External Credentials: Overview

In addition to logon credentials, users on SAS Viya systems might need external credentials for accessing databases and other third-party products. This document describes administrative tasks to manage external credentials using 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*.

External Credentials: How To

About the Domains Page

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

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

<table>
<thead>
<tr>
<th>Domain Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>authentication domain</td>
<td>Makes stored credentials (user IDs and passwords) available to designated identities to facilitate connections to servers that require a password.</td>
</tr>
<tr>
<td>connection domain</td>
<td>Makes stored credentials (user IDs) available to designated identities to facilitate connections to servers that do not require authentication.</td>
</tr>
<tr>
<td>encryption domain</td>
<td>Makes a stored credential (an encryption key) available to designated identities to facilitate loading of encrypted files. See <em>Encryption in SAS Viya: Data at Rest</em>.</td>
</tr>
</tbody>
</table>
Navigation

The Domains area is available if you are a member of the SAS Administrators group and you have opted into your assumable groups.

1. In the applications menu ( ), select Administration ➔ Manage Environment.
2. In the navigation bar, locate the Security section and click Domains 🌐.
3. You can select one of two views from the Domains page. The default view is Domains. From the View dropdown list, select one of the following views:

   | Domains          | Lists all domains displayed. Domains is the default view. There are three types of domains: Authentication, Connection, and Encryption. On the Domains page, you can view the information for each domain that is defined, or you can create a new domain.
   |                  | Note:
   |                  | This view is available only to SAS Administrators.
   |                  | Note:
   |                  | This document discusses only the Authentication and the Connection domains. For information about the Encryption domain, see Encryption in SAS Viya: Data at Rest.

   | Credentials      | Enables you to access external databases and other third-party products requiring authentication. Credentials are associated with a specific domain for use with a specific data source type.

Manage Domains

The Domains area is available if you are a member of the SAS Administrators group and you have opted into your assumable groups.

Create a New Domain

Create an Authentication or Connection domain.

1. In the Domains view, click 🌐.

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

2. In the New Domain window, you can specify the following settings:

   | ID              | Create an ID name. Required for both Authentication and Connection domains.
   | Type            | 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. To add an identity, see the following item.
   | 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 the password. This is not needed for the Connection domain.

Note:
If the passwords do not match, you cannot save the domain.

Add a description.

3 For additional information about identities, from the New Domain window, click 🔄.
4 Add Identities. From the New Domain window, click 🔄.
   a In the left pane of the Select Identities 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 Select a user, group, or custom group. You can scroll through the list or search 🔍.
   c Move the selected user, group, or custom group to the Selected Identities pane. Click 🔄.
   d Click OK.
5 Add a user ID.
6 Add a password. Click Confirm password.
7 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, delete, or edit credentials. 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.

Refresh a Domain
1 In the Domains view, you can refresh the view.
2 Select 🔄 from the taskbar.
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 $\text{Credentials}$ from the taskbar.
3. From the Credentials for Domain window, right-click, and select Delete. Or select $\text{Delete}$ 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.

Delete a Domain
1. From the Domains area, in the Domains view, select the Domain ID. Then right-click and select Delete. Or select $\text{Delete}$ from the taskbar.
2. In the Delete 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.

Manage Credentials
The Domains area is available if you are a member of the SAS Administrators group, and you have opted into your assumable groups.

Create New Credentials
From the Domains page, select the Credentials view from the drop-down list.

Note: You are creating new credentials for an existing domain.
1. To add new credentials, click $\text{Add}$.
2. In the New Credential window, specify general settings as follows:

<table>
<thead>
<tr>
<th>Domain</th>
<th>Select an existing Authentication or Connection domain.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Identities</td>
<td>In the Select Identities window, you can select from users, groups, and custom groups. See below for instructions on selecting an identity.</td>
</tr>
<tr>
<td>User ID</td>
<td>Enter the user ID and password required to access the external data.</td>
</tr>
<tr>
<td>Password</td>
<td>Enter the password associated with Identities. Note: If a Connection domain is selected, a password is not required.</td>
</tr>
<tr>
<td>Confirm Password</td>
<td>Enter the same password as above.</td>
</tr>
</tbody>
</table>

3. For additional information about identities, in the New Credential window, click $\text{Edit Members}$.
4. To add identities, in the New Credential window, click $\text{Add}$.
   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 to the **Selected Identities** pane. Click ➔.

c Click **OK**.

5 Add a user ID.

6 Add a password. Click **Confirm password**.

**Note:** If a Connection domain is selected, a password is not required.

7 After you have entered all of the parameter settings needed, click **Save**. These credentials are now associated listed in the Credentials view for the domain that you specified.

---

**View Credential Properties**

1 In the **Credentials** view, right-click a user ID that you want to view, and select **Properties**. Or select ➔ from the taskbar. The properties are displayed in the Credentials Properties window.

**Note:** Properties that can be displayed can include User ID, Identity, Identity type, Domain ID, Domain type, Modified By, Date created, Date modified, and Created By. Not all columns are displayed by default.

2 Manage which columns are displayed:
   a At the right edge of the table, click the **Options** icon ➔, and select **Manage Columns**.
   b From the Manage columns window, select items to move from the **Hidden columns** pane to the **Displayed columns** pane. After selecting the **Hidden columns**, click the **Add** arrow ➔

**TIP** To select more than one item, use the Shift key.

**Note:** You can add or remove columns to be displayed.

c Click **OK**.

3 (Optional) 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 Identities and remove Identities (users, groups, and custom groups) from an existing credential. You must supply the credentials to edit.

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 steps.
   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 to the **Selected Identities** pane.
   c Click ➔.
   d Click **OK** to save the information.

   To remove an identity, in the Select Identities window, move the user, group, or custom group to the left pane.
   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 out of the **Selected Identities** pane. Click ➔.
   c Click **OK** to save the information.

4 Change the user ID.

**Note:** If a Connection domain is selected, a password is not required.
5 Change the password. Click **Confirm password**.
6 After you have edited all of the parameters, click **Save**.

**Delete Credentials**

Perform the following tasks in the Credentials view.
1 Right-click the user ID of the credential that you want to delete, and select **Delete**. Or select on the taskbar.
2 In the Caution window for SAS Environment Manager, this message is displayed: “Are you sure you want to delete the credential for identity 'name' with user ID 'userid'?”
3 Click **Yes**.

---

**External Credentials: Concepts**

**What Are Credentials?**

Credentials are associated with identities. Identities can be individual users, groups, or custom groups. A credential enables you to assign a user ID for external data to one or more identities. Passwords are optional. 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 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 an 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 SAS 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 his or her own credentials, then each user must be entered as a unique identity with access to the domain, and the specific credentials must be provided with each user’s 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. See Encryption in SAS Viya: Data at Rest for information about how to use Encryption domains.

Manage Personal Passwords

Introduction to the My Passwords Page
These instructions explain how to manage your stored credentials (personal passwords) for authentication domains using SAS Environment Manager. These domains are used to store credentials for authenticating to a third-party provider. The credentials are associated with users, groups, or both users and groups. This feature provides the ability to edit your passwords.

The My Passwords page is visible to all users, not just administrators. If you access the page while assuming administrator privileges, the functionality on the My Passwords page is the same as if you had not assumed administrator privileges.

Note:
You cannot add or delete credentials from the My Passwords page. You can edit the passwords only for your existing credentials or display the properties for existing credentials. Only a user with Administrator privileges can manage Identities, Domains, and User IDs using the Domains page.

The My Passwords page shows credentials only for the currently logged-in user, and only for Authentication domains.

Navigation
The My Passwords area is available to members of the SAS Administrators group. When you log on to SAS, you can opt in (yes) or opt out (no) of assumable groups to manage your passwords.

1. In the applications menu (≡), select Administration ⇒ Manage Environment.
2. In the navigation bar, locate Security and click the My Passwords icon ❌.
**View Properties**

The properties displayed by default are your User ID, Domain ID, Modified By, and Date Modified. Date Created and Created By are hidden columns.

**Note:** Your credentials are available to edit or view only after an administrator has added your identity to an Authentication Domain. See “Manage Domains” on page 2.

1. Select a row to enable the Properties and Edit buttons on the toolbar.
2. To view your Credential Properties, select the Properties icon.
3. Click Close.

**View Hidden Columns**

1. To display hidden columns on the My Passwords page, at the right edge of the table, click the Options icon and select Manage Columns.
2. From the Manage columns window, select items to move from the Hidden columns pane to the Displayed columns pane. After selecting the items in Hidden columns, click the Add arrow.

**TIP** To select more than one item, use the Shift key.

3. Click OK.

**Edit Your Password**

**Note:** Your credentials are available to edit or view only after an administrator has added your identity to an Authentication Domain. See “Manage Domains” on page 2.

1. To change your password, select the Edit icon.
2. From the Change Password window, select Password and enter a new password. Select Confirm password and confirm your new password.
3. Click Save.

**Refresh Password Properties**

Manually refresh the password properties shown on the My Passwords page by selecting the Refresh icon. A toast message is shown indicating that the page has been refreshed.

**Delete External Credentials**

Your password can be deleted only by an administrator. This must be done from the Domains view for your user identity. See “Manage Domains” on page 2.