

Allow Server to Accept ODBC Database Passwords that are MD5 Hashed

THE INFORMATION IN THIS ARTICLE APPLIES TO:

- EFT Server v5.1 and later (on Sites using ODBC for user authentication)

DISCUSSION

Passwords managed by EFT Server for ODBC-based user authentication are stored using a SHA256* one-way hash. The registry entry described below will cause EFT Server to use MD5 hash instead.

When the MD5 override is enabled, EFT Server will compare the MD5 value of the supplied password against the stored hash and if that fails it will compare the SHA-256 value of the supplied password against the stored hash. After a successful authentication (and upon password changes) the MD5 hash will be stored (overwriting the SHA-256 value if present). The same logic will occur in reverse if the MD5 override is turned off in favor of SHA-256.

Create the DWORD UseMD5PasswordHash in the following location:

32-bit:

```
HKEY_LOCAL_MACHINE\SOFTWARE\GlobalSCAPE Inc.\EFT Server 3.0
```

- or -

64-bit:

```
HKEY_LOCAL_MACHINE\Software\Wow6432Node\GlobalSCAPE Inc.\EFT Server 3.0
```

If this value is absent or is zero, the SHA-256 digest algorithm is used; otherwise, MD5 is used. Therefore, if you want to use MD5, set UseMD5PasswordHash = 1. The digest is stored in the database in Base64-encoded form.

Considerations if using an external source to populate the ODBC database:

Allow Server to Accept ODBC Database Passwords that are MD5 Hashed

If the password hash is generated externally (whether SHA256 or MD5), the resulting hash must be base-64 encoded and must not be in a [*nix style](#) MD5 or DES format (only EFT Server's native authentication supports that format).

If you are using an external source for populating the ODBC data source and users cannot log in, check that the ANONYMOUS row in the FTPSERVER_USERS is NULL for all Users (only Groups are allowed NULL). Use the value "0" for standard authentication or "1" if allowing anonymous (rare). Likewise the PASSWORD_TYPE must be set to "0" when authenticating based on a user's password hash.

GlobalSCAPE Knowledge Base

<https://kb.globalscape.com/Knowledgebase/10537/Allow-Server-to-Accept-ODBC-...>