Using SAS® Environment Manager 2.6 Administration

About This Document . . . 4
- Audience . . . 4
- Accessibility . . . 4
- Documentation Conventions . . . 4

What's New in SAS Environment Manager Administration . . . 6
- General Updates . . . 6
- Updates for SAS Visual Analytics Administrators . . . 6

Introduction . . . 8
- What Is SAS Environment Manager Administration? . . . 8
- Launching SAS Environment Manager Administration . . . 9
- Who Can Launch SAS Environment Manager Administration? . . . 9
- Initial Page in SAS Environment Manager Administration . . . 10

Folders Page . . . 12
- Introduction . . . 12
- About the Folders Page . . . 12
- Add a Folder . . . 13
- Stage a Table . . . 13
- Open a Report . . . 13
- Delete an Object . . . 14
- Rename a Folder . . . 14
- Edit an Object's Properties . . . 14
- Related Tasks . . . 15

Libraries Page . . . 16
- Introduction . . . 16
- About the Libraries Page . . . 16
- Add a Library . . . 16
- Delete a Library . . . 17
- Register Tables . . . 17
- Assign a Library to a SAS Application Server . . . 18
- Related Tasks . . . 18

Servers Page 19
Introduction 19
About the Servers Page 19
Add a Server 20
Operate a Server 20

Users Page 21
Introduction 21
About the Users Page 21
Add a User 21
Add a Group 23
Add a Role 23
Manage Memberships 24
Store DBMS Credentials 24
Update a Stored Password 25
Store Contact Information 25
Assign Capabilities to a Role 26
Manage Capabilities for a User 27
Manage Authorization for an Identity 27
Advanced Tasks 28
Related Tasks 31

LASR Page 32
LASR Servers Tab 32
LASR Tables Tab 32
Monitoring Tabs 33
Related Tasks 33

Tools Page 34
HDFS Tab 34
Alerts Tab 34

Mobile Devices Page 35
Introduction 35
About the Mobile Devices Page 35
Add a Device to a List 36
Remove a Device from a List 37
Determine When a Device Was Blacklisted 37
Advanced: Change How Devices Are Managed 37
Related Tasks 38

Backup Manager Page 39
Introduction 39
About the Backup Manager Page 39
The Scope of a Backup 40
Get Status and Details 41
Run an Ad Hoc Backup 44
Change the Backup Policy 45
Enable Scheduled Backups 46
Change the Backup Schedule 46
View Generated Log Messages 47
Use the Command-Line Interface 47
Related Tasks 47

SAS Grid Manager 48

Reference 49
Logs 49

Preferences . . . 50
Advanced Tab . . . 51
Server Categories . . . 52
Roles and Capabilities . . . 53
Tips for Interacting with Tables . . . 56
Options for Servers and Libraries . . . 56

Authorization . . . **57**
Permissions . . . 57
Examine Access . . . 58
Manage Access . . . 62
Advanced: Manage ACTs . . . 64

Troubleshooting . . . **67**
Access Issues . . . 67
LASR Issues . . . 68

About This Document

Audience

This document helps you use SAS Environment Manager Administration.

This document is part of the integrated collection of SAS 9.4 administration guides.

Accessibility

See *SAS Environment Manager Administration: Accessibility Features*.

Documentation Conventions

SAS Configuration Directory

The phrase *SAS configuration directory* refers to a host path that includes a configuration name and level.

Host	Example
UNIX:	`/opt/sas/config/Lev1`
Windows:	`C:\sas\Config\Lev1`

For more information, see "Overview of the Configuration Directory Structure" in *SAS Intelligence Platform: System Administration Guide*.

Note: For directory paths that are identical on UNIX and Windows, this document uses UNIX style path delimiters (/ instead of \).

Short Forms and Labels

The interface and this document use following short-form terminology:

Long Form	Short Form
Access control template	ACT
Hadoop Distributed File System	HDFS
SAS LASR Analytic Server	LASR server
SAS LASR Analytic Server library	LASR library
SAS LASR Analytic Server table	LASR table

Note: Not all terms are applicable to all deployments.

What's New in SAS Environment Manager Administration

General Updates

The 2.6 release of SAS Environment Manager Administration differs from the prior version as follows:

- Aesthetics and navigation paths are updated.
- A new **Mobile Devices** page helps you specify which devices can use mobile apps from SAS. See "Mobile Devices Page".

> **TIP** At this time there is no corresponding 2.6 release of SAS Environment Manager or SAS Grid Manager. (Prior versions of those applications are compatible with the 2.6 release of SAS Environment Manager Administration.)

Updates for SAS Visual Analytics Administrators

Functionality that was previously provided by SAS Visual Analytics Administrator is now provided by SAS Environment Manager Administration.

Here are key points:

- The **LASR** page helps you manage and monitor in-memory servers and data. See "LASR Page".
- The **Tools** page helps you manage metric alerts and, if applicable, co-located Hadoop. See "Tools Page".
- The **Mobile Devices** page helps you specify which devices can use mobile apps from SAS. See "Mobile Devices Page".

Here are additional details:

- You can open SAS Visual Analytics reports from the **Folders** page. See "Open a Report".
- Some SAS Visual Analytics capabilities affect access to features in SAS Environment Manager Administration. See "Capabilities".
- User preferences that were previously available in SAS Visual Analytics Administrator are available in SAS Environment Manager Administration. See "Preferences".
- You can use new methods to access SAS Environment Manager Administration. Previous access methods remain available. See "Launching SAS Environment Manager Administration".

See Also

"What's New in Administration of SAS Visual Analytics" in *SAS Visual Analytics: Administration Guide*

Introduction

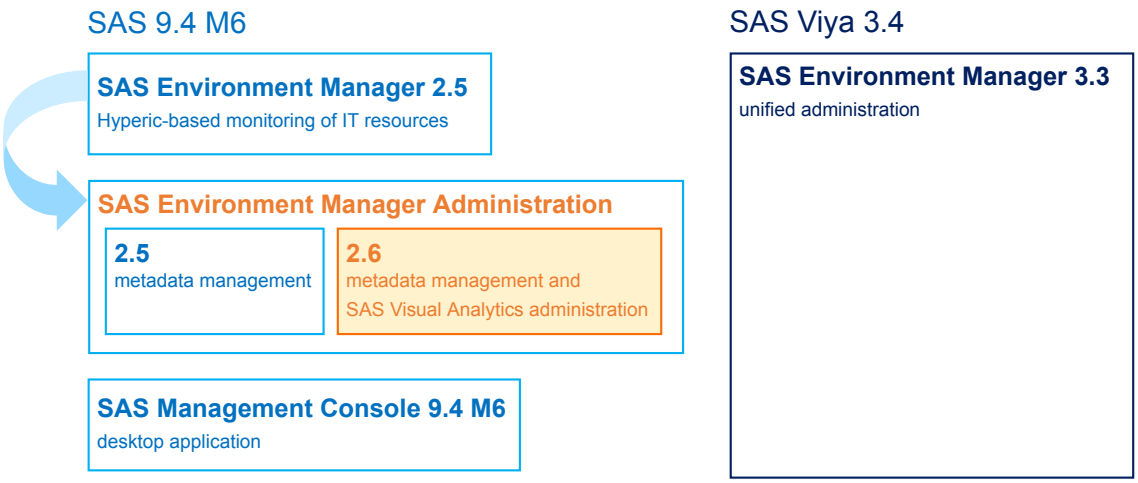
What Is SAS Environment Manager Administration?

SAS Environment Manager Administration is a web application that helps you administer a SAS 9.4 environment. The emphasis is on managing SAS metadata.

Here are key points:

- For some tasks, this application is an alternative to SAS Management Console.
- For membership and authorization metadata, this application provides enhanced views.
- For SAS Visual Analytics 7.5, this application replaces the SAS Visual Analytics Administrator application.
- Do not confuse this application (SAS Environment Manager Administration) with SAS Environment Manager. They are two separate web applications.

The following figure shows this application in the context of other administrative applications, as of May 2019. The arrow indicates that you can launch this application from SAS Environment Manager 2.5.



Note: The 2.*x* releases of SAS Environment Manager help IT operations staff manage SAS 9 computing resources. The 3.*x* releases of SAS Environment Manager help SAS administrators manage SAS Viya components.

Launching SAS Environment Manager Administration

Direct Access

In a supported browser, go to your equivalent of the following URL:

machine.company.com/SASEnvironmentMgrMidTier/

For the exact URL, open the file SAS-configuration-directory`/Documents/Instructions.html` on your middle-tier machine. Search for `SASEnvironmentMgrMidTier`.

Note: Any URL that previously provided direct access to SAS Visual Analytics Administrator now provides direct access to SAS Environment Manager Administration.

Integrated Access

1. In the banner of an integrated SAS 9 application (such as SAS Visual Analytics 7.5), click ☰.
2. In the applications menu, under **SAS VISUAL ANALYTICS**, click **Administrator**.

   If that menu item is not present, verify the following items:

   - Make sure you have the capability that this access method requires (Visual Analytics: Advanced: Manage Environment).
   - Make sure you are not in a SAS Viya application, such as SAS Visual Analytics 8.3.

   In the current browser window, the application context switches to SAS Environment Manager Administration.

Access from SAS Environment Manager

In SAS Environment Manager, click the **Administration** tab.

In a new browser window, SAS Environment Manager Administration opens.

Who Can Launch SAS Environment Manager Administration?

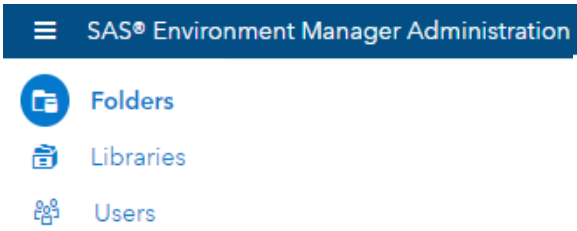
The prerequisites for launching this application vary by access method as follows:

Access Method	Availability
Direct	Any registered user.
Integrated	Anyone who has the Visual Analytics: Advanced: Manage Environment capability.
From SAS Environment Manager	Anyone who can access SAS Environment Manager. [1]

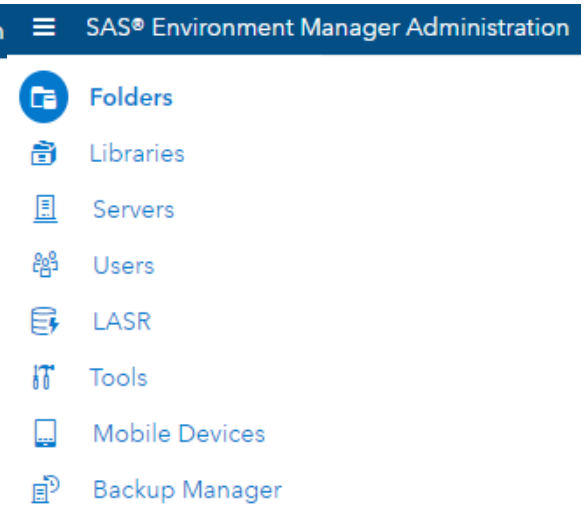
1 See Controlling Access to SAS Environment Manager in *SAS Environment Manager: User's Guide*.

Within SAS Environment Manager Administration, not all features are present in all deployments and available to all users. For example, capabilities might cause the items in the vertical navigation bar to differ as follows:

For an end user:



For an administrator:



Note: The preceding screenshots reflect a deployment that includes SAS Visual Analytics and does not include SAS Grid Manager. The end user does not have explicit group memberships. The administrator is a member of the groups SAS Administrators and Visual Analytics Data Administrators.

To troubleshoot sign-in problems, see "Access Issues".

Initial Page in SAS Environment Manager Administration

The initial display is the **LASR** page if all of the following criteria are met:

- SAS Visual Analytics is deployed.

- You access the application by selecting **Administrator** in the applications menu, or from a direct URL that previously provided access to SAS Visual Analytics Administrator.
- You have the Visual Analytics: Advanced: Manage Environment capability and either or both of the following capabilities:
  - Visual Analytics Admin: Manage LASR Analytic Server
  - Visual Analytics Admin: Monitor LASR Analytic Server

In other circumstances, the initial display is the **Folders** page (or the first page that you are authorized to see).

To navigate to a different page, click an icon in the vertical navigation bar.

> **TIP** To see the labels for the icons in the vertical navigation bar, click ›› at the bottom of the display.

See Also

- *SAS Environment Manager: User's Guide*
- "Accessing SAS Visual Analytics" in *SAS Visual Analytics: Overview*
- "Overview of the Administration Tools" in *SAS Intelligence Platform: System Administration Guide*

Folders Page

Introduction

Use the **Folders** page to perform the following tasks:

- Organize content (such as reports) and data definitions (such as libraries and tables).
- View, edit, rename, protect, and delete objects. Not all actions are supported for all objects.
- Create access control templates. See "Create an ACT".
- Register tables. See "Register Tables".
- Stage tables. See "Stage a Table".
- Open reports. See "Open a Report".

For concepts and background information, see "Working with SAS Folders" in *SAS Intelligence Platform: System Administration Guide*.

About the Folders Page

Here are details and tips:

- To locate an object, browse the folder tree in the navigation pane.

  Note: The search functionality in the application banner is not integrated with SAS Environment Manager Administration. See "Search" in *SAS 9.4 Web Applications: General Usage Help*.

- To view information about an object, select the object in the navigation pane.

  Note: A few nodes (**SAS Folders**, **sascontent**, and virtual folders) do not open an object definition.

- To delete an object, right-click the object in the navigation pane, and select **Delete**.

  Note: Not all object types support the Delete action. For example, you cannot delete an ACT. See "Advanced: Manage ACTs".

  Note: In a SAS Visual Analytics deployment that uses co-located HDFS, you can delete a physical HDFS table along with its metadata. See "How to Delete an HDFS Table" in *SAS Visual Analytics: Administration Guide*.

- To manage access to an object, use the object's **Authorization** or **Direct ACTs** tab. See "Authorization".
- It is rarely necessary to add information to the Advanced tab.

Add a Folder

1 In the navigation pane, select the folder that should be the immediate parent of the new folder.

2 Right-click, and select **New folder**.

3 Enter a name.

Stage a Table

Note: This task is applicable only if you load data from co-located or NFS-mounted storage to a distributed LASR Analytic Server. See "Distributed Server: Parallel Load" in *SAS Visual Analytics: Administration Guide*.

1 On the **Folders** page, right-click on a table. Select **Add to HDFS** (to stage to co-located HDFS) or **Add to Data Server** (to stage to NFS-mounted MapR).

2 In the displayed window, make any necessary adjustments.

Note: Specify a table name that will also be appropriate as the LASR table name. (When you later load the staged table, the LASR table name will be the same as the name of the staged table.)

3 Click **OK**.

Open a Report

This task is applicable if SAS Visual Analytics is deployed.

1 In the navigation pane, select a SAS report (2G) object.

2 Right-click, and select **View report**.

In the current browser window, the application context switches to the report viewer, which displays the selected report.

3 (Optional) To return to SAS Environment Manager Administration, click ☰ in the banner. In the applications menu, under **SAS VISUAL ANALYTICS**, click **Administrator**.

Note: If **Administrator** is not listed in the applications menu, see "Streamlining Access to Management Pages" in *SAS Visual Analytics: Administration Guide*.

In the current browser window, the application context switches back to SAS Environment Manager Administration.

Note: If SAS Visual Analytics is deployed, a **Usage Reports** button in the navigation pane provides a shortcut to administrative reports. For details, see "About the Predefined Reports" in *SAS Visual Analytics: Administration Guide*.

Delete an Object

1 In the navigation pane, select the object that you want to delete.

Note: Only objects of the following types can be deleted: folder, Base SAS library, LASR library, LASR server, table.

2 Right-click, and select **Delete**.

3 In the **Confirmation** window, click **Yes**.

Rename a Folder

1 In the navigation pane, select the object that you want to rename.

2 Right-click, and select **Rename**.

3 In the **Rename** window, edit the name.

4 Click **OK**.

Note: To rename a library, click ✎ on the library's **Properties** tab.

Edit an Object's Properties

1 In the navigation pane, select an object.

2 On the object's **Properties** tab, click ✎.

3 In the Edit Properties window, make changes as needed. Click **Save**.

Related Tasks

To copy, move, export, or import objects, use SAS Management Console. See "Using the Export SAS Package and Import SAS Package Wizards" in *SAS Intelligence Platform: System Administration Guide*.

To manage objects that are beneath the **sascontent** node, use SAS Web Administration Console. See "Use the SAS Web Administration Console " in *SAS Intelligence Platform: Middle-Tier Administration Guide*.

Libraries Page

Introduction

Use the **Libraries** page to perform the following tasks:

- View library definitions.
- Register and delete tables.
- Add, edit, and delete definitions for Base SAS and LASR libraries.
- Edit definitions for other libraries, except for values on the **Options** tab and the **Data Servers** tab.

For concepts and background, see *SAS Intelligence Platform: Data Administration Guide*.

About the Libraries Page

Here are details and tips:

- You can sort the list and choose which columns are displayed. See "Tips for Interacting with Tables".
- To filter the display, use either or both of these techniques:
  - Enter text in the filter field.
  - Select a category of library types from the drop-down list.
- To view a library's definition, right-click the library and select **Open**.
- You can navigate the data hierarchy as follows:
  - To view the properties of a table, locate the table on the parent library's **Tables** tab. Right-click the table, and select **Open**.
  - To go back to the table's parent library, click .
- To manage access to a library, use the library's **Authorization** or **Direct ACTs** tab. See "Authorization".
- Some LASR libraries have extended attributes on their Advanced tab.

Add a Library

1. On the **Libraries** page, click .
2. In the New Library window:

a Select a library type (**Base SAS Library** or **SAS LASR Analytic Server Library**).

Note: To add and manage other types of libraries, use SAS Management Console.

Note: You can add a LASR library only if SAS Visual Analytics is deployed.

b Provide the required information.

c Click **Save**. The new library definition is displayed.

3 Make changes as needed.

Here are links to detailed, type-specific documentation:

Library Type	Documentation
Base SAS	"Establishing Connectivity to a Library of SAS Data Sets" in *SAS Intelligence Platform: Data Administration Guide*.
LASR	"LASR Library Definition" in *SAS Visual Analytics: Administration Guide*, or the administrative documentation for your product.

Delete a Library

On the **Libraries** page (or the **Folders** page), right-click the library. Select **Delete**. Click **Yes** to confirm the deletion.

If the library contains registered tables, a second confirmation message is displayed. That message explains that deleting a library causes its table metadata to be deleted, and asks whether you want to proceed.

Register Tables

1 On the **Libraries** page (or the **Folders** page), right-click a library. Select **Register tables**.

If that action is not available, make sure that both of these criteria are met:

- The library is assigned to at least one server. See "Assign a Library to a SAS Application Server".
- You can launch a workspace server. You cannot launch a workspace server under an internal account (such as sasadm@saspw).
- You are authorized to register tables in the library. For requirements, see "Registering and Verifying Tables" in *SAS Intelligence Platform: Data Administration Guide*.

2 Specify the metadata folder location where the new tables should be stored.

3 Select tables to register.

Note: Any LASR tables that are already registered are listed, with check boxes that you cannot select.

4 Specify the following options as needed.

Enable case-sensitive DBMS object names
specifies whether case-sensitive names for tables and columns are supported in the metadata that you are about to generate for tables in the current library. If the check box is cleared, no support is provided. If the check box is selected, support is provided.

Enable special characters within table and column names
specifies whether special characters in names for tables and columns are supported in the metadata that you are about to generate for tables in the current library. If the check box is cleared, no support is provided. If the check box is selected, support is provided.

5 Click **OK**.

TIP You can also register tables by clicking + on a library's **Tables** tab.

Assign a Library to a SAS Application Server

Each library can be assigned to one or more servers. Assigning a library to a server means that the server is aware of the library and has access to the library. For more information, see "Assigning Libraries" in *SAS Intelligence Platform: Data Administration Guide*.

To change a library's server assignments:

1 From the **Libraries** page or the **Folders** page, open the library.

2 On the library's **Assigned SAS Servers** tab, click ✎.

3 In the Edit Assigned SAS Server window, select or clear check boxes. Click **Save**.

Related Tasks

For other library-related tasks, use SAS Management Console. See *SAS Intelligence Platform: Data Administration Guide* or the Help for SAS Management Console.

Servers Page

Introduction

Use the **Servers** page to perform the following tasks:

- View definitions for servers and their components.
- Add, edit, and delete definitions for LASR servers.
- Add a new associated machine, when you are adding a LASR server.

For concepts and background information, see "Servers in the SAS Intelligence Platform" in *SAS Intelligence Platform: Overview*.

About the Servers Page

Here are details and tips:

- To open the definition for a server or component, select it in the navigation pane.
- In the navigation pane, you can view all servers or only those servers that are in a selected category. See "Server Categories".
- In the navigation pane, you can expand or collapse the server hierarchy. Each level in the hierarchy has distinct properties. For example, see "The Structure of a SAS Application Server" in *SAS Intelligence Platform: Application Server Administration Guide*.
- To modify the properties of a LASR server, select the server and then click on the appropriate tab.

  Note: In the current release of this application, you can edit only LASR servers and their associated machines.

- To manage access to a server, use the server's **Authorization** or **Direct ACTs** tab. See "Authorization".

  Note: To learn about managing access to servers, see "Access to Server Definitions" in *SAS Intelligence Platform: Security Administration Guide*.

- Some LASR servers have extended attributes on their Advanced tab.

Add a Server

1 In the navigation pane on the **Servers** page, click [*].

Note: If SAS Visual Analytics is deployed, you can add a LASR server. In the current release, you cannot add other types of server. (To add and manage other types of servers, use SAS Management Console.)

2 In the New Server window, provide the required information.

3 Click **Save**. The new server definition is displayed.

4 Make changes as needed.

For detailed instructions, see "LASR Server Definition" in *SAS Visual Analytics: Administration Guide*.

Operate a Server

To operate a LASR server, use the **LASR** page. See "Start or Stop a LASR Server" in *SAS Visual Analytics: Administration Guide*.

To operate other servers, use SAS Management Console or scripts. See "Operating Your Servers" in *SAS Intelligence Platform: System Administration Guide*.

Users Page

Introduction

Use the **Users** page to create and manage metadata identities (users, groups, and roles).

For concepts, alternative interfaces, and background information, see "User Administration" in *SAS Intelligence Platform: Security Administration Guide*.

About the Users Page

Here are details and tips:

- Most **Users** page tasks require user administration capabilities. See "Who Can Manage Users, Groups, and Roles?" in *SAS Intelligence Platform: Security Administration Guide*.
- To open an identity definition, select a user, group, or role in the navigation pane.
- In the navigation pane, you can view all identities or only identities of a selected type (users, groups, or roles).
- In the navigation pane, the filter looks for your specified text anywhere in the name and display name fields, for the identities in the current view.
- Make changes on the **Authorization** or **Direct ACTs** tab for an identity only if you need to delegate an identity management task. See "Manage Authorization for an Identity".

Add a User

1 Identify or create an account with which the user can access the SAS Metadata Server.

In the simplest case, accounts are known to the metadata server's host. For details and exceptions, see "Authentication to the Metadata Server" in *SAS Intelligence Platform: Security Administration Guide*.

Note: You do not have to register users who need only limited, anonymous access to SAS Visual Analytics. See "Configure Guest Access" in *SAS Intelligence Platform: Middle-Tier Administration Guide*.

2 Make sure the account has any necessary host-layer privileges.

- If the user accesses servers on Windows, see "Windows Privileges" in *SAS Intelligence Platform: Security Administration Guide*.

- If the user imports or loads data in SAS Visual Analytics or starts and stops a LASR server, see "Host Account Privileges" in *SAS Visual Analytics: Administration Guide*.

3 In the navigation pane on the **Users** page, click . Select **New user**.

Note: If that action is not available, you are not authorized to add users. Sign in as someone who has user administration capabilities (for example, sasadm@saspw).

4 In the New User window, provide information as follows:

a In the **Name** field, enter a unique identifier for the user.

b Enter a display name for the user.

c Click **Save**. The new user definition is displayed.

5 In the unusual circumstance in which the new user should have only an internal account, skip this step.

On the new user's **Accounts** tab, click . In the Edit Accounts window, click the + to add an inbound login for the user. See "How Logins Are Used" in *SAS Intelligence Platform: Security Administration Guide*.

In the new row, provide information as follows:

a If the **web** authentication domain is available, see "Logons for Users Who Participate in Web Authentication" in *SAS Intelligence Platform: Security Administration Guide*.

Otherwise, select the **DefaultAuth** authentication domain.

Note: The preceding instructions assume that your deployment uses the standard authentication domains. See "Authentication Domains" in *SAS Intelligence Platform: Security Administration Guide*.

b Click in the **Stored User ID** field, and enter the user's account ID (as identified in step 1).

For a Windows account, you must enter the user ID in one of the following formats:

user-ID@domain.extension or *domain\user-ID* or *machine\user-ID*

c Leave the **Stored Password** field blank. It is not necessary to store a password for inbound (initial authentication) purposes. Click **Save**.

6 On the new user's **Member Of** tab, click , and add direct memberships for the user as follows:

Type of User	Direct Member Of
Unrestricted user	**Metadata Server: Unrestricted**
Platform administrator	**SAS Administrators**
SAS Visual Analytics administrator	**Visual Analytics Data Administrators**
SAS Visual Data Builder user	**Visual Data Builder Administrators**
SAS Visual Analytics user	**Visual Analytics Users**

Type of User	Direct Member Of
Users of other products	See your product-specific documentation.

Note: The preceding instructions assume that your deployment uses the predefined groups and roles. Users of SAS Visual Analytics get their role memberships indirectly through their group memberships. See "Initial Role Members" in *SAS Visual Analytics: Administration Guide*.

Note: Only an unrestricted user can add members to the Metadata Server: Unrestricted role. See "Create an Additional Unrestricted User".

7 (Optional) On the new user's **Accounts** tab, store additional credentials.

8 (Optional) Store contact information for the new user.

9 Validate the new user. Ask the user to sign in to an application and verify that the expected functionality is available.

Note: If necessary, see the troubleshooting information for accessing SAS Environment Manager Administration or SAS Visual Analytics. To troubleshoot access to another product, see the documentation for that product.

Add a Group

1 In the navigation pane on the **Users** page, click . Select **New group**.

2 In the New Group window:

   a Specify a name and a display name.

   b Select the **Foundation** repository, unless you know that the group should be defined in a custom repository.

   c Click **Save**. The new group is displayed.

3 On the group's **Members** tab, click , and assign direct members.

4 (Optional) On the group's **Member Of** tab, click , and add direct memberships as needed.

5 (Optional) On the group's **Accounts** tab, click + to stored shared credentials.

Add a Role

1 In the navigation pane on the **Users** page, click . Select **New role**.

2 In the New Role window:

   a Specify a name and a display name.

   b Select the **Foundation** repository, unless you know that the group should be defined in a custom repository.

   c Click **Save**. The new role is displayed.

3 Assign capabilities to the role.

4 Assign members to the role.

Manage Memberships

On the **Members** tab for a group or role, click . Add or remove direct members.

On the **Member Of** tab for a group or user, click . Add or remove direct memberships.

Here are details about the display:

- Top-level nodes represent direct relationships.
- Lower-level nodes represent nested relationships.
- Implicit relationships (automatic membership in the PUBLIC and SASUSERS groups) are not displayed. See "Metadata Groups" in *SAS Intelligence Platform: Security Administration Guide*.

Store DBMS Credentials

For background information, see "Credential Management" in *SAS Intelligence Platform: Security Administration Guide*.

Store Shared Credentials

Note: These instructions apply to third-party servers that do not accept the credentials with which users initially log on to SAS clients. These instructions are also appropriate for providing seamless access to other servers that require credentials that are different from the credentials with which users initially log on to SAS clients.

1 Identify or create the group that you will use to manage the shared DBMS account. For example, if you want all registered users to share the account, use the SASUSERS group.

2 On the group's **Accounts** tab, click + to add a login.

   a In the **Domain** column, select the authentication domain for the DBMS.

   Note: In the DBMS server metadata, the authentication domain is specified on the connection object.

b In the **Stored User ID** column, enter the DBMS user ID.

c In the **Stored Password (Optional)** column, store the DBMS password.

3 On the group's **Members** tab, make sure that everyone who needs to use the shared account is a member.

Store Personal Credentials

Follow the instructions in the preceding topic, but add the login to a user definition instead of a group definition.

Note: If a user has more than one available login in a particular authentication domain, the login that is closest to the user is used. If there is tie, you might not be able to predict which login is used. One example of a tie is when a user is a direct member of two groups and both groups have logins in the same authentication domain.

Update a Stored Password

1 On the **Accounts** tab of the user or group whose external password has changed, click the cell that you need to update.

Note: Logins are visible only if you have user administration capabilities, you are looking at your own user definition, or you are looking at the definition for a group that you belong to.

2 In the Store Password (Optional) window, enter and confirm the new password.

Store Contact Information

On a user's **Contact Information** tab, click ✎.

Note: You cannot store contact information for groups or roles.

Note: If you batch synchronize users and want to preserve contact information that you enter interactively, use a consistent value in the **Type** field. In your synchronization code, you can use this value to define exceptions that exclude this data from the batch update.

Assign Capabilities to a Role

Here are details about the **Capabilities** tab:

- For a brief description of the currently selected capability or category, open the **Capability Details** pane from the right edge of the application. For more information about a capability, see the documentation for the associated product or component. For example, see the capabilities documentation for SAS Visual Analytics or SAS Environment Manager Administration.

  Note: The **Capability Details** pane also includes an **Origins** section that explains how the currently selected capability is assigned to the current role.

  CAUTION
  In the Edit Capabilities window, clicking an item's text affects the item's check box status. To view properties for an item without inadvertently affecting the item's assignment status, use the **Capabilities** tab instead of the Edit Capabilities window. (Or, in the Edit Capabilities window, click a **Details** button.)

- The interface does not display implicitly assigned capabilities (for example, members of the **Metadata Server: Unrestricted** role always implicitly have all of the listed capabilities).

The initial capabilities-to-roles mapping is appropriate in many cases. If necessary, you can change the set of capabilities that a role provides.

CAUTION
There is no automated method for reverting a role back to its original set of capabilities. Instead of adjusting the capabilities of a predefined role, consider creating a new role. Before you alter role capabilities, make sure you have a complete and current backup. See "About Backing Up and Restoring Your SAS Content" in *SAS Intelligence Platform: System Administration Guide*.

To change a role's capabilities, use either or both of the following techniques:

- On the role's **Capabilities** tab, click ✎. Incrementally add or remove capabilities from the role by selecting or clearing check boxes.

  CAUTION
  In the Edit Capabilities window, clicking an item's text affects the item's check box status.

  Note: You cannot see or alter implicitly assigned capabilities.

  Note: You cannot completely clear the check box for a contributed capability. You can directly add a capability on top of a contributed capability. Removing a direct capability reveals a contributed capability, if a contributed capability is present.

- On the role's **Contributing Roles** tab, click ✎. Select one or more check boxes to give the current role all of the capabilities of one or more other roles.

For more information, see "Metadata Roles" in *SAS Intelligence Platform: Security Administration Guide*.

Manage Capabilities for a User

Each user has all of the capabilities that are provided by any of his or her roles. To manage capabilities for a user, adjust the user's memberships or change the assignments of capabilities to roles.

To prevent a user from having a particular capability, make sure that user is not in any role that provides that capability. Here are tips:

- A capability can be provided by multiple roles, so you must investigate all of the user's roles.
  - Use the user's **Member Of** tab to find all of the user's explicit and indirect role memberships.
  - If the user has a well-formed definition, the user is automatically a member of any roles that are assigned to the implicit groups (PUBLIC and SASUSERS). Use the **Member Of** tab for each of those implicit groups to find any associated role memberships.

  Note: The **Member Of** tab lists both groups ( ) and roles ( ). Only roles provide capabilities.
- Each role's **Capabilities** tab indicates all of the direct and contributed capabilities that the role provides.
- Each role's **Capabilities** tab includes a **Capability Details** pane that provides a description of the currently selected capability or category. The **Capability Details** pane for a capability also includes an **Origins** section that explains how the selected capability is assigned to the current role.
- Capabilities are grant-based. You cannot deny a capability.
- Unrestricted users always have all explicit capabilities.

Note: There is no per-user or per-group summary of capabilities.

Manage Authorization for an Identity

IMPORTANT The **Authorization** and **Direct ACTs** tab in an identity definition do not affect that identity's access to resources.

In an identity's definition, the **Authorization** and **Direct ACTs** tab protect (or provide access to) only that identity definition. Make changes only as described in "Delegate Group or Role Management".

To examine user or group access to a resource, use the **Authorization** tab for that resource. See "View Effective Access to an Object".

> **TIP** If the user or group is not already listed on that tab, use the permissions inspector. See "Look Up an Access Information for an Identity".

To modify user or group access to a resource, use the resource's authorization-related tabs or the authorization-related tabs for one of the resource's parent objects.

Advanced Tasks

Create an Internal Account

Internal accounts have limitations and should not be used for regular users. For more information, see "SAS Internal Authentication" in *SAS Intelligence Platform: Security Administration Guide*.

You might create an internal account for temporary use in verifying the effects of changes to capability assignments.

1 In the navigation pane on the **Users** page, click . Select **New user**.

Note: If that action is not available, you are not authorized to add users. Sign in as someone who has user administration capabilities (for example, sasadm@saspw).

2 In the New User window, provide information as follows:

   a In the **Name** field, enter a new identifier for the account. When you use the account, you will sign in using this identifier appended with the string `@saspw` (for example, test@saspw).

   b Click **Save**. The new user definition is displayed.

3 On the **Accounts** tab, click .

   In the **Internal account** section of the Edit Accounts window, select the **Use internal account** check box. Enter and confirm a new password for the account. Set other options as needed.

4 On the **Member Of** tab, click , and add direct memberships as needed.

5 Verify that the internal account can sign in.

Note: To determine whether an existing user has an internal account, examine the **Internal account** section of the user's **Accounts** tab. If a user has an internal account, their internal user ID is listed in that location. Internal accounts are visible only if you have user administration capabilities or you are looking at your own user definition.

Manage Internal Account Policies

1 Sign in as someone who has user administration capabilities (for example, sasadm@saspw).

2 Open the definition for a user who has an internal account.

Note: Regular users do not have internal accounts.

3 On the user's **Accounts** tab, click .

4 In the **Internal Account** section, make changes as needed. Here are tips:

- General policies are managed at the server level. See "How to Change Internal Account Policies" in *SAS Intelligence Platform: Security Administration Guide*.
- The **Accounts** tab displays only those settings that can be managed on a per-user basis.
- There are two distinct expiration settings. Do not confuse the account expiration date with the password expiration period.
- In the **PASSWORD** section, the expiration settings are available only when the **Password is exempt from the general password expiration policy** check box is selected.

5 Click **Save**.

Manage External Identity Information

In general, you should not make changes on an identity's **External Identities** tab.

For details and exceptions, see "External Identities" in *SAS Intelligence Platform: Security Administration Guide*.

Delegate Group or Role Management

Introduction

This section explains how to delegate certain user administration tasks to a non-administrator. In the current release, delegated user administration is supported in only SAS Management Console.

To enable someone who does not have user administration capabilities to manage a particular group or role, use a direct grant of the appropriate permission (ManageMemberMetadata or ManageCredentialsMetadata).

Note: It is possible to delegate by granting the WriteMetadata permission, but that is not the preferred approach.

Note: The grant can be explicit or from an access control template.

Delegate Member Management

On the **Authorization** tab of a group or role, grant the ManageMemberMetadata permission to the non-administrator who should be able to add and remove members for that group or role.

Delegate Credential Management

On the **Authorization** tab of the group, grant the ManageCredentialsMetadata permission to the non-administrator who should be able to add and remove logins for that group.

Create an Additional Unrestricted User

Note: If a user should be an administrator, but does not need unrestricted access to metadata, do not use these instructions. Instead, simply add the user to the SAS Administrators group.

1 Sign in as an unrestricted user (for example, sasadm@saspw).

   Note: If there are no unrestricted users, see the information about the adminUsers.txt file in "Unlock an Internal Account" in *SAS Intelligence Platform: Security Administration Guide*.

2 Create a new registration for the user.

   In the **Name** field in the New User window, specify a value that can be used in an internal account ID. For example, if you enter `tara`, the user's internal account ID is `tara@saspw`.

   Note: By creating a separate registration, you enable the user to choose whether to sign in with or without unrestricted privileges. See "Add Dual Users" in *SAS Intelligence Platform: Security Administration Guide*.

3 On the user's **Accounts** tab, add an internal account. It is not necessary to add a login.

4 On the user's **Member of** tab, make the user a direct member of the **Metadata Server: Unrestricted** role.

Revoke Access to Management Pages

In the initial configuration, non-administrators have access to the **Folders**, **Users**, and **Libraries** pages in SAS Environment Manager Administration, mirroring the availability of corresponding plug-ins in SAS Management Console. Activities in those functional areas are constrained by permissions and implicit capabilities, so it is not strictly necessary to block access at the level of the user interface.

If you want to hide those pages from non-administrators, modify the membership or capabilities of the Management Console: Content Management role. Here are examples:

- On the **Members** tab of the Management Console: Content Management role, remove SASUSERS. If appropriate, assign a more specific group to that role.
- On the **Capabilities** tab of the Management Console: Content Management role, remove one or more capabilities (**Data Library Manager**, **Folder View**, and **User Manager**).

Note: For details about SAS Management Console roles and capabilities, see "Administering Roles" in *SAS Intelligence Platform: Desktop Application Administration Guide*.

Delete an Identity

CAUTION

When you delete a user, group, or role, you lose all of that identity's metadata associations. Creating a new identity with the same name does not restore the associations.

1 On the **Users** page, locate the identity that you want to delete.

2 Right-click the identity, and select **Delete**.

Note: If that action is not available, you are not authorized to delete identities. Sign in as someone who has the required capabilities (for example, sasadm@saspw).

3 In the confirmation message box, click **Yes**.

Related Tasks

To batch import and synchronize identity information, use the user import macros. See "Overview of User Bulk Load and Synchronization" in *SAS Intelligence Platform: Security Administration Guide*.

See Also

- "SAS Internal Authentication" in *SAS Intelligence Platform: Security Administration Guide*
- "Uniqueness Requirements" in *SAS Intelligence Platform: Security Administration Guide*
- "Who Can Manage Users, Groups, and Roles?" in *SAS Intelligence Platform: Security Administration Guide*

LASR Page

The **LASR** page is present if SAS Visual Analytics 7.5 is deployed.

LASR Servers Tab

You can use the **LASR Servers** tab to start (▷), stop (■), and get status for a LASR server. For instructions and details, see "Operating Servers" in *SAS Visual Analytics: Administration Guide*.

The **Status** column uses the following icons:

	Running
	Stopped
	Over capacity
	Unknown

LASR Tables Tab

You can use the **LASR Tables** tab to load, unload, reload, and get status for LASR tables. For instructions and details, see "Loading Data" in *SAS Visual Analytics: Administration Guide*.

The **Status** column uses the following icons:

	Loaded
	Loaded and compressed
	Loaded, with additional full copies
	Loaded, with additional full copies and compressed
	Unloaded
	Unknown

Monitoring Tabs

The **Monitor Resources** and **Monitor Processes** tabs are present if your SAS Visual Analytics deployment includes a distributed LASR server. For details, see "Distributed Server: Monitoring" in *SAS Visual Analytics: Administration Guide*.

Use the controls at the top of the **Monitor Processes** tab as follows:

- To view top resource consumers, select a **Top 5** or **Top 10** item in the **Selection** drop-down list. If no application instances appear in the graphs, no application instances have a resource utilization greater than zero for the current criteria.
- To filter application instances, enter text in the **Filter** field. Only those application instances that have an ID that contains the specified value appear in the graphs.

Related Tasks

To set permissions or attributes on a LASR library or table, open the library or table from the **Folders** page (or the **Libraries** page).

To set permissions or attributes on a LASR server, open the server from the **Folders** page (or the **Servers** page).

To add a LASR library, use the **Libraries** page. See "LASR Library Definition" in *SAS Visual Analytics: Administration Guide*.

To add a LASR server, use the **Servers** page. See "LASR Server Definition" in *SAS Visual Analytics: Administration Guide*.

To limit the amount of space that a LASR server can use to host tables, see "Limiting Space for Tables" in *SAS Visual Analytics: Administration Guide*.

Tools Page

The **Tools** page is present if SAS Visual Analytics 7.5 is deployed.

HDFS Tab

The **HDFS** tab is present if your SAS Visual Analytics deployment uses co-located HDFS.

The **HDFS** tab provides a host-layer view of HDFS folders and tables. The view is not mediated by metadata or by your permissions. Instead, a privileged account retrieves the information that this tab displays.

Note: If the tab is expected but not present, make sure you have the **Visual Analytics Admin: Browse HDFS** capability. See "Capabilities".

Note: If the tab does not provide the expected information, make sure the LASR monitor is running. See "Supporting the HDFS Browse Features" in *SAS Visual Analytics: Administration Guide*.

You can use the **HDFS** tab to perform the following tasks:

- Browse HDFS folders and tables.
- View row count, columns, column information, and block information for tables that have been added to HDFS. Information about block distribution, block redundancy, and measures of block utilization is provided.
- Delete HDFS tables that are stored in SASHDAT format. (Files that are stored in other formats are listed, but they cannot be deleted.)

For details, see "Distributed Server: Co-located HDFS" in *SAS Visual Analytics: Administration Guide*.

Alerts Tab

The **Alerts** tab displays only LASR metric alert definitions that are created in SAS Visual Analytics.

You can use the **Alerts** tab to delete other users' alert definitions.

For details, see "Managing Alerts and Notifications" in *SAS Visual Analytics: Administration Guide*.

Mobile Devices Page

The **Mobile Devices** page is present if SAS Visual Analytics 7.5 or SAS Enterprise BI is deployed.

Introduction

Use the **Mobile Devices** page to specify which devices can use mobile apps from SAS.

You can manage devices either by exclusion or by inclusion.

- If you manage by exclusion, all devices can use mobile apps from SAS except those that are on the blacklist. A blacklist is a list of mobile devices that are not authorized to use mobile apps from SAS.
- If you manage by inclusion, only devices that are on the whitelist can use mobile apps from SAS. A whitelist is a list of mobile devices that are authorized to use mobile apps from SAS.

Here are key points:

- The mobile device lists affect devices, not users. To manage what a particular user can see or do in mobile apps from SAS, use permissions and capabilities.
- A deployment enforces only one mobile device list (either the blacklist or the whitelist). In a new deployment the blacklist is enforced, so there are no device-level barriers to participation.
- You can modify both lists. Making changes to a list that is not currently enforced can help accommodate a future change.

For related information, including capabilities, configuration properties, logging, and troubleshooting, see Manage Devices and "Configuration Properties: Transport Services" in *SAS Intelligence Platform: Middle-Tier Administration Guide*.

About the Mobile Devices Page

Here are details and tips:

- By default, the **Logon History** tab displays the most recent sign-in event for each device. The following occurrences are sign-in events:
  - a connection attempt that comes from a new source (a unique combination of device ID and user ID)
  - a connection attempt that is accompanied by a device change (such as a new operating system version or application version)

  To view previous sign-in events that are accompanied by a device change, select the **Include device history** check box.
- On the **Logon History** tab, the **Status** column provides information about a sign-in event. The **Status** column does not indicate the current status of a device connection. The **Status** column uses the following icons:

✓	Success
⊗	Failure (authentication)
!	Failure (device in the blacklist)
⊘	Failure (device not in the whitelist)
○	Unknown

- When you right-click on a device on the **Logon History** tab, remember that only one list is in use. Adding a device to the list that is not in use has no immediate effect. For example, if your deployment uses the blacklist, adding a device to the whitelist has no immediate effect.
- On the **Blacklist** and **Whitelist** tabs, each cell in the **User ID** column contains the user ID that connected (or attempted to connect). The user ID is provided for the purpose of helping you identify a device. If no user has attempted to connect from a particular device, no user ID is listed for that device. If multiple users have attempted to connect from a particular device, all of those user IDs are listed.
- The **Management History** tab displays device management events, such as adding a device to a list or removing a device from a list. The **Admin ID** column provides the user ID of the administrator who performed each action.
- When you right-click on a device in the blacklist or whitelist, you can choose either a move action or a remove action. In terms of immediate effect, there is no difference between these two actions.

Add a Device to a List

1. Select the **Blacklist** or **Whitelist** tab.
2. Click +. Enter the device ID in the Add to Blacklist or Add to Whitelist window.
3. Click **Save**.

Here are additional details:

- To add multiple devices, click ⧺.
- The device IDs that you enter are not validated by the software.

  Note: A device ID is a unique identifier (usually a hardware device number) that is determined and communicated by the connecting mobile app.

- For a device that has already connected (or attempted to connect), you can initiate this task from the **Logon History** tab. Right-click on the device, and select **Add to Blacklist** or **Add to Whitelist**.

Remove a Device from a List

To remove a device from the blacklist, right-click on it on the **Blacklist** tab, and select **Move to whitelist**.

To remove a device from the whitelist, right-click on it on the **Whitelist** tab, and select **Move to blacklist**.

Determine When a Device Was Blacklisted

1. Use the **Blacklist** tab to obtain the device ID.
2. On the **Management History** tab, select **Device ID** from the drop-down list.
3. Click in the text field, and enter the device ID.

> **TIP** You can use the same process to determine when a device was whitelisted.

Advanced: Change How Devices Are Managed

CAUTION
These are deployment-level instructions that affect all access to mobile apps from SAS.

To switch from enforcing one list to enforcing the other:

1. Verify that the list that you intend to enforce is appropriately populated.
   - If you enforce the whitelist, the whitelist should contain all eligible devices. The blacklist is ignored.
   - If you enforce the blacklist, the blacklist should contain all excluded devices. The whitelist is ignored.
2. On the tab for the list that you want to enforce, click **Enable**. In the confirmation window, click **Yes**.

Note: In the standard configuration, only unrestricted users and members of the SAS Administrators group can perform this task. The ability to perform this task is controlled by WriteMetadata access to the software component **Visual Analytics Transport Service 7.5**.

Related Tasks

To require passcode protection, use a capability. See “Lock SAS Visual Analytics App with a Passcode ” in *SAS Intelligence Platform: Middle-Tier Administration Guide*.

To limit the duration of offline access, use a capability. See “Use the Time-out Setting to Prevent Access” in *SAS Intelligence Platform: Middle-Tier Administration Guide*.

To prevent local caching of report data, use a capability. See “Prevent Report Data from Being Cached on the Device” in *SAS Intelligence Platform: Middle-Tier Administration Guide*.

To enable your mobile apps to include SAS Visual Analytics content, see “Mobile Software Development Kits” in *SAS Intelligence Platform: Middle-Tier Administration Guide*.

To resolve access issues, see “Troubleshooting: SAS Visual Analytics App” in *SAS Intelligence Platform: Middle-Tier Administration Guide*.

Backup Manager Page

Introduction

To set up and perform integrated backups, click **Backup Manager**.

Here are the default settings for backups:

- By default policy, backups are retained for 30 days.
- By default, backups are scheduled for Sundays at 1:00 a.m.
- By default policy, backups are local. The backup for each component is written to only that component's host machine.

  IMPORTANT It is strongly recommended that you specify a central vault location for secondary storage of backups.

- By default policy, notifications of unsuccessful backups and recoveries are sent to the email address that was specified during deployment. You can designate different recipients.

IMPORTANT Backup Manager is a plug-in to the Deployment Backup and Recovery tool. Neither the plug-in nor the tool performs a backup of the entire SAS deployment. To formulate a complete and coordinated backup strategy, see " Best Practices for Backup and Restore" in *SAS Intelligence Platform: System Administration Guide*.

About the Backup Manager Page

Here are key points:

- The **Backup Manager** page is available to users that are unrestricted and users that are members of the SAS Administrators group. You cannot configure (expand or reduce) the availability of the **Backup Manager** page or any task on that page.
- When you access the **Backup Manager** page, there might be a brief delay. In some deployments, it takes a few minutes to discover assets in your deployment that are available for backup.
- Here is a quick reference for which tasks are available on each tab:

Tab	Tasks
History	Start an immediate backup.

Tab	Tasks
	View status, details, and sources for operations (backups and recoveries).
Policy	Enable scheduled backups. View or modify the backup policy. View information about currently configured backup sources.
Schedule	View or modify the backup schedule.

- The **Backup Manager** page does not support the following tasks:
  - Restore (recover) content from a backup.
  - Configure (include or exclude) sources for backups.

  To restore content or configure the scope of backups, use the command-line interface.
- The **Backup Manager** page uses diagrams to depict participating resources and machines. You can manipulate the diagrams as follows:
  - Click a node to collapse its child nodes.
  - Click the node again to expand it so that its child nodes reappear.
  - Zoom in or out by clicking the diagram to select it and then pressing **Ctrl** while scrolling the mouse wheel.
  - If parts of the diagram are not visible, click and drag to move the entire diagram right, left, upward, or downward.

The Scope of a Backup

Summary

The Backup Manager does not perform a backup of the entire SAS deployment.

For information about what is and is not backed up, see the "Purpose and Scope" section in "About the Deployment Backup and Recovery Tool" in *SAS Intelligence Platform: System Administration Guide*.

Which Sources Participate?

The **Policy** tab provides Read-only information about participating sources.

- To see a list of sources, select **Configuration**. In the **Sources** section, expand nodes to see the following details:

  Host
  the host name of the machine where the source is located.

Included
indicates whether the source is currently included or excluded from backups.

Note: On the **Backup Manager** page, this setting is Read-only. To include or exclude a backup source, use the command sas-update-backup-config.

Operating system
the host name of the machine where the source is located.

Configurable path
the path to the configuration directory for this source. This field is not applicable to all source types.

SAS config
the path to the `Levn` directory that is associated with this backup source.

Includes and **Excludes**
lists any filters that are associated with this backup source.

- To see a diagram that has a node for each source, click **Source View**. If the associated host machines are not already displayed, click a source to see its associated host machine.
- To see a diagram that has a node for each host machine, click **Machine View**. If the associated sources are not already displayed, click a machine to see the sources that are on the machine.

TIP Backup sources are discovered automatically. To filter physical data or add or remove tiers, servers, or database instances from the backup configuration, use the command sas-update-backup-config.

Get Status and Details

View a List of Operations

On the **History** tab, select an operation type (**Backup Details** or **Recovery Details**).

A list of pending, running, and completed operations of the specified type is displayed. Here are details:

- The **Backup Details** list includes backups that have been purged due to the retention policy.
- You can customize the display by sorting, removing, or freezing columns. See “Tips for Interacting with Tables”.
- You can filter the display by a selected field.

TIP To filter the display by status, select **Status** in the **Filter by** drop-down list. Then enter one of the following filter values: `cancelled`, `not started`, `completed`, `completed with analysis warnings`, `completed with warnings`, `purged`, `failed`, `running`, `fatal`, `unknown`.

For each operation, the following information is displayed:

Status
contains one of the following icons, indicating the status of the backup or recovery operation:

	The backup or recovery has not yet started.
	The backup or recovery is currently running (in progress).
	The backup or recovery completed without errors or warnings.
	The backup or recovery completed with warnings.
	The backup has been purged due to the retention policy.
	The backup or recovery completed with errors.
	The backup or recovery encountered a fatal error.
	The backup or recovery was canceled.
	The status of the backup or recovery cannot be determined.

Backup ID or **Recovery ID**
the unique identifier of the backup or recovery, based on the date and time that the backup or recovery started (for example, 2015-02-01T03_13_01). For backups, the ID is also the name of corresponding backup directory.

Backup Name
for an ad hoc backup, the specified name.

User ID
the user ID of the user that ran the backup or recovery.

Size
for a backup, the total size of the files that were backed up.

Start Time
the date and time that the backup or recovery started running.

Note: The corresponding command is sas-list-backups.

View an Operation's Properties

To view properties for a particular backup or recovery:

1 On the **History** tab, select the operation.

2 Click .

The **Properties** pane provides the same information that is in the main display, with the following additional items:

- any comments that were specified when the backup or recovery was run.

- the end date and time for the backup or recovery.

Note: The corresponding command is sas-display-backup.

View an Operation's Source List

To view a list of the sources for a particular backup or recovery:

1 On the **History** tab, select the operation.

2 In the vertical navigation bar on the right, select ⛁.

The **Sources** pane lists the sources for the currently selected backup or recovery. An icon next to each source indicates the status of its backup or recovery.

By default, the backup sources are as follows:

Metadata Server
the SAS Metadata Server, including all registered metadata repositories, the repository manager, and the server's configuration directory.

Content Server
the SAS Content Server repository.

Config Directories
the contents of the `Data` directories, `SASEnvironment` directories, and server configuration directories for each server on the SAS server tier. (If symbolic links in these directories point to other locations, the referenced locations are not backed up.)

Database
the databases that are managed by the SAS Web Infrastructure Platform Data Server. By default, all of the databases are backed up. You can modify the backup configuration so that only selected databases are backed up.

Note: If you are using a third-party vendor database for the SharedServices database, the Deployment Backup and Recovery Tool cannot back it up.

Note: **Custom** indicates that additional directories under *`SAS-configuration-directoryn`*`/Levn` were backed up or recovered.

Note: For recoveries, only the sources that were recovered are listed.

3 To view details about a source, expand its node in the **Sources** pane.

The following details are displayed:

- the host name of the machine where the source is located
- the status of the source's backup or recovery
- the directory location of the source's local backup files on the host machine
- the total size of the backup files for this source
- the directory location of the source's configuration files

- the operating system of the source's host machine

View an Operation's Source Diagram

To view a diagram of the sources for a particular backup or recovery:

1. On the **History** tab, select the operation.
2. In the vertical navigation bar on the right, select ⛁.
3. At the top of the **Sources** pane, click **View Diagram**.

Here are details:

- The root node specifies the ID of the operation.

  Note: The ID is based on the date and time that the backup or recovery started (for example, 2018-09-01T03_13_01). For backups, the ID is also the name of corresponding backup directory.

- Under the root node, a child node is displayed for each backup source that was included in the backup or recovery.
- Under each source node, a child node is displayed for each host machine for that source.
- An icon on each node indicates the status of the backup or recovery.
- To see the size of the files that were backed up or recovered, place your pointer on a node.

  Note: For recoveries, size information is not available on the root node.

Run an Ad Hoc Backup

1. Sign in to SAS Environment Manager Administration using an appropriate account. See "User Credentials for Performing Backups" in *SAS Intelligence Platform: System Administration Guide*.
2. On the **History** tab, click **Start Backup**.

   Note: If that action is not available, make sure **Backup Details** is selected.

3. In the Start Backup window, enter a unique name, and click **Start Backup**.

   The status of the backup is displayed in the first row.

Note: The corresponding command is sas-backup.

Change the Backup Policy

1 On the **Policy** tab, select **Configuration**.

2 Click .

3 In the Edit Configuration window, make changes as needed. Here are details:

Scheduled allowed
Specifies whether scheduled backups are to run. If you clear this check box, the backup schedule is ignored.

Vault location
If you have a homogeneous operating system environment, use this field to specify the path to a central, network-accessible location to store backups. If a vault location is specified, backups are automatically copied from the various host machines to the vault following each backup operation. A vault is highly recommended to avoid the loss of backup files in the event that a host machine fails.

The path that you specify must meet these requirements:

- The path must already exist.
- All of the host machines that are included in the backup must be able to access the vault location using the specified path.
- You cannot specify a path that is currently used to store a host machine's local backups.
- On Windows machines, specify a UNC path.
- On Windows systems, make sure that the backup user has Read and Write access to the vault location. See "Specifying a Backup User to Access a Central Vault Location or a Clustered Metadata Server (Windows Only)" in *SAS Intelligence Platform: System Administration Guide*.
- On UNIX, make sure the SAS Installer user for each server and middle-tier machine has Read and Write access to the central vault location. After granting permissions on UNIX, you must restart the SAS Deployment Agent.

Note: You can use this field to specify or change a vault location only if you have a homogeneous operating system environment. A homogeneous environment is one in which all of the host machines that are included in the backup are in the same operating system family. For example, Solaris and HP-UX machines are both considered to be in the UNIX operating system family.

Note: In heterogeneous (mixed) operating system environments, you must leave the **Vault Location** blank and use manual steps to specify the central vault. See "Specifying a Central Vault Location in a Heterogeneous Operating System Environment" in *SAS Intelligence Platform: System Administration Guide*.

Days to retain backup
Enter the number of days that backup files are to be retained in the central vault location (if specified) and in the local backup location on each machine. Backups directories and their contents will be deleted automatically after this number of days. If no retention period is specified, backups are retained for 30 days by default.

Email List
Specify one or more recipients for failure notifications. If you do not specify any email addresses, alert messages are sent to the system administrator email address that was specified in the SAS Deployment Wizard.

Here are tips:

- Even if you enter only one address, you must click + next to your entry (and then click **Save**).
- The following special characters are not supported in email addresses: `( ) : \ ; < > [ }`
- To delete an address, click 🗑 next to the address.

Note: The corresponding command (sas-update-backup-config) provides additional options including filtering physical data, adding or removing tiers or database instances, and reorganizing metadata repositories.

Enable Scheduled Backups

1 On the **Policy** tab, select **Configuration**.

2 Make sure the **Scheduled allowed** check box is selected.

Note: If you need to change the setting, click ✎.

3 Make sure the SAS Deployment Agent is running. See "Starting and Stopping the SAS Deployment Agent" in *SAS Intelligence Platform: System Administration Guide*.

Change the Backup Schedule

Here are key points about scheduling backups:

- If you schedule multiple backups per day, be sure to leave enough time for each backup job to complete before the next scheduled backup starts.
- To avoid conflicts, do not schedule the deployment backup at the same time as the stand-alone SAS Metadata Server backups. See "About the SAS Metadata Server Backup and Recovery Facility" in *SAS Intelligence Platform: System Administration Guide*.

1 On the **Schedule** tab, click + to add a row, or click ✎ or 🗑 to edit or delete the selected row.

2 If you are editing a row, make changes in the Edit Schedule window as needed.

   a To specify a different start time, click 🕒.

   b To specify a different recurrence pattern, select or clear check boxes.

   c Click **Save**.

Note: The corresponding commands are sas-set-backup-schedule, sas-list-backup-schedule, and sas-remove-backup-schedule.

View Generated Log Messages

For details about warnings and errors, you can view generated log messages in the following log files:

- The following log file is created on the middle-tier machine:

  ***SAS-configuration-directory*/Lev1/Web/Logs/SASServer1_1/SASDeploymentBackup9.4.log**

  By default, this log reports only errors and warnings. If you want to set different logging levels, you can do so by editing SASDeploymentBackup-log4j.xml, which is located in ***SAS-configuration-directory*/Lev1/Web/Common/LogConfig/**.

- For backup, recovery, and purge operations, log files are created in the directories where local backups are stored. The default location is as follows:

  ***SAS-configuration-directory*/Lev1/Backup/Logs/** *backup-ID*

- The following log file might be useful to obtain information about server-side activity:

  ***SAS-configuration-directory*/Lev1/Backup/backupserver.log**

Use the Command-Line Interface

For information about the command-line interface, see "Using the Deployment Backup and Recovery Tool" in *SAS Intelligence Platform: System Administration Guide*. The referenced documentation provides the following information:

- an overview of tasks for configuring your backup policy and schedule
- instructions and syntax for the command-line backup tools
- how to manually define a central vault location if you have a heterogeneous (mixed) operating system environment
- how to specify a backup user (to access a central vault location or a clustered metadata server in an environment that includes one or more Windows hosts)
- how to configure settings to support host machines that use a forward proxy to communicate with the SAS Web Server
- how to perform a recovery

Related Tasks

To restore content from a backup, use the command-line interface. See "Performing a Recovery Using the Deployment Backup and Recovery Tool" in *SAS Intelligence Platform: System Administration Guide*.

SAS Grid Manager

If your deployment includes SAS Grid Manager, click **Grid Manager** to open that application.

Note: SAS Grid Manager opens in a separate browser window. See *Grid Computing in SAS*.

Reference

Logs

The log and log configuration for this application are in the SAS configuration directory on the middle-tier machine.

Log:	`/Web/Logs/server/SASEnvironmentMgrMidTier2.6.log`
Log configuration:	`/Web/Common/LogConfig/SASEnvironmentMgrMidTier-log4j.xml`

Note: Log configuration files that have an _apm suffix are used by SAS Environment Manager. Do not make changes to those files.

To change the logging level, see "Administer Logging for SAS Web Applications" in *SAS Intelligence Platform: Middle-Tier Administration Guide*.

CAUTION

Excessive logging can degrade performance. Do not use the TRACE and DEBUG logging levels unless you are directed to do so by SAS Technical Support. Remember to revert your logging level after diagnosis is complete, or as directed by SAS Technical Support.

See Also

- "View Generated Log Messages" (logs for backup and recovery)
- "Managing Audit Logs" in *Grid Computing in SAS* (logs for SAS Grid Manager)
- "Adjusting the Logging Configuration" in *SAS Visual Analytics: Administration Guide*
- "Administering Logging for SAS Servers" in *SAS Intelligence Platform: System Administration Guide*
- Information about the Last Action Log in "Administer LASR Tables" in *SAS Visual Analytics: Administration Guide*

Preferences

Introduction

To view or modify your preferences, use the Settings window. To access the Settings window, click the right-most icon in the application banner, and select **Settings**.

This topic documents user preferences that are specific to SAS Environment Manager Administration. For other preferences, see "Settings" in *SAS 9.4 Web Applications: General Usage Help*.

Preferences: Application Server

The value in the **Application server** drop-down list specifies how a SAS Application Server is selected for requests on the **LASR** page.

(auto-select)
causes an appropriate server to be automatically selected for each request. See Which Server is Used? in *SAS Visual Analytics: Administration Guide*.

server-name
forces use of a specified SAS Application Server (for example, **SASApp**). Only servers that are registered with the job execution service are listed.

Preferences: Clear Credentials Cache

To remove cached credentials from the current session:

1. In the Settings window, select **SAS Environment Manager Administration** ⇨ **Clear Credentials Cache**.
2. In the right pane, click **Clear**.
3. In the confirmation window, click **Yes**.

Preferences: Manage Environment

Resource monitor sample rate
Specifies, in milliseconds, the sampling rate that the resource monitor uses for polling the machines in the cluster. This setting is neither applicable to nor displayed for a non-distributed server.

Process monitor sample rate
Specifies, in milliseconds, the sampling rate that the performance monitor uses for polling application instances. This setting is neither applicable to nor displayed for a non-distributed server.

Show the processes that measure performance

Controls whether processes that measure performance are included in the process-monitoring graphs. To include performance measurement processes in the graphs, select the check box. If several instances of performance measurement processes are running, they can negatively impact performance. This setting is not applicable to a non-distributed server.

Record actions as SAS statements

Saves the SAS code that is generated when you perform certain tasks in SAS Environment Manager Administration. You can save all recorded code in a single file or you can save the recorded code for each task in its own file.

Note: The **File** field is required to save all recorded code in a single file. Provide the fully qualified path and name of a file that already exists on your default workspace server. Your default workspace server is the SAS Workspace Server that is part of your selected SAS Application Server. You must have Read and Write access to the specified file. The Settings window does not validate the file that you specify.

Note: The **Path** field is required to save the recorded code for each task in its own file. Specify a location that already exists on your default workspace server. Your default workspace server is the SAS Workspace Server that is part of your selected SAS Application Server. You must have Read and Write access to the specified location. The Settings window does not validate the path that you specify.

If you enable recording, the following actions are recorded:

- Start or stop a LASR server.
- Load, reload, or unload a table.
- Add a table to co-located HDFS (**Add to HDFS**) or NFS-mounted MapR (**Add to Data Server**).
- Delete a physical table from co-located HDFS or NFS-mounted MapR.

Note: You can modify and schedule recorded statements. However, metadata server connection information is not recorded. See Connection Options in *SAS Language Interfaces to Metadata*.

Advanced Tab

An object's **Advanced** tab lists any keywords, responsibilities, or extended attributes that have been specified for the object. For most objects, the **Advanced** tab is empty. Add or modify information only if your product's documentation indicates to do so.

To make changes:

1. On the object's **Advanced** tab, select a view from the drop-down list.
2. Click ✎.
3. Make changes as follows:
   - To add a row, click +.
   - To add or modify a value, click in a cell.

- To delete rows, select their check boxes and then click 🗑.

4 Click **Save**.

See Also

- "LASR Server: Extended Attributes" in *SAS Visual Analytics: Administration Guide*
- "Library-Level Attributes for Autoload" in *SAS Visual Analytics: Administration Guide*
- "Library-Level Attributes for Reload-on-Start" in *SAS Visual Analytics: Administration Guide*
- "Table-Level Attributes for Reload-on-Start" in *SAS Visual Analytics: Administration Guide*
- VA.Encryption.Enabled extended attribute (for a SASHDAT library)

Server Categories

The filter in the navigation pane on the **Servers** page enables you to limit the display to only those server types in a selected category.

Here are examples of servers in each category:

Table 1 *Servers in Each Category*

Category	Examples of Included Servers
Cloud servers	Hadoop
Content servers	Esri server, FTP server, HTTP server
Database servers	ODBC, Oracle, Teradata
Enterprise application servers	SAP server
Monitoring servers	Grid monitoring server (for SAS Grid Manager)
Proxy list	Proxy list server
SAS Application Servers	SAS Metadata Server, SAS Workspace Server, SAS Stored Process Server
SAS servers	SAS LASR Analytic Server, SAS Message Queue Polling Server, SAS/SHARE server
SAS spawners	SAS/CONNECT spawner, SAS object spawner
Scheduling servers	Operating system scheduling server, Platform Process Manager server

Note: Not all deployments include all types of servers. The filter offers only those categories that are applicable to your deployment.

See Also

"Servers Page"

Roles and Capabilities

Introduction

This topic documents capability-based access to features in SAS Environment Manager Administration. SAS Environment Manager Administration does not have its own roles and capabilities. Instead, it adopts capabilities from related components and precursor applications.

Note: The exception is the capability **Environment Mgr Mid-Tier: Manage Fonts** and its associated predefined role, **Fonts Administrator**. For information about the affected functionality, see "Make More Fonts Available" in *SAS Intelligence Platform: Middle-Tier Administration Guide*.

Note: Not all pages and features are present in all deployments. See the per-page documentation for details.

Capabilities

The following pages and features within SAS Environment Manager Administration are under capability-based management:

Page	Feature	Required Capability
Folders		Management Console: Plug-ins: Folder View
	View report	Visual Analytics: View Report and Stored process
	Add to HDFS	Visual Analytics: Advanced: Manage Environment
	Add to data server	Visual Analytics: Advanced: Manage Environment
Libraries		Management Console: Plug-ins: Data Library Manager
Servers		Management Console: Plug-ins: Server Manager

Page	Feature	Required Capability
Users		Management Console: Plug-ins: User Manager
	New (user, group, or role)	Implicit[1]
	Delete (user, group, or role)	Implicit[1]
	Edit a user, group, or role	Implicit[1]
Mobile Devices		Visual Analytics: Advanced: Manage Mobile Devices[2]
LASR		Visual Analytics: Advanced: Manage Environment
	LASR Servers tab	Visual Analytics Admin: Manage LASR Analytic Server
	LASR Tables tab	Visual Analytics Admin: Manage LASR Analytic Server
	Monitor Resources tab	Visual Analytics Admin: Monitor LASR Analytic Server
	Monitor Processes tab	Visual Analytics Admin: Monitor LASR Analytic Server
Tools		Visual Analytics: Advanced: Manage Environment
	HDFS tab	Visual Analytics Admin: Browse HDFS
	Alerts tab	There is no tab-level capability for the **Alerts** tab.
Backup Manager		See "About the Backup Manager Page".
Grid Manager	Launch point (icon)	See "SAS Grid Manager".

1 Requires implicit capabilities that are provided by the Metadata Server: User Administration role. For details and exceptions, see "Who Can Manage Users, Groups, and Roles?" in *SAS Intelligence Platform: Security Administration Guide*.

2 In a SAS Enterprise BI deployment that does not include SAS Visual Analytics, access to the **Mobile Devices** page is not under capability-based management.

Each page-level capability is a prerequisite for access to any capability-based features within a page. For example, to access the **HDFS** tab, a user must have both of the following capabilities:

- The Visual Analytics: Advanced: Manage Environment capability, which provides access to the **Tools** page.
- The Visual Analytics Admin: Browse HDFS capability, which provides access to the **HDFS** tab.

Note: To access SAS Environment Manager Administration from the applications menu, the Visual Analytics: Advanced: Manage Environment capability is required. That requirement does not apply to other access methods. See "Integrated Access".

Initial Capabilities

Note: This section documents capability-based availability of pages within SAS Environment Manager Administration. For information about who can launch this application, see "Who Can Launch SAS Environment Manager Administration?"

In a new deployment of SAS Visual Analytics, the capability-based availability of pages is as follows:

User or Group	Member Of (Role)	Pages
Guest	Visual Analytics: Basic	None.[1]
Unrestricted user	Metadata Server: Unrestricted	All.
SAS Administrators	Management Console: Advanced Metadata Server: User Administration	All, except for **LASR**, **Tools**, and **Mobile Devices**.
Visual Analytics Data Administrators	Visual Analytics: Administration	**LASR**, **Tools**, and **Mobile Devices**.
SASUSERS	Management Console: Content Management	**Folders**, **Libraries**, and **Users**.[2]

1 This is a configuration-based constraint, not a capabilities-based constraint. Do not enable guest access to SAS Environment Manager Administration.

2 See "Who Can Manage Users, Groups, and Roles?" in *SAS Intelligence Platform: Security Administration Guide*.

Here are additional details:

- The preceding table is not a comprehensive summary of functionality that is available to each listed identity. The emphasis is on information that is relevant to capability-based management in SAS Environment Manager Administration.
- If you need to expand or reduce the availability of the listed features, adjust memberships or capabilities.
- Membership in the group SAS Environment Manager Super Users does not provide access to SAS Environment Manager Administration. See "Introduction".

See Also

- "Access Issues"
- "Streamlining Access to Management Pages" in *SAS Visual Analytics: Administration Guide*
- "Revoke Access to Management Pages"
- "Roles and Capabilities" in *SAS Visual Analytics: Administration Guide*

Tips for Interacting with Tables

Here are tips for customizing the way that SAS Environment Manager Administration displays information in tables:

- To sort a table, right-click on a column heading and select **Sort**. You can sort the table by the contents of the column or add the column as a secondary sort criteria.
- To reorder the columns in a table, click on the column heading and drag the header to the new location.
- To prevent a column from being reordered, right-click on the column heading and select **Freeze**. The column is moved to the left of the table and cannot be reordered. To enable the column to be moved, right-click on the header and select **Unfreeze**.
- To select which columns are displayed, click , and select **Manage columns** from the pop-up menu. The Columns window displays a list of hidden columns and displayed columns. Select the columns that you want to display and click **OK**.
- To reduce the number of items displayed in the table, use the **Filter** field. As you enter text in the field, the table changes to display only the items that contain text that matches the text that you enter. The table is filtered dynamically as you enter text. The text that you enter as filter text is not case sensitive.

Note: Not all of the tables in SAS Environment Manager Administration offer all of the preceding features.

Options for Servers and Libraries

For details about working with metadata definitions for servers and libraries, see the following documents:

LASR server	"LASR Server Definition" in *SAS Visual Analytics: Administration Guide*
Data servers	*SAS Intelligence Platform: Data Administration Guide*
Compute servers	*SAS Intelligence Platform: Application Server Administration Guide*
LASR library	"LASR Library Definition" in *SAS Visual Analytics: Administration Guide*
Other libraries	*SAS Intelligence Platform: Data Administration Guide*

Authorization

For concepts and background information, see "Access Management" in *SAS Intelligence Platform: Security Administration Guide*.

Permissions

The following table documents general purpose permissions and permissions that have a special purpose in SAS Visual Analytics.

Permission	Affected Actions
Administer (A)	On a LASR library, load and import tables. On a LASR server, stop the server or set a tables limit.
Read (R)	On a LASR table, read data. On a LASR library, load and import tables. On an encrypted SASHDAT library, add, delete, or load data.
Write (W)	On a LASR table, unload and reload the table; append and delete rows; and edit computed columns.
ReadMetadata (RM)	View an object. For example, to see a report, table, or library, you need the ReadMetadata permission for that object.
WriteMetadata (WM)	Edit, rename, set permissions for, or delete an object. Create certain associations among objects.
WriteMemberMetadata (WMM)	On a folder, add or remove objects.
ManageMemberMetadata (MMM)	On a group or role, enables a non-administrator to modify membership. (Provides Edit access to the **Members** tab.)[1]
ManageCredentialsMetadata (MCM)	On a group, enables a non-administrator to manage shared logins. (Provides Edit access to the **Accounts** tab.)[1]

1 The **Users** page in SAS Environment Manager Administration does not offer delegated administration. If you need that feature, use SAS Management Console.

For SAS Visual Analytics task requirements, see "Permissions" in *SAS Visual Analytics: Administration Guide*.

For other permissions and contexts, see "Use and Enforcement of Each Permission" in *SAS Intelligence Platform: Security Administration Guide*.

For user administration task requirements, see "Who Can Manage Users, Groups, and Roles?" in *SAS Intelligence Platform: Security Administration Guide*.

Examine Access

Authorization Tab

Here are key points about the **Authorization** tab:

- Each object's **Authorization** tab is displayed as part of its metadata definition.
- Each object's **Authorization** tab describes access to that object. The displayed effective permissions are a calculation of the net effect of all applicable metadata-layer permission settings. Effective access does not encompass role-based constraints or constraints from other authorization layers.
- You can immediately see the impact of your access control changes across identities. For example, the impact that an explicit denial for PUBLIC has on all restricted identities that do not have offsetting direct controls is immediately apparent.
- Only permissions that are potentially applicable for an object (or its child objects) are displayed for that object.
- Only identities that participate in access controls that potentially affect the current object are displayed.
- You cannot remove identities that participate in access controls on parent objects, applied ACTs, or the repository ACT. You can remove all explicit access controls for any selected identity.

View Effective Access to an Object

Effective (net) access to an object is displayed on the object's **Authorization** tab as follows:

- The effective access icons indicate a grant ✓, a row-level grant ◐, or a denial ⊘.
- The explicit indicator icon ◆ indicates an access control that is directly set on the current object and specifically assigned to the selected identity.
- The ACT indicator icon □ indicates an access control that comes from a directly applied ACT whose pattern specifically assigns the grant or denial to the selected identity.
- The absence of an indicator icon means that a setting is indirect. The setting comes from someone else (a group that has a direct control), somewhere else (a parent object or the repository ACT), or special status (such as unrestricted). For the WriteMemberMetadata permission, indirect means that the setting mirrors the WriteMetadata setting.

In combination, icons provide information as follows:

Icon	Meaning
✓ ◆	Grant from an explicit control
✓ □	Grant from a directly applied ACT

Icon	Meaning
✓	Grant from an indirect source (such as a parent group or parent object)
◐ ◆	Row-level grant from an explicit control
◐	Row-level grant from an indirect source (a parent group)
⊘ ◆	Denial from an explicit control
⊘ □	Denial from a directly applied ACT
⊘	Denial from an indirect source (such as a parent group or parent object)

Note: The explicit and ACT indicator icons correspond to the white and green colors on the **Authorization** tab in SAS Management Console. As in SAS Management Console, if both an explicit control and an applied ACT setting are present, only the explicit indicator is displayed.

View Direct Access Controls for an Object

An object's Authorization Summary window lists any direct controls that are set on the object. A direct control can be explicit (set individually on the object) or ACT (from the pattern of an applied access control template). You can rearrange the list to group settings by identity, permission, or type (explicit versus ACT).

The summary does not show effective access or settings that are inherited from parent objects. The summary simply indicates which access controls, if any, are directly set on the current object. The summary is always read-only.

To open an object's Authorization Summary window, click on the object's **Authorization** tab.

Look Up an Access Information for an Identity

The permissions inspector enables you to look up effective permissions for any user or group. To launch the inspector, click on the **Authorization** tab.

The inspector offers the following features:

- The inspector shows the effective permissions that a selected identity has for the current object. Effective access information is displayed after you specify an identity.
- The inspector shows origins information for each effective access setting. (Click an effective access icon, and select **Show origins**.)
- The inspector uses the same icons and indicators that are used on the **Authorization** tab.

Here are some tips for using the inspector:

- The inspector is always read-only.
- The inspector does not reflect unsaved changes.

- The inspector cannot be launched from the Edit Authorization window.
- To select an identity, enter search criteria in the text box and then select a user or group. The search is against the display name, name, and description fields in user and group definitions. The search uses the "contains" criteria, so you can provide any part of the name.
- Row-level grants are indicated in the inspector, but you cannot view the associated permission conditions from the inspector. Use the **Authorization** tab to view or update a row-level permission.

Find the Source of an Effective Access Result

Overview

Permission origins identify the source of each effective permission in the metadata authorization layer. This information can be useful in troubleshooting. It answers the question: Why is this identity granted (or denied) this permission?

In the origins answer, only the controlling (winning, highest precedence) access control is shown. If there are multiple tied winning controls, they are all shown. Other, lower precedence controls are not shown in the answer.

Origins information is available on an object's **Authorization** tab. To identify the source of an effective access result, double-click on its cell, and select **Show origins**.

The following sections provide examples that use a condensed form of origins information (which differs slightly from the presentation that the software provides).

Simple Permissions Origins

The following table provides simple examples of permission origins answers. In each example, we are interested in why UserA has an effective grant on FolderA. In each example, UserA is a direct member of both GroupA and GroupB. Each row in the table is for a different (independent) permissions scenario. In the table, the first column depicts the contents of the Origins window. The second column interprets the information.

Table 2 *Origins: Simple Examples*

Origins Information	Source of UserA's Effective Grant on FolderA
UserA [Explicit]	On FolderA, an explicit grant for UserA
GroupA [Explicit]	On FolderA, an explicit grant for GroupA
GroupA [Explicit]	On FolderA, explicit grants for GroupA and GroupB
GroupA [ACT: GroupARead]	On FolderA, an ACT pattern grant for GroupA (from a directly applied ACT)
SASUSERS [ACT: GenRead]	On FolderA, an ACT pattern grant for SASUSERS (from a directly applied ACT)
GroupA [ACT: GroupARead]	On FolderA, ACT pattern grants for GroupA and GroupB (from two different directly applied ACTs)

Origins Information	Source of UserA's Effective Grant on FolderA
GroupB [ACT: GroupBRead]	**Note:** Two settings are shown because they are tied and they both win (UserA is a direct member of GroupA and GroupB).
GroupA [ACT: GroupABRead] GroupB [ACT: GroupABRead]	On FolderA, ACT pattern grants for GroupA and GroupB (from the same directly applied ACT) **Note:** Two settings are shown because they are tied and they both win (UserA is a direct member of GroupA and GroupB).
UserA is unrestricted.	UserA's status as an unrestricted user (someone who is unrestricted is always granted all permissions)

Inherited Permissions Origins

In many cases, the controlling setting is not on the current object. Instead, the controlling setting is defined on a parent object and inherited by the current object.

The following table provides examples in which the controlling setting comes from a parent object. Because the source of the effective permission is a parent object, the answer must identify which parent object has the controlling setting. For this reason, the answers in the following examples identify both a parent object (the object that has the controlling setting) and the controlling setting, itself.

In each example, we are interested in why UserA has an effective grant on FolderA. In each example, UserA is a direct member of both GroupA and GroupB. Each row in the table is for a different (independent) permissions scenario. In the table, the first column depicts the contents of the Origins window. The second column interprets the information.

Table 3 *Origins: Inheritance Examples*

Origins Information	Source of UserA's Effective Grant on FolderA
ParentFolderA UserA [Explicit]	On ParentFolderA, an explicit grant for UserA
ParentFolderA GroupA [Explicit]	On ParentFolderA, an explicit grant for GroupA
ParentFolderA GroupA [Explicit] GroupB [Explicit]	On ParentFolderA, explicit grants for GroupA and GroupB
ParentFolderA GroupA [ACT: GroupARead]	On ParentFolderA, an ACT pattern grant for GroupA (from a directly applied ACT)
GreatGrandParentFolderA	On GreatGrandParentFolderA, an ACT pattern grant for SASUSERS (from a directly applied ACT)

Origins Information	Source of UserA's Effective Grant on FolderA
SASUSERS [ACT: GenRead]	
ParentFolderA GroupA [ACT: GroupARead] GroupB [ACT: GroupBRead]	On ParentFolderA, ACT pattern grants for GroupA and GroupB (from two different directly applied ACTs)
GrandParentFolderA GroupA [ACT: GroupABRead] GroupB [ACT: GroupABRead]	On GrandParentFolderA, ACT pattern grants for GroupA and GroupB (from the same directly applied ACT)

For more information, see "Object Inheritance" in *SAS Intelligence Platform: Security Administration Guide*.

Manage Access

Set an Explicit Grant or Denial

1 On the object's **Authorization** tab, click ✎.

Note: If that icon is not present, you are not authorized to set permissions for the current object.

2 In the **Effective Permissions** table, locate the identity to which you want to assign an explicit control. If the identity is not listed, click + to open the Add Identities window.

Note: In the Add Identities window, only user administrators can successfully search by user ID. Regular users cannot see other users' IDs.

Note: An explicit grant of the ReadMetadata permission is automatically set for each identity that you add.

3 In the **Effective Permissions** table, double-click on a cell. From the cell's drop-down list, select either **Deny** or **Grant**.

Note: When the drop-down list collapses, notice that the cell contains an explicit control indicator ◆

Note: If the selected identity is an unrestricted user, all permissions are granted and you cannot make changes.

4 If you changed a group's access, review the impact on the other listed identities. Controls that you add for a group can affect access for all members of that group.

5 Click **Save**.

Set a Row-Level Permission

To set a row-level permission for a LASR table, see "Row-Level Security" in *SAS Visual Analytics: Administration Guide*.

To set other types of fine-grained permissions, use SAS Management Console. For example, to set a row-level permission for a metadata-bound table, see "Providing Fine-Grained Access Using Condition Permissions" in *SAS Guide to Metadata-Bound Libraries*.

Apply an Access Control Template

Use ACTs to avoid having to repeatedly set the same explicit permissions for the same identities on multiple objects. When you apply an ACT to an object, the ACT settings are added to the object's protections.

An object's **Direct ACTs** tab indicates whether any ACTs are directly applied to the object, and enables you to apply or remove ACTs.

To directly apply an ACT to an object:

1 (Optional) Review the settings that the ACT provides, to make sure they are as expected.

   a On the **Folders** tab, locate and select the ACT.

   b In the content pane, on the **ACT Pattern** tab, examine the settings that the ACT provides.

2 Locate and select the object to which you want to apply an ACT.

3 On the object's **Direct ACTs** tab, click ✎.

   Note: If that icon is not present, you are not authorized to set permissions for the current object.

4 In the Apply and Remove ACTs window, select the check box for the ACT that you want to apply.

   Note: Do not apply the repository ACT (which is usually named Default ACT) directly to any object. The repository ACT participates through inheritance, serving as an access control parent of last resort.

5 Click **Save**. On the **Direct ACTs** tab, the ACT that you applied is listed.

6 On the **Authorization** tab, review the effects of your changes. The applied ACT contributes its pattern of settings to the object's protections. The object might also have explicit controls, other applied ACTs, and inherited settings.

Examine the Settings that an ACT Provides

Here are key points:

- Do not confuse an ACT's **Pattern** tab with its **Authorization** tab. The two tabs look similar but have very different purposes and effects.
- The display is sparsely populated. A pattern consists of only the specific settings that the ACT provides. The display does not reflect the effective access that the ACT provides.
- The display includes only participating identities. If you want to calculate the effect of an ACT on an unlisted identity, review the identity precedence principles. See "Precedence Principles and Examples" in *SAS Intelligence Platform: Security Administration Guide*.
- The display uses the same grant ✓ and denial ⊘ icons that are used on the **Authorization** tab. An ACT cannot provide row-level permissions.

> **TIP** For an alternate, read-only display of an ACT's pattern, click 🔓 on the ACT's **Pattern** tab. You can organize the **Pattern Summary** display by identity or permission.

See Also

- "Tips for Efficiently Using Permissions" in *SAS Intelligence Platform: Security Administration Guide*
- "About Access Management" in *SAS Intelligence Platform: Security Administration Guide*
- "Types of Access Controls" in *SAS Intelligence Platform: Security Administration Guide*

Advanced: Manage ACTs

Locate an ACT

In the foundation repository, ACTs are stored in the following metadata folder: **SAS Folders** ⇨ **System** ⇨ **Security** ⇨ **Access Control Templates**.

In custom repositories, the navigation path includes a repository (for example, **SAS Folders** ⇨ ***repositoryA*** ⇨ **System** ⇨ **Security** ⇨ **Access Control Templates**).

Create an ACT

1. On the **Folders** page, navigate to **SAS Folders** ⇨ **System** ⇨ **Security** ⇨ **Access Control Templates**.
2. Right-click **Access Control Templates**, and select **New access control template**.
3. In the New Access Control Template window:
   a. Specify a name.
   b. Click **Save**.
      The new ACT is saved to the Foundation repository and displayed.
4. On the **ACT Pattern** tab, add the settings that the ACT provides to every object to which it is applied. See "Define an ACT's Pattern".

5 On the ACT's **Authorization** tab, add settings to protect the ACT. For example, one approach is to add an explicit denial of WriteMetadata for PUBLIC and an offsetting explicit grant of WriteMetadata for SAS Administrators.

> **IMPORTANT** Prevent regular users from modifying or removing an ACT.

6 To use the ACT, apply it to one or more objects.

Protect an ACT

> **IMPORTANT** Prevent regular users from modifying or removing an ACT.

To protect an ACT, make changes on its **Authorization** tab. For example, one approach is to add an explicit denial of WriteMetadata for PUBLIC and an offsetting explicit grant of WriteMetadata for SAS Administrators.

Delete an ACT

CAUTION
One ACT can protect thousands of objects. Deleting an ACT affects every object to which that ACT is applied. Review the current usage of an ACT before you delete it.

You cannot delete an ACT using this application. You can use SAS Management Console to perform that task.

Define an ACT's Pattern

CAUTION
One ACT can protect thousands of objects. Changes that you make to an ACT's pattern affect every object to which that ACT is applied. Before you change an ACT's pattern, review its current usage and make sure you understand the settings that it currently provides.

To define the settings that an ACT provides:

1 If the ACT is not already open, locate and open it.

2 On the **ACT Pattern** tab, click ✎.

3 In the **Edit Pattern** window, make changes as needed.

- You can add (+) and remove (🗑) identities.
- You can add, remove, or change a pattern setting by clicking in the appropriate cell.

Click **Save**.

Examine Usage of an ACT

In each ACT's definition, the **ACT Usage** tab lists the objects to which that ACT is directly applied. This centralized view can help you identify any gaps in your access control implementation, and anticipate the impact of any changes that you make to the ACT.

The list of objects on the **ACT Usage** tab is always read-only. To apply or remove an ACT for a particular object, use that object's **Direct ACTs** tab.

Each **ACT Usage** tab also indicates whether the ACT serves as a repository ACT. Each repository has a designated repository ACT. By default, every repository ACT is named **Default ACT**.

Designate the Repository ACT

If you are an unrestricted user, you can click ✎ on any ACT's **ACT Usage** tab to designate that ACT as the repository ACT for the repository in which it exists. Clicking ✎ on the **ACT Usage** tab of the currently designated repository ACT enables you to remove that designation.

CAUTION

Selecting or clearing the check box that designates whether an ACT is the repository ACT can significantly disrupt access. Before you change the **Use this ACT as the repository ACT** setting, make sure you understand the implications. The settings that are defined on a repository ACT's **ACT Pattern** tab provide the highest point of control for that repository. Users must have ReadMetadata and WriteMetadata access at the repository level. Broadly denying access at that level is not a workable approach.

Troubleshooting

Access Issues

Issue: A particular user cannot sign in.

Resolution:

- If the error message is `Public access denied`, make sure that the user has a well-formed definition in metadata. In a user's metadata definition, this problem can be caused by a user ID that is not in a qualified format. This problem is not caused by passwords or authentication domain assignments. See "Add a User".
- If the user attempts access using a direct URL, but is redirected to SAS Home, make sure the user is authorized to access SAS Environment Manager Administration.

Issue: Nobody can sign in.

Resolution:

- Make sure that the metadata server and the middle tier are running. See "Operating Your Servers" in *SAS Intelligence Platform: System Administration Guide*.

Issue: A particular user cannot access certain features in SAS Environment Manager Administration.

Resolution:

- Make sure that the user has the required capabilities.
- Make sure that the user has the required permissions. For example, if you do not have the WriteMetadata permission for an object, the **Edit** icon is not present on any of that object's tabs.
- Make sure that the user is not connecting as a guest. See "Configure Guest Access" in *SAS Intelligence Platform: Middle-Tier Administration Guide*.
- Make sure the user is in the intended application. Click the right-most icon in the banner, and select **About**. In the About window, make sure the product name is SAS Environment Manager Administration.

  Note: The administrative tool for the SAS Viya platform is entirely separate, but it has a similar name, SAS Environment Manager.

Issue: Nobody can access certain features in SAS Environment Manager Administration.

Resolution:

- Make sure that the features should be present in your deployment. Here are examples:
  - The **LASR** and **Tools** pages are present if SAS Visual Analytics is deployed.
  - Within the **LASR** page, the **Monitor** tabs are present if a distributed LASR server is deployed.
  - Within the **Tools** page, the **HDFS** tab is present if co-located HDFS is deployed.

- Make sure the specific functionality is supported. For example, nobody can use this application to edit values on the **Options** tab for a server other than the LASR server.

Issue: After providing DBMS credentials interactively, you cannot access an associated data source.

Resolution:

If you think you might have inadvertently entered invalid credentials, clear your credentials cache. See “Preferences: Clear Credentials Cache”.

Note: Clearing the cache removes your cached credentials from the current session. The next time you attempt to access the data source, you are prompted for credentials.

LASR Issues

See Load, Reload, and Import Issues and Server Operation Issues in *SAS Visual Analytics: Administration Guide*.

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. Copyright © 2019, SAS Institute Inc., Cary, NC, USA. All Rights Reserved. January 2023 2.6-P1:evadmfun

THE POWER TO KNOW.