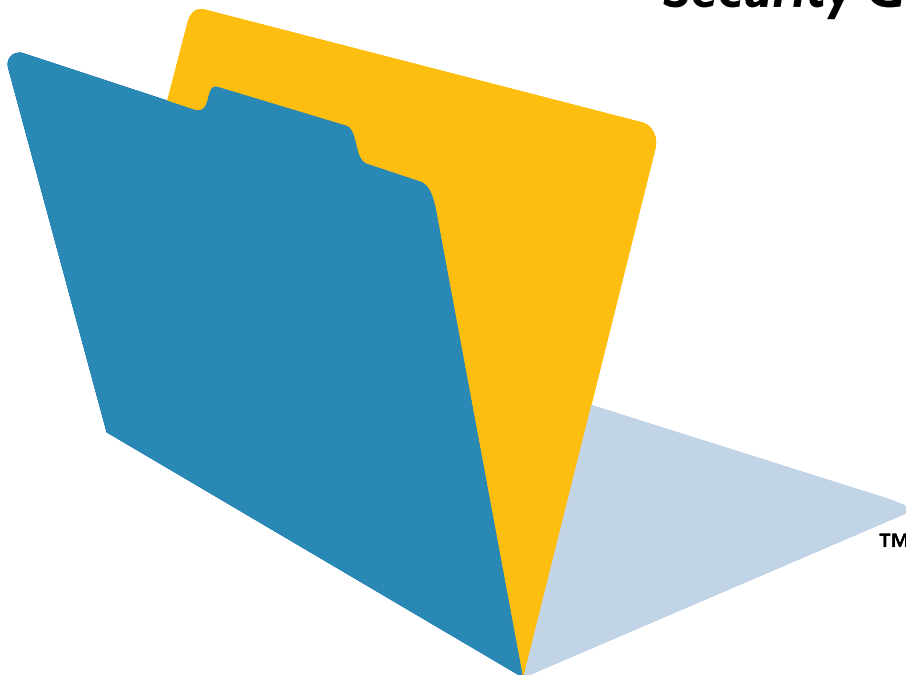


For Windows and Mac OS

# FileMaker Pro

## ***Web Publishing Security Guidelines***



© 2002 FileMaker, Inc. All Rights Reserved.

FileMaker, Inc.

5201 Patrick Henry Drive

Santa Clara, California 95054

[www.filemaker.com](http://www.filemaker.com)

FileMaker is trademark of FileMaker, Inc., registered in the U.S. and other countries. ScriptMaker and the file folder logo are trademarks of FileMaker, Inc. Portions of some screen shots are reprinted by permission from Microsoft Corporation. Portions of some screen shots are copyright 1996–2000 Netscape Communications Corp. All rights reserved. These screen shots may not be reprinted or copied without the express written permission of Netscape. All other trademarks are the property of their respective owners.

FileMaker documentation is copyrighted. You are not authorized to make additional copies or distribute this documentation without written permission from FileMaker. You may use this documentation solely with a valid licensed copy of FileMaker software.

All other trademarks are the property of their respective owners.

Mention of third party companies and products is for informational purposes only and does not constitute an endorsement. FileMaker assumes no responsibility with regard to the selection, performance, or use of these products. All understandings, agreements or warranties, if any, take place directly between the vendor and prospective users.

**This page intentionally left blank.**

# Contents

## Chapter 1

### ***Introduction to FileMaker Pro web security***

Protecting your databases from outside attacks	5
Physical security	5
Operating System security	6
Firewall protection	6
Web server security and the Web Companion	7
Secure Sockets Layer (SSL) security for Custom Web Publishing	7
Protecting your data in FileMaker Pro	8
Considerations when designing databases for web publishing	8
Securing data for web publishing within FileMaker Pro	12
FileMaker Pro access privileges	13
FileMaker Pro Web Security Database	14
Additional security features in FileMaker Pro	15
Web Companion configuration	15
The cdml_format_files folder	16

## Chapter 2

### ***How to secure your data in FileMaker Pro web publishing***

Protecting data for Instant Web Publishing	17
Defining passwords	17
Specifying access privileges as the security method for Instant Web Publishing	19
Record-by-record protection for Instant Web Publishing using FileMaker Pro access privileges	19
Specifying default layouts in databases published with Instant Web Publishing	21
Recommendations	22
Protecting Custom Web Publishing solutions	22
Using access privileges to protect Custom Web Publishing	23
Using the Web Security Database to protect Custom Web Publishing	23
Record-by record protection with the Web Security Database	24

## Chapter 3

### ***Using the Web Security Database***

How the Web Security Database works	29
Installing the Web Security Database	30
Enabling the Web Security Database	30
Assigning Web Security to your databases	32
Protecting specific records in a database using the Web Security Database	35
Changing Web Security settings remotely from the Web	36
Web Security Database tips	41

## **Chapter 4**

### ***Using the cdml\_format\_files folder***

Protecting your CDML format files	43
cdml_format_files folder examples	44
cdml_format_files folder tips	44

## **Chapter 5**

### ***Using SSL protection with Custom Web Publishing***

Example: Configuring SSL with Microsoft IIS	47
Part 1: Generating a private key pair and Certificate Signing Request (CSR)	47
Part 2: Entering your certificate	48
Part 3: Enabling and configuring SSL and other certificate features	49
Part 4: Testing your new SSL enabled web site	49

## ***Index***

I-1

# **Chapter 1**

## ***Introduction to FileMaker Pro web security***

FileMaker® Pro software enables you to create powerful database solutions and publish them to your intranet or the Internet, so that users browse, search, and update the databases through a browser.

When FileMaker Pro databases are used individually, shared on a peer-to-peer basis, or shared using FileMaker Server, FileMaker Pro security consists of *passwords* and *access privileges*. Passwords protect access to your databases, and the access privileges associated with those passwords determine your guests' ability to create, edit, delete, or export records, design layouts, and so forth. This is a security model that is both simple and powerful. Because sharing with FileMaker Pro guests or the Local and Remote Data Access Companions should only take place within the protected environment of a local area network, there is virtually no risk of an outside attack; data shared in these situations is very secure.

When you share your FileMaker Pro databases over the Web or over an intranet, your networking environment is more complex, and your security needs are typically more complex as well. In those situations, you can use either access privileges or the FileMaker Pro *Web Security Database* with Custom Web Publishing to protect your databases. Before you publish your databases on the Web, carefully consider your security needs, and follow the security procedures explained in this document. As the primary purpose of this document is to provide guidelines for FileMaker Pro web security, other aspects of web security are identified more generally. For more information about these topics, consult your network administrator, third-party documentation, or other network professional.

The security concerns for your web-published databases can be divided into two broad categories: the need to protect your database files from outside attacks, and the need to protect your actual data from being improperly viewed, manipulated, or deleted.

### ***Protecting your databases from outside attacks***

#### ***Physical security***

First, consider the physical security of your host machine. The host computer should be a dedicated machine stored in a locked room, where it is secured to an immovable object such as a large desk, computer cabinet, or specialty anchoring hardware. The machine should be secured so that its hard drive cannot be removed. Also consider the physical security of backup copies of files and databases that may be stored on portable media, such as tapes and diskettes. Finally, access to the host machine should be controlled, and only the minimum number of people necessary to deploy and maintain your databases should have access to it.

You may not need this degree of security, but be aware that each step removed from the ideal represents an increase in the physical vulnerability of your host machine.

When assessing the physical security of your network, consider that the use of wireless networking devices, such as the Apple AirPort and other 802.11b networking cards and base stations, can pose some special security challenges. These devices can broadcast your network traffic beyond the walls of your building, so it is extremely important to encrypt your wireless networking signals. If you choose to use these devices as part of your network, always use the maximum level of signal encryption available.

### ***Operating System security***

The security mechanisms of the operating system on the host computer need to be used to ensure that access to the directories holding the FileMaker Pro databases and related files are properly controlled. System user IDs, passwords and directory access privileges should be controlled so that only the people authorized to administer and maintain the FileMaker databases or the system as a whole will have access to the files.

You should review settings for remote access, such as file sharing and FTP, to ensure that direct access to upload or download files from the host computer are restricted in a manner that prevents inappropriate access to your files.

### ***Firewall protection***

When you share your FileMaker Pro databases over the Web or an intranet, you use the TCP/IP networking protocol. You may also use the TCP/IP protocol when you share databases peer-to-peer, or through FileMaker Server. TCP/IP conforms to standards that are supported by many different operating systems, including Mac OS, Windows, Linux, UNIX, and others. The wide use of TCP/IP is both a strength and a weakness. Like a highway that carries a lot of traffic, TCP/IP is excellent for moving data, but the protocol itself doesn't provide much protection for the data that travels over it.

Whenever you host a FileMaker Pro database using TCP/IP, the same protocol that allows your guests to connect to your data can also allow uninvited visitors access to your host machine, server software, databases, and perhaps even to other guest machines on your internal network. So it is important to control the access to these components, and place some barricades in the path of any uninvited visitors.

The most common barricade method used is the *firewall*, which separates your network into two distinct environments: a public environment that is termed "outside the firewall," and a private environment, usually referred to as "behind the firewall." Users on the outside of the firewall will only have access to those TCP/IP or hardware addresses you choose to expose to outside guests. This allows you to concentrate your security on those server machines that are exposed, while allowing your other machines behind the firewall to operate with fewer safeguards.

## ***Web server security and the Web Companion***

The software you use to publish databases, images, and other content to the Web is called *web server* software. Web server software performs the critical task of processing and fulfilling requests for data. When someone enters a web address into their browser, they are requesting the web server software at that address to locate data or an image and download it to their machine, where it can be displayed in their browser. To protect the integrity of this process, your web server has its own security mechanism.

The FileMaker Pro *Web Companion* is a plug-in component of FileMaker Pro. The Web Companion functions as an HTTP server/web server/Common Gateway Interface (CGI) application, communicating with web browsers that request data from or submit data to a FileMaker Pro database.

When you publish your data using FileMaker Pro *Instant Web Publishing*, the FileMaker Pro Web Companion functions as the web server, and security is provided by FileMaker Pro access privileges. As with FileMaker Pro desktop publishing, access via Instant Web Publishing is controlled by passwords. For more information about FileMaker Pro access privileges, see “FileMaker Pro access privileges” on page 13.

When you publish your data using FileMaker Pro *Custom Web Publishing*, you can use the FileMaker Pro Web Companion as your web server. If you are using FileMaker Pro Unlimited software and the FileMaker Web Server Connector, you can use third-party web server software, such as Microsoft Internet Information Server (IIS) or Apache Web Server. If you are using the FileMaker Pro Web Companion as your web server, security is provided by either access privileges or the Web Security Databases. See “Securing data for web publishing within FileMaker Pro” on page 12 for a comparison of these methods to determine which is best for your needs. If you are using a third-party web server with Custom Web Publishing, your web server software may offer additional security features. Consult the documentation included with your web server software for more information.

## ***Secure Sockets Layer (SSL) security for Custom Web Publishing***

The Secure Sockets Layer (SSL) protocol is a standardized method for allowing encrypted and authenticated communication between web servers and web browsers. SSL can provide a commercial level of authentication, privacy and data integrity through encryption. Many web designers turn to SSL protection when security is the highest priority. For example, when receiving credit card information from a customer using a web browser, many web sites will use SSL to encrypt and secure the communication to prevent other people on the Internet from obtaining this information. Encryption through SSL converts information being exchanged between web servers and web browsers into unintelligible information through the use of mathematical formulas known as *ciphers*. These ciphers are then used to transform the information back into understandable data by the intended recipient through *encryption keys*.

**Note** SSL protection is only available to users of Custom Web Publishing with FileMaker Pro Unlimited, and only through the use of the FileMaker Web Server Connector (FMWSC) and third-party web server software, such as Microsoft Internet Information Server (IIS). For more information on enabling SSL with FileMaker Pro Unlimited, see chapter 5, “Using SSL protection with Custom Web Publishing.”

## ***Protecting your data in FileMaker Pro***

Just as you use different components to protect your computer and network hardware from outside attack, FileMaker Pro relies upon a variety of features to provide security for your data when you publish it on the Web. FileMaker Pro web publishing security is both flexible and layered: “flexible security” means that you can change your access permissions on a user-by-user or record-by-record basis, if desired. “Layered security” means that different security features provide different areas of protection.

### ***Considerations when designing databases for web publishing***

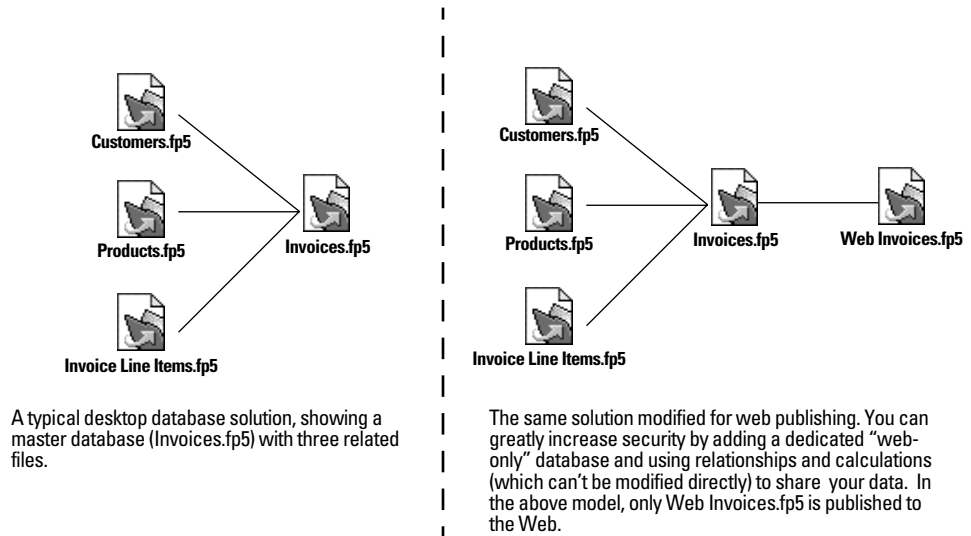
Because security is such an integral part of the design of your databases, you must consider your security needs when you are planning your database schema. *The key to providing the maximum amount of security for your database is to begin by designing your database with security in mind.*

Follow these suggestions when you design your databases for web publishing:

1. Use dedicated “web-only” databases, if possible. Make sure they contain only the layouts, scripts, and field definitions that you want to expose to the public.

For example, you may have a system of sales databases with names such as Invoices.fp5, Invoice Line Items.fp5, Customers.fp5, and Products.fp5, where Invoices.fp5 is the master file, and the other databases are related to it. If you want customers to view their own invoices on the Web, you could create a file called Web Invoices.fp5, and use relationships and calculations to Invoices.fp5 to make a customer’s invoices available to them via web publishing. In this example, only the Web Invoices.fp5 file is shared to the Web (File menu > Sharing, with Web Companion selected). The other databases (Invoices.fp5, Invoice Line Items.fp5, Customers.fp5 and Products.fp5) are not shared in order to prevent direct access from the Web.





**Note** In general, use your “web-only” database only for web publishing. It is not a good practice to enable databases published to the Web to also be enabled for Local/Remote Data Access or shared as Multi-User. It is easier to manage security if you use a web-only database as the front-end to your solution for web users, and keep this separate from considerations for access to the same solution from FileMaker Pro clients, the Data Access Companions, or other clients.

If you are publishing the FileMaker Pro database over your intranet (such as a local area network behind a firewall), you can use any access privileges you may have set up for current users of the database. You can provide a more limited web-only password when users are accessing the database via a web browser.

**2.** Review all scripts, and eliminate all scripts that could be used to perform inappropriate actions, or should not be executed by a web user.

A script might include actions that should be controlled by access privileges, such as Edit and Delete records.

A script might also include actions that are not controlled by access privileges, such as Send Mail, or actions that might not be designed to be executed from the Web. For example, a script step that will cause a prompt or message window to be displayed on the host computer will “hang” the system when executed from the Web.

Also, consider the side effects of scripts that execute a combination of steps that are controlled by access privileges. For example, if a script includes a step to Delete Records, and a web user does not have a password that allows record deletion, the script will not execute the Delete Records script step. However, the script will continue to run, and subsequent steps in the same script may be executed. This could cause unexpected results.

In general, create a “web-only” database with a minimum set of scripts that are intended to be used from the Web and have no harmful side effects if they are executed by any web user.

Here is a partial list of script steps that may cause problems when used with web-published databases:

- Edit
- Delete
- Show Omitted
- Open
- Close
- Set Multi-User
- Delete all
- Replace
- Send Mail
- Quit

**Note** The Web Security Database can be used to disable specific web users from running any scripts in a database, but cannot be used to selectively allow specific scripts to be executed.

**3.** It is recommended that you assign Edit and Delete privileges to web-only passwords only if they are necessary. See “Recommendations” on page 22 and “Web Security Database tips” on page 41 for more information.

**4.** Use access privileges as the recommended method of applying security for Instant Web Publishing, and configure record-by-record security, if additional security is necessary. See “Protecting data for Instant Web Publishing” on page 17 for more information.

**Note** If a 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.

**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 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 different level of security.

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

**5.** 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 online Help on defining groups.

**6.** If you have an open database on a host computer, but you don't want to publish it on the Web, be sure Web Companion sharing isn't enabled for that database.

**7.** To prevent a published database from displaying on the built-in home page, rename the database to include an underscore character at the end of the filename, before any filename extension (for example, Orders\_ or Orders\_.fp5). If you change the filename, you may need to change references to the file in relationships and scripts. (Alternatively, you can consider not enabling Web Companion sharing for the primary database, and using a web-only database as a front-end to the primary database, as described above.)

**Note** This naming method will not prevent the name of the database from being displayed in response to the CGI request `-dbnames`.

**8.** Use the Web Security Database as an alternate method of applying security for Custom Web Publishing, and configure security for users and fields. For additional security, do not use blank passwords, and do not use the All users option. See “Protecting Custom Web Publishing solutions” on page 22 for more information.

**9.** For Custom Web Publishing, FileMaker recommends that you use additional security measures, such as the Secure Sockets Layer (SSL) protection offered by third-party web server software.

For information on configuring SSL protection for FileMaker Pro Unlimited software using Microsoft Internet Information Server (IIS), see “Example: Configuring SSL with Microsoft IIS” on page 47.

**10.** Test your security.

Using a browser, you can test your web-published databases to see what elements are exposed. For example:

- To view the names of the databases that are published to the web, enter this address in your browser:

`http://<your IP address>/FMPro?-format=-fmp_xml&-dbnames`

You should only see the names of those databases you intend to publish to the web.

- To view the fields that are available on the Web for a record in your database, enter this address in your browser:

`http://<your IP address>/FMPro?-db=abc.fp5&-format=-fmp_xml&-findany`

You should only see the names of the fields you intend to expose for that record.

- To view the script names in a database, enter this address in your browser:

`http://<your IP address>/FMPro?-db=abc.fp5&-format=-fmp_xml&-scriptnames`

You should only see the names of the scripts you intend to expose for that database.

- To view the layout names in a database, enter this address in your browser:

`http://<your IP address>/FMPro?-db=abc.fp5&-format=-fmp_xml&-layoutnames`

You should only see the names of the layouts you intend to expose for that database.

To personalize the above examples for your testing environment, substitute your IP address or localhost for “<your IP address>,” and the actual name of your database for “abc.fp5.”

**Note** If you are interested in creating a secure data environment and do not have the experience or skills to ensure complete security, contact a FileMaker Solutions Alliance (FSA) member who specializes in security. For more information on FSA developers see [www.filemaker.com/developers/fsa\\_members.html](http://www.filemaker.com/developers/fsa_members.html).

## Securing data for web publishing within FileMaker Pro

FileMaker Pro provides two methods of web publishing: Instant Web Publishing and Custom Web Publishing.

FileMaker Pro also provides two primary methods of web security: access privileges and the Web Security Database.

- Databases published with Instant Web Publishing must use FileMaker Pro access privileges to provide web security.
- Databases published with Custom Web Publishing may use either access privileges or the Web Security Database.

Access privileges and the Web Security Database differ as follows:

Feature	Supported by FileMaker Pro access privileges	Supported by FileMaker Pro Web Security Database
Password protection	Yes	Yes
User ID/User name verification	No	Yes
Disallow searching using a specific field	No	Yes
Administer security privileges remotely	No	Yes
Security for a field across an entire database	Yes	Yes
Security for a particular record	Yes	Yes
Security for a field by password	Yes	No
Scripting	Indirectly – Scripting capabilities reflect the privileges associated with a particular password. For example, if a password permits creating new records, then scripted creation of new records is allowed.	Yes – Scripting capabilities are Boolean. For example, you can either enable or prevent a user from performing all scripts.
Control browsing of records	Yes	Yes

Feature	Supported by FileMaker Pro access privileges	Supported by FileMaker Pro Web Security Database
Control updating of records	Yes	Yes
Control deleting of records	Yes	Yes

**Important** In general, it is best to secure your data at as low a level as possible, at the record and/or field level. The best means of doing this is to use FileMaker Pro access privileges. Access privileges provides data security regardless of the method used to access the data, whether it is through FileMaker Pro networking, the Remote Data Access Companion (RDAC), Instant Web Publishing, or Custom Web Publishing. In some instances when using Custom Web Publishing, you may require the additional security features provided by the Web Security Database.

### ***FileMaker Pro access privileges***

Access privileges let you set different types of access for different users, control access to database functionality, and create record-level access based on customized criteria.

When used with the Web Companion, access privileges allow you to give web users:

- browse access
- edit access
- delete access
- the ability to create records
- access to data in records based on custom criteria

The Web Security Database will not override assigned access privileges if a “Database Password” is placed in the Web Security Database. When the Web Security Database is used in combination with FileMaker Pro access privileges, access privilege definitions take precedence over any user permissions and field restrictions that you have set in the Web Security Database. In other words, you can’t add Web Security Database privileges to a database if those privileges have been denied by FileMaker Pro access privileges.

**Important** Don't forget that access privileges also let you set other types of access for users, such as the ability to export records, design layouts, change passwords, and print. These privileges should be disabled for web-only passwords. A password assigned for web use can also be used by a FileMaker Pro user. Unless you disable these other actions, a user accessing the database using FileMaker Pro and a web-only password may have more privileges than you intend, such as the ability to modify the database design.

Passwords and groups are the primary methods of assigning access privileges in FileMaker Pro databases:

- *Passwords* control access to and limit activities within a database file. You may have several passwords in one database file. For example, one password can allow users to create and edit records, while another password only allows users to view (browse) records.

- *Groups* are a means of aggregating and administering passwords that confer the same level of access to all passwords in a particular group. Use groups to classify users and control their access to specific fields or layouts in a database file. While passwords restrict activities across an entire database or to specific records, groups can restrict editing in particular fields.

**Note** While groups can also be used to restrict access to specific layouts in the FileMaker Pro desktop environment, these restrictions are not respected when accessing FileMaker Pro data from the web. Consequently, you should not use “hidden” or restricted layouts as part of your security model.

For more information on configuring access privileges for use with web publishing, see chapter 2, “How to secure your data in FileMaker Pro web publishing.” For more general information on access privileges, consult FileMaker Pro Help.

### ***FileMaker Pro Web Security Database***

The FileMaker Pro Web Security Database is a set of three related databases that work together to protect databases published using Custom Web Publishing.

The Web Security Database lets you provide user name and password protection to multiple FileMaker Pro databases. You can set specific user permissions and field restrictions for each database, and update or change those settings directly from your web browser.

The Web Security Database includes two types of files: databases for providing web security and HTML files for changing the web security settings remotely. When users attempt to access your protected database on the web, their web browser will display a user name and password dialog box, and they will be required to input both a user name and a password before proceeding. This behavior is potentially more secure than that offered by access privilege protection, in which only a password is required (user name data is ignored by access privilege protection).

With the Web Security Database, once a user name and password are established, that information is sent by the web browser with every request to the Web Companion. The Web Companion then checks those values against the settings configured in the Web Security Database and grants permissions or field restrictions based on the specified privileges.

Remember, you can use access privileges or the Web Security Database when using Custom Web Publishing. Determine which security method delivers the specific features you need before you begin developing your custom web pages. For more information on creating custom web pages for use with FileMaker Pro, see the *FileMaker Pro Unlimited Administrator’s Guide*, *FileMaker Developer’s Guide*, or the FileMaker, Inc. web site at [www.filemaker.com](http://www.filemaker.com).

For more information on the Web Security Database, see “Using the Web Security Database” on page 29.

## Additional security features in FileMaker Pro

In addition to the two primary security mechanisms explained in the previous section, FileMaker Pro uses the following features to provide security for your web published databases: Web Companion configuration and the `cdml_format_files` folder.

### Web Companion configuration

The Web Companion offers two important security features: the ability to log the IP addresses, dates, and times of all requests, and the ability to limit access to only those IP addresses you specify in advance.

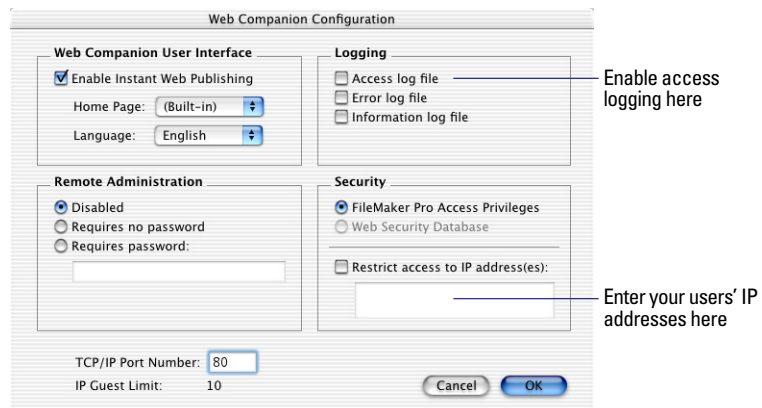
Use access logging to learn important information about the users who access your database through the Web Companion. You can identify users who are foreign to your network, and get accurate counts of the number of Web Companion guests your database is serving.

Use the **Restrict access to IP address(es)** feature to limit web access to only those IP addresses that you specify in advance. If you plan on hosting your database to a select group of web users whose IP addresses you already know, you will effectively create a closed network when you enter those IP addresses in the **Restrict access to IP address(es)** area of the Web Companion Configuration dialog box.

Both of these security features can be enabled from the Web Companion Configuration dialog box.

To open the Web Companion Configuration dialog box:

- Mac OS and Windows: Select **Edit menu > Preferences > Application Preferences**. From the **Plug-ins** tab, select **Web Companion** and click **Configure**.
- Mac OS X: Select **FileMaker Pro menu > Preferences > Application Preferences**. From the **Plug-ins** tab, select **Web Companion** and click **Configure**.



**Important considerations for using the Web Companion**

- Do not enable the Web Companion unless you intend to publish your database over the web, and have enabled password and access privilege protection or are using the Web Security Database.
- In general, database files should not be stored in the Web folder (or sub-folders).
- Do not enable remote administration via the Web Companion unless you intend to administer your databases remotely. Remote administration enables you to:
  - administer the Web Security Database remotely
  - use the `-dbopen` CGI action
  - use the `-dbclose` CGI action
  - download FileMaker Pro files from the FileMaker Pro Web folder
  - use the HTTP PUT command for uploading files into the Web folder

With Remote Administration enabled it is possible to use HTTP PUT to place a CDML format file within the Web folder. A file could include the `FMP-Include` tag, which could specify a CDML format file that was in the `cdml_format_files` folder. You can limit your exposure to such an attack by only enabling remote administration when absolutely necessary.

**Important** Only enable Remote Administration if you need to use it. Consider using SSL to secure remote administration communications (which will contain database names, user IDs and passwords) in order to prevent other Internet users from obtaining this information. For more information, see “Secure Sockets Layer (SSL) security for Custom Web Publishing” on page 7.

***The cdml\_format\_files folder***

If you’re doing Custom Web Publishing, use the `cdml_format_files` folder to restrict browser clients from directly viewing the source code of your CDML format pages. This prevents the source code and logic of your web site design from being viewed by guests, while still allowing the Web Companion to serve your data.

For more information on using the `cdml_format_files` folder with Custom Web Publishing, see chapter 4, “Using the `cdml_format_files` folder.”



# Chapter 2

## ***How to secure your data in FileMaker Pro web publishing***

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

### ***Protecting data for Instant Web Publishing***

To secure your database for 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 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 different 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 as a guest, or with a password that provides limited access. To create additional passwords, you must reopen the file as the host, with a master password.

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

### Tips for creating and maintaining passwords

When FileMaker Pro databases are used individually, shared on a peer-to-peer basis, or shared using FileMaker Server, FileMaker Pro security consists of passwords and access privileges. Passwords protect access to your databases, and the access privileges associated with those passwords determine your guests' ability to create, edit, delete, or export records, design layouts, and so forth. This is a security model that is both simple and powerful.

The following are suggestions for creating secure passwords:

- Secure passwords are typically more than eight characters in length, and include at least one numeric digit.
- Passwords are less secure when they include strings that are easily guessed, such as names (especially the names of family and pets), birth dates, anniversary dates, and, in particular, the words *password*, *default*, *master*, *admin*, and similar standard terms.
- Change passwords frequently.
- Use passwords only once.
- If possible, assign a unique password for each user.
- When creating a password for a Web published database or remote administration, use only a combination of the characters A through Z, with at least one numeral. Do not include spaces, special characters, or high ASCII characters in your password, as these may be interpreted incorrectly over the Web.
- If you are publishing the FileMaker Pro database over your intranet (such as a local area network behind a firewall), you can assign any access privileges you may require for current users of the database. You should consider creating more limited passwords for users who are accessing the database via a web browser.
- You will always need at least one master password if you are creating a group of passwords.

In addition, you and the users of your database should practice good management of known passwords:

- Do not record your passwords in a master file (especially if it is not, in turn, secured by a password and encryption) or list.
- Do not share passwords with other users; always go to the owner or administrator of a database to obtain the correct password to be used.

Passwords protect access to your databases; however, passwords should not be viewed as a 100% secure form of protection. You should take other reasonable measures to protect access to your files and information, and not rely solely on passwords; for example:

- If you use FileMaker Developer, consider using the FileMaker Developer Tool to remove the administrator password when appropriate.
- If you host a FileMaker Pro database on a server, the administrator should use OS level security settings and passwords restrict access to the directories and files to authorized personnel only.
- Protect the physical security of the computers, hard drives, and backup storage media where the database files reside.
- For web-shared solutions, especially on the Internet, consider 2 (or more) machine configurations, firewalls, SSL and other standard Internet technologies and practices in order to protect access to your database and to protect the communication between users' browsers and the server.

### ***Specifying access privileges as the security method for Instant Web Publishing***

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

1. Choose Edit menu > Preferences > Application.

Mac OS X: Choose FileMaker Pro 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 6 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 as a guest, or with a password that provides limited access. To create the additional passwords explained in this example, you must reopen the file as the host, 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.

**18.** Click Create to create the password “manager\_password” with the privileges described above.

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

**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 19.

**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.

**Note** The following layout preferences are not used when you suppress the Instant Web Publishing navigation and command interface. If you suppress these controls, your users will be completely dependent on your buttons and scripts to manage your database solutions when in a browser.

**Important** 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 online Help on defining groups.

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**.

## ***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, consider disabling edit and delete privileges for all passwords to be used on the Web for Internet users. If different forms of security are 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***

There are two methods of protecting Custom Web Publishing solutions: FileMaker Pro access privileges or the Web Security Database.

**Important** When you publish databases using FileMaker Pro Custom Web Publishing, you make it possible for the Web Companion to use XML and/or CDML to execute commands in FileMaker Pro. The ability to use XML and/or CDML is intrinsic to Custom Web Publishing, and cannot be disabled, however, the execution of these commands can be limited or prohibited using the security methods described below.

## ***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 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 17, which are the same for 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 19, which are the same for 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 introduced 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 19, which are the same for 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 specialized security for your Web/intranet published databases in Custom Web Publishing. See Chapter 3, "Using the Web Security Database," on page 29, for a complete description of this feature.

### **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 6/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 use with 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**.
- Mac OS X: Choose **FileMaker Pro 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 PasswordRecord. 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 PasswordRecord field 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 PasswordRecord in the Field Name column.**7.** In the Field Restrictions column, select the security options for this field as described in the following sections.

For more information on the Web Security Database, see “Using the Web Security Database” on page 29.

**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="PasswordRecord"
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. -->
  ...
  <P>Password : <INPUT TYPE="text" NAME="PasswordRecord"
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. -->
  ...
  <P>Password : <INPUT TYPE="text" NAME="PasswordRecord"
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.



# Chapter 3

## *Using the Web Security Database*

The FileMaker Pro Web Security Database is a set of three related databases working together to protect your databases published on an intranet or the Internet. Designed to work with your custom web pages, the Web Security Database lets you provide user name and password protection to multiple FileMaker Pro databases. You can optionally set specific user permissions and field restrictions for each database, and update or change those settings directly from your web browser.

With a Web Security user name and a password, web users can do one or more of the following in your published database(s):

- Browse records
- Create records
- Edit records
- Delete records
- Perform scripts
- View all except certain restricted fields
- Search all except certain restricted fields
- Edit all except certain restricted fields
- Enter a special value in a restricted field and view, edit, or delete only those records that contain the exact matching value
- Modify or delete records containing exact matching values in the restricted field

**Important** The Web Security Database is not designed to work with FileMaker Pro Instant Web Publishing. The ExactSearch, ExactUpdate, and ExactDelete field restrictions do not function properly in Instant Web Publishing. For information about creating custom web pages using the FileMaker Pro Unlimited or FileMaker Developer products, go to [www.filemaker.com](http://www.filemaker.com). In FileMaker Pro, choose Help menu > FileMaker on the Web.

### *How the Web Security Database works*

The Web Security Database includes two types of files: databases for providing web security and HTML files for changing the web security settings remotely. Web security is controlled by a main database named Web Security.fp5 and two related databases named Web Users\_.fp5 and Web Fields\_.fp5.

When users attempt to access your protected database on the Web, the web browser displays a user name and password dialog box.



Once you establish a user name and password, they are sent by the web browser with every request to the web server. The FileMaker Pro Web Companion checks these values against the settings configured in the Web Security Database, and then determines if any user permissions or field restrictions exist for a specific action.

## Installing the Web Security Database

When you install FileMaker Pro, the Web Security Database files are automatically installed in Web Security/Databases folder. If the folder isn't there, then you'll need to do a custom install. See the *FileMaker Pro Getting Started Guide* for information on installing FileMaker Pro Web Support, which includes the Web Security Database.

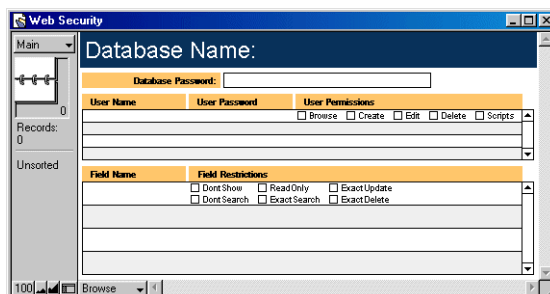
**Note** Do not install the Web Security Database to the Web folder unless you intend to use Remote Administration. For more information, see “Changing Web Security settings remotely from the Web” on page 36.

## Enabling the Web Security Database

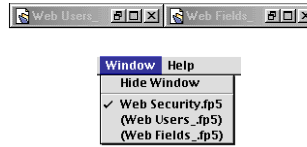
The Web Security Database must be open before you can enable it in FileMaker Pro.

1. In FileMaker Pro, choose File menu > Open and open the Web Security.fp5 file.

(FileMaker Pro/Web Security/Databases/Web Security.fp5)



The related files, `Web Users.fp5` and `Web Fields.fp5`, also appear in separate (usually minimized) windows (Windows) or in the Window menu (Mac OS).

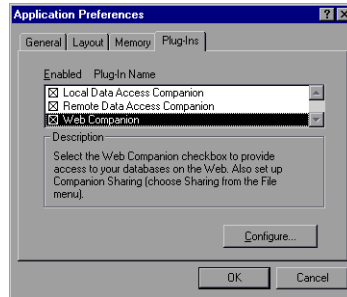


2. Choose Edit menu > Preferences > Application.

Mac OS X: Choose FileMaker Pro menu > Preferences > Application.

3. In the Application Preferences dialog box, click the Plug-Ins tab (or choose Plug-Ins from the pop-up menu).

4. Select the Web Companion checkbox to enable the Web Companion plug-in.



**Note** If Web Companion doesn't appear in the Application Preferences dialog box, you must install the Web Companion plug-in (see the *FileMaker Pro Getting Started Guide*).

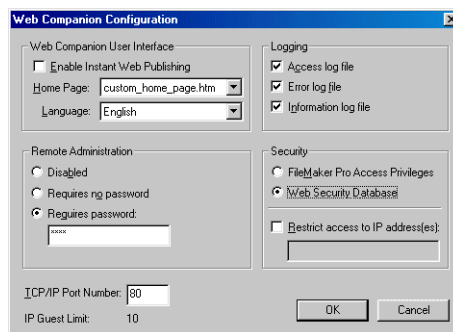
You only need to enable the Web Companion plug-in once for the FileMaker Pro application. To do so, you must have a connection to the Internet or an intranet. (For information, see chapter 14, "Publishing databases on the Web" in the *FileMaker Pro User's Guide*.)

5. With Web Companion selected, click Configure.

6. In the Web Companion Configuration dialog box, make sure that Enable Instant Web Publishing is not selected (the Web Security Database is not designed to work with FileMaker Pro Instant Web Publishing).

7. Select Web Security Database to enable it.

**Note** The Web Security Database option is not available (dimmed) when the Web Security.fp5 database is not open.



8. For Remote Administration, select Disabled if you do not plan to do remote administration.

**Note** Because of the additional risks to database security, FileMaker, Inc. strongly recommends that you leave Remote Administration disabled unless you are certain that you need to use this feature.

9. For Remote Administration, select Requires password and enter a password in the box if you want to access the Web Security Database settings later from the Web. Requiring a password for remote administration ensures that unauthorized web users cannot gain access to the Web Security Database and other files located in the Web folder. It is not recommended that you do remote administration without a password.

10. Click OK to close the Web Companion Configuration dialog box.

11. Click OK to close the Application Preferences dialog box.

12. Choose File menu > Sharing and make sure that the database is shared via the Web Companion.

**Important** When you select the Web Security Database as your method of security, you must create a record in the Web Security Database for each database you intend to share over the web. With this security method, web users will only be able to access those databases that are configured in the Web Security Database.

## Assigning Web Security to your databases

To protect one or more databases with the Web Security Database, you create a record for each database. In each record, you set up user names, passwords, and permissions for each user, and field restrictions for each database.

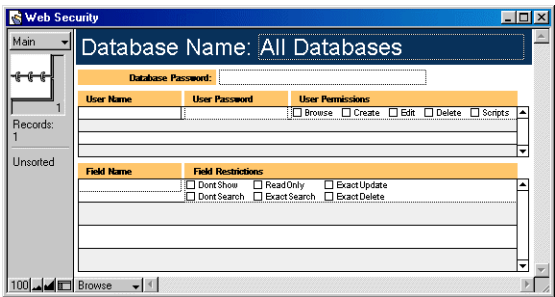
1. In the Web Security.fp5 database, create a record for each database you want to protect by choosing Records menu > New Record.

2. In the Database Name field of each new record, type the name of the database you want to protect.





Or, type All Databases in the Database Name field of one record if you want to make the same user permissions and field restrictions for all of your published databases.



3. If the database has a password set up with FileMaker Pro access privileges, and you want that password's restrictions to be added to those of the Web Security database, type that password in the Database Password field. In most cases, you should type the master password here.

**Note** Any access privilege restrictions placed on the Database Password in FileMaker Pro override the Web Security Database permissions. Web access privileges can never be greater than the privileges provided by the Database Password, regardless of the settings in the Web Security Database.

4. Type the first user name in the User Name field.

5. Type a password in the User Password field.

When creating a password, use only the characters A through Z, numerals, or a combination of the two. Do not include spaces in your password. This minimizes the possibility that you will choose characters that may be interpreted incorrectly over the Web.

**Important** Do not use leading or trailing spaces in user names or passwords for remote administration, access privileges, or the Web Security Database.

6. Select one or more of the following permissions for the user.

Select this user permission	To allow the specified web user to do the following
Browse	Browse records in the database, subject to any field restrictions set below
Create	Add records to the database, subject to any field restrictions set below
Edit	Modify records in the database, subject to any field restrictions set below
Delete	Remove records from the database, subject to any field restrictions set below
Scripts	Run scripts defined in the database

7. Repeat steps 4 through 6 to add permissions for other users.

You can type **All Users** in the **User Name** field to create privileges that apply to any web user. These privileges override more restrictive privileges set for other users. Therefore, if you set **All Users** to be able to browse, create, and edit records, then any other user names you enter for this database can also browse, create, and edit records regardless of the user permissions you set for them.

Leave the **User Password** field blank if you’re setting privileges for **All Users**. (FileMaker Pro displays an alert if you attempt to enter a password for **All Users**.)



**8.** In the **Field Name** field, type the name of any field that you want to restrict for this database (be sure to type the defined field name, not the name of a field label) and select one or more of the following restrictions for the field.

When this field restriction is selected	Web users can do the following
DontShow	View all fields in a record except this field. If a field with this restriction appears in the web page, a blank value is returned as if the field were empty.
DontSearch	Specify search criteria in any field except this field. Web users cannot search for data in this field.
ReadOnly	View but not edit data in this field.
ExactSearch	Retrieve only those records containing exact matching values to the search criteria specified for this field. A record is not returned unless an exact match is made with the field’s value in the database.  If ExactSearch is assigned to a field, the “equals” operator must be used with that field when it is present in a search action. Also, if the ExactSearch restriction is set for any field, then the -findall and -findany actions cannot be used with that database.
ExactUpdate	Edit only those records containing a value that exactly matches the value specified by the user for this field in a search. Web users cannot edit this field itself.
ExactDelete	Delete only those records containing a value that exactly matches the value specified by the user for this field in a search. Web users cannot edit this field.

## ***Protecting specific records in a database using the Web Security Database***

The ExactSearch, ExactUpdate, and ExactDelete field restrictions provide record-level security for your databases on the Web. You can limit web user access to specific records in your databases by creating a special field value for those records that only authorized users know, and applying the ExactSearch, ExactUpdate, or ExactDelete field restrictions to the field. Web users are required to enter the correct value in a search, and only those records containing the value can be displayed, edited, or deleted. By adding the DontShow field restriction to the field, unauthorized web users will not be able to see the value when the records are displayed.

**Note** When using the ExactSearch restriction for any field, the `-findall` and `-findany` actions cannot be used with that database.

The ExactSearch, ExactUpdate, and ExactDelete field restrictions can also be applied to related fields by adding the relationship name and a double colon to the field name. Web users must enter a non-blank value for the related field when searching the database. The value cannot contain any FileMaker Pro wildcard or range search characters (\*, @, !, =, //, “..”, or “...”).

**Note** See “Record-by record protection with the Web Security Database” on page 24 for additional examples of how to implement this protection.

To protect specific records in a database using the Web Security Database:

1. In FileMaker Pro, define a field in the database to contain the special field value.

YourSecretCode:

2. Enter the special field value for the field in each specific record you want to protect.

YourSecretCode: ch5rries

3. In a text editor or HTML authoring program, create an HTML text field in your search web page. Include the equals operator in the search string, and use the same name as the field you defined in the database.

```
<P><FONT SIZE="+2"><B><TT>Enter your secret code here</TT></B></FONT><BR>
<INPUT TYPE="hidden" NAME="-Op" VALUE="eq">
<INPUT TYPE="text" NAME="YourSecretCode" VALUE="" SIZE="35"></P>
```

4. In the Web Security.fp5 database, type the name of the field in the Field Name field, and select the DontShow and ExactSearch field restrictions.

If you're setting restrictions for a related field, type the relationship name, a double colon, and then the field name in the Field Name field.

relationship::YourSecretCode

Now, in order to retrieve the protected records, web users must type the special field value in the HTML text field on the search page.

**Note** All fields that you have set with the **ExactSearch**, **ExactUpdate**, or **ExactDelete** field restrictions must be present in the HTML form or script that specifies the search action. For example, if two fields are specified in the Web Security Database with these field restrictions, but only one of the fields is on the search page, then an error is generated when a web user attempts a search.

### ***Changing Web Security settings remotely from the Web***

Using the Web Security Database HTML files, you can make changes to the Web Security Database permissions and field restrictions remotely from your web browser. Changes made this way do not require restarting FileMaker Pro, disconnecting your web server, or disrupting your web server's performance.

Consider using SSL to secure remote administration communications (which will contain database names, user IDs and passwords) in order to prevent other Internet users from obtaining this information. See “Secure Sockets Layer (SSL) security for Custom Web Publishing” on page 7 for more information.

To remotely change Web Security Database settings:

- 1.** Move the Security folder and its contents from the Web Security folder (inside the FileMaker Pro folder) into the root level of the Web folder.

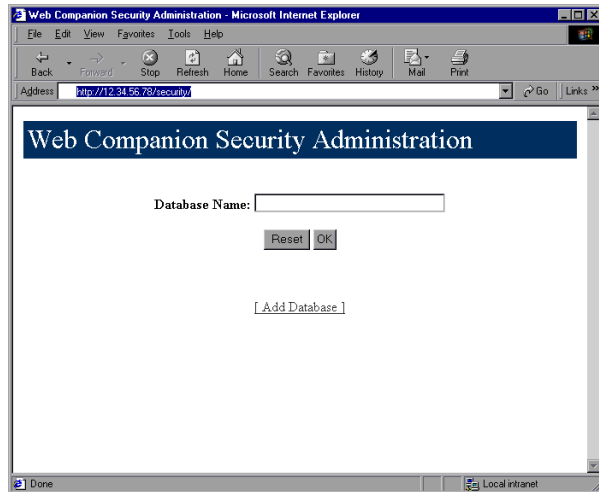
This enables the Web Companion to serve the Security HTML pages on the Web.

- 2.** In the Remote administration area of the Web Companion Configuration dialog box, make sure that **Requires password** is selected and a password is entered in the box. (See “Enabling the Web Security Database” on page 30.)

**Note** Although remote administration can be enabled for use without a password, such use is absolutely *not* recommended.

- 3.** In your web browser, type the IP or DNS address for the computer where the Web Security Database is open, and type `/Security`.

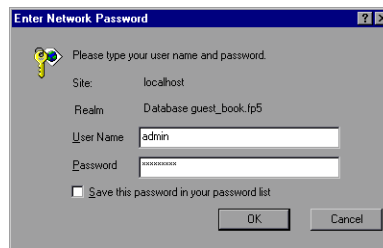
For example, type `<your IP address>/Security` where “<your IP address>” is the IP address of the host machine. This enables the Web Companion to display the default.htm file that's located inside the Security folder.



4. In the **Database Name** text box on the Web Companion Security Administration page, type the name for the web security record containing user permissions or field restrictions that you want to change and click **OK**.

If a page contains a **Reset** button, you can click **Reset** to clear the form.

5. At the password prompt, type **admin** in the **User Name** field, type the password that you specified for Remote Administration in the Web Companion Configuration dialog box, and click **OK**.



**Type "admin" in the User Name box**

On the resulting web page, you see a summary of the user permissions and field restrictions for the specified database. You can remove the web security record of this database from the Web Security Database by clicking the **Delete Database** button on this page.

If the password for the database was changed in FileMaker Pro, you can type the new password in the **Database Password** box and click **Update Password** to update the web security record.

**guest\_book.fp5 Database**

Database Password:

User Name	Password	Permissions
<a href="#">Alice</a>	apricots	Browse Create Edit Delete Scripts

Click on User Name to update or delete. [\[Add User\]](#)

Field Name	Restrictions
<a href="#">Title</a>	Don't Show Exact Search

Click on Field Name to update or delete. [\[Add Field\]](#)

[\[ View a Different Database \]](#)

6. Click the underlined link to a user name that you want to change permissions for.

On the User Permissions page, you can remove the user name from the web security record by clicking the **Delete User** button.

**User Permissions**

Database Name: guest\_book.fp5

User Name:

User Password:

User Permissions:

- ☒ Browse
- ☒ Create
- ☒ Edit
- ☒ Delete
- ☒ Scripts

[\[ View guest\\_book.fp5 Database \]](#) [\[ View a Different Database \]](#)

7. Change the user password and permissions as desired and then click **Update User**.

The record for the specified database is updated in the Web Security Database.

8. Click the **View <filename.fp5> Database** link to return to the summary page.

9. To add a user, click the **Add User** link on the summary page for the specified database.

The Add User page appears. This enables you to create permissions for a new user in the database record.

**Add User**

Database Name: guest\_book.fp5

User Name:

User Password:

User Permissions:

- ☐ Browse
- ☐ Create
- ☐ Edit
- ☐ Delete
- ☐ Scripts

[\[ View guest\\_book.fp5 Database \]](#) [\[ View a Different Database \]](#)

**10.** On the Add User page, enter the desired user name, password, and permissions, and then click Add User.

**11.** Click the View <filename.fp5> Database link to return to the summary page.

**12.** Click a field's underlined link on the specified database's summary page to change the restrictions for the field in the specified database.

**Field Restrictions**

Database Name: guest\_book.fp5

Field Name:

Field Restrictions:

- ☒ Don't show this field.
- ☐ Don't allow searching on this field.
- ☐ Make this field read-only.
- ☒ Require an exact match on this field when searching for records.
- ☐ Require an exact match on this field when updating records.
- ☐ Require an exact match on this field when deleting records.

[\[ View guest\\_book.fp5 Database \]](#) [\[ View a Different Database \]](#)

**13.** On the Field Restrictions page, change the field's restrictions as desired and then click Update Field.

**14.** Click the View <filename.fp5> Database link to return to the summary page.

**15.** To add a field, click the Add Field link on the summary page for the specified database.

The Add Field page appears. This enables you to create restrictions for a new field in the database.

**Add Field**

Database Name: guest\_book.fp5

Field Name:

Field Restrictions:

- ☐ Don't show this field.
- ☐ Don't allow searching on this field.
- ☐ Make this field read-only.
- ☐ Require an exact match on this field when searching for records.
- ☐ Require an exact match on this field when updating records.
- ☐ Require an exact match on this field when deleting records.

[\[ View guest\\_book.fp5 Database \]](#) [\[ View a Different Database \]](#)

**16.** On the Add Field page, enter the desired field name and field restrictions, and then click Add Field.

**17.** Click View a Different Database to return to the Web Companion Security Administration page.

**Web Companion Security Administration**

Database Name:

[\[ Add Database \]](#)

**18.** To add a database, click the Add Database link on the Web Companion Security Administration page

The Add Web Database page appears. This enables you to add a new database record to the Web Security Database.



Add Web Database

You must create at least one user when adding a new database.

New Database Name:

New Database Password:

New User Name:

New User Password:

New User Permissions:

☐ Browse

☐ Create

☐ Edit

☐ Delete

☐ Scripts

Add Database

Reset

[View a Different Database](#)

19. In the New Database Name box, enter the name of the database you want to create a web security record for.

20. If the database has a password set up for FileMaker Pro access privileges whose permissions you wish to add to those of the Web Security Database, enter it in the New Database Password box. For more information, see “Assigning Web Security to your databases” on page 32.

21. Enter the first user name and the desired password and permissions. Then click Add Database. The summary page for the new database record appears. From this page, you can add more user names and permissions and set field restrictions for the new database.

products.fp5 Database Added

Database Password:

Update Password

Delete Database

User Name	Password	Permissions
<a href="#">Terry</a>	tangerine	Browse Create Edit Delete Scripts

Click on User Name to update or delete. [Add User](#)

Field Name	Restrictions
------------	--------------

Click on Field Name to update or delete. [Add Field](#)

[View a Different Database](#)

Web Security Database tips

Keep these points in mind when using the Web Security Database:

- In the Web Security Database, you can set user permissions for Browse, Create, Edit, Delete, and Scripts. The Web Security Database permissions for Create, Edit, and Delete do not restrict ScriptMaker scripts from performing these actions. Use access privileges to secure databases that have ScriptMaker™ scripts. Scripts that include the New, Duplicate, Edit, Delete, or Export Records script steps should be protected by access privileges, although you can also use the Web Security Database to prevent all scripts from being executed on a user-by-user basis.

- Passwords entered in the Web Security Database restrict user access to databases as a whole, but do not restrict field-level permissions on a user-by-user basis. Use access privileges to restrict field-level access for a given password (or group of passwords), and use the Web Security Database to restrict field-level access for an entire database.
- Do not enable Multi-User for the Web Security Database.
- Do not enable the RDAC plug-in on the machine that is web hosting your databases (including the Web Security Database), unless you have also configured FileMaker Pro access privileges to properly secure the direct access to your data using this access method. RDAC will enable all TCP/IP users, including web users, to use ODBC to work with your database.
- Strongly consider password-protecting all databases in the Web Security Database (Web Users.fp5, Web Fields.fp5, and Web Security.fp5) with the same password(s), as this will make their use and administration much easier.
- The Web Security Database gives you the option of entering a Database Password for each database it protects. This password has to be a valid password created through FileMaker Pro access privileges. If this password has access restrictions associated with it, they will be combined with those created in the Web Security Database.
- You can't add Web Security Database permissions for users if those permissions are not already associated with the Database Password. To avoid privilege conflicts, it is better not to mix the two FileMaker Pro security schemes. Therefore, for Database Password, enter the secured database's master password. If no password is entered here (and the database has access privilege passwords), the Database Password will default to the password that the database is currently open with on the desktop, which may not be the master password.
- Disable Web Companion file sharing for the Web Security Database.
- The Web Companion performs a validation check of the Web Security Database the first time a web request is received with the Web Security Database enabled. All of the Web Security Database's own fields, and all expected value list entries for those fields, must be verified before web serving can commence. If problems are detected, web users will be informed that Security is disabled (and their requests will not be acted on). For this reason, it is strongly recommended that fields and value lists inherent to the Web Security database itself (and its related databases) not be altered in any way.
- FileMaker Pro Unlimited only: When you run the FileMaker Web Server Connector (FMWSC) on a Windows machine, you must use *basic authentication*. Basic authentication prompts your users to enter both a user name and a password when they log on to the database. To use basic authentication with the Web Security Database, you must create a record in the Web Security Database for each user listing their user name and password, as described in "Assigning Web Security to your databases" on page 32. The user names and passwords you list must match those of valid accounts on the web server machine, except when "all users" is specified in the Web Security Database.

**Note** User names and passwords passed between the Web Companion and FMWSC are sent as clear text.

# Chapter 4

## *Using the `cdml_format_files` folder*

FileMaker Pro 6 introduces a new feature to protect the source code and structure of your CDML format files: the `cdml_format_files` folder.

Located at the root level of the FileMaker Pro folder, the `cdml_format_files` folder provides a way to protect your format files (files that are specified using the `-format` parameter) when publishing databases using Custom Web Publishing.

Unlike the FileMaker Pro Web folder, the `cdml_format_files` folder cannot be accessed directly by the FileMaker Pro HTTP server. Instead, the Web Companion searches this folder for CDML format files during CGI requests. The Web Companion will forward the results of a search or other action that references a CDML format file located in this folder, but it will deny any attempts to view the source code information of files located within it.

### *Protecting your CDML format files*

The easiest way to protect one or more CDML files in an existing solution is to copy the entire directory into the `cdml_format_files` folder and then delete the CDML format files from their original locations within the Web folder. No modifications to the content of the solution are necessary. Copying the entire folder will leave duplicate copies of static content, such as image files and standard HTML pages, in the `cdml_format_files` folder. This will make it easier for you to maintain your solution, and your site will function normally, but you should be aware that the Web Companion will only access static content from within the Web folder.

For Windows development, we recommend managing your CDML format files together with other related files in a development directory, either in a separate development folder that is not published to the web or in the appropriate sub-folder under the `cdml_format_files` folder. By using a development directory, you can edit your files and preserve the file references used in relative links typically managed by HTML authoring environments. You can then separately publish the public files into the appropriate sub-folder of the Web folder when ready for web users to see, and if needed publish the CDML format files into the appropriate sub-folder of the `cdml_format_files` folder.

For Mac OS development, you can manage your files in the same way using a development directory as described above. Another option is to manage the CDML files in the `cdml_format_files` folder, and use aliases within the `cdml_format_files` sub-folders to point back to the corresponding sub-folder in the Web folder. This will typically resolve any broken link/missing image problems when working in HTML authoring environments. For example, you can have an alias in the `cdml_format_files` copy of the site named 'images' which points back to the images folder in the Web folder, rather than copying the entire images sub-folder under the `cdml_format_files` folder.

**Important** For better security, we do not recommend placing aliases to locations outside of the Web folder within the `cdml_format_files` folder or Web folder.

### ***cdml\_format\_files folder examples***

A request for a format file is handled by following the current path into the `cdml_format_files` folder. If the file is not found there, a second search is performed within the corresponding directory within the Web folder.

- In FileMaker Pro 5.5 a request that included the format file parameter `-format=MyFormat.htm` resulted in a search for `/Web/MyFormat.htm`. In FileMaker Pro 6, the search is made for `/cdml_format_files/MyFormat.htm`. If the file is not found, a second search is performed for `/Web/MyFormat.htm`. If the file is still not found, then the error `Format file not found: The format file "<filename>" could not be found` is returned.
- If a solution is within a sub-directory inside of the Web folder, then a copy of that directory structure must exist within the `cdml_format_files` folder. Assuming you have a Web solution in the `/Web/MyFolder/` directory, a request for the format file `-format=MyFolder/MyFormat.htm` in FileMaker Pro 5.5 would have resulted in a search for `/Web/MyFolder/MyFormat.htm`. In FileMaker Pro 6, the search is made for `/cdml_format_files/MyFolder/MyFormat.htm` first, then, if the file is not found, a second search for `/Web/MyFolder/MyFormat.htm` is performed.

### ***cdml\_format\_files folder tips***

- The `cdml_format_files` folder lies outside of the Web folder. Any HTTP request attempting to access it directly will result in a "file not found" error.
- The `cdml_format_files` folder is intended to be a repository for your CDML format files only. Image files, XSLT and/or CSS style sheets, or other types of files will not be recognized or served by the Web Companion if they are placed in this folder. For convenience, you may place duplicate copies of these files in the `cdml_format_files` folder, but these files can only be served by the Web Companion if they are also present in the Web folder.
- FileMaker, Inc. does not recommend storing databases in the Web folder (or sub-folders). Databases can be stored in any file folder on the system, including the `cdml_format_files` folder. However, their placement in the `cdml_format_files` folder serves no distinct purpose from other folders on the system, and consequently is not recommended.
- The `cdml_format_files` folder will not be accessed by the `-dbopen` action. Databases placed within the `cdml_format_files` folder can be used in a solution. But they must be launched by some means other than the `-dbopen` command. Optionally, you may decide to leave one or more databases within the Web folder in order to use the `-dbopen` command. Because this command is only available when remote administration is enabled, be aware that enabling remote administration also enables support for the HTTP PUT command, which can compromise security in the Web folder.
- The `FMP-Include` tag checks for the path to the `cdml_format_files` folder. No error is returned when this tag is used, since the `FMP-Include` tag is used to add content to a document being processed by the Web Companion.

You do not need to change any code containing the `FMP-Include` tag, since the new behavior of the Web Companion causes it to automatically search for format files within the `cdml_format_files` folder. Protect files containing the `FMP-Include` tag by copying it to the `cdml_format_files` folder.

**Note** With remote administration enabled it is possible to use HTTP PUT to place a CDML format file within the Web folder. Such a file could include the `FMP-Include` tag which could specify a CDML format file that was in the `cdml_format_files` folder. You can prevent such an attack by only enabling remote administration when absolutely necessary.

**Important** Although the FileMaker Pro HTTP server cannot make HTTP requests within the `cdml_format_files` folder directly, this feature is intended to provide security for CDML format files only. This feature is not intended to protect data, provide any additional system integrity, or prevent an attack by other means.

**This page intentionally left blank.**

# Chapter 5

## ***Using SSL protection with Custom Web Publishing***

The Secure Sockets Layer (SSL) protocol is a standardized method for allowing encrypted and authenticated communication between web servers and web browsers. Encryption through SSL converts information being exchanged between web servers and web browsers into unintelligible information through the use of mathematical formulas known as ciphers. These ciphers are used to transform the information back into understandable data by the intended recipient through encryption keys.

The actual instruments used to provide SSL protection are termed *SSL certificates*. SSL server certificates satisfy the need for confidentiality, integrity, and authentication. These certificates form the basis of an Internet trust infrastructure by allowing web sites to offer safe, secure information exchange to their customers. Server certificates are the first step to setting up an SSL environment, and are available from independent, third-party Certificate Authorities (CAs), such as VeriSign ([www.verisign.com](http://www.verisign.com)).

CAs issue certificates to individuals, organizations, and web sites. To implement SSL you must request and then install a digital certificate on a web server. You can enable SSL capabilities after the certificate has been successfully installed.

SSL server certificates fulfill two necessary functions:

- SSL server authentication to allow web users to verify a web server's identity. Web browsers automatically check to see if a server's certificate and public ID are valid and have been issued by a certificate authority (CA).
- SSL encryption to allow a secure channel of communication that enables information sent between a web browser and a web server to be encrypted, preventing information from being intercepted over the Internet. SSL encryption also monitors the integrity of the data being sent over the Internet and determines whether it has been altered in any way during transit. This allows information to be sent securely and confidentially.

**Note** SSL protection is only available to users of Custom Web Publishing with FileMaker Pro Unlimited software, and only through the use of the FileMaker Web Server Connector (FMWSC) and third-party web server software, such as Microsoft Internet Information Server (IIS).

### ***Example: Configuring SSL with Microsoft IIS***

#### ***Part 1: Generating a private key pair and Certificate Signing Request (CSR)***

1. In Microsoft IIS, open Administrative Tools and then the Internet Services Manager. Right-click and select **Properties** for the web site you want.

2. Select the **Directory Security** tab in the Web Site Properties window. In the **Secure communications** section, click **Server Certificate**.

The IIS Certificate Wizard dialog box appears.

3. In the Server Certificate window, select **Create a new certificate**, then click **Next**.

4. In the Delayed or Immediate Request window, select **Prepare the request now, but send it later**, then click **Next**.

5. In the Name and Security Settings window, type a name for the new certificate.

The name should be easy for you to remember.

6. Choose the encryption strength for your server, then click **Next**.

**Note** Choose the highest encryption strength you are permitted. 128-bit SSL is the most powerful encryption compatible with both U.S. and worldwide versions of Microsoft Internet Explorer and Netscape browsers.

7. In the Organization Information window, select or type your organization's name and your organizational unit (your department). Click **Next**.

8. In the Your Site's Common Name window, enter the full domain name for your web site. For Internet sites use a valid DNS. You can also use a computer's NETBIOS name for intranet servers. Click **Next**.

9. In the Geographical Information window, select your country/region, your state/province, and your city/locality. Click **Next**.

10. In the Contact Information window, enter the name, phone number, and email address for the administrator requesting the certificate. Click **Next**.

11. In the Certificate Request File Name window, specify a location to save the certificate request. Depending on how you are requesting the certificate and which Certificate Authority you are using, you may need to copy and paste the certificate request into a web browser or send it via email. Click **Next**.

12. In the Request File Summary window, confirm that the information you have entered is correct, then click **Next**.

The IIS Certificate Wizard should now confirm that you have successfully created a certificate request. If you have not determined which certification authority you would like to use, you can select a link from this window for a list of CAs that offer services for Microsoft products.

13. To close the IIS Certificate Wizard, click **Finish**.

## ***Part 2: Entering your certificate***

1. After you have received your certificate from your Certification Authority (most likely via email), copy the portion that begins with -----BEGIN CERTIFICATE----- to the portion that ends with -----END CERTIFICATE----- and paste it into Note Pad or a similar text editor.

2. Save the file as **Certificate.CER**

**Note** If you have used a different method for obtaining a certificate you may not need to save the file. For example, if you have used a Certificate Server, the .CER file may have been downloaded to a specified location. If you have received a .CER file, you can proceed to the next line.



3. Open Administrative Tools and then the Internet Services Manager. Right-click and select Properties for the web site for which you want to enable the certificate.
4. Select the Directory Security tab in the Web Site Properties window. In the Secure communications section, click Server Certificate.
5. In the IIS Certificate Wizard dialog box, click Next.
6. Select Process the pending request and install the certificate, then click Next.
7. Select the location of the .CER file, then click Next.
8. The IIS Certification Wizard displays the summary of the Certificate. Verify that the information is correct, then click Next.
9. Click Finish to complete the installation of your certificate.

### ***Part 3: Enabling and configuring SSL and other certificate features***

1. In the Secure Communications section of the Directory Security tab for the web site, the Edit button should now be enabled. Click Edit.
2. Select Require secure channel (SSL).
3. Select Require 128-bit encryption, if applicable.
4. Click Apply, and then click OK to enable SSL and close the property window.

**Note** You can also specify how your site will handle client certificates, enable client certificate mapping, and enable the certificate trust list in this property window.

### ***Part 4: Testing your new SSL enabled web site***

1. Attempt to access your site by typing `http://localhost/Postinfo.html` in the address bar of your web browser.

You should receive an error message:

The page must be viewed over a secure channel

The page you are trying to view requires the use of "https" in the address.

HTTP 403.4 – Forbidden: SSL required

Internet Information Services

**Note** The Postinfo.html page is a standard HTML page found in the root folder of the default web site.

2. Attempt to access the same web page by typing `https://localhost/Postinfo.html` in the address bar of your web browser.

If you can view the Postinfo.html page you have successfully installed the certificate.

**Note** You may see a security alert stating that the certificate is not from a trusted root CA. Ignore this alert, and click Yes to continue to the web page.

**This page intentionally left blank.**

# ***Index***

## **A**

- access log file 15
- access privileges
  - compared to Web Security Database 12
  - defining 17
  - described 13
  - record-level protection 19
  - using with Custom Web Publishing 22
  - using with Instant Web Publishing 10
- AirPort technology, data security with 6

## **B**

- blank passwords 17

## **C**

- CDML format files 16
  - protecting 43
- CDML tags 22
- cdml\_format\_files folder
  - about 16
  - using 43
- certificates 47
- CGI applications 7
  - script commands 22
- ciphers 7, 47
- Custom Web Publishing
  - access privilege protection 22
  - Web Security Database protection 23–27

## **D**

- databases, designing for security 8
- dbclose CDML tag 16
- dbopen CDML tag 16, 44
- default.htm 36
- design tips, for web publishing 8
- DontSearch 24, 34
- DontShow 24, 34

## **E**

- encryption keys 7, 47
- equipment security 5
- ExactDelete 26, 34
- ExactSearch 25, 34
- ExactUpdate 26, 34

## **F**

- fields, displaying on Web layouts 11
- FileMaker Pro Unlimited 8, 42
- FileMaker Solutions Alliance 12
- firewalls 6
- FMP-Include tag 44
- FMWSC 8, 42
- FSA members 12

## **G**

- groups, passwords for 14
- guests, restricting access to 15

## **H**

- hardware, securing 5
- host machine 5
- HTML files
  - in Web Security Database 14, 25, 36
- HTTP PUT command 16, 44
- HTTP server 7, 43

## **I, J, K**

- Instant Web Publishing
  - access privilege protection 17–22
- IP addresses, restricted access 15, 19, 24

## **L**

- layouts, for web publishing 21
- log data on users 15

## **M, N, O**

- master passwords 10, 23
- Microsoft Internet Information Server (IIS) 8, 47

## **P, Q**

- passwords 13
  - blank 17
  - defining 17
  - master 10, 23
- Postinfo.html 49

## **R**

- ReadOnly 24, 34
- record-by-record protection
  - using access privileges 19
  - using Web Security Database 24, 35
- remote administration
  - and cdml\_format\_files folder 44
  - risks with enabling 16
  - setting up 36

## **S**

- scripts 9, 12, 22, 41
- Secure Sockets Layer (SSL)
  - about 7
  - using 47
- security, in database design 8

## **T**

- TCP/IP 6
- testing security 11

## **U, V**

- underscore character 11
- user names 14

## **W**

- Web Companion
  - about 7
  - security features of 15
- Web folder 16, 43
- web layouts 21
- web security
  - access privileges vs. Web Security Database 12
  - design considerations 8
- Web Security Database
  - compared to access privileges 12
  - described 14, 29
  - enabling 24, 30
  - installing 30
  - record-level protection 24, 35
  - using 23–27, 32–42
- Web Security folder 36
- Web Security.fp5 23, 32
- web servers 7
- wireless technology, data security with 6

## **X, Y, Z**

- XML 22, 44