Encryption in SAS® Viya™ 3.2: Data at Rest

Encryption for Data at Rest: Overview

This document provides instructions for administrative tasks for encrypting files in the SASHDAT format and for encrypting tables in caslibs. This document assumes that you are familiar with the data and caslib concepts that are explained in *SAS Cloud Analytic Services: Fundamentals*.

CAS supports encryption as an option for tables in caslibs. SAS Viya uses the Advanced Encryption Standard (AES) with 256-bit keys to encrypt data at rest. The encryption applies to source tables, not to tables resident in memory. Encryption can be applied to individual tables or to all tables in a library. Each table can have a unique encryption key, or a single key can be set at the library level in order to have a shared key for all tables in the library.

Administrators for SAS Viya deployments can choose to encrypt specific data that is "at rest" within the environment. Specifically, you can encrypt files in the SASHDAT format, and you can encrypt tables in caslibs using AES encryption. You can specify encryption for a caslib only when it is created. To change it you must re-create the caslib.

Note: Cloud Foundry supports these caslib types: Path based, DNFS, HDFS, LASR, and Hadoop.

Use the method that best meets your needs. Here are supported interfaces:

- To manage encryption domains interactively, use the SAS Environment Manager tasks.
- To programmatically encrypt data files, use the CASLIB statement tasks.

How To (SAS Environment Manager)

Introduction

The SAS Environment Manager Security Domains area makes a stored credential (an encryption key) available to designated identities to facilitate loading of encrypted files. By default, when you are creating a new caslib, encrypting that caslib is disabled. If you choose to enable encryption, this can be done by creating an encryption domain, and then using that domain to create a CAS library for DBMS data.

In the Domain area, you can perform the following tasks.

2

- Create a new encryption domain
- Add users or group identities to the security domain
- Create an encryption key (passphrase)

You must be a member of the *SAS Administrators* group and assume groups when you log in to the SAS Environment Manager in order to create and manage Domains.

In the SAS Environment Data area, you can create and manage caslibs. By default, caslibs are not encrypted. You can encrypt the tables in your caslibs by associating the caslibs with an encryption domain.

CAUTION! Be sure to keep a separate record of your encryption key Once an encrypted caslib is created, it is not possible to change the encryption key setting or change the domain. Once created, the encryption key value cannot be retrieved through the software. If the caslib is deleted, the tables remain encrypted. You can define a new caslib using the same path and domain with the same encryption key.

Note: When the encrypted data is loaded into the CAS Server, it is decrypted at load time, and only normal CAS authorizations apply to accessing the loaded data.

The following instructions explain how to encrypt the tables in your caslibs using SAS Environment Manager.

Navigation

The Domains area is available only if you are a member of the *SAS Administrators* group.

From the side menu (☰), under **SAS Environment Manager**, select **Security** ⇨ **Domains** .

There are two views that can be selected from the **Domains** page. From the **View** drop-down list, you can select one of the following views:

Domains
lists all domains that you can see. This is the default view. There are three types of Domains: Authentication, Connection, and Encryption. You can create a new encryption domain.

When you create an encryption domain, you cannot delete that domain. SAS Viya uses the Advanced Encryption Standard (AES) with 256-bit keys to encrypt data at rest.

Credentials
Credentials are not used by Encryption Domains. For information, see *SAS Viya Administration: External Credentials*

.

Manage Encryption Domains

SAS Viya uses the Advanced Encryption Standard (AES) with 256-bit keys to encrypt data at rest.

Create a New Encryption Domain

1 In the **Domains** view, click .

2 In the New Domain window, specify general settings as follows:

ID	Create an ID name. Enter a unique ID for your encryption domain.
Type	Select the type of domain. There are three domain types, Encryption, Authentication, and Connection. Select **Encryption** from the list of available domains

Identities	From the Select Identities Window, you can select from users, groups, and custom groups. See below for how to add an identity.
Encryption key	Encryption passphrase or key
Confirm encryption key	Enter the same passphrase as above.
Description	Add a description.

For additional information about identities, from the New Domain window, click ⓘ.

3 To add identities, from the New Domain window, click +.

To add an Identities member, from the Select Identities window, perform the following tasks.

a In the left pane of the Edit Members window, select **Users**, **Groups**, or **Custom Groups** from the drop-down box.

Note: A best practice is to use a custom group here. Then you can simply add additional users to this custom group as needed to grant access to use the encryption key to load encrypted files.

b Move the user, group, or custom group to the right. Click  .

c Click **OK** to save the information.

4 After you have entered all of the parameter settings needed, click **Save**.

View Properties of an Encryption Domain

1 In the **Domains** view, select an ID row for Type Encryption.

2 Right-click, and select **Properties**. Or select  from the taskbar. From the **Domain Properties** window, the ID, Type, Description, Date created, Date modified, who created the domain, and who modified the domain is displayed.

3 Click **close**.

Edit an Encryption Domain

If you are a member of the domain, you can add identities to and remove identities (users, groups, and custom groups) from an existing Encryption Domain and change the description. You cannot change the type of domain.

From the Select Identities window, perform the following tasks.

1 In the **Domains** view, select a domain ID.

2 Right-click, and select **Edit**. Or select  from the taskbar.

3 To add or remove an Identity, from the Edit Domain window, click +.

From the Select Identities window, move the user, group, or custom group to the right pane to add an identity.

a In the left pane of the Edit Members window, select **Users**, **Groups**, or **Custom Groups** from the drop-down menu.

b Move the user, group, or custom group to the right. Click  .

4

c Click **OK** to save the information.

From the Select Identities window, move the user, group, or custom group to the left pane to remove an identity.

a In the right pane of the Edit Members window, select **Users**, **Groups**, or **Custom Groups** from the drop-down menu.

b Move the user, group, or custom group to the left. Click  .

c Click **OK** to save the information.

4 For additional information about identities, click  .

5 Edit the **Description** of the Encryption Domain.

6 After you have entered all of the parameter settings needed, click **Save**.

Delete Encryption Domains

Encryption domains cannot be deleted in the current release. If you try to delete an Encryption domain, you will receive the following message: “Encryption domains cannot be deleted in the current release”.

Manage Caslibs

For additional information, see “Manage Caslibs” in *SAS Viya Administration: Data*.

Create Caslibs with Encryption Enabled

If you want to encrypt the tables in a caslib, you must turn on encryption when you create the caslib. You cannot edit an existing caslib and encrypt it.

1 From the side menu (), under **SAS Environment Manager**, select **Data** , and select **Libraries** from the drop-down view.

In the **Libraries** view, click  .

2 In the New CAS Library window, specify general settings as follows:

Server	Select a server. Only servers to which you are authorized to add a global caslib are listed. See Caslib Management Privileges.
Data source type	Select the type of data source. The **Data Source** area will automatically display the settings for the selected data source. Only PATH, HDFS, and DNFS can be encrypted.
Path	Specify data source-specific information for the caslib.
Name	Specify a name for the caslib.

3 Depending on the data source type that you selected, different settings are available on the **Data Source** area. Below are data sources that enable you to encrypt the data.

- PATH
- HDFS

- DNFS

For further information about these data sources and the specific parameters for each data source, see the addCaslib action in *SAS Viya: System Programming Guide*.

4 On the **New CAS Library** pane, select **Enable encryption**. Select a domain from the list of available domains or create a new domain by selecting .

Note: Only Encryption domains appear in the drop-down menu once you select **Enable encryption**.

5 After you have entered all of the parameter settings needed, Click **Save**.

Modify a Caslib

You can change the caslib path or change the description of a caslib that is encrypted. The new path will use the same encryption domain defined in this caslib. It is not possible to change the encryption domain assigned to a caslib.

1 From the side menu ( ), under **SAS Environment Manager**, select **Data** , and select **Libraries** from the drop-down view.

In the **Libraries** view, select a global caslib.

2 Right-click, and select **Edit**. Or select from the taskbar.

3 In the **Edit CAS Library** window, change the caslib path or description as needed.

4 Click **Save**.

When editing a caslib, some restrictions apply:

- Only `Path` based libraries can be edited.
- You cannot edit a personal caslib.
- You cannot change the encryption domain assigned to a caslib. If you need to do this, you will need to create a new caslib.

View Properties of an Encrypted Caslib

1 In the **Libraries** view, select a caslib.

2 Right-click, and select **Properties**. Or select from the taskbar. Read-only information is displayed.

Note that the Encryption domain is displayed.

Delete an Encrypted Caslib

You need the appropriate authorization to delete a caslib.

CAUTION! When you delete a caslib, all associated in-memory tables are immediately dropped.

1 In the **Libraries** view, select a caslib.

2 Right-click, and select **Delete**. Or select from the taskbar.

3 In the confirmation window, click **Yes**.

Note: Deleting a caslib does not affect persisted files in the corresponding data source. The persisted encrypted Sashdat files remain in the data source. If the user needs access to these files, the original encryption passphrase is required.

Manage Tables

An encrypted caslib can contain a mix of encrypted and unencrypted tables. However, loading any table still requires the user to be a member of the encryption domain.

Display Encryption Status of Tables in a Caslib

1. In the **Libraries** view, select a caslib.
2. Right-click, and select **Tables**. Or select  from the taskbar.

   A list of the tables that are assigned to the caslib is displayed.
3. Customize which columns are displayed in the Data area by selecting  and selecting **Columns**. The Columns panel opens. It contains all available columns for the currently selected table, caslib, or server.

   Display the Encryption column. In the Columns window, move Encryption from the **Hidden columns** list to the **Displayed columns** list and click **OK**.

   The Encryption column displays whether a table is encrypted or not. Values are AES for encrypted tables and NONE if the table is not encrypted.

Import an Unencrypted Table into an Encrypted Caslib

1. In the **Libraries** view, select a caslib.
2. Right-click, and select **Import**. Or select  from the taskbar.
3. In the Import Data To CAS Library window, specify one or more files to import, and click **OK**.

   For details, see *SAS Viya: Self-Service Import*.
4. Verify that the table was loaded into an encrypted caslib. In the **Libraries** view, select your encrypted caslib.
5. Right-click, and select **Tables**. Or select  from the taskbar.

   A list of the tables that are assigned to the caslib is displayed. Note that your new table shows the AES encryption status of the caslib if you have the **Encryption** column displayed. See “Display Encryption Status of Tables in a Caslib ” on page 6.

How To (Programming Tasks)

SAS Cloud Analytic Services supports encryption of SASHDAT files at the file level and at the directory level. As an administrator, you might want to simplify encryption for data at rest by configuring caslibs with an encryption password so that all files in a directory are encrypted. For information that describes how to set an encryption password at the directory level, see CASLIB Statement, DATASOURCE options in *SAS Cloud Analytic Services: Language Reference*.

For an example of using the CASLIB statement to encrypt caslibs, see Encrypt Tables in a Caslib in *SAS Cloud Analytic Services: Language Reference*.

Encryption for Data at Rest: Concepts

What Is a Domain?

Overview

Domains are used to store both the credentials (passwords and keys) required to access external data sources and the identities that are allowed to use those credentials. A domain contains one or more references to identities (users or groups) who have access to the credentials in the domain. A user can gain access to the credentials either directly with their user ID or indirectly as a member of a group that is defined as in identity.

The ID, or name, of a Domain is used in the definition of a non-Path based CAS library to access and load tables from external databases. A domain is associated with a caslib to provide access. External sources include LASR, Oracle, Teradata, Hadoop, Postgres, and Impala. Users of a caslib with an associated domain do not have to know or enter database credentials to access or load external data.

Note: Cloud Foundry supports these caslib types: Path based, DNFS, HDFS, LASR, and Hadoop.

There are three Domain types: Authentication, Connection, and Encryption.

What Is an Encryption Domain?

An Encryption domain is used to store an encryption key that is required to read data at rest in a path assigned to a caslib. The Identities selected in this Encryption domain have access to the key. When you create a Path based caslib, you can select the ability to enable Encryption. You then select or create an Encryption domain to assign an encryption key. Tables imported to this caslib will now be encrypted. If the path contains preexisting tables, those tables are not encrypted. Users that are not defined in Identities as individuals or as members of a group are not able to load data from this caslib.

Encryption domains are used to store encryption keys that can then be associated with a caslib of type PATH, HDFS, or DNFS.

What Is a Connection Domain?

A Connection domain is used when the external database has been set up to require a user ID but no password. For information about using Connection Domains, see *SAS Viya Administration: External Credentials*

What Is an Authentication Domain?

An authentication domain is a name that facilitates the matching of logins with the servers for which they are valid. Authentication domains are used to store credentials that are used to access an external source (for example, an Oracle database) that can then be associated with a caslib of the appropriate type.

The software attempts to use only the credentials that it expects to be valid for a particular resource or system. The software's knowledge of which credentials are likely to be valid is based entirely on authentication domain assignments.

Authenticating to SAS can be done through SAS logon. For more information, see *SAS Viya Administration: Authentication*

For information about using Authentication Domains, see *SAS Viya Administration: External Credentials*

Defaults

In a new deployment, encryption for data at rest is not automatically enabled. You can configure encryption of data that is added to PATH, HDFS, and DNFS caslibs by using the SAS Environment Manager and the Programmatic interface.

Encrypting Caslibs

CAS supports encryption as an option for tables in caslibs. The encryption applies to source tables, not to tables resident in memory. Encryption can be applied to individual tables or to all tables in a library. Each table can have a unique encryption key, or a single key can be set at the library level in order to have a shared key for all tables in the library.

The key must be passed on all read actions for an encrypted table unless the encryption is being handled at the library level. In that case, the server recognizes that encryption is set for the entire caslib and attempts to retrieve the key automatically.

Best Practices for Encrypting Tables in Caslibs

Here are a few best practices for encrypting data at rest.

- Only PATH, HDFS, or DNFS files can be encrypted.
- It is probably best not to have mixed tables in a caslib path.
- When you create a caslib and enable encryption, it is the new imported tables that are encrypted and stored in the path. Make sure that the path is empty first before you import the tables that you want encrypted at rest. Only the userids and groups in the domain or who know the key will be able to read that data.
- Encryption of data at rest has some performance costs, and user and administrative overhead. Sites must balance the goals of security and performance when deciding to encrypt data. Users and administrators must keep track of keys (passphrases and passwords) when accessing the data. The system will use additional CPU resources when loading and saving encrypted tables.

Reference

PROC PWENCODE

The PWENCODE procedure enables you to encode passwords. Encoded passwords can be used in place of plaintext passwords in SAS programs that access databases and various servers. For details, see *SAS Viya Visual Data Management and Utility Procedures Guide*.