CHAPTER 2

Using Access Control

Overview of Access Control Tasks

You can perform some or all of the following tasks to set up and maintain user and group access to SAS/EIS data sets and applications. Many of the task descriptions suggest that you perform certain steps or verify that certain conditions exist before you start the actual task. Be sure to follow these suggestions before beginning a task to ensure successful completion.

The tasks associated with access control are grouped into the following categories and are located on the indicated pages:

Each of the following sections describes the tasks associated with a particular category.

Establishing the Access Control Environment

Preliminary Requirements

You activate access control for EIS applications by completing the following steps:

- Make sure that you have write access to the SASHELP.AC and SASHELP.MB catalogs.
- Select an access control key, which is a password used to protect and encrypt your access control files and to protect access to the Access Control Setup window.
- Select a location for your access control files.
  - Your access control files contain information about users and groups and hold the access control lists that define access to data, applications, and functions for each group of users.
  - The access control files should be stored in a location that is available to all users of your applications at all times. Users who do not have access to the access control files will not be allowed to start any EIS application.
  - You can store your access control files on any network location that can be locally mapped from your users' workstations–for example, a directory on a Novell network drive for PC users or an NFS-mounted volume for UNIX users. You can also choose any location that is accessible through a SAS/CONNECT server or a SAS/SHARE server that supports Remote Library Services (RLS).

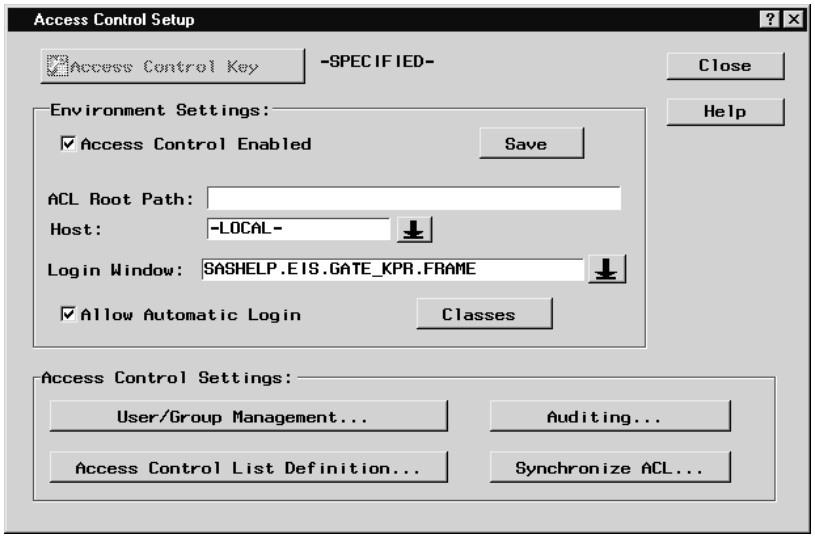
Initializing the Environment

The following steps describe how to set up the access control environment in your SAS/EIS session:

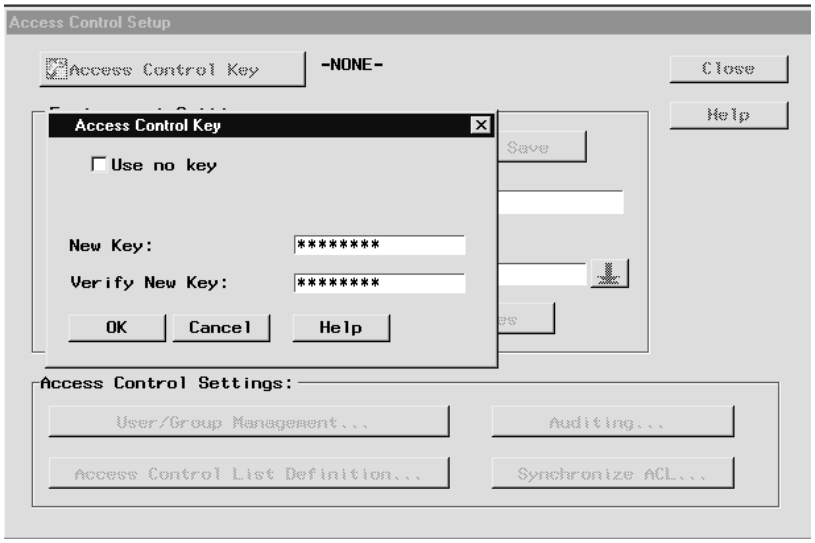
1 Invoke SAS/EIS software by selecting from the menu bar in a SAS window

Solutions ▶ EIS/OLAP Application Builder

2 Open the Access Control Setup window by selecting **Setup** from the EIS Main Menu and **Access Control** from the Setup window's Multidimensional Applications group.



3 In the Access Control Setup window, select Access Control Key. When the Access Control Key window appears, type the default access control key, **SASADMIN**, in the New Key field and in the Verify New Key field. Select OK.



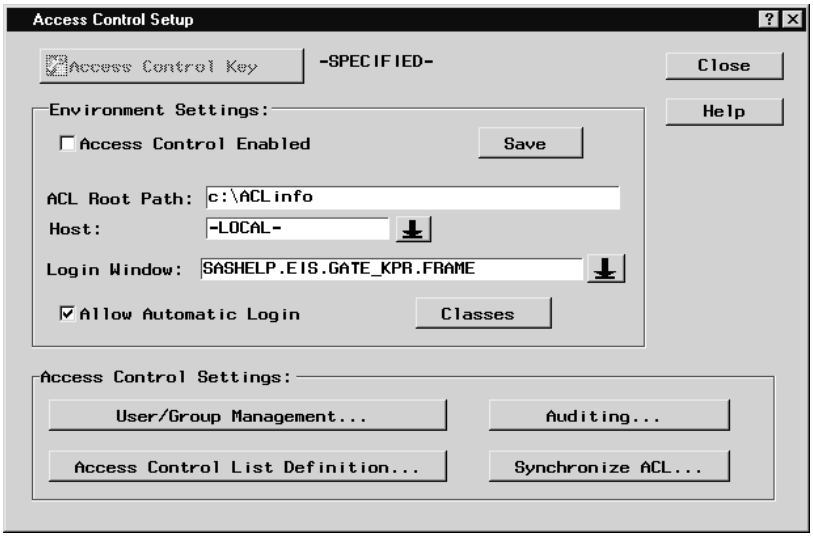
You can choose not to use any key on your access control files by selecting **Use no key** in the Access Control Key window.

Note: The access control key is stored in the SASHELP.MB catalog. Make sure that this catalog or a copy of this catalog is used for all applications that use SAS/EIS access control. △

4 Now, exit your SAS/EIS session so that the appropriate catalogs can be updated with this information.

5 Start SAS/EIS software again. Open the Access Control Setup window by selecting **Setup** from the EIS Main Menu and **Access Control** from the Setup window's Multidimensional Applications group. When prompted by the Access Control Key window, type the access control key that you selected previously and select OK.

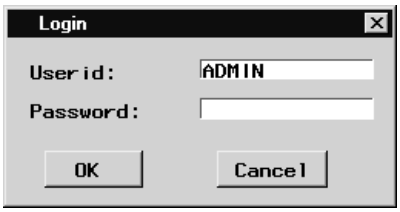
6 In the Access Control Setup window, the **Environment Settings** region is now active. Type the path and, optionally, the name of a server in the ACL Root Path and the Host fields, and press the Enter key.



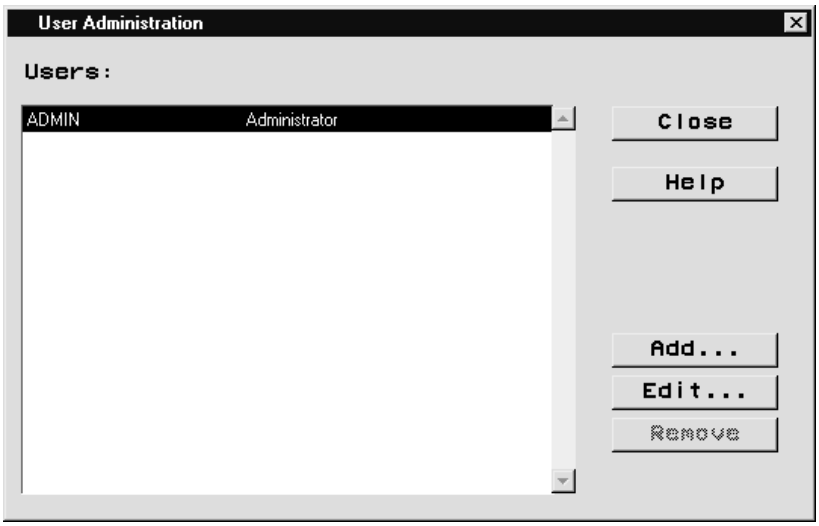
7 Select the **Access Control Enabled** check box.

8 Select Save. The system verifies that the ACL Root Path and Host values are valid and creates the access control files in the directory that you specified. The userid, ADMIN, is created automatically, with ADMIN as the initial password.

9 Now, exit your SAS/EIS session and all active SAS/EIS applications. The next time that you start a SAS/EIS session, you will be prompted to specify a valid userid and password in the Login window. In the Userid field, type **ADMIN**; in the Password field, type **ADMIN**.



10 Open the Access Control Setup window, and select User/Group Management and then User Management to open the User Administration window.



11 Notice that **ADMIN** is the only user at this point and that it is pre-selected. Select Edit, and type a password. Select OK and Close to return to the Access Control Setup window. The next time you log on, use the new password.

Note: The access control setup information is physically stored in the SASHELP.AC catalog. For all applications that use SAS/EIS access control, make sure that this catalog, or a copy of it, is being used. △

Setting Up Users And Groups

Access control definitions always define access to data, applications, or functions for groups of users. In other words, an access control group is a collection of users with identical access rights.

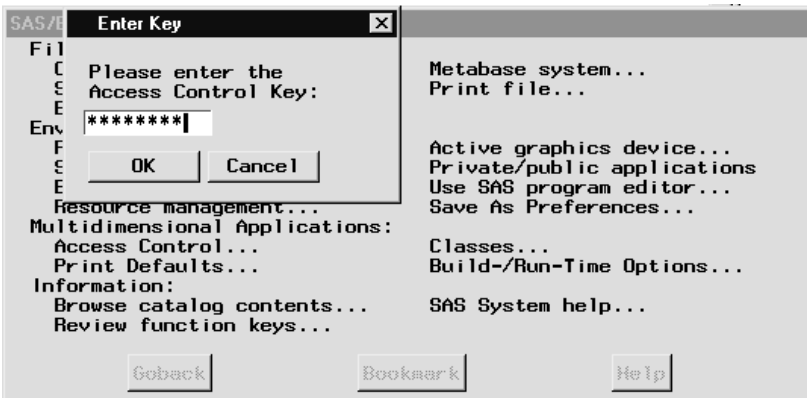
Before you begin

1 Compile a list of the users of your application. You might use IDs from software access control systems or security systems that already exist in your organization. Also, determine the groups of users with different access rights.

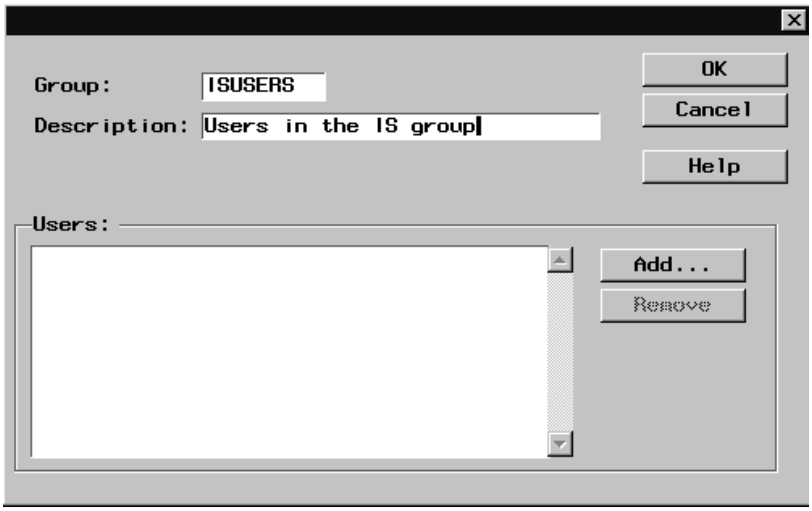
2 Activate access control.

Then, follow these steps:

1 Open the Access Control Setup window by selecting **Setup** from the EIS Main Menu and **Access Control** from the Setup window's Multidimensional Applications group. In the Enter Key window, type the access control key and select OK.



2 Select **User/Group Management** and **Group Management** to open the Group Administration window. Note that the **SYSTEM** and **USERS** groups have been created for you already. To create additional groups, select Add to open the Group Administration (2) window, type in the name and description of a group, and select OK to return to the User Administration window. The name of the group you added appears in the list.



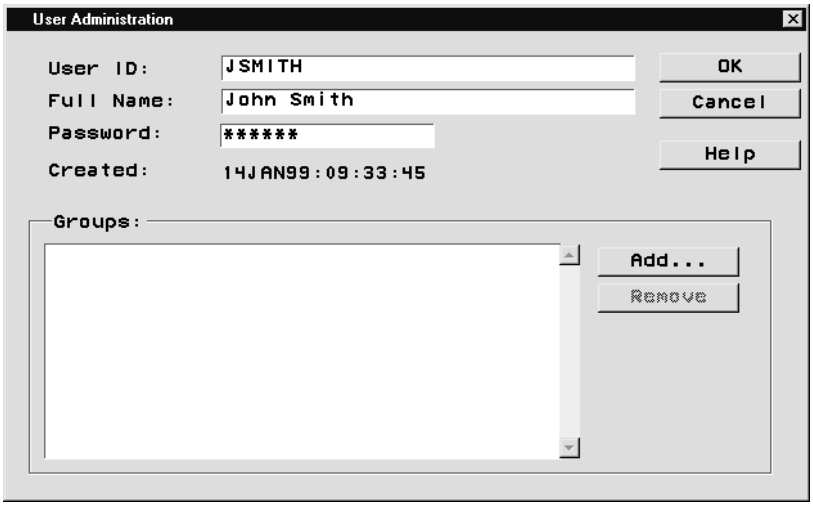
Note: You do not need to add users to your groups now. You can assign a group to a user as you define the user's ID. △

3 After you have defined the groups that you need, close the Group Administration window.

Note: You can now define IDs for the users of your application or you can do this at a later time. △

4 To define user IDs, select **User/Group Management** and then **User Management** to open the User Administration window, which displays a list of users. To add a user, select Add to open the User Administration (2) window. Next, type an ID and a password, and select one or more groups for the user. Optionally, you can add a full name for the user. Follow these steps for each user you add. When you have completed all additions, select OK and Close to return to the Access Control Setup window.

Note: For additional information, see "Assigning Multiple Groups to a User" on page 19. △



You have now defined your initial User/Group structure. You can repeat these steps at any time to change descriptions, to add or remove users or groups, to change group assignments, or to reset passwords.

Controlling Access to Data

Controlling Access to Your Applications' Data

You can define data access restrictions for groups of users on each existing metabase registration. For each combination of group and registration, you can do the following:

- deny access to the entire table
- drop or keep hierarchies
- drop or keep ANALYSIS/COMPUTED columns
- hide ANALYSIS columns
- drop or keep CATEGORY columns
- drop or keep hierarchy levels
- set initial drill levels
- drop or keep statistics for individual ANALYSIS/COMPUTED columns
- drop or keep data values and totals
- hide the special Total value
- hide or show data values
- define initial drill subsets

Below are some guidelines to follow when you assign access using the Drop, Keep, and Hide tags in your access lists.

- Drop columns or hierarchies to remove them from any reports and selection windows for the users in the selected group. Keep columns or hierarchies to display only those in any reports or selections windows.
- Drop data values to remove them from the report and any selection windows. The dropped data values will not be included in the summarization process. Keep data values to make sure only the selected data values are being used in the report, even

if data values are being added to the database. Although you can define a mix of Drop and Keep tags, the Keep tags will always take precedence over the Drop tags.

- Hide ANALYSIS columns to remove them from reports and selection windows, but have them available internally as input to COMPUTED columns.
- Hide data values and the special Total values to remove values from the report and any selection lists but include them in the summarization process.
- Set Initial hierarchy levels and data values to define an initial drill status.

Removing Columns from Your Applications

You can use access control to dynamically remove columns from users' reports. Reports built using columns that are denied for a given group of users will not display those columns when a user of that group runs the report. Also, when users build reports using a restricted metabase registration, the columns denied to them will not be available for selection.

Before you begin

1. Make sure that the data used in your applications is available in your session. Data access control restrictions are assigned to metabase registrations. Make sure that you assign your access control definitions to the same registrations used in your applications.
2. Activate access control.

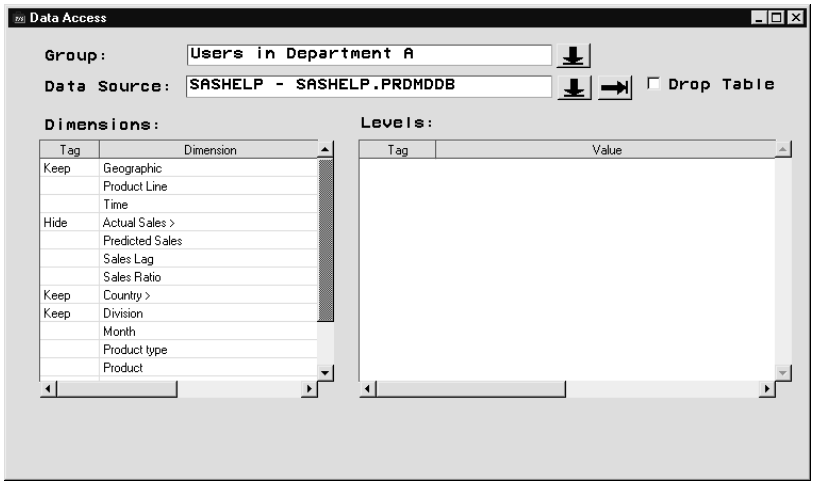
Then, follow these steps:

1. Open the Access Control Setup window by selecting **Setup** from the EIS Main Menu and **Access Control** from the Setup window's Multidimensional Applications group. When you are prompted to do so, type the access control key.
2. In the Access Control Setup window, select **Access Control List Definition** and **Data Access Control**.
3. In the Data Access Control Definition window, select a group and a metabase registration. Then, select column names in the Dimensions list box and use either the pop-up menu or from the menu bar select

   Actions ▶ Set Dimension Tag

   to complete one of the following tasks:

   - drop or keep CATEGORY columns. Removing CATEGORY columns also removes them from any hierarchies to which they belong.
   - drop or keep ANALYSIS/COMPUTED columns. You might want to remove an ANALYSIS column from the report but still have it available as part of a COMPUTED column. To do this, select Hide instead of Drop. The Hide tag prevents the user from seeing or selecting the column, but the column is still available for calculating COMPUTED columns.
   - drop or keep statistics for individual ANALYSIS/COMPUTED columns. For each analysis column, you can select the set of statistics to be made available to users.
   - drop or keep hierarchies. The CATEGORY variables that make up a hierarchy are still available to users for display and selection.
   - drop or keep hierarchy levels. The CATEGORY variable that makes up a hierarchy level is still available to users for display and selection.



Note: Dropping a column removes it from the reports. Keeping columns removes from the reports all columns except those tagged with the Keep tag. Although you can define a combination of Drop and Keep tags in an access list, Keep tags always have precedence over Drop tags. △

Subsetting Data for Your Applications

You can use access control to exclude data from the reports for groups of users.

Before you begin

1. Make sure that the data used in your applications is available in your session. Data access control restrictions are assigned to metabase registrations. Make sure that you assign your access control definitions to the same registrations used in your applications.
2. Activate access control.

Then, follow these steps:

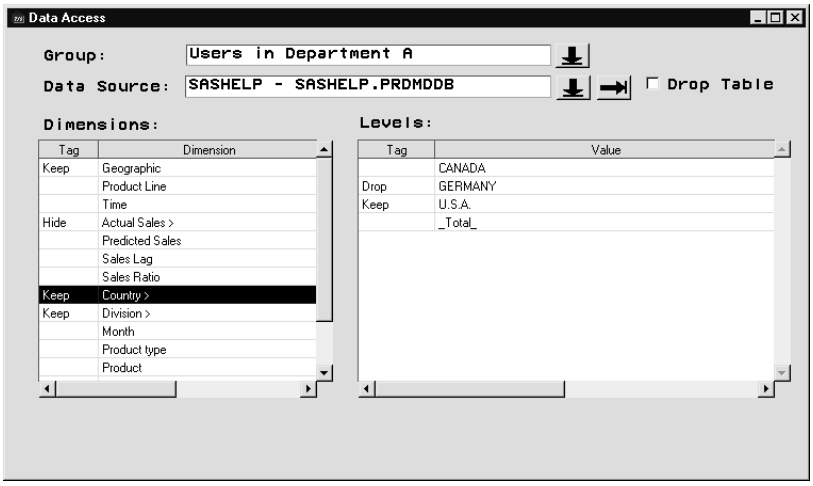
1. Open the Access Control Setup window by selecting **Setup** from the EIS Main Menu and **Access Control** from the Setup window's Multidimensional Applications group. When prompted, type the access control key.
2. In the Access Control Setup window, select **Access Control List Definition** and **Data Access Control**.
3. In the Data Access Control Definition window, select a group and a metabase registration. In the Dimensions list box, select the name of a **CATEGORY** data column. To populate the Levels list with the unique data value of that column, either double-click on the column name or from the menu bar select

   Actions ▶ Display Levels

   In the Levels list, select any data values and use the pop-up menu or select from the menu bar

   Actions ▶ Set Level Tag

   to choose a Drop or Keep tag for the selected data values.



Note: Use Drop to remove a value from the report. Use Keep to make sure that only those values tagged with Keep for the selected CATEGORY variable are included in the report. Although you can define a mix of Drop and Keep tags, the Keep tags always take precedence over the Drop tags. △

Removing Data from Reports without Subsetting

You might want to prevent users from seeing certain detail values while allowing them to see the overall numbers in a report. You can use the access control's Hide and Show tags to remove data values from your report's display while including the values in the summarization process.

Before you begin

1. Make sure that the data used in your applications is available in your session. Data access control restrictions are assigned to metabase registrations. Make sure that you assign your access control definitions to the same registrations used in your applications.
2. Activate access control.

Then, follow these steps:

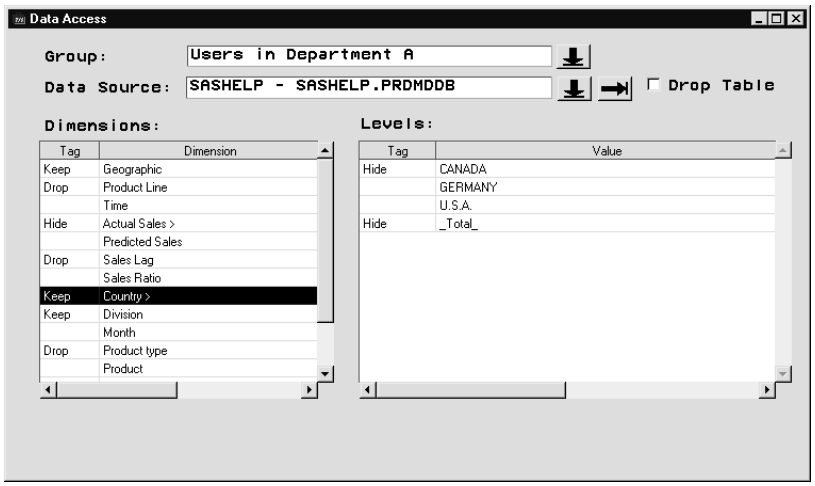
1. Open the Access Control Setup window by selecting **Setup** from the EIS Main Menu and **Access Control** from the Setup window's Multidimensional Applications group. When prompted, type the access control key.
2. In the Access Control Setup window, select **Access Control List Definition** and **Data Access Control**.
3. In the Data Access Control Definition window, select a group and a metabase registration. In the Dimensions list box, select the name of any **CATEGORY** data column. Use Hide to remove a value from the display. Use Show to make sure that only those values tagged with Show for the selected CATEGORY variable are shown in the report In the Dimensions list box, select the name of any CATEGORY data column. To populate the Levels list box with the unique data value of that column, either double-click on the column name or from the menu bar select

   Actions ▶ Display Levels

   In the Levels list box, select any data values, and use the pop-up menu or from the menu bar select

   Actions ▶ Set Level Tag

to choose a Hide or Show tag for the selected data areas.



Note: Although you can define a combination of Hide and Show tags, the Show tags always take precedence. △

You can also hide the special Total value. Typically, you might want to avoid showing a total row or column in tables with hidden values because the total that is displayed does not represent the total of the data values displayed.

Setting Initial Drill Levels for Your Applications

You can use access control to set initial drill levels for groups of users. You can control the view of the data that users have when they first enter their application. At any time, a user can navigate up or sideways from an initial drill level.

Before you begin

1. Make sure that the data used in your applications is available in your session. Data access control restrictions are assigned to metabase registrations. Make sure that you assign your access control definitions to the same registrations used in your applications.
2. Activate access control.

Then, follow these steps:

1. Open the Access Control Setup window by selecting **`Setup`** from the EIS Main Menu and **`Access Control`** from the Setup window's Multidimensional Applications group. When prompted, type the access control key.
2. In the Access Control Setup window, select **`Access Control List Definition`** and **`Data Access Control`**.
3. In the Data Access Control Definition window, select a group and a metabase registration.

   You can define which hierarchy level to display first when a user opens a report. To set an initial hierarchy level, follow these steps

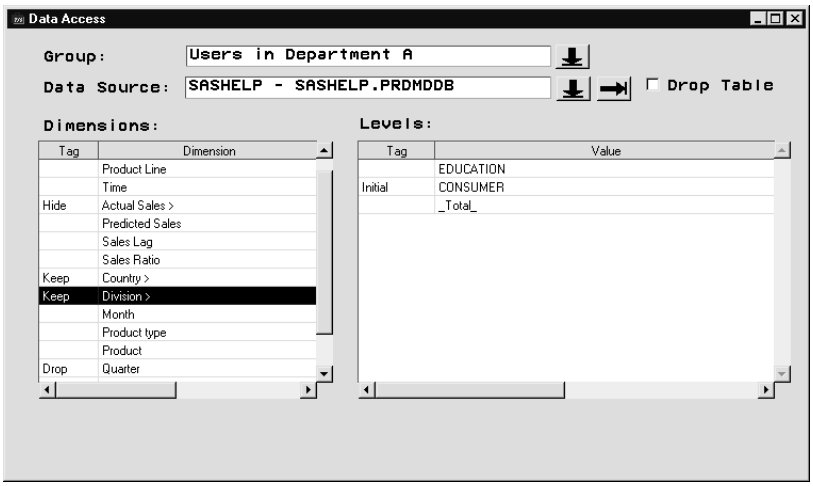
   a. In the Dimensions list box, select the name of a hierarchy. To display the hierarchy level in the Levels list box, either double-click on the hierarchy's name, or from the menu bar select

   Actions ► Display Levels

b In the Levels list box, select a hierarchy level and use either the pop-up menu or from the menu bar select

Actions ► Set Level Tag

to place the Initial tag on the item.



Note that the initial hierarchy levels will be picked up only by hierarchies that are displayed as a user opens a report.

You can also define the subset to be applied as a user first opens a report. The initial subset is not permanently applied and can be removed by the user when navigating the report. To set an initial subset, follow these steps

a In the Dimensions list box, select the name of a CATEGORY column.

b To display the data values in the Levels list box, either double-click on the column's name, or from the menu bar select

Actions ► Display Levels

c In the Levels list box, select data values and use either the pop-up menu or from the menu bar select

Actions ► Set Level Tag

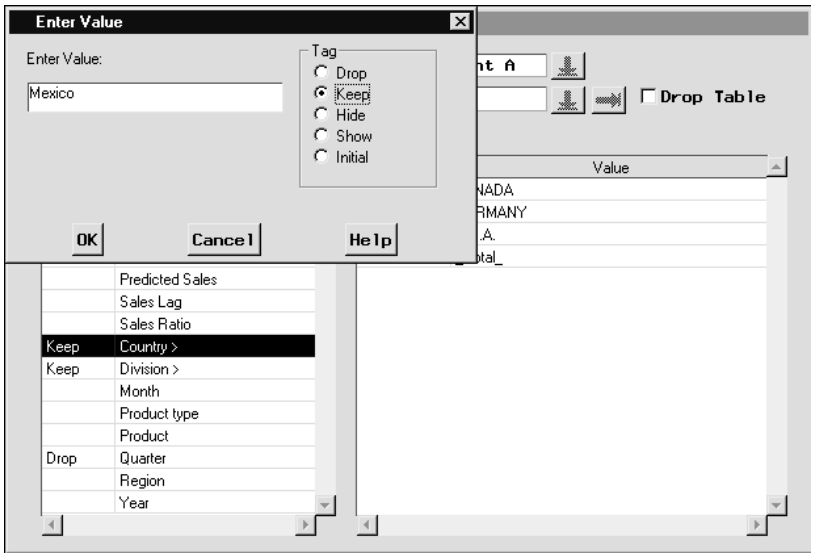
to place the Initial tag on the items.

Providing Access Control Tags for New Values

When you define an Access Control list, you need to have the structure of all your data sources available in the form of metabase registrations. However, you might not have the full set of production data at your disposal.

If you need to set access control tags on data values that are not currently available in the data source but which will be there for the production version of your application, you can use the Add Value selection on the pop-up menu or in the Actions menu.

You can use the Add Value item to set any tag; for example, you can use it to subset data, remove data from a display, and to set initial subsets. Follow the steps in any of the three previous subtopics to display the levels of a CATEGORY column. Then select Add Value on the pop-up menu or in the Actions menu.



Any values entered in the Enter Value window are added to the Access Control list for the current CATEGORY column. You can change the tag that you selected in the Enter Value window. To remove a value added through Add Value, reset the tag to None.

You can use Add Value to specify macro variable references. The macro variable references will be resolved at application run time only. This allows you to add dynamic elements to your Access Control list. For example, to implement a subset that always points to the current month, first set macro variable *&currmonth* with a Keep tag in the Month dimension. Then, be sure to set *&currmonth* when you invoke the application. For example, you can specify the following statement:

```
call symput('currmonth,put(date(),month.));
```

Note: Undefined macro variables in the ACL for a given data source will lead to a run-time error of the application. △

Controlling Access to Applications

Controlling Access to Your Applications

For each group of users, you can deny access to individual applications or application databases.

Before you begin

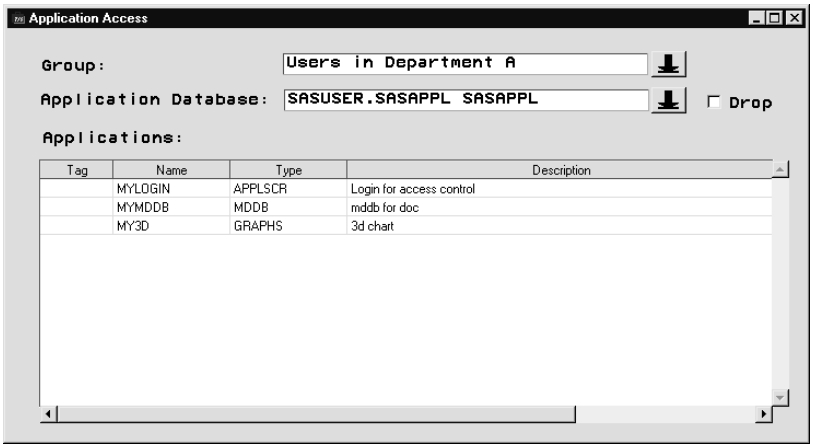
1. Make sure that the application databases and applications that make up your SAS/EIS application are available.
2. Activate access control.

Then, follow these steps:

1. Open the Access Control Setup window by selecting **Setup** from the EIS Main Menu and **Access Control** from the Setup window's Multidimensional Applications group. When you are prompted, type the access control key.
2. In the Access Control Setup window, select **Access Control List Definition** and **Application Access Control**.

3 You can drop or keep entire application databases or individual applications. The following guidelines apply:

- Dropping an application database ensures that no user in the selected group will be allowed to run any application in the application database.
- Dropping an application ensures that no user in the selected group will be allowed to run this application within this application database.
- Keeping an application ensures that the users in the selected group will only be allowed to run this application within this application database (and any other applications within this application database that are tagged Keep).



Note: Although you can define a combination of Drop and Keep tags, the Keep tags always take precedence. △

Controlling Access to Your Applications' Functions

For each group of users, you can deny access to certain parts of the SAS/EIS environment and disable parts of the default run-time functionality of multidimensional EIS reports.

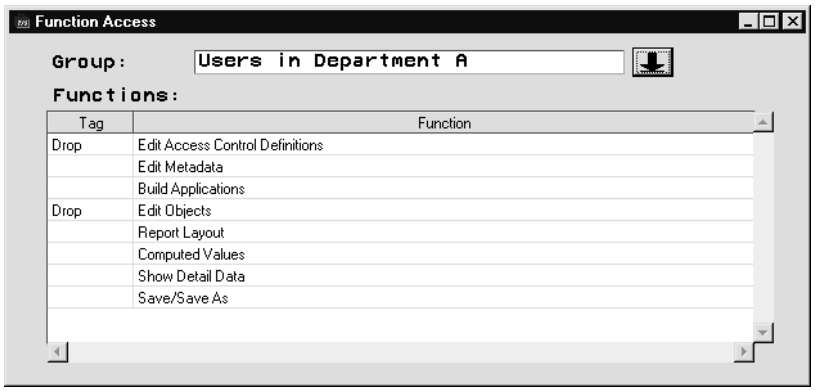
Before you begin

- Activate access control.

Then, follow these steps:

1 Enter the Access Control Setup window by selecting **Setup** from the EIS Main Menu and **Access Control** from the Setup window's Multidimensional Applications group.

2 In the Access Control Setup window, select **Access Control List Definition** and then **Function Access Control**.



The Function Access Control Definition window allows you to restrict access to certain areas of the EIS environment and to certain functions within reports.

- You can deny access to the
  - Access Control Setup window
  - Metabase definition windows
  - Build Application windows
  - Object Database windows.
- You can make the following run-time selections unavailable:
  - Report Layout
  - Computed Values
  - Show Detail Data
  - Save/Save As.

Controlling the Application Run-Time Environment

Customizing the Run-Time Environment

In addition to controlling the data, applications, and application features that users can access, you can use access control to customize the run-time environment for applications at your site. You can perform some or all of the following tasks depending on your site and your users' requirements.

Controlling the Type of Messages That Are Presented to the User

When users display reports that were defined by using columns that have been removed with access control, warning or error messages might be produced, indicating that columns are being removed from the report.

By default, a generic error message is displayed in a dialog box when a report cannot be displayed because columns that are essential for the report to display have been removed. Also, any messages about dropped columns are written to the log.

You can control the level of messages to display for individual users by completing the steps below.

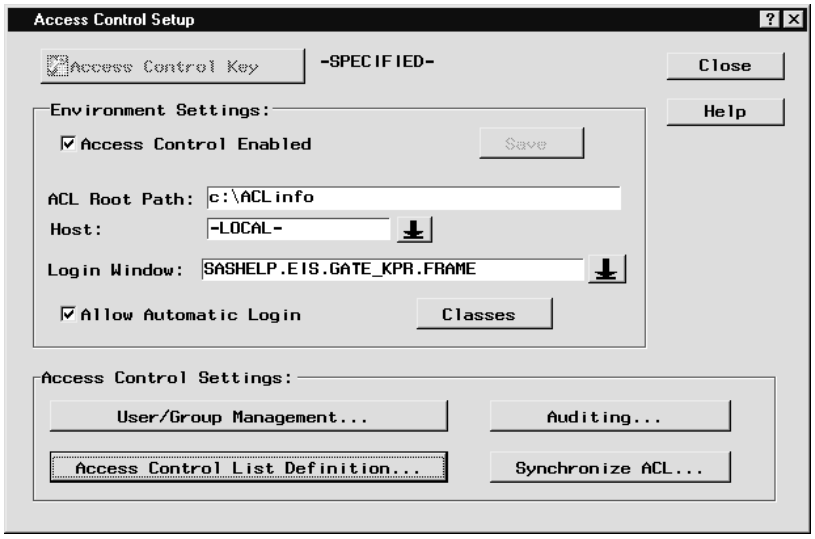
1 Open the Build-/Run-time Options window by selecting **`Setup`** from the EIS Main Menu and **`Build-/Run-time Options`** from the Setup window's Multidimensional Applications group.

2 In the Build-/Run-time Options window, set the message level for dialog messages and log messages. The message level values will be stored in the current user's profile.

Logging In without Displaying a Login Dialog Window

Users already could have identified themselves to their computer systems as they logged in to networks or security software installed at your site. To avoid displaying another login screen as users start their SAS/EIS applications, specify the USER= and PASSWD= options on the EIS and RUNEIS commands. When these options are set to a valid value, a login window does not display.

Make sure that the **Allow Automatic Login** check box in the Access Control Setup window is checked. (It is active by default.)



If you start your SAS/EIS application in an AUTOEXEC.SAS file or by using the -INITCMD invocation option, you can pick up the current user's ID and password from the external access control system, assign it to an environment variable or SAS macro variable, and set your USER= option to that value.

Building Customized Login Windows

The Access Control facility provides two default login windows. Use the arrow beside the Access Control Setup window's Login Window field to select either

- □ Default Login Dialog (the default)
- □ Login Dialog with Change Password.

You can also specify the four-level name of any SAS/AF FRAME or SCL entry, or a SAS/EIS Application Screen Builder application as the login window.

To build your own Login window using the SAS/EIS Application Screen Builder object, follow these steps:

1 Use the Build EIS facility to create an Application Screen Builder object. In your Application Screens Builder frame, add the class SASHELP.EIS.LOGIN.CLASS to your Components list. (To add a class to your Components list, click the right mouse button in the Components window and select **Add Classes**.)

2 Drag the recently created Login Composite class onto your application frame. Now add any additional elements to your frame.

3 To use the new Login window, specify the four-level name of the Application Screen Builder applications (for example, mylib.myappdb.login.applscr) in the Login Program field of the Access Control Setup window, and then save the new setting.

To build your own Login window using a SAS/AF FRAME or SCL entry, follow these steps:

1 In your FRAME or SCL entry, use the object ID of the SAS/EIS access control subsystem, which is stored in the local environment as a numeric item named SECURITY_OBJECT.

2 To check for a valid User ID/password pair, use the security object's _login method (see the online Help for SASHELP.MB.ACLSERV.CLASS for details on the _login method's syntax). On valid login attempts, close your AF application and return a positive numeric value as your application's ENTRY parameter; return 0 when you close with unsuccessful login attempts.

3 To use the new Login window, specify the four-level name of the entry (for example, mylib.mycat.login.frame) in the Login Program field in the Access Control Setup window, and save the new setting.

Enabling Access Auditing

You can log the time and duration of a user's access application and data.

Before you begin

□ Activate access control.

Then, follow these steps:

1 Open the Access Control Setup window by selecting **`Setup`** from the EIS Main Menu and **`Access Control`** from the SAS/EIS Setup window's Multidimensional Applications group.

2 Select Auditing to open the Access Audit Setup window.

3 Specify a location for your log file. To select an Audit File Path and Host, follow the same rules given to set up your ACL Root Path and Host in "Initializing the Environment" on page 4.

4 Choose the events that you want to log, and activate Enable Access Auditing.

5 Select OK to check the path, create the LOG file, and save the settings

The access audit setup information is physically stored in the SASHELP.AC catalog. For all applications that use SAS/EIS access auditing, make sure that this catalog, or a copy of it, is being used.

6 To enable the new settings, close your SAS/EIS session and all active SAS/EIS applications; then restart your SAS/EIS session.

Assigning Multiple Groups to a User

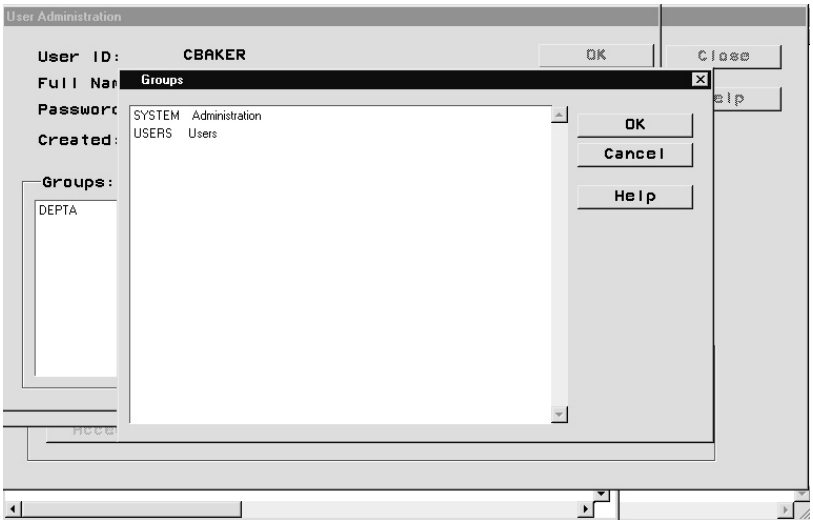
You can assign multiple groups to a user. Users with multiple groups have the combined access rights of all groups to which they belong. Data, applications, or functions are removed for them only if they are dropped or hidden or not kept for all the groups to which the user belongs. To assign multiple users to a group, select multiple groups in the user's definition window.

Before you begin

□ Activate access control.

Then, follow these steps:

1. Open the Access Control Setup window by selecting **Setup** from the EIS Main Menu and **Access Control** from the Setup window's Multidimensional Applications group. When you are prompted, type the access control key.
2. Select User/Group Management and User Management.
3. Select a userid and select Edit. In the user's definition, select Edit next to the group list. Then, select the groups you want to assign to the user.



Customizing the Access Control Environment

Setting Up Multiple Access Control Environments

If you support different sets of SAS/EIS applications with different sets of users, you can set up multiple access control environments.

The information entered in the Access Control Setup window and the Access Audit Setup window is stored in and retrieved from the SASHELP.AC catalog.

Follow these steps:

1. After typing the access control setup information for one environment, make a copy of the SASHELP.AC catalog.
2. Type different access control setup information, and make another copy of the SASHELP.AC catalog.
3. Make sure the correct copies of the AC catalog are distributed into the correct users' SASHELP images.

Querying Access Control Settings

To find out about your access control settings, you can open the Access Control Setup window to view the current values in the Environment Settings list box and select User/Group Management or Access Control List Definition to view the current values in the Access Control Settings list box.

To query the access control settings programmatically, refer to "Creating Access Control Definitions Programmatically" on page 21.

Changing the Administrator's Password

You should rarely need to change the administrator's password. The steps below describe how to change the password when necessary.

Before you begin

- Make sure you have write access to your SASHELP.MB catalog.

Then, follow these steps:

1. Change the password to the new values on all data sets that were created by using the current administrator's password. If access control is activated, these are the files in your ACL root path.
2. If you have activated access auditing, you also need to change the password on the LOG data set in the Audit File path. Use PROC DATASETS or menu-driven SAS facilities to change the password on these data sets.
3. Use the following method call to change the administrator's password in the SASHELP.MB catalog:

```
CALL METHOD ('SASHELP.MB.APWUTIL','CREAAPWM', flag, pw-value, rc);
```

where

flag	is 0 or 1. 0 indicates to not use a control key; 1 indicates to use a control key.
pw-value	is the value of the new control key. If *flag* is 0, this value is ignored
rc	is 0 if the update was successful; 1 if it was not successful.

Creating Access Control Definitions Programmatically

In addition to defining access control definitions interactively by using the User/Group Management and Access Control Definition windows, you can also create user and group data sets and access control list data sets by using

- data management tools, for example, the SAS DATA step
- the SCL methods provided in the access control administration (ACLADMIN) class.

Refer to online Help for the SASHELP.MB.ACLADMIN.CLASS for details on how to create Access Control data sets using SCL methods.

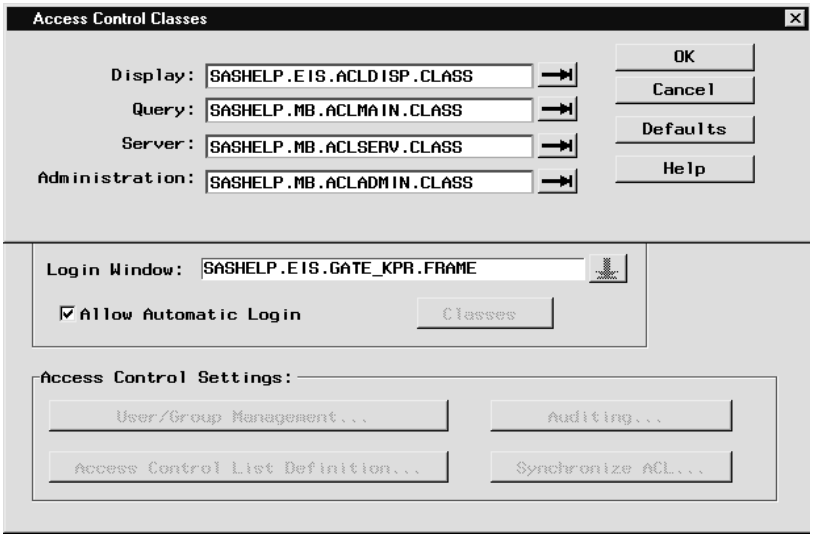
Overriding the Default Behavior of Access Control

Your site might have special access control requirements that are not met by the default set of functionality available in the SAS/EIS access control facility.

Refer to online Help for the Access Control Server class, SASHELP.MB.ACLSERV.CLASS, for details on how to change the structure and format of access control files or for specifics on dealing with non-standard client/server configurations.

Refer to online Help for the Access Control Query class, SASHELP.MB.ACLMAIN.CLASS, for details on how to change the way that the access control information is retrieved and returned.

Specify your access control subclasses in the Access Control Classes window. To open the Access Control Classes window, open the Access Control Setup window and select Classes.



Setting Up the Access Control Environment Programmatically

In addition to using the access control windows to perform setup and maintenance tasks, the access control facility provides methods to set up the access control environment programmatically.

To change any of the access control settings using SCL, you must have write access to the SASHELP.AC catalog and a SAS/AF Software license to run the BUILD environment.

Setting the ACL Setup Parameters

This method re-creates the entry SASHELP.AC.ACLINIT.SCL.

```
CALL METHOD ('SASHELP.EIS.ACLUTIL', 'CREAACLI', rc,  flag, aclroot,
    aclserv,login_window, autouser_enabled, libsec, pw_encrypt);
```

Where...	Is type...	And contains...
rc	N	a flag that indicates if the update was successful, where 0 indicates that the update was successful and 1 indicates that it was not.
flag	C	a flag that activates or deactivates security. Valid values are Y and N.
aclroot	C	the path of a directory that holds the ACL files.
aclserv	C	the name of the remote session or share server for *aclroot*. If the session is local, this parameter should be blank.
login_window	C	the four-level name of the AF application or APPLSCR application to use for login.
autouser_enabled	C	a flag that indicates whether to allow the use of &AUTOUSER at login. Valid values are Y and N.

Where...	Is type...	And contains...
libsec	C	a flag that indicates when the ACL library is allocated, where Y indicates that the ACL library is allocated before and deallocated after each access to the ACL files. N indicates that the ACL library is allocated once at access control server allocation and deallocated at access control server termination.
pw_encrypt	C	a flag that indicates whether to encrypt the PASSWORD values, where Y indicates that the PASSWORD variable values should be encrypted in the PASSWD data set. N indicated that the user passwords should not be encrypted.

Setting the Administrator's Password

This password is used to create and access ACL files and to enable access to the password support feature. Set the flag to 0 if you do not want to use a password.

```
CALL METHOD('SASHELP.MB.APWUTIL','CREAAPWM',flag, pw-value,rc);
```

Where...	Is type...	And contains...
flag	C	a flag that indicates whether to activate the password, where 1 specifies to activate the password. 0 specifies to deactivate the password.
pw-value	C	the text of the password. The value for this parameter must follow the current SAS file password syntax conventions.
rc	N	a flag that indicates whether the update was successful, where 0 indicates that the update was successful. 1 indicates that the update was not successful.

Setting the Audit Parms

This method re-creates the entry SASHELP.AC.ACLLOG.SCL, which is used to track activities associated with the access control facility.

```
CALL METHOD  ('SASHELP.EIS.ACLUTIL','CREALOG', rc, flag, logroot,
    logserv, logtime, data, appl);
```

Where...	Is type...	And contains...
rc	N	a flag that indicates whether the update was successful, where 0 indicates that the update was successful. 1 indicates that the update was not successful.
flag	C	a flag that indicates whether to activate access logging, where Y activates access logging. N deactivates access logging.
logroot	C	the path of a directory that holds the LOG file.
logserv	C	the name of the remote session or share server for *logroot*. If the session is local, this parameter should be blank.
logtime	C	a flag that indicates whether to log full SAS/EIS access time. Valid values are Y or N.
data	C	a flag that indicates whether to log data source access. Valid values are Y or N.
appl	C	a flag that indicates whether to log application access. Valid values are Y or N.

Querying ACL Setup Values and Password

Use the following job to query the current ACL settings and the current administrator's password:

```
length security_enabled $1
       aclroot          $200
       aclserv          $17
       logroot          $200
       logserv          $17
       login_window     $35
       autouser_enabled $1
       libsec           $1
       pw_encrypt       $1
       admin_pw         $16
       pw_active        8
       audit_enabled    $1
       logtime          $1
       logdata          $1
       logappl          $1

;

init:
/* Administrator's password */
call method('sashelp.mb.aclapwm','aclapw',pw_active,admin_pw);
put pw_active=;
put admin_pw=;

/* Security Enabled? */
call method('sashelp.ac.aclinit','aclinit',security_enabled);
put security_enabled=;
```

```
/* ACL Root */
call method('sashelp.ac.aclinit','aclrt',aclroot,aclserv);
put aclroot=;
put aclserv=;

/* Login Window */
call method('sashelp.ac.aclinit','acllw',login_window);
put login_window=;

/* AUTOUSER Enabled? */
call method('sashelp.ac.aclinit','aclau',autouser_enabled);
put autouser_enabled=;

/* Secure Libref? */
call method('sashelp.ac.aclinit','libsec',libsec);
put libsec=;

/* Encrypt User passwords? */
call method('sashelp.ac.aclinit','pwencrpt',pw_encrypt);
put pw_encrypt=;

/* LOG Root */
call method('sashelp.ac.acllog','logrt',logroot,logserv);
put logroot=;
put logserv=;

/* Log LOGIN/LOGOUT? */
call method('sashelp.ac.acllog','logopt',logtime,logdata,logappl);
put logtime=;

/* Log Data Access? */
put logdata=;

/* Log Application Access*/
put logappl=;
return;
```

Maintaining Access Control Lists

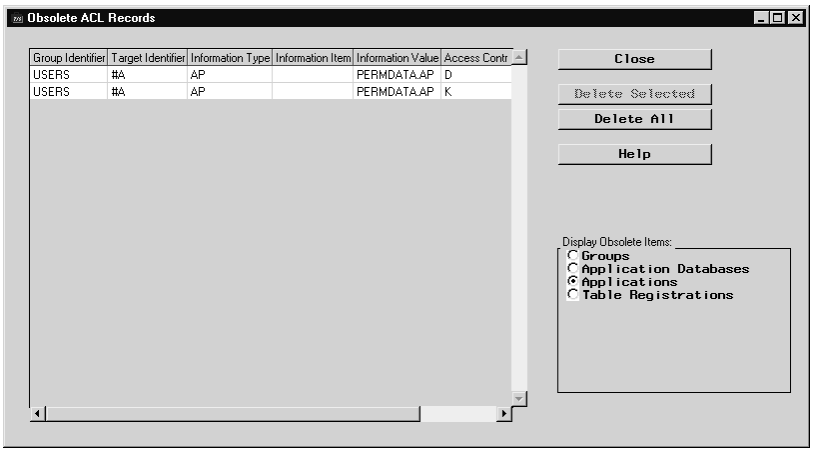
Removing Obsolete Records from An Access Control List

As you make changes to your access control environment, you might delete users or groups, data registrations might be removed, data values become obsolete, and so on. If your Access Control list has entries for any of these deleted items, these entries are obsolete. Although they do not have any serious adverse effects, they increase the size of the Access Control list unnecessarily and can eventually negatively affect performance. We recommend that you regularly clean up your Access Control list by running the synchronization tool that is provided by the SAS/EIS access control facility by using the steps described below.

1 Start Access Control synchronization by clicking on Synchronize ACL in the Access Control Setup window. This starts a process that can take several minutes,

depending on the size of your Access Control list. Every record in the list is cross-checked against your current environment, and any records referring to entities that are not found are flagged for deletion.

2 When the cross-checking task is complete, the Obsolete ACL Records window is displayed.



All the obsolete records that were found during the process are displayed in the window, grouped by the following categories:

Groups	lists records for groups that do not exist in the current access control environment.
Application Databases	lists records with application databases or applications in application databases that do not currently exist.
Applications	lists records with applications that do not currently exist.
Table Registrations	lists records with metabase table registrations that do not currently exist.
Hierarchies	lists records with the HIERARCHY table attribute contents that do not currently exist for the given table.
Hierarchy Levels	lists records with HIERARCHY table attribute levels that do not currently exist for the given hierarchy.
Analysis Columns	lists records with ANALYSIS or COMPUTED columns that do not currently exist in the given table.
Statistics	lists records with statistics that are not currently available for a given analysis column.
Category Columns	lists records with CATEGORY columns that do not currently exist in the given table.
Category Levels	list records with data values that do not currently exist in the given table.
Macro Variables	lists all macro variables referenced in the Access Control list. Note that macro variable references are always listed. Use this facility to delete macro variables from your Access Control list.

Note: The lists in this window enable you to check and mark for permanent deletion each record that was found obsolete. To start permanent deletion of all selected records, close the window. △

Note: For additional information on the synchronization process, refer to the _checkACL method Help information for SASHELP.MB.ACLADMIN.CLASS. △

Troubleshooting

Occasionally, after you set up the access control environment, some users might encounter problems when they try to access SAS/EIS software or run their applications. This section describes some techniques that you can use to determine the cause(s) and suggests possible solutions for correcting the following problems:

- The access control system does not initialize.
- Users are not able to log in.
- The access control system does not initialize and you need to find out the current access control settings.
- The defined access control restrictions are not being applied to a particular user.

What If the Access Control System Does Not Initialize?

When a user attempts to start an EIS application by using either the **EIS** or the **RUNEIS** command, one of the following error messages is displayed:

1

```
''The Access Control subsystem cannot be started at this time.  You
will not be able to run the application.  Please contact your system
administrator.''
```

The following are possible reasons that the user encountered a problem:

- The SASHELP.AC catalog does not exist.
- One or all of the access control data sets (PASSWD, GROUPS, ACL, and, optionally, LOG) cannot be accessed for any of the following reasons:
  - files deleted
  - files damaged
  - files open by another process or user
  - no file or directory authorization
  - different password on the files than the current access control key
  - remote session not active
  - any of the AF classes necessary to start access control are not available
  - you have specified an incorrect value for the EIS or RUNEIS command options, USER= or PASSWD=. Force an interactive login by removing the command options or by setting USER=' '.

2

```
''The Access Control subsystem is not active at this time.  Please
start the system using the correct login procedure, or contact your
system administrator.''
```

A possible reason that this message was issued is that the user has just activated access control and is trying to run an application without completely leaving the EIS session and all active EIS applications.

3

```
''Your Access Control account information cannot be retrieved at this
time.  Please try again or contact your system administrator.''
```

A possible reason that this message was issued is that the PASSWD data set in the ACL Root Path is not readable.

4

```
''Your Access Control account information is incomplete.  You will
not be able to run the application.  Please contact your system
administrator.''
```

A possible reason that this message was issued is that the group information for the user is missing from the PASSWD file. Make sure that the user is assigned to at least one group.

What If Users Are Not Able to Log In?

When users try to log in by typing their ID and password, they receive the following message repeatedly, although the values in the Userid and Password fields are correct:

```
''Invalid Userid/Password Pair.  Try again.''
```

A possible solution is to change the pw_encrypt option. See “Querying ACL Setup Values and Password” on page 24 for more information.

When the Access Control System Does Not Initialize, How Can You Find Out the Current Access Control Settings?

Typically, you will enter and update the access control settings by using the windows provided with the access control feature. However, if the system does not initialize and you need to find out the current settings of some of the parameters, you a can get this information programmatically by using the access control utility programs. See “Querying ACL Setup Values and Password” on page 24 for more information.

What If the Access Control Restrictions Are Not Being Applied for a Particular User?

If access control restrictions are not being a applied for a user, first check to see if the user belongs to more than one group. For users who belong to more than one group, the access control system applies only those restrictions that are defined for all groups to which the user belongs.

The correct bibliographic citation for this manual is as follows: SAS Institute Inc., *SAS/EIS® Software: Administrator's Guide, Version 8*, Cary, NC: SAS Institute Inc., 1999.

SAS/EIS® Software: Administrator's Guide, Version 8

Copyright © 1999 SAS Institute Inc., Cary, NC, USA.

ISBN 1–58025–506–X

All rights reserved. Printed in the United States of America. No part of this publication may be reproduced, stored in a retrieval system, or transmitted, by any form or by any means, electronic, mechanical, photocopying, or otherwise, without the prior written permission of the publisher, SAS Institute, Inc.

U.S. Government Restricted Rights Notice. Use, duplication, or disclosure of the software by the government is subject to restrictions as set forth in FAR 52.227–19 Commercial Computer Software-Restricted Rights (June 1987).

SAS Institute Inc., SAS Campus Drive, Cary, North Carolina 27513.

1st printing, October 1999

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.

IBM, ACF/VTAM, AIX, APPN, MVS/ESA, OS/2, OS/390, VM/ESA, and VTAM are registered trademarks or trademarks of International Business Machines Corporation. ® indicates USA registration.

Other brand and product names are registered trademarks or trademarks of their respective companies.

The Institute is a private company devoted to the support and further development of its software and related services.