SAS® Viya® 3.5: Overview

Elements of SAS Viya

Introduction

This section provides a concise summary for new administrators.

Here are related topics:

- To get started with SAS Viya administration, see SAS Viya Administration: Getting Started.
- To learn about benefits of SAS Viya, see SAS Viya on the SAS website.

Key Components

Here are software components that might be of particular interest to administrators.

The analytics engine to SAS Viya	*SAS Cloud Analytic Services: Fundamentals*
A modular set of supporting services	*SAS Viya Administration: General Servers and Services*
A web application for basic administration	*SAS Viya Administration: Using CAS Server Monitor*
A web application for enterprise administration	*SAS Viya Administration: Using SAS Environment Manager*
A web application for writing and submitting code	*Getting Started with Programming in SAS Studio*
A web application for visual reporting, exploration, and modeling	*SAS Visual Analytics: Overview*
Multiple application programming interfaces	http://developer.sas.com

For information about other components, search the SAS Viya administration documentation.

Cumulative Functionality

Among some of the products on SAS Viya, available functionality is cumulative.

■ SAS Visual Analytics provides baseline functionality, including reporting and basic analytics.

■ SAS Visual Statistics provides an additional set of advanced analytic functions.

■ SAS Visual Data Mining and Machine Learning provides a second additional set of advanced analytic functions.

Note: All of the preceding products offer both programming and visual interfaces.

Selective Deployment (Optional)

By default, all of your software is deployed. As a convenience for special circumstances, it is possible to deploy only a subset of components. A programming-only deployment excludes general services and visual interfaces. For example, a programming-only deployment of SAS Visual Analytics does not include the SAS Visual Analytics web application.

Note: SAS supplies two versions of SAS Studio: SAS Studio 5.2 (Basic) and SAS Studio 5.2 (Enterprise).. SAS Viya programming-only deployments use SAS Studio 5.2 (Basic). For a comparison of the two SAS Studio versions, see "SAS Studio 5.2" in *What's New in SAS 9.4 and SAS Viya*.
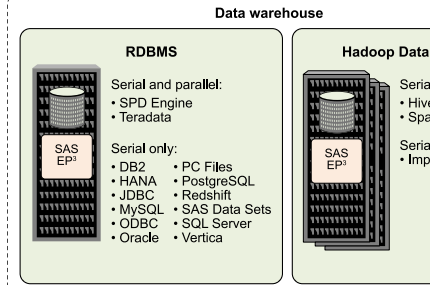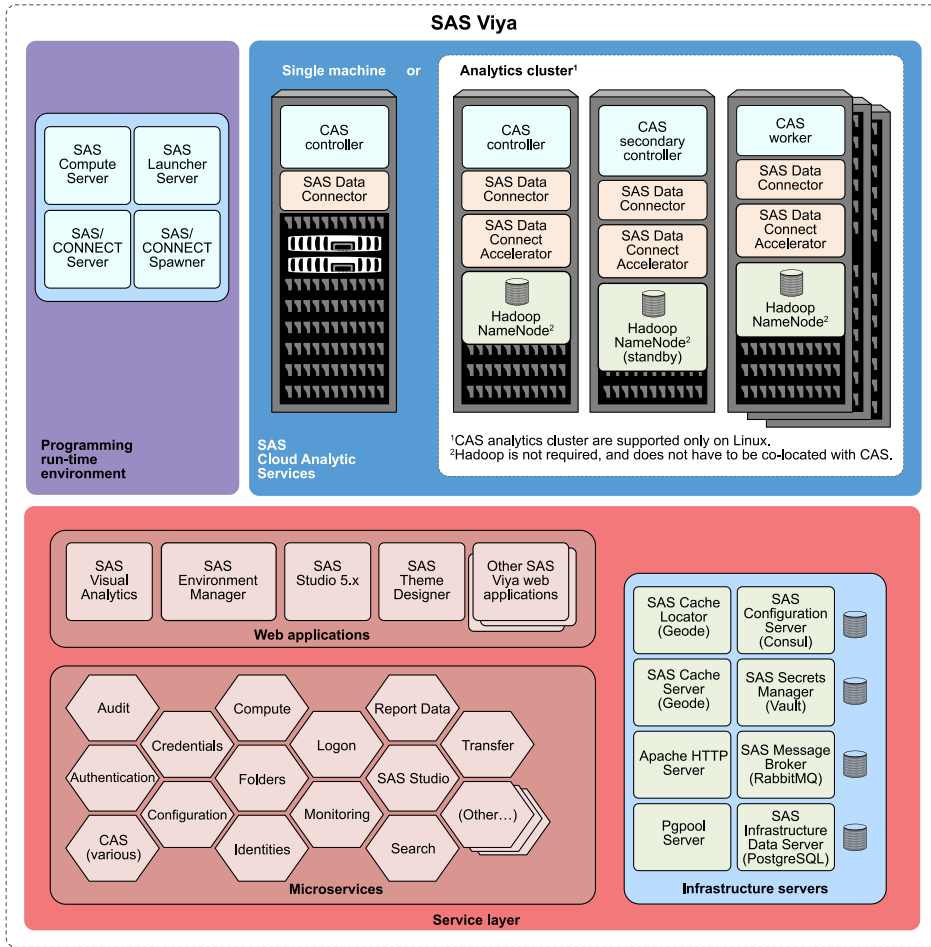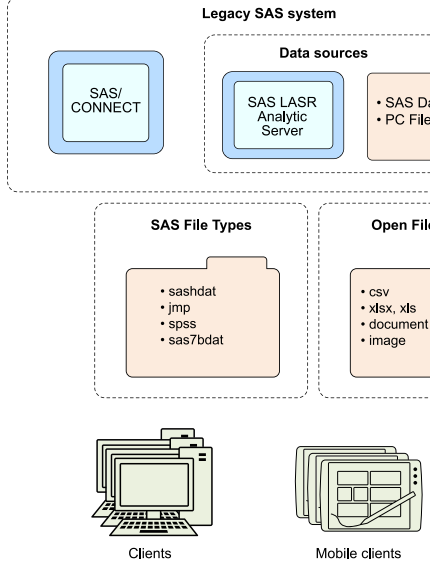
Diagrams by Deployment Type

Full Deployment (Native Operating Systems)

The following diagram shows the components in a SAS Viya full deployment:

SAS Viya

Single machine or **Analytics cluster**[1]

Programming run-time environment

SAS Compute Server | SAS Launcher Server
SAS/CONNECT Server | SAS/CONNECT Spawner

SAS Cloud Analytic Services

CAS controller
SAS Data Connector

CAS controller
SAS Data Connector
SAS Data Connect Accelerator
Hadoop NameNode[2]

CAS secondary controller
SAS Data Connector
SAS Data Connect Accelerator
Hadoop NameNode[2] (standby)

CAS worker
SAS Data Connector
SAS Data Connect Accelerator
Hadoop NameNode[2]

[1]CAS analytics cluster are supported only on Linux.
[2]Hadoop is not required, and does not have to be co-located with CAS.

Service layer

Web applications

SAS Visual Analytics | SAS Environment Manager | SAS Studio 5.x | SAS Theme Designer | Other SAS Viya web applications

Microservices

Audit | Compute | Report Data
Credentials | Logon | Transfer
Authentication | Folders | SAS Studio
Configuration | Monitoring | (Other...)
CAS (various) | Identities | Search

Infrastructure servers

SAS Cache Locator (Geode) | SAS Configuration Server (Consul)
SAS Cache Server (Geode) | SAS Secrets Manager (Vault)
Apache HTTP Server | SAS Message Broker (RabbitMQ)
Pgpool Server | SAS Infrastructure Data Server (PostgreSQL)

Data warehouse

RDBMS

SAS EP[3]

Serial and parallel:
• SPD Engine
• Teradata

Serial only:
• DB2 • PC Files
• HANA • PostgreSQL
• JDBC • Redshift
• MySQL • SAS Data Sets
• ODBC • SQL Server
• Oracle • Vertica

Hadoop Data

SAS EP[3]

Seria...
• Hiv...
• Spa...

Seria...
• Imp...

[3]SAS Embedded Process is not required for serial connections.

Legacy SAS system

SAS/CONNECT

Data sources

SAS LASR Analytic Server

• SAS Da...
• PC File...

SAS File Types

• sashdat
• jmp
• spss
• sas7bdat

Open File...

• csv
• xlsx, xls
• document...
• image

Clients

Mobile clients

Programming-Only Deployment (Native Operating Systems)

The following diagram shows the components in a SAS Viya programming-only deployment:
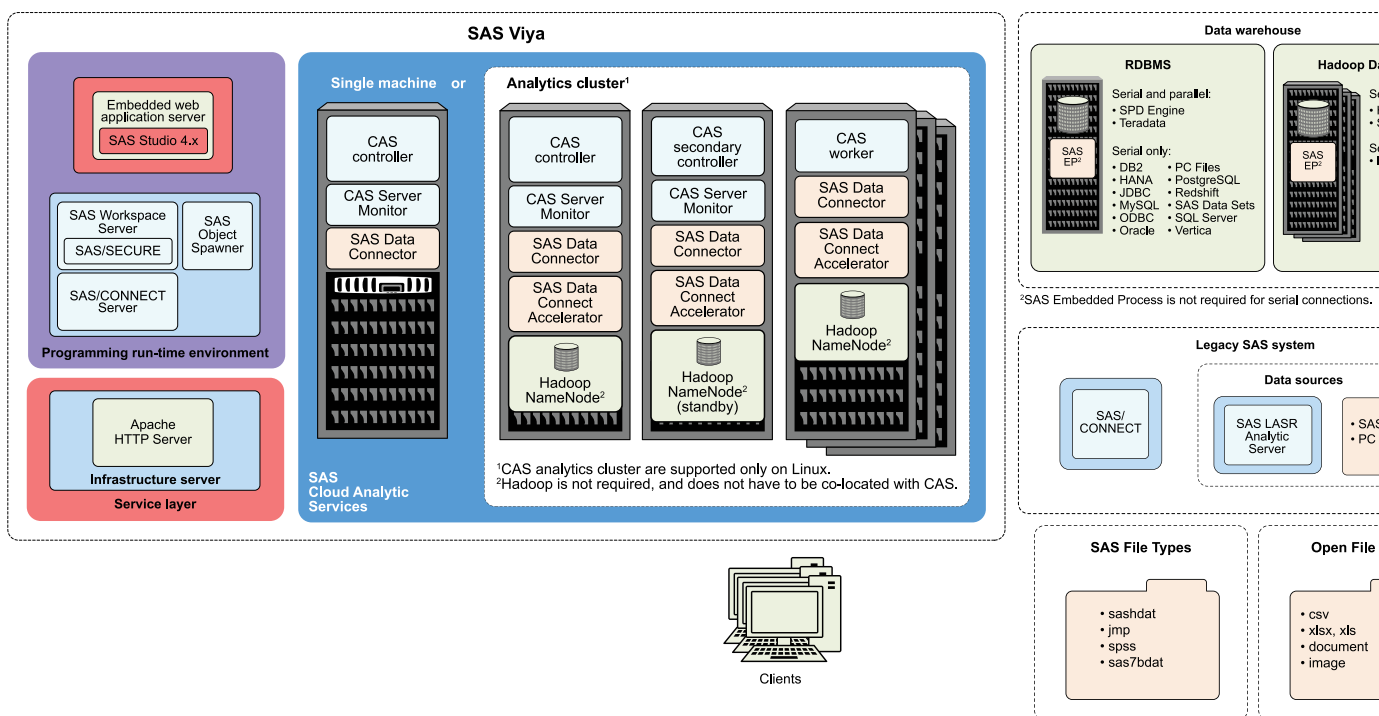
Security in SAS Viya

Authentication

Authentication is the aspect of security that verifies the identity of a user or service account.

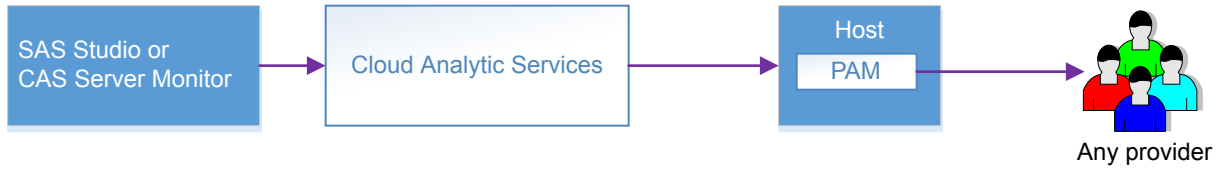When you sign in, one of the following authentication patterns is used:

Pattern	Description	Usage
Host authentication	Requests are sent to the appropriate host and processed by any authentication mechanism supported by that host. Programming-only deployments use this pattern exclusively. Other deployments use dual authentication for access to CAS from SAS Studio 5.2 (Basic). **Note:** You can configure the host to use pluggable authentication modules (PAM). SAS provides starter PAM	When you sign in to SAS Studio 5.2 (Basic) from a URL that is similar to https://*reverse-proxy-server*/SASStudio/, you are prompted for a user ID and password. The associated object spawner asks its host (which is also the host of the SAS Studio 5.2 (Basic) web application) to validate your credentials. That validation enables the object spawner to launch a workspace server for you. When you access CAS from SAS Studio 5.2 (Basic), you must authenticate to the host of the target CAS server.

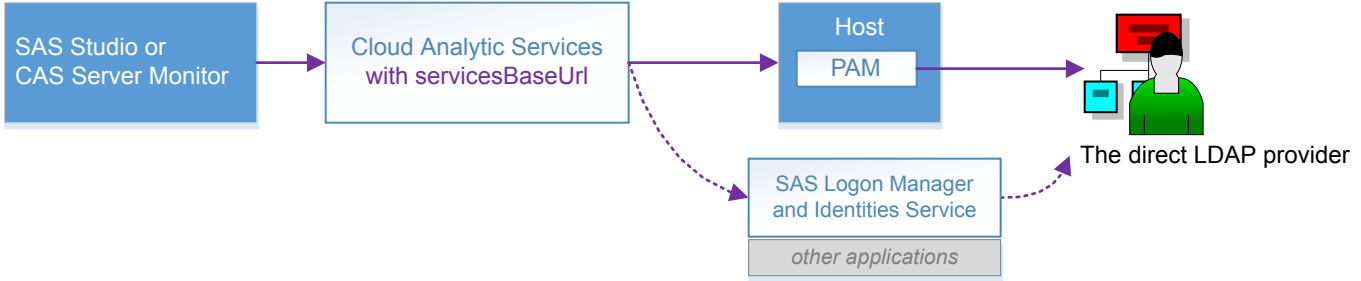| Pattern	Description	Usage
	configuration files for CAS and SAS Studio 5.2 (Basic). You can create an authinfo file for use with PAM in command-line access and batch processing programs to CAS. Credentials for the user ID that runs the program are supplied from the authinfo file.	When you sign in to CAS Server Monitor, you must authenticate to the host of the target CAS server.
Direct LDAP authentication	Requests are sent to and processed by your designated direct LDAP provider, unless you configure front-end single sign-on using Kerberos, Open Authorization (OAuth), or Security Assertion Markup Language (SAML). Kerberos, OAuth, and SAML are alternate mechanisms for identity verification by the logon service, not alternate sources of user and group information for the identities service. Note: User and group information is always obtained from your designated direct LDAP provider.	SAS Drive enables you to access the visual interfaces, for example, SAS Visual Analytics or SAS Environment Manager. When you sign in to SAS Drive from a URL that is similar to https://*reverse-proxy-server*/SASDrive/, a user ID and password are required to authenticate to SAS Logon Manager, using this pattern. Before you can submit a command-line request to a general service (for example, the backup service or the transfer service), you must authenticate using this pattern.
Host and direct LDAP authentication	Requests are authenticated using both host authentication and direct LDAP authentication. If the servicesBaseUrl option is specified, CAS requires dual authentication. To facilitate this pattern, use one of these approaches: ■ Ensure that all requests are ultimately processed by the same authentication provider. For example, configure the SAS Studio 5.2 (Enterprise) and CAS hosts to use the same LDAP provider that is designated for direct LDAP authentication requests in your deployment. ■ Ensure that each affected user has a single set of credentials that are valid for all applicable authentication providers.	In a full deployment, dual authentication occurs for access to CAS from SAS Studio 5.2 (Enterprise). In a programming-only deployment, CAS Server Monitor provides a web-based interface for administration. Note: When you access CAS from a web application such as SAS Visual Analytics or SAS Environment Manager, your OAuth token is validated.

The following high-level conceptual drawings illustrate key points from the preceding table:

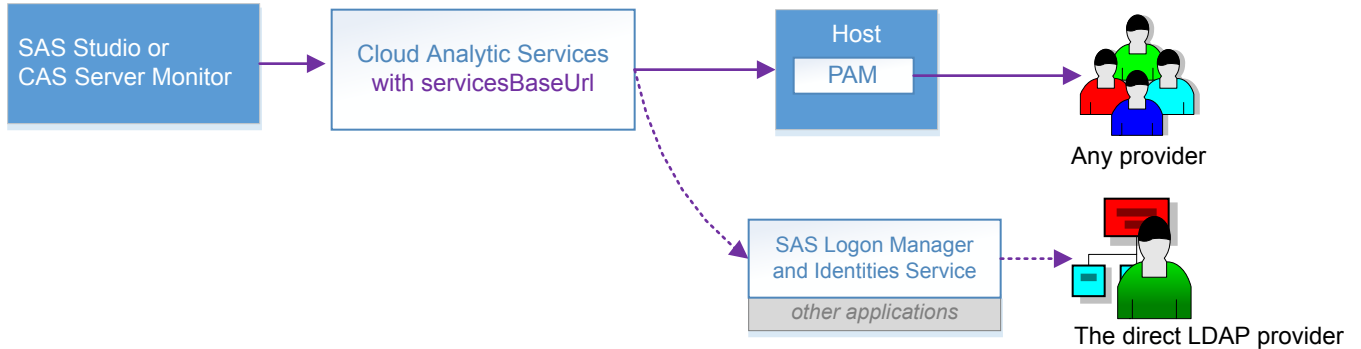**Figure 1** *Authentication from SAS Studio or CAS Server Monitor to CAS*
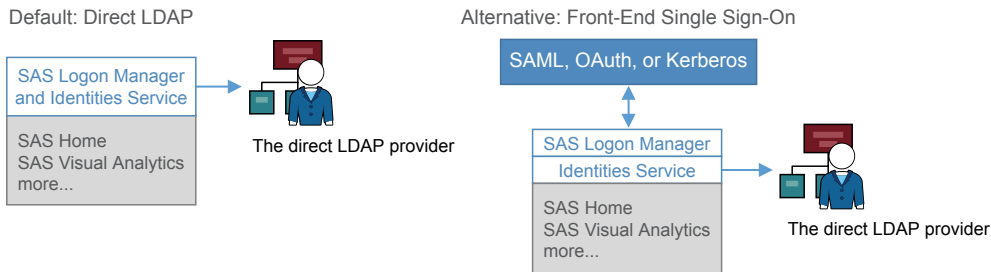
Host Authentication

SAS Studio or CAS Server Monitor → Cloud Analytic Services → Host / PAM → Any provider

Dual Authentication: Shared Provider

SAS Studio or CAS Server Monitor → Cloud Analytic Services with servicesBaseUrl → Host / PAM → The direct LDAP provider

SAS Logon Manager and Identities Service
other applications

Dual Authentication: Different Providers

SAS Studio or CAS Server Monitor → Cloud Analytic Services with servicesBaseUrl → Host / PAM → Any provider

SAS Logon Manager and Identities Service
other applications → The direct LDAP provider

Figure 2 *Authentication from Other Applications*

Default: Direct LDAP

SAS Logon Manager and Identities Service
SAS Home
SAS Visual Analytics
more... → The direct LDAP provider

Alternative: Front-End Single Sign-On

SAML, OAuth, or Kerberos

SAS Logon Manager
Identities Service
SAS Home
SAS Visual Analytics
more... → The direct LDAP provider

After you sign in, you have seamless access to SAS Viya and, in some contexts, to external data sources.

For more information, see the following documents:

SAS Viya Administration: Authentication

SAS Viya Administration: Identity Management

SAS Viya Administration: External Credentials

Authorization

Authorization is the aspect of security that determines which resources are available to which users. The SAS Viya authorization layer consists of two authorization systems:

- CAS authorization system
- general authorization system

Each system uses a distinct model to protect a distinct class of resources. The general authorization system is not applicable in a programming-only deployment.

Initial and default access are restrictive:

- Any access that is not granted is implicitly disallowed.
- Predefined objects are protected by predefined rules or access controls.
- Only members of special groups or roles have access to privileged administrative functionality.
- Access to objects that users add is managed by inheritance, other influencing rules, and any direct settings.
- Regular users have limited Write access. They can write to their personal folder, the shared Public folder, and the shared Public caslib.

For more information, see the following documents:

SAS Viya Administration: Orientation to Authorization

SAS® Viya Administration: CAS Authorization

SAS Viya Administration: General Authorization

SAS Viya Administration: Identity Management

Encryption

Encryption is the aspect of security that protects data by converting it into an unintelligible form in transmission or in storage.

For data in motion,

- In a SAS Viya full deployment, TLS security is provided by default and follows the highest standards. At installation SAS Viya provides self-signed certificates to provide HTTPS access to SAS Drive out of the box. You can increase the encryption strength and coverage by completing additional configuration.

■ In a SAS Viya Linux programming-only deployment and a Windows deployment, security artifacts are provided to configure TLS security. You can increase the encryption strength and coverage by completing additional configuration.

For data at rest in a new deployment, encryption is not automatically enabled. You can configure encryption of data that is added to PATH, HDFS, and DNFS caslibs.

For more information, see the following documents:

Encryption in SAS Viya: Data in Motion

Encryption in SAS Viya: Data at Rest

Web Security

Web security is the aspect of security that deals with securing against certain types of attacks on web applications and utilizing the security features that are available in modern web browsers.

SAS Viya provides properties that are configured, by default, to protect against the web security risks that are listed below. You can disable or change the properties, based on your environment. For example, you might have to configure Cross-Origin Resource Sharing (CORS) to allow origins in your company's domain. This allows SAS web pages to be included in other web pages inside your company's network.

For more information about the SAS Viya configuration properties, see the following:

Property	Description	Default Settings
Cross-Origin Resource Sharing	Technique for relaxing the browser same-origin policy, allowing Javascript on a web page to consume a REST API served from a different origin.	The following cross-origin requests are configured: ■ User credentials are used ■ All HTTP headers are allowed ■ All HTTP methods are allowed ■ Same origins are allowed
Cross-Site Request Forgery (CSRF)	Prevents attacks that force a user to execute unwanted actions on a web application in which they are currently authenticated.	The following options are configured: ■ All requests that use an authenticated HTTP session, except GET and HEAD requests, must pass a CSRF token specified by the server.

Property	Description	Default Settings
		■ Referrers internal to the deployment are allowed
X-Frame-Options	Avoids clickjacking attacks by making sure that your content is not embedded in other sites.	Same origin
Content-Security-Policy	Exposes and reduces the risk of data injection and cross-site scripting (XSS) attacks.	default-src 'self'; script-src 'self' 'unsafe-inline' 'unsafe-eval'; img-src 'self' *.sas.com blob: data:; style-src 'self' 'unsafe-inline'; child-src 'self' blob: data: mailto:;
X-Content-Type-Options	Prevents the browser from interpreting files as something other than what is declared by the content type in the HTTP headers (content sniffing).	nosniff
Note: The protections brought by this property are largely superseded by a strong content security policy. It is recommended to use the content-security-policy instead. X-XSS-Protection	Stops web browser from loading pages when XSS attacks are detected.	1; mode=block

For information about these web attacks, see the following OWASP pages:

■ Attacks

■ OWASP Secure Headers Project

■ Cross-Site Request Forgery (CSRF)

■ Cross-Origin Resource Sharing

SAS 9 and SAS Viya

Summary

SAS 9 customers continue to benefit from their investment in SAS 9 as they begin to make use of SAS Viya functionality and features. From within familiar SAS 9 interfaces, projects, and code, customers can access the performance enhancements that SAS Viya provides.

- On most hosts, SAS 9.4M5 is tightly integrated with SAS Viya. See SAS 9.4M5 Integration with SAS Viya in *What's New in Base SAS: Details*. (The exceptions are z/OS and 32–bit Windows.)

- All releases of SAS can use SAS/CONNECT as a bridge to SAS Viya. See the appendix Sharing Data Between SAS 9 and SAS Viya using SAS/CONNECT in *SAS/CONNECT for SAS Viya User's Guide*.

- SAS Viya visual web applications share a single sign-on and logout with the SAS 9 environment.

Here are some of the methods for accessing SAS 9 data from SAS Viya:

- In SAS Visual Analytics, use self-service import. See SAS Data Explorer: User's Guide.

- In SAS Environment Manager, interactively load data. See Data Administration: How to (SAS Environment Manager) in *SAS Viya Administration: Data*.

- In SAS Enterprise Guide or SAS Add-In for Microsoft Office (7.13 or later), move data from SAS 9 to CAS. See the topic "Configure Your Environment to Use the Upload to CAS Task" in the SAS Enterprise Guide or SAS Add-In for Microsoft Office chapter in *SAS Intelligence Platform: Desktop Application Administration*.

- Write code to load data. See Load Data to a Caslib in *An Introduction to SAS Viya Programming*.

- If a more seamless method is not available, use SAS/CONNECT for SAS 9 and SAS Viya to move and share data. See the appendix Sharing Data Between SAS 9 and SAS Viya using SAS/CONNECT in *SAS/CONNECT for SAS Viya User's Guide*.

Note: Not all deployments and releases include all products and support all methods.

Note: Your site must license and install SAS Viya to access SAS Viya functionality. By default, when you order SAS Viya, you receive SAS Visual Analytics. All analytical procedures are separate licenses: SAS Econometrics Procedures, SAS Optimization Procedures, SAS Forecasting Procedures, SAS Visual Data Mining and Machine Learning Procedures, SAS Statistics Procedures, and SAS Viya Procedures.

Considerations: Interacting with SAS 9 Data

Manage User-Defined Formats

If you access SAS 9 data from SAS Viya, you must make any user-defined formats available to your CAS session. See SAS Cloud Analytic Services: User-Defined Formats.

Considerations: Accessing CAS from SAS 9.4M5

IMPORTANT You cannot connect to the SAS 9.4 Metadata Server from SAS Viya 3.5.

Find CAS

If a SAS 9.4M5 client session cannot find CAS, make information about the host and port of the CAS server available. For example, add the following line to your SAS Application Server sasv9_usermods.cfg or appserver_autoexec_usermods.sas file:

```
CASHOST=("primary-controller-host-name" <"backup-controller-host-name">) CASPORT=port;
```

Here is an example with a CAS backup controller:

```
CASHOST=("mysrv01" "mysrv02") CASPORT=5570;
```

Here is an example without a CAS backup controller:

```
CASHOST=("mysrv01") CASPORT=5570;
```

For more information, see CASHOST= System Option.

Authenticate to CAS

If a SAS 9.4M5 client session cannot authenticate to CAS, create an authinfo file, store CAS credentials in the SAS 9 metadata, or use a different authentication mechanism. See *SAS Viya Administration: Authentication*.

Conform to CAS Encryption Requirements

If a SAS 9.4M5 client session does not meet the encryption standards of the CAS server, make an appropriate certificate available. See "Configure SAS 9.4 Clients to Work with SAS Viya" in *Encryption in SAS Viya: Data in Motion*.

SAS Visual Analytics Administration

Tasks

SAS Viya Administration documentation is applicable to SAS Visual Analytics. Links to specific SAS Visual Analytics topics that deserve special attention are included here:

- Promoting data and report content
- Granting guest access
- Managing user-defined formats
- Loading geographic polygon data as a CAS table
- Loading data for reports
- Making data available to CAS
- Using the reports alert service

- Using the report data service
- Using the report packages service
- Using the report renderer service
- Understanding identity management concepts
- Modifying rules that affect access to functionality
- Using the Maps service to obtain polygon information

Samples

Sample data and reports are provided to help you get started.

The sample data is located by default in the `/opt/sas/viya/config/cas/default/samples/`. Access it on the **Data Sources** tab of the Open Data Source window. Double-click on cas-shared-default (or the name of your default CAS server), and double-click on **Samples**.

The six sample data sets are:

COSTCHANGE.sashdat
 provides historical data on vehicle maintenance, to monitor changes in costs

PROMO_EFFECTIVENESS_X_EFFECTS_2.sashdat
 provides data on the impact of a 25% discount on dog food sales

RAND_RETAILDEMO.sashdat
 provides retail sales information for customer purchases across multiple sales departments and stores

SW_LAKE_RT_SENSOR_WATERQUALITY.sashdat
 provides a wide range of water-quality metrics for lake water

WARRANTY_CLAIMS_0117.sashdat
 provides data on warranty claims for car repairs

WATER_CLUSTER.sashdat
 provides data on home water consumption

The sample reports are based on some of the sample data. Access these reports by selecting **Open** from the ⋮ Menu, and expand: **Products ⇨ SAS Visual Analytics ⇨ Samples**. The three sample reports are:

Retail Insights
 report generated for the RAND_RETAILDEMO.sashdat and PROMO_EFFECTIVENESS_X_EFFECTS_2.sashdat sample data

Warranty Analysis
 report generated for the COSTCHANGE.sashdat and WARRANTY_CLAIMS_0117.sashdat sample data

Water Consumption and Monitoring
 report generated for the SW_LAKE_RT_SENSOR_WATERQUALITY.sashdat and WATER_CLUSTER.sashdat sample data

SAS Studio Administration

Overview

SAS system administrators must balance organizational security expectations with the features and flexibility that SAS Studio brings to programmers, data scientists, and business analysts.

IT administrators and business sponsors should evaluate the risks and benefits that are associated with providing the SAS Studio programming tool to authorized and trusted users. Often it is this programmatic access through a web browser that prompts concerns about application security. SAS provides options that administrators can use to implement security protections that are appropriate for their organization's risk tolerance.

SAS Studio is a programming tool that is delivered as a web application. Programmers and business analysts use SAS Studio to develop customized analytic applications that use the full power of the SAS programming language. SAS Studio enables authorized programmers and business analysts to access the host system in support of their programming work. This support includes the ability to read and write from file systems, save their work locally, import code, analyze data sets, and programmatically access file systems, network drives, and specific machines.

Security Reviews and Updates

As part of the software development and release cycle, SAS performs a variety of security scans and other tests. Potential security issues are evaluated and addressed before newer versions of SAS Studio are released.

Updates and new releases of SAS software might include security updates in addition to product fixes and enhancements. SAS encourages administrators to keep the software at their site up-to-date.

Security Options Specific to SAS Studio

Disabling Upload and Download Actions

Setting the configuration properties `allowUpload` and `allowDownload` to `false` disables the icons for upload and download operations in server files and folders within the SAS Studio user interface.

These SAS Studio configuration properties do not prevent browsers or code from performing upload or download tasks. Instead, these properties limit the ability to upload and download code and data only within the context of SAS Studio functions.

Specifying File Navigation Options

SAS administrators can use file navigation options to set the initial files and folders that are displayed in SAS Studio. By setting a starting point, the administrator defines the top level of the directory structure that users can see; they can navigate down the tree, but not up. Users can create shortcuts that provide a starting point for file system navigation that proceeds lower in the structure, but not higher.

Specifying Session Time-Outs

You can use session time-out settings to reduce potential exposure from sessions that are left logged on when they are not in use.

- For the SAS Compute Server, the administrator can set the `sessionInactiveTimeout` attribute.

- The `sas.studio.abandonedSessionTimeout` property sets the time-out for abandoned sessions in SAS Studio and on the SAS Compute Server. The default value is 5 minutes.

Configure General SAS Viya Security Options

NOXCMD Option

By default, the `-noxcmd` attribute is set for the Compute Server so that external commands are disabled. When `-noxcmd` is set, the following functions are disabled:

- the PIPE device type in the FILENAME statement

- the CALL SYSTEM routine

- the %SYSEXEC macro

- any facility that SAS uses to execute a shell-level command

To enable external commands, an administrator can enable the `allowXCMD` attribute in SAS Environment Manager.

LOCKDOWN Statement

In multi-tenant environments, use the SAS LOCKDOWN statement and system option to limit file system access and to limit some SAS language features. Some sites might use LOCKDOWN to help prevent users from accessing system files, including executable files. The LOCKDOWN feature can be used in addition to implementing the SAS options NOXCMD and file system controls in the operating system.

Note: The LOCKDOWN system option applies to all SAS products and solutions that are running in your SAS deployment. You should review your complete SAS deployment when evaluating this option. LOCKDOWN must be enabled in multi-tenant deployments.

When using the LOCKDOWN feature, it is strongly recommended that you follow these best practices:

- Ensure that the physical resources on the locked-down server are protected by appropriate operating-system permissions (also known as environment hardening). The LOCKDOWN feature is not intended to replace operating-system protections.

- Ensure that the NOXCMD system option has also been enabled on any servers where LOCKDOWN is enabled.

- Understand the scope of SAS language commands and file-system commands that are restricted when LOCKDOWN is used. Consult with SAS programmers and analysts to understand the impact of these restrictions in achieving business goals.

For more information about the LOCKDOWN system option and the LOCKDOWN statement, see "LOCKDOWN System Option" in *SAS Viya Administration: Programming Run-Time Servers*.

Passing an HTTP GET Request through SAS Studio

A malicious insider who has logon credentials for SAS Studio, and who has access to the underlying file system, might be able to retrieve sensitive files in a SAS Viya deployment that lacks system-based security hardening controls.

SAS Studio and the SAS Compute Server present a few unique security considerations for SAS administrators:

- The GET request is considered core to the functioning of SAS Studio. Using this command, users can access only those files that they have operating-system permission to access.

- In order for the GET request URL to resolve in a browser, the user must have already logged on to SAS Studio to obtain a valid token.

- The system administrator determines which files are accessible through an HTTP GET request by applying file system permissions for each user. SAS Studio does not override file system security.

Note: Access to SAS content is controlled by the OAuth token that is obtained from SAS Logon Manager and by your authorization rules.