

## Understanding Security for SAS® Visual Analytics 8.2 on SAS® Viya®

Antonio Gianni, Faisal Qamar, SAS Institute Inc.

### ABSTRACT

Have you been using SAS® for more than a decade? Did you start using Base SAS®, then progress to more advanced tools like SAS® Enterprise Guide® and SAS® Data Integration Studio? Well, get ready for SAS® Viya®—the new cloud-enabled, in-memory analytics engine developed by SAS. SAS Viya is the new engine with which the next generation of SAS products are being delivered, with SAS® Visual Analytics being one of many exciting new offerings. This paper broadly discusses several security topics of SAS Visual Analytics and SAS Viya with emphasis on application, data, and content authorization. The target audience for this paper are SAS Administrators implementing SAS Viya security, but anyone looking to understand these concepts can benefit.

### INTRODUCTION

Working with a new security framework can be challenging at first because of the multi-faceted and multi-layered nature of implementing an integrated security model. You will be introduced to four aspects of SAS Viya security including Identity Management, Authentication, Encryption, and Authorization. You then take a deep dive into the new two-tier authorization model introduced with SAS Viya that consists of the SAS® Cloud Analytic Services (CAS) Authorization System and the General Authorization System (GA). The goal is for you to gain the knowledge and confidence to begin your journey into designing and implementing a comprehensive security model for your existing or future SAS Viya projects. This paper is a supplement to the official online [SAS® Help Center](#). Many of the examples and definitions are taken directly from the [SAS Viya 3.3 Administration](#) pages.

### IDENTITY MANAGEMENT

When a user or process initiates a request for resources in SAS Visual Analytics, the system must determine its identity before it can allow or deny the request. The request for resources can take on three main forms:

- Access to a SAS product or specific functionality within an application
- Permission to work with SAS Viya content, such as reports and data plans
- Permission to access and analyze data stored in SAS Cloud Analytic Services (CAS)

At the heart of identity management are users and groups and their associated properties. For example, user identities include properties like Name, ID, and associated (Member Of) groups while group identities also include Members belonging to the group. Please be aware that user and group identities are no longer stored internally to SAS (metadata). All users and standard group identities are stored and managed by your organization's LDAP-based identity providers. Some of the more popular identity providers are Microsoft® Active Directory™ and OpenLDAP™. Read-Only access to the provider is required so that SAS can obtain identity information after a user has been authenticated. Authentication is covered in detail later in the paper.

There are two identity-related tasks that continue to be managed within SAS Viya:

- Managing the membership of custom groups and CAS roles
- Giving users, groups, and custom groups access to SAS functionality

SAS® Environment Manager is the new graphical web application that replaces the SAS® 9.4 SAS® Management Console and is the primary interface for user-management functionality in SAS Viya. The terms custom groups and CAS roles are defined and explained in the next section.

## CUSTOM GROUPS AND CAS ROLES

### What are custom groups and how are they useful?

A custom group is a group that exists in SAS Viya but not in your identity provider. Your deployment includes a set of predefined custom groups, which provide an easy way to give users access to specialized functionality out-of-the-box (OOTB). When adding a new group to your identity provider is not convenient, you can create your own custom group to give its members similar permissions. SAS Viya authorization controls do not differentiate between standard and custom groups, so you are free to use them for added flexibility. In larger deployments identities are primarily managed centrally by IT using standard provider tools.

SAS Viya does not support internal user accounts that you might have been familiar with in SAS 9.4. The exception is a singular administrative account called *sasboot* used to initially configure the connection to your identity provider and set up the administrative users. After setting up the identity provider connection and the first administrative users, the *sasboot* account is generally used only if the connection to the identity provider fails.

### SAS Visual Analytics Predefined Custom Groups

The custom groups in **Table 1** are provided OOTB with your deployment. These groups provide an easy way to give users and groups access to the appropriate data, content, or functionality. Later in this presentation you learn how to set up your own custom groups to control access to specific application functions, or entire web applications for some of your users.

Custom Group	Permission Scope
SAS Administrators (Assumable)	All tasks in SAS Environment Manager
	All content including Folders, Reports, and Data Plans
	Full access to CAS Server actions via CAS Superuser role <b>Note:</b> Access to data (CAS libraries) is not included
Application Administrators	Can access <u>Publish Tile</u> and <u>Manage Published</u> from SAS Home
	Can access <u>SAS Theme Designer</u> from SAS Home
Data Builders	Provides access to <u>SAS Data Studio</u> features
Esri Users	Can access <u>Esri</u> systems for geo map access

**Table 1. Description of Predefined Custom Groups**

The SAS Administrators group is a predefined assumable custom group. This means that when a user who is a member of an assumable group logs on, they have the option to assume the elevated privileges, or to simply log on as a standard user. This feature enables the same credential to be used for SAS users who perform the administrator role in addition to the developer or analyst role at their organization.

The highly privileged assumed memberships remain in effect until the user signs out, but as a best practice should be used only to perform specific administrative tasks.

### Assumable Groups

Do you want to opt in to all of your assumable groups?

SASAdministrators

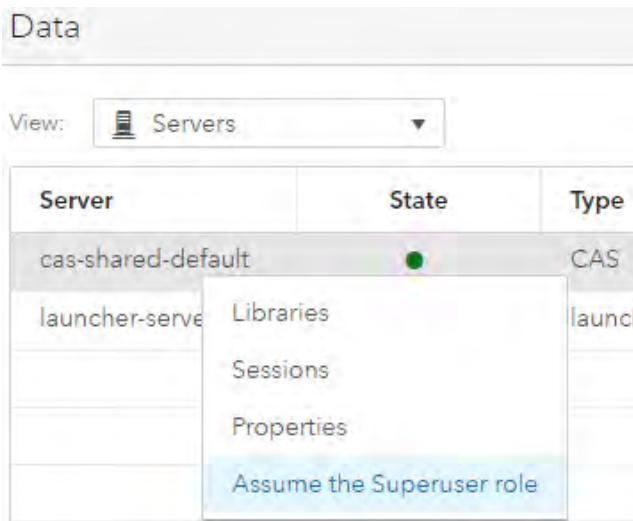
**Display 1. Assumable Groups Opt in Selection**

## Introduction to SAS® Cloud Analytic Services Roles

In addition to standard and custom groups described in the previous section, the SAS Cloud Analytic Services (CAS) Server implements the concept of Roles. There are three different roles in CAS: Superuser, Data, and Action. SAS Visual Analytics currently implements only the Superuser role described in **Table 2**. Note that OOTB SAS Administrators have been assigned the Superuser role and the role is active only when explicitly assumed in the SAS Environment Manager.

Role	Description	Is the Role Assumable?	Initial Members
Superuser	<p>Provides unrestricted access to a CAS server. Only a Superuser can perform the following tasks:</p> <ul style="list-style-type: none"> <li>■ Stop the server.</li> <li>■ Add and remove nodes.</li> <li>■ Manage role membership.</li> <li>■ See and manage the paths list.</li> </ul> <p>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.</p> <p><b>Note:</b></p> <p>By default, the users that are assigned this role have unrestricted access to metadata. However, they do not have unrestricted access to data (CAS libraries). To give users with this role unrestricted access to data, you must modify access controls to explicitly grant them access.</p>	Yes	<p>SAS Administrators (in a full deployment)</p> <p>Process owner for the server</p> <p>Analytics gateway account ( sas.analyticsGateway)</p>

**Table 2. SAS Cloud Analytic Services Superuser Role**



### Display 2. Assuming the Superuser Role

For each CAS server designate at least one user (other than the server's process owner) to the Superuser role.

**TIP:** When managing identities:

- Limit membership in administrative roles and groups.

- Assume the SAS Administrators group membership 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.

## AUTHENTICATION

Authentication is the process of verifying the identity of a user that is attempting to log on to a web application or trying to access other system resources. Authentication determines whether a user (or another identity) is who they claim to be. As previously discussed, a user's identity is the basis for all authorization decisions made by SAS Viya. This includes which features a user has access to and the actions that can be performed by the user against the available resources in the system. A user's credentials (username/password) are verified during initial log on. A successful verification results in the user's identity being established such that access requests can now be evaluated.

SAS® Logon Manager is a web application that handles all authentication requests for SAS Visual Analytics and is accessed via the Apache HTTP Server. SAS Logon Manager supports the following protocols:

- Direct LDAP authentication (LDAP)<sup>1</sup>
- Host authentication
- Kerberos
- Security Assertion Markup Language (SAML)
- OAuth and OpenID Connect
- Pluggable authentication modules (PAM) extending UNIX host authentication

The [How To](#) section of the [Authentication](#) chapter in [SAS Viya 3.3 Administration](#) contains extensive details into the configuration steps required for each protocol.

## SINGLE SIGN-ON

Single sign-on (SSO) is an authentication model that enables users to access a variety of computing resources without being repeatedly prompted for their user IDs and passwords.

For example, SSO can enable a user to access SAS web applications running on a Linux server with the credentials that are already established during logon to the Windows workstation.

The SAS Logon Manager is used to implement third-party SSO products. SAS Viya supports the following SSO products:

- Kerberos
- SAML
- OAuth

## EXTERNAL CREDENTIALS

In addition to log on credentials, users of SAS Viya might need external credentials for accessing databases and other third-party products. This functionality is supported using the [Domains](#) page in SAS Environment Manager where you can manage credentials used to establish connections from SAS Viya to a variety of external data sources.

---

<sup>1</sup> The same LDAP provider (for example, Microsoft Active Directory) can be used for both authentication and identity management discussed in the previous section.

## ENCRYPTION

Encryption is the process that protects data by encoding it using complex algorithms. These algorithms are called ciphers and can be used to encrypt and decrypt the data in your SAS Viya deployment. Encrypted data remains unintelligible during transmission (data in motion) and in storage (data at rest). Identities need access to a secret key to render the data useful.

The SAS Viya deployment process provides a default level of encryption for data in motion. SAS Viya is deployed with Transport Layer Security (TLS) to secure network connections and is fully compliant with SAS security standards. SAS Viya provides self-signed certificates to provide HTTP and HTTPS access to SAS Web Applications out-of-the-box. You can increase the encryption strength and coverage by completing additional configuration.

Encryption is also supported for data at rest, but is not automatically enabled. You can configure encryption for your CAS source data.

The How To sections of the Encryption chapter in [SAS Viya 3.3 Administration](#) contains extensive configuration details for both types of Encryption.

## AUTHORIZATION

Authorization determines which resources are available to which users. When an access request is made, the authorization system will determine if the request is Authorized or Not Authorized. The authorization outcome is determined based on the access controls and rules that are defined in the system. The SAS Viya authorization layer uses two authorization systems:

- Cloud Analytic Services (CAS) authorization system
- General authorization system (GA)

The systems are independent but work in harmony to achieve a robust, integrated security model for your data and content. **Table 3** highlights some key similarities and difference:

### Similarities

- Both systems can share the same identity provider.
- Both systems implicitly disallow any access that is not granted.
- Both systems can be administered using SAS Environment Manager or a command-line interface.

### Differences

	CAS Authorization System	General Authorization System
Basis:	DBMS-style access control.	Attribute-based access control.
Targets:	CAS objects, such as caslibs and tables.	Most other objects, such as folders and reports.
Inheritance:	Through a hierarchy of objects (for example, from a caslib to its tables).	Through a hierarchy of containers (for example, from a folder to its members).
Precedence:	By object hierarchy (closest wins), then by identity type (user wins), and then by type of setting (denial wins).	By type of setting (Prohibit always wins).
Row-level access:	You can attach a filter to a grant of the Select permission on a table.	(Not applicable).
Conditional access:	(Not applicable).	You can attach a Boolean expression to any rule.
Highest privileges:	An assumable role (Superuser) is exempt from authorization requirements throughout a CAS server, except for data access requests.	An assumable group (SAS Administrators) is granted broad access throughout the general authorization system.*

\* The SAS Administrators group is not unrestricted (exempt from authorization requirements). Access is provided by a predefined rule.

**Table 3. Characteristics of SAS Viya Authorization**

You must have a solid understanding of the **Table 4** terms to gain a working knowledge of the security models. These elements are the building blocks for how access controls are implemented in both authorization systems. In the following sections, you learn about the features and scope of each system using concrete examples. In the remaining sections of this paper key terms are formatted with an underline to help refer-back to these definitions.

## Key Terms

Access control or rule	<p>A composite of authorization elements.</p> <p>CAS example: An access control grants the ReadInfo permission to groupA on caslibA.</p> <p>General example: A rule grants the Add permission to groupA on folderA.</p>
Setting	<p>An indication of whether (and to what extent) access is provided.</p> <p>CAS values: Grant, Row-Level Grant, Deny</p> <p>General values: Grant, Conditional Grant, Prohibit, Conditional Prohibit</p>
Permission	<p>A type of access.</p> <p>CAS values: ReadInfo, Select, LimitedPromote, Promote, CreateTable, DropTable, DeleteSource, Insert, Update, Delete, AlterTable, AlterCaslib, ManageAccess</p> <p>General values: Create, Read, Update, Delete, Secure, Add, Remove</p>
Principal	<p>The user, group, or construct to which an access control or rule is assigned.</p> <p>Examples: UserA, GroupA, Authenticated Users</p>
Target	<p>A resource or set of resources.</p> <p>CAS examples: tableA, caslibA</p> <p>General examples: folderA, reportA</p>
Condition	<p>In a conditional rule, the constraint expression.</p> <p>General example: <code>currentUser() == #preferenceOwner</code></p>
Filter	<p>In a row-level grant, the constraint expression.</p> <p>CAS examples: <code>User='SUB::SAS.Userid', sales&gt;1000</code></p>
Effective access	<p>A context-neutral description of the net result of all relevant access controls or rules. Effective access does not incorporate evaluation of conditions.</p> <p>CAS values: Authorized, Not Authorized, Row-Level</p> <p>General values: Authorized, Not Authorized, Conditional</p>
Access outcome	<p>The authorization decision for a specific access request.</p> <p>CAS values: Authorized, Not Authorized, Row-Level Authorization</p> <p>General values: Authorized, Not Authorized</p>

**Table 4. SAS Viya Authorization Key Terms**

### PRINCIPALS AND AUTHENTICATED USERS

Access controls and rules can be assigned to the following Principals:

- Individual users or service accounts
- Custom groups or LDAP groups
- Authenticated Users (AU) - principal type that represents all authenticated users
- Guest - supports guest access
- Everyone - principal type that represents all principals (GA only)

## CLOUD ANALYTIC SERVICES (CAS) AUTHORIZATION SYSTEM

### CAS SERVER CASLIBS, FILES, AND TABLES

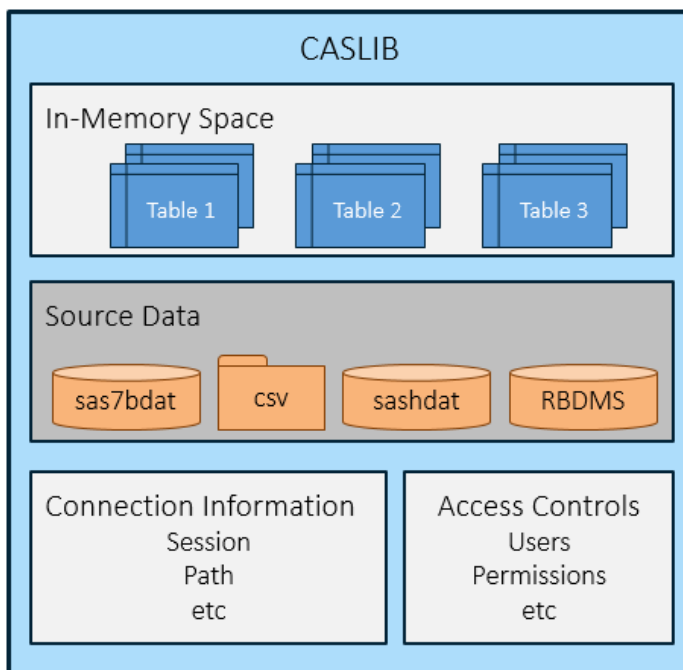
SAS Cloud Analytic Services (CAS) is the server that provides the run-time environment for data management and analytics with SAS Viya. CAS uses a distributed cluster of hardware and software referred to as CAS workers to provide the computing power for analytical processing.

CAS Authorization manages access to the following items:

- Caslibs
- CAS tables and the rows within the tables
- CAS actions – discrete functions that are performed in CAS

A caslib is used to access all data in the CAS server. A caslib in concept is like a traditional SAS library representing a collection of files, but has some unique "super container" properties to support the modern data analytics lifecycle in SAS:

- A caslib is associated with a data source and includes the connection information for the data source. For example, the data source can be a directory (PATH) or the host, port, and other connection information for a database.
- The data in the associated data source is referred to as a file. For path-based caslibs, these files are SASHDAT files, CSV files, SAS data sets, and so on.
- For server-based caslibs, such as an Oracle® database, the term file is still used to create a distinction between data from the caslib's data source and an in-memory copy of the data.
- A caslib provides access to in-memory tables that have been loaded into memory.<sup>2</sup>
- A caslib also provides access controls that define what groups and users are authorized to do with the contents of the caslib.



**Figure 1. Logical Caslib Representation**

<sup>2</sup> CAS performs analysis only on in-memory tables.



## CAS AUTHORIZATION, INHERITANCE, PERMISSIONS, AND PRECEDENCE

This section covers the mapping between CAS permissions and the functionality they control in the SAS Visual Analytics (that is, SAS Environment Manager). You also learn about inheritance behavior and precedence rules that play a key role in the overall CAS authorization evaluation process.


### CAS Inheritance







Access control permissions flow through a hierarchy of objects. Each parent object conveys settings to its child objects. Each child object inherits settings from its parent object. There are three different hierarchy relationships in CAS but the most relevant is the first:







1. Permissions flow from a caslib to its tables.
2. Permissions flow from a table to its columns (not supported by SAS Visual Analytics 8.2).
3. Permissions flow from an action set to its actions (abstracted in visual interfaces, but note that almost all action sets and actions are available to all users).

Note: Each caslib always inherits denials of all permissions for Authenticated Users. Those inherited denials prevent access unless there are grants of higher precedence.

### Mapping between CAS Permissions and SAS Environment Manager Activities








**Table 5** summarizes common activities in SAS Environment Manager  but the same rules apply to similar tasks found in other SAS Viya products. Note that a permission enforced on a table can be conveyed from its parent caslib via inheritance.




Permission	Enforcement		Associated Activities
	Caslib	Table	
ReadInfo	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	View Caslibs and Tables, View Columns, View Authorization View Properties 
Select		<input checked="" type="checkbox"/>	Read data values in a Table 
LimitedPromote		<input checked="" type="checkbox"/>	Load existing Table into memory Required for Just-in-time load of Table into memory 
Promote	<input checked="" type="checkbox"/>		Import and Load Data Table from any source Caslib 
CreateTable	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Save a Table 
DropTable		<input checked="" type="checkbox"/>	Unload Table from memory 







































































Permission	Enforcement		Associated Activities
	Caslib	Table	
DeleteSource		<input checked="" type="checkbox"/>	Delete a physical source Table 
Insert		<input checked="" type="checkbox"/>	Add rows to a Table 
Update		<input checked="" type="checkbox"/>	Change rows in a Table 
Delete		<input checked="" type="checkbox"/>	Delete rows from a Table 
AlterTable		<input checked="" type="checkbox"/>	Change structure of Table 
AlterCaslib	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Change the properties of a caslib
ManageAccess	<input checked="" type="checkbox"/>		Edit Authorization 

**Table 5. Permission and Associated Activities**

Multiple permissions are sometimes required to perform an activity with CAS resources. **Table 6** summarizes the required permissions per activity.

Activities	Required Permissions for Activities	
	Caslib	Table
View Caslibs and Tables  	ReadInfo	ReadInfo
View Authorization 	ReadInfo	ReadInfo
Edit Authorization on Caslib 	ReadInfo ManageAccess	NA
Import Table 	ReadInfo, Select CreateTable, Promote (or LimitedPromote)	NA
Import Table Replace 	ReadInfo	ReadInfo, Select CreateTable LimitedPromote
Create New Caslib <sup>3</sup> 	Global Caslib Management Privileges	NA

<sup>3</sup> You set Caslib Management Privileges in the properties of a CAS Server found in  **Data**  
View:  **Servers** and selecting the CAS server (for example, cas-shared-default) properties .

Activities	Required Permissions for Activities	
	Caslib	Table
Edit Caslib properties        	ReadInfo AlterCaslib	NA
Delete Caslib <sup>4 5</sup>        	ReadInfo, ManageAccess Global Caslib Management Privileges	NA
View Caslib and Table properties        	ReadInfo	ReadInfo
View Table Column        	ReadInfo	ReadInfo
Edit Authorization on Table        	ReadInfo	ReadInfo ManageAccess
Load Table        	ReadInfo	ReadInfo, Select LimitedPromote, or Promote(caslib)
Unload Table        	ReadInfo	ReadInfo DropTable
Delete a physical source Table        	ReadInfo	ReadInfo DeleteSource (DropTable)
Just-in-time load <sup>6</sup>  SAS Report	ReadInfo	ReadInfo, Select LimitedPromote, or Promote(caslib)
Query Data Table 	ReadInfo	ReadInfo, Select
Add rows to a Table 	ReadInfo	ReadInfo, Insert
Change rows in a Table 	ReadInfo	ReadInfo, Select Update
Delete rows from a Table 	ReadInfo	ReadInfo, Select Delete
Change structure of Table 	ReadInfo	ReadInfo, Select AlterTable

**Table 6. Activities and Required Permissions**

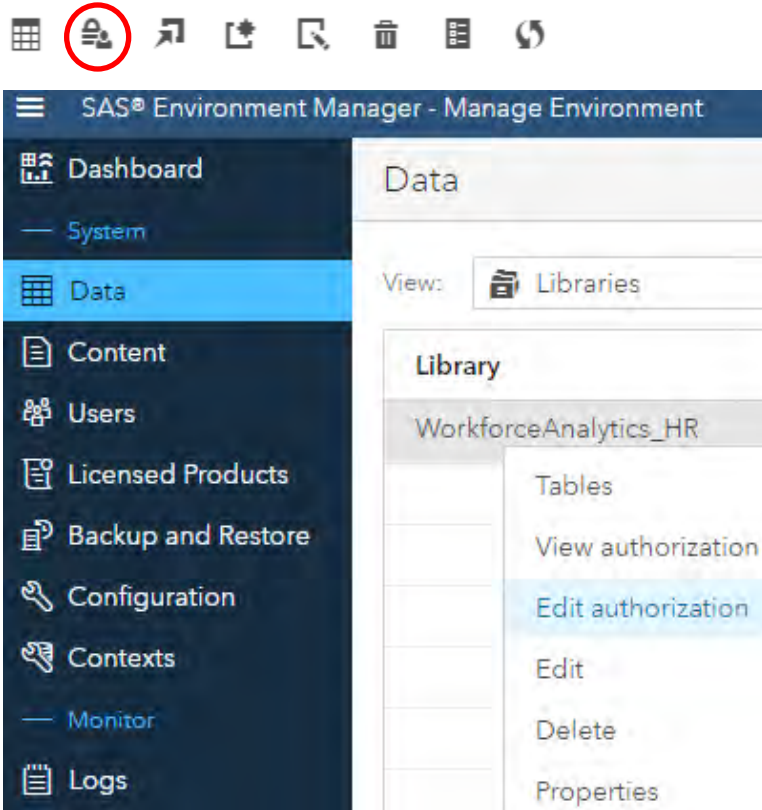
<sup>4</sup> When you delete a caslib all associated in-memory tables are immediately unloaded.

<sup>5</sup> Deleting a caslib does not affect persisted files in the corresponding data source.

<sup>6</sup> If necessary, opening a SAS Report will automatically load dependent CAS tables into memory.

## Securing CAS Resources

SAS Environment Manager is the interface used to interactively manage access to caslibs, tables, and row-level permissions. The Authorization window is accessed from the contextual menu or taskbar icon when you select a caslib or data table.



**Display 3. SAS Environment Manager Authorization Menu**

The View/Edit Authorization window in **Display 4** describes the full set of Access Control Entries (ACEs) applied to the selected caslib or data table.

WorkforceAnalytics\_HR

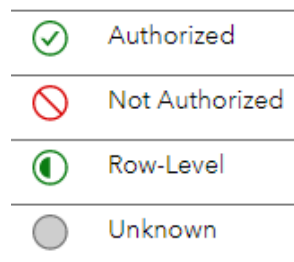
Show individual permissions + ✕ ↺ ?

Principal	Access Level	ReadInfo	Select	LimitedPromote	Promote	CreateTable	DropTable	DeleteSource	Insert	Update	Delete	AlterTable	AlterCaslib	ManageAccess
*HR Data Builders	Custom	✓ +	✓ +	✓ +	✓ +	✓ +	✓ +	✓ +	✓ +	✓ +	✓ +	✓ +	✓ +	✗
Authenticated Users	No Access	✗ +	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗
Human Resources	Custom	✓ +	✓ +	✓ +	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗
SAS Administrators	Full Control	✓ +	✓ +	✓ +	✓ +	✓ +	✓ +	✓ +	✓ +	✓ +	✓ +	✓ +	✓ +	✓ +
Antonio Gianni	Full Control	✓ +	✓ +	✓ +	✓ +	✓ +	✓ +	✓ +	✓ +	✓ +	✓ +	✓ +	✓ +	✓ +

**Display 4. Example Authorization Window for WorkforceAnalytics\_HR**

Rows identify the Principals and columns identify the Permissions that are relevant for the selected Target.

The Access Level slider enables you to quickly set individual permissions and Effective Access is depicted by a colored icon. A diamond indicates that a direct setting (Grant, Row-Level Grant, Deny) is assigned to the specified principal on the current object otherwise it is an inherited permission.



The Authorization window contains a great deal of information about the concepts you learned about from **Table 4. SAS Viya Authorization Key Terms**. The next section illustrates these concepts by expanding on the WorkforceAnalytics\_HR caslib example from **Display 4**.

### CASE STUDY: WORKFORCE ANALYTICS EXAMPLE

Roll up your sleeves; it's time to put the SAS Viya security concepts into practice.

You are the current SAS 9.4 System Administrator and your IT department recently deployed SAS Visual Analytics. You are given the title of "SAS Viya Tsar" and you are just getting up to speed on the new platform. As luck would have it, the Chief People Officer found out about the new killer app and is ready to get started on some workforce analytics. To support the initiative you must implement the security controls by completing these tasks.

#### Create Groups and Assign Members





1. Log on to SAS Environment Manager as a member of the predefined SAS Administrators custom group. <https://yourviyaserver/SASEnvironmentManager/>
2. At the prompt, Select Yes to opt in to all assumable groups. If you are not presented with this option, then you must get an existing member of SAS Administrators to add you to the group. If this is the initial setup and there are no existing SAS Administrators, then you must use the sasboot account to configure the LDAP connection before you can add your personal identity to the SAS Administrators group.



#### Assumable Groups

Do you want to opt in to all of your assumable groups?

SASAdministrators



Yes	No
-----	----

3. Expand the Navigation bar by selecting  from the bottom left part of the window.
4. Select  Users and  Custom Groups .

- The workforce analytics project requires two security groups to hold its members. For this example you are using custom security groups but you can also create the groups in your identity provider (for example, Active Directory) and they will be available in SAS Viya. Create the following :
  - \*HR Data Builders (HR developers responsible for the HR data-Full Access)<sup>7</sup>
  - Human Resources (HR Analyst and Report Consumers-Read Access)
- Add individual members to these groups using  (edit). For the example add yourself to both groups.

## Create New Caslib for Workforce Analytics

The project requires a single caslib to hold the HR Data Tables used in workforce analytics.

- Select  **Data** and View:  Libraries .
- Create a new caslib named WorkforceAnalytics\_HR of type PATH and Save. You will not be enabling encryption for this example.

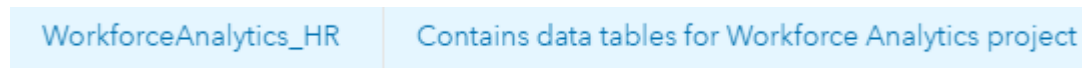


### New Caslib

Server: *	cas-shared-default
Data source type: *	PATH
Path: *	/nfs/IT_analytics_data/viya/hr/WorkforceAnalytics
Name: *	WorkforceAnalytics_HR
Description:	Contains data tables for Workforce Analytics project

## Examining Initial Access

- Select the new caslib and Edit Authorization.



A new caslib will have the following default permissions:


- Inherited denials of all permissions for Authenticated Users (AU)<sup>8</sup>
- Automatic direct grant setting for all permissions for the identity that creates the new caslib

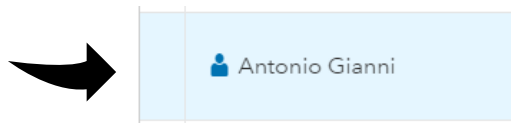
<sup>7</sup> The asterisk is just an example of a naming convention to quickly filter on a class of custom groups.


<sup>8</sup> You may notice for AU that there is a direct deny ReadInfo on all new caslibs. In CAS authorization this setting is not required and has the same effect as an inherited deny setting because of precedence rules. The same is not true in for General Authorization as you will learn in the **Precedence** section.

## Authorization Window Basics

The CAS Authorization Window has the following properties:

- There is always a row for Authenticated Users.
- There is always a row for the currently connected user.
- There is a row for each principal that has a direct Grant (Row-Level Grant) or Deny setting.
- There is a row for each principal that has any relevant inherited settings.
- 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. The identity is automatically cleared when all relevant direct and inherited settings for an identity are removed.
- You can quickly clear all the direct settings for an identity using "Delete all direct settings". Click on the area to the left of the principal to highlight the row, then .





- When you examine your own effective access information, the returned information does not reflect your Superuser status if you have assumed that role.
- Only the permissions that are relevant for an identity (direct or inherited) are displayed for that object.
- Origins information identifies the highest precedence access control (or access controls) that cause a specific effective access result. Click on the permission colored icon to view this information. *Effective access: Authorized* 

## CASE STUDY CONTINUED

You are ready to secure the new WorkforceAnalytics\_HR Caslib for the project. Per the security requirements you are going to grant the following permissions.

- All permissions minus Manage Access to \*HR Data Builders
- Read Access plus Limited Promote to Human Resources
- Full Control to SAS Administrators

## Secure WorkforceAnalytics\_HR Caslib

1. From the Edit Authorization window select Add identities .
2. Filter on Custom Groups and using the right arrow  move \*HR Data Builders, Human Resources and SAS Administrators to the Selected Identities list and then OK to confirm.
3. Verify that there is a new row for each group displaying Not Authorized for all permissions.
4. Grant all permissions (-Manage Access) to \*HR Data Builders.

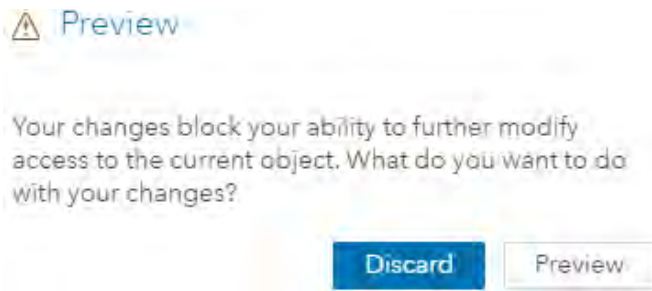
**TIP:** Move the slider to Full control to quickly set direct grants to all individual permissions, then change the direct grant setting for Manage Access to **none** (click on colored icon to bring up direct setting options).

5. Grant ReadInfo, Select, and LimitedPromote to \*HR Data Builders.

**TIP:** Move the slider to Read to quickly set direct grants on ReadInfo, Select individual permissions, then change the direct setting for LimitedPromote to **Grant**.

6. Grant Full Control to SAS Administrators using the Access level Slider.
  7. Select Preview to see the effect of the changes, then Save to commit.
  8. Open the Edit Authorizations Window again and verify the settings. They should match **Display**
- #### 4. Example Authorization Window for WorkforceAnalytics\_HR.
9. Go back in Edit Authorization window and change the ManageAccess from none to Direct deny for \*HR Data Builders.
  10. Next, clear the Direct settings for yourself (confirm Remove warning with yes). Select Preview.

What happened?



This example illustrates how a user can inadvertently block her or his own access. Since you belong to the SAS Administrators group you can always assume the Superuser role and Edit Authorization on any caslib or table but a standard user would need a Superuser to grant them back access.

11. Select **Discard** and change ManageAccess back to none for \*HR Data Builders.
12. Clear the Direct settings for yourself (confirm Remove warning with yes). Select Preview and Save.

What happened?

You don't get a warning this time because you have an inherited grant on ManageAccess from belonging to the SAS Administrators group that is no longer blocked by the direct deny you were previously inheriting from \*HR Data Builders.

This illustrates the concept of Precedence which is covered in the next section. The important takeaway here is, before you add a direct denial for a group that you belong to, make sure you have a higher precedence (offsetting) direct grant.

### Loading Salary Data Table for Workforce Analytics

For this example you can use a sample salary data set (CSV format) from the web or create your own.

1. Select **Data** and View: **Libraries**.
2. Select WorkforceAnalytics\_HR caslib and Import a new Table called Salaries.







3. Select **Import** tab and **Local File** to navigate to the salary.csv.
4. Verify the target table name of salary and WorkforceAnalytics\_HR Target destination.
5. Finally, select **Import Item**, you should then see a confirmation.

✔ The table was successfully imported on Feb 25, 2018 01:18 PM and is ready for use.

6. Close the Import window and verify the state of the new salary table.



Table	State	Source Table N...	Row Count
SALARY		SALARY.sashdat	100

7. The import process created a SALARY.sashdat in the destination caslib from the original salary.csv file. The table was also loaded into memory.
8. Examine the authorization of the SALARY table.
9. All permissions inherit from the caslib which is illustrated by the absence of any direct grants on the table. Recall direct grants are marked by a diamond   |  .
10. Close the authorization window and try loading and unloading the SALARY table into memory. Experiment with different permission to see if your results agree with **Table 6. Activities and Required Permissions**.
11. If you accidentally (or intentionally) block your own access, assume the Superuser role to get yourself out of trouble.

## AUTHORIZATION DECISION PRECEDENCE

Precedence in CAS Authorization is straightforward once you get the basics. Recall that objects have an implicit deny with the absence of any inherited or direct grant. An inherited or direct deny has a higher precedence than a grant set at the same level.

There are two basic precedence paradigms to consider for CAS authorization:

- Object: Tables (higher) -> Caslib (lower)
- Principal: Individual Users (highest) -> Groups -> Authenticated Users (lowest)

### Notes:

At a minimum you must be granted ReadInfo on caslib to view a table.

All Group memberships are at the same level of precedence; nested "distance" is not evaluated.

## How Access Is Evaluated

A direct access control on a table wins over inherited settings from a caslib regardless of principal.

Example 1:

- Antonio has a direct grant of ReadInfo on the WorkforceAnalytics\_HR caslib
- Authenticated Users has a direct denial of ReadInfo on the SALARY table
  - Effective access is Not Authorized for Antonio on the SALARY table

Example 2:

- Antonio has a direct grant of ReadInfo on the WorkforceAnalytics\_HR caslib
- Authenticated Users has a direct denial of ReadInfo on the SALARY table
- Antonio has a direct grant of ReadInfo on the SALARY table
  - Effective access is Authorized for Antonio on the SALARY table

## Authorization Decision Process

**1st Scenario:** If a user (principal) has direct access controls on the table, those access controls determine the outcome, period. The following criteria are evaluated until there is a match and outcome can be determined.

1. If there is a setting specifically assigned to the requesting user, that setting wins.
2. If there is a denial from a group, the outcome is Not Authorized.
3. If there is a grant from a group, the outcome is Authorized.
4. If there is exactly one row-level grant from a group, the outcome is Row-Level Authorization (authorized for rows within the applicable filter).
5. 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).
6. If there is a setting for Authenticated Users, that setting wins.

**2nd Scenario:** If there are no relevant direct access controls on the table, direct access controls on the parent caslib determine the outcome in a similar manner.

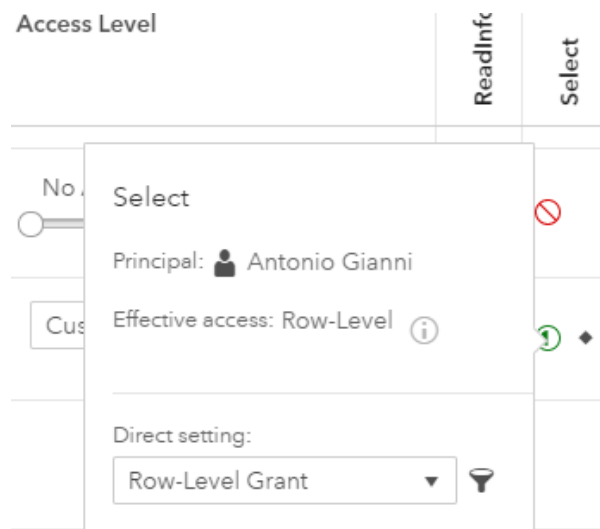
1. If there is a setting specifically assigned to the requesting user, that setting wins.
2. If there is a denial from a group, the outcome is Not Authorized.
3. If there is a grant from a group, the outcome is Authorized.
4. If there is a setting for Authenticated Users, that setting determines the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

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

## 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 match the associated filter.

For example, you can use a row-level grant to enable Antonio to see only those rows in the SALARY table where the value of Region is "West". In this scenario, Antonio (the VP of the West region) could see only his own workers' Salaries and not those of the other regions.



Identify a user or group for the filter  
Set row-level grant on Select for SALARY Table  
Filter Expression Region="West"



The [Concepts](#) section of the CAS Authorization chapter in [SAS Viya 3.3 Administration](#) contains extensive details about filter syntax. The **Identity-Based Substitution** parameters are particularly useful. 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.

Substitution Parameter	
SUB::SAS.Userid	Determines whether a data value is the same as the requesting user's authenticated ID
SUB::SAS.IdentityGroups	Determines whether a data value matches any of the requesting user's group memberships

**Table 7. Row-Level Select Filter Substitution Parameter**

This enables you to define powerful filters like

```
MANAGER_USER_ID='SUB::SAS.Userid' OR 'HR Executives' IN ('SUB::SAS.IdentityGroups')
```

## HOST LEVEL ACCOUNTS AND SECURITY CONSIDERATIONS

There are two important host level accounts:

Host Accounts	Purpose
sas	Installer and service account that enables the SAS Viya software to run
cas	Service account that runs Cloud Analytic Services server (shared identity)

**Table 8. SAS Viya Host Service Accounts**

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 (cas). In this scenario, end-user data access authorization decisions are exclusively enforced by the CAS access controls and not by the security defined on the host layer. Only the shared identity permissions are verified in this scenario, so it is not necessary to mirror CAS layer access permissions on the host, but you should continue to protect files per your IT data security policies.

## CAS TIPS AND GENERAL RECOMMENDATIONS

Best practices for SAS Viya are emerging, and here are some which apply to most SAS Viya implementations:

- Limit membership to SAS Administrators group and Superuser roles.
- Apply security controls to a caslib and leverage inheritance.
- Limit the use of direct permissions on individual tables.
- Apply security to group principals rather than individual users.
- Access that is not granted is implicitly denied, so do not set unnecessary denials.
- Remember, a new table is initially protected only by access controls inherited from its caslib.
- Apply CAS access controls in bulk using the scriptable command-line interface.

For more detail see [SAS Viya Administration: Command-Line Interfaces](#).

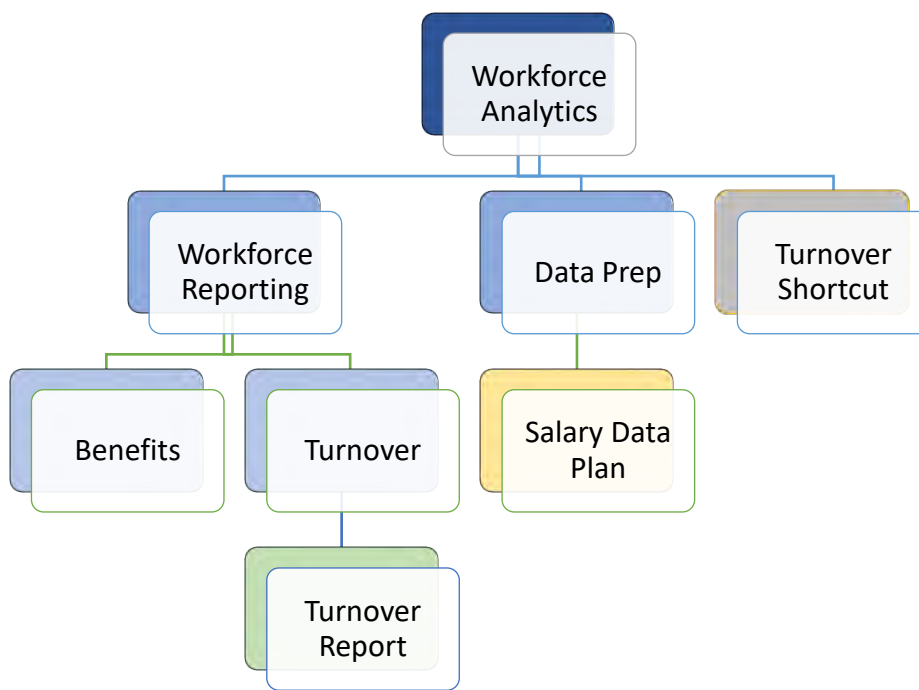
## SAS VIYA GENERAL AUTHORIZATION

### GENERAL AUTHORIZATION CONTENT

General Authorization (GA) manages access to the following SAS Visual Analytics content:


- Folders and SAS VA Reports
- References: Shortcuts to other content
- Data Plans: SAS® Data Studio content type to help you prepare your data for CAS

A folder is a container that holds content. A folder can hold other folders, reports, and references. **Figure 2** shows a typical folder hierarchy for organizing content.



**Figure 2. Example Content Hierarchy in SAS Viya**

### GENERAL AUTHORIZATION, INHERITANCE, PERMISSIONS, AND PRECEDENCE

This section covers the mapping between General Authorization (GA) permissions and the functionality they control in the SAS Visual Analytics and SAS Environment Manager  Content.

You also learn about inheritance behavior and precedence rules that play a key role in the overall GA authorization evaluation process.

#### General Authorization Inheritance


Permissions flow through a hierarchy of folders (containers). Each folder can convey settings to its child members but this is optional. Each child member inherits conveyed settings from its parent folder if they are set using the second set of convey settings in the authorization window.

















































- Permissions flow from folders to reports and plans.
- Permissions **do not** flow from folder to a reference member (such as a shortcut) but anyone with Read access to a folder can see all reference members in that folder and can delete them with Remove access.

Note: Each folder always has implicit prohibits of all permissions for Authenticated Users (AU). Those implicit prohibits prevent access unless there are grants of higher precedence.

**TIP:** The next statement is important and will be repeated. Once you set grant convey permissions broadly (for example, Authenticated Users) on a folder there is no way to "break" inheritance the way you might expect. If you attempt to break the permission flow with a prohibit to AU on any of the object's descendants, that prohibit rule always wins for all users. Prohibit rules have absolute precedence no matter the origin. This is covered again in the [precedence](#) section.













































## Mapping between GA Permissions and SAS Visual Analytics Activities

**Table 9** summarizes common activities in SAS Environment Manager  but the same rules apply to similar tasks in other SAS Viya products. Note that a permission enforced on a report can be conveyed from its parent folder via inheritance.

Permission	Enforcement		Associated Activities
	Folder	Member	
Read	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	View Content, Add as shortcut, View Authorizations Create/Save New Content         
Update	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Edit Content properties, Rename, Move to Folder, Create/Save New Content   
Delete	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Delete Content       
Secure	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Edit Authorizations       
Add	<input checked="" type="checkbox"/>		Create New Folder, Create/Save New Content to Folder, Move to Folder        
Remove	<input checked="" type="checkbox"/>		Move to Folder
Export	<input checked="" type="checkbox"/>		Export Content from Folder       
Requires SAS Administrator privileges			
Import	<input checked="" type="checkbox"/>		Import Content from Folder       
Requires SAS Administrator privileges			

**Table 9. General Authorization Permission and Associated Activities**

Multiple permissions are sometimes required to perform an activity with SAS Viya content. **Table 10** summarizes the required permissions per activity.

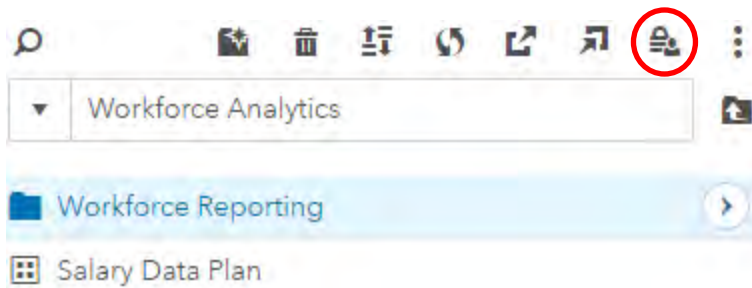
Activities	Required Permissions for Activities		
	Member(Child)	Current Parent Folder	New Parent Folder
Create New Folder      	Read*	Add	
	* Not required but If you don't have Read you won't be able to see it!		
Delete Content      	Delete*	Remove	
	* Also need Delete on member(child) descendants of type container.		
View Authorization      	Read		
Edit Authorization      	Secure		
Move to Folder      	Update	Remove	Add
Rename      	Update		
Add as shortcut      	Read		
Create and Save Report 	Read, Update	Add	
Update Content Properties 	Update		

**Table 10: Activities and Required Permissions**

### Securing Visual Analytics Content

SAS Environment Manager is the interface used to interactively manage access to folders, reports, and data plans (permissions are not set on shortcuts).

The authorization window is accessed from the contextual menu or taskbar icon when you select a content item as shown in **Display 5. SAS Environment Manager Authorization Menu**.



### Display 5. SAS Environment Manager Authorization Menu

The View/Edit Authorization window in **Display 6** describes the full set of access control entries (ACEs) applied to the selected item.

Principal	Read	Update	Delete	Secure	Add	Remove	Read (convey)	Update (convey)	Delete (convey)	Secure (convey)	Add (convey)	Remove (convey)
Workforce Reporting												
Authenticated Users	⊘	⊘	⊘	⊘	⊘	⊘	⊘	⊘	⊘	⊘	⊘	⊘
Human Resources	✓	⊘	⊘	⊘	⊘	⊘	✓	⊘	⊘	⊘	⊘	⊘
SAS Administrators	✓	✓	✓	✓	✓	✓	⊘	⊘	⊘	⊘	⊘	⊘
Workforce Analytics Admins	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Antonio Gianni	✓	✓	✓	✓	✓	✓	⊘	⊘	⊘	⊘	⊘	⊘

### Display 6. Example Authorization Window for Workforce Reporting

This should look familiar; the GA authorization window has the same basic properties as CAS but offers different permission types appropriate for SAS Viya content. Diamonds still mark direct settings (Grant, Conditional Grant, Prohibit, and Conditional Prohibit) assigned to the specified principal. In this example, the absence of diamonds tells you all the permissions are inherited.

Notice there are two sets of permissions. The first set is for the folder itself (stand-alone object) while the second set, marked by (convey), is for the folder acting as a container. The convey permission enables access to flow from parent folders to its descendants including reports, data plans, or other folders.

### GA Authorization Window

The GA authorization window also has some differences when compared to CAS:

- "Delete all direct settings" and the permission slider are currently not implemented.
- When examining your own effective access information, the returned information presumes that all assumable memberships are in effect.
- Origins information identifies the contributing rules that cause a specific Effective Access result. Click on the permission colored icon to view this information ⓘ.

#### Contributing Rules

Principal	Setting	Target Name
Workforce Analytics Admins	Grant	/Workforce Analytics (folder)

Display 7: GA Origins for Read Permission on Workforce Reporting Folder

## General Authorization Precedence

In SAS Viya GA precedence is simple. The only factor that affects precedence is the type of rule (grant or prohibit). Prohibit rules have **absolute** precedence.

### How Access Is Evaluated

- If there is a relevant prohibit rule, no matter the origin the effective access is Not Authorized.
- A direct grant setting assigned to you has less precedence than a prohibit setting that is assigned to Authenticated Users. You are an authenticated user, therefore, prohibit wins.
- A direct grant on a report has less precedence than a prohibit setting that is conveyed from its parent. Prohibit always wins.

These rules are reinforced in the following examples:

Example 1:

- Antonio has a direct grant of Read on the Turnover Report
- Authenticated Users has a prohibit Read on the Turnover Report
  - Effective access Read is Not Authorized for Antonio on the Turnover Report

Example 2:

- Antonio has a direct grant of Delete on the Turnover Report
  - Authenticated User has a prohibit Delete (convey) setting on the Turnover (parent folder)
    - Effective access for Delete is Not Authorized for Antonio on the Turnover Report
- Since Antonio is an Authenticated User the prohibit wins.

**Caution:** Do not set prohibit rules on content for Authenticated Users. As a best practice just let the implicit prohibit settings work for you.





**Administrators and Superusers are also authenticated users!**

## CASE STUDY PART 2: EXPANDING ON THE WORKFORCE ANALYTICS EXAMPLE

Change Request!

The Chief People Officer loves the new self-service analytics SAS Viya provides for her organization and she wants to kick-off a new top-secret initiative "Project Khush" (pKhush) where just a handful of her best analysts are privy. She requests you to set up a restricted content area in SAS Viya for the tiger team known as the "Hotshots". You start working on the task without hesitation.

### Create Groups and Assign Members

1. Log on to SAS Environment Manager assuming the SAS Administrators group (opt in).
2. Select  Users and  Custom Groups .
3. pKhush requires two new security groups to hold its members. Once again, you are creating custom security groups.
  - Hotshots Administrators (full access to data and content for pKhush)
  - Hotshots Analysts (Read-Only access to data and full access to content for pKhush)
4. Add yourself to Hotshots Administrators .
5. Manage individual members of these groups as needed.



## Create New Caslib for Project Khush

1. Select  Data and View:  Libraries .

Data tables for pKhush can be imported to the same caslib that is already defined for workforce analytics, but this would require applying permissions to individual tables. You learned previously that it's best to create a new caslib, keeping security simple by allowing the caslib -> table inheritance work for you. It's tedious and error prone to set permissions at the table level and should be done only in edge cases.

2. Create a new caslib pKhush\_HR of type PATH and Save. In this case you still append \_HR to easily identify/filter on data associated with a specific division within a company.



3. Examine the Initial Access. Is this what you expect? Review CAS authorization section if you need a refresher.

## Secure pKhush\_HR Caslib and Load Data

You need to secure the new pKhush\_HR caslib so just the Hotshots Administrators and Hotshots Analysts have access.

Per the security requirements for pKhush you are going to grant the following permissions:

- Full control to Hotshots Administrators
- Read Access plus Limited Promote to Hotshots Analysts

You are confident, you got this....

4. From the Edit Authorization window select Add identities  and so on.


If you need help, review the section on CAS authorization.

Note: You are not granting any permissions to SAS Administrators (you are really keeping this project discreet), but how could the "SAS Administrators" help if a user or group is accidentally blocked?

You guessed it, by assuming the Superuser role and making the appropriate authorization updates to grant back access.

5. For the case study, load at least one highly confidential "turnover" data file to the pKhush\_HR caslib. Verify that the expected permissions are inherited.

Library: pKhush\_HR Filter by:

Table	State	Source Table Name
TURNOVER_RATES		TURNOVER_RATES.sashdat

Principal	Access Level	ReadInfo	Select	LimitedPromote	CreateTable	DropTable	DeleteSource	Insert	Update	Delete	AlterTable	ManageAccess
Authenticated Users	No Access	⊗	⊗	⊗	⊗	⊗	⊗	⊗	⊗	⊗	⊗	⊗
Hotshots Administrators	Full Control	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙
Hotshots Analysts	Custom	⊙	⊙	⊙	⊗	⊗	⊗	⊗	⊗	⊗	⊗	⊗

**Display 8. Confidential Turnover Rates Data Source**

## Implementing the Content Folder Hierarchy to Support Workforce Analytics and Project Khush

The process of designing a content folder hierarchy appears trivial at first look, but you have some important decisions to make based on how you want to apply permissions. Even though the entire team is working on workforce analytics, the requirements state that you must be more selective in how you grant access to the pKhush content and data. On the CAS data side, you met this requirement with a secured caslib where just the Hotshots have access. You need to do the same for pKhush content related to Turnover analysis. There are two basic approaches:

1. Implement the hierarchy as shown in **Figure 2. Example Content Hierarchy in SAS Viya**, where the Turnover folder is a child of Workforce Reporting. Organizationally this is logical and convenient for general Human Resources analyst that are also members of Hotshots Analysts. The drawback with this option is that you are limited in the use of convey permissions. In short, convey is used effectively only at a level where the remaining children all have the same access. At a minimum you would need to apply direct permissions through the first three levels of the Workforce Reporting branch of the hierarchy:

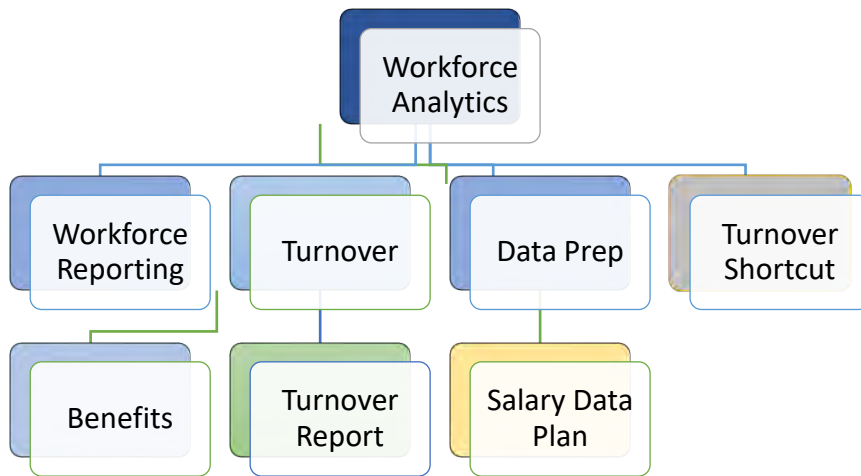
Workforce Analytics (Direct) <-**Top Level Folder**

- Workforce Reporting (Direct)
  - Benefits (Direct + Convey)
  - Turnover (Direct + Convey)
    - Turnover Report (Inherited)
- Data Prep (Direct + Convey)
  - Salary Data Plan (Inherited)

This is reasonable since you have just two folders under Workforce Reporting, but imagine if you had 20 folders at that level that all shared the same permissions with Turnover being unique.

What should you do then? Bingo!

2. You would move Turnover out from Workforce Reporting and make it a second-level folder as seen in **Figure 3**. Here you can apply direct permissions through just the first two levels to meet your requirements. Evaluate and test a folder design pattern that works best for your specific project requirements.



**Figure 3. Flattened Alternate Content Hierarchy**

Workforce Analytics (Direct)

    Workforce Reporting (Direct + Convey)

        Benefits (Inherited)<sup>9</sup>

    Turnover (Direct + Convey)

        Turnover Report (Inherited)


    Data Prep (Direct + Convey)

        Salary Data Plan (Inherited)

Refer to [SAS Viya 3.3 Administration](#) for step-by-step documentation on creating and securing folders.

- Authorization / General Authorization / How to (Authorization Window)
- Content / Content Management: How To

## GENERAL AUTHORIZATION RULES AND ACCESS TO FUNCTIONALITY

SAS Viya provides an initial set of rules to control access to functionality including giving all authenticated users access to baseline functionality for a typical user. These rules impact any user who successfully logs on. Initially, all authenticated users have access to SAS Visual Analytics and the Dashboard, Data, and Content pages in SAS Environment Manager. To meet your specific requirements you can modify the OOTB rules or create new rules to customize the functionality at your site using the General Authorization Rules page  [Rules](#).

The Rules page is an advanced interface available only to SAS Administrators OOTB. You would normally use the simpler authorization window to view and manage permissions in SAS Viya, but behind the scenes, all the GA permissions are implemented as rules. Rules are a powerful tool that enables you to make customizations to your SAS Viya environment.

<sup>9</sup> This is the level where you benefit most by using convey rules.

Here are a few examples of the type of enhancements you can make using custom rules:

- Set permissions conditionally on a folder (e.g. Hotshots Analyst can view a report just on Tuesdays).
- Setup a rule to allow users who are not SAS administrators to create top-level folders.
- Restrict access to functionality in the visual interfaces, like the ability to import data or export from a report.

Refer to [SAS Viya 3.3 Administration](#) for extensive documentation on creating and managing General Authentication Rules.

- Authorization / General Authorization / Concepts
- Authorization / General Authorization / How to (Rules Page)
- Identity Management / Concepts / Supported Adjustments to Existing Rules

## SAS VIYA GA TIPS AND RECOMMENDATIONS

- Limit membership in administrative groups.
- Use groups, not individual users as principals.
- Use folders, not individual content items as targets.
- Flatten the content hierarchy to better leverage (**convey**) permissions.
- Grant selectively and try to avoid the use of prohibit settings.
- Do not set unnecessary prohibits.
- If you are seeing unexpected results, verify you have not set a prohibit on AU.
- Manage permissions in bulk using the scriptable command-line interface.

For more detail see [SAS Viya Administration: Command-Line Interfaces](#)

## CONCLUSION

Building out a well-rounded security model to protect your content and data assets is an essential part of any successful SAS Viya project. The SAS engineers worked diligently on developing a product that would integrate well with the security solutions commonly found in the enterprise today. I think they have succeeded with most protocols working out-of-the-box or with minimal configuration.

You have been introduced to the security landscape for SAS Visual Analytics on SAS Viya. You learned about the four pillars of a comprehensive security model: Identity Management, Authentication, Encryption, and Authorization. I hope the material and case study give you the insight required to be successful on your SAS Viya projects and generate ideas on how you can tackle your security requirements. Don't be afraid to experiment; this is how you learn and find out what is possible. I wish you luck in your implementation efforts.

## REFERENCES

- SAS Institute Inc. 2018. *SAS® Viya® 3.3 Administration*. Available at [SAS® Help Center](#)

## ACKNOWLEDGMENTS

We thank the outstanding folks at SAS Global Enablement & Learning for blazing the trails for the rest of us with your blogs, insights and training events. We also thank the SAS Technical Writers for their awesome work on the SAS Viya documentation. This paper would not have been possible without your efforts.

## RECOMMENDED READING

### [SAS® Help Center](#)

- SAS® Viya® 3.3 Administration
- SAS® Visual Analytics 8.2
- SAS® Viya® 3.3 for Linux: Deployment Guide

## CONTACT INFORMATION

Your comments and questions are valued and encouraged. Contact the authors at:

Antonio Gianni  
100 SAS Campus Drive  
Cary, NC, 27513  
SAS Institute Inc.  
[antonio.gianni@sas.com](mailto:antonio.gianni@sas.com)  
[www.linkedin.com/in/antonio-gianni](http://www.linkedin.com/in/antonio-gianni)  
<http://www.sas.com>

Faisal Qamar  
SAS Institute Inc.  
[faisal.qamar@sas.com](mailto:faisal.qamar@sas.com)

SAS and all other SAS Institute Inc. product or service names are registered trademarks or trademarks of SAS Institute Inc. in the USA and other countries. ® indicates USA registration.

Other brand and product names are trademarks of their respective companies.

SAS Institute Inc., SAS Campus Drive, Cary, NC 27513-2414

December 2017