Global Enablement & Learning

Recommended SAS® 9.4 Security Model Design: Core Artefacts

First Edition

Contact Information

Name: David Stern

Title: Principal Technical Architect, SAS Global Enablement & Learning

Phone Number: +44 1628 490851 Cell: +44 7775 754259

E-mail address: David.Stern@sas.com

THE POWER TO KNOW.

Revision History

Version	By	Date	Description
0.1	David Stern	September 2016	Initial creation, separated out from Core Principles document.
0.2	David Stern	November 2016	Updates in response to review feedback
1.0	David Stern	December 2016	Published
1.1	David Stern	December 2016	Granted permission to share with customers

References

Ref	Document Title	By	Date	Description and source
Ref 1	Metadata Security in SAS® 9.4 – Step-by-Step	Johannes Jørgensen, Cecily Hoffritz	September 2013	Fourth version of Metadata Security in SAS® – Step-by-Step, for SAS® 9.4. Contains a best practice for security implementation and [at the time of publication] has been the de facto standard [for implementation of SAS metadata security] for more than 7 years in Denmark. Source: http://misksapm.na.sas.com/KnowledgeSharingApplication/AdvSearchDisplayArtifact.jsp?Entry_ID=4156

Table of Contents

1 Introduction

1.1 Series Overview

Figure 1 below is an overview of this series of papers, which together represent the GEL recommended practices for security model design in SAS 9.4.

GEL is an abbreviation used widely in these papers, to refer to the SAS Global Enablement and Learning team, part of SAS Global Consulting Services.

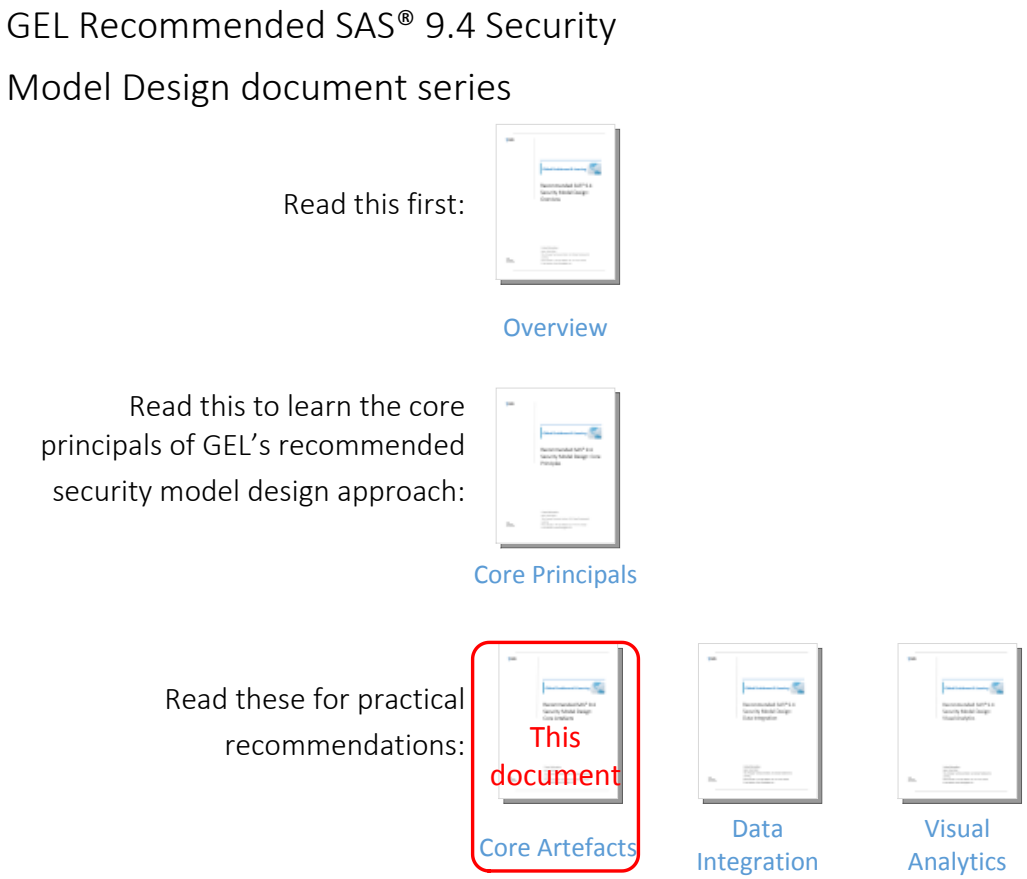


Figure 1 - Overview of papers in this series

1.2 Purpose of this paper

This paper is the first edition of the GEL Recommended SAS 9.4 Security Model Design for **Core Artefacts**, which you should implement on all SAS deployments.

It is one of a series of papers discussing recommended practices for security model design in SAS 9.4. If you have not done so already, you should start by reading Recommended SAS® 9.4 Security

Model Design: **Core Principles**. We intend that this paper be used as an extension of the guidance in that document, rather than as an alternative, or as a standalone document.

See other papers in the "Recommended SAS® 9.4 Security Model Design" series for solution-specific recommendations, which build on the content in this paper.

You may find this process quicker and easier if you use the set of scripts that we have developed to 'turbocharge' (i.e. speed up) your security model setup. The GEL Turbo scripts and accompanying resources are discussed in the **Core Principles** paper.

1.3 Why does this paper have so little content?

There are very few 'core' artefacts in the first edition of our recommended design. The main 'core' content is a set of ACTs, and we mention the top-level metadata and filesystem folders, but several sections of this paper are essentially empty. Why all the 'padding'?

The reason is that we have organised this paper so that its structure is consistent with the structure of the two solution-specific papers, which we hope will help the reader navigate the papers as a set more easily. You should find that after a first reading, you can apply the recommendations in this paper to set up the core parts of a tenant security structure a new environment quite quickly: **there isn't a lot to do for the core content, but what little there is must be done first**.

1.4 Assumptions

This paper assumes you have read the Recommended SAS® 9.4 Security Model Design: Core Principles paper.

This paper also assumes that you can make a consistent system-wide backup, from which you know you can successfully restore, before you make any changes recommended in this paper. We further assume that you have done so immediately before you begin making changes, and may make additional backups at sensible points throughout the process of making these changes.

1.5 Permission to share this document

2 Naming conventions for multitenancy and multi-environment ecosystems

There are no names in the artefacts described in this paper which need to allow for multiple-environment ecosystems, and the only thing necessary to support multitenancy is the use of the tenant's name in the ACT names and (if applicable) the folders discussed in this document.

This section is here to keep the section numbers in this paper consistent with those in the two solution-specific papers.

3 Static metadata groups

'Static metadata groups' in SAS metadata are static in the sense that the process of synchronising groups with Active Directory or another LDAP provider does not create or destroy them.

There are no static metadata groups universal to all solutions, in the current GEL recommended security model design. See other solution-specific papers in this series for the groups recommended for each solution.

This section is present in this paper, even though it has no content, in order to keep the sections of this Core Artefacts paper in line with the sections in the solution-specific papers.

4 Metadata folders

For single-tenant SAS deployments, there are no metadata folders that are universal to all solutions, in the current GEL recommended security model design. See other solution-specific papers in this series for the metadata folders recommended for each solution.

Multi-tenant SAS deployments should have a top-level folder for each tenant, which is named for the tenant organisation, company, project etc. These folders should be directly under SAS Folders if possible, to help minimise the depth of the folder structure for each tenant.

For very large and complex multitenancy designs only (and we recommend this only in designs with more than e.g. 20-30 separate tenants), it may be impractical to put each tenant's top-level folder directly under SAS Folders. In that case, further sub-structure can be used *sparingly*, *with restraint*. Deep folder structures are more confusing and laborious to navigate.

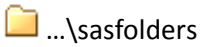
Additional bespoke subfolders are common, and where appropriate should mirror similar bespoke folders in the filesystem folder structure. However, again, exercise restraint, and follow the guidelines in the **Core Principles** paper**.**

5 Filesystem folders

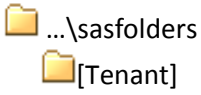
Your architect should choose the location of the folders below, which will contain user-created content and must be on a disk, volume, mountpoint or drive that is large enough and suitably configured for the types of data and the most common ways in which the user-created data will be accessed.

As discussed in the Core Principals paper, for multi-tenancy SAS deployments, your architect may choose to have each tenant's sasfolders directory be same (with a named subdirectory per tenant), or he or she may choose to have a separate sasfolders directory per tenant. Having a separate sasfolders directory per tenant gives you the flexibility to store different tenants' filesystem content on different disks, volumes, mountpoints or drives, each with their own separate allocation of disk space, if you wish to. Having separate sasfolders directory paths per tenant also allows you to back their content up separately. Doing this might be useful so that you can restore one tenant's content separately from the others, and it is also useful if you might ever be required to destroy backups belonging to one tenant (e.g. because they decide to no longer lease space in your SAS deployment), and would not wish to destroy backups for the other tenants.

For single-tenant SAS deployments, only one filesystem folder is universal to all solutions, called sasfolders. You may choose another name for the 'sasfolders' folder if you prefer. The name 'sasfolders' is meant to mirror the "SAS Folders" top-level folder in metadata.



Multi-tenant SAS deployments will have a top level folder beneath this for each tenant, which is named for the tenant organisation, company, project etc.



The sasfolders folder (directory), or the tenant's subfolder, contains all the subfolders (subdirectories) and files belonging to the tenant. These may include a large variety of configuration files, tables Base SAS (and other types of filesystem-based) libraries, files for secured libraries, format and macro catalogues, XML, CSV and other text and binary files used as input or produced as output, and any other sort of file used by end users or the applications they use for doing their work.

The specific folder (directory) structure used to organise these assets is specific to the solution or application which the SAS deployment serves. See the solution-specific papers in this series for the metadata folders recommended for each solution. Additional subfolders for bespoke purposes are

common, and where appropriate should mirror similar bespoke folders in the metadata folder structure.

6 Libraries

There are no libraries which are universal to all solutions, in the current GEL recommended security model design. See the solution-specific papers in this series for the libraries recommended for each solution.

7 Modifications to AppServer Config Files

In this section, an entry in the main sasv9_usermods.cfg file is shown with the following placeholder strings:

Placeholder string	Substitute this with
`[tenant]`	The tenant's name written without spaces
`sasfolders_dir`	The full path to that tenant's sasfolders directory

Following the suggested template configuration lines, an example is shown in which the placeholder strings have been substituted for a tenant called "Rigel" whose sasfolders directory is at D:\sasfolders on Windows, or /opt/sas/data/sasfolders on Unix.

7.1 SASApp/sasv9_usermods.cfg

The only line we add to sasv9_usermods.cfg as part of the 'core' content is one to define a variable in which contains the path to the 'sasfolders' filesystem folder described in section 5 above. This can then be used in library definitions, and in other solution-specific configuration variables described in the relevant papers. This section explains how.

For each tenant using the SAS deployment, add one copy of a line as shown in the sections below, to the sasv9_usermods.cfg file in each AppServer Context which users belonging to that tenant will use.

Spaces are allowed in the sasfolders_dir directory path on both Windows and Unix/Linux.

In the same way that option to use separate 'sasfolders' folder per tenant gives you the flexibility to store different tenants' filesystem content on different disks, having a separate *config file variable* per tenant gives you the flexibility to manage each tenant's disk space independently. It also gives you the flexibility to move one tenant's sasfolders content to a new location (e.g. to a new, larger or faster disk) later on, without having to also move all the other tenant's content to the same location at the same time.

Take care when editing sasv9_usermods.cfg to not specify invalid values: an error reading the config file can prevent SAS from starting a workspace, batch or other SAS session.

7.1.1 Windows

Note that on Windows you must enclose the sasfolders_dir directory path in double quotes, even when there are no spaces in the path.

```
-SET [tenant]_sasfolders "sasfolders_dir"
```

Here is what this might look like with the placeholder strings replaced with example values:

```
-SET Rigel_sasfolders "D:\sasfolders"
```

7.1.2 Unix and Linux

Note that on Unix and Linux, the sasfolders_dir directory path on Unix does not need to be quoted unless it contains spaces. If the sasfolders_dir directory path contains spaces, you should enclose it in either single or double quotes. The tenant name cannot contain spaces.

```
-SET [tenant]_sasfolders sasfolders_dir
```

Here is what this might look like with the placeholder strings replaced with example values:

```
-SET Rigel_sasfolders /opt/sas/data/sasfolders
```

8 Access Control Templates

8.1 Abbreviations for Names of Permissions in ACTs

In describing the Access Control Templates below, we use these abbreviations for the permissions:

Abbreviation	Permission	Controls
RM	Read Metadata	Ability to see a metadata object
WM	Write Metadata	Ability to edit, delete, or set permissions for an object. To delete an object, you also need the WriteMemberMetadata permission for the object's parent folder.
WMM	Write Member Metadata	Ability to add, modify and delete metadata objects in folders. To enable a group to interact with a folder's contents but with not the folder itself, grant WMM and deny WM
MMM	Manage Member Metadata	Change the membership of the Group and Role. Cannot change security or other account attributes.
MCM	Manage Credentials Metadata	Manage accounts and trusted logins of User and Group. Cannot change security or other account attributes.
CM	Check in Metadata	Check in and check out objects in a change-managed area. The CheckInMetadata permission is applicable only in SAS Data Integration Studio.
R	Read	Read data through certain objects (for example, cubes, information maps, and tables that are accessed through the metadata LIBNAME engine)
W	Write	Update data through certain objects (for example, data that is accessed through the metadata LIBNAME engine and publishing channels)
C	Create	Add data through the metadata LIBNAME engine
D	Delete	Applies to normal tables and metadata-bound tables. For normal tables, delete data through the metadata LIBNAME engine.

		For metadata-bound tables, delete rows in a physical table. In order to use SAS to delete data from a metadata-bound table, you need the Delete permission on the corresponding secured table object. You also need the Select permission on that object.
I	Insert	Applies to metadata-bound tables. Add rows to a physical table. For example, in order to use SAS to add data to a metadata-bound table, you need the Insert permission on the corresponding secured table object.
U	Update	Applies to metadata-bound tables. Update rows in a physical table. For example, in order to use SAS to update data in a metadata-bound table, you need the Update permission on the corresponding secured table object. You also need the Select permission on that object.
S	Select	Applies to metadata-bound tables. Read rows within a physical table. For example, in order to use SAS to read data from a metadata-bound table, you need the Select permission on the corresponding secured table object.
CT	Create Table	Applies to metadata-bound tables. Create a new physical table. For example, in order to use SAS to add a table to a metadata-bound library, you need the Create Table permission on the corresponding secured library object. Rename a physical table (if that action creates a new table, rather than overwriting a preexisting table). For example, if you rename TableA to TableB in a metadata-bound library that does not already contain a TableB, you need the Create Table permission on the corresponding secured library object. You also need the Alter Table permission on TableA's corresponding secured table object.
DT	Drop Table	Applies to metadata-bound tables. Delete a physical table. For example, in order to use SAS to delete a metadata-bound table, you need the Drop Table permission on the corresponding secured table object.

AT	Alter Table	Replace a physical table. For example, in order to use SAS to replace a metadata-bound table, you need the Alter Table permission on the corresponding secured table object. Rename a physical table. For example, in order to use SAS to rename a metadata-bound table, you need the Alter Table permission on the corresponding secured table object. You also need the Create Table permission on the corresponding secured library object. Perform other administrative updates on a physical table, such as modifying variable names and labels. For example, in order to use SAS to change labels in a metadata-bound table, you need the Alter Table permission on the corresponding secured table object.
A	Administer	Operate (monitor, stop, pause, resume, refresh, or quiesce) certain SAS servers and spawners
E	Execute	
all	All permissions	Means grant all (G: all) or deny all (D: all) permissions in the ACT to this group or user

8.2 Recommended Core Access Control Templates

Table 1 below shows the Core Access Control Templates that you should modify and create as part of the security model design on every SAS 9 system you deliver.

Create or Modify: ACT Name	User or Group	Permissions Granted (G) or Denied (D)
Modify: Default ACT (Repository ACT) **Apply explicit grant of WMM for SAS Administrators**	PUBLIC	D: all
	SAS Administrators	G: RM WM **WMM** CM A
	SAS System Services	G: RM WM
	SASUSERS	G: RM WM CM
Modify: SAS Administrator Settings **Very important note: we have applied explicit**	SAS Administrators	G: RM WM **WMM** CM A
	SAS System Services	G: RM

grant of WMM for SAS Administrators group		
Create: [Tenant] PUBLIC and SASUSERS Denied ACT	PUBLIC	D: all
	SASUSERS	D: all
Create: [Tenant] SAS General Servers ACT	SAS General Servers	G: RM R S
Create: [Tenant] SASUSERS Read Only ACT	SASUSERS Read Only ACT	G: RM R S D: WM WMM MMM MCM CM W C D I U CT DT AT A E

Table 1 – GEL Recommended 'Core' Access Control Templates to include in any security model design

See the GEL Recommended SAS 9.4 Security Model Design documents for SAS Visual Analytics and SAS Data Integration Studio for additional ACTs which we also recommend you create and apply to objects if your SAS deployment includes SAS Visual Analytics or SAS Data Integration Studio.

8.2.1 About SAS Administrators and Multitenancy

The design shown in these papers uses only the default SAS Administrators group (created when the SAS Intelligence Platform is deployed), and its ACT the 'SAS Administrator Settings' ACT, to provide a single SAS Administrators group whose members can administer metadata for ALL the tenants in the system. This design would not provide for decentralized administration, and separate administrators for each tenant.

It is certainly possible to design a separate 'administrators' group for each tenant, who would typically be granted:

- Full control of metadata belonging to that tenant – not just of the relevant area(s) of the metadata folder structure, but also ACTs, Groups, Servers, OLAP Schemas, Secured Libraries and any other artefacts belonging to the tenant.
- No access at all to metadata belonging to other tenants
- *Optionally* read access to data owned by the tenant. However, some customers require separation of duties between developers, data administrators and metadata administrators. Metadata administrators may be responsible for promoting metadata content between deployments in an ecosystem, and perhaps for maintaining folder structures and permissions but they may not be authorized to see the underlying data in the systems they administer.

Their permissions may be defined so that they do not have Read (and for metadata-bound libraries, Select) access to data belonging to their tenant organization.

9 Apply Access Control Templates

9.1.1 Where to apply core ACTs

In a standard SAS deployment, the group SASUSERS has RM and WM permissions for metadata objects below Server Manager in SAS Management Console which include server contexts and servers. Examples of these are SASApp, SASMeta, SAS Content Server and object spawner. RM and WM permissions allow any registered account to see and modify servers.

Server-side metadata objects are per default not protected and need to be, as shown by the ACT settings below. The [Tenant] SASUSERS – Read Only ACT is a multi-purpose ACT used on folders as well as here. The Read permission is not applicable to server objects, so applying this ACT does not grant broader permissions than are required.

Table 2 below shows where you should apply core ACTs to a range of metadata object types, mainly so that only SAS Administrators can modify them, and everyone can only read and use (but not change) them.

Objects and their location in the Plug-in Tab	**Core ACTs to apply**
SAS Management Console	
Environment Management	
Authorization Manager	
Access Control Templates	
All ACTs	SAS Administrator Settings [Tenant] SASUSERS Read Only ACT
Reason: Only SAS Administrators should have permission to modify ACTs in your security model. Everyone (i.e. SASUSERS) has RM on every ACT: anyone can see the design of any ACTs, but read-only.	
SAS Management Console	
Environment Management	
Server Manager	
SASApp[1], and **SASMeta**	SAS Administrator Settings [Tenant] SASUSERS Read Only ACT

[1] Additional DI-specific ACTs are recommended if your deployment includes DI Studio; see relevant paper.

…plus any new general-purpose Application Server Contexts you create	
Reason: Only SAS Administrators should have permission to modify Application Server Contexts. Everyone (i.e. SASUSERS) needs RM for the two default AppServer Contexts. *SASUSERS are prevented from altering metadata for servers below SASApp because SASUSERS – Read Only has been applied at this level.* *Note: The GEL Turbo applies these ACTs to SASApp and SASMeta. By customizing one of its CSV files, you could easily make it also apply these ACTs to other Application Server Contexts you have created as part of your metadata design, or you could manually apply the ACTs above to new Application Server Contexts.*	
SAS Management Console	
Environment Management	
Server Manager	
All other server definitions *outside* SASApp[1] and SASMeta	SAS Administrator Settings [Tenant] SASUSERS Read Only ACT
Reason: Only SAS Administrators should have permission to modify server definitions. Everyone (i.e. SASUSERS) needs Read Metadata for all server definitions that are not part of an application server context.	
SAS Management Console	
Environment Management	
Server Manager	
SASApp	
SASApp – Logical <all logical server definitions>	SAS Administrator Settings [Tenant] SASUSERS Read Only ACT
Reason: Only SAS Administrators should have permission to modify logical server definitions. Everyone (i.e. SASUSERS) needs Read Metadata for all logical server definitions.	
SAS Management Console	
Environment Management	
Server Manager	
All spawner definitions	SAS Administrator Settings [Tenant] SASUSERS Read Only ACT
Reason: Only SAS Administrators should have permission to modify logical server definitions. Everyone (i.e. SASUSERS) needs Read Metadata for all spawner definitions.	

Table 2 – Metadata objects which should have GEL recommended 'core' ACTs applied to them

See also the GEL Recommended SAS 9.4 Security Model Design documents for SAS Data Integration Studio or SAS Visual Analytics, for details of additional ACTs you should apply to Application Server Contexts if you have those solutions in your SAS deployment.

9.1.2 Apply ACTs to Metadata Folders

The GEL recommended security model design has no core metadata folders for single-tenant SAS deployments, and only one top level folder named for the tenant in a multitenant security model design. The ACTs we recommend you apply to metadata folders are solution-specific. Therefore, *this document* does not list folders to which you should apply ACTs.

See the GEL Recommended SAS 9.4 Security Model Design documents for SAS Visual Analytics and SAS Data Integration Studio, for details of which folders you should secure with both core ACTs described in Table 2 above, and with the solution-specific ACTs described in those documents.

The SAS platform has a significant number of metadata folders in it when deployed. You should consider the folders in your specific SAS deployment, and include these in your design to the extent that you decide whether SASUSERS in general should see each of them, or not.

The core ACTs defined in this paper are also applied to other objects (e.g. your own metadata folders, ACTs and servers) as described in each of the solution-specific papers.

10 Filesystem folder permissions and ownership

10.1.1 Windows Security

On Windows, three levels of permission are used in security windows directories:

Abbreviation	Permission	Controls
F	Full Control	Users with this permission can do anything with the object
C	Change	Read-write. Users with Change permission can edit the object, but cannot change *permissions* on the object.
R	Read	Read only.

Secure the sasfolders directory on the filesystem like this:

Folder	Windows Security Settings
…\sasfolders	Remove all inherited settings. Set on "this folder only" SYSTEM: F Installers: F Administrators: F Users: R

10.1.2 Unix and Linux Security

There is only one core group in the GEL recommended design for Unix and Linux:

Unix Group	Members
sas	SAS Installation User (sas or sasinst) SAS General Servers user (sassrv)

The GEL Recommended SAS 9.4 Security Model Design documents for SAS Visual Analytics and SAS Data Integration Studio describe additional solution-specific groups which should be created for use in securing the Unix or Linux filesystem on SAS deployments which include those solutions.

Secure the sasfolders directory on the filesystem like this:

Folder	Unix Security Settings	
	Owner (user:group)	Permission pattern
…/sasfolders	sas:sas	2770

Other filesystem directories are recommended in the GEL Recommended SAS 9.4 Security Model Design documents for SAS Visual Analytics and SAS Data Integration Studio. Those documents

describe how their solution-specific directories should be secured on the filesystem, using the sas group and other solution-specific groups.

SAS INSTITUTE INC. WORLD HEADQUARTERS SAS CAMPUS DRIVE CARY, NC 27513
TEL: 919 677 8000 FAX: 919 677 4444 U.S. SALES: 800 727 0025 WWW.SAS.COM