Identity Management Overview

User and group identities are stored and managed by your organization's identity provider (for example, Microsoft Active Directory or LDAP). Read-Only access to the provider enables SAS to authenticate users and obtain identity information at sign-on. You can also add users to custom groups that are persisted in SAS.

SAS identity management includes:

- setting up and maintaining the connection between SAS Viya and your identity provider.
- managing the membership of custom groups and CAS roles.
Identity Management How To

Manage CAS Role Memberships
For each CAS server, make sure to designate at least one user (other than the server’s process owner) to the Superuser role.

Add or Remove CAS Role Members (in CAS Server Monitor)
The CAS (Superuser) role provides unrestricted access to all CAS objects and actions within the associated CAS server.

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

1. Sign in to CAS Server Monitor with an account that is already a CAS (Superuser).
2. In the left navigation bar, select 🔄.
3. On the Configuration page, select the Administrators tab.
   Note: On this tab, you see the sas.deploymentBackup user and the SASAdministrators group. Neither of these is in use and can be ignored or removed.
4. To add a member:
   a. Click Add.
      Note: If the Add button is not present, you are not signed in as a CAS (Superuser).
   b. In the Add Administrator window, enter a user or group name, select the appropriate identity type, and select the CAS or Data radio button.
      TIP The user and group names that you enter are not validated. You can enter any user or group name from your identity provider.
   c. Click OK to save your changes.
5. To change a role assignment:
   a. Click in the appropriate row, and select Modify. You cannot change the assignment for the account that starts the server.
   b. In the Edit Administrator window, select Data or CAS, and click OK.
6. To remove a role assignment, click in the appropriate row, and select Delete. You cannot remove the account that starts the server.
7. Under Administrators, review the results.
8. Verify that full administrative privileges are available when designated users sign in to CAS Server Monitor. For example, any user who sees the Add button on the Administrators tab is a CAS administrator (Superuser).
Identity Management Concepts

CAS Server Roles

Superusers have unrestricted access to CAS and are exempt from all CAS authorization requirements. The account that starts a CAS server is automatically assigned to that server’s Superuser role.

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

See Also

Using graphical user interfaces to manage CAS server roles:
- Manage CAS Role Memberships on page 2

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

SAS Cloud Analytic Services: System Programming Guide

User Management: Interfaces

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

<table>
<thead>
<tr>
<th><strong>CAS Server Monitor</strong></th>
<th>A graphical web application that is embedded in the CAS server.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Access Control action set</strong></td>
<td>A programmatic interface for CASL (the CAS procedure), Python, and Lua. See <em>SAS Cloud Analytic Services: System Programming Guide</em>.</td>
</tr>
</tbody>
</table>