How can I secure sensitive information (connection strings and AppSettings) in EFT Server's Secure Ad Hoc Transfer (SAT) module?

THE INFORMATION IN THIS ARTICLE APPLIES TO:

- EFT Server (All Versions)

QUESTION

How can I secure sensitive information (connection strings and AppSettings) in EFT Server's Secure Ad Hoc Transfer (SAT) module?

ANSWER

It is highly recommended that you use the delegated administration feature of EFT Server to create a new administrative account that can be used by the Secure Ad Hoc Transfer (SAT) module. This isolates the username/password for the Web application, independent of EFT Administrator. Also, if the EFT Server has multiple Sites, you should grant access to this Secure Ad Hoc Transfer application only to the Site that is used by this application. After the installer has completed successfully, set up a new administrator account in EFT Server, then create a base64-encoded password.

Using Encode64 is not enough for some production environments. Microsoft .NET provides system administrators the ability to secure sensitive information using the Windows Data Protection application programming interface (DPAPI) protected configuration provider and the Aspnet_regiis.exe tool. .NET Framework 2.0 introduced a protected configuration feature that allows you to encrypt sensitive configuration file data by using a command line tool. You can use the Aspnet_regiis.exe tool to encrypt sensitive data, such as connection strings stored in SAT's Web.config file.

For more information, refer to the Microsoft Developer Network article "How To: Encrypt Configuration Sections in ASP.NET 2.0 using DPAPI."

GlobalSCAPE Knowledge Base
https://kb.globalscape.com/Knowledgebase/10480/How-can-I-secure-sensitive-i...