Securing Your FileMaker Server

Last Modified on 11/19/2026 12:48 pm EST

This guide explains security precautions to implement due to recent FileMaker Server attacks. It is intended for system administrators and IT specialists.

For AI-powered threats targeting FileMaker and other technology platforms, there are several security precautions aACE Software recommends implementing. Claris addressed recent AI attacks on FileMaker servers with recommendations for security precautions.

aACE Software has no reason to believe that aACE 6 is significantly vulnerable to these recent attacks. However, we have both optional and recommended precautions for the immediate and near term. If your server cannot be accessed from the internet or uses a VPN for access, most of the recommended precautions do not apply to you as the AI attacks scanned servers on port 443.

Table of Contents

- What We Know, aACE 6, and Our Next Steps
- Immediate Action Items
- Short Term Action Items

What We Know, aACE 6, and Our Next Steps

Claris explained some attack methods. Here are some essential details as they pertain to FileMaker Server:

- The attacks used port 443 to scan servers.
- The attacks seek to access files through the FileMaker Data API. Therefore, disabling the Data API and other incoming access services prevents this particular attack vector.
- The attacks target files that permit access through a guest account or other forms of automatic authentication.
- The attacks seek to extract data through layouts.
- If an attacker is successful, they might gain access to data contained in fields accessible through those layouts, subject to the file's security configuration.

For more information on how the attacks work from Claris, refer to Lock Down Your

FileMaker Server (https://content.claris.com/e/526331/claris-news-nov2026-article-2a/9xq85r/2657441317/h/4nmYwMphwXSLxwgOiVE8-S2DT-bmMe8wXXIzenwaUa4).

aACE Software is confident that aACE 6 solutions are not significantly vulnerable to these reported attack methods because we do not use a guest account or automatic authentication for aACE data files. However, aACE does have a number of other files that use a guest account for automatic authentication. These files either present aACE data in a particular way (e.g. Reports) or transmit aACE data from the data file to a third party (e.g. our integrations).

Some of these other files that use a guest account temporarily retain small amounts of data cached as part of recent transactions. If any of these files were compromised and cached data were exposed, an attacker's access would be constrained by the file's security configuration, including the fields accessible through its layouts. As a matter of practice, we include relatively few fields on the layouts in these files, and any cached data is retained only for a short period of time. An attacker would also need to identify these relevant files and layouts.

Top

Immediate Action Items

As a customer, there are some immediate actions you are able to complete to increase security for your FileMaker Server. aACE Software recommends disabling unused incoming access services, enabling database filtering, disabling guest account and automatic authentication login functionality, and determining if your server was targeted during the attacks.

For a comprehensive list of immediate action items from Claris, refer to Protecting FileMaker Server from Automated Attacks (https://support.claris.com/s/answerview?anum=000049228&language=en_US).

Disabling Unused Services and Enabling Logging

The most effective way to secure your FileMaker Server against the attack methods Claris mentioned is to disable unused services. Examples of raw services that receive incoming access to aACE include FileMaker WebDirect or the Web Publishing Engine, Data API, OData, and ODBC/JDBC. These incoming access services are used by various technologies for aACE, such as mobile apps, the new ADS, and aACE in a web browser. Integrations are not a technology that uses incoming access services because the access is outgoing from

aACE.

If you are not using specific mobile apps or custom technologies that require the incoming access services, we suggest disabling the unused incoming access services. It is important to note that there might be some risk to disrupting existing functionality.

To audit your incoming access services and disable ones you are not using:

1. Log in to the FileMaker Server Admin Console.
2. Go to **Connectors** > **Web Publishing** > disable **Primary Machine**, if the Web Publishing Engine and FileMaker Webdirect are not in use.
   Disabling the Web Publishing Engine also disables FileMaker WebDirect and XML.
3. Select **FileMaker Data API** > disable **FileMaker Data API**, if it is not in use.
4. Select **ODBC / JDBC** > disable **ODBC / JDBC**.
   This is old security technology and should already be disabled.
5. Select **OData** > disable **OData**, if it is not in use.

After you disable unused incoming access services, enable logging for the FileMaker Data API and/or FileMaker WebDirect if you are using these technologies:

1. In the FileMaker Server Admin Console, select **Logs** > **Log Settings**.
2. If FileMaker Data API is enabled, enable **Allow FileMaker Data API Script Log**.
3. If FileMaker WebDirect or the Web Publishing Engine is enabled, enable **Allow Web Publishing Script Log**.

Enabling Filter Databases and DenyGuestAndAutoLogin

For additional security, you should enable database filtering. If you manage your own FileMaker Server, you should also enable denying guest account and automatic authentication functionality if your files do not utilize these login methods.

Enabling Filter Database in Client Applications

The Filter Database in Client Applications option in the FileMaker Server Admin Console hides the list of databases on the server from anyone who asks for them without signing in to the server. To enable database filtering:

1. Log in to the FileMaker Server Admin Console.
2. Go to **Configuration** > **Clients**.
3. Enable **Filter databases in client applications**.

Enabling DenyGuestAndAutoLogin

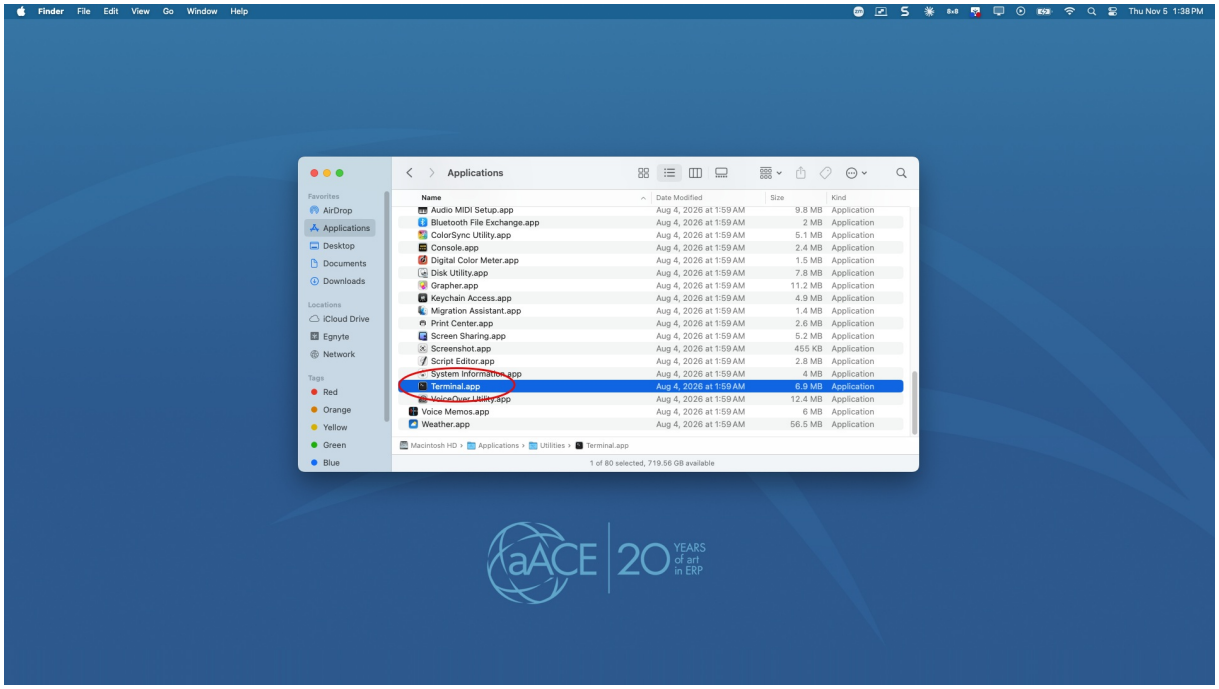
If you are managing your own FileMaker Server, enabling the DenyGuestAndAutoLogin preference for FileMaker servers prevents guest accounts and users using automatic authentication functionality from accessing the databases. This preference is server-wide and is not located in the FileMaker Server Admin Console and is only accessible by a Command Line Interface.

> If you enable DenyGuestAndAutoLogin but have a FileMaker database that uses a guest account or automatic authentication functionality, FileMaker Server will ignore these login methods. If a database relies on these login methods, it will break. If any of your databases must use automatic authentication or guest accounts, you must enable DenyGuestAndAutoLogin per file and configure your guest accounts with stricter privileges (https://help.claris.com/en/pro-help/content/protecting-databases.html).

If you do not manage your own FileMaker Server, you cannot enable DenyGuestAndAutoLogin.

To enable server-wide DenyGuestAndAutoLogin:

1. On the Mac that hosts your FileMaker Server, select **Finder** > **Applications** > **Utilities**.
2. Open **Terminal.app**.
   If you are on Windows, locate and open Command Prompt.



3. Enter the following command into Terminal, then select Return:

   Plain text

```
fmsadmin set serverprefs DenyGuestAndAutoLogin=true
```

4. If prompted, enter your Admin Console username and password.

Reviewing Logs

You can review logs to determine if your server might have been targeted by an attack. For more information on identifying if your server was affected, refer to the Claris guide Protecting FileMaker Server from Automated Attacks (https://support.claris.com/s/answerview?anum=000049228&language=en_US).

If you require assistance, contact our aACE team at support@aacesoft.com ().

Top

Short Term Action Items

The recent attacks do not appear to exploit vulnerabilities in PHP or FileMaker Server itself. However, the following actions should be taken in the short term to address other ongoing attacks (e.g. PHP2Shell) and legacy vulnerabilities that have been resolved in more recent versions of FileMaker Server.

Disabling or Removing PHP

aACE does not require PHP for your FileMaker Server. If you are not aware of any custom solutions or services that require PHP, your IT professional should disable or remove it. Otherwise, make immediate arrangements to apply necessary security patches.

Upgrading FileMaker Server

Older versions of FileMaker Server should be upgraded to FileMaker Server 26. If you are uncertain about the appropriate next steps, contact support@aacesoft.com ().