SAS Data Preparation on SAS Viya. SAS Data Agent is the server that provides the environment to move data.

Encryption in SAS Viya 3.5: Data at Rest
   Provides information about how to encrypt data at rest (data stored in databases, file servers, endpoint devices, and various storage networks) in a SAS Viya deployment on Linux and Windows platforms. You can encrypt your data programmatically and by using SAS Environment Manager.

Encryption in SAS Viya 3.5: Data in Motion
   Provides information about how to harden encryption in a SAS Viya deployment using Transport Layer Security (TLS) on Linux and Windows platforms.

SAS Event Stream Manager 6.2: Using SAS Event Stream Manager
   Includes information related to authentication options for SAS Event Stream Processing servers.

SAS Event Stream Processing 6.2: JavaScript API Reference
   Explains how to write a simple function to authenticate server delegates with the ESP server.

SAS Event Stream Processing 6.2: Publish/Subscribe API Reference
   Provides information about how to enable authentication through the publish/subscribe APIs.

SAS Event Stream Processing 6.2: Implementing Security
   Provides information about how to enable encryption and authentication on TCP/IP connections to SAS Event Stream Processing Studio. It also explains how to set up access control on engine, project, query, and window objects.

   Contains information relating to the type of authentication methods used by SAS Event Stream Processing servers in a deployment. It also contains information about how to set the correct authentication properties when creating or editing properties for a SAS Event Stream Processing server using SAS Event Stream Processing Studio.

SAS Event Stream Processing 6.2: WebSocket API Reference
   Includes information about authentication handshaking for the API.

SAS Job Execution Web Application 2.2: User’s Guide
   Provides information about authorization for SAS Viya jobs. You can search for the following topic in the document:
      - Security for SAS Viya Jobs

   Contains general information about passwords and security. You can search for the following topics in the document:
      - Blotting Passwords and Encryption Key Values
Encrypting Variable Values

Encryption and Integrity Constraints

SAS Data File Encryption

SAS Micro Analytic Service 5.4: Programming and Administration Guide

Discusses how to configure HTTP and HTTPS web services through the DS2 HTTP package and explains DS2 HTTP package support for security-related methods. It also discusses how to negotiate mechanism support of Kerberos and NTLM, how to access to REST API endpoints via authorization rules, and how to work with Python and SAS Micro Analytic Service.

You can search for the following topics in the document:

- Secure DS2 HTTP Package Usage
- Compile and Execute Python Modules Using Alternate Credentials
- SAS Micro Analytic Service Security and Authorization
- Working with Python and SAS Micro Analytic Service
- Moving Objects by Using the SAS Viya Transfer Service
- Verifying module status via REST endpoints
- Obtaining metrics for SAS Micro Analytic Service via REST endpoints

SAS Model Manager 15.3: Administrator’s Guide

Explains usage of SAS Environment Manager to manage identities and authorization. Permissions are provided for SAS Model Manager, by default.

You can search for the following topic in the document:

- Managing Permissions

SAS Viya 3.5 Administration: Auditing

Provides information about actions that generate audit records. Some actions that generate audit records related to security are logon attempts, logoff attempts, access of authorization rules, and updates of authorization rules.

SAS Viya 3.5 Administration: Authentication

Provides information about configuring in-bound and out-bound authentication in a SAS Viya deployment on Linux and Windows platforms with the following software:

- LDAP
- Kerberos
- OAuth and OpenID Connect
- SAML (Security Assertion Markup Language)
- PAM (pluggable authentication module)

SAS Viya 3.5 Administration: Orientation to Authorization

Provides an introduction to the SAS Viya authorization layer. It consists of the Cloud Analytic Services (CAS) authorization system and the general authorization system, which are used to protect distinct classes of resources. Complete details are provided in the following documents:

- SAS Viya 3.5 Administration: Cloud Analytic Services Authorization
- SAS Viya 3.5 Administration: General Authorization
- SAS Viya 3.5 Administration: Access to Functionality
SAS Viya 3.5 Administration: Backup and Restore
Provides complete details about the scheduling of backups to protect the integrity of content and configuration information stored in SAS Viya components. This information is relevant following the deployment of SAS Viya.

SAS Viya 3.5 Administration: CAS Fundamentals
Provides information about using CAS securely with authorization, authentication, and encryption of data at rest and data in motion. You can click the following link to the specified topic in the document:
- Security

SAS Viya 3.5 Administration: Using the Command-Line Interfaces
Provides information with examples about the following searchable topics in the document:
- Audit
- CAS Authorization
- General Authorization
- Identities

SAS Viya 3.5 Administration: Configuration Properties
Identifies system properties, application properties, and services properties that deal with authentication, SAS Secrets Manager, Logon, Identities, Domains, and other security. It also references security properties that are documented in other security documents.

SAS Viya 3.5 Administration: External Credentials
Describes administrative tasks to securely manage external credentials using SAS Environment Manager. SAS Viya users might need external credentials for accessing databases and other third-party products.

SAS Viya 3.5 Administration: Identity Management
Explains the storage and management of user and group identities by the organization’s identity provider (for example, Microsoft Active Directory). Read-Only access to the provider enables SAS to authenticate users and to obtain identity information at sign-on.

SAS Viya 3.5 Administration: Infrastructure Servers
Describes the infrastructure servers that make up a SAS Viya deployment. SAS Secrets Manager is a server that uses Vault (based on HashiCorp Vault) to store and generate secrets such as TLS certificates. The SAS Secrets Manager is supported only in a full deployment on the Linux platform.

SAS Viya 3.5 Administration: Mobile
With the SAS Visual Analytics App, enables mobile device users to view and interact with reports that can contain a variety of charts, graphs, gauges, tables, and other report objects. The administrator can control how a mobile device that runs the SAS Visual Analytics App can access reports and data that is located on a SAS Visual Analytics server. Administrative features, rules, and properties (alone or in combination) are used to control access to the server data and reports from the app.

You can search for the following topics in the document:
- Blacklist and Whitelist Features
- Passcode Feature
- Prevent Mobile Devices from Storing Report Data
- Offline-Access Time-Out Feature
- Remote report data rule
- Limit functionality in the app
SAS Viya 3.5 Administration: Multi-tenancy
Contains information about the following security tasks:
- Maintaining data isolation across multiple tenants, a provider tenant, and SAS Viya applications. SAS Viya end-user software can be shared between tenants or used exclusively in individual tenants.
- Separating the provider administrator and tenant administrator roles to maintain data isolation.
- Using the LOCKDOWN system option and the LOCKDOWN statement so that multiple tenants and the provider tenant always run in lockdown mode.
- Updating Apache Server to use custom certificates.

SAS Viya 3.5 Administration: Overview
Provides a brief overview of the types of security that are provided in a SAS Viya deployment. You can click the following link to the specified topic in the document:
- Security in SAS Viya

SAS Viya 3.5 for Containers: Deployment Guide
Provides information about the security requirements for Authentication and TLS default settings and how to enhance those settings in a SAS Viya container deployment. You can search for the following topics in the document:
- Security Requirements
- Enable Host Authentication
- Pre-deployment Hadoop Tasks

SAS Viya 3.5 for Linux: Deployment Guide
Provides information about the security requirements for LDAP and TLS default settings and how to enhance those settings in a SAS Viya deployment on the Linux platform. You can search for the following topics in the document:
- Security Requirements
- Post-installation Tasks
- Pre-deployment Hadoop and Spark Tasks
- Teradata Deployment: Configuring SAS In-Database Technologies
- Perform Linux Tuning
- User and Group Requirements
- Kerberos Requirements

SAS Viya 3.5 for Windows: Deployment Guide
Provides information about the security requirements for LDAP, Authentication, and TLS default settings and how to enhance those settings in a SAS Viya deployment on the Windows platform. You can search for the following topics in the document:
- Security Requirements
- Post-installation Tasks
- User Account Requirements

SAS Viya 3.5 Universal Printing
Provides information about how to use SAS system options to secure PDF documents. See the topic about Creating PDF Files Using Universal Printing.
Here is a list of SAS 9.4 documents that contain security-related information:

**Application Messaging with SAS 9.4**
- Provides information for CALL routines that enable you to set access control. You can search for the following topics in the document:
  - CALL MSMQGETQSEC Routine
  - CALL MSMQSETQSEC Routine
  - Configuring WebSphere MQ Client Access
  - FILENAME Statement, JMS Access Method
  - FILENAME Statement, ACTIVEMQ Access Method

**Base SAS 9.4 Procedures Guide**
- You can search for the following SAS procedures for security-related information in the document:
  - PROC AUTHLIB is a utility procedure that manages metadata-bound libraries.
  - PROC HTTP uses HTTPS protocol when certificates of the trusted service are configured. It supports several types of authentication and enables you to specify the type to use in order to bypass negotiation. Supported authentication types include user authentication (direct and via a proxy), NTLM (New Technology LAN Manager), Kerberos, and other HTTP authentication. Beginning in SAS 9.4M6, PROC HTTP included an SSLPARMS statement that enables you to override the global secure communication settings for the SAS system with local settings for the PROC HTTP request. The SSLPARMS statement takes SSL system options as input.
  - PROC PWENCODE enables you to encode passwords.
  - PROC S3 includes information about using server-side encryption with AWS (Amazon Web Services) data, securing a PROC S3 configuration file, and options that enable you to manage authentication with AWS.
  - PROC SOAP uses the HTTPS protocol when certificates of the service to be trusted are configured. This truststore and its password must be provided to the SAS session by setting Java system options.

**DataFlux Authentication Server: Administrator’s Guide and Help**
- Note: This information is also available in the SAS Help interface.

Documents authentication as it is done on the former DataFlux Data Management Platform. Almost all the clients and servers that formerly used the Auth Server now use SAS Metadata Server for authentication, by default. The Auth Server does authentication only. Authorization is handled locally on the servers of SAS Data Management Platform. This guide and the Help explain how to configure connections to as many as three authentication providers in three separate domains. Also, information is provided on how user profiles are created and stored on the local host of the Auth Server. The server also provides additional server access controls that are implemented in configuration files. This server is now configured to run DataFlux Secure, by default. TLS can also be enabled, as appropriate.
DataFlux Data Management Server: Administrator’s Guide
Describes how the DataFlux Data Management Server maintains local authorization and other
local access controls with groups and IP addresses. The server authenticates on SAS Metadata
Server, by default. The DataFlux Data Management Server does not use the authorization
features of SAS Metadata Server. DataFlux Secure is installed, by default. TLS can also be
enabled, as appropriate.

DataFlux Secure 2.7: Administrator’s Guide
Describes the use of AES (Advanced Encryption Standard) encryption, TLS (Transport Layer
Security) protection for HTTP, and FIPS (Federal Information Processing Standards) compliance
to meet government regulations. This version of SAS/SECURE is now delivered in a disabled
state, by default, on all the former components of the Data Management Platform.

Encryption in SAS 9.4
Provides information about installing, configuring, and using SAS and third-party products to
encrypt data in motion. It also discusses SAS proprietary, SAS/SECURE, industry-standard
encryption algorithms, and third-party strategies (TLS and SSH) for protecting data and
credentials in a networked environment. In SAS 9.4, SAS/SECURE is included with the Base SAS
software, making strong encryption available in all deployments (except where prohibited by
import restrictions). This document includes SAS system options and environment variables used
to configure TLS on all of the IOM servers.

You can search for the following system options and environment variables in the document:
- ENCRYPTFIPS= System Option
- NETENCRIPT= System Option
- NETENCYPTALGORITHM= System Option
- NETENCYPTKEYLEN= System Option
- SSLCALISTLOC= System Option
- SSLCACERTDIR= System Option
- SSLCACERTDATA= System Option
- SSLCERTISS= System Option
- SSLCERTLOC= System Option
- SSLCERTSERIAL= System Option
- SSLCERTSUBJ= System Option
- SSLCLIENTAUTH= System Option
- SSLCRLCHECK= System Option
- SSLCIPHERLIST= System Option
- SSLCRLLOC= System Option
- SSLMODE= System Option
- SSLMINPROTOCOL= System Option
- SSLPKCS12LOC= System Option
- SSLPKCS12PASS= System Option
- SSLPVTKEYLOC= System Option
- SSLPVTKEYPASS= System Option
- SSLSNIHOSTNAME= System Option
- SSL_USE_SNI Environment Variable
- **SAS_VIYA_TOKEN Environment Variable**
- **CAS_CLIENT_SSL_CA_LIST Environment Variable**

**Grid Computing in SAS 9.4**
Provides information about how to set up authentication for SAS Grid Manager (using SAS Workload Orchestrator) and how to use Kerberos authentication for SAS Grid Manager for Platform and SAS Grid Manager for Hadoop.

**SAS 9.4 BI Web Services: Developer's Guide**
Provides information about authentication. You can search for the following topic in the document: Overview of Security for Web Services.

**SAS 9.4 Companion for UNIX Environments**
Includes information about file permissions and SAS functions that relate to directory and file permissions. It also contains SAS procedures, SAS statements, and SAS system options that relate to file permissions, assigning passwords to SAS files, and locking files.

**SAS 9.4 Component Objects: Reference**
Provides comprehensive information about SAS component objects. When declaring a hash object, you can use a SAS data set option to specify a password for a data set.

**SAS 9.4 Data Set Options: Reference**
Provides comprehensive information about SAS data set options. Data set options specify actions that apply only to the specified SAS data set. Some data set options provide security for your data sets, such as passwords and encryption. This document includes the ENCRYPT= and ENCRYPTKEY= SAS data set options. They both support AES (Advanced Encryption Standard) encryption.

**SAS 9.4 DATA Step Statements: Reference**
Provides comprehensive information about SAS DATA step statements. Some statements provide security options for data sets and views, such as passwords. The FILE and INFILE statements include information that pertains to security settings.

**SAS 9.4 DS2 Language Reference**
Provides comprehensive information about the SAS DS2 language. You can search for the following topics about DS2 language elements in the document:

- PACKAGE statement
- THREAD statement
- ENCRYPT= table option
- ENCRYPTKEY= table option
- PW= table option

**SAS 9.4 FedSQL Language Reference**
Provides comprehensive information about the SAS FedSQL language. You can search for the following topics about FedSQL language elements in the document:

- ENCRYPT= table option
- ENCRYPTKEY= table option
- PW= table option

**SAS 9.4 Foundation Services: Administrator's Guide**
Provides information about the Security Service. This service provides authentication, propagation of user identity context across distributed security domains, and protected resource access policy administration.

Provides information about the User Service. This service provides access to authenticated user context, access to global, solution-wide, and application-specific profiles, and access to personal objects.
You can search for the following topics in the document:

- Understanding Service Deployments
- Modifying the Session and User Service Configurations

**SAS 9.4 Global Statements: Reference**

Provides comprehensive information about SAS global statements. The following individual statements include information that pertains to security settings.

You can search for the following topics in the document:

- `FILENAME` Statement
- `FILENAME` Statement, FTP Access Method: AUTHDOMAIN, PASS, USER arguments
- `FILENAME` Statement, Hadoop Access Method: PASS, USER arguments
- `FILENAME` Statement, SFTP Access Method: PASS, USER arguments
- `FILENAME` Statement, URL Access Method: AUTHDOMAIN, PASS, USER arguments

**Note:** HTTP or HTTPS can be used to access files.

- `FILENAME` Statement, WEBDAV Access Method AUTHDOMAIN, PASS, USER arguments
- `LIBNAME` Statement, AUTHADMIN argument
- `LIBNAME` Statement, WebDAV Server Access: AUTHDOMAIN, PASS, USER arguments
- `LOCK` Statement

**Note:** The LOCK statement enables you to acquire, list, or release an exclusive lock on an existing SAS file.

- `SAS_FTP_AUTHTLS` Environment Variable

**SAS 9.4 Guide to Metadata-Bound Libraries**

Provides information about how to set up and administer metadata-bound libraries. Each physical table within a metadata-bound library has information in its header that points to a specific metadata object (a secured table object). The pointer creates a security binding between the physical table and the metadata object. The binding ensures that SAS universally enforces metadata-layer permission requirements for the physical table regardless of how a user requests access from SAS.

The guide also contains several topics that are related to encryption of the data sets in metadata-bound libraries.

**SAS 9.4 Hadoop Configuration Guide for Base SAS and SAS/ACCESS**

Discusses Kerberos security requirements for Hadoop. You can search for the following topics in the document:

- Configuring SAS/ACCESS for Hadoop
- Configuring SPD Engine
- Using the SAS Deployment Manager to Obtain Hadoop JAR and Configuration Files
- Using the Hadoop Tracer Script to Obtain the Hadoop JAR and Configuration Files

**SAS 9.4 In-DATABASE Products: Administrator's Guide**

Discusses Kerberos security requirements for configuring SAS Embedded Process for Hadoop.
SAS 9.4 In-Database Products: User’s Guide
Discusses Kerberos security requirements for performing in-database processing in Hadoop and Teradata.

SAS 9.4 Integration Technologies: Directory Services Reference
Provides information about LDAP security. You can search for the following topic in the document:
- Understanding LDAP Security

SAS 9.4 Integration Technologies: Java Client Developer’s Guide
Provides information about encryption and authentication. You can search for the following topics in the document:
- Java Client Security
- Connecting with Directly Supplied Server Attributes
- Security Service

Provides information about encryption, authentication, and COM security settings. You can search for the following topics in the document:
- Encryption Support
- Windows Client Security
- Administering Pooling
- Security Considerations (for Launching IOM Servers)

SAS 9.4 Intelligence Platform: Application Server Administration Guide
Provides instructions on how to use the following SAS system options and SAS statement using a SAS Application Server. The guide also includes platform-specific instructions for using TLS.
- Spawner Invocation Options
- LOCKDOWN System Option
- SECPACKAGE System Option
- SECPACKAGELIST System Option
- SSPI System Option
- PROTOLIBS System Option
- USERCONFIG System Option
- LOCKDOWN Statement
- TLS Support for IOM Servers

SAS 9.4 Intelligence Platform: Data Administration Guide
Provides information about how data set security and table-level security are used to create metadata for the tables in a library. Tables are registered using SAS Management Console or PROC METALIB. You can search for the following topic in the document:
- Managing Table Metadata

SAS 9.4 Intelligence Platform: Desktop Application Administration Guide
Provides information about using SAS Management Console to manage servers, libraries, security, metadata objects, roles, logs, backup and recovery, scheduling, and message queues.

SAS 9.4 Intelligence Platform: Installation and Configuration Guide
Provides descriptions of SAS Deployment Wizard configuration prompts and instructions about setting up certificates for SAS deployments. It also identifies key reasons for using internal accounts, and it defines the required accounts and privileges.
You can search for the following topics in the document:

- Setting Up Users, Groups, and Ports
- Internal User Accounts

**SAS 9.4 Intelligence Platform: Middle-Tier Administration Guide**

Documents the security features that are provided by the middle tier. It also provides information about methods of authenticating the middle-tier components.

You can search for the following topics in the document:

- Configuring SAS Web Server Manually for HTTPS
- Configuring SAS Web Application Server to Use HTTPS
- FIPS 140-2 Compliance
- Support for CA SiteMinder
- Support for IBM Tivoli Access Manager WebSEAL
- Support for Integrated Windows Authentication
- Support for TLS with Client Certificate Authentication
- Using the SAS Anonymous Web User with SAS Authentication
- Web Authentication

**SAS 9.4 Intelligence Platform: Overview**

Provides a high-level overview of security in the SAS Intelligence Platform.

**SAS 9.4 Intelligence Platform: Security Administration Guide**

Provides the security features of the SAS Intelligence Platform. It includes essential information for all security administrators. Topics include authorization, authentication, encryption, and user administration. The guide also contains a checklist to help secure your deployment.

**SAS 9.4 Intelligence Platform: System Administration Guide**

Provides security information about loggers for metadata server events. It describes security-related properties that can be set in the metadata server configuration file. It also describes options that control the assignment and management of passwords for internal users.

You can search for the following topics in the document:

- About Metadata Server Loggers
- Overview of Initial Roles, Groups, and Users
- Promoting Access Controls
- Promoting Secured Data Folders, Secured Library Objects, and Secured Table Objects
- Promoting Security Objects and Server Objects
- Reference Information for omaconfig.xml
- Who Can Do What: Credential Requirements for SAS Management Console Tasks

**SAS 9.4 Language Reference: Concepts**

Contains general information about passwords and security. You can search for the following topics in the document:

- Blotting Passwords and Encryption Key Values
- Creating PDF Files Using Universal Printing
- Encrypting Variable Values
- Encryption and Integrity Constraints
- SAS Data File Encryption

**SAS 9.4 V9 LIBNAME Engine: Reference**
Contains general information about passwords and security. If a V9 engine feature has an interaction with passwords or encryption, the information is included in the topic.

Provides information about how to use SAS passwords to secure unsecured DSN definitions.

**SAS 9.4 Logging: Configuration and Programming Reference**
Provides information about how to generate audit messages for metadata-bound libraries. You can search for the following topic in the document:
- Audit Messages for Metadata-Bound Libraries

**SAS 9.4 Management Console: Guide to Users and Permissions**
Provides instructions about using SAS Management Console to administer users, groups, and roles, to set permissions, and to work with ACTs. You can search for the following topics in the document:
- Access Management Tasks
- Exercises in Access Management
- Exercises in User Administration
- User Administration Tasks

**SAS 9.4 Management Console: User Manager Plug-in**
Provides instructions on how to administer users, groups, and roles using SAS Management Console.

Note: This information is available only through the SAS Help interface.

**SAS 9.4 OLAP Server: MDX Guide**
Discusses member-level authorizations that are applied as permission conditions for SAS OLAP cubes. It also discusses the default member for a cube and both Virtual Members and Security Totals.

You can search for the following topic in the document:
- SAS OLAP Security Totals and Permission Conditions

Provides information about SAS authorization permissions for SAS OLAP cubes and the different components of a cube. Authorization functions are available in either SAS OLAP Cube Studio or the Authorization Manager plug-in in SAS Management Console.

You can search for the following topic in the document:
- Authorization Permissions

Provides information about how to implement authorization for channels and subscribers. You can search for the following topic in the document:
- Implement Content Restrictions in the SAS Metadata Authorization Layer

**SAS 9.4 Scalable Performance Data Engine: Reference**
Includes some encryption details that are different from the Base SAS V9 engine. You can search for the following topic in the document:
- Encrypting SPD Engine Data Sets
SAS 9.4 Security Considerations for SAS Studio
Describes security controls that are available to SAS Administrators who are managing the Basic (multi-user) and Enterprise editions of SAS Studio running in a SAS 9.4 environment.

SAS 9.4 Stored Processes: Developer’s Guide
Contains information about hiding passwords and other sensitive data from SAS log. It also explains how SAS Stored Process Web Application uses the SAS Logon Manager for web authentication.

You can search for the following topics in the document:
- Hiding Passwords and Other Sensitive Data
- Authentication in the SAS Stored Process Web Application

SAS 9.4 System Options: Reference
Provides reference information about SAS system options that pertain to security and authentication. It also contains SAS functions and SAS procedures that process system options.

You can search for the following topics in the document:
- AUTHINFO= System Option
- AUTHPROVIDERDOMAIN System Option
- EMAILHOST= System Option
- EMAILAUTHPROTOCOL= System Option
- EMAILPW= System Option
- HTTPSERVERPORTMAX= System Option
- HTTPSERVERPORTMIN= System Option
- PDFSECURITY= System Option
- PDFPASSWORD= System Option
- PRIMARYPROVIDERDOMAIN= System Option
- SERVICESBASEURL= System Option

SAS Analytical Data Set Builder 6.3: Administrator’s Guide
Includes information related to user roles and permissions. It also contains details about perform administrative tasks to define users, assign roles, and add users to groups.

Note: This is a secure document that is available on a password-protected site.

You can search for the following topics in the document:
- Define Users, Assign Roles, and Add Users to User Groups
- Roles and Capabilities

SAS Anti-Money Laundering 7.1: Administration Guide
Provides information about administering security for users and groups. It includes roles, permissions, and capabilities.

Note: This is a secure document that is available on a password-protected site.

SAS Anti-Money Laundering 7.1: Installation and Configuration Guide
Provides information about administering security for users and groups. It includes roles, permissions, and capabilities. It also provides information about creating a metadata user account for the post-installation steps.
SAS Asset and Liability Management 5.1.2: Installation and Configuration Guide
Provides information about securing SAS Asset and Liability Management. It includes defining users, roles, and groups, and configuring metadata accounts.

Note: This is a secure document that is available on a password-protected site.

SAS Business Rules Manager 3.3: Administration Guide
Provides information about administering security for groups, roles, and capabilities. It also provides information about configuring your deployment for HTTPS and verifying certificates.

You can search for the following topics in the document:
- Configure Your Deployment for HTTPS
- Configuring Users, Groups, and Roles
- Performing Post-installation Tasks

SAS Cloud: Account Administrator’s Guide
Includes information about access control for users and groups in a tenant in the SAS Cloud with the App Central web interface.

SAS Commodity Risk Analytics 4.2: Administrator’s Guide
Provides information about securing SAS Commodity Risk Analytics. It includes defining users, roles, and groups, and configuring metadata accounts.

Note: This is a secure document that is available on a password-protected site.

You can search for the following topic in the document:
- Configuring Transport Layer Security

SAS Credit Scoring 6.3: Administrator’s Guide
Includes information about user roles and permissions. It also contains administrative tasks to define users, assign roles, and add users to groups.

Note: This is a secure document that is available on a password-protected site.

You can search for the following topics in the document:
- Define Users, Assign Roles, and Add Users to User Groups
- Roles and Capabilities

SAS Customer Due Diligence 7.1: Administrator’s Guide
Provides information about administering security for users and groups. It includes roles, permissions, and capabilities. It also provides information about creating a metadata user account for the post-installation steps.

Note: This is a secure document that is available on a password-protected site.

You can search for the following topics in the document:
- Administration
- Installation
Post-Configuration

SAS Customer Due Diligence 7.1: Installation, Configuration, and Administration Guide
Provides information about administering security for users and groups. It includes roles, permissions, and capabilities. It also provides information about creating a metadata user account for the post-installation steps.

Note: This is a secure document that is available on a password-protected site.

SAS Customer Intelligence 360: Onboarding Guide
Provides information about using SAS App Central to perform account administration functions for SAS Customer Intelligence 360, including adding users, assigning users to roles and environments, and managing email templates.

SAS Customer Intelligence 360: User’s Guide
Provides information about using SAS Customer Intelligence 360 offerings, including role management for existing users and information about how to gain access to the external API gateway. API information includes whitelisting domains and generating a JSON Web Token (JWT). The JWT is then included as an authorization token when the user submits REST API calls through the external gateway.

Note: This is a secure document that is available on a password-protected site.

You can search for the following topic in the document:

- Setting Up the External API Gateway

SAS Data Remediation 2.4: User's Guide
Explains how to restrict access to data remediation issues by setting permissions by subject area. It also provides details about new roles in SAS Management Console that are used to control access in SAS Data Remediation.

You can search for the following topic in the document:

- Working with SAS Data Remediation Administration

SAS Decision Manager 5.2: Administration Guide
Provides information about administering security for groups, roles, and capabilities. It also provides information about configuring your deployment for HTTPS, configuring your deployment for single sign-on authentication, and configuring users that are authenticated through Kerberos.

SAS Embedded Process: Deployment Guide
Discusses Kerberos security requirements for deploying the SAS Embedded Process for Hadoop.

You can search for the following topics in the document:

- Deploying SAS Embedded Process Manually
- Deploying SAS Embedded Process Using a Parcel or Stack
- Overview of SAS Embedded Process Deployment for Hadoop
- Upgrading or Uninstalling SAS Embedded Process for Hadoop

SAS Enterprise Guide 8.2 and SAS 8.2 for Microsoft Office: Administrator’s Guide
Provides instructions about customizations, encryption, managing libraries, configuration for IWA (Integrated Windows Authentication), configuration for grid computing and parallel execution, and working with roles.

SAS Environment Manager 2.4 Security Administration Module Documentation
Provides instructions about managing metadata access using SAS Environment Manager.
SAS Environment Manager 2.5 Administration: User’s Guide
Provides information about how to administer users and metadata access with SAS Environment Manager. It also provides instructions about managing metadata access using SAS Environment Manager, and it provides information about how to administer users, groups, and roles using SAS Environment Manager in order to track user activity and manage access.

SAS Environment Manager: User Manager Module 2.2 Documentation
Provides information about how to administer users, groups, and roles using SAS Environment Manager in order to track user activity and manage access.

SAS Episode Analytics 4.4: Administration
Provides information about user groups, capabilities, and metadata permissions.

Note: This is a secure document that is available on a password-protected site.

SAS Federation Server 4.2: Administrator’s Guide
Provides instructions to configure permissions and privileges for SAS Federation Server and to configure data using administration DDL statements. It also gives details about encryption, data source authorization, and SAS Federation Server authorization that is available through the server.

SAS Forecast Server 15.1: Administrator's Guide
Provides information about how to specify security permissions for users and groups. It discusses layers of security that are divided into capabilities, metadata permissions, project ownership and sharing, and file system permissions. It also contains pre-installation information about using SAS scripts to grant permissions to user groups on the UNIX platform.

SAS Forecasting for Desktop 15.1: Administrator’s Guide
Provides information about how to specify security permissions for users and groups. It discusses layers of security that are divided into capabilities, metadata permissions, project ownership and sharing, and file system permissions. It also contains pre-installation information about using SAS scripts to grant permissions to user groups on the UNIX platform.

SAS High-Performance Analytics Infrastructure 3.9: Installation and Configuration Guide
Describes how to deploy the analytics environment with Kerberos, how to use SSH, and how to encrypt SASHDAT files. You can search for the following topics in the document:

- Encrypting SASHDAT Files
- Preparing for Kerberos
- Review Passwordless Secure Shell (SSH) Requirement

SAS Infrastructure for Risk Management 3.6: Administrator’s Guide
Provides information about administering security for users and groups. It includes roles, permissions, and capabilities. It also provides information about creating a metadata user account in the contexts of pre-installation and post-installation tasks.

You can search for the following topics in the document:

- Grant Linux directory permissions
- Apply SAS security updates
- Configure HTTPS as the SAS Infrastructure for Risk Management Web Connection
- Configure the Development Environment
- Configure the LOCKDOWN Feature
- Configure the Metadata Accounts for SAS Infrastructure for Risk Management
- Create Roles, Groups, and Users
- Define Groups
Set Up User Accounts Required for Deployment

SAS Intelligent Planning Suite 8.2: Administrator’s Guide
Includes information about user roles and permissions. It also provides information about creating an ETL user account.

Note: This is a secure document that is available on a password-protected site.

You can search for the following topics in the document:
- Managing Permissions
- Create a Group for ETL Users

SAS IT Resource Management 3.9: Administrator’s Guide
Provides information about using the lockdown feature and accessing third-party collectors.

SAS IT Resource Management 3.9: Migration Guide
Provides information about encrypting passwords.

SAS IT Resource Management 3.9: Report Center Guide
Provides information about permissions, credentials, authorization, authentication, running with secure sockets layer protocol, sign-on and sign-off, and time-outs.

SAS Marketing Automation 6.5: Administrator’s Guide
Provides information about administering security for users and groups. It includes roles, permissions, capabilities, and access control templates.

Note: This is a secure document that is available on a password-protected site.

SAS Marketing Optimization 6.5: Administrator’s Guide
Provides information about administering security for users and groups. It includes roles, permissions, capabilities, and access control templates.

Note: This is a secure document that is available on a password-protected site.

SAS MDM 4.3: Administrator’s Guide
Provides information about authentication, authorization, auditing, and encryption. You can search for the following topic in the document:
- Security Consideration for SAS MDM

SAS MDM 4.3: User’s Guide
Provides information about authentication and authorization. You can search for the following topic in the document:
- Security Consideration for SAS MDM

SAS Merchandise Allocation 4.2: Installation and Configuration Guide
Describes how to implement HTTPS and TLS security when setting up web server and web application server instances. It includes details about using the security Audit Log feature to capture a record of security-related events for accountability and to control security by authenticating users based on their IDs and passwords. It also explains how to use user groups to provide and restrict user access to certain features and functions.

Note: This is a secure document that is available on a password-protected site.

You can search for the following topics in the document:
SAS Merchandise Planning 6.8: Installation and Configuration Guide

Configure Single Sign-on
Setting up Users and Groups
SAS Merchandise Allocation Security

This guide describes how to implement HTTPS and TLS security when setting up web server and web application server instances. It includes details about using the security Audit Log feature to capture a record of security-related events for accountability and to set security properties for the application. It also explains how to control security by authenticating users based on their IDs and passwords, how to use user groups to provide and restrict user access to certain features and functions, and how to grant user group access to each interface object (such as a menu item, toolbar button, or option) in the application.

Note: This is a secure document that is available on a password-protected site.

You can search for the following topics in the document:
- Create the SAS Merchandise Planning User Accounts
- Configuring Single Sign-on
- About User and Group Setup
- Setting Up User Groups
- Configuring User Groups
- Configuring Users
- Configuring a SAS Web Server Instance for the Application
- Setting Application Properties

SAS Micro Analytic Service 2.5M2: Programming and Administration Guide

This guide discusses how to configure HTTP and HTTPS web services through the DS2 HTTP package and explains DS2 HTTP package support for security-related methods. It also discusses how to negotiate mechanism support of Kerberos and NTLM, how to access REST API endpoints via authorization rules, and how to work with Python and SAS Micro Analytic Service.

You can search for the following topics in the document:
- Secure DS2 HTTP Package Usage
- Compile and Execute Python Modules Using Alternate Credentials
- SAS Micro Analytic Service Security and Authorization
- Working with Python and SAS Micro Analytic Service
- Moving Objects by Using the SAS Viya Transfer Service

SAS Model Implementation Platform 3.2: Administrator’s Guide

This guide describes how to set up security for SAS Model Implementation Platform, including defining users, roles, and groups, configuring metadata accounts, and managing risk work groups.

Note: This is a secure document that is available on a password-protected site.

You can search for the following topics in the document:
- Change the Passwords for the SAS Risk Common Data Server
- Configure Metadata Accounts for SAS Model Implementation Platform
- Create Roles, Groups, and Users
Create SAS Users and Groups
Enable Users to Manage Objects in SAS Model Risk Management
Managing Access to Objects with Risk Work Groups
Register Your Risk Work Groups
Set Up User Accounts

SAS Model Manager 14.3: Administrator’s Guide
Provides information about web authentication. You can search for the following topic in the document:
Configure Your Deployment for Single Sign-On Web Authentication

SAS Real World Evidence 4.4: Administration
Provides information about user groups, capabilities, and metadata permissions.

Note: This is a secure document that is available on a password-protected site.
You can search for the following topic in the document:
Security

SAS Real-Time Decision Manager 6.5: Administrator’s Guide
Provides information about administering security for users and groups. It includes roles, permissions, capabilities, and access control templates.

Note: This is a secure document that is available on a password-protected site.
You can search for the following topic in the document:
Security Administration

SAS Regulatory Content for EBA Taxonomies: Installation Guide
Includes pre-installation and post-installation instructions that provide information about default users, groups, and roles. It also includes instructions to configure the user access setup using SAS Management Console.

Note: This is a secure document that is available on a password-protected site.
You can search for the following topics in the document:
Set Entity-Level Security for Validation Rules Summary Report
User Access Setup for SAS Risk and Finance Workbench
Using the Default Metadata User Accounts

SAS Regulatory Risk Management 6.1 Content Release: Installation Guide
Includes pre-installation and post-installation instructions that provide information about default users, groups, and roles. It also includes instructions to configure the user access setup using SAS Management Console.

Note: This is a secure document that is available on a password-protected site.
You can search for the following topics in the document:
Set Entity-Level Security for Validation Rules Summary Report
User Access Setup for SAS Risk and Finance Workbench
Using the Default Metadata User Accounts

SAS Risk and Finance Workbench 3.2: Administrator's Guide
Provides information about securing SAS Risk and Finance Workbench. It includes details about defining users, roles, and groups, configuring metadata accounts, and registering risk work groups.

Note: This is a secure document that is available on a password-protected site.

SAS Risk Governance Framework 7.4: Administration and Customization Guide
Provides information about securing the product and customizing administration roles.

Note: This is a secure document that is available on a password-protected site.

You can search for the following topics in the document:
- Security Administration
- Customizing Roles and Loading Users

SAS Risk Governance Framework 7.4: Installation and Configuration Guide
Provides information about securing Apache Solr.

Note: This is a secure document that is available on a password-protected site.

You can search for the following topic in the document:
- Configure Security for Apache Solr

SAS Scalable Performance Data Server 5.4: Administrator's Guide
Provides information about setting up and administering a SAS Scalable Performance Data (SPD) Server. Beginning with SPD Server 5.3, the server supports secure sockets communication via Transport Layer Security (TLS). The secure sockets communication is provided for SAS clients and SAS Federation Server clients.

Beginning in SPD Server 5.4, SPD Server supports FIPS 140-2 security compliance by enabling you to store passwords in a password database that uses a FIPS 140-2-approved encryption algorithm. When the server or a client is configured with FIPS-capable OpenSSL libraries, the server is capable of FIPS compliant communication.

The server supports various forms of authentication, including registration in a proprietary password database, LDAP security, and metadata-based security.

The server controls user access to data by requiring users to specify a server domain to make a data connection instead of by specifying the physical location of server tables. User access to specific server resources is subject to ACL security.

You can search for the following topics in the document:
- Configuring Secure Sockets Communication
- Configuring Server Domains
- Enabling FIPS 140-2 Compliance for SPD Server
- Encrypting SPD Engine Data Sets
- Managing Users and Passwords
- Security
SAS Social Network Analysis Server 6.2: Administration Guide
Provides information about using SAS Management Console to set up and administer the solution. It describes parameters in the Configuration Manager, database tables, and configuration files that control aspects of the user interface.

It also provides information about enabling direct access to an alert when a user logs in and about launching external applications from inside the solution. Examples of stored processes code are also included.

Note: This is a secure document that is available on a password-protected site.

You can search for the following topics in the document:
- Direct Alert Details Access
- Configuring External Applications

SAS Social Network Analysis Server 6.2: Installation and Configuration Guide
Contains information about creating the SAS Social Network Analysis Server user accounts and setting up investigator accounts.

Note: This is a secure document that is available on a password-protected site.

SAS Time Series Studio 15.1: Administrator's Guide
Provides information about how to specify security permissions for users and groups. It discusses layers of security that are divided into capabilities, metadata permissions, project ownership and sharing, and file system permissions. It also provides information about creating operating system accounts for product administrators and users. For post-installation, there is information about managing roles and capabilities and creating operating system accounts on UNIX platforms.

SAS Visual Analytics 7.5: Installation and Configuration Guide (Distributed SAS LASR)
Provides information about configuring users and groups. It also provides information about how to deploy and authenticate Visual Analytics interactivity. You can search for the following topics in the document:
- Create SAS Users and Groups
- Deploying the Servers and Middle Tier
- Defining Groups
- Defining User Accounts

SAS Visual Analytics 7.5: Administration Guide
Provides information about security that is specific to SAS Visual Analytics.

SAS Visual Analytics App
Describes security features available in the app and features that affect the security of reports the users might view in the app. App is free and available for iOS, Android, and Windows 10.


Provides information about how to configure authentication, authorization, encryption, how to enhance encryption, and how to encrypt the key password for TLS. You can search for the following topic in the document:
- Configure Security
SAS Visual Scenario Designer 6.3: Administrator’s Guide

Includes instructions about how to use SAS Management Console to manage servers and add users. It also includes details about host account privilege information for accounts that load data, import data, or start or stop (or both) SAS LASR Analytic Server. It includes information about how to generate executable *.sas files from a SAS Visual Scenario Designer deployment using a macro. It also provides details about how to load client-specific data using scripts (provided by SAS) and how to access the PostgreSQL database.

Note: This is a secure document that is available on a password-protected site.

You can search for the following topics in the document:
- Getting Started
- Batch Server Deployment
- Post-installation Considerations

SAS/ACCESS 9.4 for Nonrelational Databases: Reference

Contains information about authentication and security when accessing nonrelational DBMSs. Individual database information includes options that pertain to security settings. You can search for the following topics in the document:
- LIBNAME Statement Specifics for MongoDB
- Security Considerations for the PI System

SAS/ACCESS 9.4 for Relational Databases: Reference

Contains data integrity and security information including details about DBMS security and SAS security. The individual database information includes options that pertain to security settings.

You can search for the following topics in the document:
- Data Integrity and Security
- The DBMS-specific reference includes the following topics:
  - LIBNAME Statement Specifics for Amazon Redshift and Encryption with Amazon Redshift
  - LIBNAME Statement Specifics for Impala
  - LIBNAME Statement Specifics for MySQL
  - LIBNAME Statement Specifics for PostgreSQL
  - LIBNAME Statement Specifics for SAP HANA
  - LIBNAME Statement Specifics for Snowflake
  - Security: Authentication with Teradata

SAS/CONNECT 9.4 User’s Guide

Describes how to encrypt data in server and client transfers, how to set up network security, how to start the SAS/CONNECT spawner securely, and how to authenticate the client. It also contains all the spawner start-up encryption options and examples of maintaining the SAS server and SAS/CONNECT spawner and using encryption.

Contains information about configuring SAS/CONNECT to use a firewall. It also includes details about client authentication and passwords, and locked-down SAS sessions. It also contains details about SAS system options for connecting to metadata servers and SIGNON and RSUBMIT options for passwords and authentication domains that are used to connect to the server.

SAS/CONNECT Spawner encrypts the client's user ID and password during sign-on by default. There are also security options that can be specified for TLS encryption.

You can search for the following topics in the document:
Data Security for SAS/CONNECT or SAS/SHARE Servers
UNIX: TCP/IP Access Method
Configure SAS/CONNECT for Use with a Firewall
Enhanced Password Support on z/OS
Locked-Down SAS Sessions
Specify Encryption Options for Data Security
Benefits of Using a Spawner to Sign On to a Server
Enable Encryption for Spawner Sign-ons
Server Security Using Client Authentication
Use SSPI to Access a Secured Server
Passwords in a Script File

SAS/IntrNet 9.4: Application Dispatcher
Provides information about security for the Application Broker, web server, Application Server, and programs, as well as information about restricting access to data sources. You can search for the following topics in the document:
Application Dispatcher Security
Configuration File Directives
PROC APPSRV Statement
Specifying HTTP Methods
Using DebugMask and ServiceDebugMask

Using SAS Risk Work Groups
Explains how administrators can use risk work groups to organize users into logical groupings that can access objects and data across SAS risk solutions.

Note: This is a secure document that is available on a password-protected site.