Kofax TotalAgility - What type of password hashing and encryption is used in KTA, and what are the differences in these terms?

3018113

Question / Problem:
What algorithm is used for password hashing and encryption is used in KTA

Answer / Solution:

Password Encryption

In order to protect this data in transit we encrypt these variables if the user wishes to do so. This encryption/decryption is done on the server to avoid any storage of the cryptographic key on the client. This is done using APIs Encrypt() and Decrypt() methods in CryptoHelper using 3DES algorithm in v7.5 and below. In v7.6 this was changed to AES.

Password Hashing

Both versions of KTA use Scrypt for resource password hashing (as defined in System Settings).

We strongly recommend the preconfigured Scrypt encryption algorithm.

SHA-1 is also available; however, recent advances in cryptanalysis have detected weaknesses in the SHA-1 algorithm. Scrypt is much stronger.

Applies to:

<table>
<thead>
<tr>
<th>Product</th>
<th>Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Kofax TotalAgility</td>
<td>7.5</td>
</tr>
<tr>
<td></td>
<td>7.6</td>
</tr>
</tbody>
</table>