Enable WTC authentication by Site's authentication manager, and a session-specific one-time passcode

THE INFORMATION IN THIS ARTICLE APPLIES TO:

- EFT v7.2.1 and later

EFT v8.0 and later store Advanced Properties in a JSON file. When you upgrade from EFT v7.4.x to EFT v8, the non-default settings that you have defined in the registry will be added to the Advanced Properties file during upgrade. (Default settings become part of the EFT configuration files.) For a more on how to use advanced properties, and a spreadsheet of the advanced properties, please refer to the "Advanced Properties" topic in the help for your version of EFT.

DISCUSSION

The advanced properties below will enable WTC authentication by the Site's authentication manager (e.g., AD/LDAP) and then with a session-specific, one-time passcode (e.g., a code sent via text or email message).

1. After creating the advanced properties below, restart the EFT server service, then log in to EFT with your AD/LDAP password.
   - In versions prior to v7.4.13, you would be asked to provide your LDAP/AD password twice.
   - In v7.4.13 and later, setting UseAuthManagerPasswordForMultistep to any non-zero value will skip the second AD/LDAP authentication.
2. After authenticating with AD/LDAP, EFT sends a request to the SMS authentication server to get your token; enter that token in the login screen.

- UseAuthManagerWithMultiStep
- UseAuthManagerPasswordForMultistep (added in v7.4.13
- AuthManagerWithMultiStepChallenge

In EFT v8 and later:

Add the name:value pairs to the AdvancedProperties.JSON file in EFT's \ProgramData\ directory as described in the "Advanced Properties" topic in the online help for your version of EFT.

"UseAuthManagerPasswordForMultiStep ": true

}

In versions prior to v8.0:

Create the following registry entry:

HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\GlobalSCAPE Inc.\EFT Server 4.0**Config**\

Value name: UseAuthManagerWithMultiStep

Type: DWORD

Default Value: false

Cached: yes

Backup/Restore: yes

Description: When non-zero, causes authentication to FIRST use the Site's authentication manager and, if succeeded, proceed to RSA/RADIUS authentication to finish authentication.

Value name:

UseAuthManagerPasswordForMultistep (added in v7.4.13)

Type: DWORD

Default Value: 0/false

Cached: yes

Backup/Restore: yes

Enable WTC authentication by Site's authentication manager, and a session-specific one-time passcode

Description: When non-zero, EFT, after successful authenticating user with their password against site's auth manager, uses the password to authenticate the user against RSA/RADIUS.

Value name: AuthManagerWithMultiStepChallenge

Type: STRING

Default Value: Enter the RSA SecurID token to complete authentication:

Max Length: 255

Cached: yes

Backup/Restore: yes

Description: Specifies the challenge text to display after succeeding with authentication manager authentication, prompting user for RSA/RADIUS input.

GlobalSCAPE Knowledge Base
https://kb.globalscape.com/Knowledgebase/11267/Enable-WTC-authentication-by...