



Autodesk® FMDesktop™ 2009

Autodesk®

Facility Manager
Security Guide

Customer and Administration Building, Ditzingen, Germany - Design by Barkow Leibinger Architects

Copyright © 2003 - 2008 Autodesk, Inc.

Table of Contents

1 Introduction	3
Methods of Security	3
2 Share-Level Security	5
Implementing Share-Level Security	5
Removing Share-Level Security	6
3 User-Level Security	7
4 Alternate Methods of Securing Facility Manager	8
Microsoft Access 2003 Runtime Files.....	8
Hiding Form Components	8
Removing Reports from Facility Manager	9

1 Introduction

Security in Facility Manager is handled through the built-in functions of Microsoft® Access™, a component of Microsoft® Office®. It is beyond the scope of these instructions to describe Microsoft Access database security and all of its concepts and nuances in great detail. Autodesk strongly recommends that you consult outside resources, such as Microsoft Access on-line help, related reference books, and the Microsoft website for a more complete understanding of Microsoft Access security. Keep in mind that implementing security in Facility Manager is not the same thing as implementing security on your computer or network. Facility Manager can only be as secure as the environment in which it is used. The forms of security described in this document are not intended to be a substitute for system and network security.

The Facility Manager application consists of these components:

- **Facility Manager** - The user interface of the application. It is used to view, query, markup, report on, print, and publish facility drawings and associated data or documents. Facility Manager allows users to plan, track, and manage project and move information. Project, move, and maintenance related work requests can be managed as well.
- **FMDesktop Database** - The database component of Facility Manager and the central component of the entire FMDesktop suite. It is used to store all of the facility data as well as links to related documents and drawings.
- **Facility Manager Resource Folders** - The shared object storage component of the FMDesktop suite. They are used to store the drawings, graphics, documents, reports, and other resources used by all of the components of FMDesktop.

Important: Do not implement Microsoft Access security on the FMDesktop database (FMData.mdb). Facility Manager contains all of the Microsoft Access database objects (for example, queries, forms, reports, macros and modules) and links to the data tables in the FMDesktop database. Make sure that all users will be able to link to FMData.mdb by assigning Open/Run permission for the database to all users and groups.

Methods of Security

There are two basic forms of Microsoft Access security that can be implemented for Facility Manager:

- **Share-Level Security (Setting a Database Password)** – to control who can open the program.
- **User-Level Security** – to control the use of specific Facility Manager features by authorized users.

There are some other methods that can be used to secure the Facility Manager program. They are described in detail in the section of this document called Alternate Methods of Securing Facility Manager.

The most powerful and flexible method of protecting Facility Manager is User-level security, but the complexity of User-level security (and the time you will invest maintaining it) may be more than your organization needs. Additionally, you must have Microsoft Access 2003 or higher installed on at least one computer to implement User-level security for Facility Manager. Please review all security options before deciding which type of security is best suited for your organization's needs.

Note: Assistance with setting up User-level security is considered customization and is subject to current pricing for customization services. Customization services are separate from Technical Support services and are not included as part of any Technical Support package offered by Autodesk. For information about customization services, see Professional Services in the Facility Manager online help or User's Guide.

2 Share-Level Security

Share-level security, or setting a database password, is an easy way to prevent unauthorized users from opening Facility Manager. Share-level security is easy to implement and maintain. Authorized users are required to enter a password before opening Facility Manager. Unauthorized users are unable to open the program. Once an authorized user has opened Facility Manager, however, Share-level security cannot restrict what program features that user can access.

Implementing Share-Level Security

- 1) Close Facility Manager. If the program is being used on a network, make sure no other users have the program open.
- 2) Make a backup copy of the Facility Manager 2009.mdb file, and store it in a secure place.
- 3) Open Facility Manager for exclusive use.
 - **If you are using Access Runtime files**, add the /excl extension to the program shortcut.
 - **If you are using the full version of Access**, click File>Open, select Facility Manager 2009.mdb, click the arrow next to the Open button, and then click Open Exclusive. Hold down the SHIFT key, and click the Open button.
- 4) After the program opens, click Tools>Security, and click Set Database Password.

Note: If the Security option is not displayed on the Tools menu, press the **Alt, Shift, and S** keys at the same time.

- 5) For Password, enter your database password. (Passwords are case-sensitive.)
- 6) For Verify, re-enter your password, and click OK. Your Facility Manager database password is set.
- 7) Each time a user tries to open Facility Manager, a dialog displays requesting the database password.

Note: Write down your database password and keep it in a safe place. If your database password is lost or forgotten, you cannot open Facility Manager or retrieve the information contained in the program. If you are using Access Runtime files, remove the /excl extension from the program shortcut to allow other users to open the program.

Removing Share-Level Security

After you have implemented Share-level security for Facility Manager, the Set Database Password option on the Tools>Security menu changes to Unset Database Password. To remove Share-level security:

- 1) Open Facility Manager for exclusive use.
 - **If you are using Access Runtime files**, add /excl to the program shortcut.
 - **If you are using the full version of Access**, click File>Open, select Facility Manager 2009.mdb, click the arrow next to the Open button, and then click Open Exclusive. Hold down the SHIFT key, and click the Open button.
- 2) On the Access menu, click Tools>Security, and click Unset Database Password.

Note: If the Security option is not displayed on the Tools menu, press the **Alt, Shift,** and **S** keys at the same time.

- 3) For Password, enter the current password.
- 4) Click OK.
Your Facility Manager database password is now removed.
- 5) You can now open Facility Manager without entering a password.

3 User-Level Security

Assistance with setting up User-level security is considered customization and is subject to current pricing for customization services. Customization services are separate from Technical Support services and are not included as part of any Technical Support package offered by Autodesk. For information about customization services, see Professional Services in the Facility Manager online help or User's Guide.

It is beyond the scope of these instructions to describe Access User-level security and all of its concepts and nuances in great detail. Autodesk strongly recommends that you consult outside resources (for example, Access on-line help, Access reference books, and the Microsoft website) for a more complete understanding of User-level security.

It is crucial that you understand Access User-level security before you begin implementing it for Facility Manager. Implementing User-level security is a complex and time-consuming process. Considering the time involved, it may be more security than your organization requires for a software program. Please review all of your options before implementing User-level security for Facility Manager.

User-level security is the most flexible and secure method of protecting the sensitive data, code, and the design of objects in Facility Manager. With User-level security, you control what users and groups of users can do in the application.

After establishing User-level security:

- Facility Manager users are required to log on using unique accounts and passwords. The password confirms the user's identity by checking the name and password against data in the workgroup information file.
- The functions the user can perform in the secured program are dependent on the permissions you have assigned to that user. Permissions can be granted or denied for any object in Facility Manager.

4 Alternate Methods of Securing Facility Manager

There are several alternative methods for securing Facility Manager:

- 1) **Opening Facility Manager Using Access Runtime Files** – Runtime files do not allow users to go into Design View.
- 2) **Hiding Form Components** – Use Access to hide fields, command buttons, drop-down lists, and other objects on Facility Manager forms.
- 3) **Removing Reports from Facility Manager** – Remove selected reports from the Facility Manager database to prevent users from seeing the information contained in them.

Microsoft Access 2003 Runtime Files

When you install Facility Manager, you can also install Access 2007 Runtime files to your computer. The Runtime files are scaled-down versions of Access 2007 that allow users who do not have a full installation of Access 2007 on their computers, to open Facility Manager. **You cannot customize Facility Manager using the Access 2007 Runtime files.** It is not necessary to have Access 2003 or higher installed on every user's computer. Ideally, you will have only one person in your organization that is in charge of maintaining security and customization for Facility Manager. It is only necessary that Access 2003 or higher be installed on this user's computer. The Facility Manager shortcuts on the Windows Start menu are configured to open the programs using the Runtime files.

Hiding Form Components

Hiding form components is an easy way to deny users the ability to view selected objects on the Facility Manager forms. You can hide any object on the forms, including fields, labels, drop-down lists, command buttons, pages, or the entire form. Hiding a component involves changing the value of a component's **Visible** property from Yes to No. Because forms must be opened in Design View to hide their components, **you must have Access 2003 or higher installed on your computer** and use it to open the MDB version of the program file.

- 1) Open Access and use it to open Facility Manager 2009.mdb.
- 2) Open the form that contains the component you want to hide.
- 3) Go to Design View.
- 4) Double-click the component you want to hide to open its Property form.
- 5) Double-click the **Visible** property located on the Format tab to change the value from Yes to No.
- 6) Close the Property form.
- 7) On the Access toolbar, click Save to save the new settings.
- 8) Go to Form View and the component is no longer visible in Facility Manager.

Removing Reports from Facility Manager

Removing and deleting reports from the Facility Manager program file is a good way to prevent unauthorized users from accessing sensitive reports. You can remove reports from the Select Report(s) drop-down list using the **Remove** button on the Report form, but doing so does not permanently delete them. **You must open Facility Manager using Access 2003 or higher and delete the reports from the database container to remove reports permanently.** You can import them from the original program file if you want to add them back later.