## SAS® Viya® 3.4 Administration: Cloud Analytic Services Authorization

**CAS Authorization: Overview**  
- Introduction: 2
- Navigation: 3
- Examine Access: 3
- Set an Access Level: 4
- Add a Direct Access Control: 5
- Remove a Direct Access Control: 5
- Remove Multiple Direct Access Controls: 5
- Examples: Manage Access to a Caslib: 6
- Add Row-Level (Filtered) Access: 7
- Identify the Source of Effective Access: 8

---

**CAS Authorization: How to (Authorization Window)**  
- Introduction: 2
- Navigation: 3
- Examine Access: 3
- Set an Access Level: 4
- Add a Direct Access Control: 5
- Remove a Direct Access Control: 5
- Remove Multiple Direct Access Controls: 5
- Examples: Manage Access to a Caslib: 6
- Add Row-Level (Filtered) Access: 7
- Identify the Source of Effective Access: 8

---

**CAS Authorization: How to (CAS Server Monitor)**  
- Introduction: 8
- Navigation: 8
- Examine Access to a Caslib: 9
- Provide Public Access to a Caslib: 9
- Selectively Grant Access to a Caslib: 10
- Selectively Limit Access to a Caslib: 11
- Resolve Duplicate Access Controls: 11

---

**CAS Authorization: Concepts**  
- Scope: 12
- Key Terms: 12
- Principals: 13
- Administrators: 13
- Inheritance: 13
- Permissions: 13
- Permissions by Task: 14
- Row-Level Access: 16
- Column-Level Access: 19
CAS Authorization: Overview

To learn about the Cloud Analytic Services (CAS) authorization system, see Concepts.

To manage access, use the interface that best meets your needs. Here are suggestions:

- To interactively manage access, use the Authorization window (or, in a programming-only deployment, use CAS Server Monitor).
- To script management of CAS access controls in a full deployment, use the command-line interface. See CLI Examples: CAS Authorization in SAS Viya Administration: Using the Command-Line Interfaces.
- For comprehensive programmatic management of CAS access controls, use CAS actions. See the Access Control action set in SAS Viya: System Programming Guide.

CAUTION! Do not rely exclusively on CAS access controls to protect data. You must also consider direct host access. See Host Access Considerations.

CAS Authorization: How to (Authorization Window)

Introduction

These instructions explain how to manage access to caslibs, tables, and rows using SAS Environment Manager.
Navigation

1. In SAS Data Explorer, locate and select a global caslib or table.

   **TIP** You can access SAS Data Explorer by selecting Manage Environment from the applications menu (≡) and then clicking in the navigation bar. For other access methods, see SAS Data Explorer and the Choose Data Window in SAS Data Explorer: User’s Guide.

2. Right-click, and select View authorization or Edit authorization.

   **Note:** If Edit authorization is not enabled, you are not authorized to modify access to the selected object.

Examine Access

Scope

The scope of the display is as follows:

- There is always a row for Authenticated Users.
- There is always a row for you, the currently connected user who is using the display.
- There is a row for each principal that is assigned to an access control that affects access to the current object.
- If you add an identity and do not give that identity at least one direct setting, that identity is automatically removed from the display.
- You cannot directly remove a row. If you remove all direct settings for an identity and there is no other reason for that identity to be displayed, that identity is automatically removed from the display.
- Only the permissions that are relevant for an object (directly or for inheritance purposes) are displayed for that object.
- The display does not reflect the impact of CAS role membership or status.

Permissions

For each principal and permission, the following icons describe effective (net) access to the current caslib or table.

<table>
<thead>
<tr>
<th>Icon</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>✅</td>
<td>Authorized</td>
</tr>
<tr>
<td>❌</td>
<td>Not Authorized</td>
</tr>
<tr>
<td>Ⓡ</td>
<td>Row-Level</td>
</tr>
<tr>
<td>ⓔ</td>
<td>Unknown</td>
</tr>
<tr>
<td>✷</td>
<td>Direct*</td>
</tr>
</tbody>
</table>

* Indicates that a permission is directly assigned to the specified principal on the current object.
**Access Levels**

The **Access Level** column provides an alternative to interacting with individual permissions.

- When you manage access, each access level is a shortcut for adding a set of direct access controls.
- When you view access information, each access level is a shorthand description of a set of effective permissions.

<table>
<thead>
<tr>
<th>Access Level</th>
<th>Permissions</th>
</tr>
</thead>
<tbody>
<tr>
<td>No access</td>
<td>None</td>
</tr>
<tr>
<td>Read</td>
<td>Only ReadInfo and Select</td>
</tr>
<tr>
<td>Write</td>
<td>All except ManageAccess and AlterCaslib</td>
</tr>
<tr>
<td>Full control</td>
<td>All</td>
</tr>
<tr>
<td>Custom</td>
<td>Any other combination, including any row-level access</td>
</tr>
</tbody>
</table>

**Table 1  Access Levels**

Note: Access levels exist only in the presentation layer in SAS Environment Manager. CAS stores and evaluates individual permissions, not cumulative access levels.

**Set an Access Level**

1. Open the Edit Authorization window for a CAS object.
2. If the principal that you want to work with is not already listed, click ![persona]. In the Add Identities window, move the user or group to the right pane, and click **OK**.
   
   **Note:** If guest access is enabled, you must select **Add Identities** after you click ![persona]. Or, if you need to add Guest to the display, select **Add Guest** after you click ![persona]. See **Guest Access** in *SAS Viya Administration: Authentication*.
3. In the **Access Level** column, click and drag a gauge to adjust access.
   
   **Note:** If a gauge is not displayed, select an access level other than **(custom)** from the drop-down list.
   
   **Note:** Each time you change an access level, direct access controls are added as needed to meet the definition of the new access level. If you want to discard all unsaved changes, click **Cancel**.
   
   **CAUTION! Reducing the access level for a group that you belong to might block your access.** To preserve your access, make sure you have a higher precedence (offsetting) direct grant. If you are a Superuser, this precaution is not strictly necessary.
4. If you modified access for a group, click **Preview**. Examine the impact of the change on other principals. For example, increasing the access level for Authenticated Users from **No access** to **Full control** affects all authenticated users who do not have a more specific denial.
5. Click **Save**.
Add a Direct Access Control

1 Open the Edit Authorization window for a CAS object.

2 If individual permissions are not already displayed, select the **Show individual permissions** check box.

3 If the principal that you want to work with is not already listed, click ![user or group]. In the Add Identities window, move the user or group to the right pane, and click **OK**.
   
   Note: If guest access is enabled, you must select **Add Identities** after you click ![user or group]. Or, if you need to add Guest to the display, select **Add Guest** after you click ![user or group]. See Guest Access.

4 Click the effective access icon (for example, ![access]) for the principal and permission that you want to modify.

5 In the pop-up window, select **Grant** or **Deny** in the **Direct Setting** drop-down list.
   
   **CAUTION!** Before you deny access for a group that you belong to, make sure you have a higher precedence (offsetting) direct grant. If you are a Superuser, this precaution is not strictly necessary.

6 If you modified access for a group, click **Preview** in the Edit Authorization window.
   
   - Notice that a diamond is displayed in the cell that you modified. The diamond indicates that effective access comes from a direct setting.
   - Examine the impact on other principals. For example, a direct denial for GroupA affects all members of GroupA who do not have their own direct settings.

7 Click **Save**.

Remove a Direct Access Control

1 Open the Edit Authorization window for a CAS object.

2 In a cell that includes a diamond, click the effective access icon.

3 In the pop-up window, select **(none)** from the **Direct settings** drop-down list.

4 In the Edit Authorization window, notice that the new effective access value is unknown (○). Click **Preview**.
   
   - Notice that the new effective access value is known. Or, if you removed the only setting that made the associated user or group a relevant principal for the current object, the user or group is no longer included in the display.
   - If you modified access for a group, examine the impact on other principals.

5 Click **Save**.

Remove Multiple Direct Access Controls

1 Open the Edit Authorization window for a CAS object.

2 In a row that includes at least one direct setting, click the first cell. The row is selected.

3 Click ![X] to remove all direct access controls for the selected identity.

4 Notice that effective access for any affected cells is unknown (○). Click **Preview**.
Notice that all effective access values are known. Or, if the associated user or group is no longer a relevant principal for the current object, the user or group is no longer included in the display.

If you modified access for a group, examine the impact on other principals.

Click **Save**.

**Examples: Manage Access to a Caslib**

**Provide Public Access to a Caslib**
To give all users Read access to a new global caslib that you added:

1. Open the caslib’s Edit Authorization window. (See [Navigation](#).)
2. In the row for Authenticated Users, increase the **Access Level** to **Read**.
3. Click **Save**.

**Provide Selective Access to a Caslib**
To give a particular user Read and Write access to a new global caslib that you added:

1. Open the caslib’s Edit Authorization window. (See [Navigation](#).)
2. Click in the table toolbar.
3. In the left pane of the Add Identities window, locate the user. Move the user to the right pane, and click **OK**.
4. In the Edit Authorization window, increase the user’s **Access Level** to **Write**.
5. Click **Save**.

**Block All Access to a Caslib**
To block all access for a particular identity:

1. Open the caslib’s Edit Authorization window. (See [Navigation](#).)
2. If the identity is not already listed, click in the table toolbar.
   
   In the left pane of the Add Identities window, locate the user, group, or custom group that you want to block. Move that identity to the right pane, and click **OK**.
3. In the Edit Authorization window, decrease the identity’s **Access Level** to **None**.
4. If the identity is not an individual user, click **Preview**. Examine the impact of your change on other listed identities.
5. Click **Save**.

**Limit Write Access to a Caslib**
To allow only Read access for a particular identity:

1. Open the caslib’s Edit Authorization window. (See [Navigation](#).)
2 If the identity is not already listed, click in the table toolbar.
   In the left pane of the Add Identities window, locate the user, group, or custom group that you want to block. Move that identity to the right pane, and click OK.

3 In the Edit Authorization window, decrease the identity’s Access Level to Read.

4 If the identity is not an individual user, click Preview. Examine the impact of your change on other listed identities.

5 Click Save.

Provide Row-Level (Filtered) Access

To make different subsets of rows available to different identities, set one or more row-level grants. Each row-level grant includes a filter that limits the available rows.

1 Open the Edit Authorization window for a CAS table.

2 If the principal that you want to work with is not already listed, click in the Add Identities window, move the user or group to the right pane, and click OK.
   Note: If guest access is enabled, you must select Add Identities after you click . Or, if you need to add Guest to the display, select Add Guest after you click . See Guest Access in SAS Viya Administration: Authentication.

3 If individual permissions are not displayed, select the Show individual permissions check box.

4 In the Select column, click an effective access icon.

5 In the pop-up window, select Row-level Grant from the Direct setting drop-down list.

6 In the Row-Level Filter window:
   a Specify an expression that includes only the rows that the principal should be able to access. The basic format is: column-name operator value. Here are basic examples:

<table>
<thead>
<tr>
<th>Type of Filter</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>Numeric</td>
<td>sales&lt;1000</td>
</tr>
<tr>
<td>Character</td>
<td>Make='Ford'</td>
</tr>
<tr>
<td>Dynamic</td>
<td>user='SUB::SAS.Userid'</td>
</tr>
</tbody>
</table>

   For details, see Row-Level Access.
   Note: If you view or edit a filter that was initially created programmatically, you might see escape characters and a different pattern of quotation marks.

   b Click OK.

7 In the Edit Authorization window, next to the new setting, notice that a diamond is displayed. The diamond indicates that effective access comes from a direct setting.

8 If you modified access for a group, click Preview. Examine the impact on other principals.

9 Click Save.
Identify the Source of Effective Access

To determine which access control causes a particular effective access result, examine the origins information for that result.

1. Open the View Authorization window for the target CAS object.
2. Click the effective access icon for which you want origins information.
3. In the pop-up window, next to the Effective Access value, click 📊.
   
   Note: The icon is disabled if you have changes that you have neither saved nor previewed.

4. In the Origins window, review the displayed information.
   - The Source object field indicates where the determinative access control is set.
   - The Principals field indicates which identity the determinative access control are assigned to.

   Note: If multiple access controls of equal precedence cause the result, multiple principals are listed.

   For more information, see Origins of Effective Access.

CAS Authorization: How to (CAS Server Monitor)

Introduction

These instructions explain how to manage access to global caslibs using CAS Server Monitor in a programming-only deployment.

TIP To manage access at the table, column, or row level, use another interface.

Navigation

1. In CAS Server Monitor, beneath the SAS Cloud Analytic Services banner, click 🗝.
2. On the Configuration page, select Access Controls.
3. In the Caslibs list, select the caslib.

Here are details:
- All of the global caslibs that you are authorized to see are listed.
- To see any new global caslibs, click 🗝. The Caslibs list is not updated automatically.
- Session and personal caslibs are not listed because you cannot set access controls on them. Resources in session and personal caslibs are not sharable with other users.
- The Global Caslib Creation and Session Caslib Creation caslibs do not contain data. These special caslibs determine which non-administrators can add and delete caslibs. See Caslib Management Privileges in SAS Viya Administration: SAS Cloud Analytic Services.
- Any predefined caslibs have appropriate access controls.
Examine Access to a Caslib

On the Configuration page, under Access Controls, the columns for the selected caslib are populated as follows:

<table>
<thead>
<tr>
<th>Column</th>
<th>Content</th>
</tr>
</thead>
<tbody>
<tr>
<td>Applies To</td>
<td>Specifies a type of access control principal.</td>
</tr>
<tr>
<td>Identity</td>
<td>Specifies the name (unique identifier) for an access control principal.</td>
</tr>
<tr>
<td>Grant</td>
<td>A check mark indicates that access to the selected caslib is authorized for the specified principal and permission.</td>
</tr>
<tr>
<td>Deny</td>
<td>A check mark indicates that access to the selected caslib is not authorized for the specified principal and permission.</td>
</tr>
<tr>
<td>Activity</td>
<td>Specifies a permission, such as Select.</td>
</tr>
</tbody>
</table>

The rows for a new custom caslib are initially populated as follows:

- For the user who added the caslib, there is initially a row for every permission, because that user has a direct setting for each permission.
- For Authenticated Users, there is always a row for every permission, because Authenticated Users has an inherited setting for each permission.
- For other identities, there is a row for each direct setting. For example, if UserA has a direct grant of the Select permission, there is a Select row for UserA.

Provide Public Access to a Caslib

To give all users access to a new global caslib that you added:

1. On the Configuration page, select Access Controls.
2. In the Caslibs pane, select the caslib.
3. Click Edit.
4. In the Edit Access Controls window, adjust settings as follows:
   a. In the Authenticated Users row for Read Info, select the Grant radio button.
   b. Click Add Row. In the new row at the end of the page, select Authenticated Users, the Grant radio button, and the Select activity.
   c. If you want to also provide Write access, add rows that grant the following additional permissions to Authenticated Users: Insert, Update, Delete, Create Table, Drop Table, Delete Source, Alter Table, Limited Promote, Promote Table (Promote).

   **TIP** As an alternative to adding each row individually, click Add Set, and select Add Set from the drop-down list. In the new Authenticated Users rows for Alter Caslib and Manage Access, click ⭕ to delete those direct access controls. In the remaining new rows, select the Grant radio button.
Selectively Grant Access to a Caslib

This example gives UserA Read and Write access to a new global caslib that you added:

1. On the Configuration page, under Access Controls, select the caslib.
2. Click Edit.
3. In the Edit Access Controls window, click Add Set, and select Add User Set from the drop-down list.
4. In the next window, enter UserA in the User name field. Click OK.
5. In the Edit Access Controls window, select the Grant radio button in each UserA row, except the Alter CASLib and Manage Access rows.
6. At the end of UserA’s Alter CASLib and Manage Access rows, click 
7. Click OK to save your changes.
8. Under Access Controls, review the results of your changes.

Note: UserA does not have rows for Alter CASLib and Manage Access, because you did not give UserA direct access controls for those permissions. Unless UserA is a member of a group that has direct access controls for those permissions, UserA’s effective access for those permissions comes from Authenticated Users.

Here are some additional details about editing access controls:

- To add a single row, click Add Row.
- To provide a complete set of editable rows for an identity, click Add Set and then select the appropriate item:
  - For a group, select Add Group Set.
  - For a user, select Add User Set.
  - For Authenticated Users, select Add Set.
  - For guest users, select Add Guest Set.
    Note: By default, guest access is not enabled. See Guest Access in SAS Viya Administration: Authentication.
- To delete a direct access control, click 
- You cannot change or delete inherited settings. You can add a direct access control that has precedence over an inherited setting.
Selectively Limit Access to a Caslib

About Setting Direct Denials

**CAUTION!** Identity names that you enter are not validated. For sensitive data, do not grant access to Authenticated Users and then rely on selective direct denials. The safer practice is to verify that access is broadly denied, and then grant access selectively.

**CAUTION!** Do not block your own access. Before you add a direct denial for a group that you belong to, make sure you have a higher precedence (offsetting) direct grant. If you are a CAS administrator (Superuser) or Data administrator, this precaution is not strictly necessary.

Block All Access for an Identity

To block all access for an identity:

1. On the **Configuration** page, under **Access Controls**, select the caslib.
2. Click **Edit**.
   
   Note: If the **Edit** button is disabled, you are not authorized to set permissions for the selected caslib.
3. In the **Edit Access Controls** window, click **Add Row**.
4. In the new row, select an identity type, enter a name (unique identifier), make sure the **Deny** radio button is selected, and select the **Read Info** activity.
5. Click **OK** to save your changes.
6. Under **Access Controls**, review the results of your changes.

Block Write Access for an Identity

To block Write access for an identity:

1. On the **Configuration** page, under **Access Controls**, select the caslib.
2. Click **Edit**.
   
   Note: If the **Edit** button is disabled, you are not authorized to set permissions for the selected caslib.
3. In the **Edit Access Controls** window, click **Add Set**, and select **Add Group Set** or **Add User Set**.
4. In the next window, enter the user or group name (unique identifier). Click **OK**.
5. In the identity’s **Read Info** and **Select** rows, click **Deny**.
6. In the identity’s remaining rows, make sure the **Deny** radio button is selected.
7. Click **OK** to save your changes.
8. Under **Access Controls**, review the results of your changes.

Resolve Duplicate Access Controls

You cannot save more than one direct setting for a particular caslib, principal, and permission. Here are examples:
You cannot save two direct grants of the Update permission for UserA on caslibA.

You cannot save both a direct denial and a direct grant of the ReadInfo permission for UserA on caslibA.

If the error message Access control has duplicates is displayed twice in the Edit Access Controls window, there is one duplicate direct setting. Delete one of the settings that have the error message. One error message remains. You can now save your changes by clicking OK again.

CAS Authorization: Concepts

Scope

CAS authorization manages access to the following CAS objects:
- caslibs
- CAS tables and columns
- CAS action sets and actions

CAS authorization requirements do not apply in the following circumstances:
- The requesting user has assumed a role that is exempt from all applicable authorization requirements. For example, the user has assumed the Superuser role, and the request is to add a caslib.
- The target object is not potentially sharable. For example, the target is a table in a personal caslib, a session caslib, or the session scope of a global caslib.

Note: Not all interfaces expose all aspects of CAS authorization.

Key Terms

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access control</td>
<td>A composite of authorization elements.</td>
</tr>
<tr>
<td></td>
<td>Example: An access control grants ReadInfo to GroupA on caslibA.</td>
</tr>
<tr>
<td>Target</td>
<td>A resource.</td>
</tr>
<tr>
<td></td>
<td>Examples: tableA, caslibA</td>
</tr>
<tr>
<td>Principal</td>
<td>The user, group, or construct to which an access control is assigned.</td>
</tr>
<tr>
<td></td>
<td>Examples: UserA, GroupA, Authenticated Users</td>
</tr>
<tr>
<td>Permission</td>
<td>A type of access.</td>
</tr>
<tr>
<td></td>
<td>Values: ReadInfo, Select, LimitedPromote, Promote, CreateTable, DropTable, DeleteSource, Insert, Update, Delete, AlterTable, AlterCaslib, ManageAccess</td>
</tr>
<tr>
<td>Setting</td>
<td>An indication of whether (and to what extent) access is provided.</td>
</tr>
<tr>
<td></td>
<td>Values: Grant, Row-Level Grant, Deny</td>
</tr>
<tr>
<td>Filter</td>
<td>In a row-level grant of the Select permission, the constraint expression.</td>
</tr>
<tr>
<td></td>
<td>Example: User='SUB::SAS.Userid', sales&gt;1000</td>
</tr>
<tr>
<td>Term</td>
<td>Definition</td>
</tr>
<tr>
<td>--------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Effective access</td>
<td>A context-neutral description of the net result of all relevant access controls. Values: Authorized, Not Authorized, Row-Level</td>
</tr>
<tr>
<td>Access outcome</td>
<td>In an access request, the authorization decision. Values: Authorized, Not Authorized, Row-Level Authorization</td>
</tr>
</tbody>
</table>

**Principals**

The principal in an access control is the user, group, or construct to which the access control is assigned. The CAS authorization system supports the following principals:

- an individual authenticated user
- a user group (a custom group or a group in your authentication provider)
- Authenticated Users (the construct that represents all authenticated users)
  
  **Note:** In some programmatic contexts, this construct corresponds to the group that is named `*`.
- Guest (the identity type that facilitates guest access)
  
  **Note:** Guest is not part of Authenticated Users.

**Administrators**

CAS roles provide per-server assumable access to administrative functionality. For example, the Superuser role is exempt from authorization requirements throughout a CAS server, except for data access requests. See CAS Server Roles in SAS Viya Administration: Identity Management.

**Inheritance**

Access flows through a hierarchy of objects. Each parent object conveys settings to its child objects. Each child object inherits settings from its parent object.

Here are the inheritance relationships:

- Access flows from a caslib to its tables.
- Access flows from a table to its columns.
- Access flows from an action set to its actions.

**Note:** Each caslib always has inherited denials of all permissions for Authenticated Users. Those inherited denials prevent access if there are no higher precedence grants.

**Permissions**

<table>
<thead>
<tr>
<th>Permission</th>
<th>Data Enforcement Levels</th>
<th>Affected Activities</th>
</tr>
</thead>
<tbody>
<tr>
<td>ManageAccess</td>
<td>✓</td>
<td>✓</td>
</tr>
</tbody>
</table>

*Data Enforcement Levels: Caslib, Table, Column*
<table>
<thead>
<tr>
<th>Permission</th>
<th>Data Enforcement Levels*</th>
<th>Affected Activities</th>
</tr>
</thead>
<tbody>
<tr>
<td>ReadInfo</td>
<td>✓</td>
<td>View and traverse objects.</td>
</tr>
<tr>
<td>LimitedPromote</td>
<td>✓</td>
<td>Promote from source in the same caslib.**</td>
</tr>
<tr>
<td>Promote</td>
<td>✓</td>
<td>Promote from any caslib.</td>
</tr>
<tr>
<td>CreateTable</td>
<td>✓</td>
<td>Save (persist) a table.</td>
</tr>
<tr>
<td>DeleteSource</td>
<td>✓</td>
<td>Delete a physical source table.***</td>
</tr>
<tr>
<td>DropTable</td>
<td>✓</td>
<td>Remove a table from global scope.***</td>
</tr>
<tr>
<td>Select</td>
<td>✓</td>
<td>Read data values.</td>
</tr>
<tr>
<td>AlterCaslib</td>
<td>✓</td>
<td>Change the properties of a caslib.</td>
</tr>
<tr>
<td>AlterTable</td>
<td>✓</td>
<td>Change the attributes or structure of a table.</td>
</tr>
<tr>
<td>Insert</td>
<td>✓</td>
<td>Add rows.</td>
</tr>
<tr>
<td>Delete</td>
<td>✓</td>
<td>Delete rows.</td>
</tr>
<tr>
<td>Update</td>
<td>✓</td>
<td>Change data values.</td>
</tr>
<tr>
<td>Execute</td>
<td>✓</td>
<td>Run an action.</td>
</tr>
<tr>
<td>Load</td>
<td></td>
<td>Load an action set.</td>
</tr>
</tbody>
</table>

* You can set permissions at or above the level where they are enforced. See also [Access to Actions](#).

** If no table is specified in the request, LimitedPromote is checked at the caslib level.

*** To delete any direct access controls, the ManageAccess permission is required.

### Permissions by Task
To complete a task, you must have sufficient access to all relevant data objects. The following tables document permissions that are required for selected tasks.

#### Table 2  Simple Tasks

<table>
<thead>
<tr>
<th>Task (CAS Action)</th>
<th>Caslib</th>
<th>Table</th>
<th>Column</th>
</tr>
</thead>
<tbody>
<tr>
<td>Set caslib permissions</td>
<td>ReadInfo  ManageAccess</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Modify caslib properties</td>
<td>ReadInfo  AlterCaslib</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Set table permissions</td>
<td>ReadInfo  ReadInfo  ManageAccess</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Task (CAS Action)</td>
<td>Caslib</td>
<td>Table</td>
<td>Column</td>
</tr>
<tr>
<td>------------------------------------------</td>
<td>--------</td>
<td>----------------</td>
<td>--------</td>
</tr>
<tr>
<td>Modify table properties*</td>
<td>ReadInfo</td>
<td>ReadInfo</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Select</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>AlterTable</td>
<td></td>
</tr>
<tr>
<td>Load a table from a caslib's data source (loadTable)</td>
<td>ReadInfo</td>
<td>ReadInfo</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Select</td>
<td></td>
</tr>
<tr>
<td>Transfer and load an entire file (upload)</td>
<td>ReadInfo</td>
<td>ReadInfo</td>
<td>-</td>
</tr>
<tr>
<td>Transfer rows to the server (addTable)</td>
<td>ReadInfo</td>
<td>ReadInfo</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Select</td>
<td></td>
</tr>
<tr>
<td>Move a table to global scope (promote)</td>
<td>ReadInfo</td>
<td>ReadInfo</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Promote**</td>
<td></td>
</tr>
<tr>
<td>Remove a table from global scope (dropTable)</td>
<td>ReadInfo</td>
<td>ReadInfo</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td></td>
<td>DropTable</td>
<td></td>
</tr>
<tr>
<td>Delete a file (deleteSource)</td>
<td>ReadInfo</td>
<td>ReadInfo</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td></td>
<td>DeleteSource</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>(ManageAccess)**</td>
<td></td>
</tr>
<tr>
<td>Persist a file (save)</td>
<td>ReadInfo</td>
<td>ReadInfo</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td></td>
<td>CreateTable</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>(DeleteSource)†</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Read data</td>
<td>ReadInfo</td>
<td>ReadInfo</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Select</td>
<td></td>
</tr>
<tr>
<td>Insert rows</td>
<td>ReadInfo</td>
<td>ReadInfo</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Insert</td>
<td></td>
</tr>
<tr>
<td>Update rows</td>
<td>ReadInfo</td>
<td>ReadInfo</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Select</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Update</td>
<td></td>
</tr>
<tr>
<td>Delete rows††</td>
<td>ReadInfo</td>
<td>ReadInfo</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Select</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Delete</td>
<td></td>
</tr>
</tbody>
</table>

* You cannot alter a table that has fine-grained constraints (row-level filters or column-level denials) that apply to you.

** For promotion of a table within the same caslib, LimitedPromote for the table (instead of Promote for the caslib) is sufficient.

*** ManageAccess is required if the request involves deletion of direct access controls.

† DeleteSource is required to replace a source table.

†† This entry is included only for completeness. Currently, there is no CAS action for deleting rows.
### Table 3  Compound Tasks

<table>
<thead>
<tr>
<th>Task (CAS Actions)</th>
<th>Required Permissions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Import (upload + save + dropTable + loadTable + promote)</td>
<td>Caslib: ReadInfo, CreateTable, Promote′</td>
</tr>
<tr>
<td></td>
<td>Table: ReadInfo, Select, (DeleteSource, DropTable)</td>
</tr>
<tr>
<td>Just-in-time load (loadTable + promote)</td>
<td>Caslib: ReadInfo, Promote′</td>
</tr>
<tr>
<td></td>
<td>Table: ReadInfo, Select</td>
</tr>
<tr>
<td>Delete a global-scope table (dropTable + deleteSource)</td>
<td>Caslib: ReadInfo</td>
</tr>
<tr>
<td></td>
<td>Table: ReadInfo, DeleteSource, DropTable</td>
</tr>
</tbody>
</table>

* LimitedPromote for the table (instead of Promote for the caslib) is sufficient.

** DeleteSource is required to replace a source table. DropTable is required to replace a global-scope table.

For information about who can add and delete caslibs, see Caslib Management Privileges in SAS Viya Administration: SAS Cloud Analytic Services.

### Row-Level Access

#### Overview of Row-Level Access

A row-level grant includes a filter that limits the Select permission on a table. A user who has row-level access to a table can view only those rows that are within the associated filter. See also Application and Persistence.

For example, you can use a row-level grant to enable groupA to see only those rows in tableA where the value in the Toy_Price column is 25. Here is an overview of the process:

1. On tableA, give groupA a row-level grant of Select permission.
   
   Specify the following filter: \( \text{Toy\_Price}=25 \)
   
   **Note:** For detailed instructions, see “Provide Row-Level (Filtered) Access”.

2. Make sure that groupA has ReadInfo access to tableA and its parent caslib.

3. Make sure that groupA is not a member of another group that has a grant or denial of the Select permission on tableA.

4. Verify that when a member of groupA accesses tableA, the expected rows are returned.

#### Syntax for Row-Level Filters

<table>
<thead>
<tr>
<th>Operator (Alias)</th>
<th>Example Filter</th>
</tr>
</thead>
<tbody>
<tr>
<td>Contains (?)</td>
<td>( \text{Toy_Type} \text{ Contains 'cars'} )</td>
</tr>
<tr>
<td>Not Contains</td>
<td></td>
</tr>
<tr>
<td>In</td>
<td>( \text{Toy_Type} \text{ In ('dolls' 'cars' 'animals')} )</td>
</tr>
<tr>
<td>Not In</td>
<td></td>
</tr>
<tr>
<td>Operator (Alias)</td>
<td>Example Filter</td>
</tr>
<tr>
<td>-----------------</td>
<td>----------------</td>
</tr>
<tr>
<td>Between</td>
<td>Toy_Price Between 20 AND 30</td>
</tr>
<tr>
<td>Not Between</td>
<td>Toy_Type Like 'd%'</td>
</tr>
<tr>
<td>= (EQ)</td>
<td>Toy_Price=25</td>
</tr>
<tr>
<td>&gt; (GT)</td>
<td>Profit &gt; (Sales * .5)</td>
</tr>
<tr>
<td>&lt; (LT)</td>
<td></td>
</tr>
<tr>
<td>&lt;&gt;</td>
<td></td>
</tr>
<tr>
<td>&gt;= (GE)</td>
<td></td>
</tr>
<tr>
<td>&lt;= (LE)</td>
<td></td>
</tr>
<tr>
<td>^= (NE, ~=)</td>
<td></td>
</tr>
<tr>
<td>+</td>
<td></td>
</tr>
<tr>
<td>-</td>
<td></td>
</tr>
<tr>
<td>/</td>
<td></td>
</tr>
<tr>
<td>*</td>
<td></td>
</tr>
<tr>
<td>**</td>
<td></td>
</tr>
<tr>
<td>()</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>AND (&amp;)</td>
<td>Toy_Type='cars' OR Toy_Type='dolls'</td>
</tr>
<tr>
<td>OR (</td>
<td>, !)</td>
</tr>
<tr>
<td>NOT</td>
<td></td>
</tr>
<tr>
<td>Is Missing</td>
<td>Toy_Type Is Not Null</td>
</tr>
<tr>
<td>Is Not Missing</td>
<td></td>
</tr>
<tr>
<td>Is Null</td>
<td></td>
</tr>
<tr>
<td>Is Not Null</td>
<td></td>
</tr>
</tbody>
</table>

**Identity-Based Substitution**

Identity-based substitution is a powerful and concise technique for defining row-level access. You can use substitution to implement any number of per-user access distinctions with a single row-level filter.

Identity-based substitution parameters map a user’s authenticated ID or group memberships to values in a specified column in your data. Values are dynamically substituted into the filter at run time, as appropriate for each requesting user. Here are the supported substitution parameters:
### Substitution Parameters Table

<table>
<thead>
<tr>
<th>Substitution Parameter</th>
<th>Description and Example</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>SUB::SAS.Userid</strong></td>
<td>Determines whether a data value is the same as the requesting user’s authenticated ID.</td>
</tr>
<tr>
<td></td>
<td><code>empID='SUB::SAS.Userid'</code></td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> If the casing of your user IDs might not match the casing of corresponding values in your data, use the <code>upcase</code> function on both sides of the expression. For example: <code>upcase(empID)=upcase('SUB::SAS.Userid')</code></td>
</tr>
<tr>
<td><strong>SUB::SAS.IdentityGroups</strong></td>
<td>Determines whether a data value matches any of the requesting user’s group memberships.</td>
</tr>
<tr>
<td></td>
<td><code>FacilityRegion In ('SUB::SAS.IdentityGroups')</code></td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> The comparison is against each group’s unique name, so your data must contain unique group names. In a group definition in SAS Environment Manager, the <strong>Group ID</strong> field contains the group’s unique name.</td>
</tr>
</tbody>
</table>

Here are additional details:

- Only the substitution parameters in the preceding table are supported. (Other substitution parameters that are supported in SAS 9 are not applicable in SAS Viya.)
- Both substitution parameters return values in the casing in which they are received. (In SAS 9, the `SAS.Userid` parameter always returns values in the uppercase format.)
- You can use the `accessControl.isAuthorizedTables` action to see how an identity-driven filter resolves for you.

### Example: User ID Substitution

If a `tableB` has an `empID` column with values that match the user IDs with which users authenticate, you might assign this filter to Authenticated Users:

```
empID='SUB::SAS.Userid'
```

At request time, each user’s ID is substituted into the right side of the expression. In a request from userA, the expression resolves as:

```
empID='userA'
```

As a result, userA gets only those rows where the value in the `empID` column is `userA`.

### Example: Membership Substitution

If `tableC` has a `FacilityRegion` column with values that match the unique names for user groups, you might assign this filter to an AllRegions group:

```
FacilityRegion In ('SUB::SAS.IdentityGroups')
```

At request time, each affected user’s list of group memberships is substituted into the right side of the expression. In a request from user13 (who is a member of the grp7, grp9, and AllRegions groups), the expression resolves as:

```
FacilityRegion In ('grp7','grp9','AllRegions')
```

As a result, user13 gets only those rows where the value in the `FacilityRegion` column is `grp7`, `grp9`, or `AllRegions`.

**Note:** Authenticated Users is not one of the listed memberships, because it is an access control principal, not a user group.
Using Functions in Row-Level Filters

Not all functions work in row-level filters. The following functions are supported:
- upcase
- lowcase
- substr

Other functions might work, but are outside the current scope of support.

Multiple Filters and Cumulative Access

If multiple row-level filters are applicable to a user, only the highest precedence filter provides access. If there is an identity precedence tie (the user is a member of multiple groups, each of which has a filter), the user can access any row that meets any of the filters.

Here are details:

The filters for multiple row-level grants provide cumulative access only if all of the following circumstances exist:
- The requesting user does not have a direct access control for the Select permission.
- None of the requesting user’s groups have a direct grant or denial for the Select permission.
- Two or more of the requesting user’s groups have row-level grants.

Note: All custom and LDAP groups have equal precedence, regardless of any nested memberships.

Note: A filter for a row-level grant that is assigned to Authenticated Users is never cumulative (joined with other filters by OR). Authenticated Users is a construct that has lower precedence than any group.

Column-Level Access

CAS supports column-level permissions, where a user can access some (but not all) columns in a table. You can use the Access Control action set to set column-level permissions. See also Application and Persistence.

To prevent a user from accessing a column, deny the user both the ReadInfo permission and the Select permission for that column. Denying both permissions ensures that the user cannot access the column through any CAS action or interface.

Note: Do not rely exclusively on a denial of the ReadInfo permission on a column to hide that column. Not all CAS actions require the ReadInfo permission at the column level.

CAUTION! Not all interfaces can successfully interact with tables that have column-level permissions. Before you provide a production implementation of column-level permissions, verify that results in all applicable interfaces are acceptable.

For example, in SAS Visual Analytics, column-level access is not supported and can yield unexpected results. If userA lacks access to any column that is included in a SAS Visual Analytics report object, userA cannot see any data in that report object.

Access to Actions

Action sets and actions that have no access controls are available to all authenticated users. As a result, almost all action sets and actions are available to all users. In general, the ability to perform a particular task is managed by access controls on the target data, not by access controls on actions.

An exception is actions for adding nodes and stopping the server. The initial configuration denies Authenticated Users the Execute permission for those actions. Initially, only Superusers can add nodes or stop the server.
Here are additional details:

- The ReadInfo and Execute permissions are enforced for actions.
- The ReadInfo and Load permissions are enforced for action sets.
- Unregistered action sets are subject to access constraints that are defined on the _UNREGISTERED action set. The initial configuration denies Authenticated Users the Load permission on the _UNREGISTERED action set.

**Note:** An unregistered action set is an action set that is not listed in the database of action sets that SAS provides. SAS solutions use only registered action sets.

**Note:** An attempt to load an action set that does not exist generates an access denied error message, because no such action set is known and registered. For example, if you do not correctly specify the action set name in a load request, an access denied error message is generated.

- The identity type Guest has the same access to non-administrative actions as Authenticated Users. That access is relevant only for sites that choose to enable guest access. See Guest Access in SAS Viya Administration: Authentication.

### Authorization Decisions

#### Precedence

In the CAS authorization system, precedence is determined by where an access control is set and who an access control is assigned to.

- Direct access controls have precedence over inherited settings.
- The principal precedence hierarchy is relatively flat. It consists of only the following three levels: 1) individual users, 2) user groups, and 3) the construct Authenticated Users.

**Note:** All user group memberships are at the same level of precedence, even if groups are nested.

Direct access controls have precedence over inherited access controls, regardless of who the principal is. For example, if only the following access controls exist, then UserA cannot access TableA:

- UserA has a direct grant of ReadInfo on caslibA.
- Authenticated Users has a direct denial of ReadInfo on TableA, which is in caslibA.

**Note:** One way to enable UserA to access TableA is to add a direct grant of ReadInfo for UserA on TableA. UserA's direct grant has precedence over the direct denial for Authenticated Users.

#### How Access Is Evaluated

Each access request initiates an authorization decision process. That process terminates when an outcome is reached. For example, here is the authorization decision process for the Select permission in a request to access data in a CAS table:

1. If there are relevant direct access controls on the table, those access controls determine the outcome as follows:
   a. If there is a setting that is specifically assigned to the requesting user, that setting determines the outcome.
   b. If there is a denial from a group, the outcome is Not Authorized.
   c. If there is a grant from a group, the outcome is Authorized.
If there is exactly one row-level grant from a group, the outcome is Row-Level Authorization (authorized for rows within the applicable filter).

If there are two or more row-level grants from groups, the outcome is Row-Level Authorization (authorized for any row that is within any of the applicable filters). See Multiple Filters and Cumulative Access.

If there is a setting for Authenticated Users, that setting determines the outcome.

If there are no relevant direct access controls on the table, direct access controls on the parent caslib determine the outcome as follows:

- If there is a setting that is specifically assigned to the requesting user, that setting determines the outcome.
- If there is a denial from a group, the outcome is Not Authorized.
- If there is a grant from a group, the outcome is Authorized.
- If there is a setting for Authenticated Users, that setting determines the outcome.

If there are no relevant direct access controls on the table or the parent caslib, the outcome is Not Authorized.

Access Control Transactions

If you want to preview the results of changes to CAS access controls before you save those changes, use an access control transaction. Here are examples:

- When you have unsaved changes in a CAS object's Authorization window, you can click Preview. Review the results, and then save or cancel your changes.
- When you manage CAS authorization using the command-line interface, you can choose to check out an object, modify its access controls, and then commit or roll back the changes. In the command-line interface, a transaction is automatically started when you check out an object.
- When you manage CAS authorization programmatically, you can choose to start a transaction and check out one or more objects before you make changes. When the transaction is open, any whatIsEffective actions that you run incorporate the effects of your unsaved changes. Review the results, and then commit or roll back your changes.

Here are key points about access control transactions:

- This feature is for only changes to access controls. This feature does not provide transaction support for interactions with data or with any other aspect of CAS objects.
- In SAS Environment Manager, access control transactions are used when CAS access controls are managed.
- In programmatic and command-line interfaces, use of access control transactions is optional. You do not have to use a transaction in order to modify CAS access controls. Use access control transactions if you want to preview the results of your changes or ensure that nobody else is modifying access controls for the same objects at the same time.

Origins of Effective Access

Origins information explains effective access by answering the question: Why does this identity have this effective access to this object?
Origins information identifies the highest precedence access control that causes the access outcome for a particular identity, object, and permission. If there are multiple tied highest precedence access controls, origins information includes all of them. Additional, lower precedence controls are not included.

The following table provides simple examples of origins information. Each row in the table is for a different (independent) scenario. In each example, we are looking at why UserA has an effective access value of Not Authorized for the ReadInfo permission on TableA. UserA is a member of GroupA and GroupB. TableA is in CaslibA.

<table>
<thead>
<tr>
<th>Highest-Precedence Access Control (or Controls)</th>
<th>Origins Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>On TableA, a direct denial for UserA.</td>
<td>TableA, UserA</td>
</tr>
<tr>
<td>On TableA, a direct denial for GroupA.</td>
<td>TableA, GroupA</td>
</tr>
<tr>
<td>On TableA, direct denials for GroupA and GroupB.</td>
<td>TableA, GroupA, GroupB</td>
</tr>
<tr>
<td>On TableA, a direct denial for Authenticated Users.</td>
<td>TableA, Authenticated Users</td>
</tr>
<tr>
<td>On CaslibA, a direct denial for UserA.</td>
<td>CaslibA, UserA</td>
</tr>
<tr>
<td>On CaslibA, a direct denial for GroupA.</td>
<td>CaslibA, GroupA</td>
</tr>
<tr>
<td>On CaslibA, direct denials for GroupA and GroupB.</td>
<td>CaslibA, GroupA, GroupB</td>
</tr>
<tr>
<td>On CaslibA, a direct denial for Authenticated Users.</td>
<td>CaslibA, Authenticated Users</td>
</tr>
<tr>
<td>There are no relevant access controls.</td>
<td>Caslib default</td>
</tr>
</tbody>
</table>

**TIP** To obtain origins information in the Authorization window, see Identify the Source of Effective Access.

**Reduced Visibility: Hidden Caslibs**

A hidden caslib is omitted from most lists of caslibs. Tables in a hidden caslib are omitted from most lists of tables. A caslib is hidden if its hidden parameter is set to true. You can set the hidden parameter in the tables.addCaslib action.

Hiding a caslib does not protect the caslib or limit access to the caslib’s data. Hiding a caslib just reduces visibility by preventing the caslib and its tables from being listed in certain contexts. In those contexts, hidden caslibs and their tables are unlisted for all users and administrators, regardless of roles and access controls. Hiding a caslib affects everyone equally.

For example, two of the predefined caslibs (AppData and ReferenceData) are hidden. Users can use the data in those caslibs because appropriate predefined access controls are in place. However, those caslibs (and their tables) are not listed in most contexts. They are excluded from selection lists in SAS Visual Analytics.

**TIP** Hide a caslib only if you have users who must be able to use that caslib’s data but should not see that caslib or its tables in most lists.

Here are examples of contexts in which hidden caslibs are listed:
On the Data page in SAS Environment Manager, hidden caslibs are listed.

In the tables.caslibinfo action, hidden caslibs are listed if you specify the value true for the showHidden parameter.

Application and Persistence of CAS Access Controls

About This Topic

This topic applies to direct access controls at the table, column, and row levels. For conciseness, this topic refers to all such controls as table-level controls.

This topic refers to table-level controls being set on or persisted to a source file or in-memory table. That phrasing is an abstraction. On disk, CAS access controls are written to an item store. In the item store, each table-level control is associated with a metadata representation of either a source file or an in-memory table. For more information about the item store, see “cas.PERMSTORE=’path’” in SAS Viya Administration: SAS Cloud Analytic Services.

Name-Based Controls

Introduction

In CAS authorization, each table-level control is associated with either a source file or an in-memory table. In most cases, table-level controls are associated with source files. For simplicity and predictability, the best practice is to set controls on source files, because that ensures that the controls are associated with source files. Such controls are called source-based controls.

In certain specialized workflows, table-level controls are instead associated with in-memory tables. Such controls reference in-memory tables by their names, so they are called name-based controls. The following sections explain how name-based controls are created and used.

Creation of Name-Based Controls

In general, each table-level control that you set is tied to a source file for one of the following reasons:

- When you set the control, you specify or select a source file (for example, cars.sashdat).
- When you set the control, you specify or select an in-memory table (for example, CARS), and CAS persists the control to the corresponding source file (for example, cars.sashdat).

The exception, in which table-level controls are name-based, occurs in the following circumstances:

- You set controls on an in-memory table that has no corresponding source file.
- You set controls on an in-memory table that is disconnected from its source file (cross-caslib data).

<table>
<thead>
<tr>
<th>Table 5</th>
<th>Summary: Creation of Name-Based Controls</th>
</tr>
</thead>
<tbody>
<tr>
<td>Scenario</td>
<td>Is a Name-Based Control Created?</td>
</tr>
<tr>
<td>You set a direct access control on a source file.</td>
<td>No</td>
</tr>
<tr>
<td>You set a direct access control on an in-memory table that was loaded from a source file in the same caslib.</td>
<td>No</td>
</tr>
<tr>
<td>You set a direct access control on an in-memory table that was loaded from a source file in a different caslib.</td>
<td>Yes</td>
</tr>
</tbody>
</table>
Scenario: Are a Name-Based Control Created?

You set a direct access control on an in-memory table that has no corresponding source file. Yes

Important: The best practice is to set table-level controls on persisted data (data that has been saved as a source file within a caslib), not on in-memory data.

Usage of Name-Based Controls: Data Access

In general, table-level protections for in-memory data are provided by source-based controls. The exception, in which table-level protections are provided by name-based controls, occurs in the following circumstances:

- The in-memory table has no source file.
- The in-memory table has a source file that has no direct access controls.
  
  Note: Name-based controls are used in this circumstance only after an August 2020 hot fix.
- The in-memory table is disconnected from its source file. (The source file is in a different caslib.)

Table 6  Summary: Usage of Name-Based Controls for Access to In-Memory Data

<table>
<thead>
<tr>
<th>Scenario</th>
<th>Are Name-Based Controls Used?</th>
</tr>
</thead>
<tbody>
<tr>
<td>The in-memory table has a connected source file that has direct access controls.</td>
<td>No</td>
</tr>
<tr>
<td>The in-memory table has a connected source file that has no direct access controls.</td>
<td>Yes*</td>
</tr>
<tr>
<td>The in-memory table has no connected source file.</td>
<td>Yes</td>
</tr>
</tbody>
</table>

* After an August 2020 hot fix.

Usage of Name-Based Controls: Table Loads

Note: This section applies after an August 2020 hot fix. Prior to that hot fix, name-based controls are never used in evaluation of requests to load tables.

In evaluation of a request to load a table, name-based controls are used only if all of the following circumstances exist:

- The source file has no direct access controls.
- The destination in-memory table has name-based controls.
- The destination in-memory table is in the same global caslib as the source file.
- The load table request meets all of the following criteria:
  - The request specifies promote=True.
  - The request does not specify the vars parameter.
  - The request does not specify the where parameter.
  - The request either does not specify a name for the destination table or specifies the default name for the destination table (in the casOut parameter).
Disadvantages of Name-Based Controls

Although name-based controls can be useful in certain specialized workflows, relying on name-based controls is not a preferred approach. Here are key points to consider before using name-based controls:

- In the context of data access, name-based controls can be circumvented by specifying a different destination name in a load action.
- Name-based controls can duplicate or conflict with source-based controls, which might cause confusion or yield unintended results.

**TIP** If any source-based control exists for a table, no name-based controls are examined for that table. This differs from access control precedence, which examines only those controls that are relevant to a specific request.

- Name-based controls are created in only specific circumstances, and it is not always obvious whether those circumstances exist.

**TIP** If you want to avoid creating name-based controls, use the following practices:

- When you set access controls using a CAS action or command-line interface, specify a source file, including its file extension, in the table parameter.
- When you set access controls using SAS Data Explorer, open the CAS Authorization window from a source file, not an in-memory table.

- Name-based controls are used in only specific circumstances, and it is not always obvious whether those circumstances exist.

**TIP** The best way to avoid use of name-based controls is to make sure they are never created. If you want to minimize use of any name-based controls that are created, use the following practices:

- Avoid workflows that provide access to cross-caslib data.
- Avoid workflows that provide access to unpersisted in-memory data.

- Name-based controls are not included in responses to requests for authorization information for a source file. For example, any name-based controls for the in-memory table CARS are not included in a response to a request to list controls for the source file cars.sashdat. Similarly, any name-based controls for the in-memory table CARS are not included in a response to a request to describe effective access to the source file cars.sashdat.

Persistence of Access Controls

When You Save Data

When you save data, any direct access controls are managed as follows:

- If the original source file is replaced, direct access controls are persisted. A replacement can occur only for a source file that matches the specified output name and extension. Here are details:
  - For the file extension, replacement uses SASHDAT by default. For example, if the specified output name is cars, the resulting source file (cars.sashdat) can replace only an existing source file cars.sashdat, not an existing source file cars.csv.
For the file name, on a case-sensitive file system, replacement requires a case-sensitive match. For example, if the specified output name is cArS, the resulting source file on Linux (cArS.sashdat) can replace only an existing source file cArS.sashdat, not an existing source file cars.sashdat.

Note: If you do not meet the case-sensitive match requirement, you might have multiple source files that differ only in the casing of their names. In that situation, it is useful to understand that source file names are not case sensitive in the context of authorization. For example, if a caslib has loaded tables from two source files (cars.sashdat and cArS.sashdat), authorization processes do not distinguish one source file from the other. A single set of access controls applies to both source files and their loaded tables. Adding or deleting access controls for any of those entities affects all of those entities.

- If a new source file is created, direct access controls are not persisted to the new source file. Access to the new source file is determined by access controls on its parent caslib.
- If a different existing source file is overwritten, direct access controls are not persisted. Access to the existing source file is unaffected.

Here is an example:

1. You add access controls to the source file CARS.csv.
2. You load the source file CARS.csv to global scope.
3. You modify the in-memory table CARS (for example, you add a calculated column).
4. You save the in-memory table CARS, specifying to replace any existing same-named source file. In the save request, you do not specify a file extension.
5. A new source file CARS.sashdat is created. The access controls that you set on the source file CARS.csv are not replicated on the new source file.

Note: In this example, a replacement did not occur because the in-memory table was loaded from a CSV source file and you did not specify the CSV file extension as part of the output name in the save request.

In workflows that involve saving data, the best practice is to establish and maintain any direct access controls on the target (post-preparation) files. By default, such access controls survive activities such as deletion and replacement.

The Ambiguity Problem

If you specify or select an in-memory table when you set access controls, the results might be unexpected. In a caslib that contains multiple same-named source files, it might not be obvious which of those source files corresponds to the table that is currently in memory.

Here is an example:

1. caslibA includes the source files CARS.csv and CARS.sashdat.
2. Someone loads CARS.csv to global scope.
3. In SAS Data Explorer, someone else specifies or selects the in-memory table CARS when setting access controls, incorrectly assuming that they are protecting the source file CARS.sashdat.
4. The new access controls are written to the source file CARS.csv, not to the source file CARS.sashdat.

Considerations for Rows and Columns

Row-level filters and column-level access controls are applied to requests to access or save data, not to requests to load data. (There is an exception for loading of cross-caslib data.)

For example, if tableA has a row-level filter that enables userA to see only those rows where the value in the MAKE column is Ford, the filter is applied as follows:
If userA loads tableA, all rows are loaded.

If userA accesses tableA, userA sees only those rows where the value for MAKE is Ford.

As explained in the preceding sections, row-level filters and column-level access controls are not persisted when a user saves a table as a new or different table. The following information continues the preceding example:

If userA saves tableA to the file from which tableA was loaded, the replaced table contains only those rows where the value for MAKE is Ford. This reduction in scope affects all subsequent loads of tableA and all access by subsequent users. Some users might access fewer rows than intended. Because the row-level filter still exists on the source file and can further reduce access, no users access more rows than intended.

If userA saves tableA to a different file, the new source file contains only those rows where the value for MAKE is Ford. This reduction in scope affects all subsequent loads of tableA and all access by subsequent users. Some users might access fewer rows than intended. Because the row-level filter does not exist on the new source file, some users might access more rows than intended.

Considerations for Cross-Caslib Data

In most workflows, data does not move across caslibs. For example, when you load and promote data, you are usually performing a same-caslib activity, moving data from session scope to global scope in the same caslib.

In a few workflows, data does move across caslibs. For example, if you promote data from one caslib to another, or copy data from one caslib to another, you are performing a cross-caslib activity. The target data that results from a cross-caslib activity is referred to as cross-caslib data.

Cross-caslib data has no ongoing relationship to the source (original) caslib and file. Changes to access controls on the source caslib and file have no effect on cross-caslib data.

Access to cross-caslib data is subject to access controls on the target caslib and file. Avoid performing cross-caslib activities on sensitive data. If you must perform cross-caslib activities on sensitive data, make sure the target caslib and file have appropriate protections.

TIP If the source data for a cross-caslib activity has fine-grained constraints (row-level filters or column-level denials), make sure the cross-caslib activity is performed by an identity that has sufficient access to the source data. Any constraints on the source data are applied during the cross-caslib activity, and are based on the identity that performs the cross-caslib activity. Subsequent access to the cross-loaded data cannot be expanded to include data that was unavailable to the identity that performed the cross-caslib activity.

CAS Authorization: Guidelines

The following guidelines can contribute to simplicity and security:

- Limit membership in administrative roles.
- Minimize the use of individual tables as targets.
- Minimize the use of individual users as principals.
- Remember that any access that is not granted is implicitly denied. Do not set unnecessary denials.
- If you deny someone access to part of a table (using a column-level or row-level access control), make sure that identity cannot update or insert rows in that table.
- Perform a backup before and after you make significant changes to your system.
CAS Authorization: Troubleshooting

Unrecognized Principals
If the Authorization window displays a warning icon next to a principal’s name, that principal does not exist in the identities service.

- If the principal is a host account (for example, cas) that does not exist in your LDAP provider, you can ignore the warning icon.
- If the principal is an internal service account (for example, sas.ops-agentsrv, sas.searchIndex or sas.search), you can ignore the warning icon.
- If the principal should still exist in the identities service, make sure the identities service can still contact your LDAP provider.
- Otherwise, consider deleting the access controls that are assigned to the principal that no longer exists.
  Note: Deletion of a custom group does not cause automatic deletion of rules in which that custom group is the principal.

Inability to Modify Access

- Make sure the target object is global-scope (not in a personal caslib or session scope).
- Make sure you have the ManageAccess permission for the target object. Or, assume a role that is exempt from that permission requirement. See “Assume the Superuser Role” in SAS Viya Administration: Identity Management.
- If you get the following error: "The access controls for table {name} are being blocked by a loaded table of the same name", select or specify a source file (for example, tableA.sashdat), not an in-memory table. See “Application and Persistence of CAS Access Controls” on page 23.
- If you get the following error: "The object {name} {type} is currently locked, so you cannot modify its access controls", the target object is already participating in an active access control transaction. Either wait for the lock to be released, or terminate the CAS session in which the object is locked. See “Access Control Transactions” on page 21.

Unintended Loss of Access

Reinstall Access: Instructions for Users
If you inadvertently block your own access to an object, contact an administrator for assistance.

Note: Anyone who has the ReadInfo and ManageAccess permissions for the object can reinstall your access.

Reinstall Access: Instructions for Administrators
1 In the applications menu (≡), under Administration, select Manage Environment.
   Note: These instructions use SAS Environment Manager. You can instead use an alternate interface.
2 In the navigation bar, click ⌘.
3 On the Servers page, right-click on a server, and select Assume the Superuser role.

Note: If the Assume the Superuser role action is not available, you are not a member of the Superuser role for the selected server. If your Superuser role membership is exclusively through the SAS Administrators group, make sure you have opted in to that membership in your current session.

---

**CAS Authorization: Interfaces**

All CAS authorization requirements and constraints are always fully enforced. However, not all interfaces expose all CAS authorization features.

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

<table>
<thead>
<tr>
<th>Interface</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access Control action set</td>
<td>Programmatic interfaces for CASL (the CAS procedure), Python, Lua, and R.</td>
</tr>
<tr>
<td>REST API</td>
<td>The REST interface for CAS.</td>
</tr>
<tr>
<td>SAS Java Client Interface for SAS Viya</td>
<td>The Java programming interface for CAS actions.</td>
</tr>
<tr>
<td>Command-line interface</td>
<td>A simple, scriptable interface that includes commands for managing access at the caslib, table, and row levels in a full deployment.</td>
</tr>
<tr>
<td>SAS Environment Manager</td>
<td>A graphical web application for managing access at the caslib, table, and row levels in a full deployment.</td>
</tr>
<tr>
<td>CAS Server Monitor</td>
<td>A graphical web application for managing access at the caslib level in a programming-only deployment.</td>
</tr>
</tbody>
</table>

---

**CAS Authorization: Host Access Considerations**

**Why Host Access Matters**

If host-layer access requirements are not met, grants in the CAS authorization layer do not provide access.

If host-layer access protections are not in place, denials in the CAS authorization layer do not fully prevent access.
Which Host Account Matters

The account under which a CAS server process runs must have appropriate host-layer access to target directories and files. Depending on context, that account is either an individual user’s personal host account or the CAS server’s shared service account. The following table provides examples:

<table>
<thead>
<tr>
<th>Context</th>
<th>Identity of the CAS Process</th>
</tr>
</thead>
<tbody>
<tr>
<td>A request from the SAS Visual Analytics web application to a CAS server on Linux.</td>
<td>The CAS server’s shared service account.*</td>
</tr>
<tr>
<td>A request from the SAS Visual Analytics web application to a CAS server on Windows.</td>
<td>The requesting user’s individual host account.</td>
</tr>
<tr>
<td>A request in a programming-only deployment.</td>
<td>The requesting user’s individual host account.</td>
</tr>
</tbody>
</table>

* Unless the requesting user is a member of the custom group CASHostAccountRequired.

Host Access in a Programming-Only Deployment

In a programming-only deployment, every user accesses a CAS server’s host files and directories using their individual host account. Users must have host access, so it is possible for them to access the back-end machine directly, bypassing the CAS authorization layer.

If you have sensitive data, ensure that all CAS access distinctions are mirrored in the host authorization layer. For example, if you use the CAS authorization system to deny userA Read access to a path-based caslib called caslibA, you must also set up host access controls that prevent userA from accessing that caslib (directory). Without such protection, userA could use a host command to copy files from the caslibA directory to the directory for a caslib that userA can access from CAS.

Host Access in a Full Deployment

Note: This section applies to a CAS server on Linux. Host access from a CAS server on Windows is always under each user’s individual identity.

In a full deployment, host access from CAS is sometimes under individual identity and sometimes under a shared identity. Here are details:

- For users who access CAS only from a programming interface such as SAS Studio, all host access from CAS is under each user’s individual identity. For such users, you must mirror CAS layer access distinctions in the host layer.

- For users who access CAS only from a visual interface such as SAS Visual Analytics or SAS Environment Manager, all host access from CAS is under a shared identity. Such users need CAS layer access to data, but they do not need host access to data. Only the shared identity needs host access to data.

  For such users, there is no reason to create host access controls that mirror your CAS access controls. Of course, you should always host protect your resources in accordance with your security requirements.

- For users who access CAS from both types of interface, host access and experience vary depending on the type of interface that is used. For example, the personal caslib that they use from programming interfaces is not automatically accessible from the visual interfaces.

  You can align access and experience for such users by assigning them to the CASHostAccountRequired group. For members of that group, host access from CAS is always under individual identity. Before you use
this approach, review the associated limitations. See The CASHostAccountRequired Custom Group in SAS Viya Administration: Identity Management.

Using CAS to Modify Host Access

You can use CAS to add host access controls to a new directory or file in the following circumstances:
- You add a caslib of the type PATH or DNFS and specify to create a directory (on Linux).
- You save a table to a file (on Linux).

This functionality is provided by the permission parameter in the CAS actions tables.addCaslib and tables.save. Here are the available fixed values:

<table>
<thead>
<tr>
<th>Value</th>
<th>Octal</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Private</td>
<td>700</td>
<td>Grants Read and Write access to only the owner.</td>
</tr>
<tr>
<td>GroupRead</td>
<td>750</td>
<td>Grants Read and Write access to the owner.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Grants Read access to the owning group.</td>
</tr>
<tr>
<td>GroupWrite</td>
<td>770</td>
<td>Grants Read and Write access to the owner and the owning group.</td>
</tr>
<tr>
<td>GroupWritePublicRead</td>
<td>775</td>
<td>Grants Read and Write access to the owner and the owning group.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Grants Read access to everyone.</td>
</tr>
<tr>
<td>PublicRead</td>
<td>755</td>
<td>Grants Read and Write access to the owner.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Grants Read access to everyone.</td>
</tr>
<tr>
<td>PublicWrite</td>
<td>777</td>
<td>Grants Read and Write access to everyone.</td>
</tr>
</tbody>
</table>

* These octal values are for directories. For saved files (SASHDAT and CSV), the executable bit is not set.

Here are additional details:
- The owner is the host account that creates the directory or file. the owner always gets full access, regardless of whether you use the permission parameter. Use the permission parameter to further refine access.
- The owning group is the host group that is the primary group for the owner.
- You can specify an octal. You are not limited to the fixed values that are listed in the preceding table.

Access to Files in the Public Caslib

Initially, all users have host-layer Write access to the directory for the Public caslib. To limit host-layer Write access to that directory, adjust host-layer access controls.

For example, on a Linux directory you can set a user ownership access flag that is called the sticky bit. If the sticky bit is set for the Public caslib’s directory, only the host account that creates a file in that directory can remove that file. If the sticky bit is not set for the Public caslib’s directory, any user with Write access to the directory can remove files from that directory.

Note: For information about the Public caslib, see Predefined Caslibs in SAS Viya Administration: Data.