

Api Gift Decryption Document

Decryption Details for `EncryptedVirtualCollections`

The `EncryptedVirtualCollections` field in the response is encrypted data that can be decrypted using the following specifications:

Decryption Specifications:

- **Algorithm:** AES (Advanced Encryption Standard)
- **Mode:** CBC (Cipher Block Chaining)
- **Initialization Vector (IV):** `oFRna73mXaze01xY` (16 characters, ASCII-encoded)
- **Key (Password):** Retrieve your unique *Decryption Password* from your account settings.
- **Input Format:** Base64-encoded string (encrypted data)
- **Output Format:** UTF-8 plaintext

Decryption Steps:

1. **Decode the Encrypted Data:** Convert the Base64-encoded string into raw encrypted bytes.
2. **Configure AES Decryption:**
 - Use the AES algorithm in CBC mode.
 - Provide the *Decryption Password* as the key.
 - Use the IV (`oFRna73mXaze01xY`) for decryption.
3. **Decrypt the Data:** Pass the raw encrypted bytes through the AES decryption process.
4. **Convert to Plaintext:** Decode the resulting bytes to retrieve the original string in UTF-8 format.

Important Notes:

- The *Decryption Password* is unique to each user and must be securely retrieved from your api keys (actually, this is your secret-key).
- The IV is a static value: `oFRna73mXaze01xY`.
- Ensure proper handling of sensitive data during decryption to avoid exposing credentials or decrypted data.