SAS® Viya® Platform: Access to Functionality

2020.1 - 2024.12

This document might apply to additional versions of the software. Open this document in SAS Help Center and click on the version in the banner to see all available versions.

Access to Functionality: Overview

This document is about access to applications, selected features, and selected components.

Here is a summary of the initial distribution of access to functionality:

SAS Administrators group	Provides access to all applications and features.

Other predefined custom groups	Provide access to certain specialized applications and features. See “Predefined Custom Groups” in *SAS Viya Platform: Identity Management*.
Authenticated Users principal type	Provides access to most applications and features. **Note:** The Authenticated Users principal type is a construct that represents everyone who signs in.

If the initial distribution is appropriate, your only task is to assign users who need specialized or administrative access to the appropriate predefined groups.

If the initial distribution is not appropriate, you must expand or restrict access. Use either of the following approaches:

basic approach
: In the basic approach, you work with only those rules that target a documented URI. Your changes are limited, consisting of adding rules, changing rule principals, and modifying rule descriptions. See “Access to Functionality: How To (Basic Approach)” on page 2.

advanced approach
: In the advanced approach, you make more extensive changes. For example, you might modify additional fields or target undocumented URIs. See “Rules Page” in *SAS Environment Manager: User’s Guide*.

CAUTION
Managing access to functionality can be a complex task. Use the advanced approach only if you have a thorough understanding of target URIs, the functionality that you want to restrict, the effect of each permission, and the interactions with any related rules. Make sure that you have a current backup of your deployment before you begin. Test your changes to make sure that they do not have unintended effects.

Access to Functionality: How To (Basic Approach)

IMPORTANT Modifying access to applications does not affect access to underlying services. For example, a user who cannot access SAS Environment Manager might still be able to access the folders service through another interface.

Tips and Techniques

Planning

1. Identify the access levels that you need.
2. Decide which documented URIs fit each access level.
3. Identify or create a group for each access level.

Key Points

- Avoid use of Prohibit rules. Instead, use selective grants to provide selective access.
- You do not have to add rules that grant access to the SAS Administrators group. That group has a universal grant.
- To grant the same access to two distinct groups, make a copy of the original rule. Specify one group as the principal in the original rule and the other group as the principal in the new rule.

Consider Giving Baseline Access to Authenticated Users

Unless it is unacceptable for all authenticated users to have at least the lowest level of access, leave Authenticated Users as the principal in the rule (or rules) for the lowest level of access. Here are examples:

- All users are implicitly members of Authenticated Users, so they can view reports. If this is acceptable, leave the predefined grant of /SASVisualAnalytics/** assigned to Authenticated Users. If this is not acceptable, change the principal from Authenticated Users to a designated group.
- If you want to hide other applications from Authenticated Users, you must change the principal in each relevant rule, so that access is no longer granted to Authenticated Users.

CAUTION

Never prohibit Authenticated Users. Prohibiting Authenticated Users blocks access for all authenticated users. That block has absolute precedence. It cannot be mitigated by more specific grants. Instead, make sure that Authenticated Users is not granted access. Any access that is not granted is implicitly denied.

Consider Using Nested Groups

You can establish cumulative levels of access by making each higher-privilege group a member of the next-most-privileged group.

For example, if your intent is to make functionality in web applications available as follows:

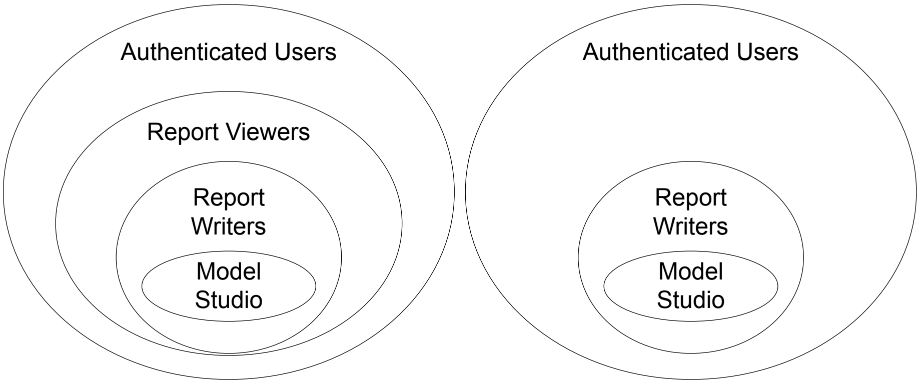
	Availability by Group		
Functionality	**Report Viewers**	**Report Writers**	**Model Studio**
View reports in SAS Visual Analytics.	✓	✓	✓
Write and edit reports in SAS Visual Analytics.		✓	✓
Build models in Model Studio.			✓

Then specify principals in authorization rules as follows:

Rule Principal (Group)	Rule Target (URI)
Report Viewers[1]	/SASVisualAnalytics/**
Report Writers	/SASVisualAnalytics_capabilities/edit
Model Studio	/ModelStudio/**

[1] Or, if it is acceptable for all authenticated users to view reports in SAS Visual Analytics, omit the Report Viewers group and leave Authenticated Users as the principal.

The following figure depicts the nested group memberships that work with the rules that are described in the preceding table:



In both membership structures, the Model Studio group is a member of the Report Writers group. In the first structure, the Report Writers group is a member of the Report Viewers group. In the second structure, there is no Report Viewers group. Instead, all authenticated users have report viewing privileges.

Example Instructions

Initially, all authenticated users can access the Edit mode in SAS Visual Analytics. Here is one way to restrict that access:

1. Find a documented URI that affects the functionality that you want to restrict.

   In this example, the relevant URI is /SASVisualAnalytics_capabilities/edit.

2. Sign in to SAS Environment Manager as an administrator.

3. On the **Users** page, create or identify the group that should be able to edit reports.

   In this example, you create a custom group named `Report Writers`, with a group ID of `ReportWriters`.

4. On the **Rules** page, locate and edit the relevant rule.

   a. Enter `/SASVisualAnalytics_capabilities/edit` in the **Search** field, and click the search icon.

   b. Right-click the rule, and select **Edit**.

   c. In the Edit Rule window:

      1. Change the **Principal Type** to **Group**.

      2. In the **Principal** field, specify the appropriate group ID.

         In this example, specify `ReportWriters`.

   d. Update the **Description** field to reflect your changes.

   e. Click **Save**.

   > **TIP** As a safer alternative to directly editing the rule, you can copy the rule, modify the copy of the rule, and then disable the original rule.

5. Verify that access to the Edit mode in SAS Visual Analytics is available, as expected.

   > **TIP** One way to test access is to sign in without assuming your membership in the SAS Administrator’s group. In this example, you should have different results depending on whether you are a member of the Report Writers group.

   > **TIP** If access is broader than expected, make sure that there are no other rules that grant the same functionality (the same URI) to another principal.

Access to Functionality: Application URIs

IMPORTANT Modifying access to applications does not affect access to underlying services. For example, a user who cannot access SAS Environment Manager might be able to access the folders service through another interface.

The following table provides examples of application URIs that you can use as rule targets in the basic approach to managing access to functionality. Here are key points:

- Not all deployments include all applications.
- Most of the predefined rules for documented URIs grant access to Authenticated Users. In the following table, exceptions are noted.
- In general, access to functionality is controlled by the Read permission. Some predefined rules grant additional permissions.
- For details about a predefined rule, see the rule’s description. On the **Rules** page in SAS Environment Manager, right-click the rule and select **Properties**.
- To manage access to an application that is not listed below, see the documentation for that application.
- To manage access to features within an application, see the documentation for that application.

Table 1 URIs for Applications

Application	URI	Notes
SAS Conversation Designer	/SASConversationDesigner/**	
SAS Data Explorer	/SASDataExplorer/**	Feature-level access is supported.
SAS Data Studio	/SASDataStudio/**	Initially granted to Data Builders.
SAS Drive	/SASDrive/**	Feature-level access is supported. Starting in the 2024.12 release, SAS Drive is disabled by default. To enable SAS Drive see “Enable SAS Drive Application” on page 9. SAS Drive will be formally retired in the 2025.06 (June 2025) release.
SAS Environment Manager	/SASEnvironmentManager/	Page-level access is supported.
SAS Graph Builder	/SASGraphBuilder/**	
SAS Information Catalog	/SASInformationCatalog/	Feature-level access is supported.
SAS Lineage Viewer	/SASLineage/**	
SAS Model Manager	/SASModelManager/	
Model Studio	/ModelStudio/**	
SAS Studio	/SASStudio/**	
SAS Theme Designer	/SASThemeDesigner/**	Initially granted to Application Administrators.
SAS Visual Analytics	/SASVisualAnalytics/**	Feature-level access is supported.

Application	URI	Notes
SAS Visual Analytics App	/SASMobileBI/**	Feature-level access is supported.
SAS Workflow Manager	/SASWorkflowManager/**	
Welcome to SAS Viya	/SASLanding/**	Starting in the 2024.10 release, Welcome to SAS Viya replaces SAS Drive as the default SAS Viya landing page. To change the default SAS Viya landing page, see “Change the Initial SAS Viya Landing Page for SAS Users” in *SAS Environment Manager: User’s Guide*.

Enable SAS Drive Application

Starting in the 2024.12 release, the SAS Drive application is disabled by default. The content management functionality of SAS Drive is now available on the **Content** page in SAS Environment Manager. For more information see “SAS Drive Deprecation in December 2024” in *SAS Environment Manager: User’s Guide*.

Administrators can enable SAS Drive until the product is formally retired in the 2025.06 (June 2025) release.

To use the search feature within SAS Drive, you must enable the search indexing. See “searchindex - scheduledEnabled” in *SAS Viya: Configuration Dictionaries* for instructions.

Use the following steps to enable SAS Drive:

1 Sign in to SAS Environment Manager as an administrator.

2 Navigate to the **Rules** page.

3 On the **Rules** page, locate and edit the rule whose **Object URI** is `/SASDrive/**`.

> **TIP** Enter **`/SASDrive/**`** in the **Search** field, and click the search icon.

4 The following two rules are displayed:

Table 2 SAS Drive Rules

Object URI	Principal	Setting	Permissions
/SASDrive/**	Authenticated Users	Grant	Read
/SASDrive/**	Everyone	Prohibit	Read

Right-click the rule with `Everyone` as **Principal** and select **Edit**.

5 In the Edit Rule window slide the **Rule status** to *false*.

6 Click **Save**.

7 To validate, log out and log back in. Verify that you see **Share and Collaborate** from the applications menu, or enter the following URL: **`https://`*`prod.host.com`*`/SASDrive`**.