Which encryption algorithms are supported in UniData and UniVerse

U2 TECHNICAL SUPPORT NOTICE 1/2008

Applications built on the U2 dataservers, UniVerse and UniData, are able to encrypt data either through Automatic Data Encryption (ADE) or by use of the BASIC ENCRYPT function. Either approach requires selecting an encryption algorithm. At UniData 7.1.20, 7.2.0 (and higher) and UniVerse 10.2.12 (and higher) the algorithms available will conform to Rocket Software standards. When you upgrade to either of these releases, you will to need take account of this standardization of encryption algorithms.

IF YOUR APPLICATION EMPLOYS ENCRYPTION ALGORITHMS YOU MUST ENSURE BEFORE YOU UPGRADE THAT THE ENCRYPTION ALGORITHM YOU USE IS ONE OF THOSE LISTED AS SUPPORTED.

If your application currently uses an encryption algorithm that is not supported at UniData 7.1.20, 7.2.0 (and higher) and UniVerse 10.2.12 or higher numbered releases, and you proceed with the upgrade, your encryption functionality will cease working and your previously encrypted data will become inaccessible.

Encryption Algorithms Supported at UniData 7.1.20, 7.2.0 and UniVerse 10.2.12 and higher

aes-128-cbc		cast	des	rc2
aes-128-ecb	bf	cast-cbc	des-cbc	rc2-40-cbc
aes-192-cbc	bf-cbc	cast5-cbc	des-cfb	rc2-64-cbc
aes-192-ecb	bf-cfb	cast5-cfb	des-ecb	rc2-cbc
aes-256-cbc	bf-ecb	cast5-ecb	des-ede	rc2-cfb
aes-256-ecb	bf-ofb	cast5-ofb	des-ede-cbc	rc2-ecb
			des-ede-cfb	rc2-ofb
			des-ede-ofb	rc4
			des-ede3	rc4-40
			des-ede3-cbc	
			des-ede3-cfb	
			des-ede3-ofb	
			des-ofb	
			des3	
			desx	

Preparation For Upgrade

If you currently use an encryption algorithm that appears in the above list your encryption functionality will be unaffected.

If you currently use an algorithm that does not appear in the list above you will need to take action.

If You Use the BASIC ENCRYPT Function for Storing Data

1. Select your new encryption algorithm
2. Back up the encrypted data files/records/fields
3. Decrypt the data files/records/fields
4. Modify all BASIC programs to use the new standard algorithm
5. Encrypt the data files/records/fields with the new standard algorithm

You are now ready to upgrade.

NOTE: If you use BASIC ENCRYPT only for data in motion (i.e., you do not store encrypted data) only step 4 applies. The new standard algorithm must also match with the encryption algorithm used by the third party application communicating with the U2 application.

If You Use Automatic Data Encryption

1. Consult the U2 product documentation for the command line procedures to decrypt encrypted files/records/fields
2. Encrypt the files/records/fields with the new standard algorithm

   or

   Use the UniAdmin tool to decrypt the data
3. Use the UniAdmin tool to encrypt the data with the new standard algorithm

You are now ready to upgrade.

NOTE: If you have used the SSL Config Editor to create an SSL Property List that specifies a non standard algorithm you will need to use this tool to modify the SSL Property List to use the new standard algorithm.

ADDITIONAL RESOURCES

For further information on how to decrypt and encrypt data please see the relevant U2 documentation manuals.

There is additional information in the U2 Knowledge base accessible at

https://u2tc.rocketsoftware.com

Search for article number 1314320 or the title “How to change your encryption algorithm in UniVerse ADE”.