SAS® Viya™ 3.2 Administration: External Credentials

External Credentials: Overview

SAS Viya deployments require credentials for external accounts and credentials for accessing databases and other third-party products requiring authentication. This document describes administrative tasks that manage these credentials using the SAS Environment Manager.

To enable users to retrieve data from existing sources such as databases (for example, Oracle and Teradata connections), the business user must have the appropriate credentials, and SAS Viya must be able to use those credentials.

This document assumes that you are familiar with the data and caslib concepts that are explained in *SAS Cloud Analytic Services: Fundamentals*.

SAS Environment Manager can be used to manage these credentials along with other administrative tasks of that external system.

External Credentials: How To

About the Domains Page

The **Security** ⇨ **Domains** page in SAS Environment Manager enables you to manage the following types of domains and credentials:

authentication domain
: makes stored credentials (user IDs and passwords) available to designated identities to facilitate connections to servers that require password.

connection domain
: makes stored credentials (user IDs) available to designated identities to facilitate connections to servers that do not require authentication.

encryption domain
: makes a stored credential (an encryption key) available to designated identities to facilitate loading of encrypted files. See *Encryption in SAS Viya: Data at Rest*.

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. On the Domain page,you can view the information for each domain that is defined, or you can create a new domain.

Note: This document discusses only the Authentication and the Connection domains. Information about the Encryption domain can be found at *Encryption in SAS Viya: Data at Rest*.

Credentials
These credentials are used to access external databases and other third-party products requiring authentication. Credentials are associated with a specifc domain for use with a specific data source type.

Manage Domains

Create a New Domain

Create an Authentication or Connection domain. For information about creating an Encryption domain, *Encryption in SAS Viya: Data at Rest*

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

You can also create a new domain when you are adding a caslib.

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

ID	Create an ID name. Required for both Authentication and Connection domains.
Type	Select the type of domain. There are three domain types, Authentication, Connection, and Encryption. Select **Authentication** or **Connection** from the list of domains.
Identities	From the Select Identities window, you can select from users, groups, and custom groups. See below for how to add an identity.
User ID	Enter the User ID that has access to the external data. All identities connect using this User ID.
Password	Enter the password for the user ID that can connect to the external database. This is not needed for the Connection domain.
Confirm password	Confirm the password. This is not needed for the Connection domain. **Note:** If the passwords do not match, you will not be able to save the domain.
Description	Add a description.

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

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. Then you can add additional users to this custom group as needed to grant access to the external data. Be sure to assign correct permission for this custom group in the associated caslib Authorization.

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

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

3 After you enter all of the parameter settings needed, click **Save**.

View Properties of the Domain

1 In the **Domains** view, select an ID of type Authentication or Connection.

2 Right-click, and select **Properties**. Or select from the taskbar. In the Domain Properties window, properties pertaining to that domain are displayed. Examples of properties displayed are the ID, type, description, date created, date modified, who created the domain, and who modified the domain.

3 Click **Close**.

View Credentials and Edit Identities of the Domain

1 In the **Domains** view, select an ID of type Authentication or Connection.

2 Right-click, and select **Credentials**. Or select from the taskbar. In the Credentials for Domain window, the credentials associated with your domain are displayed.

3 You can add or delete credentialsfrom this window. See Manage Credentials on page 4 for the details.

Edit a Domain

If you are a member of the domain, you can change the description. You cannot change the type of domain.

1 In the **Domains** view, select an ID that is of domain type Connection or Authentication.

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

3 Edit the **Description** of the Authentication Domain.

4 Click **Save**. The edited Authentication or Connection domain is now listed in the **Domains** display.

Refresh a Domain

1 In the **Domains** view, you can refresh the view.

2 Select from the taskbar. From the Domain Properties window, the domains and their properties are updated.

Delete Credentials from a Domain

1 In the **Domains** view, select an ID that is of domain type Connection or Authentication.

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

3 From the Credentials for Domain window, right-click, and select **Delete**. Or select from the taskbar.

4 In the Caution window, this message is displayed: “Are you sure you want to delete the credential for identity 'identity' with user ID 'userid'?”.

5 Click **Yes** or **No**.

Delete a Domain

1 In the Domain window, the **Domain** View, right-click, and select **Delete**. Or select from the taskbar.

2 In the Caution window, this message is displayed: “If a library is associated with this domain, you will not be able to access the data in the library after you delete the domain. Are you sure you want to delete the connection or authentication domain named '*your-domain*' and all credentials associated with the domain?”

3 Click **Yes** or **No**.

Manage Credentials

Create New Credentials

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

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

Domain	Select an existing *Authentication* or *Connection* domain.
Identities	In the Select Identities window, you can select from users, groups, and custom groups. See below for instructions on selecting an identity.
User ID	Enter the user ID and password required to access the external data.
Password	Enter the password associated with the **User ID**.
Confirm Password	Enter the same password as above.

For additional information about identities, in the New Credential window, click ⓘ.

3 To add identities, in the New Credentials window, click +.

To add an Identities member, in 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.

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**. These credentials are now associated with a Domain in the **Domains** display. The added identity is now also listed in the Credentials view.

View Credential Properties

1 In the **Credentials** view, select a User ID that you want to view.

2 Right-click, and select **Properties**. Or select from the taskbar. The properties are displayed in the Credentials Properties window. Properties that are displayed can include User ID, Identity ID, Identity type, Domain ID, Domain type, Date created, Date modified, who created the domain, and who modified the domain.

3 Click **Close**.

4 You can also create a new credential for an existing domain from this view. When you create a new credential, the Domain is already filled in for you in the New Credential window. You can also, delete a credential from this view. Follow the steps in Create New Credentials on page 4 and Delete Credentials on page 6 for details.

Edit a Credential

If you are a member of the group or custom group, or are a user associated with the selected credentials, you can add and remove lidentities (users, groups, and custom groups) to an existing credential. You will also need to supply the credentials that enable you to edit these credentials.

Do the following in the Select Identities window:

1 In the **Credential** view, select **User ID**.

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

3 To add identities, in the Edit Credentials window, click +.

To add an identities member, in 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.

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

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

In 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 After you enter all of the parameter settings needed, Click **Save**. The added identity type is now also listed in the Credentials view. The removed identity is no longer in the Credentials view.

Delete Credentials

Perform the following tasks in the Credentials view.

1. Select the user ID of the credential that you want to delete.
2. Right-click, and select **Delete**. Or select  on the taskbar.
3. In the Caution window for SAS Environment Manager, this message is displayed: “Are you sure you want to delete the credential?”.
4. Click **Yes**.

External Credentials: Concepts

What Are Credentials?

A credential is used to store the user ID and password required to access an external data source. Credentials are associated with identities. Identities can be individual users, groups, or custom groups. A credential enables you to assign a user ID and password for external data to one or more identities. For example, you can use a custom group called OracleUsers as an Identity and assign an Oracle user ID and password. The individual users or groups in this OracleUsers custom group do not need to know the Oracle credentials. These individual users will have access through this OracleUsers custom group credential definition.

What Is a Domain?

Overview

Domains are used to store both the credentials 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 access 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 caslib 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 Authentication Domain?

An authentication domain is a name that facilitates the matching of logons 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.

Each user ID and password is valid within a specific scope. For example, the user ID and password that you use to log on to your computer at work are probably not the same as the user ID and password that you use to log on to a personal computer at home. It is also common for database servers and web servers to have their own authentication mechanisms, which require yet another, different, user ID and password.

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. For this reason, you must correctly assign an authentication domain to each set of resources that uses a particular authentication provider, and also assign that same authentication domain to any stored credentials that are valid for that provider.

For example, assume that the user wants to define an Oracle caslib name "oralib" and to allow the Oracle users to access this caslib. From SAS Environment Manager, the administrator first creates a custom group of users called "orausers," and then defines a domain called "oracle." For the domain, they add "orausers" to the list of identities that have access to the credentials. They then provide a set of credentials (user ID and password) that give access to the oracle database and schema that they plan to use in the caslib. Note that in this case, all users are accessing the schema using a shared set of credentials. Finally, when defining the caslib, the administrator associates the caslib with the "oracle" domain.

Note: If the intent is for each user to access the schema using their own credentials, each user needs to be entered as a unique identity with access to the domain, and their specific credentials provided with their record.

Authenticating to SAS can be done through SAS Logon. See "Authentication: Overview" in SAS Viya Administration: Authentication.

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.

What Is an Encryption Domain?

An Encryption domain is used to store an encryption key. This key is required to read data at rest in a path assigned to a caslib. See *Encryption in SAS Viya: Data at Rest* for information about how to use Encryption domains.