SAS® Viya® 3.5 Administration:
Identity Management

Identity Management: Overview .......................................................... 2

Identity Management: How To (SAS Environment Manager) .................. 2
  View User and Group Information ................................................. 2
  Manage Custom Groups ............................................................... 3
  Manage Profile Pictures (Avatars) .................................................. 5
  Reload Identities Cache ............................................................... 5

Identity Management: How To (CAS Server Monitor) .......................... 6
  Add or Remove CAS Role Members .............................................. 6

Identity Management: How To (CLI) ................................................. 7
  Examples .................................................................................... 7
  Details ....................................................................................... 8

Identity and Access Management Integration with Azure ....................... 9
  LDAP and SCIM Requirements .................................................... 10
  Disable LDAP ............................................................................. 10
  Register the OAuth Client for Azure ............................................ 11
  Create an Authorization Rule for Azure AD .................................. 13
  Configure SCIM .......................................................................... 13

Identity Management: Reference ....................................................... 17
  Initial Users .............................................................................. 17
  Custom Groups .......................................................................... 17
  Identities .................................................................................. 20

Identity Management: Guidelines ...................................................... 22

Identity Management: Troubleshooting .............................................. 23
  Cannot Sign In to SAS Drive ....................................................... 23
  Cannot Sign In to SAS Studio ..................................................... 23
  Cannot Access Cloud Analytic Services ...................................... 23
  Cannot Sign In to CAS Server Monitor ....................................... 23
  Cannot View Users and Group Members ..................................... 24
  Cannot Access Esri Geographic Mapping Resources .................... 24
  Cannot Retrieve List of Users or Groups ..................................... 24
  Cannot Update User Information ............................................... 25
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.
   - 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 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

<table>
<thead>
<tr>
<th></th>
<th>Linux</th>
<th>Windows</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>/var/log/sas/viya/identities/default</td>
<td>\ProgramData\SAS\Viya\var\log\identities\default</td>
</tr>
</tbody>
</table>

See Also
- "Identities Synchronization" on page 21
- SAS Viya Administration: Access to Functionality

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

Identity Management: How To (CLI)

The following examples assume that you have already signed in to SAS Viya at the command line. See “Command-Line Interface: Preliminary Instructions” in SAS Viya Administration: Using the Command-Line Interfaces.

Examples

Example: Add user1 to the group that has the ID 4444.

    sas-admin identities add-member --user-member-id user1 --group-id 4444

Example: Create a group with the name Salesgroup, the group ID 8888, and the description of “Custom sales group”.

    sas-admin identities create-group --id 8888 --name Salesgroup --description "Custom sales group"

Example: Remove user1 from the sales and marketing groups.

    1 sas-admin identities list-memberships --user-id user1
    2 sas-admin identities remove-member --group-id sales-group --user-member-id user1
    3 sas-admin identities remove-member --group-id marketing-group --user-member-id user1

1  Verify the groups that user1 belongs to.

2  Remove user1 from the group that has the group ID sales-group.

3  Remove user1 from the group that has the group ID marketing-group.

Example: Show details about the group that has the group ID ABC.

    sas-admin identities show-group --id ABC
Example: Validate the LDAP configuration values.

Note: These values are not used for setting up LDAP.

You can use any of the following commands to validate the LDAP configuration values:

Note: The identities validate-config command is available beginning with SAS Viya 3.4 in July 2019 and later deployments.

```
1 sas-admin identities validate-config --ldap-url "url" --ldap-userDN "userDN"
   --ldap-password password --ldap-group-baseDN "group-baseDN"
   --ldap-user-baseDN "user-baseDN"
2 sas-admin identities validate-config --file path-to-file
3 sas-admin identities validate-config --ldap-userDN "userDN" --ldap-password
   --file path-to-file
```

1 Specify the LDAP configuration values via the command line.
2 Specify a file that contains the LDAP configuration values.

Note: You can include the LDAP configuration values in a separate file by using the file option. The file that you specify can be of the type JSON or YML.

The password that is used to connect to the LDAP server must be Base64-encoded. If you specify a password in the file, you must explicitly encode the password.

3 Specify a file that contains the LDAP configuration values. Use the ldap-userDN and ldap-password options to specify a different LDAP user and password to override these values from the file. If a command contains LDAP options and the file option, the LDAP option values override the values in the file.

Note: You can include the LDAP configuration values in a separate file by using the file option. The file that you specify can be of the type JSON or YML.

The password that is used to connect to the LDAP server must be Base64-encoded. If you specify a password in the file, you must explicitly encode the password.

Details

- If a group is created with no name, the specified ID is used for the name.
- The following identities commands list only 50 items at a time by default:
  - list-groups
  - list-members
  - list-memberships
  To list more than 50 items, you can use the --limit option.

Example:

```
sas-admin identities list-members --group-id ABCD --limit 100
```
Consider the following key points about the identities validate-config command:

- You can use this command only on a secure (TLS-enabled) environment.
- The password that is used to connect to the LDAP server must be Base64-encoded. If you specify the password with the \--ldap-password\ option, the CLI encodes it for you. If you specify the password in the JSON or YML file, you must encode the password explicitly.
- The file that you specify with the \--file\ option can be of the type JSON or YML.
- Here is a typical file of the type YML that is used for validating your LDAP configuration values:

```
Note: Enter the URL definition on a single line. Multiple lines are used here to improve readability.

sas.identities.providers.ldap.connection:
  host: multi-tenant-ldap.sun.com
  password: xxxxxxxxxxxx=
  port: 389
  url: ldap://$\{sas.identities.providers.ldap.connection.host\}:
    $\{sas.identities.providers.ldap.connection.port\}
  userDN: cn=admin,dc=sun,dc=com

sas.identities.providers.ldap.group:
  baseDN: DC=SUN,DC=com
  accountId: cn
  objectClass: groupOfUniqueNames
  objectFilter: (objectClass=groupOfUniqueNames)

sas.identities.providers.ldap.user:
  baseDN: DC=SUN,DC=com
  accountId: uid
  objectClass: inetOrgPerson
  objectFilter: (objectClass/inetOrgPerson)
```

See Also

“Command-Line Interface: Overview” in SAS Viya Administration: Using the Command-Line Interfaces

Identity and Access Management Integration with Azure

Azure AD customers have a choice between Lightweight Directory Access Protocol (LDAP) and System for Cross-domain Identity Management (SCIM).

Review the sections below to use SCIM to enable user provisioning between Azure Active Directory (Azure AD) and SAS Viya and configure single sign-on.
LDAP and SCIM Requirements

SAS Viya needs to retrieve user identities and group membership information from the customer’s identity management system.

SAS Viya must be configured using LDAP (which is enabled by default). You can also configure using SCIM instead of LDAP (which must be disabled) to authenticate users with single sign-on using Azure. If you use SCIM, follow the appropriate steps. See “Additional Authentication Topics” SAS Viya Administration: Authentication.

Using SAML or OpenID Connect (OIDC) will be required if you choose SCIM.

**IMPORTANT** By default, Identity Management is shipped with LDAP enabled. If you do not wish to use LDAP, you can disable it using the instructions below.

With LDAP, SAS Viya talks directly to your on-premises active directory LDAP server to pull user and group identities into SAS. Therefore, SAS Viya deployment needs to be able to reach your intranet to query the LDAP server.

**IMPORTANT** With SCIM, you configure Azure AD to push user and group identities into SAS Viya. Therefore, Azure AD must be able to reach your SAS Viya deployment over the internet. A valid certificate from a third-party certificate authority (DigiCert, Verisign, and so on) is required.

Disable LDAP

**Note:** By default, SAS Viya is configured to use LDAP as the identity provider. If you do not want to use LDAP, you may disable it using the instructions below.

1. Verify that you can log in as the sasboot user. Once LDAP is disabled, you can log in only as the sasboot user. The Identity and Access Management Integration with Azure “Identity and Access Management Integration with Azure" on page 9 steps must be completed for whichever single-sign on method you are choosing to configure.

2. From SAS Environment Manager, navigate to the configuration definitions for the Identities service. For more information, see “Edit Configuration Instances” in SAS Viya Administration: Configuration Properties.

3. Update the `spring` configuration:
   a. In the Definitions list, select `spring`.
   b. Next to Identities Service, click Edit Configuration.
   c. Remove the `identities-ldap` from the active profiles.
   d. Click Save.
Note: The cache can be enabled or disabled without any effect on integrating with Azure.

4 Add the `sas.identities.providers` configuration:
   a In the Definitions list, select `sas.identities.providers`.
   b In the top right corner of the window, click **New Configuration**.
   c In the **New sas.identities.providers** Configuration dialog box, set the `ldap.enabled` flag to **false**.
   d Click **Save**.

5 Restart the Identities Service. For more information, see “General Servers and Services: Operate (Linux)” in *SAS Viya Administration: General Servers and Services*

---

### Register the OAuth Client for Azure

Azure AD requires an access token to access the SAS Viya APIs. This will need to be a long-level token to avoid having to update the Azure AD configuration often.

1 Use one of the following methods to register the OAuth client with Azure:

   - **Manual client registration**

     1 Set an environment variable, containing the content of the Consul token that is specified in the manifest in the site.yaml file. Here is an example:

        ```bash
        export CONSUL_TOKEN=token_from_manifest
        ```

        The Consul token can be obtained from the file system for SAS Viya 3.5. On Linux, this is as follows:

        ```bash
        /opt/sas/viya/config/etc/SASSecurityCertificateFramework/tokens/consul/default/client.token
        ```

        **Note:** Run the command on a single line.

        **Note:** If you plan to copy and paste commands from this guide (in PDF), SAS recommends that you copy from the HTML- formatted version of this guide instead. Copy and paste from PDF might introduce extraneous line breaks or invalid characters that will cause commands to fail in your environment.

     2 Obtain a token to register the new client ID and secret.

        ```bash
        curl -k -X POST "https://<hostname>/SASLogon/oauth/clients/consul?callback=false&serviceId=app"
        -H "X-Consul-Token: $CONSUL_TOKEN"
        ```

        **Note:** The initial line of the curl command must be entered on one line. It is shown on more than one line for display purposes only.

     3 Set an environment variable, containing the content of the Bearer token.
export BEARER_TOKEN=bearer_access_token

4 Use the token to register the new client ID and secret.

curl -X POST https://<hostname>/SASLogon/oauth/clients \
-H "Content-Type: application/json" \
-H "Authorization: Bearer $BEARER_TOKEN" \
-d '{ "azure": "azure",  
"client_secret":  
"scope": ["openid", "**"],  
"resource_ids": "none",  
"authorities": ["uaa.none"],  
"access_token_validity": 473040000,  
"authorized_grant_types": ["client_credentials"] }'

Note: The access_token_validity value is for the number of seconds for which tokens are valid.

5 Get an Access token using the client credentials.

curl -k https://<hostname>/SASLogon/oauth/token \
-H "Content-Type: application/x-www-form-urlencoded" \
-d "grant_type=client_credentials" \
-u "azure:secret"

**CLI Client Registration**

1 Set an environment variable, containing the content of the Consul token that is specified in the manifest in the site.yaml file. Here is an example:

export CONSUL_TOKEN=token_from_manifest

2 Register the client, by running the OAuth command-line interface (CLI).

sas-admin --sas-endpoint https://<hostname> oauth register-client \
--grant-client-credentials \
--id azure --secret secret \
--valid-for 473040000

Note:  You should change <hostname> to specify the host name for the endpoint in your environment, and secret should be a unique secret value for registering the client.


2 Once the client is registered, get an Access token using the client credentials. Here is an example:

curl https://<hostname>/SASLogon/oauth/token \
-H "Content-Type: application/x-www-form-urlencoded" \
-d "grant_type=client_credentials" \
-u "azure:secret"

3 Copy the value of the access_token attribute from the JavaScript Object Notation (JSON) in the response and save it. You will need to specify the access_token attribute during the Azure AD configuration.
Create an Authorization Rule for Azure AD

1. Sign in to SAS Environment Manager as the sasboot user.
3. Create a new rule for Azure AD using the values in SAS Viya Administration: Orientation to Authorization.

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Principal type</td>
<td>User</td>
</tr>
<tr>
<td>Principal</td>
<td>azure</td>
</tr>
<tr>
<td>Rule type</td>
<td>Grant</td>
</tr>
<tr>
<td>Permissions</td>
<td>Click Choose and select the permissions. Select Delete, Create, and Update. Be sure to select Read.</td>
</tr>
<tr>
<td>Description</td>
<td>Provide a description, for example, Give Azure AD access to SCIM endpoints.</td>
</tr>
<tr>
<td>Rule status</td>
<td>On</td>
</tr>
<tr>
<td>Object URI:</td>
<td>/identities/scim/v2/**</td>
</tr>
<tr>
<td>Read</td>
<td>Is a required permission.</td>
</tr>
<tr>
<td>&quot;client_secret&quot;:</td>
<td>The client_secret should be chosen by the user.</td>
</tr>
<tr>
<td>&quot;access_token_validity&quot;:</td>
<td>This value represents 15 years.</td>
</tr>
</tbody>
</table>

Configure SCIM

Note: To perform this task, you must have administrator privileges in the Azure portal.

1. Log on to the Azure portal and select Azure Active Directory.
2. On the left pane, select Enterprise Applications ⇒ New Application.

This task should be completed by the portal administrator. If the Enterprise Application already exists, skip to Step 3 on page 14.
The Enterprise Application must be created by administrators as a Non-Gallery application.

Specify a name for the SAS Viya deployment and enable **User Provisioning**. Since single sign-on is required, see OpenID Connect with Azure AD Scenario or SAML with Azure AD Scenario.

3. **Select 3. Provision User Accounts.**

4. **Select Automatic** from the menu in order to access the **Admin Credentials** section.

5. In the **Admin Credentials** section, complete the following steps:
   
   a. In the **Tenant URL** field, specify the base URL to SAS Viya and append `/identities/scim/v2/`.

   Note: HTTPS is required. By required, we mean that the ingress controller for your SAS Viya environment is configured for TLS, using one of the certificate authorities listed. Also, you must have a server authentication certificate with the root certification authority being one of the following:
   - CNNIC
   - Comodo
   - CyberTrust
   - DigiCert
   - GeoTrust
   - GlobalSign
   - Go Daddy
   - VeriSign
   - WoSign

   b. In the **Secret Token** field, paste the Bearer token that you created during the manual client configuration on page 11.

   c. Click **Test Connection**.

      If you configured the system correctly, you will receive a successful response.

      Note: You must allow IP addresses that are used by the Azure AD provisioning service to make SCIM requests to the SAS Viya deployment. For a list of IP addresses for each service tag and region, see Azure IP Ranges and Service Tags – Public Cloud. You can download and program these IP addresses into your firewall, as needed. The reserved IP address ranges for Azure AD provisioning can be found under the AzureActiveDirectoryDomainServices section.

6. In the **Mappings** section, click **Synchronize Azure Active Directory Users to customappsso**.

   In the Attribute Mapping window that opens, complete the following steps:

   a. Ensure that **Enabled** is set to **Yes**.

   b. Attribute mappings define how attribute mappings are synchronized between Azure Active Directory and customappsso. The following attributes are supported by SAS Viya:
Pay careful attention to the mapping for userName. Azure defaults this field to userPrincipalName. This MUST match what you use for the username with single sign-on. If you leave the defaults, this works perfectly with SAML because the SAML single sign-on configuration in Azure defaults the Unique User Identifier to user.userprincipalname. However, if you are going to set up single sign-on with OIDC and configure it to use email, change the userName mapping to use mail instead of userPrincipalName.

<table>
<thead>
<tr>
<th>Azure Active Directory Attribute</th>
<th>customappsso Attribute</th>
</tr>
</thead>
<tbody>
<tr>
<td>userPrincipalName</td>
<td>userName</td>
</tr>
<tr>
<td>Switch([IsSoftDeleted], , “False”, “True”, “True”, “False”)</td>
<td>active</td>
</tr>
<tr>
<td>displayName</td>
<td>displayName</td>
</tr>
<tr>
<td>jobTitle</td>
<td>title</td>
</tr>
<tr>
<td>mail</td>
<td>emails[type eq “work”].value</td>
</tr>
<tr>
<td>streetAddress</td>
<td>addresses[type eq ”work”].street...</td>
</tr>
<tr>
<td>city</td>
<td>addresses[type eq ”work”].locality</td>
</tr>
<tr>
<td>state</td>
<td>addresses[type eq ”work”].region</td>
</tr>
<tr>
<td>postalCode</td>
<td>addresses[type eq ”work”].postal...</td>
</tr>
<tr>
<td>country</td>
<td>addresses[type eq ”work”].country</td>
</tr>
<tr>
<td>telephoneNumber</td>
<td>phoneNumbers[type eq ”work”]...</td>
</tr>
<tr>
<td>mobile</td>
<td>phoneNumbers[type eq ”mobile”]...</td>
</tr>
<tr>
<td>facsimileTelephoneNumber</td>
<td>phoneNumbers[type eq ”fax”].va...</td>
</tr>
<tr>
<td>mailNickname</td>
<td>externalId</td>
</tr>
</tbody>
</table>

Click **Delete** to delete the other attributes.

- Click **Save**.

7 In the **Mappings** section, click **Synchronize Azure Active Directory Groups to customappsso**.

In the Attribute Mapping window that opens, complete the following steps:

- Ensure that **Enabled** is set to **Yes**.
b Click **Delete** to delete all attributes, except **displayName** and **members** attributes, which are supported by SAS Viya.

8 Ensure that the **Provisioning Status** is set to **on** and **Scope** is set to **sync only assigned users and groups**.

Click **Save**.

If you receive an error, complete the following steps:

The generated client tokens are typically less than 1024 bytes. However, with the entire SCIM configuration, the limit might be exceeded. If this is the case, you need to reduce the size of the token. One way to do this is by changing the JWT signing key. By default, SAS Viya uses a 2048 byte RSA key to sign tokens. This impacts the size of the digital signature on your JWT tokens because a large signing key results in a large digital signature.

a Generate a new signing key on any Linux host, using OpenSSL:

```
openssl genrsa -out private.pem 1024
```

b Open the private.pem file and copy the text.

c Log on to SAS Environment Manager and navigate to the configuration definitions. For more information, see “Edit Configuration Instances” in SAS Viya Administration: Configuration Properties.

d In the **Definitions** list, select **sas.logon.jwt**.

e In the top right corner of the window, click **New Configuration**.

f In the New sas.logon.jwt Configuration dialog box, paste the contents of the private key into the **signingKey** field. Leave the default values for the remaining fields.

g Click **Save** and log out of SAS Environment Manager.

SAS Viya 3.5 requires a restart of all services to discover the new signing key.

h Obtain a new access token. For more information, see “Register the OAuth Client for Azure” on page 11.

```
Note: The size of the token should be smaller than when you previously created it.
```

i In the Azure portal, navigate to **Admin Credentials** and paste the new Bearer token. Then, test the connection again to make sure it accepts the new token.

You should now be able to Save the configuration.

Before Azure will start syncing users and groups, the time it can take might vary between 20 minutes to several hours. This is dependent upon the total number of users and groups. Once the syncing is complete, you will see the status of how many users and groups have been synchronized and be able to view the audit logs.

**IMPORTANT** You might have to delete all existing users from SAS if you are clearing state and restarting the synchronization from Azure. Additionally, you need to pickup users where only the case in the userName has changed.
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. You 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.

**Application Administrators**

- Can access selected administrative functions within applications.

- 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.

**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 19.

### 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, or a valid host credential must be stored in the Credentials service.
- 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.

**Note:** From SAS Data Studio, if valid host credentials exist in the Credentials service (even if there is no host account), a CAS session will run under the stored credentials.

- 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>
<thead>
<tr>
<th>User Scenario</th>
<th>CASUSER Path Location</th>
<th>Session Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>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.</td>
<td>CASDATADIR/casuserlibraries/username</td>
<td>Sessions run under the CAS server user (cas). The directory and all files within it are owned by the cas user.</td>
</tr>
</tbody>
</table>
## User Scenario

<table>
<thead>
<tr>
<th>CASUSER Path Location</th>
<th>Session Information</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>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.</strong></td>
<td>Sessions run under the user’s host account.</td>
</tr>
<tr>
<td><strong>User starts CAS sessions from SAS Studio 4, Base SAS, or SPRE, regardless of whether the user is a member of the CASHostAccountRequiredGroup.</strong></td>
<td>SAS Studio 4, Base SAS, and SPRE sessions always run under the user’s host account, and use the <strong>$HOME/casuser</strong> CASUSER path location. Sessions run under the CAS server user (cas). The directory and all files within it are owned by the cas user.</td>
</tr>
</tbody>
</table>

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 5. 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`
- `sas.identities.providers.ldap.connection.port`
- `sas.identities.providers.ldap.connection.password`
- `sas.identities.providers.ldap.connection.userDN`

- `sas.identities.providers.ldap.group.accountId`
- `sas.identities.providers.ldap.group.baseDN`
- `sas.identities.providers.ldap.group.distinguishedName`
- `sas.identities.providers.ldap.group.member`
- `sas.identities.providers.ldap.group.memberOf`
- `sas.identities.providers.ldap.group.objectClass`
- `sas.identities.providers.ldap.group.objectFilter`
- `sas.identities.providers.ldap.group.searchFilter`

- `sas.identities.providers.ldap.use.accountId`
- `sas.identities.providers.ldap.use.baseDN`
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 Drive

Ensure that you initially sign in as the sasboot user. For more information, see “Sign In as the sasboot User” in SAS Viya for Linux: Deployment Guide.

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.

<table>
<thead>
<tr>
<th>Interface</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SAS Environment Manager</td>
<td>A graphical enterprise web application. See “Identity Management: How To (SAS Environment Manager)”</td>
</tr>
<tr>
<td>CAS Server Monitor</td>
<td>A graphical web application that is embedded in the CAS server. See “Manage CAS Roles” in SAS Viya Administration: Using CAS Server Monitor</td>
</tr>
<tr>
<td>Access Control action set</td>
<td>A programmatic interface for SAS (the CAS procedure), Python, R, and Lua. See Access Control Action Set</td>
</tr>
<tr>
<td>Command-line interface</td>
<td>A simple scriptable interface that provides commands for managing identities. See SAS Viya Administration: Using the Command-Line Interfaces</td>
</tr>
</tbody>
</table>