INFO: AES Encryption

Summary

AES128 encryption is supported in the Unitrac XML API as of Unitrac v2.14. The remainder of this document describes the implementation of the encryption.

More Detail

Encryption is optional and its use is determined by the client side of the connection by responding to the login challenge with an encrypted response. After the response to the challenge the connection is either always encrypted or it’s always in the clear. The reception of a clear text message on an encrypted connection or the reception of an encrypted message on a clear text connection causes the connection to be dropped.

The encryption key for the connection is derived from the user’s Unitrac password. The password is equivalent to a pre-shared secret known to both Unitrac and the user. An MD5 hash is created to which the user’s name, password and a fixed string are added. The resulting 16-byte (128-bit) hash is used as the key.

Encryption of a Unitrac API XML message occurs as follows.

1. A random 16-byte initialization vector (IV) is generated.
2. The Unitrac XML API UTF-16 message string is converted to UTF-8.
3. The UTF-8 string is padded to the next higher integer multiple of the block size (16 bytes for AES). Padding is accomplished using the PKCS2 padding algorithm.
4. The padded UTF-8 string is encrypted using the key and IV.
5. The encrypted string is converted to Base64.
6. The Base64 string is converted to UTF-16 and wrapped in a Unitrac XML API envelope. The envelope contains the algorithm and IV.

An example of an encrypted message is shown below.

```
<unitrac>
  <encrypted params="ALG=AES128;IV=ED0DD4B94C38FD43A00B5AD12773BE45"
      guid="32E83EB7B57226408DB2F55E7B3EFFCA" date="2008-02-21 20:49:18.682">
    <innermsg>
      mwEimsOdl8XYcZ+7A30BWYXWc4Msv4U3MjHjhEsMZxZ3HEh90neL9gBMPJtDdMkAjQ0PzsPyruS1
      LCN0+rPrrD7ZxumgvrYrHgigd7gVoRsZ3bfjEsTBVO0olRGH5cr6qTBHeSr2LhXpomSOpiD2aA==
    </innermsg>
  </encrypted>
</unitrac>
```

Decryption follows the inverse of the encryption process.