AllFusion® Model Manager

Administrator Guide

r7.2

CA Product References

This document references the following CA products:

- AllFusion® Model Manager
- AllFusion® ERwin® Data Modeler
- AllFusion® Process Modeler

Contact Technical Support

For online technical assistance and a complete list of locations, primary service hours, and telephone numbers, contact Technical Support at http://ca.com/support.

Contents

Chapter 1: Modeling in the Multi-User Environment

AllFusion Model Manager (AllFusion MM) coordinates the development and management of models created with AllFusion ERwin Data Modeler (AllFusion ERwin DM) and AllFusion Process Modeler (AllFusion PM).

This section contains the following topics:

The Administrator's Tasks

When you install the AllFusion MM software, the administrator role is automatically granted Administrator security status. This allows the administrator to assign user permissions and perform all required maintenance or administrative tasks.

An administrator's responsibilities can be categorized as follows:

- Create and delete the mart
- Install, initialize, and upgrade the software
- Develop and administer standards
- Administer security
- Manage user sessions
- Create and maintain a library structure
- Generate reports and perform other administrative tasks

Initialize a New AllFusion MM Mart

Before you can begin working in the mart, you must initialize AllFusion MM to prepare it for use with both AllFusion ERwin Data Modeler and AllFusion Process Modeler. If a previous version of AllFusion MM is detected, the Update button displays. Create and Update are mutually exclusive and the text of the Update/Create button changes depending if a previous version of the mart is detected.

To initialize a new AllFusion MM mart

1. Connect to AllFusion MM during the initial installation.

   The AllFusion MM Manger opens.

2. Select one of the following fields:

   Truncate Log Before Any Action to truncate the transaction log

   If you are using Microsoft SQL or Sybase this helps prevent running out of disk space during the initialization or update. (Available only when using Microsoft SQL Server or Sybase).

   Oracle MMUSER security role

   If you are using Oracle, select the name of the Oracle MMUSER security role, the name of the tables in Table Tablespace, and the name of the indexes in Index Tablespace. For further information regarding the Oracle role MMUSER, see the section on creating the database in the AllFusion Model Manager Implementation guide.

   Click one of the following options:

   Create

   Creates an empty mart, and then you manually open and save existing models to convert your data.

   Update

   Updates the current AllFusion MM mart to be compatible with the current AllFusion ERwin DM release. This button is enabled only when an earlier version of a AllFusion MM is recognized.

   Convert

   Creates a new mart with the current version and automatically copies the data from the old mart into the new mart. The information in the old mart is retained.

   Delete

   Removes an AllFusion MM mart no longer in use.

   The current status of the mart including the name, size, and real-time update statistics display in the dialog.

You can also view real-time conversion statistics when converting from one AllFusion MM version to another.

Delete an AllFusion MM Mart

You can delete an AllFusion MM mart that is no longer in use.

Note: Removing the AllFusion MM mart is a drastic measure and should only be done after careful consideration. Be sure to back up your database prior to removing the mart in case you want to revert back to the prior version some time in the future.

To delete a AllFusion MM mart

1. Connect to the AllFusion MM mart during the initial installation.

   The AllFusion MM Manager opens.

2. Click Delete.

   The AllFusion MM mart is deleted. Verify that the m7Master and m7License tables no longer exist. If they do exist, remove them manually using your DBMS tools.

Microsoft SQL Server 2005 Permissions

For SQL Server 2000, you only need to have public assigned in order to save to the mart. However, when the repository is on an SQL Server 2005 instance, you need to have the bulkadmin permission designated as well. The ability to do bulk inserts (which was permitted by public, previously) is no longer part of the public permission. You must explicitly define this permission or when you attempt to save a model to a new AllFusion Model Manager instance created using an SQL Server 2005 database, an error "You do not have permission to use the bulk load statement." is returned.

Custom Security Message at Connection

You can add a custom message on the AllFusion MM Connection dialog. The message displays whenever a connection is made to the mart from any of the client applications.

A sample stored procedure is provided for each supported database in the Samples folder. It contains enough code to return the message "Welcome to AllFusion Model Manager". You can modify the sample to change the text or you can write a custom procedure with logic to determine the database user id and lookup table for an appropriate message to display. The message can be up to 1000 characters long, the procedure should return 4 separate strings each a maximum of 250 characters in length.

This custom message displays once you are authenticated for connection to the desired mart, but before the connection dialog is closed.

If you choose Cancel, the current session is disconnected, and the connection dialog continues to display. You can try connecting again or connect to a different mart.

Add a Stored Procedure to Activate a Custom Message at Connection

You can add a custom message based on a stored procedure. If the stored procedure is supplied, then the feature is active, otherwise the feature is dormant. You must create a procedure named M7x_GET_PRIVACY_MESSAGE. During connection to the mart, the existence of the procedure is verified.

To add a stored procedure to activate a custom message at connection

1. Connect to a database editor and copy the template. Make changes to the template and save as a script file.

   The script file is saved.

2. Connect to AllFusion MM as the schema owner, and compile the script as M7x_GET_PRIVACY_MESSAGE.

   The procedure is created.

Sample SQL and Sybase Stored Procedure

```
IF EXISTS (SELECT * FROM sysobjects WHERE id = object_id('dbo.m7x_Get_Privacy_Message'))
    DROP PROCEDURE dbo.m7x_Get_Privacy_Message
go
CREATE PROCEDURE dbo.m7x_Get_Privacy_Message
   @string1         varchar(250) output,
            @string2         varchar(250) output,
            @string3         varchar(250) output,
            @string4         varchar(250) output
AS
```

```
BEGIN
        --Declare
        -- Ensure to initialize strings to avoid un-necessary results
        SELECT    @string1 = '',
                        @string2 = '',
                        @string3 = '',
                        @string4 = ''
    -- Add custom code here for extra validations
   /* Formatted message would go here. Ensure that the content of the message does not exceeed 1000 chars
        Failure to do so will result in truncation */
        Select @string1 = 'This stored procedure will be implemented by the customer based on their current
requirements. Depending on the DBMS additional validations can be ' +
        ' made by the end user to suit their privacy requirements.'
        Select @string2 = Char(13) + Char(10) + 'Currently the procedure can return up to 1000 characters.
Customer responsible for limiting each of the return strings to <= 250 chars, other wise there could be unexpected
errors returned by server.'
        Select @string3 = ' Use native DBB functions for special ASCII characters like CRFL, LF, TAB etc.,'
        Select @string4 = Char(13) + Char(10) + 'Prior to exiting the proc make sure to limit the strings to 250
chars'
        -- Safety check to limit 250 chars
        SELECT    @string1 = left(@string1, 250),
                        @string2 = left(@string2, 250),
                        @string3 = left(@string3, 250),
                        @string4 = left(@string4, 250)
END
go
GRANT ALL ON m7x_Get_Privacy_Message TO PUBLIC
go
```

Sample Oracle Stored Procedure

```
CREATE OR REPLACE PROCEDURE m7x_Get_Privacy_Message (
        p$string1   IN OUT varchar2,
        p$string2   IN OUT varchar2,
        p$string3   IN OUT varchar2,
        p$string4   IN OUT varchar2,
   p$gen_err_code IN OUT NUMBER
        )
AS
-- Declarations here
```

```
BEGIN
    -- Ensure the return parameter is set to Zero for success
            p$gen_err_code := 0;
            p$string1 := '';
            p$string2 := '';
            p$string3 := '';
            p$string4 := '';
    -- Add custom code here for extra validations
    -- Formatted message would go here. Ensure that the content of the message does not exceed 1000 chars
    -- Failure to do so will result in truncation */
            p$string1 := 'This stored procedure will be implemented by the customer based on ' ||
            'their current requirements. Depending on the DBMS additional validations can be ' ||
            'made by the end user to suit their privacy requirements.';
            p$string2 := Chr(13) || Chr(10) || 'Customer responsible for limiting each of the return strings to <= 250
chars, otherwise there could be unexpected errors returned by server.';
            p$string3 := ' Use native DB functions for special ASCII characters like CRFL, LF, TAB etc.,';
            p$string4 := Chr(13) || Chr(10) || 'Prior to exiting the proc make sure to limit the strings to 250 chars';
            -- Safety check to limit 250 chars
            p$string1 := SubStr(p$string1, 1, 250);
            p$string2 := SubStr(p$string2, 1, 250);
            p$string3 := SubStr(p$string3, 1, 250);
            p$string4 := SubStr(p$string4, 1, 250);
            RETURN;
END m7x_Get_Privacy_Message;
/
DROP PUBLIC SYNONYM m7x_Get_Privacy_Message
CREATE PUBLIC SYNONYM m7x_Get_Privacy_Message FOR m7x_Get_Privacy_Message
GRANT ALL ON m7x_Get_Privacy_Message TO PUBLIC
/
```

Standards Tools

A naming standards tool and data type standards tool help your workgroup create and manage model naming and data type standards. Because naming and data type standards use external files, the administrator may also manage these files in AllFusion MM.

How You Manage Your Licensing

When you purchase the product, you receive a license key. The license key specifies the maximum number of authorized users that your installation supports. Each time you add a user, the number of users is verified to determine if you have exceeded the limits of your license agreement.

As part of the administrative process, you must assign a security profile to each user. When a user enters a login name to connect to AllFusion MM, AllFusion MM checks whether the login name has a valid security profile and verifies that the maximum number of users is not exceeded. An error message displays when you exceed the maximum number of users allowed by your license.

If you have exceeded your maximum number of users and want to add additional users, you must do one of the following:

- Upgrade your license.
- Remove one of the existing users and add the new user.
- Purchase AllFusion® Model Navigator, which includes special editions of AllFusion ERwin DM and AllFusion PM for those users who need read-only access to the mart. You can use AllFusion Model Navigator (AllFusion MN) to open and print models and generate reports, but you cannot save changes to the mart or save to a file. You can use the Security Manager to assign AllFusion MN users to a special security profile (Guest) that is not counted toward your license agreement.

Chapter 2: Security

This section contains the following topics:

Security

A comprehensive security system prevents unauthorized users from adding, modifying, or deleting objects in the mart. To ensure security, all objects are divided into hierarchical security classes and all users are assigned to a security profile.

Security profiles determine who can change the data contained in AllFusion MM. By understanding the activities that each member of a workgroup performs, you can assign the necessary privileges and customize permissions to meet the exact needs of the workgroup.

You can assign users to the predefined security profiles or create customized profiles to fit your environment. By assigning a user to more than one security profile, you can customize each user's permission to manipulate different objects in the mart. This role-based security provides complete control over model access and updates, with the flexibility to restrict users by library, model, subject area, and entity.

To manage security, you must be assigned the Administrator security profile for the mart. When you first initialize the mart, you assign the Administrator security profile to your database user name (the dbo for Microsoft SQL Server or Sybase or schema owner for Oracle). You can also assign administrator permission to another database user for day-to-day security management.

The administrator can also add and delete users from AllFusion MM. Security administration is performed using the Security Manager when connected to AllFusion MM.

The Security Manager

The Security Manager assigns user security profiles and creates custom security profiles. You must be connected to AllFusion MM in order to open the Security Manager.

Note: The Security Manager starts automatically at the end of the installation and initialization process for you to assign user security profiles immediately after you create an AllFusion MM mart.

To start the Security Manager, choose Security from the Services menu. The Security Manager dialog opens, displaying the existing users in the User list.

The User pane lists the users you define in your DBMS. You must add, change, and delete users directly from the DBMS. For example, you can use the Enterprise Manager in Microsoft SQL Server. You must assign each DBMS user to a security profile.

Every user with a security profile is counted as a licensed user. Your registration ID determines the maximum number of users that can access the mart. If the number of users exceeds the limit of your license agreement, a warning message prompts you to remove the unauthorized users.

Note: For more information, see Understanding Your License Agreement.

Security Profile Manager Dialog

While only an administrator can change permissions associated with a profile, anyone can view the permissions. The Security Profile Manager dialog lets you view the permissions associated with a profile, and lets the administrator change permissions.

Default Security Profiles - AllFusion ERwin DM

The Default Security Profiles for AllFusion ERwin DM are shown below. An X in a security profile column means the permission is granted; a blank means that permission is denied.

Use the following table to determine which permissions are needed to create, modify, or delete objects. Find the object you want to update in the AllFusion MM Object column, and then locate the corresponding permission in the AllFusion MM Permission column.

Permission Object Class	AllFusion MM Object	AllFusion MM Permission	AllFusion MM Default Security Profile for AllFusion ERwin DM		
			Administrator	Modeler	Architect
Mart	Library	Manage Mart	X		
		Create Library	X	X	
		Delete Library	X	X	
		Update Library	X	X	
Library	Model (Mart model)	Create Model	X	X	X
		Delete Model	X	X	X
		Update Model	X	X	X
Model	Entity (for example, Entity Name, Entity Definition, Table Properties) Relationship (for example, Rolename, Name, Verb Phrase, Cardinality, Type) Stored Display, Text Block	Create Entity	X	X	X
		Delete Entity	X	X	X
		Update Entity	X	X	X

Permission Object Class	AllFusion MM Object	AllFusion MM Permission	AllFusion MM Default Security Profile for AllFusion ERwin DM		
			Administrator	Modeler	Architect
	Domain (for example, Domain Name, Datatype, Default Value, Definition, Null Option, Validation Rules)	Create Domain	X	X	X
		Delete Domain	X	X	X
		Update Domain	X	X	X
	Data Rule	Create Data Rule	X	X	X
		Delete Data Rule	X	X	X
		Update Data Rule	X	X	X
	Bitmap	Create Bitmap	X	X	X
		Delete Bitmap	X	X	X
		Update Bitmap	X	X	X
	Data Source	Create Data Source	X	X	X
		Delete Data Source	X	X	X
		Update Data Source	X	X	X
	Data Source Table	Create Data Source Table	X	X	X
		Delete Data Source Table	X	X	X
		Update Data Source Table	X	X	X
	Data Source Column	Create Data Source Column	X	X	X
		Delete Data Source Column	X	X	X
		Update Data Source Column	X	X	X
	Subject Area	Create Subject Area	X	X	X
		Delete Subject Area	X	X	X
	UDP Key	Create UDP Key	X	X	X
		Delete UDP Key	X	X	X
		Update UDP Key	X	X	X

Permission Object Class	AllFusion MM Object	AllFusion MM Permission	AllFusion MM Default Security Profile for AllFusion ERwin DM		
			Administrator	Modeler	Architect
Entity	Attribute (for example, Attribute Properties, Column Properties)	Create Attribute	X	X	X
		Delete Attribute	X	X	X
		Update Attribute	X	X	X
Subject Area	Subject Area (Change membership of subject area)	Manage Subject Area	X	X	X

Default Security Profiles - AllFusion PM

The Default Security Profiles for AllFusion PM are shown below. An X in a security profile column means the permission is granted; a blank means that permission is denied.

Use the following table to determine which permissions are needed to create, modify, or delete objects. Find the object you want to update in the AllFusion MM Object column, and then locate the corresponding permission in the AllFusion MM Permission column.

Permission Object Class	AllFusion MM Object	AllFusion MM Permission	AllFusion MM Default Security Profiles for AllFusion PM		
			Administrator	Architect	Modeler
Mart	Library	Manage Mart	X		
		Create Library	X	X	X
		Update Library	X	X	X
		Delete Library	X	X	X
Library	Model (Mart)	Create Model	X	X	X
		Delete Model	X	X	X
		Update Model	X	X	X

Note: The Viewer and Guest security profiles for AllFusion ERwin DM and AllFusion PM are initially assigned no permissions.

Security Profiles

If you have an Administrator profile, you can assign a user to a profile applicable to a specific database, library, model, or subject area. Administrators can assign users to more than one profile. For example, a user can have a different profile for different libraries. In Library Production, the Administrator can assign a user to the Architect profile, which grants extensive read and write privileges to that library. In a Library Test, that same user can be assigned to the Viewer profile, which causes them to have read-only permission in that library.

Assign a User to a Security Profile

You can control the actions that the user can perform on an object by assigning a user to a security profile. By assigning a user to more than one security profile, you can customize each user's rights to manipulate objects in the mart. You must assign at least one security profile to each user.

To assign a user to a security profile

1. Click Security on the Services menu.

   The Security Manager dialog opens.

2. Select the user for which you want to assign security and drag the icon for the user from the User list onto the security profile icon in the Security Profile list.

   The user is displayed within the security profile chosen.

3. Click OK.

   The dialog closes and the user is assigned to the security profile.

Change a User's Security Profile

You can modify security permissions for a user by changing the user's security profile.

To change a user's security profile

1. Select Security on the Services menu.

   The Security Manager dialog opens.

2. Select the user from the security profile in the Security Profile list, and drag the user's name back to the User list.

   The user name appears in the User list.

3. Select the user from the User list and drag that user to the new security profile in the Security Profile list.

   The user name now appears under the new security profile.

Remove a User From a Security Profile

You can control the actions that a user can perform on an object using a security profile. If you no longer want a user to have the permissions contained in a security profile, you can remove the user from that Security profile in the Security Manager.

To remove a user from a security profile

1. Click Security on the Services menu.

   The Security Manager dialog opens.

2. Expand the list of user names for the appropriate profile in the Security Profile list.

   The users display in the list.

3. Select the user for which you want to remove security permissions and drag the icon for the user from the Security Profile list to the User list.

   The user is removed from the Security Profile list.

4. Click OK.

   The dialog closes and the user is removed from the security profile.

Inheriting and Overriding Security Permissions

When you assign a user to a security profile, the user automatically inherits equivalent permissions on all lower-level objects. For example, if you assign a user to the Architect profile at the highest level in the object class hierarchy (the mart level), the user is automatically assigned Architect-level permissions for all object classes below it (in AllFusion ERwin DM: Library, Model, and Subject Area).

You can override the inherited security profile at a lower level for any user by simply changing the security profile of the lower level object you choose. A security profile assigned to a specific object overrides any security permissions inherited from a higher-level object class.

If you assign a user to a new security profile for an object in the mart object class hierarchy (for example, a model), the user retains all permissions granted by other security profiles, except for the permissions that the new security profile overrides.

By default, both the Viewer and Guest security profiles are read-only security profiles at the mart level. When a user is assigned to a read-only security profile, the permissions defined in that profile are automatically applied to all lower object classes in the mart object class hierarchy.

While you can assign the Viewer profile to limit the permissions of a user in a particular object class, it is better to use the Guest profile exclusively for users that use AllFusion MN to access AllFusion MM. The Guest security profile does not count toward your license limit.

Note: To add, change, or delete a security profile, you must be assigned to the Administrator security profile for the mart.

Add a Security Profile

You can control access to objects and what tasks users can perform using security profiles. Workgroup member's roles and responsibilities may change from project to project. The security features provide control over how team members work together. Security is profile-based and you can add a security profile to restrict access to data in AllFusion ERwin Data Modeler by library, model, entity, and subject area; and in AllFusion Process Modeler by library and model.

To add a security profile

1. Click Security on the Services menu.

   The Security Manager dialog opens.

2. Click Profile.

   The Security Profile Manager dialog opens.

3. Click New.

   The Profile Name Editor dialog opens.

4. Enter the name of the new profile in the Name text box, the profile description in the Description text box and click OK.

   The Profile Name Editor dialog closes.

5. Select the object class in the Object Class list and select or clear the check boxes in the Permission list and click OK.

   Note: By default, new profiles have no permissions. Permissions are granted or denied for each object class in the new profile. Repeat for each object class to which you want to assign permissions.

   The Security Profile Manager dialog closes.

Note: You must be assigned to the Administrator security profile for the mart to add, update, or delete a security profile.

Modify a Security Profile Name or Description

You can control access to objects and the tasks users can perform. Workgroup member's roles and responsibilities may change from project to project, and the security features provide control over how team members work together. Security is profile-based and you can modify a security profile to restrict access to data in AllFusion ERwin Data Modeler by library, model, entity, and subject area; and in AllFusion Process Modeler by library and model.

To modify a security profile

1. Click Security on the Services menu.

   The Security Manager dialog opens.

2. Click Profile.

   The Security Profile Manager dialog opens.

3. Select the profile that you want to modify in the Security Profile list and click Edit Profile.

   The Profile Name Editor dialog opens.

4. Modify the profile name or description and click OK.

   The name or description is updated and the Profile Name Editor dialog closes.

Note: You must be assigned to the Administrator security profile for the mart to add, update, or delete a security profile.

Change a Profile Name

You can change the name of an existing profile.

To change the name of a profile

1. Select Security from the Services menu.

   The Security Manager dialog opens.

2. Click the Profile button in the Security Manager dialog.

   The Security Profile Manager dialog opens.

3. Select the profile you want to rename and click Edit Profile.

   The Profile Name Editor opens.

4. Edit the name and click OK.

   The profile has been renamed and the Profile Name Editor closes.

Change a Profile's Permissions

You can change the permissions associated with a security profile.

To change the permissions associated with a security profile

1. Select the profile (for example, architect) and click the appropriate object class (for example, mart),
   - To grant permission to perform an activity, select the permission box.
   - To remove permission to perform an activity, clear the permission box.

   Important! Changing the Guest security profile is not permitted.
2. Click OK.

   The permissions are updated for that security profile.

Override a User's Inherited Security Permissions

You can override the security permissions automatically inherited by all permission object classes lower in the class hierarchy by the security profile you assign.

To override a user's inherited security permissions

1. Click Security on the Services menu.

   The Security Manager dialog opens.
2. Click Profile.

   The Security Profile Manager dialog opens.
3. Select the object class or individual object for which you want to override the user's inherited security permissions in the Object list, select or clear the permissions, and click OK.

   The dialog closes and the inherited security permissions are overwritten.

Delete a Security Profile

Security is profile-based and you can delete a security profile to restrict access to data in AllFusion ERwin Data Modeler by library, model, entity, and subject area; and in AllFusion Process Modeler by library and model.

To delete a security profile

1. Click Security on the Services menu.

   The Security Manager dialog opens.

2. Click Profile.

   The Security Profile Manager dialog opens.

3. Select the security profile that you want to delete in the Security Profile list and click Delete.

   The security profile is removed from the list.

4. Click OK.

   The Security Profile Manager closes and the security profile is deleted.

Note: You must be assigned to the Administrator security profile for the mart to add, update, or delete a security profile.

Chapter 3: Sessions

This section contains the following topics:

Sessions

When a user logs on to the mart, this event is recorded as the start of a *session*. During a session, the models that a user opens and the current lock mode of a model are tracked. Each session has its own Action Log, contained within AllFusion ERwin Data Modeler, which logs the transaction information containing real time changes made to a model. Once you have logged out, the Action Log is cleared.

As the administrator, you may need to terminate a user's session so that other users can access models locked by that user. The administrator can perform this task directly or assign another user the appropriate security permission to terminate user sessions. For example, if a user is working offsite on a model and has locked the corresponding model, you can terminate the user's session to unlock the model so that others can access it.

Terminate a User Session

You can terminate a user's session from the Session Manager. You can release the model lock by terminating the user's session. Terminating a session prevents the user from saving current changes back to the mart. You are asked to confirm that you want to terminate all locks held by the selected user. Any locks placed on the models opened by that user are removed and the session is terminated.

Note: You must be assigned to the Administrator security profile to terminate a session.

To terminate a session

1. Click Session from the Services menu.

   The Session Manager opens.

2. Select a user in the Users list and click Terminate.

   Any locks the user placed on models are removed and the selected session is terminated.

Interrupted Session

If you experience a system failure, all model locks are removed and the user session is terminated. When you log back into the mart after a system failure, a new session begins and you are informed if you proceed, the previous connection will be terminated.

Chapter 4: Libraries

This section contains the following topics:

Plan Your Library Structure

Before you set up your library structure in the Library Manager, you should review how the workgroup modeling process works in your organization. To help you review your workgroup modeling process, answer the following questions:

- Do you plan to use both AllFusion ERwin DM and AllFusion PM?
- If using AllFusion ERwin DM and AllFusion PM with AllFusion MM, do you plan to share entities and attributes with AllFusion ERwin DM and AllFusion PM models?
- How will AllFusion ERwin DM models be moved from the development library to the production library?
- How will your approval process for moving models be documented and enforced?
- How will AllFusion ERwin DM models be merged into the enterprise model and who will control this process?
- Will you use versioning to record a model's milestones?
- Who will have what type of access to each library?
- Will AllFusion ERwin DM models be generated to multiple target environments (such as Microsoft SQL Server and Oracle)?
- How will you be warehousing your data?

Determine Your Lifecycle Framework

Use one of the following model lifecycle frameworks you use in your organization:

Model-Driven Development

Changes to the schema are made to the model first and then forward engineered.

System-Driven Models

Changes are made directly to the schema and the schema is reverse-engineered into the model to reflect the changes.

Informational Models

Contains logical-only models, enterprise-wide models, or standards and sample models.

Business Process Models

Contains models generated by AllFusion PM.

Consider Your Library Structure

Each type of framework has different considerations that you need to think about when configuring your database and developing its supporting policies. You are not required to choose a particular framework, however, it helps to know your development process before building a library structure.

Depending on the framework, you should consider any or all of these suggestions when building a library structure:

Practical library names

Use practical and functional library names that help all users understand the purpose and type of models contained in the library. For example, you can use the popular format: Short System Name+Version+Stage (for example, Ora_8_Production).

Model naming and datatype standards (AllFusion ERwin DM)

Enforce naming and datatype standards, which is vital to efficient workgroup modeling.

Note: For more information, see the AllFusion ERwin Data Modeler Online Help.

Rules for model promotion

Define a rigid and documented model approval and promotion process using different libraries for each development phase.

Rules for model versioning

Define versioning rules using different libraries for each development version (for example, Development Beta 1).

User rights and security

Apply stricter rights to libraries that contain mature models nearing the latter stages of development. You can also apply strict rights to individual models.

Publication

Generate reports to communicate milestones in the model development process.

Schema generation rules (AllFusion ERwin DM)

Set up a library where you generate the model schema. Normally, you generate the model schema of promoted models only in the latter stages of development.

Suggested Lifecycle for the Model-Driven Development Framework

In the model-driven framework, the model is always the source of all changes. You create a new database schema by forward engineering the model. The life cycle of a model in the model-driven Development framework may follow a path like this:

- Create the library structure (for example, Development, Test, and Production) and populate them with AllFusion ERwin DM templates.
- Create the logical model in a development library.
- Promote the model to the test library when it is ready.
- Generate the schema from the test library.
- Modify the test model as required and synchronize it to the schema.
- Promote the model to the production library when it is ready.
- Publish the refreshed production model.
- Update the enterprise-wide model, if necessary.
- Incorporate changes into the development model for further changes, and repeat the process.

Suggested Lifecycle for the System-Driven Model Framework

In the system-driven framework, there is an established information system from which you can reverse engineer database tables. The life cycle of a model in the system-driven Development framework may follow a path like this:

- Create the library structure (for example, Reverse Eng, Test, Production). You should not require AllFusion ERwin DM templates since you do not create models from scratch.
- Reverse engineer the model from the information system into the designated library.
- Enhance the model with logical information and input from analysts.
- Update the model to reflect changes in the physical schema.
- Create a version of the model.
- Synchronize the schema and the model using Complete Compare.
- Publish the model.
- Repeat steps 5 through 7 as the system is modified.

Suggested Lifecycle for the Informational Model Framework

In the Informational Model framework, AllFusion MM contains AllFusion ERwin DM logical-only models, enterprise-wide models, or standards and sample models. There is no forward engineering with the intent of using the schema. The life cycle of a model in the Informational Model framework may follow a path like this:

- Create the library structure and populate them with AllFusion ERwin DM templates.
- Develop the initial model. Use reverse engineering and model new components as required.
- Publish the initial model to the appropriate parties for modification and refinement.
- Get approval, and then version the model.
- Publish the approved model.
- Update and publish models as the enterprise model evolves.

Suggested Lifecycle for the Business Process Model Framework

In the Business Process Model framework, you use AllFusion PM to design business process models that define business processes in your organization. You can optionally export entities and attributes to AllFusion ERwin DM to develop a model-driven information system that adheres to the business process rules. The life cycle of a model in the Business Process Model framework may follow a path like this:

- Create a working version of an AS-IS model of selected subjects.
- Critique and analyze the model.
- Move the model through draft, recommended, and publication versions.
- Publish the model at the end of the cycle.
- Create working TO-BE models of the model from Step 4 that incorporates management's future vision.
- Update the model as changes and enhancements are approved and as support systems are integrated into the models.
- Version the modified models based upon the approval of the changes and enhancements.
- Publish the revised models when each version becomes stable.

Move Models into Production

During the model development lifecycle, it is vital that you have an organized library structure so that only those models intended for production are moved to that level. You should structure your libraries into at least three distinct types:

Development Libraries

Contains models that are being created or updated.

Test Libraries

Contains finished models that are being tested prior to moving them to production.

Production Libraries

Contains the finished models that were tested and debugged.

After you have created your libraries, determine the security levels for each library. The following three examples should give you an idea of how you can use libraries and security together to help safeguard the project models:

- The entire modeling team can have access to the development library and read-only access to the test and production libraries. Authorized project leaders can be assigned to move models from the development library to the test library, and then from the test to the production library.
- Models from other libraries (for example, Sales and Accounting) can be merged from their own libraries in the enterprise model. Modelers working on projects in the Sales or Accounting libraries can have read-only access to the enterprise library and full access to their own projects. Assign one person or group to manage integration into the enterprise model.
- Modelers need full access to their own libraries and read-only access to the libraries of others. This type of security enhances production since everyone can see what everyone else is working on, all models are stored in one location, and permissions can be changed as different collaborations among modelers become necessary.

Libraries

Libraries are used to store AllFusion ERwin DM and AllFusion PM models that can be shared by users. Libraries can help you organize projects by grouping models together. For example, you can create a library to store models shared by a workgroup, security level, or target server. There is no limit to the number of libraries you can create, and there is no limit to the number of models you can store in a library. By organizing your business process models and data models in libraries, you can also easily manage model merging and conflict resolution.

The administrator must create libraries and determine how to structure AllFusion MM for their organization. The administrator can also grant security permission to allow other users to create, update, or delete a library. Libraries are managed in the Library Manager in the client product when connected to AllFusion MM. To open the Library Manager, choose Library from the Services menu.

Non-Archiving Libraries

You can enable the creation of models which do not retain multiple versions.This option is determined for each library. Libraries which do not retain older model versions are called non-archiving libraries. This is managed at the library level from the Library Manager. The default setting is to retain multiple model versions in the library.

For non-archiving libraries, when three-way saves occur, meaning when two or more users modify the same model simultaneously, the original model is not preserved, as the Resolve Differences session cannot show whether the left model or right model changed. You can not mark non-versioning models.

Create a New Library

You can create a new library to help you organize projects by grouping models together or to limit access. You use the Library Manager to create a new library.

To create a library

1. Click Library on the Services menu.

   The Library Manager dialog opens.

2. Select the mart name in the tree control, and type the new library name in the Name box and click Create.

   Note: The Maintain multiple versions of models in this library check box is selected by default. Clear this check box if you do not want to maintain versioning for this library (non-archiving library).

   The new library is added to the AllFusion MM mart.

3. Click the Detailed button, and type a description in the Description box.

   The Details window opens, which shows when the library was created and by whom and any active sessions.

4. Click the Brief button.

   The Details window closes.

5. Click Close to exit.

   The library is created and the Library Manager dialog closes.

Rename a Library

You can rename a library if the name no longer suits the data in the library. You cannot delete a library that has open models.

To rename a library

1. Click Library from the Services menu.

   The Library Manager dialog opens.

2. Select the library that you want to rename in the Library list, enter the new library name in the Name text box, and click Update.

   A confirmation dialog opens.

3. Click Yes to confirm.

   The library is renamed.

Delete a Library

If a Library is no longer in use, for example a test environment, you can delete it. When you delete a library, all of the models in the mart that belong to that library are also deleted. To preserve a model before you delete the library in which it is stored, you can save the model as an .erwin file. Alternatively, you can save the model in a different library. You cannot delete a library that has open models.

To delete a library

1. Click Library from the Services menu.

   The Library Manager dialog opens.

2. Select the library that you want to delete in the Library list and click Delete.

   A confirmation dialog opens.

3. Click Yes to confirm.

   The library is deleted.

Rename a Model

You can rename a model if the name no longer properly identifies the data. For example, if you want to rename a test model to a production model.

To rename a model

1. Click Library from the Services menu.

   The Library Manager dialog opens.

2. Select the model that you want to rename in the Directory list, enter a new name for the model in the Name text box, and click Update.

   A confirmation dialog opens.

3. Click Yes to confirm.

   The model is renamed.

Delete a Model

You can delete a model that is no longer in use. You cannot delete an open model.

To delete a model

1. Click Library from the Services menu.

   The Library Manager dialog opens.

2. Select the model you want to delete in the Directory list and click Delete.

   A confirmation dialog opens.

3. Click Yes to confirm.

   The model is deleted.

Chapter 5: Reports

This section contains the following topics:

Reports

Users typically work from a common set of libraries, models, and submodels, and must be able to share information about these objects with other users. One way to share information is by using reports, which detail the information and definitions for a model in a tabular format.

All users can run a number of reports in the Data Browser to view the contents of specific libraries and models, and use standard and customized reports to see model information in more detail. However, there are two specific reporting tasks that the administrator performs:

- Creating Security Manager reports
- Creating shared AllFusion ERwin DM reports

The administrator can use the Data Browser, a reporting module, to run and customize reports against the AllFusion MM mart. For example, the administrator can generate Security Manager and shared reports.

Administrative Reports

The General folder contains administrative reports organized by object class (such as Global and Diagram). The reports in each class run across the entire contents of that class and library. This folder appears in the tree control when you are connected to the mart.

As the administrator, you can use many of the reports in the General folder to help you manage the mart. For example, Global reports let you view information about existing model locks, open objects, and users.

After you run a report and generate a result set, you can:

- Use the Data Browser search features to find information in the result set
- Specify a search expression for one or more columns so that the Data Browser finds only the result set rows that satisfy all of the search expressions
- Find a change of value in a column
- Hide result set rows that do not match the search

Generate an Administrative Report

You can customize the content and appearance of the result set, after you run a report, and create and save your own custom report views.

To generate an administrative report, double-click any report name associated with the report icon. The name of the result set returned by the report is displayed below the original report, and the results appear in the Result Set Area.

Security Manager Reports

The Security Manager report provides information about the security profiles assigned to each user and the permissions associated with those profiles. A predefined security report is provided. The result set shows the following information:

User

The name of the user (for example, JSMITH).

Object Name

The Object Name is always Current Mart for a Security Manager Report.

Profile Name

The security profile name (for example, Administrator).

Profile Description

A description of the security profile (for example, Administrator).

Application

The name of the client application.

Permission

The name of the security permission (for example, Create Library).

Granted

The permission status; 1 indicates the permission is granted, 0 indicates the permission is not granted.

Generate a Security Manager Report

The Security Reports Folder contains a single report that you can generate to view information about the security profile assigned to each user and the permissions granted in each security profile. This folder appears in the tree control only when you click Report in the Security Manager dialog.

After you generate the report you can use the Data Browser features to customize the appearance of a result set, find one or more specific items in the result set, print the result set, or export the result set to HTML or other formats.

Note: You can also generate a report listing the changes you have made using the Security Manager.

To generate a Security Manager report

1. Click Security from the Services menu.

   The Security Manager dialog opens.

2. Click Report to open the Data Browser.

   The Data Browser dialog opens.

3. Expand the Security Reports folder.

   The reports are listed in the Security Reports folder.

4. Double-click the Security Report you want to run.

   The Security Manager report is generated.

Share AllFusion ERwin DM Reports in AllFusion MM

You can use the Data Browser to select individual AllFusion ERwin DM reports for company-wide use. The first time you save an AllFusion ERwin DM report in AllFusion MM, the Data Browser creates a top-level folder called Volume Reports. When you copy a report, the Data Browser keeps the folder structure associated with a report and lists it under the Volume Reports folder.

Note: Users who have the Data Browser open when a change is applied do not see the change immediately. The change appears when they reopen the Data Browser.

A user with an Administrator security profile can:

- Create, edit, and delete a shared AllFusion ERwin DM report.
- Create a new report folder to store result sets.

Note: Version and merging features are not provided for reports. If multiple administrators are editing and saving shared AllFusion ERwin DM reports to AllFusion MM, changes may be overwritten.

Create Shared Reports

The first time an administrator saves an AllFusion ERwin DM report in AllFusion MM, the browser creates a new folder called Shared AllFusion ERwin DM Reports. When a report is copied, the browser keeps the folder structure associated with a report and lists it under the Shared AllFusion ERwin DM Reports folder. For example, when the Attributes Report is saved to AllFusion MM, it becomes the Shared AllFusion ERwin DM Reports/Attributes Report.

To create a shared reports

1. Log on to the AllFusion MM mart and click Data Browser on the Tools menu.

   The Data Browser opens.

2. If the report you want to save in AllFusion MM appears in the active AllFusion ERwin DM Reports (.erp) file, you can copy them to AllFusion MM by selecting the report in the tree control and choosing the Copy Report to AllFusion MM option on the Reports menu.

   The report is saved to AllFusion MM. It can be accessed by other AllFusion MM users.

Note: If you are having trouble locating the report you want to share, it may not be in the active .erp file. Locate the .erp file containing the report by choosing Open Report File from the Reports menu and specifying the path and file name of the .erp report you want to open.

Modify a Shared Report

You can modify the contents, sort order, or format of a shared report.

To modify a shared report

1. Log on to the AllFusion MM mart that contains the shared report you want to modify, and click Data Browser on the Tools menu.

   The Data Browser opens, and the report names display in the folders.

2. Right-click the report name and choose Edit Report from the popup menu.

   The Reports dialog opens.

3. Select or clear the check boxes in the Options tab.

   The shared report is modified.

Note: Users who have the browser open when a change is applied do not see the change immediately; the change appears when they reopen the browser.

Copy a Shared Report

You can copy a shared report from AllFusion MM to a local AllFusion ERwin DM folder.

To copy a shared report from AllFusion MM to AllFusion ERwin DM

1. Log on to the AllFusion MM mart that contains the shared report you want to copy, and click Data Browser on the Tools menu.

   The Data Browser opens, and the report names display in the folders.

2. Select the report and choose Copy Report to a local file from the Reports menu.

   The selected report is copied to the AllFusion ERwin DM Reports folder.

Delete a Shared Report in the AllFusion ERwin DM Reports Folder

You can delete a report in the Shared AllFusion ERwin DM Reports folder if you no longer want to share it.

To delete a report in the shared AllFusion ERwin DM Report folder

1. Log on to the AllFusion MM mart in which you want to delete the report, and click Data Browser on the Tools menu.

   The Data Browser opens.

2. Expand the AllFusion ERwin DM Reports folder, select the report name you want to delete and click the Delete key.

   The report is deleted from the Shared AllFusion ERwin DM Reports folder.

Index