

Paper 376-2011

Best Practice Implementation of SAS[®] Metadata Security at Customer Sites in Denmark

Cecily Hoffritz and Johannes Jørgensen, SAS Institute Inc., Copenhagen, Denmark

ABSTRACT

Is it possible to design and implement metadata security so that it can be managed without you creating security conflicts? Do you need to become a metadata security guru before you dare modify the security implementation? This paper provides you with the proper insight so that you can design and implement metadata security at your site with a 100 % guarantee that you will not experience metadata security conflicts in the future.

For a number of years, Danish customers and others abroad have benefitted from a well-defined and documented metadata security best practice that is now the de facto standard for security implementations in Denmark. During this paper you are introduced to the “golden rules” of the best practice and to the steps that you need to take when you design your security setup. You are also presented with an example of a security design that has suited the requirements of most of our customers.

INTRODUCTION

Why has our metadata security best practice become popular with customers in Denmark? One of the reasons is that it provides a straightforward and very concrete step-by-step recipe on how to overcome the complexities of securing metadata. Customers also claim that they do not have the time to be philosophical, and they expect a ready-made solution that is practically self-implementing.

In order to fully understand the implications behind this best practice, it is important that you have a basic understanding of security with regard to access control templates, access control entries, and the rules of inheritance. It is also important that you understand the identity relationship between groups and users.

We provide the following six steps, which facilitate your work and provide you with a scalable and easy-to-manage security setup for SAS[®] Enterprise Business Intelligence Server and SAS[®] Enterprise Data Integration Server in SAS[®] 9.2:

Step One: Understanding the needs of your organization. Here you need to gather information about user groups and to understand which SAS applications are relevant for them.

Step Two: Understanding the needs of your SAS software. You are introduced to the way SAS applications work with reports and data, and you are given a few guidelines on folder structure.

Step Three: Understanding the golden rules for setting up metadata security. We have formulated 6 important rules, which are the backbone of our best practice and which you need to understand fully and adhere to.

Step Four: Designing access control templates. In this section you are introduced to an example design that usually covers the security requirements for most companies.

Step Five: Applying access control templates. Here you will see how easy it is to apply security to folders and to server-side system objects such as stored process repositories, schemas, etc.

STEP ONE: UNDERSTANDING THE NEEDS OF YOUR ORGANIZATION

Before designing security at your organization, you must gain some knowledge about existing functional roles or user groups, their main job tasks, and the applications that they might want to use. The following simple checklists help you ascertain this information. They are not fixed entities; you can change them to suit your needs.

GROUP CHECKLIST

This checklist gives you an overview of the organizational groups who ultimately need access to metadata, data, and applications. These groups are the ones in your active directory or other user store that you already have or plan to have synchronized into metadata.

In our experience, investigating which groups need access to the SAS platform can be time-consuming because they originally weren't created to be synchronized into a SAS metadata repository and therefore serve a different purpose. You might also have many groups, which takes time to process.

Best Practice Implementation of SAS® Metadata Security at Customer Sites in Denmark, continued

Table 1. Example of Group Checklist with a Small Selection of Groups and a Few Tasks Listed

| Group | Tasks |
|----------------------------|---|
| Administrator | System administration and IT support. |
| Data Warehouse Developer | Working in all phases of a data warehouse project. Building data marts. |
| BI Developer | Building and maintaining reporting/analysis environment. Report application help desk. |
| Sales Analyst | Customer segmentation, planning sales initiatives and analyzing their effect, supplying management with analyses. |
| Sales Relationship Manager | Sales. |
| Sales Assistant | Executing events, assisting in maintaining customer database, editing company Web site. |
| Sales Manager | Responsible for sales initiatives and targets, company Web site, and contact with the media. |
| Sales Department | Everyone working in the Sales Department. It contains the above sales groups and not individuals. |

TASK CHECKLIST

This checklist gives you some indication of level of competency or of whether groups work in a centralized function. For example, if your group belongs to a Business Intelligence Competency Center, then your job is to produce output across departments. If your group only views reports, then you are a light consumer who does not produce for others, and your future need for expert applications is probably low.

If your organization has many groups, then start with a few of them first when you fill out the checklist.

Table 2. Example of Task Checklist with Groups Applied to Tasks

| Task | Group |
|---|--|
| Viewing business reports | All |
| Creating business reports for own purpose | Sales Analyst, Sales Relationship Manager |
| Creating business reports for own department | Sales Analyst, Sales Relationship Manager |
| Creating business reports for other departments | BI Developer |
| Administering and distributing business reports | BI Developer, Sales Analyst |
| | |
| Viewing analytics | All |
| Creating analytics for own purpose | Sales Manager, Sales Analyst |
| Creating analytics for own department | Sales Analyst |
| Creating analytics for other departments | BI Developer, Sales Analyst |
| Administering and distributing analytics | BI Developer |
| | |
| Viewing data | Data Warehouse Developer, BI developer, and all groups in Sales. |
| Creating data for own purpose | Sales Analyst |
| Creating data for own department | Sales Analyst |
| Creating data for other departments | Data Warehouse Developer, BI Developer |
| Administering and distributing data | Data Warehouse Developer |

Best Practice Implementation of SAS® Metadata Security at Customer Sites in Denmark, continued

APPLICATION CHECKLIST

It is important that you acquire an overview of the purchased SAS software—especially the client applications. You can find a really good overview of the **SAS 9.2 Intelligence Platform** on the Web:

<http://support.sas.com/documentation/cdl/en/biov/63145/PDF/default/biov.pdf>



The list here shows selected standard applications for SAS Enterprise Business Intelligence Server and SAS Enterprise Data Integration Server. Your job here is to match groups with applications, as we have done.

Table 3. Example of Application Checklist with Groups Applied

| SAS® Application | | Admini- strator | DW Developer | BI Developer | Sales Analyst | Sales Assistant/ Relation- ship Man- ager | Sales Manager |
|--|--|--------------------|-----------------|-----------------|------------------|---|------------------|
| SAS® Portal | Information consumption on the web | X | X | X | X | X | X |
| | adding/modifying portlets & pages for others | | | X | | | |
| SAS® Web Report Studio (building web reports) | | | | X | X | X | X |
| SAS® Information Map Studio (building reporting data) | | | X | X | X | | |
| SAS® Add-In to MS Office | running reports with prompts | | | | X | X | X |
| | building reports and segmenting data | | | X | X | X | |
| SAS® Data Integration Studio (building data warehouses) | | | X | | | | |
| DataFlux (data cleansing, profiling & generating rules) | | | X | | (X) | | |
| SAS® OLAP Cube Studio (building cubes) | | | X | X | | | |
| SAS® Enter- prise Guide | cleansing data | | X | X | X | | |
| | creating reports | | | X | X | | |
| | creating statistics | | | | X | | |
| | writing programs | | X | X | X | | |
| SAS® Stored Processes (developing dynamic reports based on SAS programs) | | | X | X | | | |
| SAS® Management Console (managing the platform) | | X | | | | | |
| SAS® BI Dash- board | building components | | | X | | | |
| | utilizing components | | | X | X | | |





STEP TWO: UNDERSTANDING THE NEEDS OF YOUR SAS SOFTWARE

VIEWING METADATA IN SAS CLIENT APPLICATIONS

Client applications in SAS Enterprise Business Intelligence Server and SAS Enterprise Data Integration Server behave differently with regard to how they see certain metadata objects. Applications either give the choice of a  Server list view or a  Folder view or both. The way client applications can view metadata objects in Folder view and/or Server view might affect the way you design your metadata folder structure.

Best Practice Implementation of SAS® Metadata Security at Customer Sites in Denmark, continued

Table 4. A Selection of Applications in SAS Enterprise Business Intelligence Server and SAS Enterprise Data Integration Server and How They View Metadata Objects

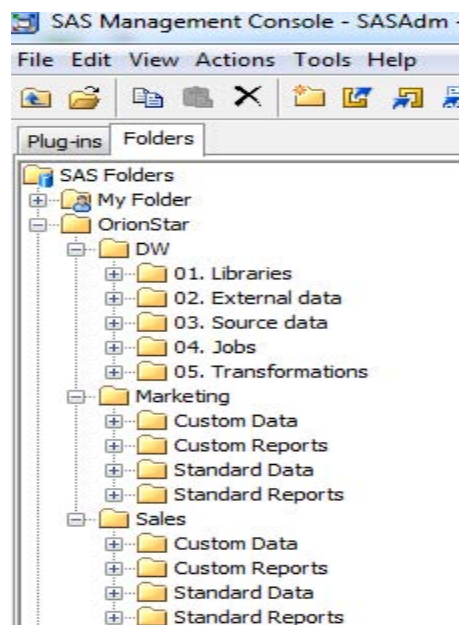
| Client Application |  Server list view |  Folder view | Comments |
|------------------------------|--|--|--|
| SAS® Enterprise Guide | SASApp Server OLAP Server Libraries Tables Cubes | Stored Processes Information Maps Cubes Tables EG projects | No libraries in folders can be viewed in Folder view. A hybrid application which in a standard installation allows you the choice to work classically with SAS (Server list view) and with metadata (Folder view). |
| SAS® Add-In to MS Office | SASApp Server OLAP Server Libraries Tables Cubes | Information Maps Tables Cubes SAS Report Files (WRS) Stored Processes | No libraries in folders can be viewed in Folder view. A hybrid application which in a standard installation allows you the choice to work classically with SAS (only Server list view) and with metadata (Folder view). |
| SAS® Information Map Studio | SASApp Server Libraries Tables Cubes Stored processes | Information Maps | Stored processes running on the standard workspace server and added to information maps. 100% metadata-aware application. |
| SAS® OLAP Cube Studio | | Information Maps Libraries Tables Cubes SAS Report Files (WRS) Stored Processes EG projects Cube jobs | Libraries show up in folders. No Server view starting with  100% metadata-aware application. |
| SAS® Data Integration Studio | | Information Maps Libraries Tables Cubes SAS Report Files (WRS) Stored Processes EG projects Cube jobs | Libraries show up in folders. No Server view starting with  |
| SAS® Web Report Studio | | Information Maps SAS Report Files (WRS) Stored processes | |

Best Practice Implementation of SAS® Metadata Security at Customer Sites in Denmark, continued

DESIGNING METADATA FOLDERS

Our experience based on workshops with customers is that a metadata folder structure can be time-consuming to design without supervision. In Denmark, SAS consultants implement a best practice folder structure for data warehouse projects and supply guidelines for the creation of BI folders. An example of a guideline is that it is easier for you to work with a metadata folder structure that mirrors your physical folder structure whenever it makes sense to do so.

This simplified and shallow folder structure allows you easy navigation and light security maintenance.



A FEW THOUGHTS BEHIND THE METADATA FOLDER STRUCTURE

The top folder, **OrionStar**, allows us to create subfolders on a per-company basis.

The **DW** folder contains numbered folders for a data warehouse project, and metadata objects below this folder may also be numbered. An example of this could be the numbering of jobs to show a dependency sequence. Source libraries are gathered into the folder **01. Libraries**, while target libraries are not registered to this folder. Here, we decided to register them in the folder **Standard Data** so they reside alongside data objects such as tables and information maps. Security-wise, it is easier for you to manage both libraries and data in the same folder, but they can be split into separate folders as well. If you then decide to hide the folder with libraries for some groups, these groups won't be able to see any table metadata in the data folder unless you open up access for one or more library objects in the hidden folder.

Note that there are no folders called Libraries in the above departmental folder structure. The reason for this is that library metadata objects don't surface in folders in Business Intelligence applications such as SAS Enterprise Guide or SAS Add-In to MS Office. Users will wonder why the folder called Libraries is empty.

Note also that we don't number departmental folders. The reason for this is that if certain folders are hidden, then their folder number is hidden as well and shows an incomplete sequence of numbered folders for users.

The idea behind the **Standard Data** departmental folder is that it typically contains data produced by data warehouse developers, and the **Standard Reports** folder is typically for reports produced by BI developers.

Unlike standard departmental folders, custom folders contain reports and data produced by selected super users from a department.

Best Practice Implementation of SAS® Metadata Security at Customer Sites in Denmark, continued

STEP THREE: UNDERSTANDING THE GOLDEN RULES FOR SETTING UP METADATA SECURITY

The following six generic golden rules are the heart and soul of our metadata security best practice. They were initially devised for SAS 9.1 and did not undergo any revisions at all for SAS 9.2. Abiding by these rules still allows you a great deal of creativity when you design your own security setup. Some of them are more meaningful later on when we present to you an example security implementation.

RULE #1: APPLY ACCESS CONTROL TEMPLATES (ACTS) TO RESOURCES

It is absolutely strictly forbidden for you to use access control entries (ACEs—that is, tick marks with white background on resources). Our recommendation for your securing resources is a combination of inheritance (tick marks with gray background) and ACTs (tick marks with green background). If you apply only ACTs and not ACEs, your life as an administrator will be easier because you can maintain all security changes centrally in the Authorization Manager plug-in of SAS Management Console.

Note that in a standard software installation and configuration, you might already see ACEs applied, which we advise you not to change, and the security design behind row-level security on maps and cubes forces you to apply ACEs.

RULE #2: ADD ONLY GROUPS IN ACTS

From a maintenance point of view, it is much easier working on a group level than on a person level. Once you design your ACTs containing groups, all you need to do is synchronize users into these groups. We suggest that you add only one group per ACT whose name is synonymous with the group.

RULE #3: ACTS WITH EXPLICIT GROUPS (NOT PUBLIC OR SASUSERS) ARE ONLY ALLOWED TO GRANT ACCESS, NEVER TO DENY IT

This is the most important rule of them all. It ensures a 100% guarantee that you no longer will experience security conflicts. Whether you are a member of more than one group or your groups are members of other groups is not an issue.

This rule is also the hardest rule for you to comply with because it is so easy to tick mark a denial for a permission to compensate for too much access on a specific resource. If you breach this rule, you will really topple the apple cart, and your compensational permission denials for explicit groups will wreak havoc on this best practice and in the end they give you a bad headache!

RULE #4: APPLY, WHENEVER NEEDED, ACTS WITH EXPLICIT GROUP(S) GRANTING ACCESS IN COMBINATION WITH ACT DENYING RM FOR SASUSERS


This rule is for situations where you want to allow selected groups to view certain metadata objects while hiding those objects from others. The process of showing metadata folders to some groups and hiding them from others is a good example of this. This rule is not in conflict with rule #3 because we are denying access for implicit groups, not for explicit groups. It allows us to rely heavily on resolving security conflicts via the identity hierarchy.

Here is an example of how this rule works. Remember, if you are registered in metadata, you are always a member of the implicit group SASUSERS, and you most probably belong to at least one explicit group. You are of course also an implicit member of PUBLIC, and a prerequisite for this best practice is that you have not changed the standard settings that deny all permissions for PUBLIC in the Default ACT.

Table 5. How Rule #4 Works

| | | | | |
|----------|---|---|--|---|
| Scenario | Access control template 1 is applied on folder A granting Read Metadata to group ABC. | = | Access control template 2 is applied on the same folder A denying Read Metadata to group SASUSERS. | The group ABC is allowed to see the folder A, while all others not belonging to ABC aren't. |
| Step 1 | ACT | = | ACT | 1. Check type of access control (not the permission). Are they equal? Here they are because the folder A is secured by 2 ACTs (rule #1 is applied here). If they are |

Best Practice Implementation of SAS® Metadata Security at Customer Sites in Denmark, continued

| | | | | |
|--------|---|----|----------------|---|
| | | | | equal, then the conflict cannot be resolved via access control type , and the identity hierarchy must be checked as well. |
| Step 2 | Explicit group  | <> | Implicit group | 2. Check identity hierarchy. Are they equal? Here they are <u>not</u> equal because the explicit group ABC wins over the implicit group SASUSERS. Your membership in the explicit group ABC will give you the grant. If you are not a member of the explicit group ABC, then you are still implicitly a member of SASUSERS and you will be denied access instead. |

RULE #5: ALWAYS APPLY THE ACT FOR ADMINISTRATORS WHEN SASUSERS HAVE BEEN DENIED ACCESS

You must always apply this rule in conjunction with rule #4. Restricted administrators are subject to access control like anybody else and are affected by an ACT denying SASUSERS access.

RULE #6: DESIGN AND DOCUMENT FIRST, AND IMPLEMENT EARLY

Design your setup and document it on paper first before you implement it. 90% of the work is the design and documentation, and once you have that in place, implementation is easy as pie. Remember that a standard initial 9.2 security setup is a closed one to users other than administrators, so your job is to implement security as early as possible to open up access for them.

STEP FOUR: DESIGNING ACCESS CONTROL TEMPLATES

OVERVIEW OF PERMISSIONS

Here is a list of permissions used in the access control templates below:

RM = Read Metadata: Ability to see a metadata object.

WM = Write Metadata: Ability to add, modify, and delete metadata.

WMM = Write Member Metadata: Ability to add, modify, and delete metadata objects in folders.

CM = Check-in Metadata: Ability to check metadata back to foundation or other repository from a project repository.

R = Read: Ability to read data.

W = Write: Ability to modify existing data.

C = Create: Ability to add new data.

D = Delete: Ability to delete data.




A = Administer: Ability to administer SAS OLAP Server and SAS Table Server.

Other permissions relating to SAS Table Server are not included here.


























OVERVIEW OF ACCESS CONTROL TEMPLATES

If you create access control templates that are similar to the ones below, they probably satisfy most of your security requirements or could be a good starting point. You see them applied in the next step.

Table 6. Example of General Use Access Control Templates. G: Grant, D: Deny, All: All Permissions

| | |
|---|--|
|  Default ACT (Repository ACT) (This is a standard setup) |  PUBLIC D: ALL  SAS Administrators G: RM WM CMA |
|---|--|

Best Practice Implementation of SAS® Metadata Security at Customer Sites in Denmark, continued

| | |
|--|---|
| |  SAS System Services G: <u>RM WM</u>  SASUSERS: G: <u>RM WM CM</u> |
|  SAS Administrator Settings (we have added WMM to the standard setting) |  SAS Administrators G: <u>RM WM WMM CM A</u>  SAS System Services G: <u>RM</u> |
|  Data Warehouse Developers ACT |  Data Warehouse Developers G: <u>RM WM CM WMM R W C D A</u> |
|  BI Developers ACT |  BI Developers G: <u>RM WMM R W C D</u> |
|  Sales Analysts ACT |  Sales Analysts G: <u>RM WMM R W C D</u> |
|  Sales Assistants ACT |  Sales Assistants G: <u>RM WMM R</u> |
|  Sales Relationship Managers ACT |  Sales Relationship Managers ACT G: <u>RM WMM R</u> |
|  Sales Managers ACT |  Sales Managers G: <u>RM WMM R</u> |
|  Sales Department - Read Only ACT |  Sales Department G: <u>RM R</u> |
|  SASUSERS - Denied ACT ^{*1)} |  SASUSERS D: <u>RM WM WMM CM</u> |
|  SASUSERS – Read Only ACT ^{*2)} |  SASUSERS G: <u>RM R</u> D: <u>WM WMM CM</u> |
|  System Users ACT ^{*3)} |  SAS General Servers G: <u>RM R</u> |

^{*1)} SASUSERS – Denied ACT denies SASUSERS permissions for reading and writing metadata and is used later to hide folders.

^{*2)} SASUSERS – Read Only ACT allows SASUSERS to read metadata and read rows of data for those with Read access in the operating system. For example, you can apply this ACT to an “Enterprise Reports” folder that the whole organization can access.









^{*3)} System Users ACT, which contains the General Servers group, allows the shared account SASSRV to read rows of data when stored processes run on the Stored Process Server.

STEP 5: APPLYING ACCESS CONTROL TEMPLATES





















SECURING YOUR CUSTOM FOLDERS NICELY AND EASILY

Securing folders can be easy if you keep it simple. Bear in mind that the more differentiated your groups need access to different folders, the more complex your security setup will be. In the simple but effective setup in the table below, each department has general Read access across all departmental folders, while specialized users from the department have supplemental grants of Write access on specific folders. To keep things simple, specialized groups such as data warehouse developers have Read and Write access across all folders, while BI developers have Read and Write access to all departmental folders.

Table 7. Applying Access Control Templates to Your Own Folders

| | |
|---|---|
|  SAS Folders | Standard protection originating from SAS Administrator Settings applied during installation |
|  My Folder | Standard protection originating from Private User Folder ACT applied during installation |
|  OrionStar | Inherited settings from  SAS Folders for Administrators, which is the only group allowed to modify this top-level company folder. |
|  DW |  SAS Administrator Settings ,  Data Warehouse Developers ACT ,  SASUSERS - Denied ACT |

Best Practice Implementation of SAS® Metadata Security at Customer Sites in Denmark, continued

| | |
|--|--|
|  1. Libraries | <p>Inherited settings from DW folder for Data Warehouse Developers and Administrators.</p> <p>Inherited exclusion for all other groups who won't see this folder.</p> |
|  2. External data | <p>Inherited settings from DW folder for Data Warehouse Developers and Administrators.</p> <p>Inherited exclusion for all other groups who won't see this folder.</p> |
|  3. Source data | <p>Inherited settings from DW folder for Data Warehouse Developers and Administrators.</p> <p>Inherited exclusion for all other groups who won't see this folder.</p> |
|  4. Jobs | <p>Inherited settings from DW folder for Data Warehouse Developers and Administrators.</p> <p>Inherited exclusion for all other groups who won't see this folder.</p> |
|  5. Transformations | <p>Inherited settings from DW folder for Data Warehouse Developers and Administrators.</p> <p>Inherited exclusion for all other groups who won't see this folder.</p> |
|  Sales | <p> SAS Administrator Settings,  Data Warehouse Developers ACT,  BI Developers ACT,  Sales Department – Read Only ACT,  System Users ACT,  SASUSERS - Denied ACT</p> |
|  Custom Data | <p> Sales Analysts ACT, Sales Manager ACT</p> <p>Inherited settings from Sales folder for BI and Data Warehouse Developers who are allowed to create data here.</p> <p>Inherited settings from Sales folder for the shared account SASSRV behind the General Servers group in the System Users ACT allowing Read access to these data so that stored processes running on the Stored Process Server can be based on them.</p> <p>Inherited settings from the Sales folder for the Sales Department allowing them to read these data.</p> <p>Inherited exclusion for all other groups who won't see this folder.</p> |
|  Custom Reports | <p> Sales Analysts ACT,  Sales Managers ACT,  Sales Relationship Managers ACT, Sales Assistants ACT</p> |
|  Standard Data | <p>Inherited settings from Sales folder for BI and Data Warehouse Developers who are allowed to create data here.</p> <p>Inherited settings from Sales folder for the shared account SASSRV behind the General Servers group in the System Users ACT allowing read access to these data so stored processes running on the Stored Process Server can be based on them.</p> <p>Inherited settings from Sales folder for Sales Assistants via Sales Department ACT who can read these standard data.</p> <p>Inherited exclusion for all other groups who won't see this folder.</p> |
|  Standard Reports | <p>Inherited settings from Sales folder for BI and Data Warehouse Developers allowing them to create reports.</p> <p>Inherited settings from Sales folder for the Sales Department who can read these standard reports.</p> <p>Inherited settings from Sales folder for the shared account SASSRV behind the General Servers group in the System Users ACT. These permissions are not necessary for this group but since they can read the data behind</p> |

Best Practice Implementation of SAS® Metadata Security at Customer Sites in Denmark, continued

| | |
|--|---|
| | standard reports the permissions remain granted. Inherited exclusion for all other groups who won't see this folder. |
|--|---|

OPENING UP STANDARD FOLDERS TO CREATE CUBES

In a standard installation, you can't create cubes because the SASApp - OLAP Schema, which you find in the folder SASApp – OLAP Schema below the folder Shared Data is tightly locked down with an inherited denial of WM, which originates from a system--applied ACE denying WM for PUBLIC on SAS Folders.

In our scenario, if you want to allow BI developers to create cubes, they need the BI Developers ACT applied to the custom folder where they will save the cube metadata object. They also need you to apply the BI Developers ACT to the folder SASApp - OLAP Schema, as shown below. This ACT has only WMM, not WM, but the OLAP schema in the folder will inherit a grant of WM, which is necessary for building cubes. Here, data warehouse developers create cubes, so you need to apply the Data Warehouse Developers ACT as well.

Table 8. Applying Access Control Templates to Create Cubes

| | |
|----------------------|---|
| SAS Folders | Standard protection originating from SAS Administrator Settings applied during installation |
| My Folder | Standard protection originating from Private User Folder ACT applied during installation |
| Shared Data | Inherited settings from SAS Folders for Administrators. |
| SASApp – OLAP Schema | Data Warehouse Developers ACT BI Developers ACT |

You need to familiarize yourself with other standard folders and their metadata objects in order to assess whether they need special consideration for selected groups.

SECURING SERVER-SIDE

In a standard configuration, the group SASUSERS has RM and WM permissions for metadata objects below Server Manager in SAS Management Console. Those metadata objects 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.

In a standard configuration, PUBLIC is a member of the role Enterprise Guide: Advanced. This allows you to open the SAS Enterprise Guide Explorer, an administrative appendix application in SAS Enterprise Guide, where you maintain metadata libraries and tables, etc. A combination of WMM given to your group on the folder where there are libraries and WM on SASApp, which you inherited via your membership of SASUSERS, allows you to delete or create libraries. You have to consider whether this is a desirable situation.

To summarize, server-side metadata objects are by default not protected and need to be, as shown below. The SASUSERS – Read Only ACT is a multi-purpose ACT used on folders as well as here. The Read permission is not necessary server-side.

Table 9. Applying Access Control Templates to Lock Down Server-Side Metadata Objects

| | |
|------------------------|--|
| SAS Management Console | |
| Environment Management | |
| Server Manager | |
| SASMeta | SAS Administrator Settings SASUSERS - Read Only ACT |

Best Practice Implementation of SAS® Metadata Security at Customer Sites in Denmark, continued

| | |
|------------------------------------|---|
| SASApp | SAS Administrator Settings Data Warehouse Developers ACT SASUSERS - Read Only ACT |
| SASApp - Logical <all definitions> | SAS Administrator Settings SASUSERS - Read Only ACT |
| SASTS - Logical Table Server | Do not change |
| <All other server definitions> | SAS Administrator Settings SASUSERS - Read Only ACT |
| <All other spawner definitions> | SAS Administrator Settings SASUSERS - Read Only ACT |
| | |

You can also create/modify data libraries and source code repositories for stored process programs and deployment directories. In SAS Management Console, you can see these types of objects grouped together if you expand the Authorization Manager plug-in and click **Resource Management ▶ By Location ▶ SAS App** (in the left pane). The objects appear in the right pane. For example, you might see Source code repositories appearing here and depending on how they are created, they assume the standard name **SP Source Directory** or a tailored one. Here, you can also see their inheritance if you log on as an unrestricted administrator and right-click an object such as **SP Source Directory** and select **Properties ▶ Authorization tab ▶ Advanced**. Note that the inheritance of SP Source Directories is not the same as the inheritance of libraries.

If you are creating stored process reports in SAS Enterprise Guide, and if an ACT has granted your group WMM on a folder, you can save your stored process report in that folder, and the underlying stored process program attached to the stored process report can be saved to the source code repository because you have an inherited WM (from Default ACT) via your membership in SASUSERS. Operating system security must be considered but is outside the scope of this paper.

Table 10. Applying Access Control Templates to the Stored Processes Source Code Directory for Sales

| | |
|---|--|
| SAS Management Console | |
| Environment Management | |
| Authorization Manager | |
| Resource Management | |
| By Location | |
| SASApp | |
| SP Source Directory (Description: Sales stored process programs) | SAS Administrator Settings Data Warehouse Developers ACT BI Developers ACT |

Best Practice Implementation of SAS® Metadata Security at Customer Sites in Denmark, continued

CONCLUSION

Throughout this paper, you have seen the golden rules of the best practice used in various scenarios, allowing you easier maintenance. The knowledge that security conflicts won't occur is especially reassuring.

As you might speculate, many groups entail just as many ACTs, and supplementary special purpose ACTs for selected groups make the number of ACTs grow even larger. Despite this, you know that you have only one point of contact when you need to revise a setting in your ACTs, and that is the Authorization Manager plug-in in SAS Management Console. You no longer need to go on roaming expeditions to lots of metadata objects to find ACEs that are hindering or allowing too much access.

Lately, we have begun to automate our setups where we have written SAS programs to create relevant ACTs and folders. With programs, we can create the same setup on other servers with development, test, and production environments. Because our best practice dictates ACTs, they are easily implemented and easy to manage, and that must be the most relevant requirement for any administrator.

RECOMMENDED READING

- <http://support.sas.com/documentation/cdl/en/biov/63145/PDF/default/biov.pdf>
- SAS Institute Inc. 2009. SAS® 9.2 *Intelligence Platform: Security Administration Guide*. Available at <http://support.sas.com/documentation/cdl/en/bisecag/61133/HTML/default/viewer.htm#titlepage.htm>.

CONTACT INFORMATION

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

Author and designer:
Cecily Hoffritz
Education Division
SAS Institute Inc.
Copenhagen, Denmark
Cecily.hoffritz@sdk.sas.com

Co-designer:
Johannes Jørgensen
Technical Consulting Centre
SAS Institute Inc.
Copenhagen, Denmark
Johannes.joergensen@sdk.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.