Why are files in EFT Server's client folder available to a connecting client without authentication?

THE INFORMATION IN THIS ARTICLE APPLIES TO:

- EFT Server, versions 5.x - 7.4.x

QUESTION

Why are files in EFT Server's client folder available to a connecting client without authentication?

ANSWER

The client folder on EFT Server (e.g., **C:\Program Files\GlobalSCAPE\EFT Server Enterprise\Client** or **C:\Program Files\GlobalSCAPE\EFT Server Enterprise\web\public\EFTClient**) provides the framework for clients connecting over a browser to interact with EFT in a user-friendly and brandable fashion. It serves up non-sensitive files to enable access to EFT over standard Web browsers: HTML, JavaScripts, cascading style sheets, images and, for those connecting to WTC, the JAR and associated files. These files, being non-sensitive and necessary for connecting clients to easily use the system, are NOT password protected. This facilitates the deployment of the "connection framework" that is sent to the browser. ***Access to any files stored in the EFT in its VFS are password protected and access controlled.***

When auditing to the ARM database, requests to these anonymous, connectivity framework resources are marked as "internal" to help differentiate from actual transfer of user data. In the "tbl_ProtocolCommands" table, the "IsInternal" field is set to "1" for all downloads of this connectivity framework.

You should not put sensitive information into the client folders in the EFT installation directory, due to the anonymous access allowed to this folder; however, if there is information that you want to provide to end-users that does not require authentication, such as a help file, license agreement, or information page, then the client folder is a convenient place to store such files.

Security is based upon risk, vulnerability, threat, and value of asset. The assets that we put into the EFT Server client folders are public things—the "framework" for transferring files between a client and EFT Server. Those that make use of the system to perform transfers may use these files or their own client; however, the things that we deploy are not

sensitive, proprietary, nor intrinsically valuable. Once obtained, it provides a *mechanism* for connecting to upload/download files, but this mechanism is fully authenticated and access controlled.

Security is a tradeoff with usability. If we access controlled all of these "/EFTClient" files and folders, then the user experience would require more authentication for the various files (i.e., the Java Applet would cause the JVM Class Loader to prompt for username/password to get to the JAR files). We have consciously chosen, after risk and threat analysis, to allow these "web transfer framework" files to NOT require authentication to balance the user experience with security. We feel confident that the trade-off is appropriate.

GlobalSCAPE Knowledge Base
https://kb.globalscape.com/Knowledgebase/10524/Why-are-files-in-EFT-Servers...