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 when using SAS Environment Manager to manage external credentials associated with.
Authentication and Connection domains. Tasks to manage identities and keys for Encryption domains can be found in “How To (SAS Environment Manager)” in Encryption in SAS Viya: Data at Rest.

To enable users to retrieve data from external data management systems (Oracle, Teradata, Facebook, Amazon, Esri, and so on), 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 explained in Caslibs, Files, and Tables. For information about using SAS Environment Manager to manage caslib data see Caslibs on the Data Sources Tab and Import Tab.

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>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 a password.</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 Encryption for Data at Rest.</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. For more information, see Accessing SAS Environment Manager.

1. Click (≡) and select Manage Environment.
2. In the navigation bar, locate the Security section and click Domains (_domains).
3. You can select one of two views from the Domains page. The default view is Domains. From the View drop-down list, select one of the following views:
Domains

Lists all domains. Domains is the default view. On the Domains page, you can view the information for each domain that is defined, or you can create a new domain.

Three default Authentication domains appear in the Domains view. These are described in Authentication Domains Defined In the Deployment on page 15.

Note: This view is available only to SAS Administrators.

Note: This document discusses only the Authentication domain and the Connection domain. For information about the Encryption domain, see Encryption for Data at Rest.

Credentials

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

Features of the tables displayed in the Domains area are as follows:

- Columns can be sorted in ascending and descending order by clicking on the column headings.
- Tables can be filtered by various column headings.
  - From the Domains view, you can use the Filter by drop-down menu to display a selected list of domains by ID and Type. When you filter by Type, you can filter on authentication, connection, or encryption. When you filter by ID, you can use any part of the ID as your filter.
  - From the Credentials view, you can use the Filter by drop-down menu to display a selected list of User IDs whose credentials are associated with domains. You can Filter by User ID, Identity, Identity Type, Domain ID, and Domain Type. When you filter by Identity Type (User, group, or custom group) or Domain Type (Authentication, Connection, Encryption), the types must match one of the values allowed to get results. For the other filter selections, you can use any part of the information contained in the table cell as your filter.
  - Refresh a table view. Select \( \mathcal{R} \) from the taskbar.
    A toast message is displayed to indicate when the Refresh has completed.

Pre-Defined Authentication Domains

The following Authentication domains are pre-defined and appear in the Domains view of SAS Environment Manager. For more information, see “Authentication Domains Pre-Defined in the Deployment” on page 15.

DefaultAuth

used to store user credentials for process launching. The DefaultAuth domain is used by CAS and the Launcher service to fetch user’s stored credentials when the Kerberos handshake fails due to expired or non-delegated credentials or when CAS or the Launcher service requests an OS-launched session using OAuth. You can change the DefaultAuth domain by changing the configuration property sas.compute.domain.default. See “Change DefaultAuth Domain” on page 6.

EsriAuth

used to store credentials for ArcGis online server definition.

Note: Only User credentials should be added to the EsriAuth domain to access premium services. No groups should be added to the EsriAuth domain.

EsriPortalAuth

used to store credentials on-premises for an Esri server or portal.
Manage Authentication Domains

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

Manage Hidden Columns

Manage which columns are displayed:

1. 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 Hidden columns to display, click the Add arrow .

   After selecting the Displayed columns to hide, click the Remove arrow →

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

3. Click OK.

Create a New Domain

Create an Authentication or Connection domain. An authentication domain can be created by specifying the domain ID. This domain ID must be unique across the system.

An administrator can create a domain that has no credentials associated with it. Until credentials are associated with a domain, it is not a functioning domain. However, credentials of users or groups can be added later to the domain. Applications can also prompt authenticated users for credentials later.

1. In the Domains view, click .

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

<table>
<thead>
<tr>
<th>ID</th>
<th>Create an ID name. Required for the Authentication domain and the Connection domain.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
<td>There are three domain types: Authentication, Connection, and Encryption. In this document, we are discussing Authentication and Connection domains. Select Authentication or Connection from the list of domains.</td>
</tr>
<tr>
<td>Description</td>
<td>Add a description.</td>
</tr>
</tbody>
</table>
   | Identities          | Select the Identities icon. You can select from users, groups, and custom groups. When you add an identity, you are prompted to enter a user ID and password.  
   |
   | Note: In the New Domain window, entering identities is optional. You can simply create the domain name and add identities later. Users can add their own credentials using the My Credentials page. |
   | User ID             | Enter the user ID that has access to the external data. All identities selected connect using this user ID.  
   |
   | Note: This field appears after you have added your ID, type, and Identities. |
**Password**
Enter the password for the user ID that can connect to the external data source. This is not needed for the Connection domain.

*Note:* This field appears after you have added your ID, type, and Identities.

**Confirm password**
Confirm the password. This is not needed for the Connection domain.

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

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

4 Add **Identities**. From the New Domain window, click ☰.

   *Note:* In the New Domain window, entering identities is optional. You can simply create the domain name. The administrator can add credentials and identities to the domain later from the **Credentials** View. See “Manage Credentials from the Credentials View” on page 9. Users can add their own credentials using the **My Credentials** area later. See “Manage My Credentials” on page 15.

   a In the left pane of the Identities window, you can filter by Users, Groups, and Custom Groups. From the drop-down menu, select ☰ Users, ☰ Groups, or ☰ Custom Groups.

   You can also filter using the search ☰.

   For more information about the types of groups and when to use them, see “Custom Groups” in SAS Viya Administration: Identity Management.

   *Note:* A best practice is to use a custom group. You can then 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. See “Identity Management: How To (SAS Environment Manager)” in SAS Viya Administration: Identity Management.

   *Note:* Only User credentials can be added to the EsriAuth domain to access premium services. No groups should be added to the EsriAuth domain.

   b Move the selected user, group, or custom group to the **Selected Identities** pane. Click ☰.

   c Click OK.

5 Add a user ID.

6 Add a password.

7 Confirm the password.

8 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, Created by, and Modified By.

3 Click **Close**.
Edit the Description of a Domain
1. From the Domains page, 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.

Delete a Domain
1. From the Domains page, in the Domains view, select the ID of a domain and right-click to select Delete. Or select ⚰️ from the taskbar.
2. In the Delete window, this message is displayed for an authentication domain that was being deleted: “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 authentication domain named 'your-domain' and all credentials associated with the domain?”
3. Click Yes or No.

View Properties of a 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. 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.

Change DefaultAuth Domain
The Compute and CAS servers can be configured to use a different DefaultAuth domain by changing the value of sas.compute.domain.default property.
1. Click (⚙️) and select Manage Environment.
2. In the navigation bar, locate the System section and click Configuration ⬇️.
3. From the Configuration window, select Definitions from the drop-down menu.
4. In the search box, type sas.compute. Double-click on sas.compute to see the configuration properties.
5. Edit the sas.compute properties. Click ⚙️.
6. From the Edit sas.compute Configuration window, change the domain.default value from DefaultAuth to another domain.
7. Click Save.
For information about the sas.compute properties, see “Compute Service” in SAS Viya Administration: Configuration Properties.

Manage Credentials from the Domains View

You can manage credentials for Authentication and Connection domains from the Domains View or the Credentials view. The operations are very similar.

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

Manage Hidden Columns

Manage which columns are displayed:

1. 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 Hidden columns to display, click the Add arrow ➔. After selecting the Displayed columns to hide, click the Remove arrow ←.

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

3. Click OK.

Add Credentials

Add credentials to an existing Authentication or Connection domain. This view is displayed as Credentials for Domain: domain-ID.

1. From the Domains page, select an existing Authentication or Connection domain ID. Right-click, and select Credentials. Or select ☰ from the taskbar. In the Credentials for Domain view, credential properties are displayed.

2. To add new credentials to the selected Encryption domain, click ⌁.

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

4. Add Identities. From the New Credential window, click ☰.

   a. In the left pane of the Identities window, you can filter by Users, Groups, and Custom Groups. From the drop-down menu, select Users, Groups, or Custom Groups.

      You can also filter using the search ☰.

      For more information about the types of groups and when to use them, see “Custom Groups” in SAS Viya Administration: Identity Management.

      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.

      Only User credentials can be added to the EsriAuth domain to access premium services. No groups should be added to the EsriAuth domain.
Move the selected user, group, or custom group to the Selected Identities pane. Click ➔.

Click OK.

Enter User ID.

Enter a password. Confirm your password by entering it again.

After you have entered all of the parameter settings needed, click Save. These credentials are now listed in the Credentials for Domain: Domain ID view.

Edit Credentials

If you are a member of the domain, you can add identities to and remove identities (users, groups, and custom groups) from an existing domain. You can also change the password.

1 In the Credentials for Domain: Domain ID view, select a credential entry.

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

3 To add and delete identities, in the Edit Credential window, click ➔.

a In the left pane of the Edit Credential window, you can filter by Users, Groups, and Custom Groups. From the drop-down menu, select Users, Groups, or Custom Groups. You can also filter using the search ☰.

For more information about the types of groups and when to use them, see “Custom Groups” in SAS Viya Administration: Identity Management.

b To add a selected user, group, or custom group to the Selected Identities pane, click ➔.

To remove a selected user, group, or custom group from the Selected Identities pane, click the Remove arrow ←.

c Click OK.

4 Enter a password.

5 Confirm the password.

6 Click Save.

Delete Credentials

Perform the following tasks in the Credentials for Domain: Domain ID view. Select a credential that you want to remove.

1 Right-click the credential that you want to delete, and select Delete. Or select ☰ on the taskbar.

2 In the Delete window, this message is displayed: “Are you sure you want to delete the credential for the identity "name" user ID "Domain ID"?”

3 Click Yes or No.

View Credential Properties

1 From the Credentials for Domains: Domain ID view, select a credential that you want to view.
2 Right-click, and select **Properties**. Or select ![Properties](image) from the taskbar. In the Credentials Properties window, credential properties are displayed.

3 Click **close**.

---

**Manage Credentials from the Credentials View**

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

**Manage Hidden Columns**

Manage which columns are displayed:

1 At the right edge of the table, click the **Options** icon ![Options](image), 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 **Hidden columns** to display, click the **Add** arrow →

After selecting the **Displayed columns** to hide, click the **Remove** arrow ←

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

3 Click **OK**.

**Add 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 ![Add](image).

2 From the New Credential window, select an existing **Authentication** or **Connection** domain from the drop-down menu.

3 After the Domain has been selected, specify the other settings in the New Credential window.

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

4 For additional information about identities, in the New Credential window, click ![Identity](image).
5 Add **Identities**. From the New Credential window, click 🔄.  
   a In the left pane of the Identities window, you can filter by Users, Groups, and Custom Groups. From the drop-down menu, select 🔄 **Users**, 🔄 **Groups**, or 🔄 **Custom Groups**.  
   You can also filter using the search 🕵️.  
   For more information about the types of groups and when to use them, see “Custom Groups” in *SAS Viya Administration: Identity Management*.  
   **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.  
   Only User credentials can be added to the EsriAuth domain to access premium services. No groups should be added to the EsriAuth domain.  
   b Move the selected user, group, or custom group to the **Selected Identities** pane. Click ➔.  
   c Click **OK**.

6 Add a user ID.

7 Add a password. Confirm your password by entering it again.  
   **Note:** If a Connection domain is selected, a password is not required.

8 After you have entered all of the parameter settings needed, click **Save**. These credentials are now listed in the Credentials view.

**View Credential Properties**

1 In the **Credentials** view of the Domains page, right-click a user ID that you want to view, and select **Properties** or select 🗂️ from the taskbar. The properties are displayed in the Credential Properties window. Only the credentials for the selected domain are displayed.  
   **Note:** Properties that can be displayed can include User ID, Identity ID, Identity type, Domain ID, Domain type, Date created, Date modified, Created by, and Modified by.  
   2 Click **close**.
   3 (Optional) You can also add a new credential using the **Credentials** view. You can delete a credential from this view also. Follow the steps in “Add New Credentials” on page 9 and “Delete Credentials” on page 11 for details.

**Edit a Credential**

If you are a member of the group or custom group, or 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 **Credentials** view of the Domains page, select a credential entry.

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

3 To add and delete identities, in the Edit Credential window, click 🔄.  
   a In the left pane of the Edit Credential window, you can filter by Users, Groups, and Custom Groups. From the drop-down menu, select 🔄 **Users**, 🔄 **Groups**, or 🔄 **Custom Groups**.
You can also filter using the search filter.

For more information about the types of groups and when to use them, see “Custom Groups” in SAS Viya Administration: Identity Management.

Note: Only User credentials can be added to the EsriAuth domain to access premium services. No groups should be added to the EsriAuth domain.

b To add a selected user, group, or custom group to the Selected Identities pane, click ➔.

To remove a selected user, group, or custom group from the Selected Identities pane, click the Remove arrow ⇐.

c Click OK.

4 Enter the user ID.

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

5 Enter the password. Edit the password if you want to change it.

6 Enter the password again to confirm the password.

7 After you have edited all of the parameters, click Save.

Delete Credentials

Perform the following tasks in the Credentials view of the Domains page.

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 Delete window, this message is displayed: “Are you sure you want to delete the credential for the identity "name" with user ID ‘userid’?”

3 Click Yes.

Configure the Web Data Access Service to Use a Forward Proxy Server to Allow Validation of Esri Premium Service Credentials

If you are using Esri Premium Services, when you validate your credentials, the web data access service makes a request to www.arcgis.com. When the server where the Web Data Access service is running does not have outbound internet access, the request fails and you will be unable to use your Esri premium services.

You can follow the steps to add forward proxy JVM options to the web data access microservice to allow it to make the request to arcgis.com through a forward proxy.

The following options enable the Esri Premium Service requests to be made through a proxy server. Any SAS Visual Analytics deployment that uses Esri Premium services must use the following options to configure outbound internet access on SAS Viya servers.

The Configuration area is available if you are a member of the SAS Administrators group and you have opted into your assumable groups. For more information, see Accessing SAS Environment Manager.
1. Click (Ξ) and select Manage Environment.

2. In the navigation bar, click 🔍.

3. The default view is Basic Services. Select All Services from the drop-down box.

4. In the All Services list, filter on Web Data Access service. Select Web Data Access service.

5. In the content pane on the right are the configuration instances for that service. If you see an existing jvm configuration instance, click ⬇️. If you do not see an existing jvm configuration instance, at the top of the content pane click New Configuration.

   If you have an existing jvm configuration for the Web Data Access service, edit the existing one and do not create a new one.

6. In the Select Definition dialog box, select jvm.

7. In the New jvm Configuration window, click +.

8. In the Add Property window, add the jvm options (Name and Value) shown in Table 1 on page 12.

   **Note:** The JAVA_OPTION_HTTPPROXYUSER option and JAVA_OPTION_HTTPPROXYPASSWORD options are necessary only when your proxy server requires authentication.

   a. In the Name field, add the options from the “Name” column in the following table.

   b. In the Value field, and the values from the “Value” column in following table. The proxy-server-name is the name of your proxy server.

   c. Click Save.

   **Table 1  JVM Options Used to Configure Esri Premium Services Access from a Proxy Server**

<table>
<thead>
<tr>
<th>Name</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>JAVA_OPTION_HTTPPROXYHOST</td>
<td>-Dhttp.proxyHost=http-proxy-server-name</td>
</tr>
<tr>
<td>JAVA_OPTION_HTTPPROXYPOR +</td>
<td>-Dhttp.proxyPort=http-proxy-port-number</td>
</tr>
<tr>
<td>JAVA_OPTION_HTTPNONPROXY</td>
<td>-Dhttp.nonProxyHosts=host-name</td>
</tr>
<tr>
<td>JAVA_OPTION_HTTPS PROXYHOST</td>
<td>-Dhttps.proxyHost=https-proxy-server-name</td>
</tr>
<tr>
<td>JAVA_OPTION_HTTPS PROXYPORT</td>
<td>-Dhttps.proxyPort=https-proxy-port-number</td>
</tr>
<tr>
<td>JAVA_OPTION_HTTPPROXYUSER</td>
<td>-Dhttp.proxyUser=proxy-username</td>
</tr>
<tr>
<td>JAVA_OPTION_HTTPPROXYPASSWORD</td>
<td>-Dhttp.proxyPassword=proxy-password</td>
</tr>
</tbody>
</table>

   For more information, see Java Documentation.

9. Restart the SAS Web Data Access service.

   **Note:** On a multiple-machine deployment, there is a sequence for starting and stopping SAS Viya servers and services. See “General Servers and Services: Operate (Linux)” in SAS Viya Administration: General Servers and Services.
Red Hat Enterprise Linux 7.x (or an equivalent distribution) and SUSE Linux Enterprise Server 12.x:
```bash
sudo systemctl restart sas-viya-web-data-access-default
```
Red Hat Enterprise Linux 6.x (or an equivalent distribution):
```bash
sudo service sas-viya-web-data-access-default restart
```
For Windows, in Windows Services Manager, right-click SAS Web Data Access service and select Restart.

The Web Data Access service should now be able to make the Esri Premium Services request through a proxy.

Perform the following to verify your credentials.

- In the applications menu (☰), from the Analytics Life Cycle section, select Explore and Visualize.
- From SAS Visual Analytics, click your user name in the top right corner and select Settings ➜ SAS Visual Analytics ➜ Geographic Mapping.
- If you have not already accepted Esri terms and conditions and enabled Esri Premium services, check those boxes.
- Enter your Esri Premium Services credentials (User ID and Password) and select Validate credentials.
- Select Close.

---

**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. 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.

In SAS Viya, SAS Environment Manager uses the credentials service to store credentials.

**What Is a Domain?**

**Overview**

Domains are used to store both the credentials required to access external data sources (for example, databases and other data sources such as Facebook and Amazon) 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. Users 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 data sources. A domain is associated with a caslib to provide access. Some examples of 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 data source credentials to access or load external data.

There are three domain types: authentication, connection, and encryption.

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 that can then be associated with a caslib of the appropriate type. They can also be used for batch processing and scheduling where you store your credentials in a domain to run jobs in batch mode.

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 named "oralib" and allow the Oracle users to access this caslib. From SAS Environment Manager, the administrator first creates a custom group of users called orauusers, and then defines a domain called "OracleAuth." For the domain, they add orauusers 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 "OracleAuth" domain.

Note: If the intent is for users to access the server with their own credentials, simply define the domain and instruct users to use the My Credentials window to enter their own credentials. See “Manage My Credentials” on page 15.

Authenticating to SAS Viya can be done through SAS Logon Manager. See Authentication: Overview.

Connection Domain

A Connection domain is used when the external source has been set up to require a user ID but no password. For example, a third-party database like Hadoop might be configured with accounts for authentication that do not require a password.

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 choose to enable encryption. You then select an encryption domain to assign an encryption key. Tables imported to this caslib are now encrypted. If the path contains preexisting tables, those tables are not encrypted. Users who are not defined in Identities as individuals or as members of a group cannot load data from this caslib. See Encryption for Data at Rest for information about how to use encryption domains.
Authentication Domains Pre-Defined in the Deployment

The following three default authentication domains are present in a full deployment of SAS Viya:

**EsriAuth**
- authentication domain to store credentials for ArcGis online server definition.
- **Note:** Only User credentials can be added to the EsriAuth domain to access premium services. No groups should be added to the EsriAuth domain.

**EsriPortalAuth**
- authentication domain to store credentials on-premises for an Esri server or portal.

**DefaultAuth**
- used to store user credentials for process launching. The DefaultAuth domain is used by CAS and the Launcher service to fetch user’s stored credentials when the Kerberos handshake fails due to expired or non-delegated credentials or when CAS or the Launcher service requests an OS-launched session using OAuth.

Esri Premium Services Needs Valid Credentials

Geo Enrichment Service from Environmental Systems Research Institute (Esri) provides a large collection of data sets, including population, income, housing, consumer behavior, and the natural environment. You can use SAS Visual Analytics to gain access to Esri premium services.

To access Esri premium services, SAS Visual Analytics must have an identity that can log in to the Esri server and must be able to validate the credentials. The identity must be a member of the Esri Users custom group and must have valid credentials to access Esri premium services. Users can be added to this group using SAS Environment Manager. The user ID and password combination of this identity is entered in the Domain (the user ID and password combination that has access to the Esri server). You can provide single identities that all users share or each user can have their own identities. See “Manage Authentication Domains” on page 4.

If your login has appropriate privilege, you can Import Esri data into a caslib. See “Importing Esri Data for Geoenrichment and Geocoding” in SAS Data Explorer: User’s Guide.

If you are using Esri premium services (requires validation of credentials) and the SAS Viya server where the web data access service is running, does not have direct internet access to reach www.arcgis.com, you need to configure options that allow direct internet access to the proxy server. See “Configure the Web Data Access Service to Use a Forward Proxy Server to Allow Validation of Esri Premium Service Credentials” on page 11 for details.

Manage My Credentials

Introduction to the My Credentials Page

These tasks explain how to manage your stored credentials for authentication and connection domains using SAS Environment Manager. These domains are used to store credentials for authenticating and connecting to third-party providers, to the CAS Server, and to the SAS Compute Server. The credentials are associated with users, groups, or both users and groups.
The My Credentials page is visible to all users, not just administrators. If you access the page while assuming administrator privileges, the functionality on the My Credentials page is the same as if you had not assumed administrator privileges.

You can perform the following tasks from the My Credentials page:

**Note:** A user ID and password are required when adding and editing credentials.

- You can edit, delete, and display the properties of credentials for the currently logged-in user, and only for Authentication or Connection domains.
- You can add credentials to an authentication or connection domain, but only to domains for which your credential is not already associated.
  
  **Note:** Only a user with Administrator privileges can manage Identities, Domains, and User IDs using the Domains page.
- You can modify what columns are displayed on the page. All columns are displayed by default.

### Navigation

The My Credentials page is available when you log on to SAS, and you opt in (yes) or opt out (no) of assumable groups to manage your credentials. For more information, see Accessing SAS Environment Manager.

1. In the applications menu (≡), in the navigation bar, select **Administration ➔ Manage Environment**.

2. In the navigation bar, locate **Security** and click the **My Credentials** icon ⚪.

### Add New Credentials

You can add credentials to an existing domain. Only an administrator can add a domain. See “Manage Authentication Domains” on page 4.

**Note:** You can add credentials to an authentication or connection domain, but only to a domain where your user credential is not already associated.

1. To add new credentials, click ⚪.

2. From the New Credential window, select an existing Authentication or Connection domain from the drop-down menu.
   
   **Note:** This list of domains displayed in the drop-down menu are domain names with which your personal credential is not associated.

3. Add a user ID.

4. Add a password and confirm your password by entering it again.
   
   **Note:** If a Connection domain is selected, a password is not required.

5. Click **Save**.
Manage Columns Displayed on My Credentials Page

All columns are displayed by default on the My Credentials page. Properties displayed are User ID, Domain ID, Modified By, Date Modified, Created By, and Date Created.

1 To manage the columns that are displayed on the My Credentials 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 between the Displayed columns pane and the Hidden columns pane. After selecting the items to display or hide, click the Add arrow ⇨ or the Remove arrow ←.

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

3 Click OK.

View the Properties of Your Credentials

You can view the properties of the credentials for the currently logged-in user, and only for Authentication or Connection domains.

1 Select a row to enable the Properties, Edit, and Delete icons on the toolbar.

2 To view your Credential Properties, right-click a user ID that you want to view, and select Properties or select the Properties icon FAQ.

3 Click Close.

Edit Your Credentials

1 Select a row to enable the Edit, Properties, and Delete icons on the toolbar.

2 To change your credentials, select the Edit icon ‣.

3 From the Edit Credential window, you can change your user ID and password. For this example, select Password and enter a new password. Confirm your password by entering it again.

4 Click Save.

Refresh Password Properties

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

1. Select a row to enable the Delete, Properties, and Edit icons on the toolbar.

2. Right-click the user ID of the credential that you want to delete, and select Delete. Or select 💾 on the taskbar.

3. A Delete window appears and asks "Are you sure you want to delete the credential with user ID "yourName". Click Yes."