Enabling Remote Access to Your aACE System

Last Modified on 08/25/2020 10:19 am EDT

Note: We recommend having your **IT specialist** work through this section to ensure that these critically important steps are completed properly.

Configuring a Fully-Qualified Domain Name

We require that you have a fully-qualified domain name (e.g. "aace.mydomain.com") that is configured to forward traffic to your server's external IP address.

To obtain a fully-qualified domain name, you must first register your unique domain name (e.g. "mydomain.com") with a DNS registrar such as GoDaddy, Comodo, or NameCheap. Once you own the registered domain, you must then configure a subdomain (we recommend using "aace") by creating a new "A" type DNS record for your domain. This "A" type DNS record will need to associate your chosen subdomain with your server's external IP address, such that all traffic routed through your fully-qualified domain name will reach your server.

Configuring Your Network / Firewall

Incoming traffic through the following ports should be allowed / forwarded to your server:

- TCP 5003
  Note: Opening only TCP 5003 to your server is enough to allow your users to access your hosted aACE system.
- TCP 80
- TCP 443
  Note: TCP 80 (HTTP) and TCP 443 (HTTPS) are used by FileMaker Server to improve performance significantly over the network, especially when uploading and downloading documents. Opening these two ports is optional, but we strongly recommend that you do so to avoid any reduced performance for your users.

Cloud Servers

If your aACE server is a virtual machine running on a service such as Amazon Web Services, Google Cloud Platform, etc., then this step will require that you access the appropriate service's web portal. Ensure that all incoming traffic through the aforementioned ports is **allowed** to reach your virtual machine.

In-House Servers

If your aACE server is a physical machine that is located onsite, this step requires you to access your router's console. Ensure that all incoming traffic through the aforementioned ports is forwarded to your server's **internal IP address**.

Closing ports for security reasons is often recommended. However, even when your aACE system is hosted on your in-house server, it uses a copy of FileMaker Server (FMS), which uses these three ports to transfer data between the server and the user's computer. If you closed all three of the ports noted above, no data could be sent or received by the server. No users could to sign into aACE (or even see it listed as a hosted file).

FMS primarily uses port 5003 for logging in, navigating interfaces, updating data, etc. Closing this port would prevent all remote users from accessing the aACE system altogether.

FMS uses ports 80 and 443 to quickly and efficiently transfer documents and other larger chunks of information. Leaving them open typically improves the system's performance. Closing these two ports means that FMS would have to send those larger chunks of info using port 5003. The data would be transferred significantly slower and other users might also experience reduced performance.

Testing Your Network Configuration

After completing the tasks above, run the following tests on a machine *other than* your aACE server to confirm that the configuration was completed properly:

1. Open a browser and enter your server's **fully-qualified domain name** into the URL bar / search bar. If the test is successful, you will see a "T" logo and the words "FileMaker Database Server Website".
    - If your test was successful, then no more testing is required.
    - If your test was not successful (i.e. your browser was *not* able to find the expected page), proceed to Test #2.
2. Open a browser and enter your server's **external IP address** into the URL bar / search bar. If the test is successful, you will see a "T" logo and the words "FileMaker Database Server Website".
    - If your test was successful, then you will need to check on the configuration of your fully-qualified domain name. Ensure that the "A" type DNS record for your chosen subdomain is forwarding traffic to your server's external IP address.
    - If your test was not successful (i.e. your browser was *not* able to find the expected page), then you will need to check on your server's network / firewall configuration.

Ensure that all incoming traffic through ports TCP 80, TCP 443, and TCP 5003 is allowed / is forwarding to your server.