

FileMaker® 8

Security Guide



© 2004–2005 FileMaker, Inc. All Rights Reserved.

FileMaker, Inc.
5201 Patrick Henry Drive
Santa Clara, California 95054

FileMaker is a trademark of FileMaker, Inc., registered in the U.S. and other countries, and ScriptMaker and the file folder logo are trademarks of FileMaker, Inc.

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 persons and companies listed in the examples are purely fictitious and any resemblance to existing persons and companies is purely coincidental.

Credits are listed in the Acknowledgements document provided with this software.

For more information, visit our web site at www.filemaker.com.

Edition: 01

Contents

Chapter 1

About database security

About this guide	5
Security goals	5
Potential threats to your data	6
Planning security	7

Chapter 2

Security “Top 10” list

1. Enhance physical security	9
2. Enhance operating system security	9
3. Establish network security	10
4. Devise a plan for securing your databases	10
5. Restrict data access with accounts and privilege sets	11
6. Back up databases and other important files	12
About FileMaker Pro file recovery	13
7. Install, run, and upgrade anti-virus software	14
8. Test your security measures	14
9. Assess, iterate, and improve security measures	14
10. Upgrade to FileMaker Pro 8 and FileMaker Server 8 for security enhancements	15
Security enhancements in FileMaker Pro	15
Security enhancements in FileMaker Server	15

Chapter 3

Build security into your solutions

Restrict access with accounts and privilege sets	17
Tips for restricting file access	18
Tips for creating effective passwords	19
Considerations when hosting files with FileMaker Server	19
Web publishing security considerations	20
Tips and considerations when designing databases for web publishing	20
Protecting your databases from web-based attacks	22
Web server security	23
Use encryption or VPNs to protect data	23
Using Secure Sockets Layer (SSL) security for web publishing	23
About wireless networks	24
XML considerations	24
Considerations for Apple events and ActiveX	24

Chapter 1

About database security

FileMaker® Pro software enables you to create databases that can be used individually, shared on a peer-to-peer basis, shared using FileMaker Server, accessed via ODBC or JDBC, or shared within an intranet or with Internet users. It is critical that you think about what data is being shared, what types of vulnerabilities exist, and how to protect data and database files.

In some cases, data is not particularly sensitive, business-critical, or confidential, or the software itself is used by one individual in a secure location, or in an open, trusting environment where security considerations are not a concern. In most cases, however, data is business-critical or sensitive, and you must take steps to protect it. You should plan and implement security measures in all phases of design, testing, and deployment.

About this guide

- This document addresses security concerns for FileMaker versions 7 and 8. For information on security for previous versions of FileMaker Pro, download documents from www.filemaker.com.
- To keep current on FileMaker security issues, visit the FileMaker Security web site at www.filemaker.com/support/security, where you can sign up to receive the FileMaker Security newsletter.
- For step-by-step information on FileMaker Pro features, including defining accounts and privileges to protect database files, refer to FileMaker Pro Help.
- FileMaker Pro documentation uses the term *web publishing* to refer to databases that users can access on the Internet or on an intranet using a web browser.
- This guide uses “FileMaker Pro” to refer to both FileMaker Pro and FileMaker Pro Advanced, unless describing specific FileMaker Pro Advanced features.

Important You can download PDFs of FileMaker 8 documentation from www.filemaker.com/downloads. Any updates to this document are also available from the web site.

Security goals

There are three general issues to consider in protecting your FileMaker databases:

- Privacy
- Integrity
- Availability

Privacy of data

When designing and deploying any database, you have a responsibility to ensure that unauthorized people cannot access the data.

Integrity of data

Design a system open enough to allow authorized users to create and update data while preventing unintentional changes. You must also restrict access to unauthorized people who might try to tamper with the files. Unfortunately, there are individuals who might attempt to access your information systems and steal corporate assets.

Availability of data

Databases should only be available to users as necessary. This is a basic, but frequently overlooked, consideration. Database designers and network administrators must consider not only hackers, but also employees who have more access than is critical. Make it a design goal to provide access, both to data and to specific features, only to those who really need it. Do not enable any sharing options, like web publishing, unless it is necessary.

Potential threats to your data

You must protect your data and database design from both unintentional and intentional changes. Someone might try to copy aspects of your design, look at the data entered by your users, damage the system (perhaps using someone else's user ID), enter false data, ruin your reports and layouts, corrupt calculations, or break scripts.

The most common threats to your data include:

- Unintentional threats from known parties and accidents. Authorized users can inadvertently make mistakes, see data they shouldn't see, delete or change records that they shouldn't have access to, and delete or damage files so that the system becomes unavailable.
- Intentional threats from known parties. Consider hackers who will benefit from accessing data that they shouldn't see, who might falsify data, or intentionally try to damage the data.
- Uninvited intruders or threats from anonymous parties. Mostly, these are Internet-based threats from intruders with anonymous access who attempt to steal information, cause damage, or make web systems unavailable.

It is important to note that small businesses and larger workgroups may face the same threats, especially on the Internet. Employees in small businesses and home offices may assume they are safe because they have a low profile, but this is no longer true. Hackers use automated tools to detect and break into vulnerable systems. The value of the data will usually determine the time and resources a hacker will invest in attempting to crack a system. Often the goal of the attack is just to find a system that can be used to confuse the trail involved with attacking another target.

Small businesses are generally easier to get access to than larger organizations because they often lack good perimeter defenses (for example, firewalls maintained by experienced network administration staff), and don't have baseline security standards for their computer systems (for example, if all computers aren't using the most secure operating system versions).

Outside intruders frequently want access to the data of a workgroup or small business. Occasionally their goal is to disable the system, but it's more common to attempt to gain access to sensitive information, such as credit card numbers or identification information like passwords, and birth dates. Intruders are assumed to be located far away from the workgroup and likely to have little direct knowledge of the system. They use automated scripts to locate systems that have well-known weaknesses. Only a modest amount of security is needed to make them pick another target.

Planning security

Start by mastering the FileMaker Pro built-in security features: accounts and privilege sets. Plan on taking a flexible, multi-layered, and iterative approach to security.

- Your security plan should be flexible enough to consider an individual's unique data access requirements.
- Layer security at every area of access, including locking down computers, setting accounts and privileges in the databases, restricting access to directories, and taking other steps to protect the data.
- Continually evaluate your security to make sure it is still protecting your data. This includes verifying that users have the latest, most secure software versions, changing passwords on an ongoing basis, evaluating log files to avoid surprises, and rigorously following a backup scheme. Configure and test security options as you add structure and data to your files over time.

The table below shows how a developer or network administrator might assess variables in the workplace and associated risks.

Workplace variables	Effect on risk level
Inexperienced data entry staff; high turnover; new computer users	High risk of unintentional threats caused primarily by data entry mistakes and poor backup techniques.
Inexperienced database designer	<ul style="list-style-type: none"> • High risk of unintentional threats caused by employees having inappropriate file and database feature access. • Employees may introduce unintentional threats by sharing files without taking proper security measures. • Data is exposed if FileMaker Pro accounts and privileges are not configured correctly to protect files adequately.
Inexperienced network administrator	<ul style="list-style-type: none"> • High risk of unintentional threats caused by inadequate operating system security, poor backup techniques. • Poor network security increases the risk of intentional threats, particularly if files are shared over the web or on a wireless network. • Risks are also introduced if shared files are accessed from file servers instead of using the built-in network sharing in FileMaker Pro and FileMaker Server. Employees can make inappropriate copies of the files and can introduce record locking and potential corruption issues when files are shared with inappropriate methods.
Poor physical security	High risk of intentional threat due to possible computer theft.
Databases store sensitive or valuable data	Increased risk of intentional threats of data theft, particularly if data is shared over the web or if access to data isn't adequately monitored and protected.

Chapter 2

Security “Top 10” list

Be sure that your database files, host computers, workstations, and the networks that access them are safe from theft and corruption. This chapter covers ten security measures that you can implement to protect your data and equipment. This “Top 10” list includes the following:

- Enhance physical security
- Enhance operating system security
- Establish network security
- Devise a plan for securing your databases
- Restrict data access with accounts and privilege sets
- Back up databases and other important files
- Install, run, and upgrade anti-virus software
- Test your security measures
- Assess, iterate, and improve security measures
- Upgrade to FileMaker Pro 8 and FileMaker Server 8 for security enhancements

Each of these measures is detailed further in the rest of this chapter.

1. Enhance physical security

Evaluate your computers to make sure they are physically secure:

- The host computer should be a dedicated machine, anchored to a desk or immovable object with a lock. Secure the computer so that its hard drive cannot be removed. Restrict access to the computer by storing it in a locked room.
- Secure the client workstations that access a database. Lock the computers down and restrict access by using a screensaver that requires a password.
- Ensure the physical security of backup copies of files stored on portable media, such as tapes and CDs.

2. Enhance operating system security

Use the security features of your operating system to restrict access to important data. The network administrator should provide access only to individuals authorized to administer and maintain the system or the FileMaker databases. In addition, they should:

- Track system user IDs and passwords.
- Restrict access to the FileMaker Pro application and file directories, servers, and web pages.
- Review remote access settings for file sharing and FTP.
- Restrict file upload or download access.
- Make sure all users have the latest, most secure versions of operating system software.

- To streamline processes, you can enable external authentication, which uses accounts that have been configured in the Windows Domain Authentication or in Apple OpenDirectory. For more information, see “Security enhancements in FileMaker Server” on page 15.
- Do not put FileMaker Pro files on file servers to share them. Use the built-in networking feature in FileMaker Pro and FileMaker Server. This prevents the files from being inappropriately copied or from introducing record locking and potential corruption issues when files are shared with inappropriate methods.

3. Establish network security

Databases shared on an intranet or the Internet use the TCP/IP protocol. You may also use the TCP/IP protocol when you share databases peer-to-peer, or with FileMaker Server. Though TCP/IP is good for moving data and allowing clients to connect to your data, it was not designed with security as a primary objective. Unless you take precautions, it can provide uninvited access to your host computer, server software, databases, and perhaps to other client machines on your internal network. TCP/IP doesn't provide very much protection for data, so it is important to place barricades such as firewalls and SSL data encryption in the path of uninvited visitors. For more information on third-party products such as encryption programs, see “Use encryption or VPNs to protect data” on page 23.

- The most common barricade method used is the firewall, which separates your network into two distinct environments: a public environment that is “outside the firewall,” and a private environment that is “behind the firewall.” Users outside of the firewall will only have access to those TCP/IP or hardware addresses that you expose. You can concentrate your security on those server machines that are exposed, while allowing machines behind the firewall to operate with fewer safeguards.
- Using wireless networking devices, like the Apple AirPort and other 802.11b networking cards and base stations, can pose 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. Always use the maximum level of signal encryption available. For more information, see “About wireless networks” on page 24.

4. Devise a plan for securing your databases

When you plan your database design, also plan how to secure your FileMaker database files. It's much easier to design security into your database than to incorporate it later.

- List the areas of the file that you want to protect, such as particular tables, fields, records, layouts, value lists, and scripts. Plan the number of privilege sets you need to enforce the varying levels of file access that you require.

- Determine if you need individual accounts for each user (recommended), or accounts that multiple users can share (such as a “Marketing” or a “Sales” account).

It is possible to create a small number of accounts that are shared among many individuals (such as a “Marketing” account and a “Sales” account). However, keep in mind that shared accounts are a security risk. For better security, use individual accounts instead of shared accounts. If you intend to use shared accounts anyway, make sure you limit the access capabilities of the privilege sets that shared accounts use. Change the password occasionally, particularly when certain users no longer require access.

- Decide if you want to enable the Guest account, which permits users to open the file without logging in and providing account information. If you’re using the Guest account, assign the most limited privilege set possible; otherwise, consider disabling it.
- Determine if you need to enable any extended privileges (for example, FileMaker Network sharing or Instant Web Publishing) for certain privilege sets.
- Create the accounts you need in the file, and assign the appropriate privilege set to each account.

Consider developing a grid that lists the types of users and summarizes their privileges:

Type of users	View records	Create records	Edit records	Delete records	Modify scripts	Execute scripts	Modify Value lists	Menus
Managers	Yes	Yes	Yes	Yes	Yes	Yes	Yes	All
Marketing	Yes	Yes	Yes	Limited*	Limited*	Yes	No	Editing only
Sales	Yes	Yes	Yes	Limited*	No	Yes	No	Editing only
HR	Yes	Yes	Yes	Yes	Yes	Yes	No	All
Legal	Yes	No	No	No	No	Yes	No	Minimum
Guests	Yes	No	No	No	No	No	No	Minimum

*You can provide limited access to some features, for example deleting records, by using record-by-record privileges. For more information on record-by-record privileges, see FileMaker Pro Help.

5. Restrict data access with accounts and privilege sets

Use accounts and privilege sets to provide the most basic security method within FileMaker Pro files. With accounts and privilege sets, you can limit what users can see and do in a database file. You can restrict:

- File access: Require users to enter an account name and password in order to open a file.
- Data access: Make particular records or fields from individual tables view-only, or hide them completely.
- Layout access: Prevent users from viewing or modifying layouts in Layout mode.
- Access to value lists and scripts: Prevent users from accessing and modifying value lists and scripts, and from running scripts.

- Outputting data: Prevent users from printing or exporting data.
- Menu access: Make only a limited set of menu commands available.

When files are restricted with accounts, users must know the account name and password before opening or connecting to a database. The account name and password they enter determines which privilege set will be used, which limits what they can do in a file. For more information about accounts and privilege sets, see “Restrict access with accounts and privilege sets” on page 17.

Tips

- Your security is only as good as the user accounts and passwords you define. For more information, see “Tips for creating effective passwords” on page 19.
- Do not share your administrator-level user account name and password with anyone. This protects your files in the event that your physical security, operating system security, or network security has been bypassed.
- FileMaker Server can be configured to allow databases to perform external server authentication based on group names in place of accounts/passwords stored in the database. For increased security, do not assign the Full Access privilege set to an External Server account type. For more information, see “Security enhancements in FileMaker Server” on page 15.

Important A new FileMaker Pro file is initially unprotected. When opening files, users are automatically logged in with the Admin account, which is assigned the Full Access privilege set. To prevent others from opening a database with full access, rename the Admin account and assign a password. Before sharing the file with others, plan the security of the file and assign the necessary access levels to each user.

6. Back up databases and other important files

Develop plans for restoring data, including alternate sites and systems to run business-critical information services. A current backup can help you recover from a situation where someone loses the administrator account information for a file, or from a situation where user error (and sometimes bad database design) causes data to be deleted or modified inappropriately.

Keep the following in mind:

- Host databases with FileMaker Server and create regularly-scheduled, automated backups. Don't use third-party backup software on hosted FileMaker Pro databases. First, use FileMaker Server to make a backup copy of your database, then run your third-party backup software on the copy. Backup software can damage open, hosted databases.

For example, make local backups of files at 6:00 am, 9:00 am, 12:00 noon, 3:00 pm, 6:00 pm, and 11:30 pm weekdays. At midnight, make an incremental backup of the entire system to the enterprise backup system. Finally, Friday night at midnight, perform a full system backup. Copy and store the backup tapes at a remote location. This way, if the server goes down for some reason other than catastrophic failure of multiple drives, the more recent backup of the data files can be used, meaning a maximum of 3 hours of lost data. If there is a catastrophic drive failure, then the previous evening's tape can be used, minimizing the loss to one day's data. Of course, these procedures can be tailored to your situation and data value.

- Make sure backup copies aren't damaged or inaccessible. Verify that they are functioning properly *before* you need them. Run diagnostic tools on your hard drive and your backup files regularly.
- Ensure that you can restore an entire set of files from backup copies.
- Regularly export the data to protect against file corruption.
- Protect the backup media itself. Store backups in a separate and fire-proof location.
- Assign backup administrators who can retrieve files, in case the network administrator is unavailable.
- Plan for redundancy. If the power goes off, a universal power supply (UPS) should sustain power for at least 15 minutes, enabling you to safely close all files. If the power can't be restored in a timely fashion, consider using a generator to supply power to servers. Also consider power sources for routers and firewalls. Will communication be a problem if your Internet access is interrupted for 48 hours or longer?
- Consider how you will continue to provide services if an intruder takes down your database server and that server can't be restored to its previous condition.
- Evaluate additional scenarios that could occur, and create a plan to respond to each one.

Also, network administrators should assess risks to data systems and business-critical functions. For example, consider:

- Theft of data or theft of proprietary intellectual property.
- Disruption, theft, or damage to network infrastructure such as servers, networks, data storage, or data backup storage. Damage can be caused by password crackers or by other types of malicious sabotage and destruction. Most incidents originate from within the organization.
- Disruption or damage to the organization infrastructure such as building fires, environmental or biological hazards, floods, and so on.
- Disruption or damage to the public infrastructure, including electrical power, telecommunications (voice and data), transportation grids (roadways, buses, trains) caused by environmental conditions, or severe weather such as tornadoes or floods.

Important In the event of a server failure, such as an unexpected loss of power, hard drive failure, or software failure, use the backup files. Any system failure causing FileMaker Server to shut down inappropriately can result in corrupted files if cached data was not written to disk and the files were not closed properly. Even if the files re-open and go through a consistency check or recovery, corruption might be buried in the file. File recovery cannot guarantee that problems have been fixed.

About FileMaker Pro file recovery

Use the recovery feature when a database file is closed inappropriately and the data since the last backup must be recovered. Recovery creates a new file with a name different than the original file because it is not intended to replace the file. It is an aggressive process which might remove layouts, scripts, etc. in order to return the most data possible. The data should be exported from the recovered file and imported into a clean backup of the original database file.

Because recovery can take a long time, make local backups at an interval relating to the amount of data that could be lost.

7. Install, run, and upgrade anti-virus software

Because most computers have Internet access, they are vulnerable to viruses being transmitted through email attachments. Make sure all employees run anti-virus checking software regularly, and that they are aware of typical virus warning signs. Employees should scan all files before copying or downloading them to their computer, and they should never open unsolicited attachments, even if they're from someone they know.

Note Do not run virus protection software on open, hosted databases. First, close the databases, then run the virus protection software.

8. Test your security measures

It is important to test all scenarios to make sure user accounts are working as expected with all sharing technologies.

For example:

- Open the file using different user accounts and test each privilege set that you create. Make sure the restrictions work as planned, and make any needed corrections to your privilege sets.
- Test navigation and scripts with all user accounts. Because accounts might have different privileges, consider that access to some features, like layouts, tables, and script steps might not work for all users.
- If users are accessing your databases a variety of ways, for example, on the web with Instant Web Publishing, XML, or JDBC, test accounts from those technologies as well.
- If you're publishing files on the web, open scripts and enable **Indicate Web Compatibility** to ensure that all steps are supported. If your scripts contain steps that are not web-compatible, the **Allow User Abort** script step determines how subsequent steps are handled. For more information, see the *FileMaker Instant Web Publishing Guide*, located in the Electronic Documentation folder (inside the English Extras folder).
- Test for unexpected results. For example, open files with different user accounts and attempt to perform actions that users are not authorized to perform. Consider removing access to privilege sets where possible.
- Recruit other developers to try to access your data inappropriately.
- Run tests periodically; not just during development, but after deployment as well.

9. Assess, iterate, and improve security measures

It's important to take an iterative approach to security. For example, when new users access the database, you should re-evaluate the appropriate level of access to the data itself and the database structure, depending on the new users' job duties or roles in a company.

Ask yourself the following questions before developing a FileMaker Pro database, and on an ongoing basis, as the files change over time:

- What is valuable?
- Why is it valuable?
- How valuable is it?

- How damaging would its loss or disclosure be?
- What is the minimum level of security to prevent loss or disclosure?
- What tools can I use to implement that security?

To assess security, enable log files in FileMaker Pro and FileMaker Server and review users’ actions. You can also track actions if you include scripts and calculations that capture the user’s account name, password, and IP address.

10. Upgrade to FileMaker Pro 8 and FileMaker Server 8 for security enhancements

Security was redesigned in FileMaker Pro 7 and FileMaker Server 7. If you are upgrading from a pre-7.0 version, use the new security model for a more robust and streamlined user experience when assigning accounts and privilege sets.

Security enhancements in FileMaker Pro

- The security model is more intuitive, and functions similarly to other tools. You can create user accounts and passwords, and share privilege sets for multiple users and tables.
- Because FileMaker Pro supports multiple tables within a file, you can protect a single-file, multi-table database with one set of accounts and privilege sets.
- You can use the Get(AccountName) function to determine the current user in functions and scripts. This opens many possibilities, such as creating scripts that can only be run by particular account names.
- You can require users to specify a new password when they next open the database, and enable settings that require users to change their passwords after a specified number of days.
- You can set a minimum character length for passwords.
- With FileMaker networking, account names and passwords use a one-way encryption algorithm that prevents them from being deciphered by password-cracking tools. User account names and passwords are verified on the host computer, preventing hacking attempts on the client computer, or attempts to crack passwords with the executable or temp files. You must store your account name and password in a safe location. If you lose the account name and password, you will have to re-create the files.

Security enhancements in FileMaker Server

When you host databases with FileMaker Server, you can take advantage of a number of features that make your data more secure for both FileMaker Pro and web-based clients. For information on specific features, see the *FileMaker Server Advanced Web Publishing Installation Guide*, or the *FileMaker Server Administrator’s Guide*.

- To encrypt the user account information and the data with FileMaker networking, enable Secure connections to FileMaker Server.
- If you’re sharing files to web-based clients, enable SSL encryption in a web server application to encrypt data that is passed from the host to guest computers on the web. For more information, see “Using Secure Sockets Layer (SSL) security for web publishing” on page 23.

- You can enable and disable specific extended privileges, such as Instant Web Publishing, XML, and XSLT for the Web Publishing Engine. For example, if you know that all files on one server will be shared with Instant Web Publishing, you can disable all other types of web publishing. Even if a file includes extended privileges that allow access to XML data, access to XML data is not available while the file is hosted with that Web Publishing Engine. For more information, see the *FileMaker Server Advanced Web Publishing Installation Guide*.
- If your organization uses centrally managed authentication for users and groups such as Apple OpenDirectory or a Windows Domain, you can set up accounts that authenticate users based on your authentication server. This allows you to use your existing authentication server to control access to databases without having to manage an independent list of accounts in each FileMaker Pro database file. For more information on authenticating accounts with external servers, see the FileMaker Server Help.

Important When a database file contains one or more External Server accounts, make sure you use operating system security settings to limit direct access to the file. Otherwise, it might be possible for an unauthorized user to move the file to another system that replicates your authentication server environment and gain access to the file. Group names for accounts authenticated with the external server feature are stored as text strings. If the group name is reproduced on another system, the copied file can be accessed with the privilege set assigned to the members of the group, which might expose data inappropriately.

- Enable log files and file backup features for effective, easy database maintenance.

Chapter 3

Build security into your solutions

Developers and network administrators must assume the responsibility for managing security in the design and deployment of their database files, and for managing security on a routine basis.

Restrict access with accounts and privilege sets

The primary way to protect your files is to define accounts and privileges in FileMaker Pro. It's a good practice to restrict access to every file, with an Admin password that only you know. This will protect files if other security measures have been bypassed.

Important For information about how security settings in pre-7.0 databases convert to the current version of FileMaker Pro, see *Converting FileMaker Databases from Previous Versions*. See FileMaker Help for detailed, comprehensive information and step-by-step procedures about using account names, passwords, and privilege sets.

Accounts authenticate users who are attempting to open a protected file.

- Each account specifies an account name and (optimally) a password.
- Each database file contains two predefined accounts: Admin and Guest. The Admin account, which should be renamed for better security, is assigned the Full Access privilege set. The Guest account, which cannot be renamed, permits users to open a file without providing an account name and password. By default, the Guest account is assigned the Read-Only Access privilege set, but you can assign a different privilege set in Accounts and Privileges.
- For maximum security, create a unique account for each user.

Privilege sets specify a level of access to a database file. Each database file contains three predefined privilege sets: Full Access, Data Entry Only, and Read-Only Access.

- Each account is assigned one privilege set, which determines the level of access when someone opens a file using that account.
- You can create privilege sets to limit database access, such as which layouts and menus are available and whether printing is permitted. Privilege sets can also restrict access to records or fields from particular tables within a file.

Extended privileges determine the data sharing options that are permitted by a privilege set. You can enable privileges to access files shared with a FileMaker network, via Instant Web Publishing, Custom Web Publishing with XML or XSLT, from ODBC or JDBC clients, and FileMaker Mobile. All extended privileges are disabled by default.

Important For maximum security, create accounts that require user names and passwords for all files. Take advantage of the security features by requiring users to change passwords after a specified duration and specifying a minimum character length for passwords.

Tips for restricting file access

- Avoid automatically logging in with an account name and password specified in the File Options dialog box.
- Using the same password in each file is often convenient when users must interact with several solution files in one session. This no longer works when users change their own password (unless they change them in all files). When you create accounts, you must create them in all solution files. For convenience, you can define multiple tables in one file. Consider hosting files with FileMaker Server and using an external authentication server, such as Windows Domain or Apple OpenDirectory. For more info, see “Security enhancements in FileMaker Server” on page 15.
- If accounts are used by multiple people, change the password on a regular basis. Also, change the account name and password when people leave the group.
- Create a startup file that only interacts with critical files via scripts. The startup file doesn’t store data; instead data is moved to more critical files via scripts. Have users open the file with the default account name and password that restricts access to sensitive data and risky features, like deleting records. The scripts can perform actions you would not provide users access to, like deleting records, by enabling Run script with full access privileges.
- You can set record access privileges to view, edit, and delete certain records within each table. Limit users’ access to specific records based on a number of criteria, for example their department, job title, job responsibilities, and so on. For more information on record access privileges, see FileMaker Pro Help.

Important Limiting access to specific records introduces a more complicated data access model. Thoroughly test your solution by logging in with different user accounts and evaluating all layouts, reports, and scripts. Be sure to document the specific conditions so users will know what to expect.

- Don’t use layouts for security. The only way to protect files, for example from CGI requests or other sources, is by restricting account access on a field-by-field or table basis. For more information, see the FileMaker Pro Help topic on how layouts privileges and record privileges interact.
- If you’re converting databases from pre-7.0 versions of FileMaker Pro, be sure to review all file references in your solution, and delete the ones you don’t need. The File References dialog box displays information like folder locations and IP addresses, which can reveal information you don’t want to distribute. Review the conversion log file for information about the status and possible problems found during conversion. For more information, see *Converting FileMaker Databases from Previous Versions*
- With FileMaker Pro Advanced, you can permanently remove the Full Access privilege set and any accounts that are using the Full Access privilege set (including the Admin account). This action cannot be undone. It should only be done when you are certain no one will need to have full access to the file again. For more information, see the *FileMaker Pro Advanced Development Guide*.

Tips for creating effective passwords

- Secure passwords are more than eight characters in length, and include mixed upper and lowercase letters and at least one numeric digit. Consider combining two unrelated words, and swapping letters out for numbers, for example, b0att!me (swapping a zero for “o” and an exclamation point for an “i”).
- If files are web-published, account names and passwords should only use printable ASCII characters, for example a-z, A-Z, and 0-9. For more secure account names and passwords, include punctuation characters such as “!” and “%,” but do not include colons. If you’re hosting databases with FileMaker Server Advanced, enable SSL encryption.
- 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 the words *password*, *default*, *master*, *admin*, *user*, *guest*, *client* and similar standard terms.
- Change passwords frequently, perhaps every 30 or 90 days.
- Use passwords only once.
- Wherever possible, assign a unique password for each user. If you must share user accounts, be sure to change the password regularly.
- Do not record your passwords in a master file or list unless the file or list is well secured.
- Do not share user accounts with other users; users should only receive account names and passwords from file administrators.

Considerations when hosting files with FileMaker Server

Keep the following points in mind when hosting databases with FileMaker Server:

- If you enable remote access, be sure to require a password. See the FileMaker Server online Help for more information.
- Store FileMaker Pro files on a local server (not on network directories). One of the most important performance factors is reading and writing data quickly to disk.
- Disable file sharing or ensure that files hosted by FileMaker Server cannot be accessed directly by users. If a FileMaker Pro file can be copied from a file server, it is vulnerable to attack “off line.” For example, group names for accounts authenticated with the external server feature are stored as text strings. If the group name is reproduced on another system, the copied file can be accessed with the privilege set assigned to the members of the group, which might expose data inappropriately. For more information, see “Security enhancements in FileMaker Server” on page 15.
- Suppressing a filename in the Open Remote dialog box, or the Instant Web Publishing Database Homepage is not a replacement for using accounts and privileges to protect a file.
- FileMaker Server command line interface (CLI) commands can include account names and passwords. Make sure that unauthorized users cannot view passwords that are part of CLI commands typed onscreen. To limit access to script files and batch files that contain CLI commands with passwords, use the file ownership and permissions features of your operating system.

Web publishing security considerations

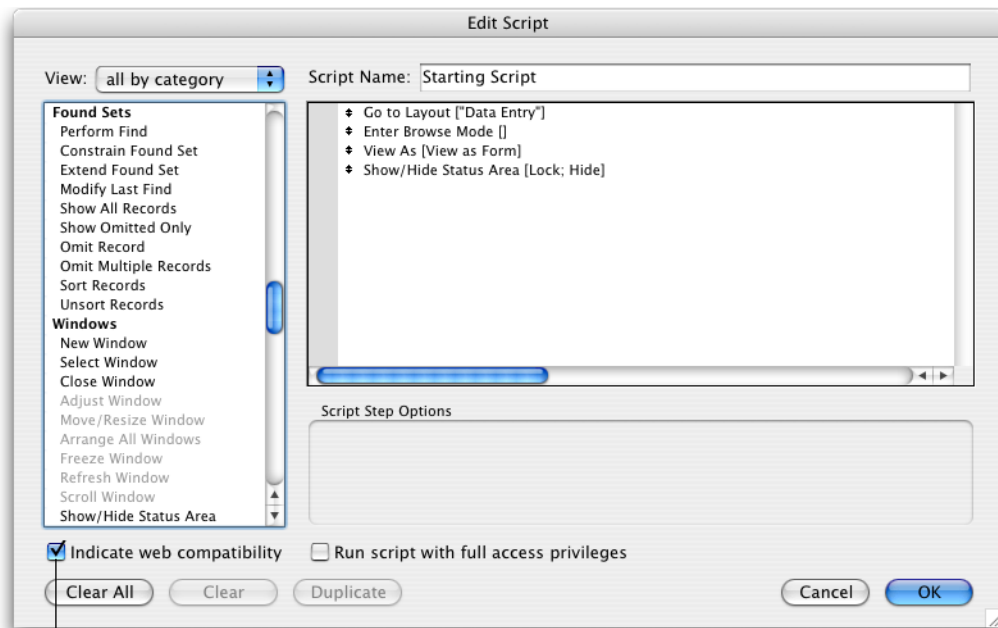
FileMaker Pro software enables you to publish databases to your intranet or the Internet, so that users can browse, search, and update the databases using web browser software. This introduces more risk than sharing files with other FileMaker Pro clients.

Tips and considerations when designing databases for web publishing

1. Define accounts and privilege sets.
 - Protect all files with user names and passwords. You can use the Guest account, which logs in with a default user name and password, if it's not practical to use unique accounts for clients. However, this makes your file available to anyone who has the IP address or domain name of the computer hosting the database.
 - Assign privileges to modify data and database structure only if necessary.
 - Enable only the required web publishing extended privileges. For example, if you are only using Custom Web Publishing with XSLT, enable its extended privilege in the appropriate privilege sets, but leave other web publishing extended privileges disabled.
2. If you are converting solutions from pre-7.0 releases, note that the Web Security Databases are no longer supported. You must transfer the accounts, passwords, and associated privileges into your converted database files in FileMaker Pro. See *Converting FileMaker Databases from Previous Versions* for more information.
3. For increased security, FileMaker Pro clients can no longer publish remotely accessed databases on the web. You can only publish files on the web from the host computer.
4. In Instant Web Publishing, you are no longer limited to predefined layouts for viewing data. All layouts are available to web users, based on their accounts. You can restrict layouts for accounts with privilege sets, but you should not rely on layouts for security. Manage access to data with tables, records, fields, scripts and value lists for the best security.
5. If Instant Web Publishing clients do not click the Instant Web Publishing Log Out button or execute a script that includes the Exit Application step, the connection to the database is still active. Data may be accessible to other web users or users might be prevented from accessing the file. In addition, web users should quit the browser to clear the account information from the web browser cache file. For more information, see the *FileMaker Instant Web Publishing Guide*, located in the Electronic Documentation folder (inside the English Extras folder).
6. Select Don't display in Instant Web Publishing homepage in the Sharing dialog box to suppress a filename from appearing in the built-in Instant Web Publishing Database Homepage. This is useful if your solution includes multiple files and you don't want all the filenames displayed. This feature should not replace defining accounts and privileges in files.

7. Consider the results of scripts.

- If a script includes a step to delete records, and a web user opens the file with an account that doesn't allow record deletion, the step to delete records won't be executed. However, the script might continue to run, which could lead to unexpected results. Consider enabling **Run script with full access privileges** to allow scripts to delete records or perform other restricted actions that users normally don't have access to with accounts and privileges. You can also restrict users from executing a specific script by modifying their privilege set and specifying scripts that have **No access** for particular users.
- Databases published on the web should include scripts that have no harmful effects if they are executed by any web user. To see script steps that are not supported, open the script and select the **Indicate web compatibility** checkbox in the Edit Script dialog box. Dimmed script steps are not supported on the web.
- If your scripts contain steps that are unsupported, for example, steps that are not web-compatible like **Send Mail**, or that users don't have privileges to execute, use the **Allow User Abort** script step to determine how subsequent steps are handled. For more information, see the *FileMaker Instant Web Publishing Guide*, located in the Electronic Documentation folder (inside the English Extras folder).



Select **Indicate web compatibility** to dim script steps that are not web-compatible

8. Do not store database files or any sensitive data in the FileMaker Pro Web folder (or sub-folders).
9. Enable log files to track the IP address of users who are accessing your web published files (as well as the date and time of requests, and other options).
10. With FileMaker Pro, you can limit access to users who use an IP address that you specify in advance. When hosting files with FileMaker Server Advanced, you can set limitations on client IP addresses in the web server application.

11. If you are hosting web-published databases with FileMaker Server Advanced, you can use additional security measures like SSL encryption that may be available with your web server application. For more information, see “Using Secure Sockets Layer (SSL) security for web publishing” on page 23. You can also disable the web publishing technologies that you are not using. For more information, see the *FileMaker Server Advanced Web Publishing Installation Guide*.
12. If you are hosting web-published databases with FileMaker Server Advanced, the Web Publishing Engine uses certain ports and protocols to communicate with FileMaker Server Advanced and your web server. You may have to open ports or allow protocols on your host computers and firewalls. For more information, see the *FileMaker Server Advanced Web Publishing Installation Guide*.
13. If you are hosting databases with FileMaker Server Advanced and using Custom Web Publishing with XML, you can test your security from a web browser to see which elements might be exposed:
 - To view the names of the databases that are published on the web with XML, enter this address in your browser:
`http://<ip:port>/fmi/xml/fmresultset.xml?-dbnames`
 - To view databases published on the web with XSLT, enter this address:
`http://<ip:port>/fmi/xsl/styleSheet_name.xsl?-grammar=fmresultset&-dbnames`
 - To view the fields for a record in your database, enter this address in your browser:
`http://<ip:port>/fmi/xml/fmresultset.xml?-db=dbname&-lay=layoutname&-findany`
 - To view the script names in a database, enter this address in your browser:
`http://<ip:port>/fmi/xml/fmresultset.xml?-db=dbname&-scriptnames`
 - To view the layout names in a database, enter this address in your browser:
`http://<ip:port>/fmi/xml/fmresultset.xml?-db=dbname&-layoutnames`

For information on query commands and parameters, see the *FileMaker Server Advanced Custom Web Publishing Guide*.

Protecting your databases from web-based attacks

Start by reviewing the security procedures explained in this document. Your host computer is both your connection to the outside world and, if unprotected, the outside world’s connection to your internal network. Verify the following:

- For web-shared solutions, especially on the Internet, consider configurations with two (or more) computers separating the database from the web publishing components, firewalls, SSL and other standard Internet technologies. This protects access to your files and protects the communication between web users’ web browser and the server.

- 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.
- When you host a FileMaker Pro database using TCP/IP, you might be allowing uninvited visitors access to your host computer and internal network. A firewall is essential to separate your network and protect files “behind the firewall,” which prevents users on the outside of the firewall from accessing any TCP/IP addresses that you have not exposed.

Web server security

The web server application performs the critical task of processing and fulfilling requests for data when you publish databases, images, and other content on the web. When users enter 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 computer, where it can be displayed in their browser. To protect the integrity of this process, your web server has its own security mechanism.

If you host databases with FileMaker Server Advanced, use a third-party web server application such as Microsoft Internet Information Server (IIS) or Apache HTTP Server to publish files on the web. You can take advantage of additional security features, like SSL encryption, to transport data from the host to the web clients more securely.

Use encryption or VPNs to protect data

Consider using encryption and VPNs (Virtual Private Networks) to protect your databases on a TCP/IP network. Encryption is the process of manipulating data (clear text) such that the result (cipher text) can be understood only by certain applications.

You can protect data by:

- Setting up a secure VPN to encrypt some (or all) of your network traffic as it travels across a Wide Area Network (WAN).
- Host databases with FileMaker Server Advanced and configure SSL encryption in the web server application.
- Combining the above.

Using Secure Sockets Layer (SSL) security for web publishing

The SSL protocol is a standardized method for allowing encrypted and authenticated communication between web servers and clients (web browsers). SSL encryption is only available to databases hosted with FileMaker Server Advanced, and is enabled in the web server application, such as Microsoft Internet Information Server (IIS) or Apache HTTP Server by the Apache Group.

SSL encryption converts information exchanged between servers and clients 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 through *encryption keys*.

For information on enabling and configuring SSL, review the documentation that accompanies your web server.

About wireless networks

Another security vulnerability to be aware of are 802.11x wireless networking devices, also called “Wi-Fi” connections, which include:

- a station (or the device with the 802.11x wireless access) such as a laptop
- an access point (wireless hub or bridge) that is the point of access to the network
- the Local Area Network itself
- an authentication server, a separate device that challenges clients when they attempt network connections

Radio frequency access to a network leaves it open to packet interception by any radio within range of a transmitter. This enables intruders to connect through wireless protocols to corporate networks. These intrusions can be made far outside the customary “working” range by using hi-gain antennas. For example, if FileMaker Server Advanced is hosting files, an intruder could access data if the files lack sufficient user account security. An intruder who knows how a WAN controls access might be able to gain access to the network, steal a valid computer address, and use its assigned IP address. A typical approach is to wait until the valid computer stops using the network and then take over its position in the network and gain access to all devices in the network or to the wider Internet.

Important When assessing the physical security of your network, password-protect and encrypt your wireless networking signals. Always use the maximum level of signal encryption available.

XML considerations

XML and XSLT stylesheets are becoming the industry standard for the access, distribution, and presentation of data. With the Custom Web Publishing feature in FileMaker Server Advanced, XSLT stylesheets can be used to filter and transform XML data. This can be used to remove or modify meta-data in XML files sent to web users (for example, to hide field names) or to statically define query string parameters (such as database and layout name values) to prevent them from being exposed to or modified by web users. For more information, see the *FileMaker Server Advanced Custom Web Publishing Guide*.

Note Data formatted as XML is essentially text. This means that it can potentially be intercepted and read unless appropriate means are used to encrypt it. Whenever you are broadcasting data with TCP/IP and hosting databases with FileMaker Server Advanced, you should use SSL encryption in the web server application. This blocks “packet sniffer” applications, which monitor network traffic and might be capable of extracting FileMaker Pro data.

Important Never enable any extended privileges unless it is necessary.

Considerations for Apple events and ActiveX

FileMaker Pro can process commands from Apple events in the Mac OS or from ActiveX in Windows. This can yield unexpected results, for example, if an external script times out and does not process the next command.

Whenever introducing third-party technology, test all scripts and user scenarios thoroughly.