## Identity Management Overview

User and non-custom group identities are stored and managed by your organization’s identity provider (for example, Microsoft Active Directory). Read-only access to the provider enables SAS to authenticate users and
obtain identity information at sign-on. Custom groups do not exist in your identity provider and are used only in accessing SAS.

Most aspects of SAS identity management are not used in a programming-only deployment. In such deployments, your operating system user management is used. However management of CAS roles is applicable in a programming-only environment.

SAS identity management includes:
- managing the membership of custom groups and CAS roles.
- giving users, groups, and custom groups access to SAS functionality.

**Identity Management How To**

**View User and Group Information**

To view user and group information:

1. In the side menu, under SAS Environment Manager, select **Users**.

2. On the **Users** page, you can do the following:
   - Select **Users**, **Groups**, or **Custom Groups** from the drop-down list in the toolbar. Custom groups are displayed when you first open the page.
     - Note: A custom group is a group that exists in SAS but not in your identity provider.
   - Type a string in the **Search** field to search for identities within the category you selected (Users, Groups, or Custom Groups). To restore the complete list of identities, clear the search field.
   - Click an identity in the left pane to see its properties in the right pane. An identity’s properties include the following:
     - basic properties including name, ID, and description
     - contact information (for users only)
     - a list of members (for groups and custom groups only)
     - a list of groups that the identity is a member of. indicates custom groups, and indicates groups from your identity provider.
     - Note: Properties for users and groups are retrieved from your directory service and are read-only. Properties for custom groups are stored in SAS and can be edited using SAS Environment Manager.
   - Access recently viewed identities by using the drop-down box at the top of the right pane.
   - Note: To add, edit, or delete users and groups (other than custom groups), use your organization’s identity provider (for example, Microsoft Active Directory) to which SAS Viya is connected.

**Manage Custom Groups**

A custom group is a group that exists in SAS Viya but not in your identity provider. Your deployment includes a set of predefined custom groups, which provide an easy way to give users access to specialized functionality. You can also create your own custom groups, which are useful if you don’t want to (or don’t have permission to) create groups in your identity provider.
Add or Remove Custom Group Members

1. On the Users page in SAS Environment Manager, select **Custom Groups** from the drop-down list in the toolbar.

2. In the left pane, click the name of the group whose members you want to update.

3. In the **Members** section of the right pane, click ** Edit Members**.

   The Edit Members window appears, with the custom group’s current members displayed in the right pane.

4. To add a member, do the following:
   
   a. In the left pane of the Edit Members window, select **Users**, **Groups**, or **Custom Groups** from the drop-down box.
   
   b. In the left pane, click the name of a user, group, or custom group identity. The identity’s properties are displayed in the far right pane.
   
   c. Click ** Add **.

5. To remove a member, do the following in the Edit Members window:

   a. In the **Select Identities** list, click the user, group, or custom group identity that you want to remove. The identity’s properties are displayed in the right pane.

   b. Click ** Remove **.

6. When you are finished adding and removing members, click **OK**.

   **Note:** If you add or remove a user, the change takes effect the next time that this user logs in to SAS Environment Manager. If the user is currently logged in, their previous memberships continue to apply.

Create a New Custom Group

Create custom groups to give members similar permissions.

1. On the **Users** page in SAS Environment Manager, select **Custom Groups** from the drop-down list in the toolbar.

2. Click ** New ** in the toolbar.

3. In the **New Custom Group** window, enter a unique name and ID for the group. You can also enter a description.

   **TIP** Create an ID that is easily recognizable. For example, for the group “Report Testers”, you could use “ReportTesters” as the ID.

4. Click **Save**.

   **TIP** You can also create a custom group by copying an existing group or custom group. To do so, click the existing group (or custom group) and select ** Copy **. You can then edit the properties and members of the new custom group as needed.
Edit a Custom Group’s Basic Properties
1. On the Users page in SAS Environment Manager, select **Custom Groups** from the drop-down list in the toolbar.
2. In the left pane, click the name of the group whose properties you want to edit.
3. In the **Basic Properties** section of the right pane, click **Edit**.
4. In the Edit Custom Group window, enter your changes to the name or description.
   **Note:** You cannot edit the ID of a custom group.
5. Click **Save**.

Delete a Custom Group
1. On the Users page in SAS Environment Manager, select **Custom Groups** from the drop-down list in the toolbar.
2. Click the custom group that you want to delete. The group’s properties are displayed in the right pane.
3. Click **Delete** in the confirmation window.

Manage CAS Role Memberships (SAS Environment Manager)
For the CAS server, make sure to designate at least one user (other than the server’s process owner) to the Superuser role. In the initial deployment, users that you add to the SAS Administrators predefined custom group have membership in the Superusers role. If you want to designate a user to the role without providing the extra privileges of SAS Administrators, follow these instructions.

Add or Remove CAS Role Members
To add or remove members of the Superuser role in SAS Environment Manager:
1. In the side menu, under SAS Environment Manager, select **Data**.
2. In the View field, select **Servers**.
3. Right-click a CAS server, and select **Assume the Superuser role**.
4. Right-click the server again, and select **Properties**.
5. In the Superuser Role Membership section of the Properties page, click **Edit**.
6. To add a member, do the following in the Select Identities window:
   - In the left pane, select **Users**.
   - In the left pane, click the name of a user. The user’s properties are displayed in the far right pane.
   - Click **Add**.
7. To remove a member, do the following in the Select Identities window:
In the Select Identities list, click the user that you want to remove. The identity’s properties are displayed in the right pane.

Note: You cannot change or remove the account that starts the server.

Click \( \rightarrow \).

8 Click OK.

9 Click Relinquish in the status bar to relinquish the Superuser role.

**Assume the Superuser Role**

In SAS Environment Manager, you become a Superuser only after you explicitly assume that role. For example, you might assume the role to troubleshoot and resolve an access issue. To assume the Superuser role:

1 In the side menu, under SAS Environment Manager, select Data.

2 In the View field, select Servers.

3 In the list of servers, right-click the name of the server for which you want to assume the role, and select Assume the Superuser role.

The status message at the bottom of the page reminds you that you have assumed the role.

4 After you perform the task that required the role, click Relinquish in the status bar.

Note: Use the Superuser role only when it is required for a specific task. Be sure to relinquish the role when you are finished.

**Manage CAS Role Membership (CAS Server Monitor)**

In CAS Server Monitor, you can designate users or groups for the Data role. In the initial deployment, users that you add to the SAS Administrators predefined custom group have membership in the Superusers role. If you want to designate a user to the role without providing the extra privileges of SAS Administrators, follow these instructions.

**Add or Remove CAS Role Members**

The CAS (Superuser) role provides unrestricted access to all CAS objects and actions within the CAS server.

To add or remove members of the CAS (Superuser) or Data role in CAS Server Monitor:

1 Sign in to CAS Server Monitor with an account that is already a CAS (Superuser).

2 In the left navigation bar, select \( \rightarrow \).

3 On the Configuration page, select the Administrators tab.

4 To add a member:

   a Click Add.

      Note: If the Add button is not present, you are not signed in as a CAS (Superuser).

   b In the Add Administrator window, enter a user or group name, select the appropriate identity type, and select the CAS or Data radio button.
The user and group names that you enter are not validated. You can enter any user or group name from your identity provider.

c Click OK to save your changes.

5 To change a role assignment:

a Click in the appropriate row, and select Modify. You cannot change the assignment for the account that starts the server.

b In the Edit Administrator window, select Data or CAS, and click OK.

6 To remove a role assignment, click in the appropriate row, and select Delete. You cannot remove the account that starts the server.

7 Under Administrators, review the results.

8 Verify that full administrative privileges are available when designated users sign in to CAS Server Monitor. For example, any user who sees the Add button on the Administrators tab is a CAS administrator (Superuser).

Manage Access to Functionality

Access to functionality determines the features that are available to a user. Initially, all authenticated users have access to functionality that is appropriate for a typical user.

Give Users Access to Additional Functionality

To give users access to additional functionality, you should begin by simply adding selected users and groups to the appropriate predefined custom group.

For details about these groups, see Predefined Custom Groups on page 9.

Note: To manage access to CAS administrative functionality separately, see CAS Server Roles on page 11.

See Also

- Access to Functionality on page 10
- Initial Rules for Access to Functionality on page 13

Adjust Rules for Access to Functionality

If you identify the need for more granular control, based on your organization’s use of Viya, here are examples of steps that you can take to adjust the level of access for a given category of users.

Restrict a Function to a Particular Group

The principal in an authorization rule is the user, group, or construct to which the rule is assigned. By default, the Authenticated Users principal (a construct that includes all authenticated users) has access to a large number of functions. If you want to restrict one or more of these functions to a particular group, follow these steps:

1 In SAS Environment Manager, select Security ⇒ Rules in the side menu.
2 Select Principal in the Filter by drop-down box, and enter authenticated users in the filter field.

3 From the subset of rules that apply to authenticated users, find the rule that corresponds to the functionality that you want to restrict. The Object URI and Description columns provide information to help identify the rule.

4 Select the rule, and click .

5 In the Edit Rule window, select group in the Principal Type field. Then select the appropriate group or custom group in the Principal field.

6 In the description field, replace All authenticated users with the name of the group for which you provided access.

   CAUTION! It is strongly recommended that you leave all of the other fields unchanged.

7 Click Save.

8 On the Rules page, right-click the rule and select Properties. Verify that the elements of the edited rule are as you intended.

Grant an Administrative or Specialized Function to a Different Group

By default, access to administrative or specialized functions are granted to predefined custom groups (such as SAS Administrators and Application Administrators). If you need to grant one of these functions to a different group of users, follow these steps:

1 In SAS Environment Manager, select Security ➔ Rules in the side menu.

2 Select Principal in the Filter by drop-down box, and enter the ID of the predefined custom group (for example, SASAdministrators) in the filter field.

3 From the subset of rules that apply to the group, find the rule that corresponds to the functionality that you want to reassign. The Object URI and Description columns provide information to help identify the rule.

4 Select the rule, and click .

5 In the principal type field, select group. Then select the appropriate group or custom group in the Principal field.

6 In the description field, replace the name of the predefined custom group with the name of the group for which you provided access.

   CAUTION! It is strongly recommended that you leave all of the other fields unchanged.

7 Click Save.

8 On the Rules page, right-click the rule and select Properties. Verify that the elements of the edited rule are as you intended.

Identity Management: Guidelines and Best Practices

The following basic guidelines contribute to simplicity and security:

- Limit membership in administrative roles and groups.
Assume administrative group memberships only when you need to perform tasks that require the extra permissions.

Assume a CAS administrative role only when you need to perform tasks that require the extra permissions, and relinquish the role when you are finished.

If you delete a custom group, any rules that are associated with this custom group still exist. Review all rules that have the deleted group as their Principal, and either reassign them to other groups, or delete them.

---

**Identity Management Concepts**

**Identity Providers**

User and group identities are stored and managed in your organization’s identity provider. SAS has read-only access to the provider, enabling SAS to authenticate users and obtain identity information at sign-on.

**Supported Identity Providers**

SAS Viya supports identity providers that are based on LDAP.

**Identities Service Configuration**

SAS Viya can connect to any LDAP server, such as Microsoft Active Directory, OpenLDAP or ApacheDS. The SAS Identities service configuration has default values appropriate for Microsoft Active Directory. For other LDAP servers overwrite these values with equivalents for your server.

To enable SAS Viya to access your identity provider, you must update the SAS Identities service configuration with the following information:

- the provider’s host, password, port, url, and userDN. If you are using Microsoft Active Directory, this is the only information you need to change.
- mappings of your provider’s identity fields to the fields used in SAS
- information to enable searching for users and groups

**See Also**

- Configure the Connection to Your Identity Provider
- “Identities Service” in SAS Viya Administration: Configuration Properties

**Identity Filtering**

When you Configure the Connection to Your Identity Provider, you can specify a filter to limit the identities that SAS Viya returns. For example, you can create a filter to exclude groups of users who do not need access. You can modify this filter at any time.

Default filters are provided at both the user and group level. See “Configuration Properties: Reference (Services)” in SAS Viya Administration: Configuration Properties for details of their usage.

If you have a large number of users, using a filter can improve performance and reduce memory requirements. In addition, user management tasks can be performed more efficiently if only relevant identities are listed in SAS Environment Manager.
Identity Caching

Identity caching is available for enhanced performance. Search requests go to the cache, reducing the number of direct requests to the identity provider. You can configure the cache refresh interval, and enable or disable the cache. The cache is enabled by default. See “Identities Service” in SAS Viya Administration: Configuration Properties.

Custom Groups

What Is a Custom Group?

A custom group is a group that exists in SAS Viya but not in your identity provider. These groups are persisted in a SAS database.

Your deployment includes a set of predefined custom groups. You can also create your own custom groups. This feature is useful if you want to create new groups of SAS users, but you don’t want to (or don’t have permission to) create groups in your identity provider.

Predefined Custom Groups

The following custom groups are provided with your deployment. These groups provide an easy way to give users and groups access to the appropriate data, content, or functionality.

Note: These groups are not supplied in a programming-only deployment.

<table>
<thead>
<tr>
<th>Group Name</th>
<th>Initial Authorizations</th>
<th>Initial Memberships</th>
</tr>
</thead>
<tbody>
<tr>
<td>SAS Administrators</td>
<td>Have access to:</td>
<td>CAS Superuser role</td>
</tr>
<tr>
<td></td>
<td>■ all tasks in SAS Environment Manager and CAS Server Monitor</td>
<td></td>
</tr>
<tr>
<td></td>
<td>■ all folders and all objects that the folders contain (for example, plans and reports)</td>
<td></td>
</tr>
<tr>
<td>Application</td>
<td>Can access the following items from SAS Home:</td>
<td>None</td>
</tr>
<tr>
<td>Administrators</td>
<td>■ Publish Tile</td>
<td></td>
</tr>
<tr>
<td></td>
<td>■ Manage Published</td>
<td></td>
</tr>
<tr>
<td></td>
<td>■ SAS Theme Designer</td>
<td></td>
</tr>
<tr>
<td>Data Builders</td>
<td>Can access SAS Visual Data Builder and advanced import features.</td>
<td>None</td>
</tr>
<tr>
<td>Esri Users</td>
<td>Can access Esri systems for geo map access.</td>
<td>None</td>
</tr>
</tbody>
</table>

Assumable Custom Groups

The SAS Administrators group is a predefined custom group. This group is assumable. When a user in this groups signs in to Viya, a prompt appears asking Do you want to opt in to all of your assumable groups?

If the user selects Yes, the user gets the extra permissions that are associated with the assumable group. If the user selects No, the user does not get the extra permissions. The selection remains in effect until the user signs out.
As a best practice, users should select **Yes** only when they need to perform tasks that require the extra permissions.

**The CASHostAccountRequired Custom Group**

The CASHostAccountRequired custom group is predefined, but not created. If you create a group with ID: `CASHostAccountRequired`, members of this group will automatically run their CAS sessions under their own host account. By default CAS sessions are run using the `cas` account.

As a consequence members of this group must have host accounts.

When you modify the membership of this group, the users that have been added or removed must log out of their sessions before the changes can take effect.

If a user has previously created sashdat files and is then added to the CASHostAccountRequired custom group they can continue to work with data in memory. However, if certain triggering events occur, such as a CAS server restart, the same user can no longer see their sashdat files as the location of these files is different for members of this group. Users in this situation should copy their sashdat files from the default location to the host CAS user path.

The original default location is: `:/opt/sas/viya/config/data/cas/default/formats/casuserlibraries/username` where `username` is the user’s host account.

The host CAS user location is: `~/.casuser/`, where the `~` represents the users home directory.

Note that files should be copied in the opposite direction for users that are removed from the CASHostAccountRequired group.

**Additional Documentation**

Here is additional documentation related to custom groups:

- Manage Custom Groups on page 2
- Access to Functionality on page 10
- Initial Rules for Access to Functionality on page 13

**Access to Functionality**

Access to functionality determines the features that are available to a user, such as the following:

- applications that the user can access
- menu items or pages that are visible to the user after an application is opened
- media types that the user can access, and the user’s permissions for that media type

**Note:** Access to CAS administrative functionality is managed separately. See CAS Server Roles on page 11.

Access to functionality (other than CAS administration) is managed by rules that target a service, a service endpoint, a media type (for example, folders or reports), or a pseudo URI. These rules are created and enforced using the general authorization model. This is the same model that is used for rules that target specific objects (for example specific folders or reports).

SAS provides an initial set of rules to control your users’ access to functionality, including the following:

- rules that give all authenticated users access to functionality that is appropriate for a typical user. These rules are applied automatically to any user who successfully signs in.
- rules that give special categories of users access to additional functionality (for example, access to administrative functions). To apply these rules, you simply add users or groups to a predefined custom group such as SAS Administrators.
In most cases, the initial rules provide a sufficient level of control. If (after gaining experience with SAS Viya) you identify the need for more granular control, you can make adjustments to the rules’ applicability.

See Also

- Initial Rules for Access to Functionality on page 13
- Adjust Rules for Access to Functionality on page 6

CAS Server Roles

Superusers have unrestricted access to CAS and are exempt from all CAS authorization requirements.

In SAS Environment Manager, the Superuser role is never initially or automatically assumed. If you are a member of a CAS server’s Superuser role, you can become a Superuser by explicitly assuming the role for that server. For example, you might assume the role to troubleshoot and resolve an access issue. After the issue is resolved, you relinquish the role.

The account that starts a CAS server is automatically assigned to that server’s Superuser role.

<table>
<thead>
<tr>
<th>Role</th>
<th>Description</th>
<th>Assumable?</th>
<th>Initial Members</th>
</tr>
</thead>
<tbody>
<tr>
<td>Superuser</td>
<td>Provides unrestricted access to a CAS server. Only a Superuser can perform the following tasks: Stop the server. Add and remove nodes. Manage role membership. See and manage the paths list. The account under which a CAS server runs is an implicit member of that server’s Superuser role. Make sure the CAS server has at least one other designated Superuser.</td>
<td>Yes</td>
<td>SAS Administrators (except in a programming-only environment) Process owner for the server</td>
</tr>
<tr>
<td>Data</td>
<td>Provides unrestricted access to caslibs, tables, and columns in a CAS server. Assign members to this role only if you have users who should have unrestricted access to data but should not be able to perform all administrative tasks. Not all interfaces support the Data role.</td>
<td>Yes</td>
<td>None</td>
</tr>
<tr>
<td>Action</td>
<td>Do not use this role. Not all interfaces support the Action role, and the role might be deprecated in the future.</td>
<td>Yes</td>
<td>None</td>
</tr>
</tbody>
</table>

See Also

Using graphical user interfaces to manage CAS server roles:
- Manage CAS Role Memberships (SAS Environment Manager) on page 4

Using the Access Control action set to manage CAS server roles:
Identity Management: Reference

Initial Users

sasboot Account

The sasboot account is an internal user account that is created during the deployment process. The account is known only to SAS. After the deployment process is completed, use this account to log on to SAS Environment Manager to Configure the Connection to Your Identity Provider and set up the administrative users.

The password for the account is expired by default. Each time the SASLogon service is started, a new URL is written to the service’s log which enables the password to be reset if necessary. The URL remains active for 24 hours. For security purposes, the URL also expires after you enter it in a browser, even if the password is not reset. For details, see, Sign In As the sasboot User

After you have set up the identity provider connection and the first administrative users, the sasboot account is generally used only if the connection to the identity provider fails. After performing the initial tasks, you should change the password. For additional security, you can then disable the password reset feature. This prevents password reset links from being written to the log each time the SASLogon service is started. Configure the Connection to Your Identity Provider.

Note: The sasboot account does not exist in a programming-only deployment.

Operating System Accounts

During deployment, two required accounts (one service account and one user account) and one group are created for you in the operating system, unless the accounts already exist. Because these accounts are required for running services during product operation, do not delete them or change their names. These accounts do not run as root. These accounts are host accounts and are not known to the identities service.

The following table identifies and describes the predefined accounts:

<table>
<thead>
<tr>
<th>Account Name and Group</th>
<th>Parameters</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>sas; member of sas group</td>
<td>Non-login service account without user restrictions. No password. You can add a password, if needed. The password does not expire. Any post-installation changes to this account do not prevent future software updates that use SAS RPM packaging.</td>
<td>This user account enables the required components to run, including the web application server for SAS Studio.</td>
</tr>
<tr>
<td>Account Name and Group</td>
<td>Parameters</td>
<td>Purpose</td>
</tr>
<tr>
<td>-----------------------</td>
<td>------------</td>
<td>---------</td>
</tr>
<tr>
<td>cas; member of sas group</td>
<td>Typical user account that is subject to user restrictions. No default password is assigned. <strong>Important</strong>: You must set a password for this account. The password eventually expires. You are prompted to set a new password. If the CAS server is running in a grid environment (with multiple CAS worker nodes), passwordless SSH is configured by default if you used an Ansible playbook for the deployment.</td>
<td>Required for managing the Cloud Analytic Services. Use this user account to log on to the CAS Server Monitor.</td>
</tr>
</tbody>
</table>

If you must log on to any of these accounts, use sudo to access them.

**Initial Rules for Access to Functionality**

SAS provides an initial set of rules to control your users’ access to functionality. In most cases, the initial rules provide a sufficient level of control. If (after gaining experience with SAS Viya) you identify the need for more granular control, you can adjust the rules.

**Initial Rules for All Authenticated Users**

All authenticated users can initially do the following:

- access selected functions within applications. For example, they can:
  - access the Dashboard, Data, and Content pages in SAS Environment Manager
  - access functionality in SAS Visual Analytics
- perform operations on folders and on the objects that the folders contain

To see the rules that provide this functionality, select Security ➤ Rules in SAS Environment Manager. Then filter by Principal, and specify Authenticated Users in the filter field.

**Initial Rules for SAS Administrators**

Users in the SAS Administrators custom group can initially access everything that is under the control of the general authorization system. For more information, see Predefined Custom Groups on page 9.

To see the rules that provide this functionality, select Security ➤ Rules in SAS Environment Manager. Then filter by Principal, and specify SASAdministrators in the filter field.

**Initial Rules for Other Predefined Custom Groups**

Users in other predefined custom groups can initially access selected functions within applications. For more information, see Predefined Custom Groups on page 9.

To see the rules that provide a group’s functionality, select Security ➤ Rules in SAS Environment Manager. Then filter by Principal, and specify the group ID in the filter field.

**Note**: In addition to the listed rules, authenticated users also receive any unopposed grants, and inherit rules from larger groups of which they are a part.
Identity Management: Troubleshooting

Sign In to SAS Studio

- Make sure the user’s account is known to the host of the SAS Studio web application. See *SAS Viya Administration: Authentication*.
- Examine the object spawner log. See *SAS Viya Administration: Logging*.
- If users cannot make a secure connection, see *Encryption in SAS Viya: Data in Motion*.

Access Cloud Analytic Services

- If the user cannot start a CAS session, make sure the user’s account meets all applicable requirements. See *SAS Viya Administration: Authentication*.
- If an error message in the CAS log states that the user "failed mid-tier authentication", the user’s credentials are not valid for your direct LDAP provider. See the discussion of dual authentication in *SAS Viya Administration: Authentication*.
- Ensure that users have a host account before adding them to the CASHostAccountRequired group. A member of the CASHostAccountRequired group without a host account cannot start the necessary CAS session.

Sign In to CAS Server Monitor

- Make sure the user’s account meets all applicable requirements. See *SAS Viya Administration: Authentication*.
- If an error message in the CAS log states that the user "failed mid-tier authentication", the user’s credentials are not valid for your direct LDAP provider. See the discussion of dual authentication in *SAS Viya Administration: Authentication*.
- If users cannot make a secure connection, see *Encryption in SAS Viya: Data in Motion*.

Access SAS Visual Data Builder

Make sure the user is a member of the Data Builders group (or the SAS Administrators group). See *Predefined Custom Groups on page 9*.

Administer SAS Home

Make sure the user is a member of the Application Administrators group (or the SAS Administrators group). See *Predefined Custom Groups on page 9*. 
User Management: Interfaces

In the following table, the shaded part of each circle is an approximation of the amount of user management functionality that a particular interface exposes. The shading indicates relative coverage. The shading does not indicate alignment of functional coverage across interfaces.

Interfaces for User Management

<table>
<thead>
<tr>
<th>Interface</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SAS Environment Manager</td>
<td>A graphical enterprise web application. See Identity Management How To on page 2.</td>
</tr>
<tr>
<td>CAS Server Monitor</td>
<td>A graphical web application that is embedded in the CAS server. See Manage CAS Role Memberships (SAS Environment Manager) on page 4.</td>
</tr>
</tbody>
</table>