



SAS® Viya® 3.5 Administration: Identity Management

Identity Management: Overview	2
Basics of Identity Management	2
LDAP Requirements	3
SCIM Requirements	4
Identity Management: Guidelines	5
How to Configure SCIM	6
SCIM IAM Integration with SAS Viya	6
Disable LDAP	6
Register OAuth Client for SCIM Client	7
Obtain an Access Token	9
Configure SCIM Provisioning in the Identity Provider	10
Configure the Private User Directory for SCIM	16
Single Sign-on	16
How to Configure LDAP	16
LDAP in Multi-tenancy: Initial Steps	16
Configure an LDAP Identity Provider	17
Set Up Administrative Users	19
Sign In Using LDAP Credentials	20
Identity Management: How To (SAS Environment Manager)	20
View User and Group Information	20
Manage Custom Groups	21
Manage Profile Pictures (Avatars)	23
Reload Identities Cache	24
Identity Management: How To (CAS Server Monitor)	24
Add or Remove CAS Role Members	24
Identity Management: How To (CLI)	25
Examples	26
Details	27

<i>How to Secure the sasboot Password</i>	28
Disable the Password Reset Feature	28
Reset the sasboot Password	29
<i>Identity Management: Reference</i>	29
Initial Users	29
Custom Groups	30
Identities	33
<i>Identity Management: Troubleshooting</i>	36
Cannot Sign In to SAS Drive	36
Cannot Sign In to SAS Studio	36
Cannot Access Cloud Analytic Services	36
Cannot Sign In to CAS Server Monitor	37
Cannot View Users and Group Members	37
Cannot Access Esri Geographic Mapping Resources	37
Cannot Retrieve List of Users or Groups	38
Cannot Update User Information	38
Cannot Log In to SAS	38
Membership in a sasapp LDAP, Custom, or Host Group Is Ignored	39
<i>Identity Management: Interfaces</i>	39

Identity Management: Overview

Basics of Identity Management

Identity management includes setting up and maintaining the connection between SAS Viya and your identity provider. Identity management also includes administrators managing the membership of custom groups and CAS roles.

By default, SAS Viya is configured to use Lightweight Directory Access Protocol (LDAP). As an alternative, you can change the configuration to use System for Cross-domain Identity Management (SCIM). LDAP must be disabled if SCIM is selected. If SCIM is used, either SAML or OpenID Connect must be used for authentication. If you use LDAP, see [“LDAP Requirements” on page 3](#). If you use SCIM, see [“SCIM Requirements” on page 4](#). The use of both LDAP and SCIM in a single, individual environment is not supported.

Using LDAP is the default strategy for pulling in identities from an external identity management system. It is oriented more toward on-premises deployments where the customer has an existing LDAP server. LDAP enables user name/password authentication with SAS Viya, which includes direct access to CAS. LDAP supports UID and GID numbers through POSIX attributes and SAS Viya uses these values if they exist. POSIX attributes are not required. LDAP should be used if SAS Viya is deployed in such a way that storage is shared between SAS Viya and other systems.

The SCIM specification is widely used in cloud environments to share identity information with applications. It is a “push” model whereby the identity management system provisions user and group identities to downstream applications such as SAS Viya, and regularly synchronizes to keep the information up to date. Since SCIM is a push model, it is largely configured from the identity

management side. The advantage of this is that you can have multiple identity management systems or tenants in an identity management system, pushing identities into SAS Viya using SCIM. From SAS Viya, we need to establish only a client identity (oauth client) and give it authorization to call the SCIM APIs on SAS Viya.

SAS identity management includes the following:

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

You can use SAS Environment Manager for most identity management tasks.

TIP Familiarize yourself with the [Predefined Custom Groups on page 30](#) .

LDAP Requirements

You can choose LDAP if you are using local file stores and local user directories.

With LDAP, SAS Viya talks directly to the LDAP server to pull user and group identities into SAS Viya. Therefore, SAS Viya deployments need to be able to directly connect to the chosen LDAP server, which is deployed to your chosen cloud provider. The LDAP connection contains user credentials, and as such encryption should always be used with an LDAP connection. SAS Viya supports both LDAPS (LDAP over SSL) and startTLS on the LDAP connection.

You have a choice of LDAP providers—any LDAP v3 compliant server is supported such as Active Directory or [OpenLDAP](#). You can use Active Directory as your LDAP provider. By default, SAS Viya pulls in identities from an external LDAP server.

- SAS Viya must connect to the LDAP server using an anonymous bind or system account.
- Users and groups are queried from LDAP via a configured base distinguished name (DN). Customers with very large LDAP forests might wish to use multiple base DN's. This is possible only if users are authenticating through single sign-on.
- Users and groups in the directory are queried from a base DN that you specify. For enterprises with very large LDAP forests, you can specify multiple base DN's, but only if users are authenticating with single sign-on, such as SAML or OAuth.
- LDAP enables user name/password authentication to SAS Viya, including direct access to CAS. Since sign-ins are critical to the security of a system, SAS Viya must query LDAP on every sign-in attempt. Accounts are authenticated using “search and bind.” First, the system binds to the LDAP server using the configured system account or anonymous bind. Next, the server searches for the directory entry that matches the user name entered by the user. Then, the server attempts to bind to LDAP using the DN of that directory entry and the password entered by the user. The user name used by SAS Viya is then set using the canonical user name queried from the LDAP attributes. Therefore, the user name appears throughout SAS Viya in the same sense as it appears in LDAP (not how it was entered by the user).
- Since sign-ins are critical to the security of a system, SAS Viya must query LDAP on every sign-in attempt. This involves a single query for the user plus dozens or even more queries for each of

the groups that the user is a member of. All of this places a very high demand on LDAP. As a result, performance is a big consideration.

- User and group membership information is cached in the SAS Viya identities service in order to service general queries. Only LDAP group memberships are cached. An example of a general query is where SAS Viya identities service responds to request such as listing groups when constructing authorization rules. This cache can take several minutes to load at start-up, is refreshed periodically, and can be refreshed by the SAS administrator in SAS Environment Manager.
- For every sign-in attempt, SAS Viya makes a single query for the user plus a query for each of the groups that the user is a member of. All of this places a very high demand on LDAP. As a result, performance is a big consideration and affects sign-in time. Connection pooling and other tuning parameters are available, so the tuning section of the administration guide should be reviewed carefully.
- LDAP supports UID, GID numbers, and secondary GID numbers through POSIX attributes. SAS Viya uses these values if they exist.

SCIM Requirements

With SCIM, you configure the identity provider to push user and group identities into SAS Viya. Therefore, the identity provider must be able to reach your SAS Viya deployment. A valid certificate from a third-party certificate authority (examples include, DigiCert, Verisign, and so on) may be required by your identity provider.

It is important to realize the direction of the network connection for firewall and security rules. The connection is initiated by the identity provider since the identity provider is the SCIM client while SAS Viya identities service is the SCIM server.

The identity management system acts as a SCIM client.

Note: SCIM 2.0 (which SAS supports) is not backward compatible with SCIM 1.1 or the deprecated SCIM 1.0.

- The identity management system needs to reach the SCIM server or SAS Viya deployment. In most cases, the URL must begin with HTTPS and have a certificate that is signed by a public certificate authority.
- From SAS Viya, administrators need to establish only a client identity (OAuth client) and give it authorization to call the SCIM APIs on SAS Viya.
- When using SCIM, CASHostAccountRequired members can run under individual users' host accounts. For more information see [“The CASHostAccountRequired Custom Group” on page 31](#)
- SAS Viya does not store passwords or accept passwords through SCIM. Therefore, user name/password authentication is not possible when using SCIM. Here are examples of scenarios that require user name and password authentication:
 - ☐ service accounts for SAS Compute Server
 - ☐ shared accounts for CAS and SAS Compute Server
 - ☐ stored credentials for an individual identity for CAS and SAS Compute Server

The SAS Viya command-line interface (CLI) enables authentication using an authorization grant instead of a user name and password combination. With such a grant, the user authenticates from a web browser in order to obtain an authorization code for the CLI. See [“Obtain an Access Token Using an Authorization Code”](#) in *SAS Viya Administration: Authentication* and *SAS Logon API* for more information.

- The standard SCIM core schema defined by RFC 7643 does not include UID and GID information. This is an important issue to consider when planning how files will be used or shared outside of the SAS Viya deployment, especially, with applications that are not SAS applications.
- Private user directories are not directly supported but can be configured.
- SAS Viya needs to retrieve user identities and group membership information from the customer's identity management system.
- Using SAML or OpenID Connect (OIDC) is required for SAS Logon Manager if you choose SCIM.

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.

How to Configure SCIM

This section provides detailed information for provisioning SCIM, including the following: registering an OAuth Client, configuring SCIM in Azure AD, configuring SCIM in Okta, and configuring a private user directory for SCIM.

SCIM IAM Integration with SAS Viya

SCIM is an optional configuration. By default, SAS Viya is configured to use LDAP as an identity provider.

Since SCIM is a "push" model, the identity provider needs to access the SAS Viya deployment over the internet. It must use HTTPS and have a certificate that is signed by a public certificate authority.

Note: Deployments in the cloud (for example, Azure AKS) can be used but require the firewall settings be updated in order to allow connections from the identity provider's IPs.

IMPORTANT Beginning with SAS Viya 3.5 and later, a new custom group named SCIM is automatically created. In addition, a new authorization rule is created. This authorization rule gives members of the SCIM custom group access to the SCIM endpoints in SAS Viya. As a result, an authorization rule no longer needs to be created manually.

Disable LDAP

Note: By default, SAS Viya is configured to use LDAP as the identity provider. Using LDAP and SCIM concurrently in a single environment is not supported. If you do not want to use LDAP, you can disable it using the instructions below.

Note: The cache can be enabled or disabled without any effect on integrating with the identity provider.

- 1 From SAS Environment Manager, navigate to the configuration definitions for the Identities service. In the applications menu (☰) under **ADMINISTRATION**, select **Manage Environment**. In the vertical navigation bar, select . In the list of services, locate the **Identities service** and select it.
- 2 Update the *spring* configuration instance:

- a In the main configuration area, enter **spring** in the **Configuration Instance Filter** field.
 - b Next to the **spring** configuration instance, click .
 - c Edit the **profiles.active** property and remove **identities-ldap**.
The **profiles.active** property should contain only **identities-local** as its current value.
 - d Click **Save**.
- 3 Add the **sas.identities.providers** configuration:
- New Configuration Setup**
- a In the top right corner of the window, click **New Configuration**.
 - b In the Select Definition window, select **sas.identities.providers**.
 - c In the New **sas.identities.providers** Configuration window, set the **ldap.enabled** flag to **off**.
 - d Ensure that the **scim.enabled** flag is set to **on**.
 - e Click **Save**.
- 4 Restart the Identities service. For more information, see [“General Servers and Services: Operate \(Linux\)” in SAS Viya Administration: General Servers and Services](#).

Register OAuth Client for SCIM Client

Overview

The identity provider needs an access token in order to access the APIs on SAS Viya. A long-lived token is required to avoid having to routinely update the identity provider configuration. Users must register an OAuth client for the identity provider and use the client credentials to generate an access token. You can perform this task using a manual client registration or a CLI client registration. Both of these methods register a new client ID, "idp-client-id", use a secret, "idp-client-secret" (select a different one for your setup), and set up the client ID to obtain tokens using client credentials with an expiration of 63070000 seconds or 2 years.

Note: After completing the registration, the client ID is now registered with the SCIM authority.

- CURL is a command line tool and a library that can be used to receive and send data between a client and a server or between any two machines connected over the internet. It supports a wide range of protocols such as HTTP, FTP, IMAP, LDAP, POP3, SMTP, and many more.
- SAS Viya CLI posts to a secure endpoint by default. See [“Command-Line Interface: Preliminary Instructions” in SAS Viya Administration: Using the Command-Line Interfaces](#). By doing so, it is requesting an OAuth token from SASLogon.

Manual Client Registration

To register a client manually, follow these steps:

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

The example below uses a password grant, but other options are available. Use an account that is a member of the SASAdministrators group:

```
INGRESS_URL=https://hostname.example.com; \
export BEARER_TOKEN=`curl -sk -X POST \
"${INGRESS_URL}/SASLogon/oauth/token" \
-u "sas.cli:" \
-H "Content-Type: application/x-www-form-urlencoded" \
-d 'grant_type=password&username=myusername&password=mypassword' | awk -F: '{print $2}'|awk -F\" '{print $2}'`
```

Note: The initial line of the CURL command must be entered on one line. Multiple lines are used here to improve readability.

- 2 Verify that the command executed correctly:

```
echo "The registration access-token is: " ${BEARER_TOKEN}
```

Output should be similar to the following:

```
The registration access-token is: eyJhbGciOi-hz_-1eQhpfd_nZcVE9stGwqjJ4WzR2doHEd
```

- 3 Register the Identity provider client ID with client_credentials grant type.

```
curl -k -X POST "${INGRESS_URL}/SASLogon/oauth/clients" \
-H "Content-Type: application/json" \
-H "Authorization: Bearer $BEARER_TOKEN" \
-H "X-Identity-Zone-Id: <tenant>" \
-d '{
  "client_id": "idp-client-id",
  "client_secret": "idp-client-secret",
  "authorities": ["SCIM"],
  "authorized_grant_types": ["client_credentials"],
  "access_token_validity": 63070000
}'
```

Note: The use of -H "X-Identity-Zone-Id: <tenant>" \ is required only for multi-tenancy.

The output should be similar to the following:

```
{"client_id": "idp-client-id", "authorized_grant_types":
["client_credentials"], "autoapprove": [], "access_token_validity": 63070000, "authorities": ["SCIM"],
"lastModified": 1628126258430, "required_user_groups": []}
```

For more information about registering a client manually see [“Register a Client Manually” in SAS Viya Administration: Authentication](#) .

CLI Client Registration

Clients can be registered with the SAS Viya platform command-line interface (CLI). Use the CLI to register an OAuth client that enables access to SAS Viya platform APIs. The OAuth CLI plug-in is required. If you have not already downloaded the SAS Viya platform command-line interface, be sure to do so.

- 1 Log in to the SAS Viya platform CLI using an account that is a member of the SASAdministrators group. Here is an example:

```
sas-viya --profile my-admin-profile auth login
```

- 2 Register the client by running the OAuth plug-in to the SAS Viya platform CLI.

The following command registers a client to obtain tokens using a password grant. Run the command without the `--grant-password` option to display all of the grant parameters.

```
INGRESS_URL=https://hostname.example.com

sas-viya --sas-endpoint ${INGRESS_URL} oauth register-client \
--grant-password \
--id idp-client-id --secret idp-client-secret \
--authorities "SCIM" \
--valid-for 63070000
```

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

The output should be similar to the following:

```
Registering new client 'idp-client-id' with grant_type password.....
idp-client-id has been registered as a client of the SAS environment at https://hostname.example.com.
Clients can use idp-client-id and idp-client-secret to obtain access tokens.
OK
```

Obtain an Access Token

Whichever method was used to register the client, administrators can obtain the access token using the client credentials.

IMPORTANT When obtaining an access token and implementing multi-tenancy, the URL should contain the tenant subdomain. The token is used only for that tenant. For example:

```
https://<tenant>.myserver.example.com/SASLogon/oauth/token
```

Here is an example:

```
ACCESS_TOKEN=`curl -skX POST "${INGRESS_URL}/SASLogon/oauth/token" \
-H "Content-Type: application/x-www-form-urlencoded" \
-d "grant_type=client_credentials" \
```

```
-u "idp-client-id:idp-client-secret"| awk -F: '{print $2}'|awk -F\" '{print $2}'; \
echo "The client access-token is: " ${ACCESS_TOKEN}; \
echo ${ACCESS_TOKEN} > ~/idtoken.txt
```

The output should be similar to the following:

```
The client access-token is: eyJhbGciOiJSUzI1NiIsImprSI6Imh0dHBzOi8vbG9jYWxob3N0L1NBU0xv...
```

Configure SCIM Provisioning in the Identity Provider

Configure SCIM Provisioning in Azure AD

Before you configure SCIM Provisioning in Azure AD (Active Directory), be aware of these requirements:

- You must have administrator privileges in the Azure (AD) portal.
- 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 **AzureActiveDirectory** section.
- If you are using Azure WAF (Web Application Firewall,) be aware that Azure WAF blocks requests to the SAS SCIM endpoint because they are identified as malicious requests. To prevent this, you should create a custom allowlist rule for the SAS SCIM endpoint “/identities/scim/v2”.

As an Azure Tenant Administrator, follow these steps to configure SCIM Provisioning:

- 1 Log on to the Azure portal and select **Azure Active Directory**.
- 2 On the left panel, select **Enterprise Applications** ⇒ **New Application** and enter **SAS Viya** in the search field. Click on **SAS Viya SSO** in the search results.
- 3 On the Create page, provide a name for your application.
- 4 Click **Create**. The new application is created.
- 5 Now you can add users and groups to your application. On the Overview page for the new application, under **Getting Started**, select **Assign users and groups**. On the Users and groups page, select **Add user/group**. On the Add Assignment page, you can add users and roles to your application. Under **Users**, select **None Selected**. On the Users page that appears, select a user from the list. Click **Select**. On the Add Assignment page, the user is now listed. Click **Assign**. The user is now displayed on the Users and groups page.

Note: A common requirement is to sync only a subset of assigned users and groups configured with the enterprise application.

- 6 Now you can provision user accounts for your application. On the Overview page for the new application, under **Getting Started**, select **Provision User Accounts**. Then select **Get started**. On the Provisioning page that opens, select **Get Started**.
- 7 On the Provisioning page that opens, select **Automatic** from the **Provisioning Mode** menu. This expands the **Admin Credentials** section.
- 8 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. In other words, the ingress controller for your SAS Viya environment is configured for TLS and is using a certificate that is issued by one of the public certificate authorities that are supported by Microsoft Authentication Services.

- b In the **Secret Token** field, paste the Bearer token that was created when you followed the process for “[Manual Client Registration](#)” on page 8.
- c Click **Test Connection**.
If you configured the system correctly, you will receive a successful response.
- d Click **Save** on the Provisioning page. The **Mappings** and **Settings** sections become active.

IMPORTANT You must save the provisioning changes before proceeding.

- 9 Now you can define attribute mappings for your application. In the **Mappings** section, click **Provision Azure Active Directory Users**.

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

- a Ensure that **Enabled** is set to **Yes**.
- b Attribute mappings define how attributes are synchronized between Azure Active Directory and customappsso. The following attributes are supported by SAS Viya:

IMPORTANT Pay careful attention to the mapping for **userName**. Azure AD maps this field to **userPrincipalName** by default. This must match what you use for the user name with single sign-on. If you leave the default settings, this works perfectly with SAML because the SAML single sign-on configuration in Azure AD maps the Unique User Identifier to *user.userprincipalname* by default. However, if you set up single sign-on with OIDC and configure it to use email, change the **userName** mapping to use *mail* instead of **userPrincipalName**.

A second mapping option is to map **userName** to **objectId** in the SCIM configuration and use **oid** in the OIDC claims. For more information about ID token claims see <https://learn.microsoft.com/en-us/entra/identity-platform/id-tokens>.

Double-click on the **userName** row. On the Edit Attribute page, modify the **Source attribute** mapping from **UserPrincipalName** to *mail*.

Table 1 *Attributes to Keep*

Azure Active Directory Attribute	customappsso Attribute
userPrincipalName	userName
Switch([IsSoftDeleted], , "False", "True", "True", "False")	Active
displayName	displayName
jobTitle	title
mail	emails[type eq "work"].value
streetAddress	addresses[type eq "work"].street...
city	addresses[type eq "work"].locality
state	addresses[type eq "work"].region
postalCode	addresses[type eq "work"].posta...
country	addresses[type eq "work"].country
telephoneNumber	phoneNumbers[type eq "work"]...
mobile	phoneNumbers[type eq "mobile...]
facsimileTelephoneNumber	phoneNumbers[type eq "fax"].va...
mailNickname	externalId

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

- c Ensure that **Enabled** is set to **Yes**.
 - d Click **Save** and confirm with **Yes**.
- 10 Return to the main Provisioning page (from the top navigation or by exiting the Users provisioning window).
- 11 In the **Mappings** section of the Provisioning page, click **Provision Azure Active Directory Groups**. In the Attribute Mapping window that opens, complete the following steps:
- a Ensure that **Enabled** is set to **Yes**.
 - b Click **Delete** to delete all attributes except **displayName** and **members**, which are supported by SAS Viya.
- 12 Click **Save** and then click **Yes** to confirm.

- 13 Now you can define settings for your application. Return to the main Provisioning page, and complete the **Settings** section:
 - a Select **Send an email notification when failure occurs**, and enter an email address in the **Notification email** field.
 - b For the **Scope** field, select **Sync only assigned users and groups**.
- 14 Set **Provisioning Status** to **On**, and click **Save**.
- 15 Click on your Enterprise Application from the top navigation or click **X** from the top right to return to the main Provisioning page.
- 16 The **Start provisioning** action is inactive if synchronization has started. Likewise, the **Stop provisioning** action is active.

The amount of time that Azure AD takes to synchronize users and groups can vary from 20 minutes to several hours. This depends on the total number of users and groups. Once the synchronizing process is complete, you can see the status of how many users and groups have been synchronized and 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 AD. In addition, you need to pickup users where only the case in the userName has changed.

Configure SCIM Provisioning in Okta

Note: SAS Viya supports SCIM 2.0. Okta supports an on-premises provisioning agent. However, it supports only SCIM version 1.

Note: You need to create another app in Okta to configure single sign-on. After this is completed, you can open a support case with Okta to merge your SCIM configuration with your single sign-on app, if desired.

To begin, log in to the Okta tenant that you are using.

- 1 Click **Admin**.
- 2 Select **Applications** from the menu and click **Add Application**.
- 3 Enter **SCIM** in the search field and a list of templates is displayed.
Look for **SCIM 2.0 Test App (OAuth Bearer Token)** in the results. You might have to select **See All Results**.
- 4 Select the template and click **Add**.
- 5 Edit the **Application label** field. Enter a name for the SAS Viya deployment.
- 6 Click **Done**.

- Go to the **Provisioning** tab, and select **Integration** from the **SETTINGS** menu. Click **Configure API Integration**. Select **Enable API Integration**.

Some fields are displayed.

In the **SCIM 2.0 Base URL** field, enter the full URL to the SAS Viya deployment plus `/identities/scim/v2`. For example: `https://myserver.example.com/identities/scim/v2`.

In the **OAuth Bearer Token** field, enter the token obtained earlier using client credentials.

Note: Do not include "Authorization" or "Bearer" in this field. Okta already includes these tokens.

Verify Test API Credentials

- Click the **Test API Credentials** to verify the connection.
- Click **Save**.
- Remain on the **Provisioning** tab and select **To App** from the **SETTINGS** menu on the left. Select the **Enable** check boxes next to **Create Users**, **Update User Attributes**, and **Deactivate Users**. SAS Viya does not store user passwords. Therefore, leave **Sync Password** disabled. You will need to set up single sign-on using SAML or OpenID Connect (OIDC) so that users can sign in.
- Click **Save**.

Navigate to the **Sign On** tab. Click **Edit** in the Settings section. Scroll down to the **Credentials Details**. Here you can choose what value Okta sends to SAS Viya for the user name field.

IMPORTANT The user name field needs to match the single sign-on configuration. By default, it uses the Okta username. Make sure **Create and update** is selected. Note that SAS Viya does not handle changes to the user name easily since existing folders, files, and so on are not migrated under the new user name.

- Click **Save**. All changes are saved.

Refer back to the **Provisioning** tab. Scroll to the **Attribute Mappings**. Notice it states that the Username is configured in the Sign-on settings. Modify the **Attribute Mappings** so that they match what is shown in the table below:

1 **Table 2** *Attribute Mappings*

Attribute	Attribute Type	Value	Apply on
Username userName	Personal	Configured in Sign On settings	None
Given name givenName	Personal	user.firstName	Create
Family name familyName	Personal	user.lastName	Create

Primary email	Personal	user.email	Create and update
Primary email type emailType	Personal	(user.email != null && user.email != "") ? 'work' : "	Create and update
Title title	Personal	user.title	Create and update
Display name displayName	Personal	user.displayName	Create and update
Primary phone primaryPhone	Personal	user.primaryPhone	Create and update
Address type addressType	Personal	(user.streetAddresses != null && user.streetAddresses != "") ? 'work' : "	Create and update
Street address streetAddress	Personal	user.streetAddresses	Create and update
Locality locality	Personal	user.city	Create and update
	None	None	None
Region region	Personal	user.state	Create and update
Postal Code postalCode	Personal	user.zipCode	Create and update
Country code country	Personal	user.countryCode	Create and update

- On the **Assignments** tab you can now assign users to this application. This can be done by choosing **People** under **FILTERS** or selecting **Groups**. Okta sends these to SAS Viya as you assign them. You should then be able to see them displayed in SAS Environment Manager.
- Go to **Push Groups** to select the groups that should be sent to SAS Viya. Click on **Push Groups**. Choose either option to find groups. When you have selected all the groups that you prefer, click **Save**. Okta immediately sends them to SAS. You can view them in SAS Environment Manager.
- Provisioning logs can be viewed by clicking the **View Logs** link near the top of the screen above the menus.

Configure the Private User Directory for SCIM

To configure the Private User Directory for SCIM, perform the following tasks:

- 1 From SAS Environment Manager, navigate to the configuration definitions for the Identities service. In the applications menu (☰), under **ADMINISTRATION**, select **Manage Environment**. In the vertical navigation bar, select .

In the list of services, select **Identities service**.

- 2 Update the *sas.identities* configuration instance:
 - a In the **main configuration** area, enter **sas.identities** in the **configuration instance Filter** field.
 - b Next to the **sas.identities** configuration instance, click .
 - c In the Edit *sas.identities* Configuration window, scroll down to the **identifier.homeDirectoryPrefix** field.
In this field, add the absolute path to the directory that contains your users' private user directory. For example: `/home`.
 - d Click **Save**.

The identities service returns a home directory in the specified location when you are using SCIM. Processes such as CAS can use this home directory.

Single Sign-on

Note: Single sign-on is required for authentication when using SCIM.

How to Configure LDAP

Use SAS Environment Manager to set up user and group authentication.

LDAP in Multi-tenancy: Initial Steps

If your site does not use multi-tenancy, complete the steps in [“Configure an LDAP Identity Provider” on page 17](#).

In SAS Viya multi-tenancy, LDAP can use a single identity provider for all tenants (a single-LDAP configuration), or separate identity providers, one for each tenant (a separate-LDAP configuration).

During Installation

For a single-LDAP configuration, during the installation of SAS Viya multi-tenancy, use your own LDAP tools to set up an identity provider. The LDAP structure is required to include the provider tenant and other tenants as separate OUs in the same LDAP branch. The initial setup needs to include only the tenants that you plan to onboard after installation.

For a separate-LDAP configuration, during installation, obtain connection information for the LDAP identity provider for each planned tenant. Connection information includes host, password, port, URL, and userDN.

During the installation of both single-LDAP and separate-LDAP configurations, add at least one user to each of your identity providers. After onboarding, the first user becomes the first SAS administrator in each tenant.

To learn about LDAP requirements in multi-tenancy, see [SAS Viya Administration: Multi-tenancy](#).

After Onboarding

After you onboard tenants, use SAS Environment Manager to add at least one user to the SAS Administrators group in the provider and in each tenant. See [“Set Up Administrative Users” on page 19](#). The new SAS Administrators can then add users and groups to their respective tenants, as described in [“Configure an LDAP Identity Provider” on page 17](#).

Configure an LDAP Identity Provider

After completing the installation of SAS Viya, you can configure an LDAP identity provider. LDAP is the default identity provider.

In multi-tenancy, LDAP configuration in SAS takes place after you onboard tenants.

To configure the connection to your identity provider:

- 1 Sign in to SAS Environment Manager as sasboot.

Note: In multi-tenancy, use sasboot to sign in to the provider tenant. To sign in to a tenant, use the sasprovider account that is created during onboarding.

- 2 Select **Configuration** from the side menu to open the Configuration page.
- 3 On the Configuration page, select **All Services** from the list and then select the **Identities service** from the list of services.
- 4 To configure connection properties in the **sas.identities.providers.ldap.connection** section, click **New Configuration**. In the New Configuration window, complete these steps:

- a Specify values for the following required fields: **host**, **password**, **port**, **url**, and **userDN**. For the remaining fields, review the default values and make changes, as necessary. The default values are appropriate for most sites.

IMPORTANT In multi-tenancy, for a single-LDAP configuration, click **New Configuration** only once to create a single-LDAP configuration. For a separate-LDAP configuration, create one new configuration for each newly onboarded tenant. Do not enable the configuration option **Apply**.

- b Click **Save**.

TIP In addition to SAS Environment Manager, you can also use the SAS Viya CLI plug-in for LDAP.

- 5 To configure user properties in the **sas.identities.providers.ldap.user** section, click **New Configuration**:

- a Specify a value for the **baseDN** required field. For the remaining fields, review the default values and make changes, as necessary. The default values are appropriate for most sites.

Note: When using the LDAP protocol, passwords are transmitted over the network as cleartext. To secure the deployment, SAS recommends that you configure encrypted LDAP connections. For more information, see [“Overview” in Encryption in SAS Viya: Data in Motion](#).

Note: In multi-tenancy, end-to-end TLS security is required.

For each property that represents a user-level field in SAS, specify a corresponding property in the LDAP server software.

TIP Consider specifying a custom filter to limit the user accounts that SAS Viya returns from your LDAP server.

- b Click **Save**.

- 6 To configure group properties, in the **sas.identities.providers.ldap.group** section, click **New Configuration**. In the New Configuration window:

- a Specify a value for the **baseDN** required field. For the remaining fields, review the default values and make changes, as necessary. The default values are appropriate for most sites.

For each property that represents a group-level field in SAS, specify a corresponding property in the LDAP server software.

TIP Consider specifying a custom filter to limit the accounts that SAS Viya returns from your LDAP server.

b Click **Save**.

- 7 To verify user and group information from the SAS Environment Manager side menu, select **Users** to open the **Users** page.

On the **Users** page, select **Users** from the list in the toolbar. Your users should appear after a few minutes. It is not necessary to restart any servers or services. Then, select **Groups** from the list to display your groups.

- 8 Verify that user and group information is displayed correctly. If not, make any necessary changes to the identities service properties, then restart the Identities and SAS Logon Manager services.

Set Up Administrative Users

In multi-tenancy, sign in to the provider tenant as sasboot. Sign in to onboarded tenants as sasprovider. At least one SAS administrator is required in all tenants. For more information about administrative roles in multi-tenancy, see [“Administration” in SAS Viya Administration: Multi-tenancy](#).

While you are signed on to SAS Environment Manager as the sasboot user, set up at least one SAS Administrator user as follows:

- 1 On the **Users** page in SAS Environment Manager, select **Custom Groups** from the list in the toolbar.
- 2 In the left pane, click **SAS Administrators**.
- 3 In the **Members** section of the right pane, click **Edit**, and add one or more members to the group (including your own account, if applicable).
- 4 Sign out from SAS Environment Manager so that you are no longer signed in as the sasboot user.
- 5 If you added your own account to the SAS Administrators group, you can sign on again to SAS Environment Manager using that account.

Open SAS Environment Manager from a URL with the following format:

protocol://name-of-ingress-host:port/SASEnvironmentManager

protocol can be http or https, depending on how you have secured your deployment.

In multi-tenancy, to maximize security, administrators in the provider tenant should not also be members of the SAS Administrators group in a tenant.

TIP Since SAS Administrators is an assumable group, the following prompt is displayed: Do you want to opt in to all of your assumable groups?. Select **Yes** if you want the extra permissions that are associated with the SAS Administrators group. The selection remains in effect until you sign out.

Sign In Using LDAP Credentials

Open SAS Environment Manager from a URL with the following format:

protocol://name-of-ingress-host:port/SASEnvironmentManager

protocol can be http or https, depending on how you have secured your deployment.

Sign in as one of the SAS Administrators that you set up in [“Set Up Administrative Users” on page 19](#).

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 3 *Identities Log File*

Linux	<code>/var/log/sas/viya/identities/default</code>
Windows	<code>\ProgramData\SAS\Viya\var\log\identities \default</code>

See Also

- [“Identities Synchronization” on page 34](#)
- [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
  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](#)

How to Secure the sasboot Password

Disable the Password Reset Feature

When you have finished configuring SCIM or LDAP and have set up the initial administrative users, you should reset the password for the sasboot user. For additional security, you can then disable the password reset feature. This action prevents password reset links from being written to the log each time the SASLogon service is restarted. Follow these steps to disable the password reset option:

- 1 Sign in to SAS Environment Manager as an administrative user and select  from the side menu to open the Configuration page.
- 2 On the Configuration page, select **Definitions** from the drop-down list.
- 3 In the left pane, select **sas.logon.initial**. Then click **New Configuration** at the top of the right pane. If a definition already exists, you can click  to edit the existing definition.
- 4 In the New sas.logon.initial Configuration window or the Edit sas.logon.initial Configuration window, set **reset.enabled** to **off**.
- 5 Click **Save**.
- 6 In order to correctly enforce this property and prevent the use of an existing rest URL, restart the SAS Logon Manager services with the following options: s:
 - For Red Hat Enterprise Linux 6.x:


```
sudo service sas-viya-saslogon-default restart
```
 - For Red Hat Enterprise Linux 7.x or later and SUSE Linux:


```
sudo systemctl restart sas-viya-saslogon-default
```

Note: After you disable this feature, you can still change the sasboot password if the existing password is known. Sign in as sasboot using the current password. Enter the URL for SAS Viya with the path `/SASLogon/change_password`. You can then complete the steps to change the password.

For more information, see [General Servers and Services: Operate](#) in *SAS Viya Administration: General Servers and Services*.

Reset the sasboot Password

After you disable this feature, you can still change the sasboot password if the existing password is known. Sign in as sasboot using the current password. Enter the URL for SAS Viya with the path `/SASLogon/change_password`. You can then complete the steps to change the password.

Identity Management: Reference

Initial Users

sasboot Account

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

Note:

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

Operating System Accounts

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

Custom Groups

What Is a Custom Group?

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

Your deployment includes a set of [predefined custom groups](#). can also create your own custom groups. This feature is useful for creating new groups of SAS users if you do not want to (or do not have permission to) create groups in your identity provider.

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

Assumable Custom Groups

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

If the user selects **Yes**, the user gets the extra permissions that are associated with the assumable group. If the user selects **No**, the user does not get the extra permissions. The selection remains in effect until the user signs out.

As a best practice, users should select **Yes** only when they need to perform tasks that require the extra permissions

Predefined Custom Groups

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

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

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

The custom groups are as follows:

SAS Administrators

Have access to the following:

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

Is an assumable group.

Members can assume the CAS Superuser role.

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

Esri Users

Can access Esri systems for geo map access.

Is not an assumable group.

Has no initial members.

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

Application Administrators

Can access selected administrative functions within applications.

Is not an assumable group.

Has no initial members.

Note: An additional custom group is predefined, but not created. If you create a group with ID: *CASHostAccountRequired*, members of this group automatically run their CAS sessions under their own host account. By default, CAS sessions run using the **cas** account. For more information, see [CASHostAccountRequired custom group on page 31](#).

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 custom group:

Table 4 CASUSER Path Location

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

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

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

Note: If a user is removed from the CASHostAccountRequired custom 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 21](#)

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 24](#). Note that reloading the set of users and groups can take several minutes to complete.

Required SCIM Attribute Mappings to Azure AD

Attribute mappings define how attributes are synchronized between Azure Active Directory and SAS Viya (customappsso). To configure SCIM provisioning with Azure AD, specific attributes are mapped during your configuration on the Azure portal.

The following attributes are required for SCIM provisioning with SAS Viya:

Table 5 Required SCIM Attribute Mappings to Azure AD

Azure Active Directory Attribute	customappsso Attribute
userPrincipalName	userName
Switch ([IsSoftDeleted], , "False", "True", "True", "False")	Active
mailNickname	externalId

The following attributes are not required but could be useful for your SCIM configuration:

Table 6 SCIM Attribute Mappings to Azure AD

Azure Active Directory Attribute	customappsso Attribute
displayname	displayname
mail	emails[type eq "work"].value

For more information see ["Configure SCIM Provisioning in Azure AD" on page 10](#).

Identities Properties That Require LDAP Attributes

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

`sas.identities.providers.ldap.connection`

`host`

`port`

`password`

`userDN`

`sas.identities.providers.ldap.group`

`accountId`

`baseDN1`

`distinguishedName`

`member`

`memberOf`

`objectClass`

`objectFilter`

`searchFilter`

`sas.identities.providers.ldap.user`

`accountId`

`baseDN1`

`distinguishedName`

`memberOf`

`objectClass`

`objectFilter`

`searchFilter`

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

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

Note: The accountId is case-sensitive and must exactly match the user name that is provided by the authentication protocol. In addition, for each supported protocol, a different format is assumed to be the user name.

See Also

- [“Identities Service” in SAS Viya Administration: Configuration Properties](#)

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 31](#).

Cannot Retrieve List of Users or Groups

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

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

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

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

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

Cannot Update User Information

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

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

Cannot Log In to SAS

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

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

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

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

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

Identity Management: Interfaces

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

 SAS Environment Manager	A graphical enterprise web application. See “Identity Management: How To (SAS Environment Manager)” .
 CAS Server Monitor	A graphical web application that is embedded in the CAS server. See “Manage CAS Roles” in <i>SAS Viya Administration: Using CAS Server Monitor</i> .

 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 SAS Viya Administration: Using the Command-Line Interfaces .
