 ­­­

01.28.2016 • Version: 1.0 • Prepared by: Lightwellinc

31 Gifts – Decrypting Reports

*Prepared for:*

31 Gifts Project Team



Table of Contents

[Overview: 3](#_Toc441753628)

[Decrypting on Linux Environment 3](#_Toc441753629)

[Decrypting on Windows Environment 3](#_Toc441753630)

# Overview:

This document is to provide the Thirty-One Gift users steps to decrypt the reports that are sent from IBM CoC.

The report will be in .csv format and encrypted in 256 bit AES in CBC mode.

# Decrypting on Linux Environment

This method is designed to be carried out on a Linux environment and uses a shell script that is provided from the Lightwell OMS team.

The shell script is named “decryptReportFile.sh” and will be provided with this document.

Steps to decrypt the file are simple:

1. Call the script and pass the encrypted report in as an argument:

Eg.

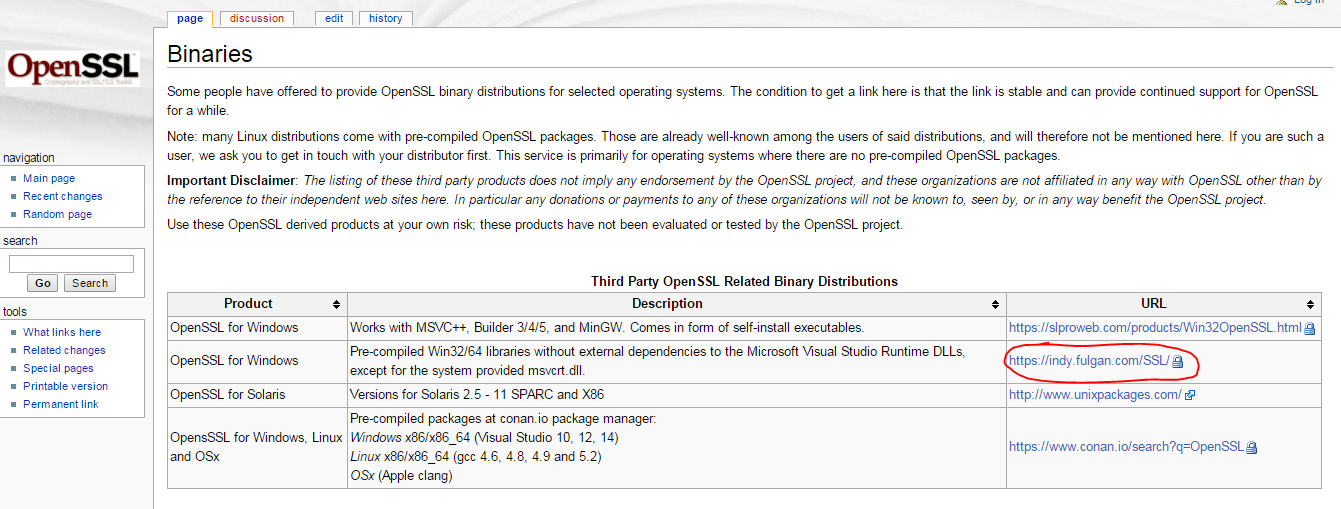
$ ./decryptReportFile.sh BackOrdersDetail\_20160128064601.csv

1. This script will decrypt the file and create a backup copy of the encrypted file in the same directory (Can be deleted)

# Decrypting on Windows Environment

This method is designed to be carried out on a Windows environment and uses a download from the Openssl wiki, there will also be the zip file provided in Box (If you get this then skip to step 3).

1. Go to: <https://wiki.openssl.org/index.php/Binaries>
2. Click on the following:



Download the Zip that relates to your OS.

1. Inside the zip folder open up a command window
2. Run the following command to decrypt the input.csv

openssl.exe aes-256-cbc -k TogAESEncryption256 -d -in input.csv -out output.csv

1. This will decrypt the file and output it to output.csv