Securing your data in FileMaker Pro web publishing

Overview

FileMaker Pro databases can be published to the Web or to an intranet by using either *FileMaker Pro Instant Web Publishing* or *FileMaker Pro Custom Web Publishing*.

- FileMaker Pro databases published using Instant Web Publishing must use FileMaker Pro access privileges for Web/intranet security.
- FileMaker Pro databases published using Custom Web Publishing can use either FileMaker Pro access privileges or the FileMaker Pro Web Security Database for Web/intranet security.

FileMaker recommends that you follow the security setup instructions in this document for the publishing method you intend to use.

FileMaker is continually evaluating security considerations and procedures for the FileMaker product line. This document contains the most current procedures and is subject to change without notice. Any and all updates of this document will be available for download from the FileMaker web site, http://www.filemaker.com.

Important This document does not explain how to prepare your databases for web publishing. For more information about Instant Web Publishing, see the FileMaker Pro *User's Guide*. For more information about Custom Web Publishing, see either the FileMaker Developer *Developer's Guide* or the FileMaker Pro Unlimited *Administrator's Guide*.

Protecting data for FileMaker Pro Instant Web Publishing

To secure your database for FileMaker Pro Instant Web Publishing, you must use FileMaker Pro access privileges to define one or more passwords for users who will be accessing your database over the Web/intranet.

Important When you use access privileges as the only means of securing your database, any valid password is potentially available for use when guests access your database over the Web/intranet. The FileMaker Pro Web Companion permits you to enter any password defined in your database. If someone is aware of a valid password, they can enter that password through a browser's password dialog box. This includes master passwords, which provide access to the entire file. Even if you define unique passwords for Web-only users, there is no way to disable your master password(s). Make sure that any master passwords you define are difficult to guess and are known only to those who need to use them. As FileMaker Pro access privileges are the only means of providing security through Instant Web Publishing, you should use Custom Web Publishing and the Web Security Database if you require a greater level of security.

For more information about FileMaker Pro access privileges, see the FileMaker Pro *User's Guide* and the FileMaker Pro online Help.

Defining passwords

To define a web access password using FileMaker Pro access privileges:

1. Open your database file, then choose File menu > Access Privileges > Passwords.

If you see the Change Password command instead of the Access Privileges command, you have opened the file with a password that provides limited access. To create additional passwords, you must reopen the file with a master password.

2. In the Define Passwords dialog box, type a password in the Password text box.

If you want web users to have access to your database without being prompted for a password each time they access it, you can define a *blank* or empty password. This password can be given the same restrictions as any other password, for example, no modification or deletion privileges.

When users access a database that contains a blank password from the Instant Web Publishing home page, they will not be prompted for a password and will automatically be assigned the blank password's privileges. This minimizes the ability to use master passwords. It also provides a way for all web users to access the database without being given passwords in advance. The disadvantage is that users who do need to log in with an alternate password will not be able to do so.

3. Select the privileges associated with this password.

4. Click Create.

If a master password with full access has not already been defined, you must define one before exiting this dialog box.

5. Click Done.

Note If the password limits browse privileges but does not limit the privilege to delete records, it is possible for users to delete records they cannot view. If FileMaker Pro detects this situation, it will display an alert when you create the password, but it will not prevent you from creating the password.

Specifying access privileges as the security method for Instant Web Publishing

After you have defined a web access password, verify that FileMaker access privileges will be the security method used with Instant Web Publishing.

1. Choose Edit menu > Preferences > Application.

2. In the Application Preferences dialog box, click the Plug-Ins tab.

3. Select the Web Companion Plug-In from the list, then click Configure.

4. In the Web Companion Configuration dialog box, make sure that FileMaker Pro Access Privileges is selected.

5. You can also restrict database access to certain client IP addresses. When the Restrict access to IP address(es) box is checked, only those IP addresses specified (explicitly or through wildcards) in the accompanying text box will be granted web access.

This restriction will apply to all databases. Access privileges will still be enforced for those IP addresses that are granted access.

6. Click OK.

7. Click OK in the Application Preferences dialog box.

Record-by-record protection for Instant Web Publishing using FileMaker Pro access privileges

You can use record-by-record access privileges in FileMaker Pro 5.5 to specify passwords that limit the ability of web users to browse, edit, or delete specific records.

You can limit users' access to records based on their department within a company, their job position, or other criteria. For example, if you have a database accessed by managers and salespeople, you can provide different levels of access to these users.

Each record in the database includes the field AccessType, and this field has the value of either `Manager` or `Sales`, thereby determining which group has access to the record. Users who are part of the Sales group will be allowed to access only those records where AccessType has the value of `Sales`. Users who are part of the Manager group will be allowed to access both types of records, where AccessType has the value of either `Sales` or `Manager`.

Here's an example of setting limited access to certain records in a database:

1. Choose File menu > Define Fields.

2. Type `AccessType` into the Field Name area, verify that the field type is Text, and click Create.

This field will store the access type for each record.

3. Click Done.

4. Choose File menu > Access Privileges > Passwords.

Note If you see the Change Password command instead of the Access Privileges command, you have opened the file with a password that provides limited access. To create the additional passwords explained in this example, you must reopen the file with a master password. If your database does not have any passwords defined, you will need to define a password with full access privileges before continuing. See the FileMaker Pro *User's Guide* or the FileMaker Pro online help for more information.

5. Type `sales_password` in the Password area. Do not click Create.

6. In the Privileges area, verify that Browse records is selected.

7. Choose Limited from the list next to the Browse records privilege.

8. In the Specify calculation dialog box, type the calculation:

```
AccessType = "Sales"
```

This calculation will determine if access is granted to this record. Access is allowed if the result of the calculation is True, and access is denied if the result of the calculation is False.

9. Click Done to save the calculation.

10. Repeat steps 5 through 8 to create the same level of limited access for record editing and record deletion privileges.

11. Click Create to create the password "sales_password" with the privileges described above.

12. Define the manager password by typing `manager_password` in the Password area. Do not click Create.

13. In the Privileges area, select Browse records.

14. Choose Limited from the list next to the Browse records privilege.

15. In the Specify calculation dialog box, type the calculation:

```
AccessType = "Sales" OR AccessType = "Manager"
```

This calculation will determine if access is granted to this record. Access is allowed if the result of the calculation is True, and access is denied if the result of the calculation is False. In this case, access will be allowed if the field AccessType contains either the value "Sales" or the value "Manager."

16. Click OK to save the calculation.

17. Repeat steps 12 through 15 to create the same level of limited access for record editing and record deletion privileges.

If a master password with full access has not already been defined. you will need to define one before exiting this dialog box.

18. Click Create to create the password "manager_password" with the privileges described above.

19. Click Done.

20. In the Security area of the Web Companion Configuration dialog box, verify that security is set to FileMaker Pro Access Privileges as described in "Specifying access privileges as the security method for Instant Web Publishing" on page 2.

21. In each record of your database, set AccessType to either `Sales` or `Manager`, as appropriate.

When users access your database over the Web, they will only be permitted to browse, edit, and delete the records to which their password gives them access. In Instant Web Publishing, when a user does not have browse access to a particular record, the record will be shown, but <No Access> will be placed in all fields. If a user does not have delete or edit record privileges, those commands will be removed from the navigation bar.

Specifying default layouts in databases published with Instant Web Publishing

Although not necessary, it will be easier for you to manage the Web security of your database(s) if you create web-only layouts for table view, form view, and searching, and specify these layouts as the defaults for these activities. These layouts should contain just the fields you intend to use for each of these functions.

To specify default layouts using Instant Web Publishing:

1. Choose File menu > Sharing.

2. In the Companion Sharing area, select Web Companion, then click Set Up Views.

3. Select the Table View tab.

4. In the Choose layout for browser viewing area, select a layout.

The layout you select will be used to generate the Instant Web Publishing "Table View" pages, so it should include only the fields you want web users to work with in Table View.

5. Select the Form View tab.

6. In the Choose layout for browser viewing area, select a layout.

The layout you select will be used to generate the Instant Web Publishing "Form View" pages, so it should include only the fields you want web users to work with in Form View.

7. Select the Search tab.

8. In the Choose layout for browser viewing area, select a layout.

The layout you select will be used to generate the Instant Web Publishing "Search" pages, so it should include only the fields you want web users to work with in Search View.

9. Click Done.

10. Click OK.

Note Layouts are not intended to be used as security measures. Limiting the fields that are displayed on web pages is part of a "best practices" approach, to minimize the accidental exposure of fields to users on Instant Web Publishing pages. Regardless of which layouts are used, all fields in the database are available to CGI requests from any web user, unless the proper access privileges are applied to restrict access on a field-by-field basis. For more information on field-by-field protection, see information in FileMaker Pro Help on defining groups.

Recommendations

On the Web, access privileges allow web users to perform authorized actions on all records in the database to which they have been granted access. For greater security, you should consider disabling edit and delete privileges for all passwords to be used on the Web for Internet users. If even more security is required, consider using Custom Web Publishing with the Web Security Database.

Review any scripts in your database. Even though a script cannot be used to perform an action prevented by a password, access privileges password protection does not prevent web users from running scripts using the CGI commands `&-script`, `&-script.prefind`, and `&-script.presort`. You need to ensure that any scripts defined in any databases you share over the Web/intranet will not perform inappropriate actions. It is safest to web publish from databases in which no scripts have been defined. Alternatively, if you need to disable the ability for web users to run scripts, you need to use Custom Web Publishing with the Web Security Database to define User Name and User Password pairs that do not have Script permissions.

Protecting Custom Web Publishing solutions

Custom Web Publishing with FileMaker Pro makes it possible to use XML and/or CDML tags to execute commands in FileMaker Pro. There are two methods of protecting Custom Web Publishing solutions: FileMaker Pro access privileges or the Web Security Database.

Using access privileges to protect Custom Web Publishing

Important When you use access privileges as the only means of securing your database, any valid password is potentially available for use when guests access your database over the Web/intranet. The FileMaker Pro Web Companion permits you to enter any password defined in your database. If someone is aware of a valid password, they can enter that password through a browser's password dialog box. This includes master passwords, which provide access to the entire file. Even if you define unique passwords for Web-only users, there is no way to disable your master password(s). Make sure that any master passwords you define are difficult to guess and are known only to those who need to use them. Use the additional protection of the Web Security Database if you require a greater level of security.

For more information about FileMaker Pro access privileges, see the FileMaker Pro *User's Guide* and the FileMaker Pro online Help.

Defining passwords

If you intend to use access privileges to protect your database, you must first define a password. Follow the instructions in "Defining passwords" on page 2, which are the same for both Instant Web Publishing and Custom Web Publishing.

Specifying access privileges as the security method for Custom Web Publishing

If you intend to use access privileges to protect your database, you must specify that it will be the security method used for Custom Web Publishing. Follow the instructions in "Specifying access privileges as the security method for Instant Web Publishing" on page 2, which are the same for both Instant Web Publishing and Custom Web Publishing.

Record-by-record protection for Custom Web Publishing using FileMaker Pro access privileges

You can use the built in record-by-record access feature in FileMaker Pro 5.5 to specify that web user passwords have only the limited ability to browse, edit, or delete specific records. Follow the instructions in "Record-by-record protection for Instant Web Publishing using FileMaker Pro access privileges" on page 3, which are the same for both Instant Web Publishing and Custom Web Publishing.

Using the Web Security Database to protect Custom Web Publishing

Use the FileMaker Pro Web Security Database to provide the most security for your Web/intranet published databases in Custom Web Publishing.

Configuring the Web Security Database

Before the Web Security Database can be enabled, you must configure it:

1. Open the database file to be protected, for example, MyDatabase.fp5.

2. Open Web Security.fp5.

This file is located in the FileMaker Pro 5.5/Web Security/Databases folder.

3. Create a new record in the Web Security Database.

4. Enter the filename `MyDatabase.fp5` in the Database Name field.

5. If you want to protect more than one file, create a separate record for each file.

6. (optional) If the file has a FileMaker Pro password whose restrictions you would like to add to those created in the Web Security Database, then enter that password in the Database Password field. If you leave this field blank, or enter the master password, no Access Privilege restrictions will be added to those used by the Web Security Database.

7. Enter a user name and password for each authorized user in the User Name and User Password fields.

8. Select the privileges for each user by enabling the appropriate checkboxes.

9. For fields that will have special restrictions, such as Don't Show, Read Only, or Don't Search, enter each field name separately under the Field Name column, and enable the appropriate Field Restrictions checkboxes.

Note Field restrictions will be applied to all users, and cannot be assigned on a user-by-user basis.

Enabling the Web Companion to use the Web Security Database

After you have configured the Web Security Database, you must select it for use in the Web Companion Configuration dialog box. To enable the Web Security Database:

1. Choose Edit menu > Preferences > Application.

2. In the Application Preferences dialog box, click the Plug-Ins tab.

3. Select the Web Companion Plug-In from the list, then click Configure.

4. In the Web Companion Configuration dialog box, select Web Security Database.

5. You can also restrict database access to certain client IP addresses. When Restrict access to IP address(es) is checked, only the IP addresses specified (through a literal IP address(es) or through wildcard combinations) will have web access.

Note Web Security Database restrictions will still be enforced for those IP addresses that are granted access.

6. Click OK.

7. Click OK in the Application Preferences dialog box.

Record-by record protection with the Web Security Database

To protect individual records with the Web Security Database:

1. Configure the Web Companion to use the Web Security databases, as described in the previous sections.

2. Open the database whose individual records you want to protect.

For example, if you want to protect records in MyDatabase.fp5, open that file.

3. Create a field to hold passwords for each record in the database.

For example, create a text field named PasswordField. Different values (passwords) can be placed into this field for different records. A user will need to know the password for a record to have access to that record.

4. In Browse mode, enter values that determine access in the PasswordField as appropriate for your needs.

For example, entering the phrase `MyPassword` in this field for a given record will require the user to enter `MyPassword` into that same field on a web form prior to submitting a search, edit, or delete request for the record.

5. In the Web Security Database, locate or create a record for MyDatabase.fp5.

6. In the record for MyDatabase.fp5, enter `PasswordField` in the Field Name column.

7. In the Field Restrictions column, select the security options for this field as described in the following sections.

Protecting records from being viewed

Use the following code to prevent restricted records from being displayed as the result of a Web-based search. Customize the VALUE tags for your databases, layouts, fields, and HTML pages.

To protect specific records from being viewed:

1. In the Web Security Database, select Exact Search for the password field.

2. In an HTML search page, enter commands similar to:

```
<FORM ACTION="FMPro" METHOD="post">
   <INPUT TYPE="hidden" NAME="-db" VALUE="MyDatabase.fp5">
   <INPUT TYPE="hidden" NAME="-lay" VALUE="Layout #1">
   <INPUT TYPE="hidden" NAME="-format" VALUE="SearchResults.htm">
...
<!-- List your search criteria here as you normally would. -->
...
   <INPUT TYPE="hidden" NAME="-op" VALUE="eq">
   <P>Password : <INPUT TYPE="text" NAME="PasswordField"
VALUE="">
```

```
...
<!-- List your other fields here as you normally would. -->
...
  <P><INPUT TYPE="submit" NAME="-find" VALUE="Start Search">
</FORM>
```

3. In the Search page in a browser, enter a value into the password field before submitting.

Only records whose password fields match the value entered on the search page will be displayed.

Protecting records from being edited

Use the following code to prevent restricted records from being edited as the result of a Web-based update or modification. Customize the VALUE tags for your databases, layouts, fields, and HTML pages.

To protect specific records from being edited:

1. Select Exact Update for the password field.

2. In an HTML edit page enter commands similar to:

```
<FORM ACTION="FMPro" METHOD="post">
  <INPUT TYPE="hidden" NAME="-db" VALUE="MyDatabase.fp5">
  <INPUT TYPE="hidden" NAME="-lay" VALUE="Layout #1">
  <INPUT TYPE="hidden" NAME="-format" VALUE="EditReply.htm">
  <INPUT TYPE="hidden" NAME="-RecID" VALUE="[FMP-currentrecid]">
  <P><B>Edit Current Record:</B>
  <P>DataField: <INPUT TYPE="text" NAME="DataField" VALUE="[FMP-
field: DataField]">
...
<!-- List your fields here as you normally would. -->
...
  <INPUT TYPE="hidden" NAME="-op" VALUE="eq">
  <P>Password : <INPUT TYPE="text" NAME="PasswordField" VALUE="">
...
<!-- List your fields here as you normally would. -->
...
  <P><INPUT TYPE="submit" NAME="-edit" VALUE="Edit Record">
</FORM>
```

3. After modifying desired fields in the Edit page in a browser, enter the password value for the current record into the password field before clicking Edit.

A valid password value will allow the record to be edited. An invalid password will bring up a security message. The password value itself cannot be modified.

Protecting records from being deleted

Use the following code to prevent restricted records from being deleted as the result of a Web-based deletion. Customize the VALUE tags for your databases, layouts, fields, and HTML pages.

To protect specific records from being deleted:

1. Select Exact Delete for the password field.
2. In an HTML edit page, include commands similar to:

```
<FORM ACTION="FMPro" METHOD="post">
  <INPUT TYPE="hidden" NAME="-db" VALUE="MyDatabase.fp5">
  <INPUT TYPE="hidden" NAME="-lay" VALUE="Layout #1">
  <INPUT TYPE="hidden" NAME="-format" VALUE="DeleteReply.htm">
  <INPUT TYPE="hidden" NAME="-RecID" VALUE="[FMP-currentrecid]">
  <P><B>Delete Current Record:</B>
  <P>DataField:  [FMP-field: DataField]
...
<!-- List your fields here as you normally would. -->
...
  <INPUT TYPE="hidden" NAME="-op" VALUE="eq">
  <P>Password : <INPUT TYPE="text" NAME="PasswordField" VALUE="">
...
<!-- List your fields here as you normally would. -->
...
  <P><INPUT TYPE="submit" NAME="-delete" VALUE="Delete This
Record">
</FORM>
```

3. In the Delete Record page in a browser, enter the password value for the current record into the password field before clicking Delete.

A valid password value will allow the record to be deleted. An invalid password will bring up a security message.