SAS® Viya® 3.4 Administration: Identity Management

Identity Management: Overview

SAS identity management includes the following:

- managing the membership of custom groups and CAS roles
- giving users, groups, and custom groups access to SAS functionality

You can use SAS Environment Manager for most identity management tasks in full deployments. SAS Environment Manager is not available in programming-only deployments.

Familiarize yourself with the predefined custom groups and CAS server roles. Based on this information, determine which of your users to add to roles and each predefined custom group.

Identity Management: How To (SAS Environment Manager)

View User and Group Information

1 In the applications menu (☰), select **Administration** ⇨ **Manage Environment**. In the navigation bar, select .

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.
- Enter a string in the **Filter** field to search for identities within the category that you selected (Users, Groups, or Custom groups). To restore the complete list of identities, clear the filter field.
- Click an identity in the left pane to see its properties in the right pane. An identity's properties include the following:
  - profile picture (avatar) that is associated with the identity
  - basic properties including name, ID, title, 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 (other than memberships in custom 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. You can also create your own custom groups, which are useful if you do not want to (or do not 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  .

   The Edit Members window displays the custom group's current members 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  or double-click the identity.
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  or double-click the identity.
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 on. If the user is currently logged on, his or her 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  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.
   - Do not assign a custom group the ID of sasapp. SAS Viya reserves the group identifier `sasapp` for internal use by services.
   - Do not assign a custom group the ID of CASHostAccountRequired. CASHostAccountRequired is a reserved custom group name.

4

- Do not use an apostrophe (‘) in a custom group ID. The use of an apostrophe (‘) interferes with the use of that group’s identity on the **Users** page in SAS Environment Manager as well as accessing that group’s identity when working with authorization.
- 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 a custom group. To do so, click the existing group (or custom group) and select . Then you can 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 .

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 , and then click **Delete** in the confirmation window.

Manage CAS Role Memberships

For each CAS server, be 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.

Manage Direct Membership in the CAS Superuser Role

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

2 Right-click a CAS server, and select **Assume the Superuser role**.

3 Right-click the server again, and select **Settings**.

4 In the Superuser Role Membership section of the Server Settings window, click .

5 To add a member, do the following in the Select Identities window:

   a In the left pane, select **Users**.

   b In the left pane, click the name of a user. The user's properties are displayed in the far right pane.

   c Click  .

6 To remove a member, do the following in the Select Identities window:

   a 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.

   b Click  .

7 Click **OK**.

8 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 or to manage format libraries. To assume the Superuser role:

1 In the applications menu (☰), select **Administration** ⇨ **Manage Environment**. In the navigation bar, select  .

2 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 reminds you that you have assumed the role.

3 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 Profile Pictures (Avatars)

1 In the applications menu (☰), select **Administration** ⇨ **Manage Environment**. In the navigation bar, select  .

2 On the **Users** page, select **Users**, **Groups**, or **Custom groups** from the drop-down list in the toolbar.

3 On the **Users** page, enter a string in the **Filter** field to search for identities within the category that you selected (Users, Groups, or Custom groups). To restore the complete list of identities, clear the **Filter** field.

4 Click an identity in the left pane to see its properties in the right pane. The profile picture appears below the identity name.

5 To add a profile picture:

   a Click on the profile picture.

   b From the Edit Profile Picture window, select **Choose Picture** from the drop-down list.

c Navigate to the image that you want to use for the profile picture, and click **Open**.

6 To remove a profile picture:

a Click on the profile picture.

b From the Edit Profile Picture window, select **Remove** from the drop-down list.

c In the Remove Profile Picture confirmation window, click **Remove**.

7 Click **Save**.

Note: When you copy a group or custom group, the profile picture is not copied to the new group. If desired, you should assign a new profile picture to the new group.

Reload Identities Cache

1 In the applications menu (☰), select **Administration** ⇨ **Manage Environment**. In the navigation bar, select .

2 On the **Users** page, select ⋮ from the toolbar, and click **Reload Identities**.

3 A Reload Identities confirmation window appears with a warning that reloading the users and groups can take several minutes. Click **Yes** if you want to continue.

4 Monitor the identities log for information about the reload. Messages about when the reload starts and completes are produced at the Info level.

The identities log file is located here:

Table 1 *Identities Log File*

Linux	`/var/log/sas/viya/identities/default`
Windows	`\ProgramData\SAS\Viya\var\log\identities\default`

See Also

"Identities Synchronization" on page 20

Identity Management: How To (CAS Server Monitor)

Add or Remove CAS Role Members

Note: Starting with SAS Viya 3.4, CAS Server Monitor is available exclusively in programming-only deployments.

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

2 In the left navigation bar, select .

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 administrator (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.

   TIP 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**.

   Note: 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**.

   Note: 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).

See Also

CAS Server Roles on page 15

Identity Management: Access to Functionality

Overview

This section is about access to applications, features, services, and service endpoints.

Initially, access to functionality is distributed as follows:

SAS Administrators group	Provides access to all applications and features.
Other predefined groups	Provide access to certain specialized applications and features.
Authenticated Users (includes anyone who signs in)	Provides access to most applications and features.

If the initial distribution is appropriate, the only task is to assign users who need specialized or administrative access to the appropriate predefined groups.

If the initial distribution is not appropriate, you must expand or reduce access by working with authorization rules as follows:

- The basic approach is to make only limited changes to only the documented rules.
- The advanced approach can include making broader changes to the documented rules, modifying undocumented rules, and adding new rules.

  CAUTION! Managing access to functionality can be an extremely complex task. Use the advanced approach only if you have a thorough understanding of target URIs, the functionality that you want to limit, the effect of each permission, and the interactions with any related rules. Make sure you have a current backup before you begin. Test your changes to make sure they do not have unintended effects.

Basic Approach: Planning

Note: For SAS Visual Analytics 8.4 (August 2019 release) and later deployments, there is no SAS Report Viewer. This functionality has been included in SAS Visual Analytics. If you are running SAS Visual Analytics 8.4 (August 2019 release) or a later deployment, replace the /SASReportViewers/** object URI associated with the Report Viewer group with the /SASVisualAnalytics/** object URI as shown in this section.

Before making changes, make a plan.

- Determine how many levels or categories of access you need.
- Decide which object URIs fit each level or category. See documented rules.
- Identify or create a group for each access level or category.

Here are tips to help with planning:

- Make appropriate use of the Authenticated Users principal. Unless it is unacceptable for all authenticated users to have at least the lowest level of access, leave Authenticated Users as the principal in the rule (or rules) for the lowest level of access. Here are examples:
  - All users are implicitly members of Authenticated Users, so they can access SAS Report Viewer. If this is acceptable, you can leave the predefined grant of /SASReportViewer/** assigned to Authenticated Users. Users can access the report viewer without any administrative intervention.
  - All users are implicitly members of Authenticated Users, so they can access SAS Visual Analytics. If this is not acceptable, change the principal in the relevant grant rule (/SASVisualAnalytics/**) from Authenticated Users to a designated group.
  - If you want to hide other applications from Authenticated Users, you must change the principal in each relevant rule, so that access is no longer granted to Authenticated Users.

    CAUTION! **`Never prohibit Authenticated Users. Prohibiting Authenticated Users blocks access for all authenticated users. That block has absolute precedence. It cannot be mitigated by more specific grants.`** Instead, do not grant access to Authenticated Users. Any access that is not granted is implicitly denied.
- Take advantage of the group structure. To establish cumulative levels of access, make each higher-privilege group a member of the next-most-privileged group.

  For example, if your intent is to make applications menu items available as follows:

Menu Item	Report Viewer Group	Visual Analytics Group	Model Studio Group
View Reports (SAS Report Viewer)	✓	✓	✓
Explore and Visualize Data (SAS Visual Analytics)		✓	✓

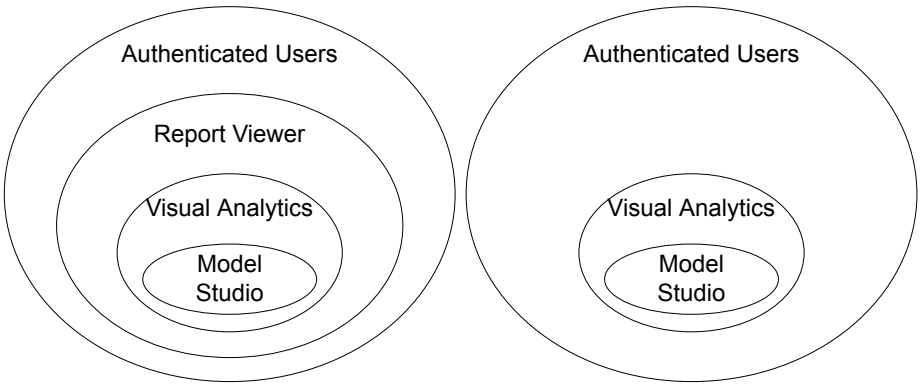
Menu Item	Report Viewer Group	Visual Analytics Group	Model Studio Group
Build Models (Model Studio)			✓

Then specify principals in authorization rules as follows:

Principal	Rule's Target objectURI
Report Viewer group	/SASReportViewer/** **Note:** For SAS Visual Analytics 8.4 (August 2019 release) and later deployments, replace the /SASReportViewers/** object URI associated with the Report Viewer group with the /SASVisualAnalytics/** object URI.
Visual Analytics group	/SASVisualAnalytics/** **Note:** For SAS Visual Analytics 8.4 (August 2019 release) and later deployments, replace the /SASVisualAnalytics/** object URI with the /SASVisualAnalytics_capabilities/edit object URI. This object URI is new beginning in SAS Visual Analytics 8.4.
Model Studio group	/ModelStudio/**

Or, if it is acceptable for all authenticated users to access SAS Report Viewer, omit the Report Viewers group.

The following figure depicts the membership structure for each approach:



- Be aware that modifying access to applications does not affect access to underlying services. For example, a user who cannot access SAS Environment Manager might still be able to access the folders service through another interface.
- To grant the same access to two distinct groups, make a copy of the original rule. Specify one group as the principal in the original rule and the other group as the principal in the new rule.
- Avoid use of prohibit rules. Instead, use selective grants to provide selective access.
- You do not have to add rules that grant access to the SAS Administrators group. That group has a universal grant.

Example of the Basic Approach to Modifying Access to Functionality

The basic approach to modifying access to functionality involves making limited changes to a documented rule. In this example, you reduce the availability of the SAS Visual Analytics web application (Explore and Visualize) so that it is available to only members of a designated group. The process involves creating or identifying an appropriate group and making that group the principal in the relevant rule.

Here are instructions:

1. In the documented rules list, find the URI for the rule that affects the functionality that you want to work with. In this example, you want to limit the ability to access SAS Visual Analytics, so the URI that you will be working with is /SASVisualAnalytics/**.
2. On the Users page, create or identify an appropriate group. Add the users for whom you want to grant the ability to access SAS Visual Analytics.
3. On the Rules page, locate and edit the rule (principal type, principal, description).
   a. In the applications menu (☰), select **Administration** ⇨ **Manage Environment**. In the navigation bar, select ⁞.
   b. Enter /SASVisualAnalytics/** in the field under **Object URI**, and click **Apply**.
   c. Select the rule, and click ✎.
   d. In the Edit Rule window, select `group` in the **Principal Type** field. In the **Principal** field, select the group that you just selected.
   e. In the **Description** field, update the description for the group for which you provided the ability to access SAS Visual Analytics.

      Click **Save**.
4. Verify that users who are in the group are able to access SAS Visual Analytics, and that users who are not in the group are not able to access SAS Visual Analytics.

   If a user has more access than is expected, make sure that there are no other rules that grant the same functionality (the same object URI) to another principal.

> **TIP** Add yourself as a member of the new group, and sign in without assuming your membership in the SAS Administrator's group.

Rules Reference

Here are rules for use with the basic approach to managing access to functionality. The following access rules are grouped by type of SAS Viya functionality. Except where otherwise specified, the functionality is initially granted to Authenticated Users. In most cases, the relevant permission is Read. For details and exceptions, see the rule properties in SAS Environment Manager.

Access Applications

Table 2 *Object URIs for Accessing Applications*

Application or Function	Object URI
SAS Environment Manager (all functionality)[1]	/SASEnvironmentManager/**
SAS Environment Manager (gatekeeper)	/SASEnvironmentManager/
SAS Graph Builder	/SASGraphBuilder/**
SAS Visual Analytics App	/SASMobileBI/**
SAS Report Viewer[3]	/SASReportViewer/**
SAS Theme Designer[2]	/SASThemeDesigner/**
SAS Visual Analytics	/SASVisualAnalytics/**
SAS Data Explorer	/SASDataExplorer/**
SAS Data Studio[4]	/SASDataStudio/**
Authorization dialog from SAS Drive[1]	/authorizationDialog
SAS Drive	/SASDrive/**
Model Studio	/ModelStudio/**

[1]Initially granted to SAS Administrators.

[2]Initially granted to SAS Application Administrators.

[3]Available in releases prior to SAS Visual Analytics 8.4 (August 2019 release).

[4]Initially granted to Data Builders.

Table 3 *Object URIs for Page-Level Rules in SAS Environment Manager*

Application or Function	Object URI	Access Rule Exists
Dashboard page in SAS Environment Manager	/SASEnvironmentManager/dashboard	✓
Data page in SAS Environment Manager	/SASEnvironmentManager/data	✓
Servers page in SAS Environment Manager	/SASEnvironmentManager/servers	✓
Content page in SAS Environment Manager	/SASEnvironmentManager/content	✓
Users page in SAS Environment Manager	/SASEnvironmentManager/identities	

Application or Function	Object URI	Access Rule Exists
Licensed Products page in SAS Environment Manager(only present in multi-tenant environments)	/SASEnvironmentManager/licenses	
Tenants page in SAS Environment Manager	/SASEnvironmentManager/tenants	
Configuration page in SAS Environment Manager	/SASEnvironmentManager/configuration	
Contexts page in SAS Environment Manager	/SASEnvironmentManager/contexts	
User Defined Formats page in SAS Environment Manager	/SASEnvironmentManager/udf	
Logs page in SAS Environment Manager	/SASEnvironmentManager/logs	
Machines page in SAS Environment Manager	/SASEnvironmentManager/machines	
Jobs page in SAS Environment Manager	/SASEnvironmentManager/jobs	✓
Domains page in SAS Environment Manager	/SASEnvironmentManager/domains	
My Credentials page in SAS Environment Manager	/SASEnvironmentManager/credentials	✓
Mobile Devices page in SAS Environment Manager	/SASEnvironmentManager/devices	
Rules page in SAS Environment Manager	/SASEnvironmentManager/rules	
Publishing Destinations page in SAS Environment Manager	/SASEnvironmentManager/destinations	

Interact with Reports and Data

For additional information about how to adjust rules associated with accessing data that is imported from social media, see "Controlling Access to Features" in *SAS Data Explorer: User's Guide*.

Action	Object URI
Create and edit reports.[1]	/SASVisualAnalytics_capabilities/edit
Import reports.	/importVASpk/**
Upload data files (via casManagement service).	/casManagement/servers/*/caslibs/*/tables

Action	Object URI
Access the **Import** window.	/casManagement_capabilities/importData
Export reports as PDF.	/reportRenderer/reports/**
Export data from reports.	/reportData_capabilities/exportData
Export detail data from reports.	/reportData_capabilities/exportDetailData
Create jobs to obtain report images (for example, thumbnails and section images).	/reportImages/jobs/**
Export report images from SAS Visual Analytics and web or mobile viewers.	/SASVisualAnalyticsCommon_capabilities/exportImage
Email or share report images from SAS Visual Analytics and web or mobile viewers.	/SASVisualAnalyticsCommon_capabilities/shareReport
Subscribe to report alerts.	/reportAlerts/**
Evaluate text templates.	/reportImages/textTemplateOutput
Manage report states for reports.	/reports/reports/*/states
Access imported Facebook data. **Note:** See the SAS Note for this feature.	/webDataAccess_capabilities/facebookImport
Access imported Google Drive data.	/webDataAccess_capabilities/googledriveImport
Access imported Google Analytics data.	/webDataAccess_capabilities/googleanalyticsImport
Access imported YouTube data.	/webDataAccess_capabilities/youtubeImport
Access imported Twitter data. **Note:** See the SAS Note for this feature.	/webDataAccess_capabilities/twitterImport
Manage comments.	/comments/**
Create models in SAS Visual Analytics.	/SASVisualAnalytics_capabilities/buildAnalyticalModel

[1]Available in SAS Visual Analytics 8.4 (August 2019 release) and later deployments.

Manage Jobs

Action	Object URI
Schedule jobs.[1]	/jobExecution/jobRequests/* /jobExecution/jobRequests/*/
Edit scheduled jobs.	/scheduler/jobs/**
Monitor jobs.	/jobExecution/jobs/**

[1]Both of the object URIs are required.

Manage Geo

Action	Object URI
Add a custom map provider.[1]	/maps/providers
Manage custom map providers (update and delete).[1]	/maps/providers/*
Use the ESRI service.	/webDataAccess/esri/user/token

[1]Initially granted to SAS Administrators.

Manage Mobile

The following table lists only the object URIs that are specific to mobile devices. You might need to work with other object URIs to manage mobile devices. For additional information about rules that affect the SAS Visual Analytics App and the SAS Software Development Kits (SDKs), see "Rules and Descriptions" in *SAS Viya Administration: Mobile*.

Action	Object URI
Cache mobile report data.	/SASMobileBI_capabilities/cacheMobileReportData
Exempt from offline time-out.	/SASMobileBI_capabilities/exemptFromOfflineTimeLimit
Exempt from requirement to enter passcode.	/SASMobileBI_capabilities/ exemptFromPasscodeRequirements
Manage mobile device blacklist, whitelist, and device access history.[1]	/deviceManagement_capabilities/manageMobileDevices
Enable natural language processing.	/reportViewerNaturalLanguageUnderstanding/ interpretations
Render reports with web content.	/SASMobileBI_capabilities/allowWebContent

[1]Initially granted to SAS Administrators.

Manage SAS Drive

The object URIs in the following table are available in SAS Visual Analytics 8.4 (August 2019 release) and later deployments.

Item	Object URI
Access the Welcome tour.	/SASDrive_capabilities/allowWelcomeTourMenu
Launch the Welcome tour.	/SASDrive_capabilities/allowWelcomeTour
Create the **SAS Videos** folder.	/SASDrive_capabilities/allowSASVideo

Item	Object URI
Add the **SAS Video** shortcuts.	/SASDrive_capabilities/allowSASVideoLinks
Upload content files.	/SASDrive_capabilities/allowUpload
Download content files.	/SASDrive_capabilities/allowDownload

Personal Folders and Preferences

Item	Object URI
Set preferences.	/preferences/preferences/@currentUser/**
Access personal history folder.	/folders/folders/@myHistory
Manage personal favorites folder.	/folders/folders/@myFavorites

Identity Management: CAS Roles

Superusers have permission-exempt access to CAS (with the exception of access to data) 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.

Note: The following built-ins actions for SAS Cloud Analytics Services require a user ID that can assume the Superuser role:

- addNode
- installActionSet
- refreshLicense
- removeNode
- shutdown

For more information about the built-ins actions for SAS Cloud Analytics Services, see Builtins Action Set: Details.

Role	Description	Initial Members
Superuser	Provides permission-exempt 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 each CAS server has at least one other designated Superuser. **Note:** By default, the users that are assigned this role have permission-exempt access to metadata. However, they do not have permission-exempt access to data (CAS libraries). To give users with this role permission-exempt access to data, you must modify access controls to explicitly grant them access.	SAS Administrators Process owner for the server Backup Administrator (sas.deploymentBackup) Report Distribution Service administrator account (sas.reportDistribution) Report Images Service administrator account (sas.reportImages) Scheduler Service administrator account (sas.scheduler) Report Alerts Service administrator account (sas.reportAlertsEval) VSD Service administrator account (sas.svi-vsd-service)
Data	Assign members to this role only if you have users who should have permission-exempt access to metadata but should not be able to perform all administrative tasks. Not all interfaces support the Data role. **Note:** By default, the users that are assigned this role have permission-exempt access to metadata. However, they do not have permission-exempt access to data (CAS libraries). To give users with this role permission-exempt access to data, you must modify access controls to explicitly grant them access.	None
Action	Do not use this role. Not all interfaces support the Action role.	None

Note: The Data role provides a subset of the abilities of the Superuser role. You cannot be a member of both the Superuser role and the Data role in the same session.

See Also

- Manage CAS Role Memberships in SAS Environment Manager
- Add or Remove CAS Role Members in CAS Server Monitor

Identity Management: Reference

Initial Users

sasboot Account

The sasboot account is an internal user account that is created during the deployment process. For details, see the deployment guide for Linux, or the deployment guide for Windows.

Note:

The sasboot account exists only in a full deployment. A full deployment includes all of the software to which you are entitled, whereas a programming-only deployment excludes SAS Drive, SAS Environment Manager, and most graphical user interfaces, and most services.

Operating System Accounts

Some user and service accounts are required on the operating system during deployment. For details, see Linux accounts and Windows accounts.

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. can also create your own custom groups. This feature is useful for creating new groups of SAS users if you do not want to (or do not have permission to) create groups in your identity provider.

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

Assumable Custom Groups

The SAS Administrators group is a predefined custom group. This group is *assumable*. When a user in this group signs in to SAS 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

Predefined Custom Groups

Certain 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.

- The custom groups effectively implement a role within SAS Viya. The members of the custom groups have access to privileges associated with the role. Search on the Rules page by the group name to see all privileges that are associated with the role.
- The predefined groups below are a part of a deployment that contains SAS Visual Analytics, SAS Visual Statistics, and SAS Visual Data Mining and Machine Learning. Some products and solutions have additional predefined groups. See the documentation for these products and solutions for information about other predefined groups.

  For example, if you have SAS Data Studio, then you have a predefined group called Data Builders. This group is not assumable, and there are no initial members.

The custom groups are as follows:

SAS Administrators
  Have access to the following:

  - all functionality that is controllable through authorization rules.
  - all folders and all objects that the folders contain (for example, plans and reports).

  Is an assumable group.

  Members can assume the CAS Superuser role.

  Note: Access to data (caslibs) is not included. For example, users in this group can create, run, and view reports only if they have explicitly been granted access to the underlying data.

Esri Users
  Can access Esri systems for geo map access.

  Is not an assumable group.

  Has no initial members.

  Note: Esri requires that organizations pay for tokens to use the Esri geographic mapping services. You can add a user or group of users to the Esri Users group to control who has access to these tokens. Therefore, you can control the cost of using Esri geographic services.

Application Administrators
  Can access selected administrative functions within applications.

  Is not an assumable group.

  Has no initial members.

Note: An additional custom group is predefined, but not created. If you create a group with ID: *CASHostAccountRequired*, members of this group automatically run their CAS sessions under their own host account. By default, CAS sessions run using the **cas** account. For more information, see CASHostAccountRequired custom group on page 18.

The CASHostAccountRequired Custom Group

Note: The CASHostAccountRequired custom group is not applicable in a Windows deployment.

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

Here are additional details about the CASHostAccountRequired custom group:

- Members of this group must have host accounts.
- If a user is a member of the CASHostAccountRequired custom group, but has no host account, then SAS Environment Manager cannot access information about the CAS Server. You might observe the following behavior:

- From SAS Environment Manager, the CAS server appears to be down even though it is not. No libraries or tables are displayed.
- From SAS Data Studio, you receive a `connection refused` or `access denied` error message when you attempt to select a CAS server.

- When you modify the membership of this group, the users that have been added or removed must log off from their sessions before the changes can take effect.
- All data associated with a user's caslib is stored in a specific CASUSER path location on the CAS controller. This location changes if the user is added as a member of the CASHostAccountRequired group:

Table 4 *CASUSER Path Location*

User Scenario	CASUSER Path Location	Session Information
User starts CAS sessions from visual interfaces (includes all SAS Viya interfaces except SAS Studio 4 and Base SAS or SPRE sessions), and user is not a member of the CASHostAccountRequiredGroup. This is the default behavior.	**CASDATADIR/ casuserlibraries/*username***	Sessions run under the CAS server user (cas). The directory and all files within it are owned by the cas user.
User starts CAS sessions from visual interfaces (includes all SAS Viya interfaces except SAS Studio 4 and Base SAS or SPRE sessions), and user is a member of the CASHostAccountRequiredGroup.	**$HOME/casuser**	Sessions run under the user's host account.
User starts CAS sessions from SAS Studio 4, Base SAS, or SPRE, regardless of whether the user is a member of the CASHostAccountRequiredGroup.	**$HOME/casuser**	SAS Studio 4, Base SAS, and SPRE sessions always run under the user's host account, and use the **$HOME/ casuser** CASUSER path location. Sessions run under the CAS server user (cas). The directory and all files within it are owned by the cas user.

If a user is added to the CASHostAccountRequired custom group, the next CAS session that is started for that user will use **$HOME/casuser** for the CASUSER path location. If this user needs to maintain access to any user files that were stored in the default CASUSER path location:

- An administrator must copy the files from the default CASUSER path location **CASDATADIR/ casuserlibraries/*username*** to **$HOME/casuser**.

  Note: If a user is removed from the CASHostAccountRequired group, files should be copied in the opposite direction.
- An administrator must adjust the permissions on the files so that the user can access them. Prior to the user being added to the CASHostAccountRequired custom group, the CAS user owned the files, and performed all read or write actions.

See Also

"Manage Custom Groups" on page 3

Identities

Identity Filtering

When configuring the connection to your identity provider, you should specify a filter to limit the identities that SAS Viya returns. For example, you can create a filter to exclude identities whose accounts are disabled or expired, or to exclude objects that represent computer resources rather than actual users or groups. You can modify this filter at any time.

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.

A default filter is provided for sites that use Active Directory. If you use another identity provider such as openLDAP, then you might need to modify the default filter. For more information about the default filter, see "Identities Service" in *SAS Viya Administration: Configuration Properties*.

Note: Identity filtering does not apply in a programming-only deployment.

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*.

Note: Identity caching does not apply in a programming-only deployment.

Identities Synchronization

Information about LDAP identities is available in SAS Environment Manager, and is synchronized with the SAS Infrastructure Data Server (PostgreSQL) periodically. The amount of time between each synchronization is determined by a configuration option, which is set to 12 hours by default.

If you want to manually synchronize the identities at any time, you can reload the identities on page 6. Note that reloading the set of users and groups can take several minutes to complete.

Identities Properties That Require LDAP Attributes

In order for the Identities service to function properly, the following identities properties must be assigned valid LDAP attributes:

sas.identities.providers.ldap.connection
- host
- port
- password
- userDN

sas.identities.providers.ldap.group
- accountId
- baseDN[1]
- distinguishedName
- member

memberOf

objectClass

objectFilter

searchFilter

sas.identities.providers.ldap.use
accountId

baseDN[1]

distinguishedName

memberOf

objectClass

objectFilter

searchFilter

[1] If you are in an Active Directory environment, this is the only required LDAP attribute for this group. Default values are provided for the other properties.

Note: The default values are valid for most implementations of Microsoft Active Directory. For other LDAP providers, such as OpenLDAP, you must provide different values for some fields. For all LDAP providers, we recommend that you review the values for the required LDAP attributes to ensure that they are configured correctly.

See Also

- "Identities Service" in *SAS Viya Administration: Configuration Properties*

Identity Management: Guidelines

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 custom rules that you created still exist. Manually delete such rules.
- As you plan your group structure, remember that you can use a group for either or both of these purposes:
  - To make shared resources available to multiple users. For example, you might use a group as the principal in an authorization rule, or you might store shared credentials for a group.
  - As a parent to other groups. For example, if groupA and groupB should have identical access to multiple resources, you might assign both groups to a parent group, and grant access to the parent group.

  Note: When you design a group structure, consider both clarity (Will others be able to interpret the structure?) and conciseness (Is the structure as minimal as possible?). In a complex authorization model, you might prioritize clarity, using more than the strict minimal number of groups, and giving each group a name that describes its purpose.

Identity Management: Troubleshooting

Cannot Sign In to SAS Studio

- Ensure that 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.

Cannot Access Cloud Analytic Services

- If the user cannot start a CAS session, ensure that 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.

Cannot Sign In to CAS Server Monitor

Note: Starting with SAS Viya 3.4, CAS Server Monitor is available exclusively in programming-only deployments.

- Ensure that 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.

Cannot View Users and Group Members

If you receive the following error while viewing users, groups, or their memberships from SAS Environment Manager or any other client, then a referral might have been encountered. SAS Viya does not process LDAP referrals.

Here is an example of this error message:

```
Load Users
An error occurred loading the list of users.
exception:
org.springframework.ldap.PartialResultException
Caused by: javax.naming.PartialResultException: Unprocessed Continuation
Reference(s); remaining name 'DC=COMPANY,DC=COM'
```

This occurs because LDAP is initialized based only on what the Identities service itself configures. Therefore, any environment variables that are set will not be processed. Connecting to the global catalog might be a viable solution.

Cannot Access Esri Geographic Mapping Resources

Ensure that the user is a member of the Esri Users group. Users that are members of the Esri Users group have access to tokens for which there is a fee. See "Esri Users" on page 18.

Cannot Retrieve List of Users or Groups

If the following error occurs while attempting to retrieve a list of users or groups that are defined in your environment, then this is due to a failed LDAP search by the Identities service:

```
[LDAP: error code 12- Unavailable Critical Extension]
```

The Identities service attempted an LDAP search for a collection of users or groups, but the request failed because the LDAP server does not support paged queries.

To resolve this, follow these steps to change the value of the **`sas.identities.providers.ldap.pagedResults`** configuration property:

1. Log on to SAS Environment Manager as an administrator.
2. Navigate to the Configuration page. From the **View** drop-down list, select **Definitions**. In the **Filter** field, enter *sas.identities.providers.ldap*.
3. From the **Identities service** drop-down list on the right pane, click  . Change the **`pagedResults`** property to **`off`**.
4. Click **Save**.

Cannot Update User Information

Any service or application that uses the Identities service pulls the associated user information from the LDAP server directly. Therefore, user information such as phone number, work address, and email address cannot be updated in SAS Viya, but must be updated in LDAP.

For example, to specify a different email address to receive SAS Visual Analytics alerts, the email address field must be updated directly in LDAP.

Cannot Log In to SAS

Ensure that no two users have the same email address in LDAP. Users might have problems logging in to SAS if another user has the same email address.

Membership in a sasapp LDAP, Custom, or Host Group Is Ignored

SAS Viya reserves the group identifier **`sasapp`** for internal use by services. Only services are members of the privileged internal group **`sasapp`**. If you also have a **`sasapp`** host group, LDAP group, or custom group, unintended results can occur. Descriptive information (such as the Authorization window and the Users page in SAS Environment Manager) reflects membership in the group. However, actual access does not reflect membership in the group. Here are details:

- When a user who is a member of a **sasapp** LDAP or custom group signs in to SAS Viya, SAS Logon Manager discards the user's **sasapp** membership information, excluding it from the user's OAuth token. By discarding that membership information, SAS Logon Manager ensures that the privileges of the **sasapp** internal group are not made available to users.
- If you specify the **sasapp** group as the principal in a general authorization rule, that rule affects only the **sasapp** internal group.
- When a user who is a member of a **sasapp** host group authenticates to CAS, CAS alters its copy of the user's membership information, replacing the **sasapp** group name with the group ID. By altering that membership information, CAS ensures that the privileges of the internal group **sasapp** are not made available to users.
- If you specify the **sasapp** group as the principal in a CAS access control, that access control affects only the **sasapp** internal group.

  Note: SAS Viya does not currently prevent the creation of a **sasapp** custom group. SAS Viya cannot prevent the creation of a **sasapp** host or LDAP group.

Identity 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.

● SAS Environment Manager	A graphical enterprise web application. See "Identity Management: How To (SAS Environment Manager)".
◕ CAS Server Monitor	A graphical web application that is embedded in the CAS server. See "Identity Management: How To (CAS Server Monitor)" on page 6.
◕ Access Control action set	A programmatic interface for SAS (the CAS procedure), Python, R, and Lua. See Access Control Action Set.
◕ Command-line interface	A simple scriptable interface that provides commands for managing identities. See "CLI Examples: Identities" in *SAS Viya Administration: Using the Command-Line Interfaces*.