THE POWER TO KNOW®

SAS® Viya® 3.3 Administration: Identity Management

Identity Management Overview

User and 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.

SAS identity management is not used in a programming-only deployment. In such deployments, your operating system user management is used.

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

Note: 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 directly, but must be updated directly 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.

Getting Started with Identity Management

After deploying, perform these tasks to set up your identities.

Give Other Users Specialized Access

In the initial deployment, authenticated users automatically have access to functionality that is appropriate for a typical user. See “Initial Rules for All Authenticated Users” on page 21.

To give additional functionality to special categories of users (for example, administrative users), follow these steps:

1. Become familiar with the predefined custom groups and their associated levels of functionality. See “Predefined Custom Groups” on page 11 and “Access to Functionality” on page 13.
2. Become familiar with the CAS server roles. See “CAS Server Roles” on page 19.
3. Based on this information, determine which of your users and groups to add to each role and each predefined custom group.
4. Add users and groups to the appropriate custom groups. See “Add or Remove Custom Group Members” on page 3 .
5. Add users and groups to the appropriate CAS server roles. See “Manage CAS Role Memberships” on page 5.

Give Users Access to Data and Content

You use the SAS Viya authorization layer to give users access to the data and content that they need to do their jobs. See Authorization Orientation for more details.

See Also

- *SAS Viya Administration: Orientation to Authorization*

Identity Management How To

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 **Search** 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 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 (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, 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 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 ⇨.

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 ⇦.

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 to SAS Environment Manager. 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.

There are many uses of custom groups, but there is one specific use-case to be aware of. By default, authenticated users who launch a CAS session will do so as the `cas` account. Files generated in such a session are saved in a folder belonging to the cas account, but in a directory path that includes the user's ID. If you prefer users to launch CAS sessions under their own account to cause their files to be saved to their UNIX directories, create and populate a custom group with ID *CASHostAccountRequired*. When members of the CASHostAccountRequired group launch a CAS session, that session runs under that user's host account, and the generated files are created under the user's home directories.

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.

   CAUTION! 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.

   > **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 ⧉. 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 ✎.

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 CAS Server Monitor, you can also designate users 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 (in SAS Environment Manager)

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

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 ✎.

6 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 ➕.

7 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 ⬅.

8. Click **OK**.

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

Add or Remove CAS Role Members (in CAS Server Monitor)

The CAS (Superuser) role provides unrestricted access to all CAS objects and actions within the associated CAS server. Members of the SAS Administrators group have access to all tasks, folders, objects, and application functionality.

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**. 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).

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

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 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 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 11.

Note: To manage access to CAS administrative functionality separately, see “CAS Server Roles” on page 19.

See Also

- “Access to Functionality” on page 13
- “Initial Rules for Access to Functionality” on page 21
- “SAS Viya Administration: General Authorization” in SAS Viya Administration: General Authorization

Adjust Rules for Access to Functionality

You might identify the need for more granular control, based on your organization’s use of SAS Viya. If so, 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 the applications menu (≡), select **Administration** ⇨ **Manage Environment**. In the navigation bar, select ☷.

2 Select **Authenticated Users** in the **Principal** drop-down box, and click **Apply**.

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, update the description for 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 is 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 the applications menu (☰), select **Administration** ⇨ **Manage Environment**. In the navigation bar, select ▤.

2 Clear any previously selected principals in the **Principal** drop-down box, and select **Add Identities**.

3 Choose **Custom Groups** from the drop-down box on the Select Identities page. Enter the ID of the predefined custom group (for example, `SASAdministrators`) in the **filter** field.

4 Click ➕.

5 Click **OK**.

6 From the Rules page, select the custom group that you just added from the **Principal** drop-down box. Click **Apply**.

7 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.

8 Select the rule, and click ✎.

9 In the **Principal type** field, select **group**. Then select the appropriate group or custom group in the **Principal** field.

10 In the **description** field, update the description for the name of the group for which you provided access.

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

11 Click **Save**.

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

Grant a Function to an Additional Group

By default, an authorization rule can have only one principal. If you need to grant the functionality of an authorization rule to an additional group of users, follow these steps to copy the rule and assign a new principal:

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

2 Locate the rule that you want to provide an additional group access to. From the ObjectURI window, select the rule and click ⧉.

3 In the **Principal type** field, select **group**. Then select the appropriate group or custom group for whom you want to grant access in the **Principal** field.

4 In the **Description** field, update the description for the name of the group for which you provided access.

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

5 Click **Save**.

See Also

- "CLI Examples: Identities" in SAS Viya Administration: Command-Line Interfaces

User 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 custom rules that you created still exist. Manually delete such rules.

Note: In order to prevent problems with logins, no two users should have the same email address in LDAP.

Identity Management Concepts

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, see "Sign In as the sasboot User" in SAS Viya for Linux: Deployment Guide.

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. See "Post-Installation Tasks" in SAS Viya for Linux: Deployment Guide.

Note:

The sasboot account exists only in a Full 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.

The following table identifies and describes the predefined accounts:

Account Name and Group	Parameters	Purpose
sas; member of sas group	UID: 1001 Group ID: 1001 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.	This user account enables the required components to run, including the web application server for SAS Studio.
cas; member of sas group	UID: 1002 Group ID: 1001 Typical user account that is subject to user restrictions. No default password is assigned. **Important**: 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.	Required for managing the Cloud Analytic Services. Use this user account to log on to the CAS Server Monitor.

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

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

The SAS Identities service configuration has default values appropriate for Microsoft Active Directory. 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, port, and connection credentials. 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

- “Post-Installation Tasks” in SAS Viya for Linux: Deployment Guide
- “Identities Service” in SAS Viya Administration: Configuration Properties

Identity Filtering

When configuring 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 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.

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 do not want to (or do not 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: 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.

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

SAS Administrators

Have access to the following::

- all tasks in SAS Environment Manager and CAS Server Monitor.
- all folders and all objects that the folders contain (for example, plans and reports).

Is an assumable group.

Members of CAS Superuser role are initial members.

Note: Access to data (CAS libraries) 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 the following items from SAS Home:

- Publish Tile
- Manage Published
- SAS Theme Designer

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 “The CASHostAccountRequired Custom Group” on page 13.

Assumable Custom Groups

The SAS Administrators group is a predefined custom group. This group is *assumable*. When a user in an *assumable* group signs in to SAS Viya, a prompt appears asking `Do you want to opt in to all of your assumable groups?` A list of assumable groups to which the user belongs appears below the prompt.

If the user selects **Yes**, the user gets the extra permissions that are associated with the assumable groups. 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 automatically run their CAS sessions under their own host account. By default CAS sessions run using the `cas` account.

Therefore, members of this group must have host accounts.

Note: 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.

If a user has previously created sashdat files and is then added to the CASHostAccountRequired custom group, the user 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 the sashdat files as the location of these files is different for members of this group. Users in this situation should copy the 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 user name 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 3
- "Access to Functionality" on page 13
- "Initial Rules for Access to Functionality" on page 21

Access to Functionality

Introduction

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 19.

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 user's 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 21
- "Adjust Rules for Access to Functionality" on page 7

Supported Adjustments to Existing Rules

CAUTION! For rules that affect access to functionality, only certain modifications to certain rules are supported. Do not modify rules that target a service, service endpoint, media type, or pseudo URI, except as specified in this topic. For instructions, see "Adjust Rules for Access to Functionality".

You can make these modifications to the following functionality rules:

- replace the principal
- update the description
- copy a rule in order to create a new rule with a changed principal.

Table A.1 Rules

Target object URI: `/deviceManagement_capabilities/manageMobileDevices` Original principal type: Group Original principal ID: SASAdministrators Original granted permissions: Delete,Read,Create,Update Affected functionality: Manage the mobile device blacklist, whitelist, and device access history.
Target object URI: `/SASEnvironmentManager/**` Original principal type: Group Original principal ID: SASAdministrators Original granted permissions: Read Affected functionality: Access all functionality in SAS Environment Manager.
Target object URI: `/SASEnvironmentManager/` Original principal type: authenticated-users Original principal ID: Original granted permissions: Read Affected functionality: Access SAS Environment Manager.

Target object URI: `/SASEnvironmentManager/dashboard`

Original principal type: authenticated-users

Original principal ID:

Original granted permissions: Read

Affected functionality: Access the **Dashboard** page in SAS Environment Manager.

Target object URI: `/SASEnvironmentManager/data`

Original principal type: authenticated-users

Original principal ID:

Original granted permissions: Read

Affected functionality: Access the **Data** page in SAS Environment Manager.

Target object URI: `/SASEnvironmentManager/content`

Original principal type: authenticated-users

Original principal ID:

Original granted permissions: Read

Affected functionality: Access the **Content** page in SAS Environment Manager.

Target object URI: `/SASEnvironmentManager/scheduling`

Original principal type: authenticated-users

Original principal ID:

Original granted permissions: Read

Affected functionality: Access the **Scheduling** page in SAS Environment Manager.

Target object URI: `/SASMobileBI/**`

Original principal type: authenticated-users

Original principal ID:

Original granted permissions: Read

Affected functionality: Access SAS Mobile BI.

Target object URI: `/SASMobileBI_capabilities/cacheMobileReportData`

Original principal type: authenticated-users

Original principal ID:

Original granted permissions: Read

Affected functionality: Cache mobile report data from within the SAS Mobile BI application. This is required for offline access to reports. For users who do not have this capability, report data is retained only on the device while the report is open.

Target object URI: `/SASMobileBI_capabilities/exemptFromOfflineTimeLimit`

Original principal type: authenticated-users

Original principal ID:

Original granted permissions: Read

Affected functionality: Provides exemption from the SAS Mobile BI offline time-out.

Target object URI: `/SASMobileBI_capabilities/exemptFromPasscodeRequirements`

Original principal type: authenticated-users

Original principal ID:

Original granted permissions: Read

Affected functionality: Provides exemption from the requirement to enter a passcode to access the SAS Mobile BI application.

Note:

If any of the mobile server connections require a passcode, then it will still be required to access the application. This is true even if the exemption rule is in effect. In addition, users can enable a passcode even if the exemption rule is in effect.

Target object URI: `/importVASpk/**`

Original principal type: authenticated-users

Original principal ID:

Original granted permissions: Delete,Read,Create

Affected functionality: Import reports.

Target object URI: `/SASReportViewer`

Original principal type: authenticated-users

Original principal ID:

Original granted permissions:,Read

Affected functionality: Access SAS Report Viewer.

Target object URI: `/SASThemeDesigner/**`

Original principal type: Group

Original principal ID: ApplicationAdministrators

Original granted permissions: Read

Affected functionality: Access SAS Theme Designer.

Target object URI: `/SASVisualAnalytics`

Original principal type: authenticated-users

Original principal ID:

Original granted permissions: Read

Affected functionality: Access SAS Visual Analytics.

Target object URI: `/SASVisualAnalytics_capabilities/buildAnalyticalModel`

Original principal type: authenticated-users

Original principal ID:

Original granted permissions: Read

Affected functionality: Create and modify analytical models in SAS Visual Analytics.

Target object URI: `casManagement/servers/*/caslibs/*/tables`

Original principal type: authenticated-users

Original principal ID:

Original granted permissions: Create

Affected functionality: Upload data files through the casManagement service.

Target object URI: `/casManagement_capabilities/importData`

Original principal type: authenticated-users

Original principal ID:

Original granted permissions: Read

Affected functionality: Access the Import Data window.

Target object URI: `/webDataAccess/esri/user/token`

Original principal type: Group

Original principal ID: EsriUsers

Original granted permissions: Read,Create

Affected functionality: Use the Esri service.

Target object URI: `/reportRenderer/reports`

Original principal type: Authenticated Users

Original principal ID:

Original granted permissions: Delete, Create, Read, Update, Remove

Affected functionality: Export PDF.

Target object URI: `/preferences/preferences/@currentUser`

Original principal type: Authenticated Users

Original principal ID:

Original granted permissions: Delete, Create, Read, Update

Affected functionality: Set preferences.

Target object URI: `/folders/folders/@myHistory`

Original principal type: Authenticated Users

Original principal ID:

Original granted permissions: Delete, Secure, Create, Read, Update, Add, Remove

Affected functionality: Access personal history folder.

Target object URI: `/folders/folders/@myFavorites`

Original principal type: Authenticated Users

Original principal ID:

Original granted permissions: Delete, Secure, Create, Read, Update, Add, Remove

Affected functionality: Manage personal favorites folder.

Target object URI: `/comments/**`

Original principal type: Authenticated Users

Original principal ID:

Original granted permissions: Read, Create, Delete, Update

Affected functionality: Manage comments.

Target object URI: `/reportImages/jobs`

Original principal type: Authenticated Users

Original principal ID:

Original granted permissions: Create, Read

Affected functionality: Create jobs to obtain report images (thumbnails, section images).

Target object URI: `/reportData_capabilities/exportData`

Original principal type: Authenticated Users

Original principal ID:

Original granted permissions: Read

Affected functionality: Export data from reports.

Target object URI: `/reportData_capabilities/exportDetailData`

Original principal type: Authenticated Users

Original principal ID:

Original granted permissions: Read

Affected functionality: Export detail data from reports.

Target object URI: `/SASVisualAnalyticsCommon_capabilities/exportImage`

Original principal type: Authenticated Users

Original principal ID:

Original granted permissions: Read

Affected functionality: Export report images from SAS Visual Analytics and web or mobile report viewers.

Target object URI: `/SASVisualAnalyticsCommon_capabilities/shareReport`

Original principal type: Authenticated Users

Original principal ID:

Original granted permissions: Read

Affected functionality: Email or share reports from SAS Visual Analytics and web or mobile report viewers.

Target object URI: `/maps/providers`

Original principal type: SAS Administrators

Original principal ID:

Original granted permissions: Create

Affected functionality: Add custom map provider.

Target object URI: `/maps/providers/*`

Original principal type: SAS Administrators

Original principal ID:

Original granted permissions: Delete, Update

Affected functionality: Manage custom map providers (update, delete).

Target object URI: `/reportAlerts/*`

Original principal type: Authenticated Users

Original principal ID:

Original granted permissions: Delete, Secure, Create, Read, Update, Add, Remove

Affected functionality: Subscribe to report alerts.

Target object URI: `/webDataAccess_capabilities/facebookImport`

Original principal type: Authenticated Users

Original principal ID:

Original granted permissions: Read

Affected functionality: Access import Facebook data.

Target object URI: `/webDataAccess_capabilities/googledriveImport`

Original principal type: Authenticated Users

Original principal ID:

Original granted permissions: Read

Affected functionality: Access import Google Drive data.

Target object URI: `/webDataAccess_capabilities/twitterImport`

Original principal type: Authenticated Users

Original principal ID:

Original granted permissions: Read

Affected functionality: Access import Twitter data.

Target object URI: `/webDataAccess_capabilities/googleanalyticsImport`

Original principal type: Authenticated Users

Original principal ID:

Original granted permissions: Read

Affected functionality: Access import Google Analytics data.

Target object URI: `/webDataAccess_capabilities/youtubeImport`

Original principal type: Authenticated Users

Original principal ID:

Original granted permissions: Read

Affected functionality: Access import YouTube data.

Target object URI: `/SASDataExplorer/**`

Original principal type: Authenticated Users

Original principal ID:

Original granted permissions: Update,Delete,Create,Read,Add,Remove

Affected functionality: Access SAS Data Explorer.

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.

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	Is the Role Assumable?	Initial Members
Superuser	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 each CAS server has at least one other designated Superuser. **Note:** By default, the users that are assigned this role have unrestricted access to metadata. However, they do not have unrestricted access to data (CAS libraries). To give users with this role unrestricted access to data, you must modify access controls to explicitly grant them access.	Yes	SAS Administrators (in a full deployment) Process owner for the server Analytics gateway account (sas.analyticsGateway)
Data	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. **Note:** By default, the users that are assigned this role have unrestricted access to metadata. However, they do not have unrestricted access to data (CAS libraries). To give users with this role unrestricted access to data, you must modify access controls to explicitly grant them access.	Yes	None
Action	Do not use this role. Not all interfaces support the Action role.	Yes	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

Using graphical user interfaces to manage CAS server roles:

- "Identity Management How To" on page 3

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

- SAS Viya: System Programming Guide

Identity Management Reference

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 necessary, 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 do the following:
  - □ 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, follow these steps:

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

2 From the **Principal** drop-down box, choose **Authenticated Users**. Click **Apply**.

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 11.

To see the rules that provide a group's functionality, follow these steps:

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

2 Uncheck any previously selected principals in the **Principal** drop-down box, and select **Add Identities**.

3 Choose **Custom Groups** from the drop-down box on the Select Identities page. Enter the ID of the predefined custom group (for example, `SASAdministrators`) in the filter field.

4 Click ➕.

5 Click **OK**.

6 From the Rules page, select the custom group that you just added from the **Principal** drop-down box. Click **Apply**.

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.

Table A.2 Interfaces for User Management

●	SAS Environment Manager	A graphical enterprise web application. See “Identity Management How To”.
◔	CAS Server Monitor	A graphical web application that is embedded in the CAS server. See “Add or Remove CAS Role Members (in 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: Command-Line Interfaces.

Identity Management: Troubleshooting

Cannot 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” in SAS Viya Administration: Logging.
- If users cannot make a secure connection, see “Encryption in SAS Viya: Data in Motion” in Encryption in SAS Viya: Data in Motion.

Cannot 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.

Cannot 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” in Encryption in SAS Viya: Data in Motion.

Cannot 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 11.

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

Make sure 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 “Predefined Custom Groups” on page 11.

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]
```

This error indicates that 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 issue, 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**.

Compute Server Cannot Determine Client Identity

If the following error results from running any application, then your product uses compute server functionality:

```
Error running compute job
COMPUTE_CONTEXT: application_name compute context
```

This error indicates that the authentication system on the compute server machine is not correctly configured to recognize users' LDAP identities.

To resolve this issue, ensure that users of products that use the compute server are provided with all of the following requirements:

- LDAP accounts for the visual interfaces
- recognition of their LDAP accounts by the operating system where the compute server is installed
- a home directory that can be accessed by the compute server each time a process starts

For more information, see “Set Up Accounts for Compute Server Users” in SAS Viya for Linux: Deployment Guide.