CHAPTER

1

Security Features

About this Document **3**
Accessibility Features of the SAS Intelligence Platform **3**
Security in the SAS Intelligence Platform **3**
Permissions Overview **4**
Roles Overview **4**
Single Sign-On Overview **5**
Encryption Overview **6**
Security Reporting and Logging Overview **6**

About this Document

This document helps you understand and use the security features of the SAS Intelligence Platform. This document assumes that you are familiar with the concepts and terminology that are introduced in *SAS Intelligence Platform: Overview*.

This document is organized as follows:

- The first four chapters contain the following basic information:
  - a brief overview of security features
  - instructions for the main security tasks
  - essential facts about SAS users, groups, and roles
  - an orientation to using SAS metadata-layer permissions
- The other chapters contain detailed reference information and instructions for specialized tasks.

Accessibility Features of the SAS Intelligence Platform

For information about accessibility for any of the products mentioned in this document, see the online Help for that product. If you have questions or concerns about the accessibility of SAS products, send e-mail to accessibility@sas.com.

Security in the SAS Intelligence Platform

The security features of the SAS Intelligence Platform offer these benefits:

- single sign-on from and across disparate systems
- secure access to data and metadata

- role-based access to application features
- confidential transmission and storage of data
- logging and auditing of security events
- access control reporting

The SAS Intelligence Platform is not an isolated system. The platform's security model cooperates with external systems such as the host environment, the Web realm, and third-party databases. To coordinate identity information, SAS keeps a copy of one ID (such as a host, Active Directory, LDAP, or Web account ID) for each user. This requirement does not apply to any users for whom a generic PUBLIC identity is sufficient.

Permissions Overview

SAS provides a metadata-based authorization layer that supplements protections from the host environment and other systems. Across authorization layers, protections are cumulative. In order to perform a task, a user must have sufficient access in *all* applicable layers.

You can use the metadata authorization layer to manage access to the following resources:

- almost any metadata object (for example, reports, data definitions, information maps, jobs, stored processes, and server definitions)
- OLAP data
- relational data (depending on the method by which that data is accessed)

CAUTION:
Some clients (such as SAS Data Integration Studio and SAS Enterprise Guide) enable power users to create and run SAS programs that access data directly, bypassing metadata-layer controls. It is important to manage physical layer access in addition to metadata-layer controls. For example, use host operating system protections to limit access to any sensitive SAS data sets. See "Host Access to SAS Tables" on page 187. △

CAUTION:
Not all permissions are enforced for all items. Enforcement of permissions other than ReadMetadata and WriteMetadata varies by item type and (for data) by the method with which a library is assigned. △

Roles Overview

The SAS implementation of roles enables you to manage the availability of application features such as menu items, plug-ins, and buttons. For example, your role memberships determine whether you can see the **`Server Manager`** plug-in (in SAS Management Console), compare data (in SAS Enterprise Guide), or directly open an information map (in SAS Web Report Studio).

Here are some key points about the SAS implementation of roles:

- Roles are an entirely separate concept from permissions. In general, roles don't affect access to metadata or data. An exception is that the unrestricted role provides irrevocable grants of all permissions in the metadata authorization layer. This enables unrestricted users to manage all metadata.

- Not all applications have roles. Applications that have roles include the SAS Add-In for Microsoft Office, SAS Enterprise Guide, SAS Management Console, and SAS Web Report Studio.
- Not all application features are under role management. An application feature that is under role management is called a capability. Each application that supports roles provides a fixed set of capabilities. You can't convert a feature that isn't a capability into a capability. However, if you add custom tasks or develop custom plug-ins, you can register those features as capabilities.
- All capabilities are additive. There are no capabilities that limit what you can do.
- Capabilities can be categorized as follows:
  - An explicit capability can be incrementally added to or removed from any role (other than the unrestricted role, which always provides all explicit capabilities). Most roles have explicit capabilities.
  - An implicit capability is permanently bound to a certain role. The metadata server's roles provide implicit capabilities. For example, the user administration role provides the capability to add users, but there is no explicit **`Create Users`** capability.
  - A contributed capability is an implicit or explicit capability that is assigned through role aggregation. If you designate one role as a contributing role for another role, all of the first role's capabilities become contributed capabilities for the second role.
- You can't assign permissions to a role or capabilities to a group.
- A user can't temporarily assume or relinquish a role; all of a user's roles are active at all times. Administrators can have two user definitions so they can function as regular users some of the time. See "How to Create a Dual User" on page 29.
- If you need detailed information about an application's capabilities and default roles, see the administrative documentation for that application.

Single Sign-On Overview

SAS provides these single sign-on (SSO) features:

- To bypass the logon prompt when launching a desktop application (such as SAS Information Map Studio, SAS Enterprise Guide, SAS Data Integration Studio, SAS OLAP Cube Studio, or SAS Management Console), use Integrated Windows authentication. The client and the metadata server must be in the same Windows domain or in domains that trust each other. See "Integrated Windows Authentication" on page 148.

  Note: An alternate method for avoiding the initial logon prompt for a desktop application is to save credentials in a client-side connection profile. This method is supported on all operating systems. If you have more than one connection profile, designate a profile that includes your credentials as your default connection profile. Some sites don't allow users save credentials in their connection profiles. See "Password Policies" on page 14. △
- To bypass the logon prompt when launching a SAS Web application (such as SAS Web Report Studio or SAS Information Delivery Portal), use Web authentication. See "Web Authentication" on page 156.
- Seamless access to data servers and processing servers is provided by mechanisms including SAS token authentication, Integrated Windows authentication, credential reuse, and credential retrieval. See "Authentication to Data Servers and Processing Servers" on page 130.

Encryption Overview

SAS offers encryption features to help you to protect information on disk and in transit. Here is an overview of encryption support in the SAS Intelligence Platform:

- Passwords in configuration files and the metadata are encrypted or encoded. Most other metadata is not encrypted.
- Passwords in transit to and from SAS servers are encrypted or encoded. You can choose to encrypt all traffic instead of encrypting only credentials.

Security Reporting and Logging Overview

Security reporting creates a snapshot of metadata-layer access control settings. SAS provides the %MDSECDS autocall macro to enable you to easily build data sets of permissions information. You can use those data sets as the data source for security reports. You can also identify changes in settings by comparing data sets that are generated at different times. See Chapter 10, "Security Report Macros," on page 115.

Security logging records security-related events as part of a system-wide logging facility. The following table describes the security log categories:

Table 1.1 Logging of Security Events

Category	Events Captured
Audit.Authentication	Authentication events, client connection information.
Audit.Meta.Security.UserAdm	Changes to users, groups, roles, logins, and authentication domains. Includes additions, deletions, modifications, and failed attempts to perform these actions.
Audit.Meta.Security.GrpAdm	Changes to memberships (for groups or roles). Includes adding members, removing members, and failed attempts to perform these actions.
Audit.Meta.Security.AccCtrlAdm	Changes to permissions, permission settings, ACTs, and passwords.* Includes additions, deletions, modifications, and failed attempts to perform these actions.
Audit.Meta.Security	The parent category for security events. Logging settings that you define for this category apply to its child categories.

* This is for passwords on objects such as Tables, Connections, and ProtectedPassthrus.