USER MANUAL

FOR

VCRYPT SYSTEMS

Contents

Figure Index

1.General Information

1.1 Purpose

The purpose of this document is to provide systematic information to use VCrypt System Windows application by various users.

1.2 System Overview

VCrypt is innovative and unique security software, which uses the cryptographic technique creating a virtual vault to secure data and application across multiple platforms using various parametric options. VCrypt runs an algorithm, which encrypts data in a fashion so that decryption is done virtually via sight-reading (at runtime).

VCrypt allows enterprises to implement multiple security policies on different vendor applications data. The software allows users to create chains of options to restrict the data/application as desired. The software finds its application in the following area: **For own self:** Securing data/application by users for their own self. **For Reselling:** Users who want to sell the data with copyright restrictions.

Highlights of this application are

- **Install and Run:** Easy to use and run software with just a click.
- **Non-Dependent on Application Source Code:** Works directly within runtime process area, so there is no requirement of host application source code.
- **Auth Keys:** Provides both hard and soft keys (12 different types of soft keys are supported).
- **Creates own "Crypto Key":** Ability to create in-house encryption mechanism & security policies making it hack proof.
- **Common/Customized encryption algorithm:** Ability to write common/customized encryption algorithm for different vendor applications.

Decryption only during Runtime: File gets decrypted only during runtime. At other times, it's always in encrypted mode Security with 256bits AES encryption.

1.3 Organization of the manual

The User Manual consists of following sections-

General Information, System Summary, Getting Started, Using the System, Index & Appendix.

General Information section explains in general terms the system and the purpose for which it is intended.

System Summary section provides a general overview of the system. The summary outlines the uses of the system's requirements, system's configuration and user access levels.

Getting Started section explains how to use VCrypt Windows application. The section presents briefly system menu.

Using The System section provides a detailed description of system functions.

2.System Summary

2.1 System Configuration

It is a desktop application which can be run on individual PCs, laptop. The application doesn't require internet connection in order to encrypt/decrypt data but in case of Two-way authentications enabled or while sharing encrypted data via third party application (online channel), net connectivity might be required. Data saved can be seen on any major internet browser. After installation of application, it can be used immediately without any further configuration.

3.Getting Started

3.1 How to download VCrypt application

3.1.1 Accessing VCrypt Website

User can download the application from VCrypt website. For this, open any internet browser (i.e. Chrome/Firefox/Internet Explorer etc) & type in the following url:

https://vcryptsystems.com on the browser bar (fig.1):

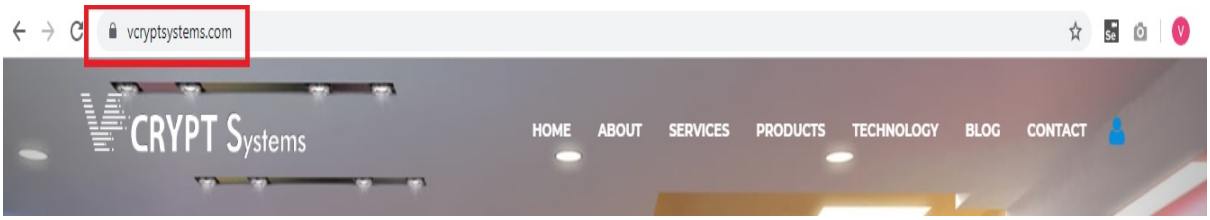

Figure 1 VCrypt Website URL

After typing in the url of VCrypt website & pressing **[ENTER]**(shown in Fig:1), homepage of website will be displayed as:

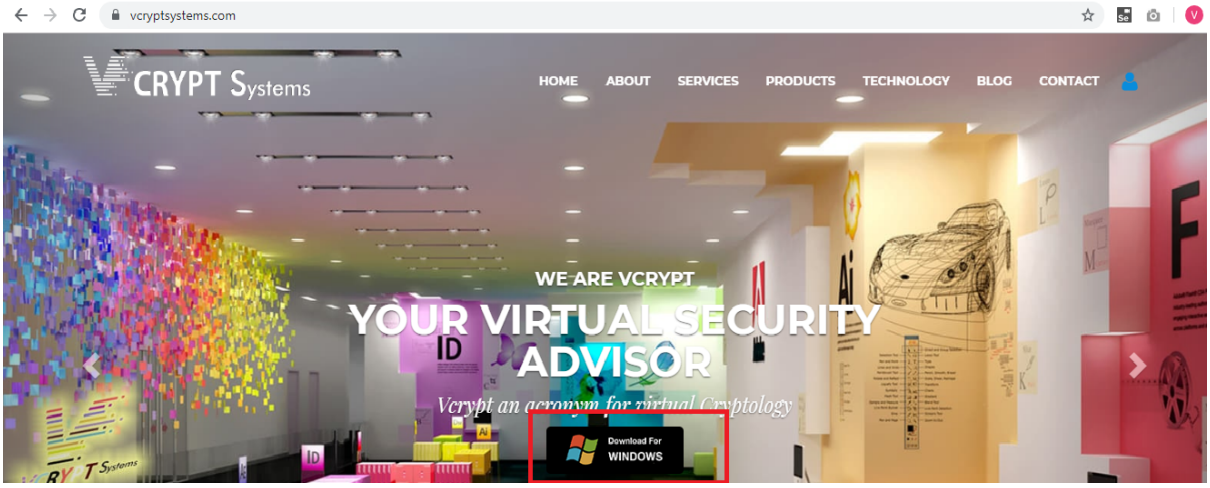

Figure 2 Homepage

3.1.2 Download demo application for VCrypt Software

On the home page of website, User click download button to start downloading VCrypt Software.

3.2 Installation

a. The Setup for VCrypt software will include :
   - ✓ X-Encryptor application
b. On desktop icons will be displayed for X-Encryptor application
c. User simply needs to click the icon in order to start running it.

On clicking X-Encryptor app icon, landing page/homepage of application will be displayed as shown in Fig 3:

Figure 3 X-Encryptor App

4 Using the System

4.1 X-Encryptor Application

4.1.1 Homepage

As soon as you open X-Encryptor application, homepage will be displayed as shown in Fig 4:

Figure 4 Homepage of X-Encryptor App

On the homepage, menus displayed in left panel tabs are as follows:

LEFT NAVIGATION PANEL:

a. **Data Encryption**

Clicking on this link will take the user to a screen where he can encrypt the files, enable two-way authentications, configure keys & save encrypted files on the system.

b. **Data Decryption**

Clicking on this link will take user to the landing page of the Data Decryption section. Here, user can decrypt the encrypted files as received via various channels.

c. **Auth Key Configuration**

Clicking on this link will take user to the landing page of Auth Key Configuration section. Here, user can configure auth keys i.e. Hardware or Soft keys required to enable Two-way authentication.

d. **Settings:**

e. **Tools:**

4.2 Data Encryption

In this section, user needs to select required Batch ID(s), Package ID(s), file extensions, source & destination folders to encrypt the data. Next step is to enable two way authentication, if required & finally configure software & hardware keys.

Data encryption translates data into another form, or code, so that only people with access to a secret key (formally called a decryption key) or password can read it. Encrypted data is commonly referred to as ciphertext, while unencrypted data are called plaintext.

There are 3 tabs under Data Encryption module:

- File Settings
- Two way authentication
- User Defined Configuration

4.2.1 File Settings

In this section, user needs to add specifications for the file, which is to be encrypted. Below is the screen for **File Settings** section:

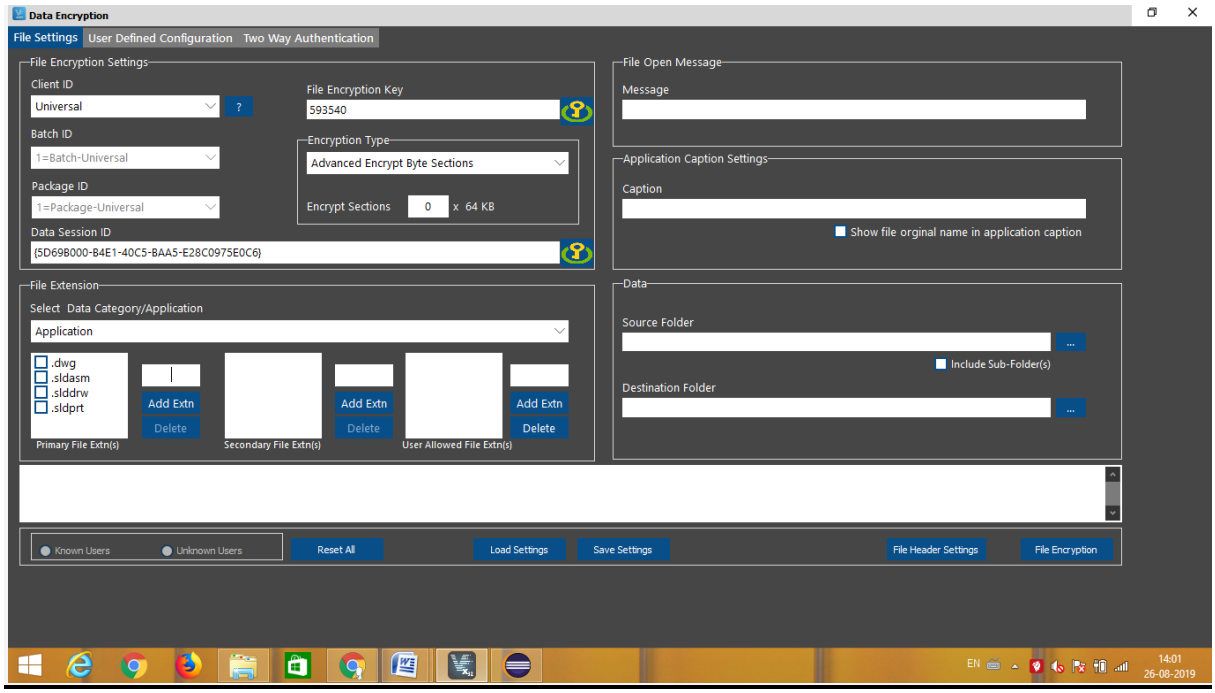

Figure 5 File Settings

Components of File Settings screen have divided into parts as shown in upcoming sections:

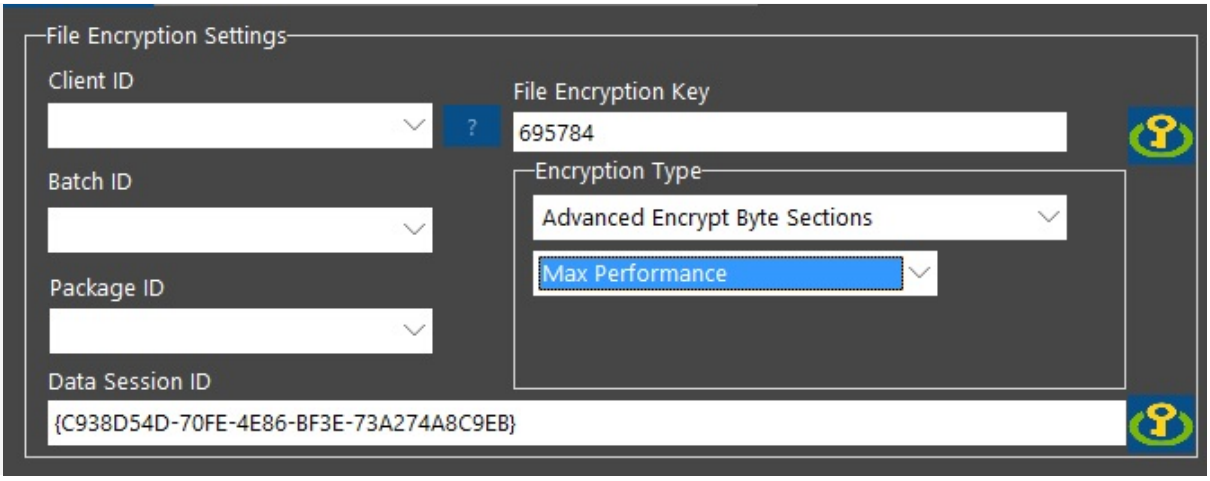

Figure 6 General File Settings

Please refer to below mentioned points for description of fields in fig. 6

Client Id

Client ID is assigned to each unique user of our website. Unique number generated at the time of purchasing VCrypt System setup. User can't set/reset this value. This is in Read only mode.

Batch Id

At the time of purchasing VCrypt software, client creates batches to identify each package & a unique ID is generated corresponding to each batch which is called as **Batch ID**. Within a batch, there can be multiple packages as defined & purchased by the client. Client can create multiple batches with the same account. Batches are created in the client config panel of VCrypt website.

Package Id

Once the batches are created by the client in configuration panel, he can define the packages within each batch. A package contains number of files required to choose a specific file type at the time of encryption. When a package is created, a unique ID is generated corresponding to each package which is called as **Package ID**.

File Enc Key

Auto generated number used as key to encrypt the file. This is helpful when we have two files with same mechanisms and we need to differentiate between the two files while encryption we use this encryption key.

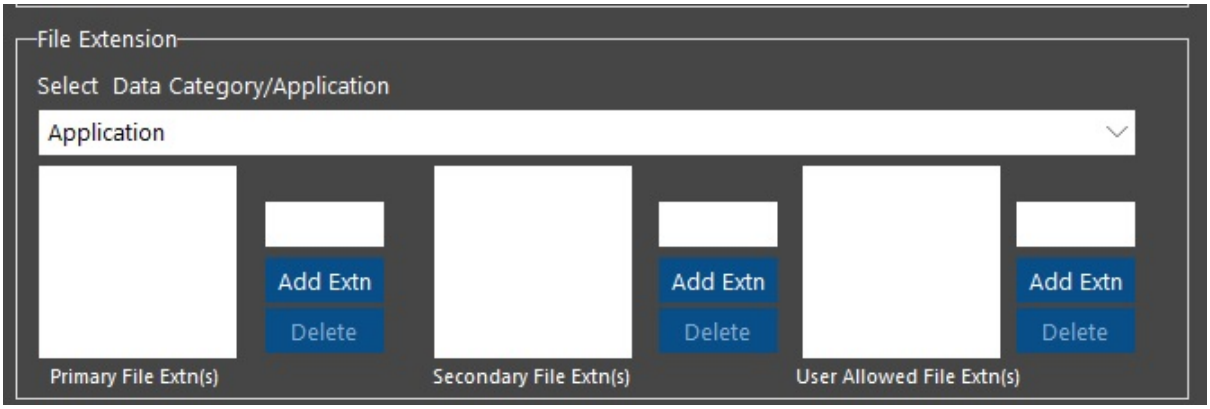

Figure 7 File Extension Settings

Please refer to below mentioned points for description of fields in fig. 7

Select file Extension:-

Data type application

List will contain number of applications supported by licensed version of Vcrypt software like MS-Word, AutoCAD etc. Client needs to select the type of application(s) for which data is to be encrypted. Encrypted files will only run in application(s) as selected & won't support other application(s).

Primary File Extensions

A **file extension** (or simply "**extension**") is the suffix at the end of a **filename** that indicates what **type** of **file** it is.

Depending upon the type of applications selected by the client, Primary file extensions corresponding to those applications will be displayed for selection. Encrypted files will support only those extensions.

Secondary File Extensions

In case the client wants to add any other secondary file extension other than selected secondary extensions, he can do so by selecting this option.

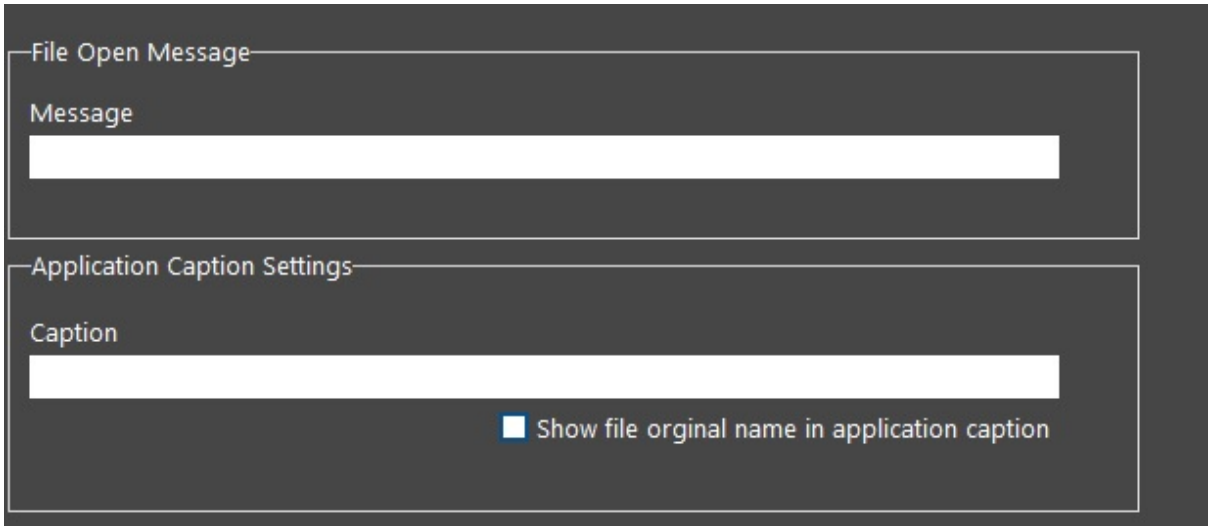

Figure 8 Fig File Message/caption Settings

File Open Message

Message displayed (in dialog box) to recipient of encrypted file when he opens that file in target application. Client can configure the message by entering required details.

Captain

Client can configure the Caption for file which will be displayed in header section when the decrypted file will open in target application. It is the file name which is displayed in the caption field.

Show File Orginal Name in Application Caption

By checking this option, Client can set the **Original File Name**(Default) as **Caption** in case he doesn't want to add any caption for the file.

Figure 9 Fig File Message/caption Settings

Source Folder

This folder contains the original files, which the client wants to encrypt. He needs to browse through Source folder to select the files for encryption.
He can also add sub folder(s) to it, if there exists any.

Destination Folder

This folder contains the encrypted files. Client needs to select the destination folder to save encrypted files. After entering required details & clicking **File Encryption** button, the Encrypted files will be saved in destination folder as selected.

4.2.2 User Defined Configuration

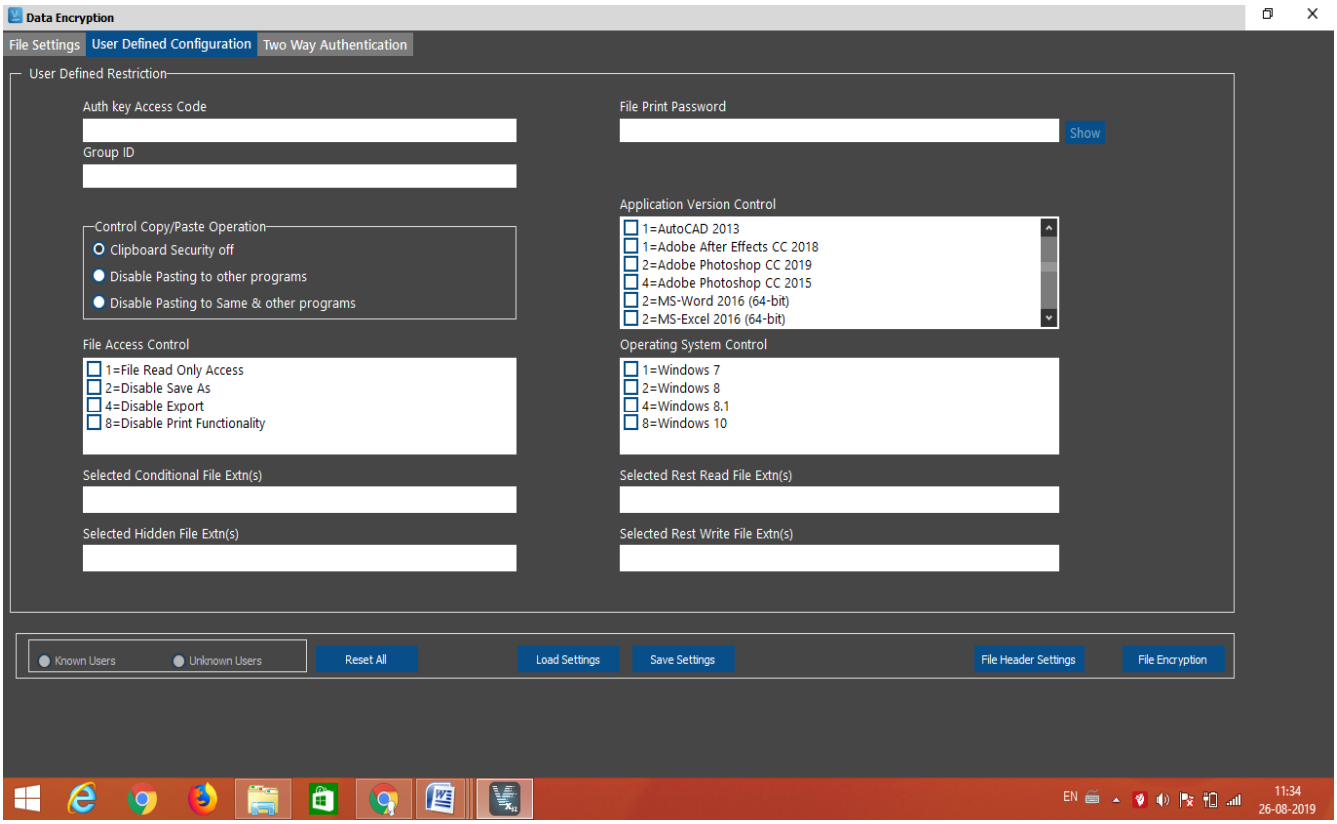

Figure 10 User Defined Configuration

User Defined Restriction

The file, which is encrypted, and we need to apply some validations to our file or need some restrictions to it we use this form. This is used to provide restrictions to our encrypted file.

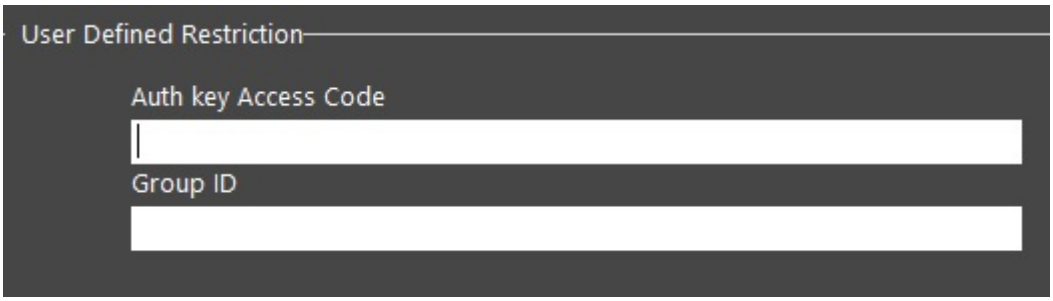

Figure 11 User Defined Restriction

Auth. key Access Code

Auth Key Access Code is used to differentiate between two files when Batch ID and Package ID are same as auth key access code is always unique.

Group Id

Group ID distinguishes between file currently in use & other file in case they share similar names. It is unique for every new file.

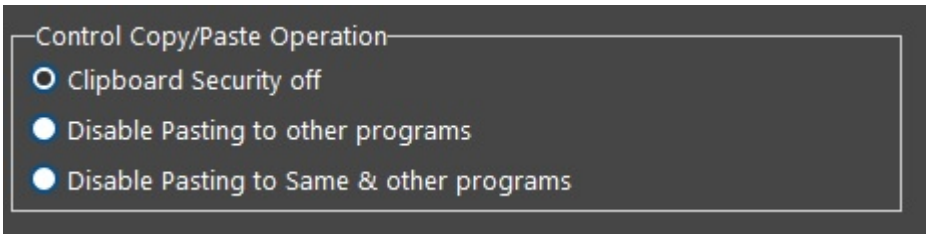

Figure 12 Control Copy/Paste Operation

Control Copy/Paste Operation

As a part of DRM (Digital Rights Management), client can control the operations to be performed on the encrypted file which will be shared with the recipient. The client can choose from below mentioned options:

Clipboard Security Off

When selected, it means that the client hasn't provided any restriction on copy/paste operation. When the copy operation is performed, the content can be saved to the clipboard and then pasted at the desired location.

Disable Pasting to other programs

When selected, it means that the client has allowed copy operation but has restricted the content to be pasted to any other file. But, pasting can be done only to the same file.

Disable pasting to same programs

When selected, it means that the client has disabled pasting operation in the same program as well.

Figure 13 File Access Control

File Access Control

This feature allows the client to control the operations in relation to accessing the file. There are number of options which the client can choose from:

i. File Read Only Access

This allows the user to only read the contents of the file without editing it.

ii. Disable Save As

This option disables the **Save As** property of the file which means that after editing the file, user cannot save the file on his system or anywhere else. This prevents the content from getting stolen or shared.

iii. Disable Export

This option restricts the user from downloading the current file in any specific format on his system/PC.

iv. Disable Print Functionality

This option restricts the user from taking print of the current file i.e. the file in use.

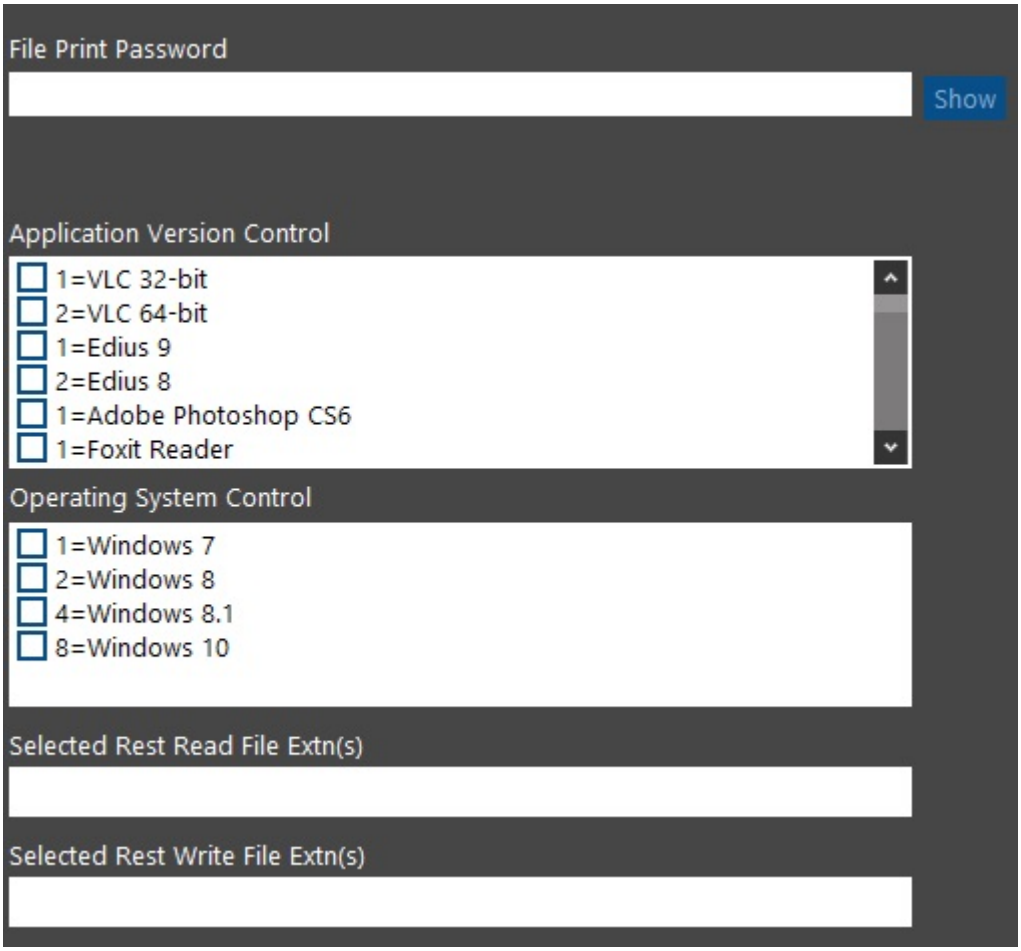

Figure 14 Operating System Control

File Print Password

This feature allows the client to set a password for the user to print the current file. The user needs to enter the file password as shared by the client for taking print of current file.

Application Version Control

When the receiver tries to decrypt the file using Launcher tool, then one of the two scenarios will be encountered:

- If the Sender hasn't selected any specific version for Target application, then receiver can open the encrypted file in any version of Target application as available on his system.
- If the Sender has selected a specific version for Target application, then file will open only if that version is available on the system of receiver.

Operating system control

This allows the client to restrict the Operating systems on which the shared file can be accessed by the receiver.

4.2.3Two Way Authentications

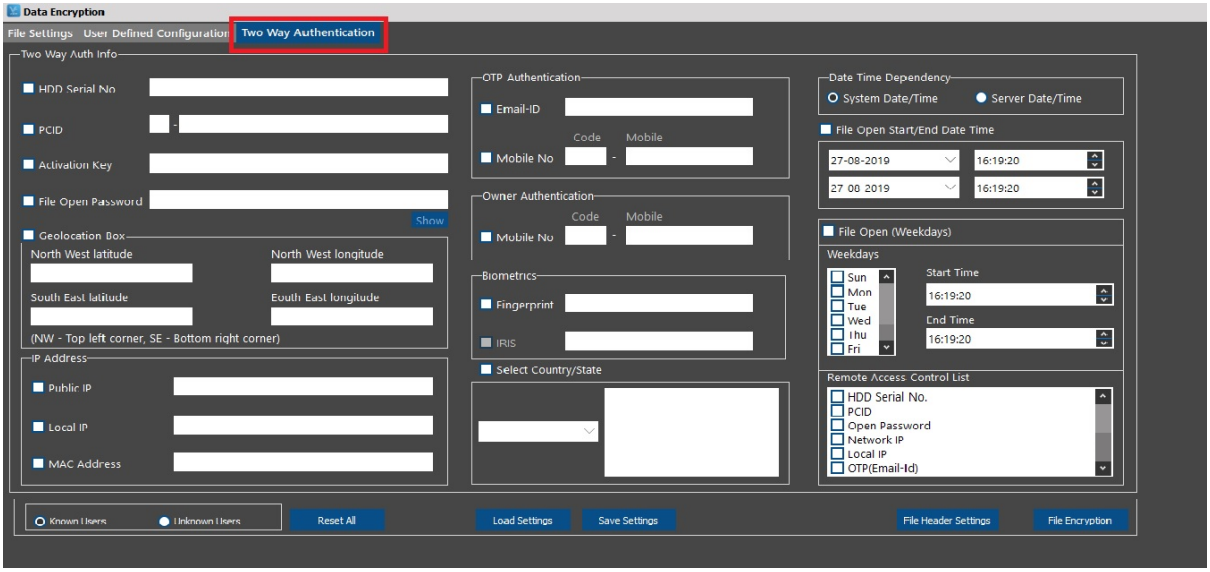

Figure 15 Two Way Authentication

Two-way authentication works with two separate security or validation mechanisms. Typically, one is a physical validation token, and one is a logical code or password. Both must be validated before accessing a secured service or product.

Two-way authentication, sometimes referred to as two-step verification or dual way authentication, is a security process in which the user provides two different authentication way to verify themselves to better protect both the user's credentials and the resources the user can access.

Its works two types of users:- Known Users and Unknown Users

Figure 16 Users

Known Users

Known users are those users who you've been able to uniquely identify based on certain unique information provided by them such as their email ID, phone number etc.

Unknown Users

An Unknown user refers to those who have visited your website or downloaded your app but have not logged in, made a purchase yet etc.

Components of **Two Way Authentication** screen have been divided into parts as shown in given below:

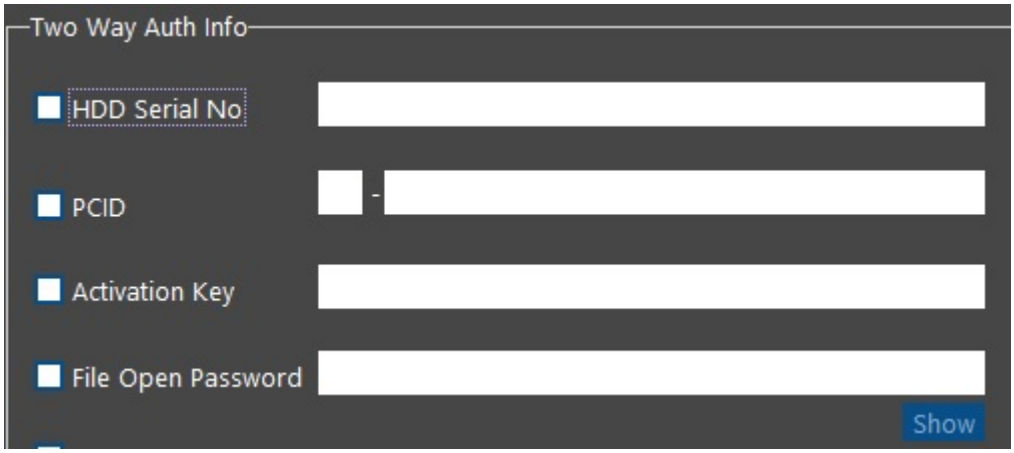

Figure 17 Two Way Auth Info

Two Way Auth info

HDD Serial No

- Refers to Serial Number of Hard disc drive
- Sender can configure these serial numbers to provide access only on those PCs having that HD

PCID

- Refers to unique ID of Receiver's PC generated at the time of Launcher installation
- Sender can configure these IDs to provide access only on those PCs

File Open Password

Refers to the Password set by Sender & shared with Receiver to open any encrypted doc.

Activation key

Unique key linked to Soft/Hardware License. Sender can configure these keys linked to the receiver of encrypted docs.

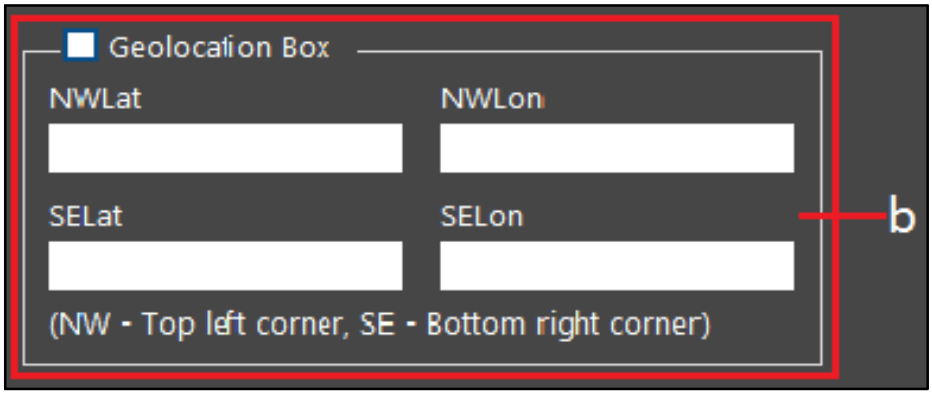

Figure 18 Geolocation settings

Geolocation Box

Geolocation is the process of finding, determining and providing the exact location of a computer, networking device or equipment. It enables device location based on geographical coordinates. Geolocation works through a pre-built GPS in a device that propagates the device's longitudinal and latitudinal coordinates.

Setting up Lat, Long Coordinates of a location in which encrypted docs can be accessed/will get opened by the recipient.

Figure 19 IP Address Settings

Public IP

An Internet Protocol (IP) address that is designated for use in a public domain, such as the Internet. An external or public IP address is used across the entire Internet to locate computer systems and devices.

Local IP

A local or internal IP address is used inside a private network to locate the computers and devices connected to it.

MAC Address

A media access control address (MAC address) of a device is a unique identifier assigned to a network interface controller (NIC).

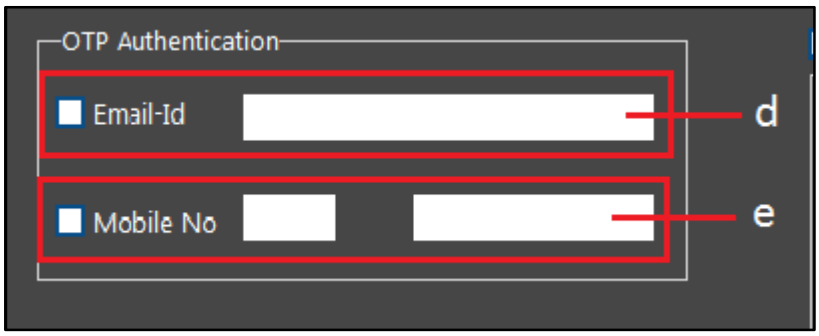

Figure 20 OTP Authentication

OTP Authentication:- Email-id & Mobile No

Email-id

When option is checked, OTP will be sent to email-id of recipient as entered here.

Mobile No

When option is checked, OTP will be sent to mobile number of recipient as entered here.

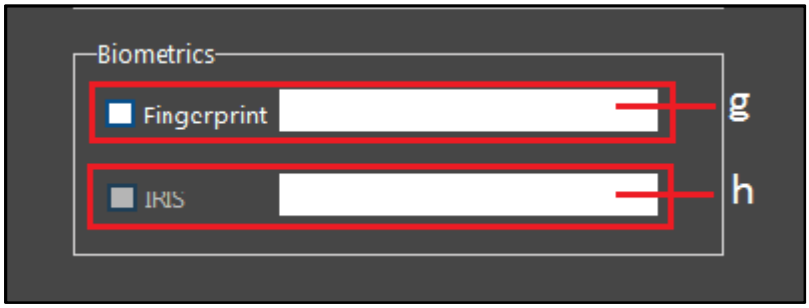

Figure 21 Biometrics

Biometrics

There are two types of biometrics- Fingerprint and IRIS.

Fingerprint

A form of biometric authentication, fingerprint authentication automatically compares a user's fingerprint to a stored fingerprint template in order to validate a user's identity. Fingerprints are unique, impossible to detect & difficult to fake without significant effort. When a fingerprint is scanned , touch ID is generated & the device compares the stored value with scanned value. If the fingerprint matches successfully, the receiver will be able to open the doc.

IRIS

Iris recognition is an automated method of biometric identification that uses mathematical pattern-recognition techniques on video images of one or both of the irises of an individual's eyes, whose complex patterns are unique, stable, and can be seen from some distance.

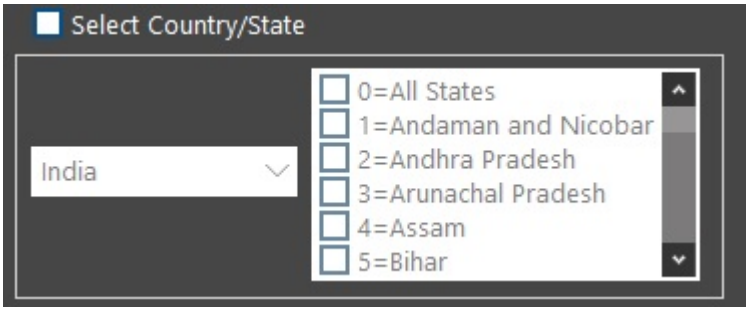

Figure 22 Country/State

Select Country /State

Users can select country and state where file encrypt is open.

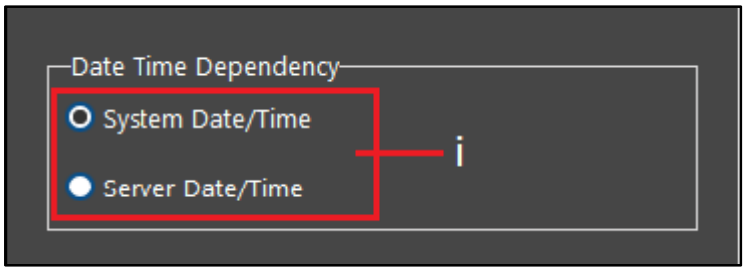

Figure 23 date time dependency

Date Time Dependency

Client can use this feature to set the date and time of server or system.

By doing so, encrypted files shared by the client will open on recipient's system on a particular date & time as per options file open and start date & time or file open week days in upcoming sections .

If System Date/Time is selected, then file will open as per recipient's system date & time settings.

If Server Date/Time is selected, file will open on recipient's system as per server date & time settings. If server data/time is selected user necessary to access online network.

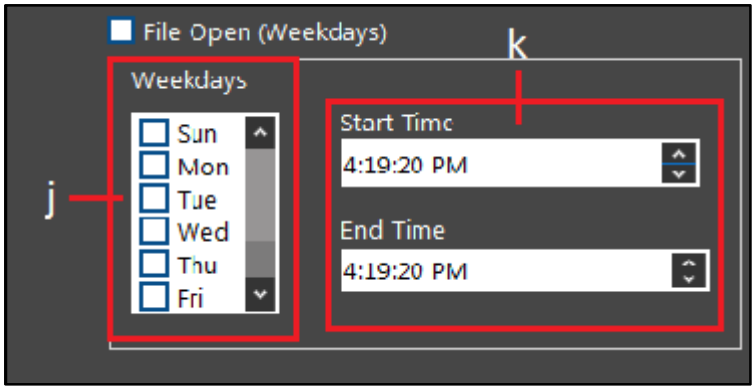

Figure 24 File Open(weekdays)

File Open (Weekdays)

Client can use this feature to restrict the recipient to open the shared encrypted file on a particular day of a week with specified Start time & End Time. Recipients won't be able to access the file on any other day or outside the limit of selected time period.

Weekdays

Client can select the day(s) of a week to restrict recipient to open the encrypted file on that day of week only. Recipient won't be able to access encrypted file as shared on any other day apart from those defined by the client.

Start time and End time

Client can define the Start Time & End Time to restrict the recipient to open the encrypted file within that time period only. Recipient won't be able to access encrypted file as shared outside the defined time period.

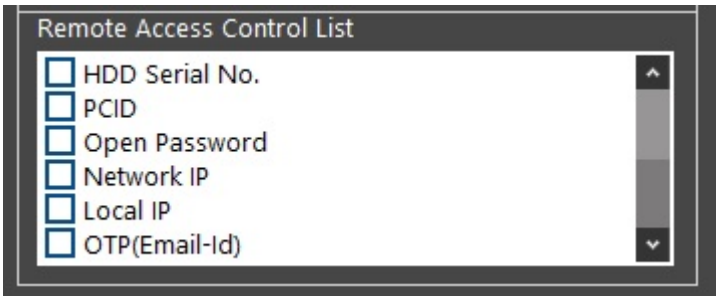

Figure 25 Remote Access Control

Remote Access Control List

Remote access control software is a tool that allows a local user to connect to and access a device, specifically a computer remotely. It refers to ability to monitor and control access to the computer or network anywhere and anytime.

HDD Serial No.	OTP(Email-id)
PC ID	OTP(Mobile No.)
Open Password	Geolocation Coordinates
Network IP	MAC address
Local IP	Auth key public-id
Duration based	Geo country/state

4.3Data Decryption

Authorized user can easily convert encrypted data to original by using OTP on registered mobile and E-mail id.

If 2 way authentication via OTP verification is enabled by the Sender, then recipient needs to provide OTP in order to access the encrypted document. OTP will be shared on receiver's email id & mobile number. On successful verification of OTP as entered by the recipient, document shared by the sender will get decrypted to be viewed by the recipient. Upon saving the document, it will again get converted to encrypted mode.

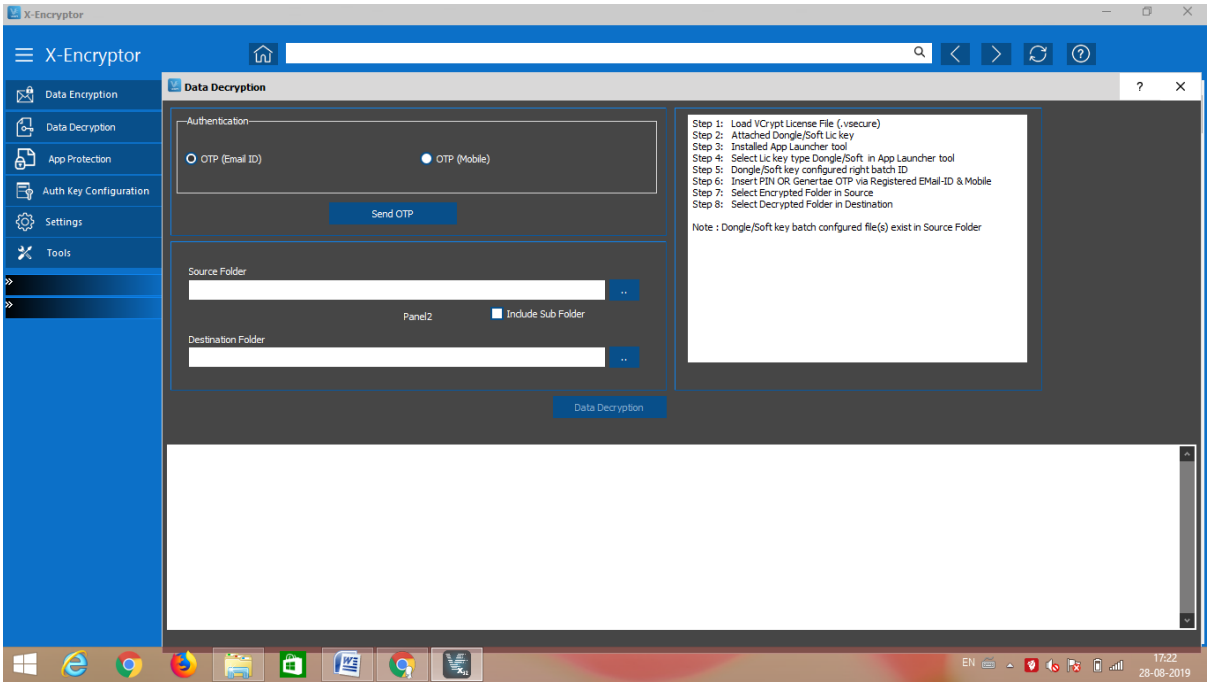

Figure 26 Data Decryption

4.4 APP Protection

User can directly protect Application executables file/ PE binary files like EXE, DLL OCX etc. It supports both 32/64-bit PE format:

As soon as an application is launched in the market, its cracks, patches are available online. There are many weak points in the developed application that results in cracking like simple key generation algorithms, weak registration schemes, application file itself is not protected against tampering or modifications of source code etc. Unprotected software is highly vulnerable to reverse engineering analysis & may result in recovering the fragments of source code or in some cases, the entire source code of the application.

VCrypt software security solution is designed to protect your windows 32/64-bit application against any such cracking, tampering or reverse engineering. It's also equipped with a build in licensing system to enable you to add license key system to your application.

The protection & licensing features can be integrated in the application using dedicated SDK.

User can protect any compiled application file for Windows as long as it's compatible with the PE (Portable Executable) format irrespective of the programming language or development environment used to create it. VCrypt software supports PE file formats like exe, dll, ocx etc.

Code, data and additional application resources are encrypted using strong cryptographic algorithms and multilayer polymorphic encryption so in case the intruder tries to remove the protection code, the application would be safe & can't be run.

Also, if the user wants to add extra **DLL** libraries to the application, it's possible to merge the main application **EXE** file with them & make it as a single output **EXE** file.

1. File settings
2. Two way Authentication
3. Users Defined Configuration

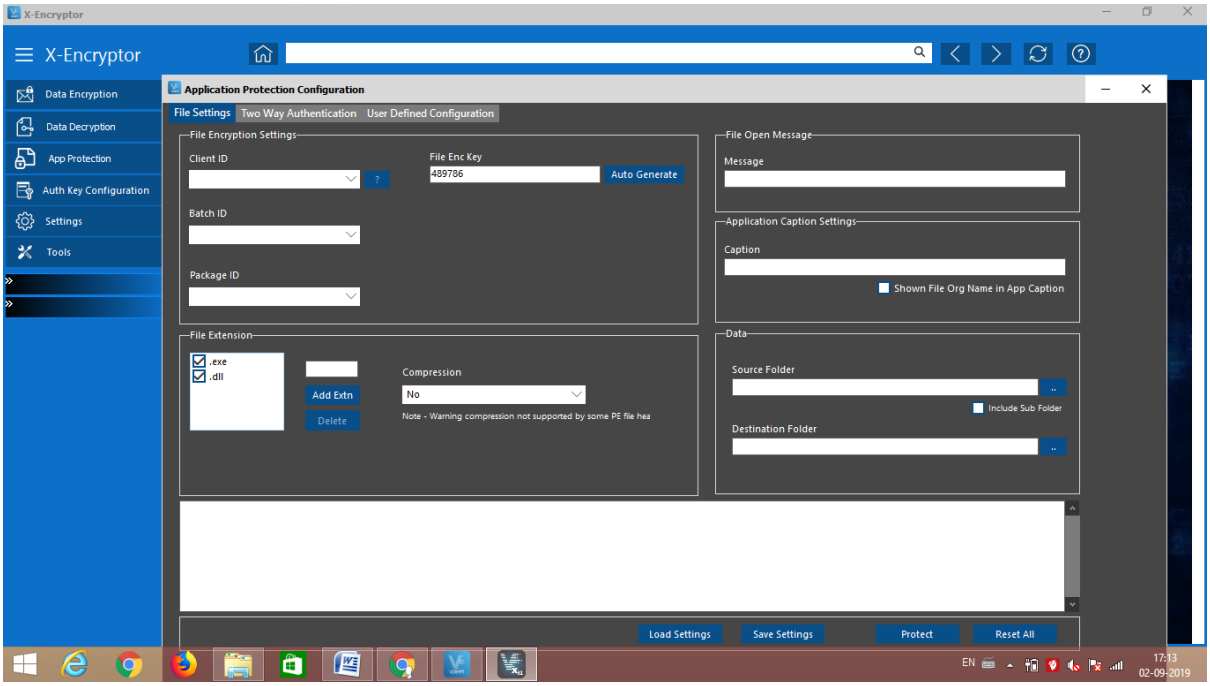

Figure 27 Application Protection Configuration

4.4.1File Settings

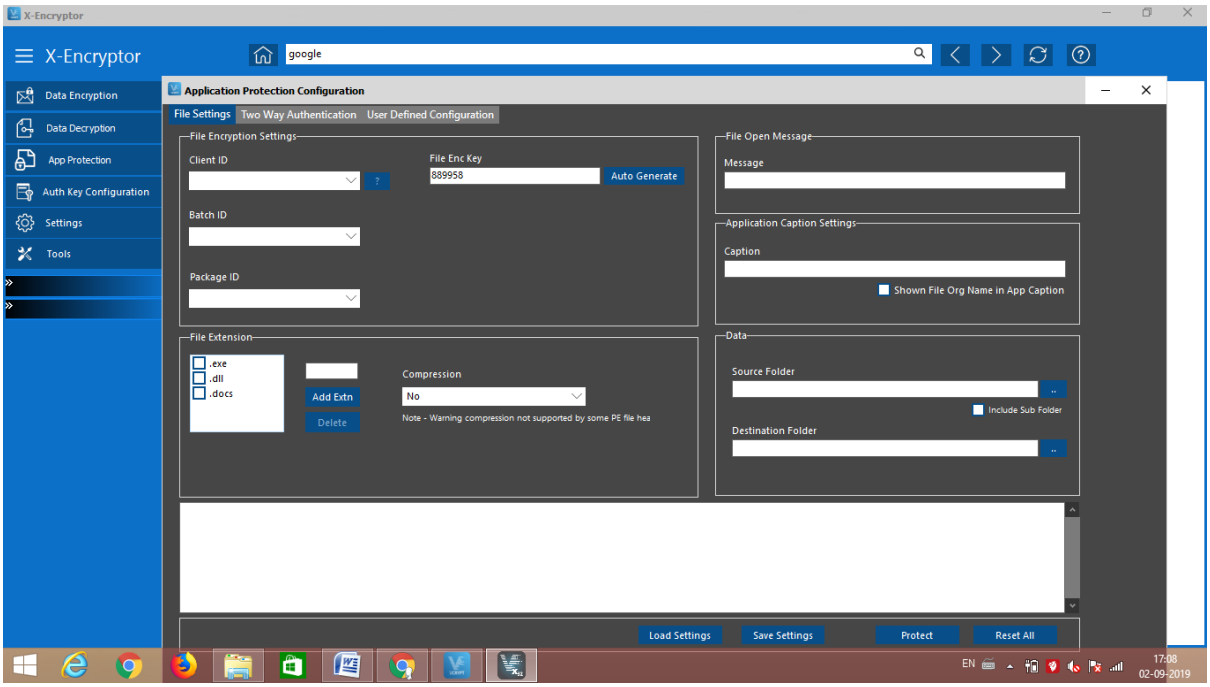

Figure 28 File Settings

Client Id

Client ID is assigned to each unique user of our website. Unique number generated at the time of purchasing VCrypt System setup. User can't set/reset this value. This is in Read only mode.

Batch Id

Refers to unique ID of batch created by client at the time of purchasing the software. Multiple batches can be created by the client for same ID/Account. It is created in the client config panel of VCrypt System website. Batch ID will be displayed for selection here in dropdown list.

Package Id

Unique ID related to package created by client under one batch. Multiple packages can be created by client under one batch. Client can add number of files under one package.

File Enc Key

Auto generated number used as key to encrypt the file. This is helpful when we have two files with same mechanisms and we need to differentiate between the two files while encryption we use this encryption key.

File Extension

A **file extension** (or simply "**extension**") is the suffix at the end of a **filename** that indicates what **type** of **file** it is.

Depending upon the type of applications selected by the client, file extensions corresponding to those applications will be displayed for selection.

File Open Message

Message displayed (in dialog box) to recipient of encrypted file when he opens that file in target application. Client can configure the message by entering required details.

Captain

Client can configure the Caption for file which will be displayed in header section when the decrypted file will open in target application. It is the file name which is displayed in the caption field.

Show File Orginal Name in Application Caption

By checking this option, Client can set the **Original File Name**(Default) as **Caption** in case he doesn't want to add any caption for the file.

Source Folder

This folder contains the original files, which the client wants to encrypt. He needs to browse through Source folder to select the files for encryption.

He can also add sub folder(s) to it, if there exists any.

Destination Folder

This folder contains the encrypted files. Client needs to select the destination folder to save encrypted files. After entering required details & clicking **File Encryption** button, the Encrypted files will be saved in destination folder as selected.

4.4.2Two way Authentication

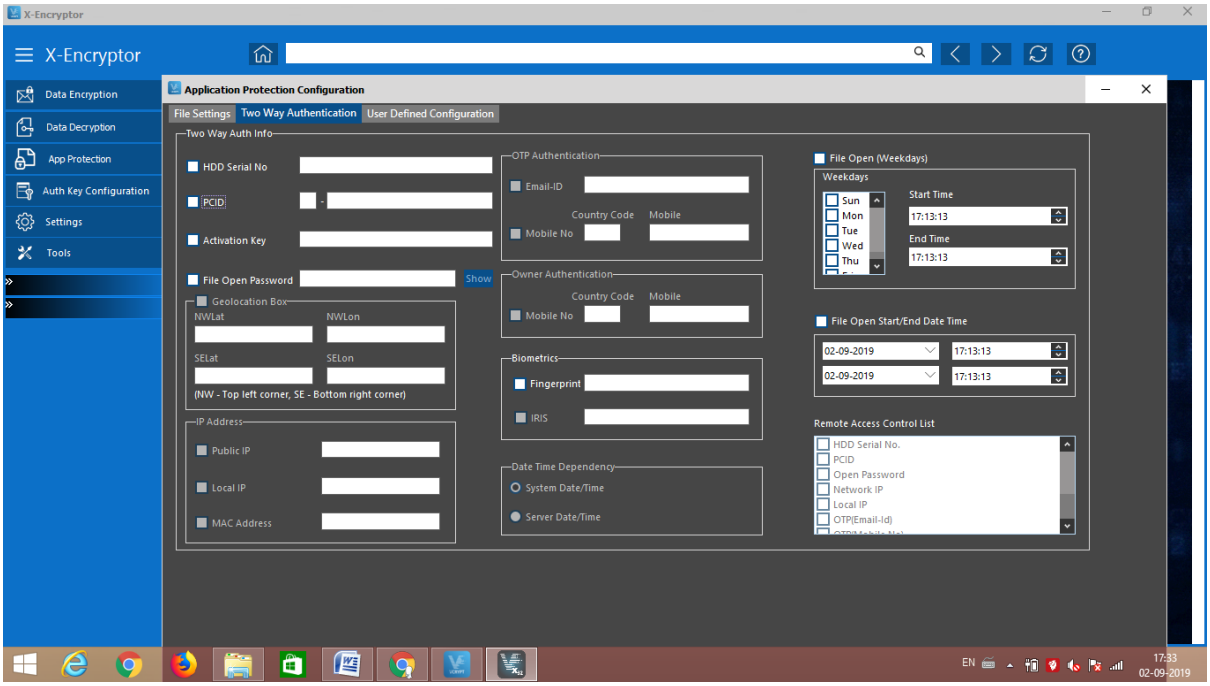

Figure 29 Two-Way Authentication

Two-way Authentication already covered in section 4.2.3.

4.4.3Users defined configuration

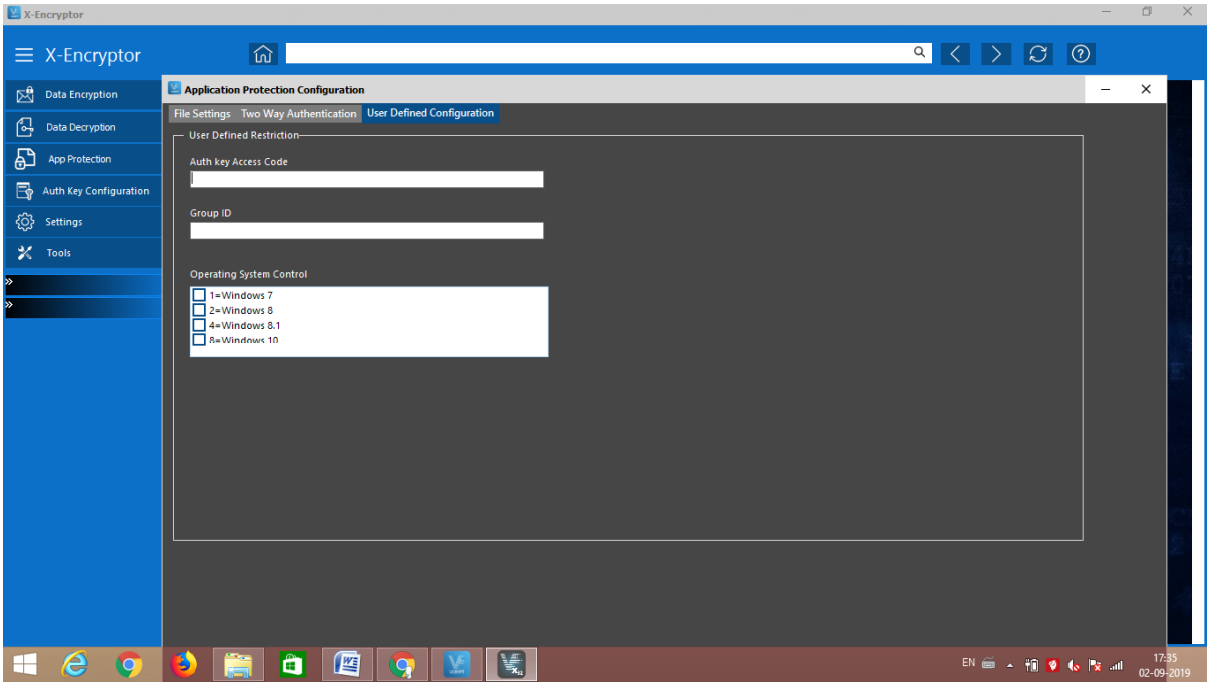

Figure 30 User Defined Configuration

Auth Key Access code

An access code is a series of numbers and/or letters that allow access to a particular system.

Auth Key Access Code is used to differentiate between two files when Batch ID and Package ID are same as auth key access code is always unique.

Group Id

Group ID distinguishes between file currently in use & other file in case they share similar names. It is unique for every new file.

Operating System Control

This allows the client to restrict the Operating systems on which the shared file can be accessed by the receiver.

5.Auth Key Configuration

User can configure Dongle H/W key OR Soft key within this module.

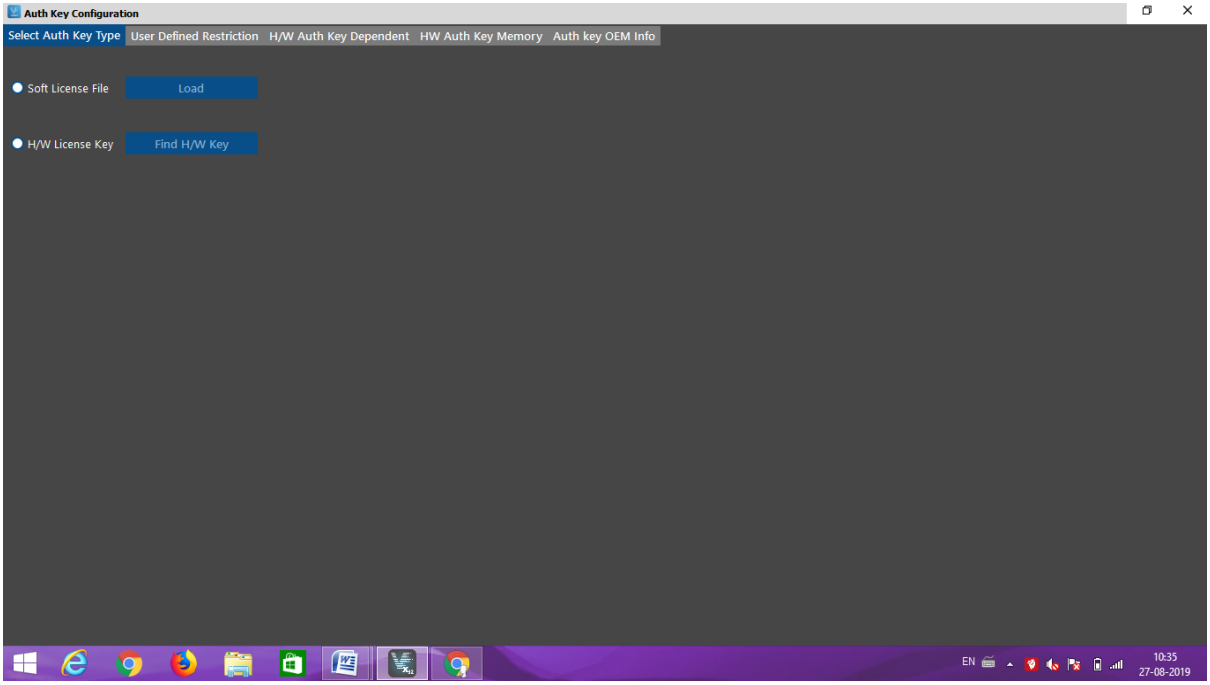

Figure 31 Auth Key Configuration

In this section, client can select the type of License for distribution purpose & hence configure required authentication keys. The Licenses fall into 2 categories:

a. Soft License
b. Hardware License

Soft License:

- PC based, will work for individual PC.
- On downloading the launcher, PC ID will get generated & gets bind up with the exe files.
- Unique PC ID will be generated on S/W(Launcher) installation which will be used further for data binding.
- Data will decrypt on specific PC if data binding is done with PC ID of receiver.
- If PC gets damaged, then license is also gone.

Hardware License:

- Includes Dongle/hardware keys .
- Floating License type.
- Reseller can distribute the h/w keys to intended recipients.
- Exe files will run on PCs with authorized h/w IDs.
- Software will unlock with configured h/w keys.
- If dongle is lost, then license also goes with it.

5.1 Select Auth Key Type

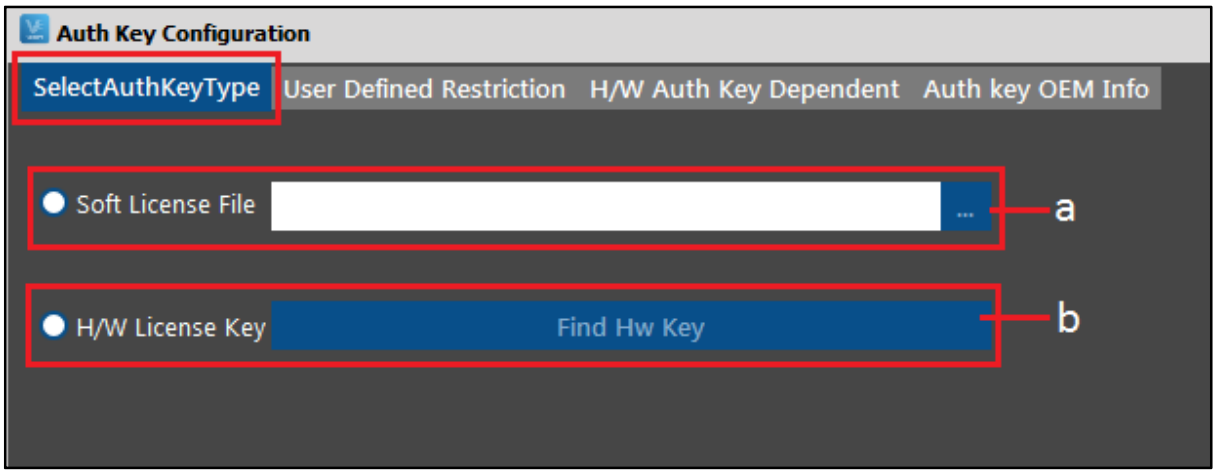

Figure 32 Select Auth Key type

Soft License File

Client will select this option to generate soft license. Client needs to browse through the location & select required file for uploading Soft License.

H/W License

Client will select this option if he wants to configure hardware device. To achieve this, client needs to attach the dongle and then click on **Find H/W key button** to read the information.

5.2 User Defined Restriction

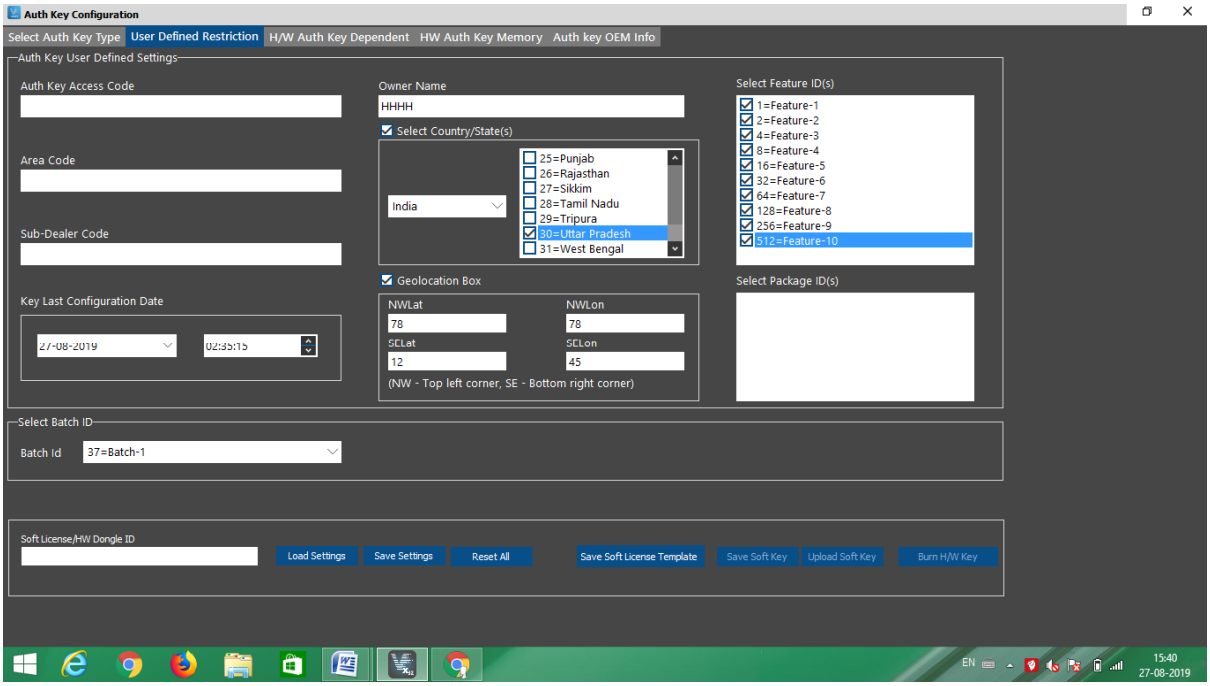

Figure 33 User Defined Restriction

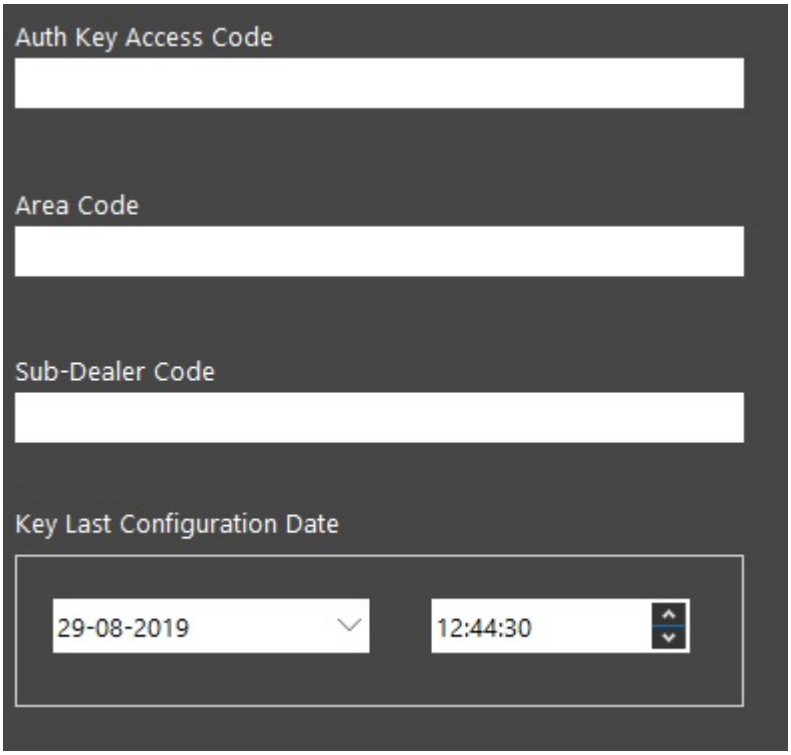

Figure 34 Select code

Auth Key Access Code

In case 2 files to be shared are having same batch id & package id, auth key access code is used to differentiate between them it's always unique. User will be able to access data with written Auth key access code & matching hardware key.

Area Code

Client needs to define the Area code where the hardware will be delivered to its licensed user.

Sub Dealer Code

It refers to Sub Dealer Code of hardware license holder. It is generated when the hardware license is purchased by the user.

Key last configuration date

Refers to the date/time when the hardware was configured for the last time. Client can set/rest this date along with time.

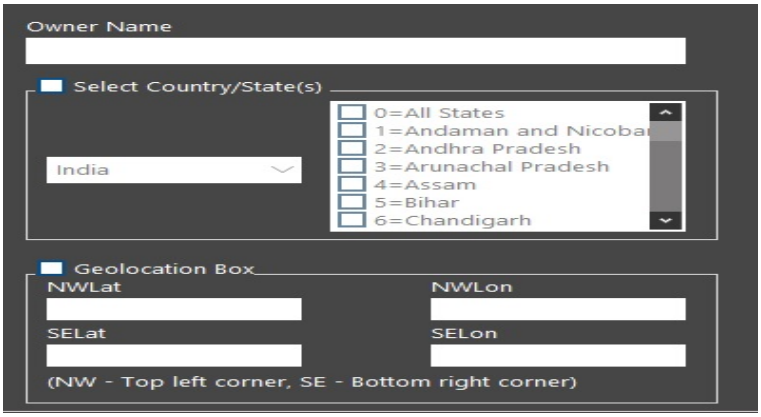

Figure 35 Owner Name and Geo-location

Owner name

Name of the person who hold hardware license.

Select Country/State

Select country and state name.

Geo-location box

It refers to the geographical location of a particular hardware where it will be accessible. Client can select the lat, long values from map and enter them here to set the geolocation for selected hardware.

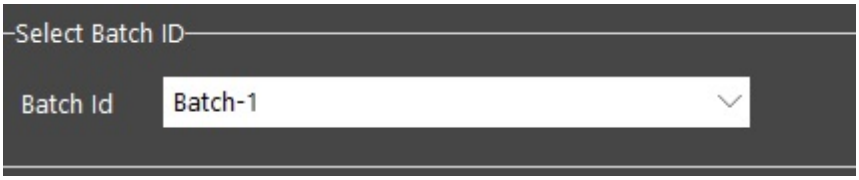

Figure 36 Batch ID

Batch id

Refers to unique ID of batch created by client at the time of purchasing the software. Multiple batches can be created by the client for same ID/Account. It is created in the client config panel of Vcrypt website. Batch ID will be displayed for selection here in dropdown list.

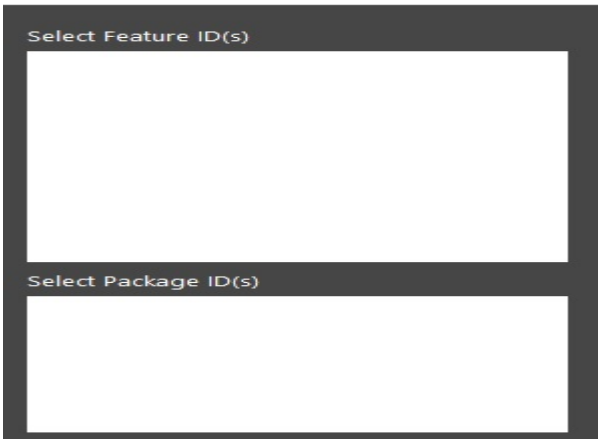

Figure 37 Features and Package

Select Package id

Unique ID related to package created by client under one batch. Client under one batch can create multiple packages. Client can add number of files under one package. Client can select the packages that need to be provided in hardware for end user.

Select Features ID(s)

List of features to be given in selected package for hardware/Soft license. Client can select the features to be given in any package.

5.3 H/W Auth Key Dependent

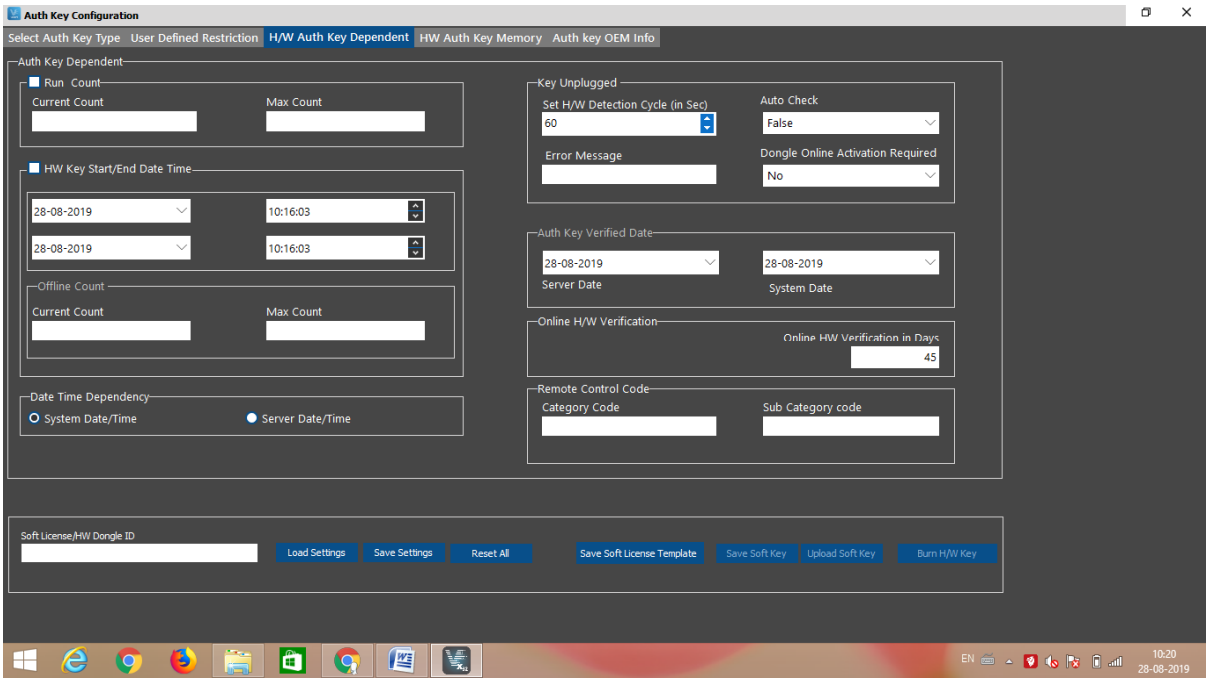

Figure 38 H/W Auth Key Dependent

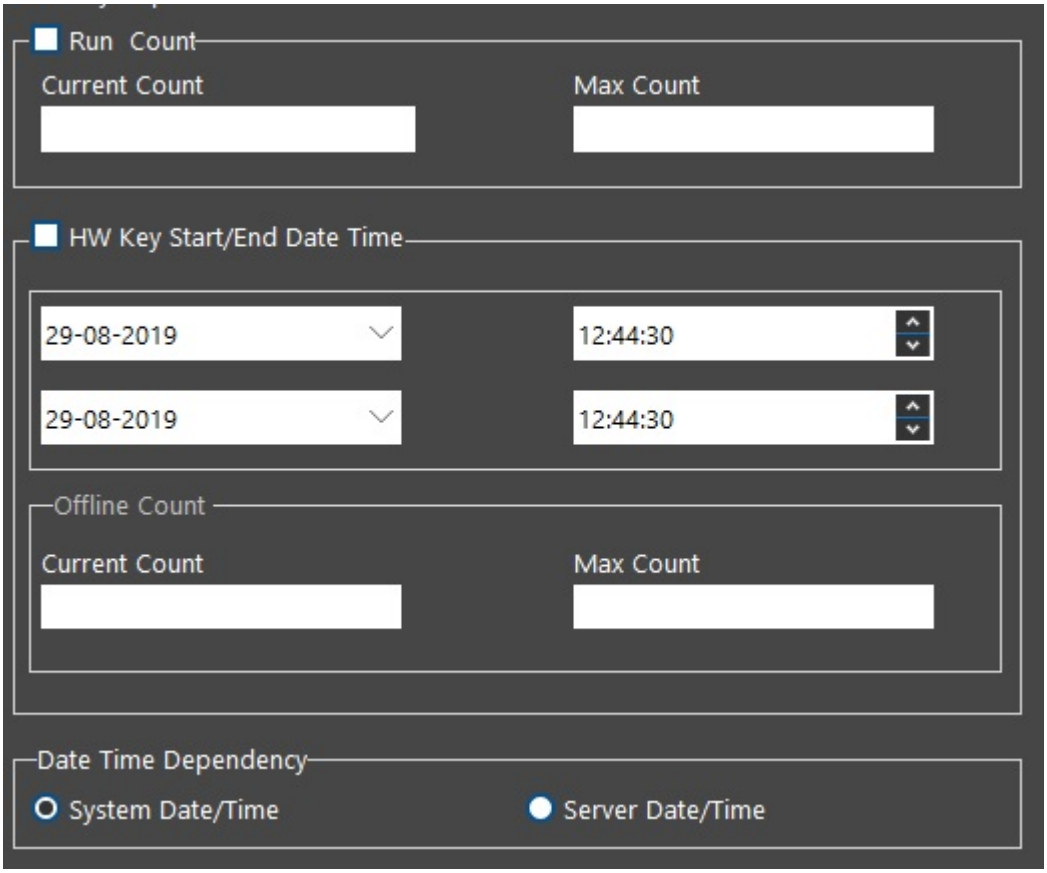

Figure 39 Run count & H/W key start/end date

Run Count

Number of times & ways in which hardware key can be plugged into/unplugged from user's system after purchasing hardware license in either online or offline mode.

Run Count is the number of times the hardware key has been run. It refers to the number of times the hardware key has been plugged in to open the application. The Client needs to check this option & enter the **Maximum Count** up to which hardware key can be plugged in by the user. It reads the values when user in Online i.e. connected to a network.

H/W Start/End Date Time

Client can restrict the H/W to work within selected duration by entering required values for Date & Time. User won't be able to access the application if H/W is read earlier than the Start Date or after the End date.

Offline Count

It refers to the number of times the hardware key has been plugged in to open the application when the user doesn't have internet access. Client needs to enter the Maximum count to use the hardware key.

Date time dependency

If System Date/Time is selected, then file will open as per recipient's system date & time settings. If Server Date/Time is selected, file will open on recipient's system as per server date & time settings. If server data/time is selected user necessary to access online network.

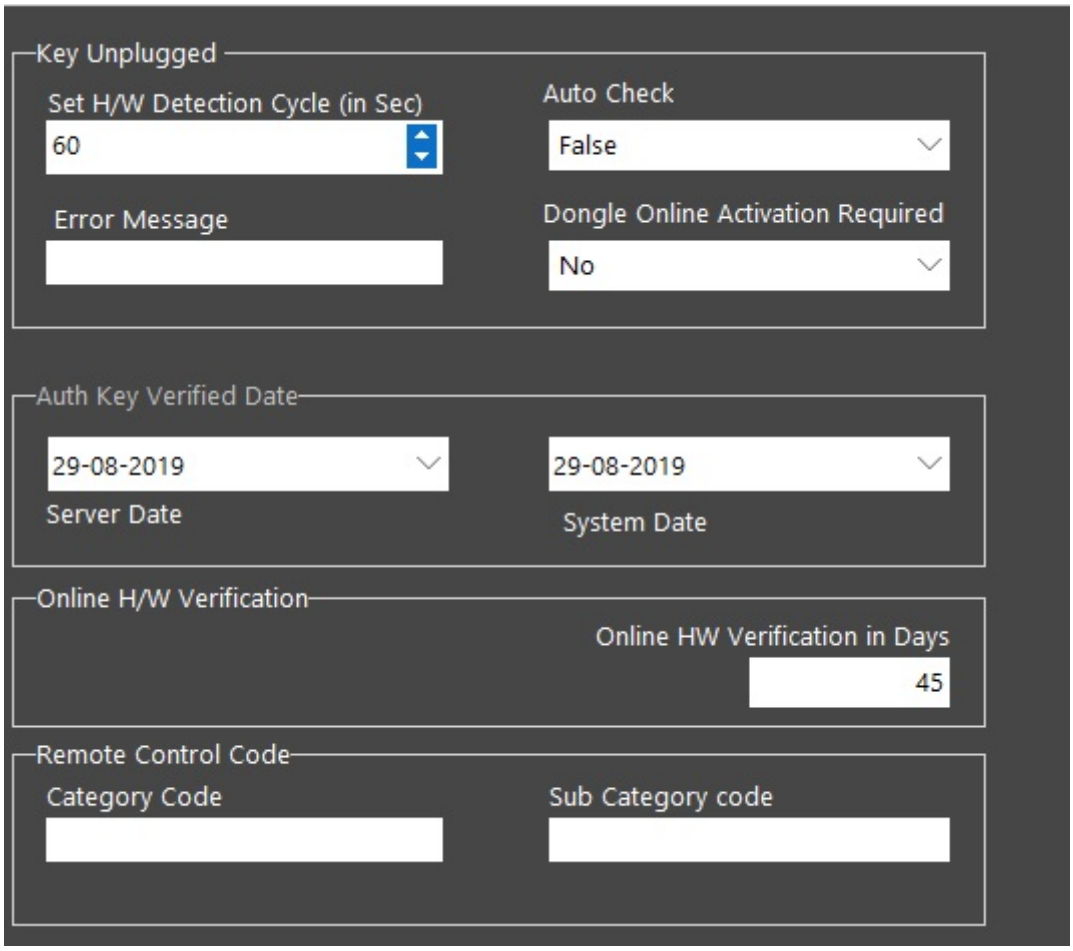

Figure 40 Key Unplugged

Key Unplugged

Client can set the duration (in sec) for the system to detect the hardware key for VCrypt application. Following settings are required under this section:

Set H/W Detection Cycle

Shows for how long the application will run without the hardware being plugged in. Client can set the duration by entering required value in seconds.

Error Message

When Hardware is not Attached/Found, required error message will be displayed. Client can select/set the Error message here.

Dongle onlne activation required

Hardware key needs to be activated before it is used for the first time. Client needs to select the suitable option to activate the H/W key. At user's end, Hardware activation requires internet access.

Auth key Verified date

For internal use. It checks if **Server Date** is in sync with **System Date**. Client can also change the settings.

5.4 Auth Key OEM Info

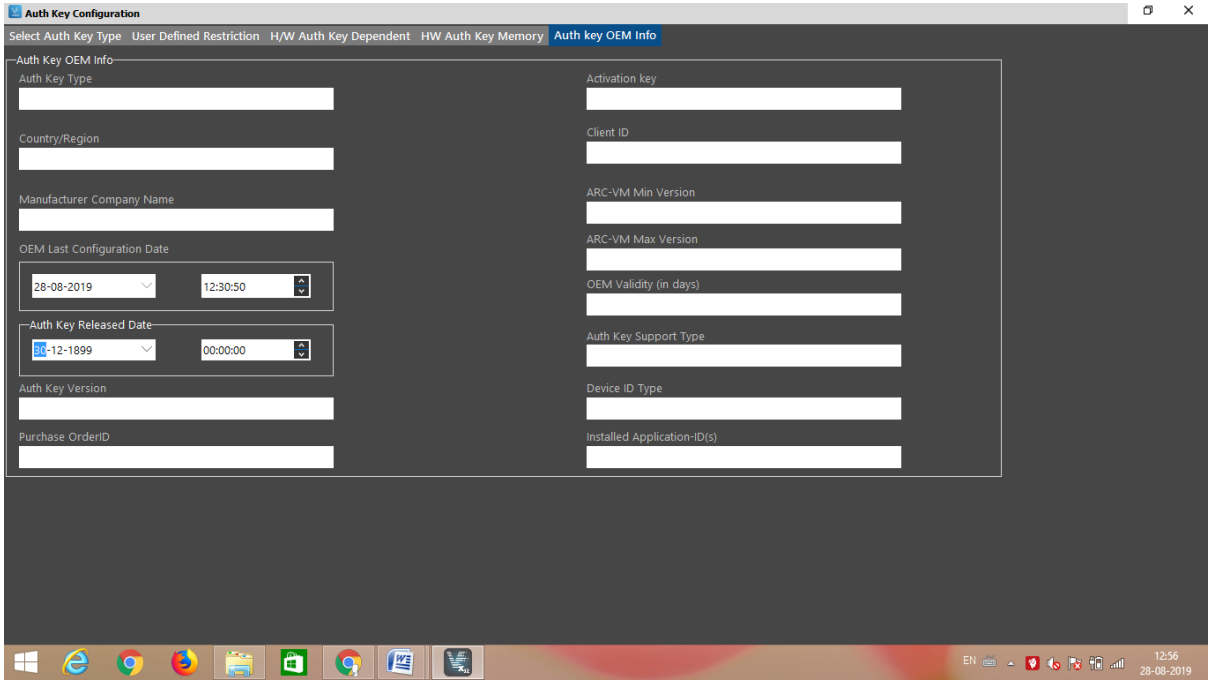

Figure 41 Auth Key OEM Info

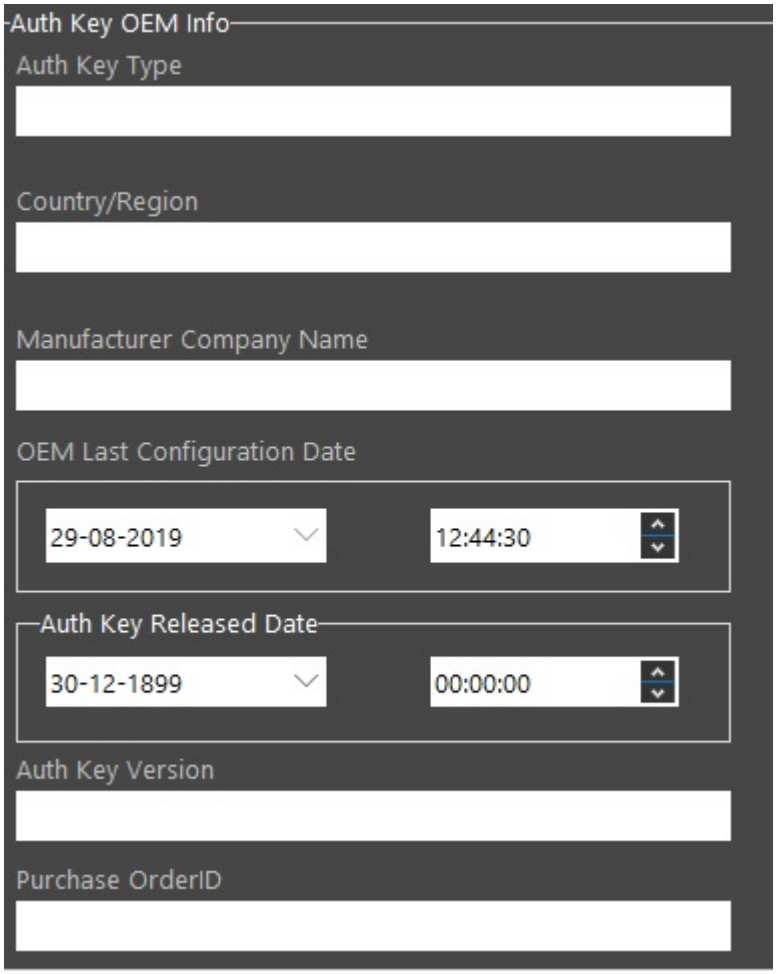

Fig. 16.(a) Auth key

Auth Key Type

It refers to the type of License purchased i.e. Hardware or Soft key.

Country/ Region

It refers to the country/region in which license will be valid & application will be accessible.

Manufacturer Name

It refers to the Product owner i.e. person who is distributing the Hardware/Soft License.

OEM Configuration Date

It refers to the date when the H/W was burnt for the last time.

Auth key released date

Auth key released date that date when the hardware /software key is purchasing and warranty started purchasing date.

Auth key version

It refers to the current version of H/W or Soft License.

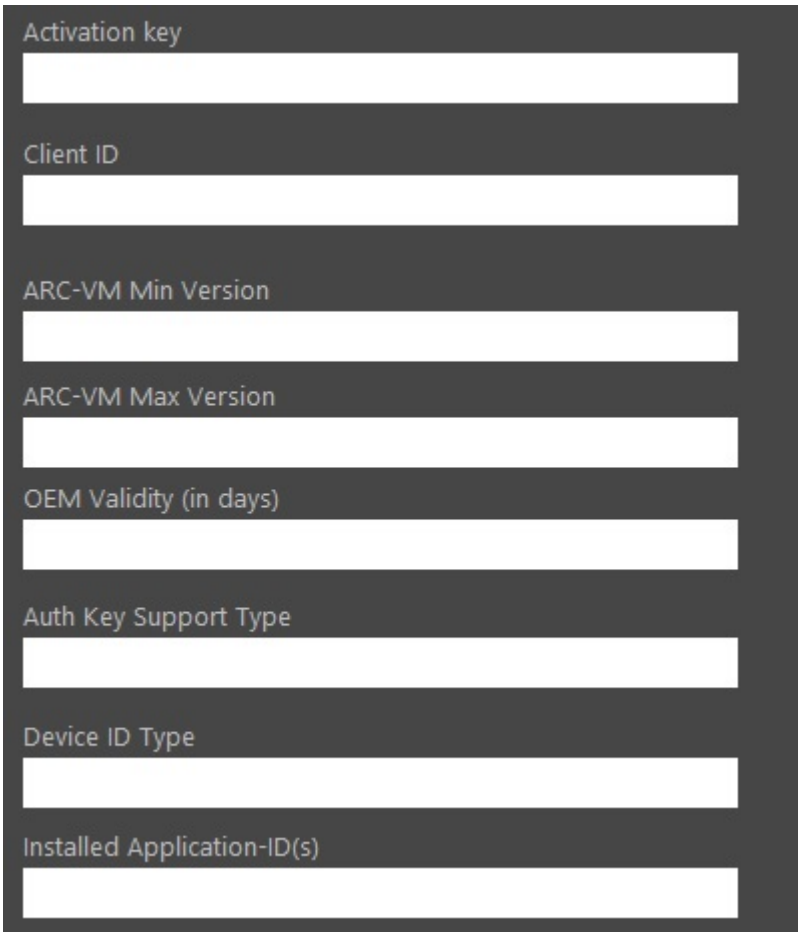

Figure 42 select ARC-VM version

Activation Key

It refers to the unique ID for H/W or Soft License to detect H/W or Software services.

Client ID:

It refers to the unique number generated at the time of purchasing VCrypt setup. Client can't set/reset this value. This is in **Read only** mode.

ARCVM Min Ver

ARCVM stands for **Advanced Runtime Cryptography Virtual Machine.** ARCVM Min version refers the minimum version supported by VCrypt application.

ARCVM Max Ver

It refers to the highest version supported by VCrypt application. VCrypt application will support all versions between ARCVM Max & ARCVM Min.

Auth Key Support Type

It refers to the type of support for selected Auth key. If Auth Key type=H/W key was selected, then it will display support types as: **Network** or **Standalone**. If Auth Key type=Soft key was selected, then it will display support type as **PCID** of target machine only.

Device ID Type

It refers to the unique ID of device. It gives information about the type of Device i.e H/W or S/W

6.Settings

Through this section, Application owner can Launcher configuration, Desktop settings for application or can remotely update manage/change the application.

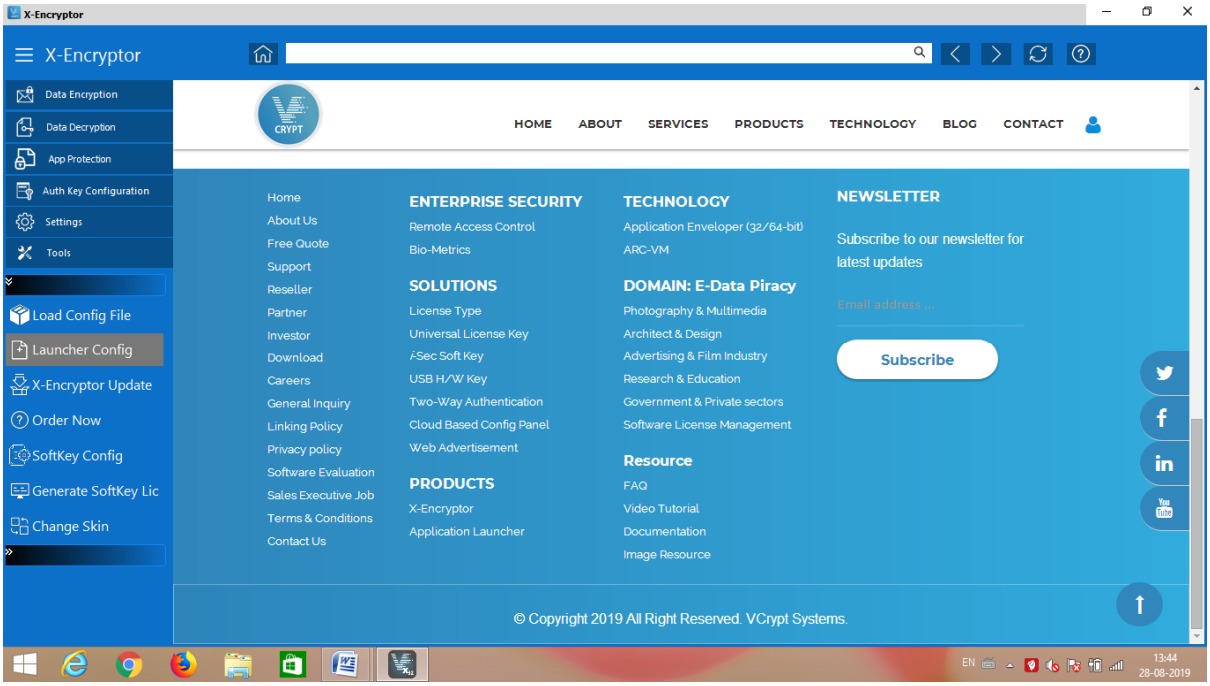

Figure 43 X-Encryptor Settings Functionality

There are 7 tabs under Settings module:-

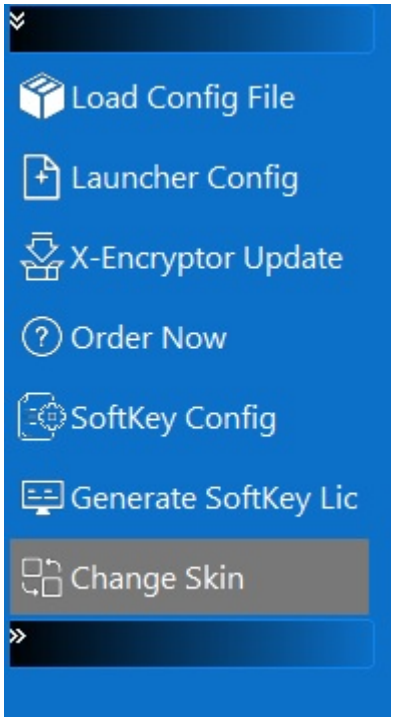

Figure 44 settings function

6.1 Load Config File

A Configuration (Config.) **file** that contains data about a specific user, program, computer or **file**. In this setting option load client Id for encryption a data file.

6.2 X-Encryptor Update

Users/clients Update a tool up to date.

6.3 Order Now

Clients purchase product and get serial key.

6.4App Launcher Configuration

In this section, application owner/Client can configure various settings for the Launcher application like a Launcher app shortcut on desktop, desktop icon, desktop app name etc. Client after configuring the Launcher as per requirements can resell/distribute it to intended users.

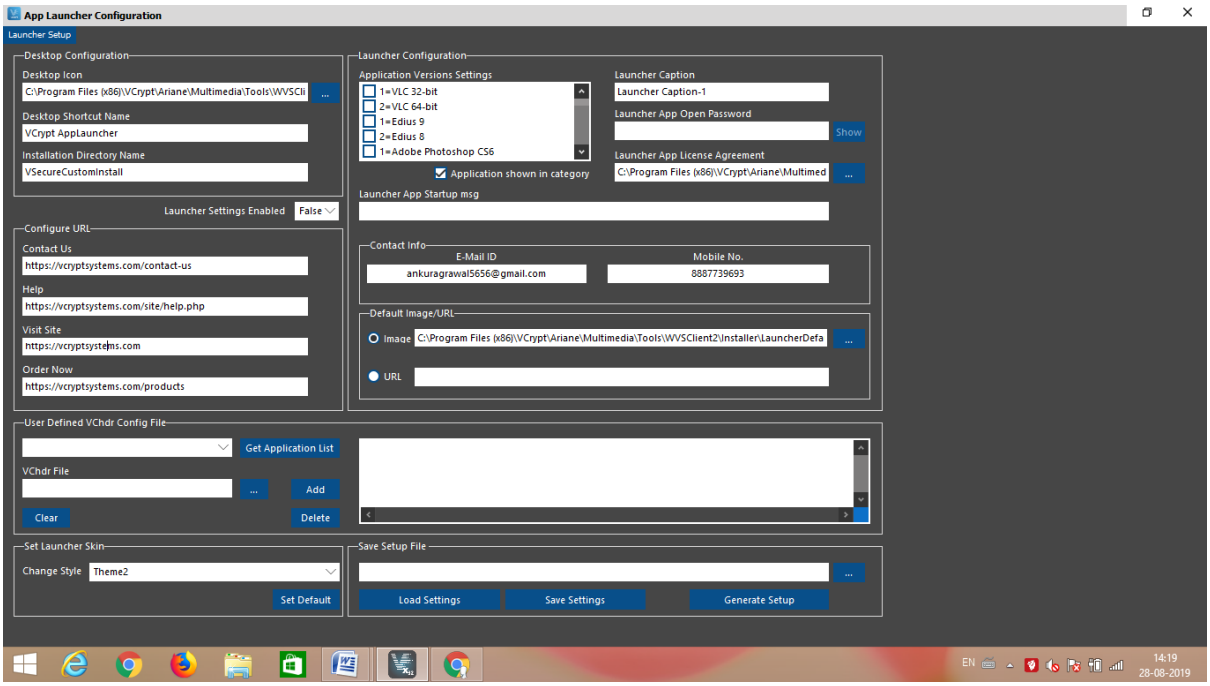

Figure 45 Launcher setup

Desktop Configuration:-

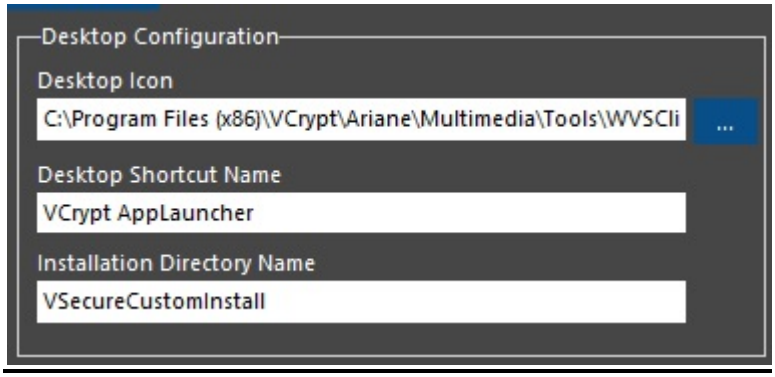

Figure 46 desktop configuration

Desktop Icon

Client can select the Launcher icon to be displayed on desktop after installation of Launcher Setup on target machine.

Desktop Shortcut Name

Client can enter the name of Launcher app to be displayed on desktop as Shortcut link.

Installation Directory Name

Client needs to enter the name of directory for launcher installation.

Figure 47 Configure URL

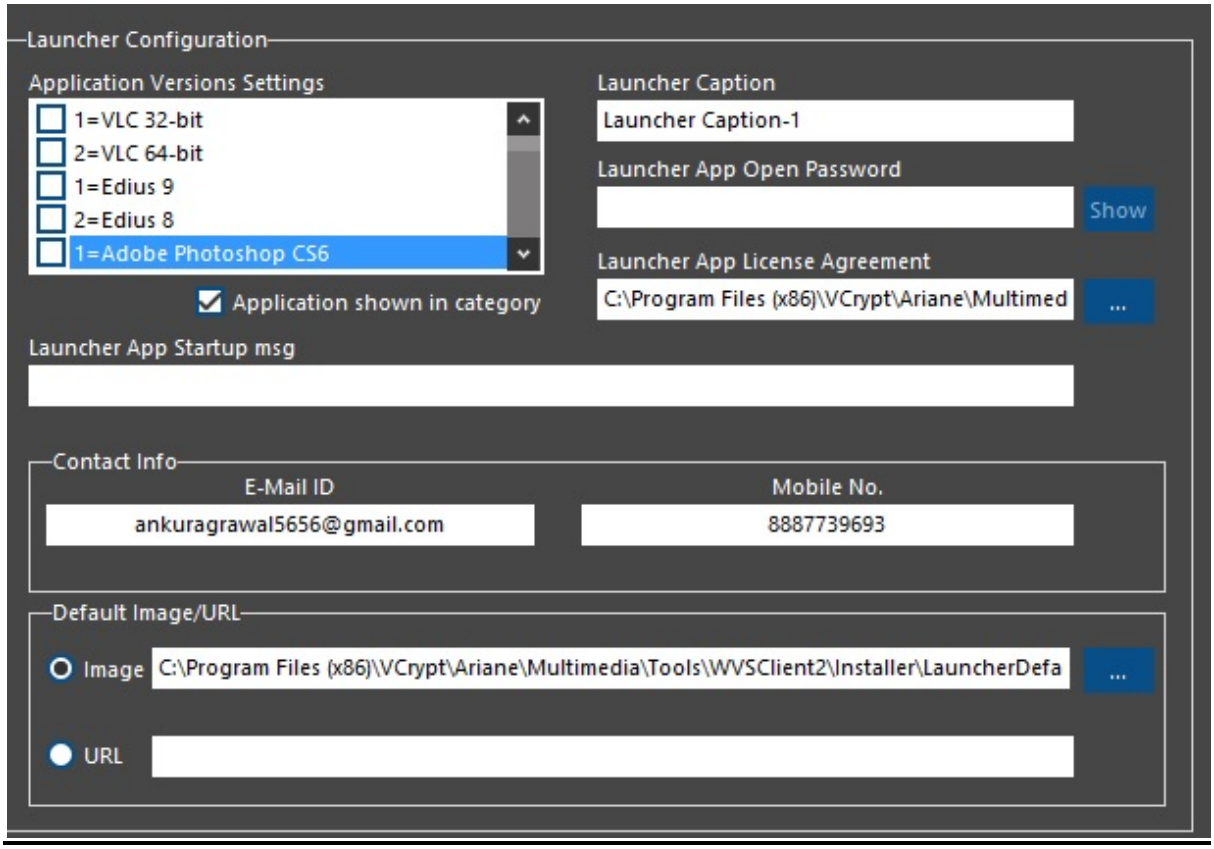

Figure 48 Launcher Configuration

Launcher Configurations

In this section, client can configure all the details required at the time of Launcher installation so as to redistribute the application to intended user. Below details are required to be filled up for Launcher configuration.

Application Versions Settings

Client can also select the versions applicable for each target application. If specific version is selected then end user can open docs only if those versions of target application are available on his system.

Launcher Caption

Client can enter the caption i.e. name of Launcher application which will be displayed in header section of Launcher application.

Launcher App Open Password

Client can set the default password to access Launcher application. End user can reset this password if required.

Launcher App License Agreement

Client can upload the file for License agreement to be shared with end user or license holder.

Launcher App Start-up msg

Client can set the message which will appear after successful installation of Launcher Application on target machine.

Default Image/URL

Client can enter the Image/URL of launcher app.

7.TOOLS

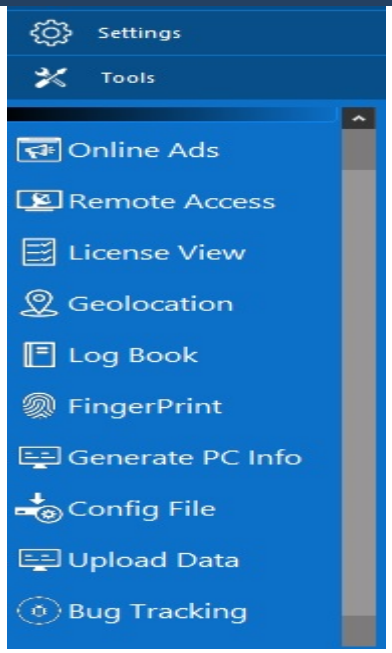

Figure 49 X-Encryptor Tools

7.1ONLINE ADS

Under this section/form the Online Ads access to particular area and date/time ads will created .

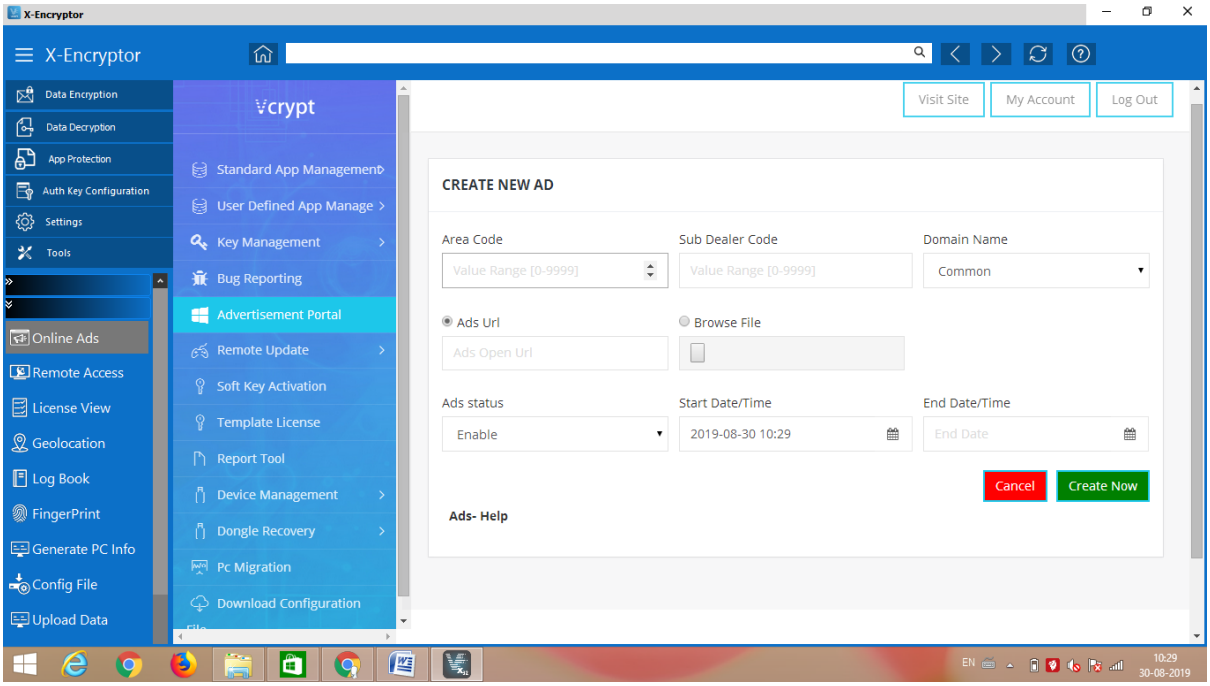

Figure 50 Online Ads

Area Code

Area code is that specific area where Aid will be created. Client needs to define the Area code where the Online Ads will create be to its licensed user.

Sub Dealer Code

Sub Dealer code refers to specific place whose area code are selected above option. It refers to Sub Dealer Code of hardware license holder. It is generated when a hardware license is purchased by the user.

Domain Name

In domain name option client choose online ads related which fields.

Ads Url

A Destination URL is simply the address of your webpage people reach when they click one of your ads. Users select one option ads Url or browse file.

Browse File

Browsing is commonly used to describe when a user reads through pages on the Internet or looks through the contents of the files on their computer. In browse file client choose online ads file.

Ads Status

Clients select ads status enable or disable.

Start Date/Time

In this option client enter date/time when aid enable.

End Date/Time

In this option client enter date/time when aid disable.

Geolocation

Clients can access customer geolocation coordinates. Users can view location own his customer by geolocation.

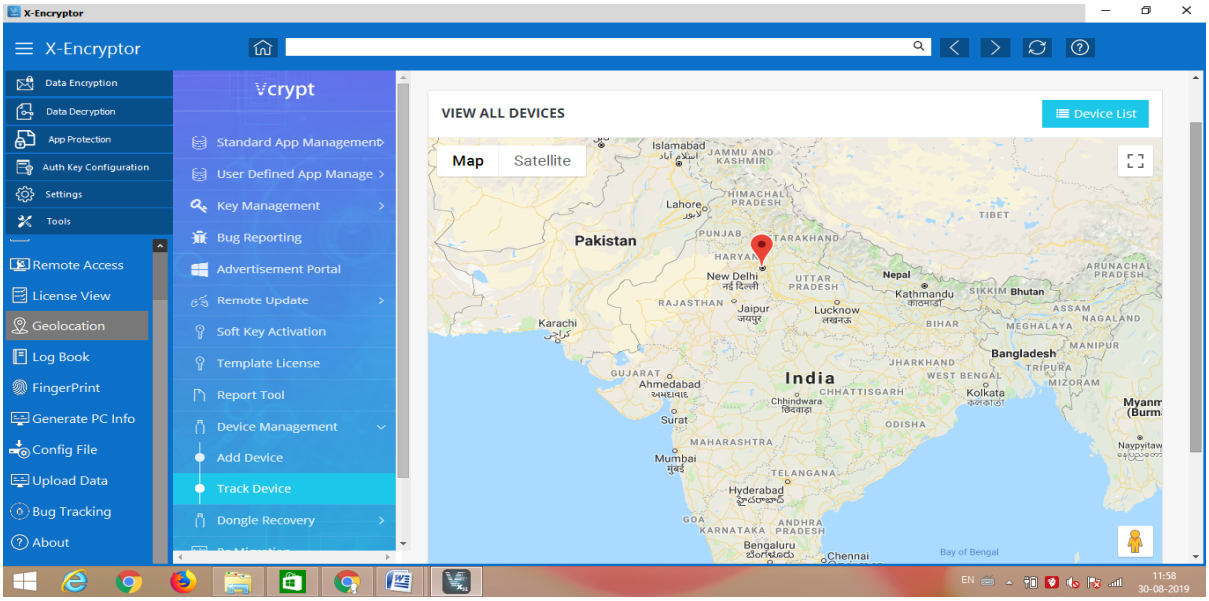

Figure 51 Geolocation

7.2 Log Book

Logbook or User Audit trail provides valuable information about the complete activity timeline of application user i.e. activities performed by him from login to logout. Real time user session monitoring helps in detecting system & data misuse by tracking user activities on the network. It also provides exhaustive reports with a complete audit trail of all user activities. This helps the concerned Organization/Application owner to detect malicious activities & security violations in real-time.

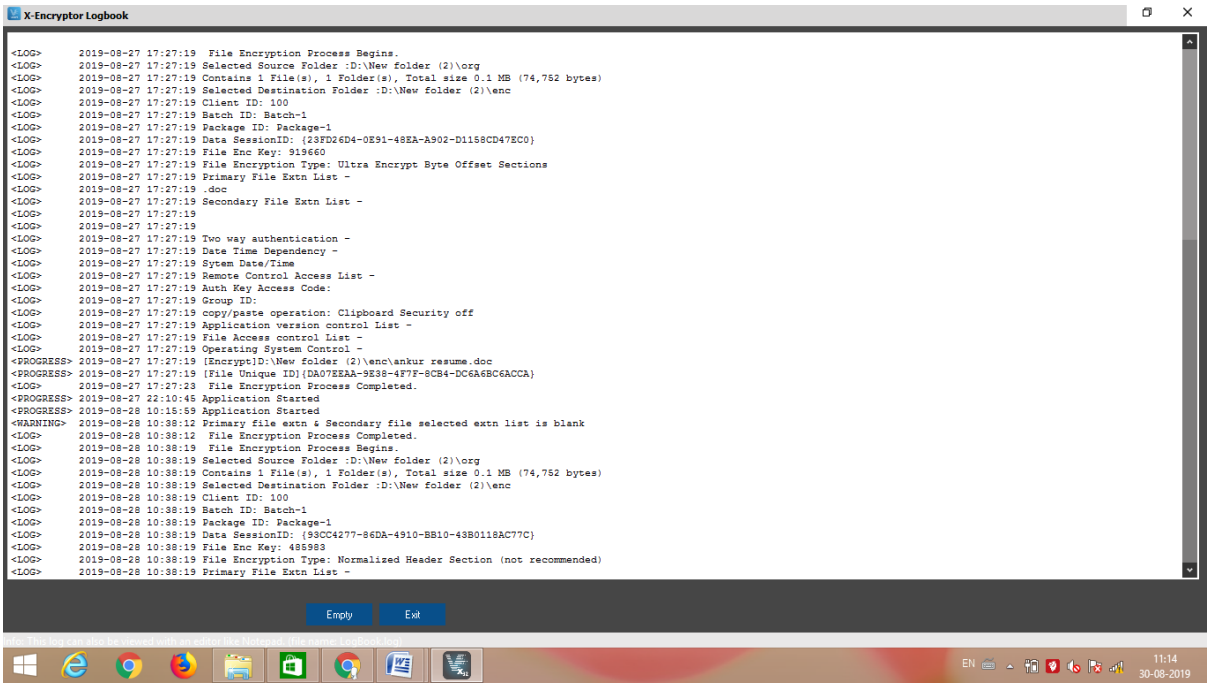

Figure 52 Log Book

Users can empty log book click on empty button.

7.3 Generated PC-Info

Users can generated PC-Info. This section provides detailed information about the PC or device on which VCrypt System application is running.

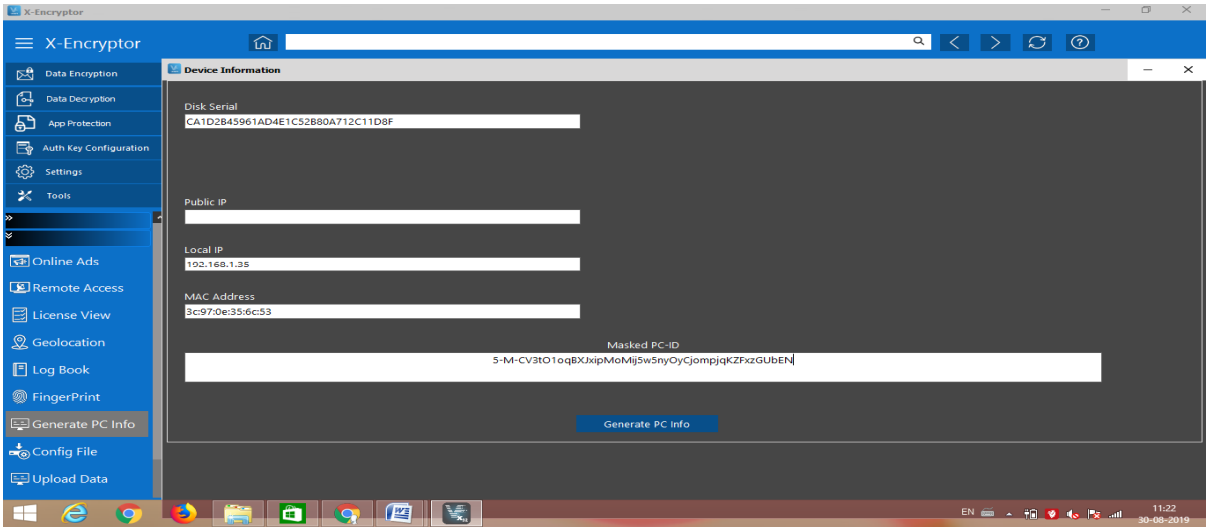

Figure 53 Generated PC Info

When clients click on generated PC Info then shows public IP, Local IP, MAC Address and Masked PC-ID.

7.4 Config File

User download config file for clients id and save from Vcrypt multimedia encryptor. User can download the file from website/server of vcrypt system. In config form User click on file location where he want save the file and enter the file name and click on save .

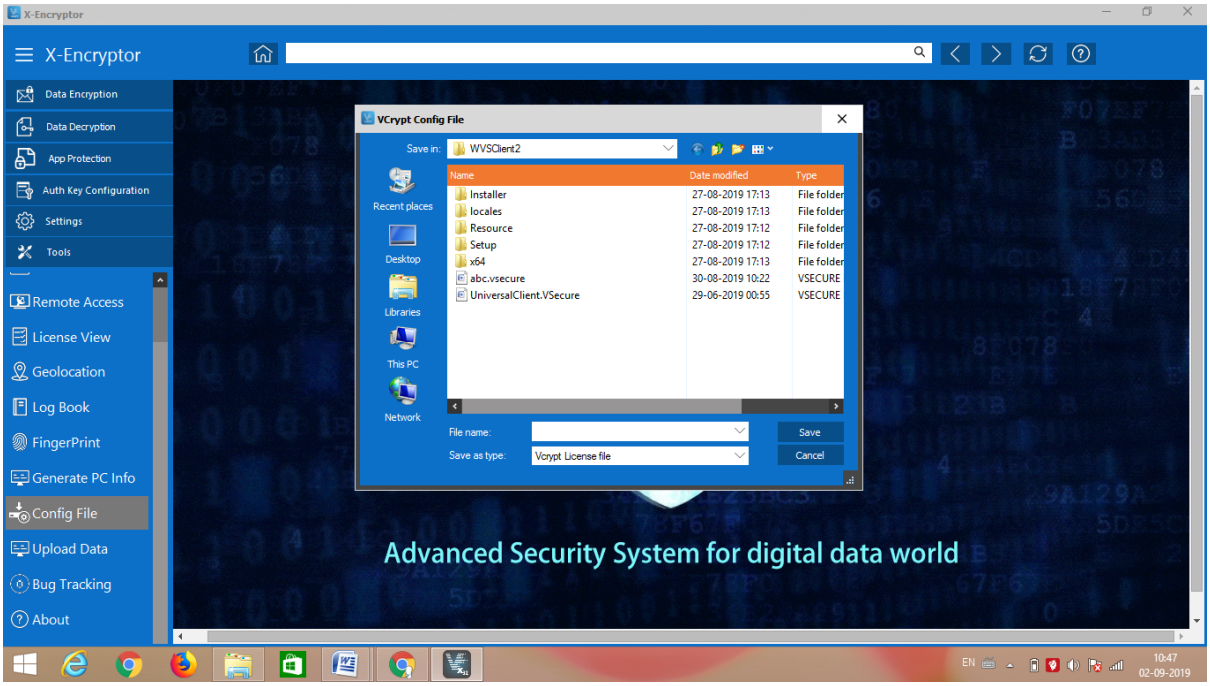

Figure 54 Config. File download

7.5 Upload Data

Uploading means data is being sent from your computer to the Internet. If clients want upload a document/project file/data to then fill data details and upload data.

7.6 Bug Tracking

A bug tracking system or defect tracking system is a software application that keeps track of reported software bugs in software development projects. It may be regarded as a type of issue tracking system.

Bug tracking is the process of capturing, **reporting**, and managing data on **bugs** that occur in software (also called errors and exceptions).

If Users found any bug in application system, then he report anytime/anywhere for bug error. Users fill up bug application form and submit.

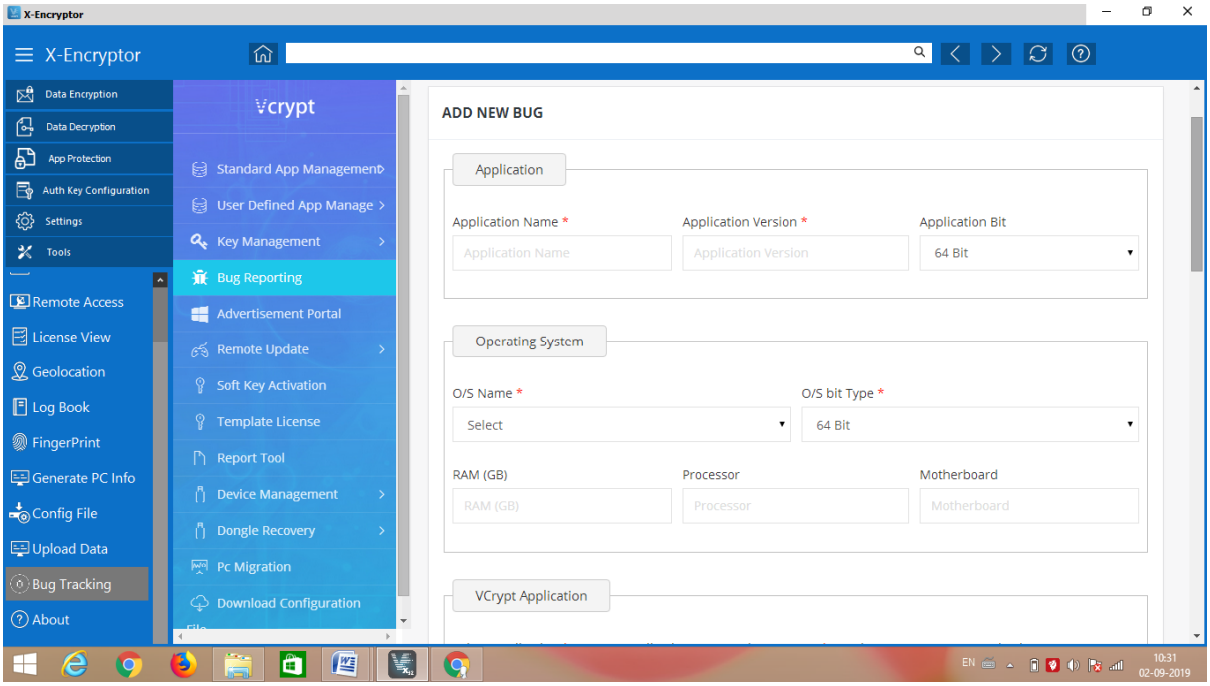

Figure 55 Bug Tracking

7.7 About Us

In about session shown the details of User PC properties. In about session show User PC-Id, product name ,product version and product license status.

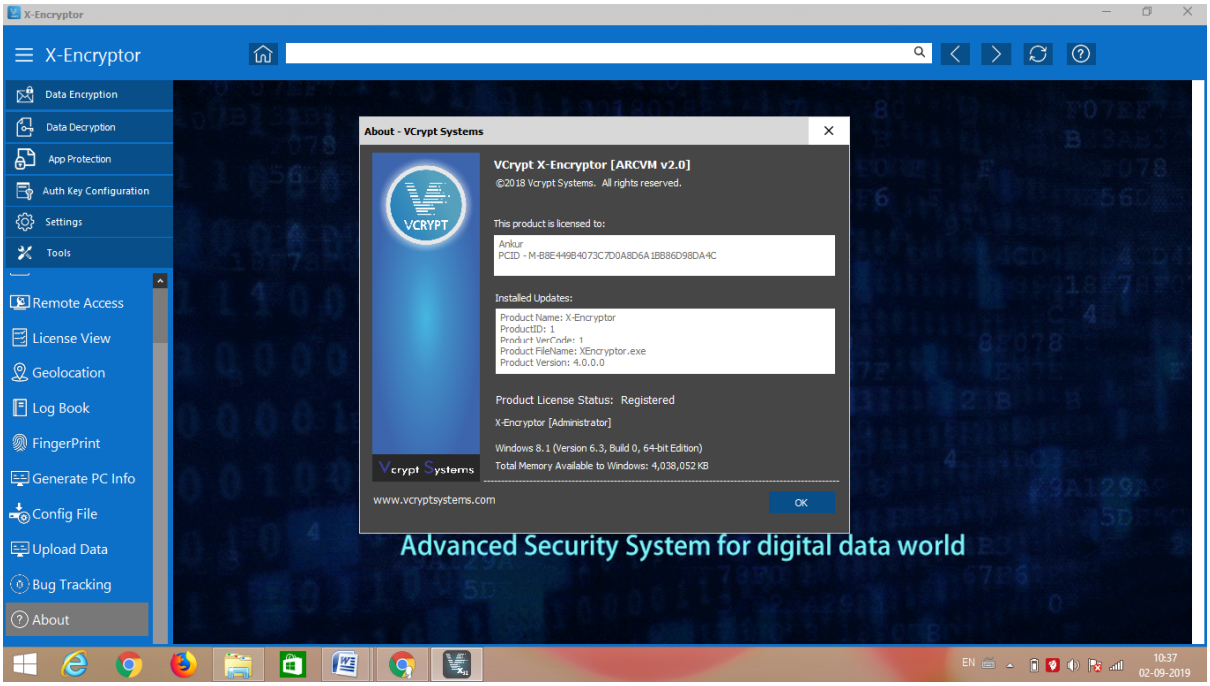

Figure 56 About

8. Application Launcher

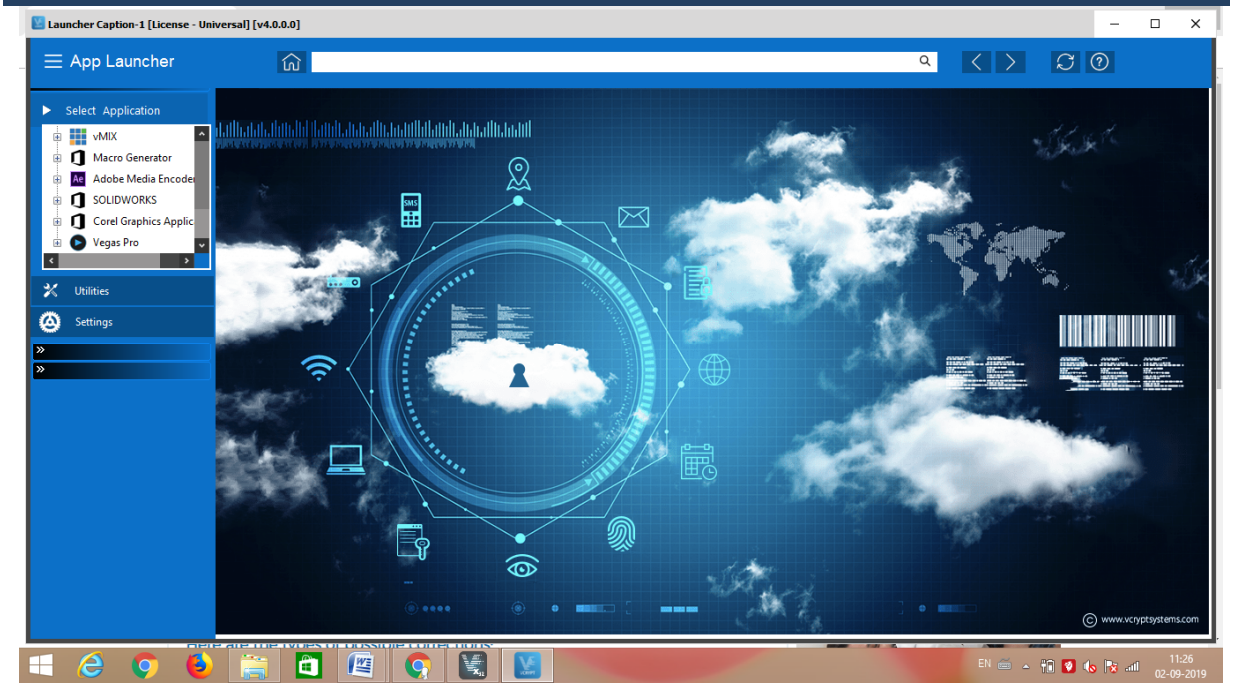

Figure 57 Application Launcher

An **application launcher** is a computer program that helps a user to locate and start other computer programs. An application launcher provides shortcuts to computer programs, and stores the shortcuts in one place so they are easier to find.

To access **Launcher** application, user needs to click on the **Launcher app icon** on Desktop screen. On successful login, user will be redirected to the homepage of application.

In application launcher, user select an application which want run to desktop.

9. Utilities under App Launcher

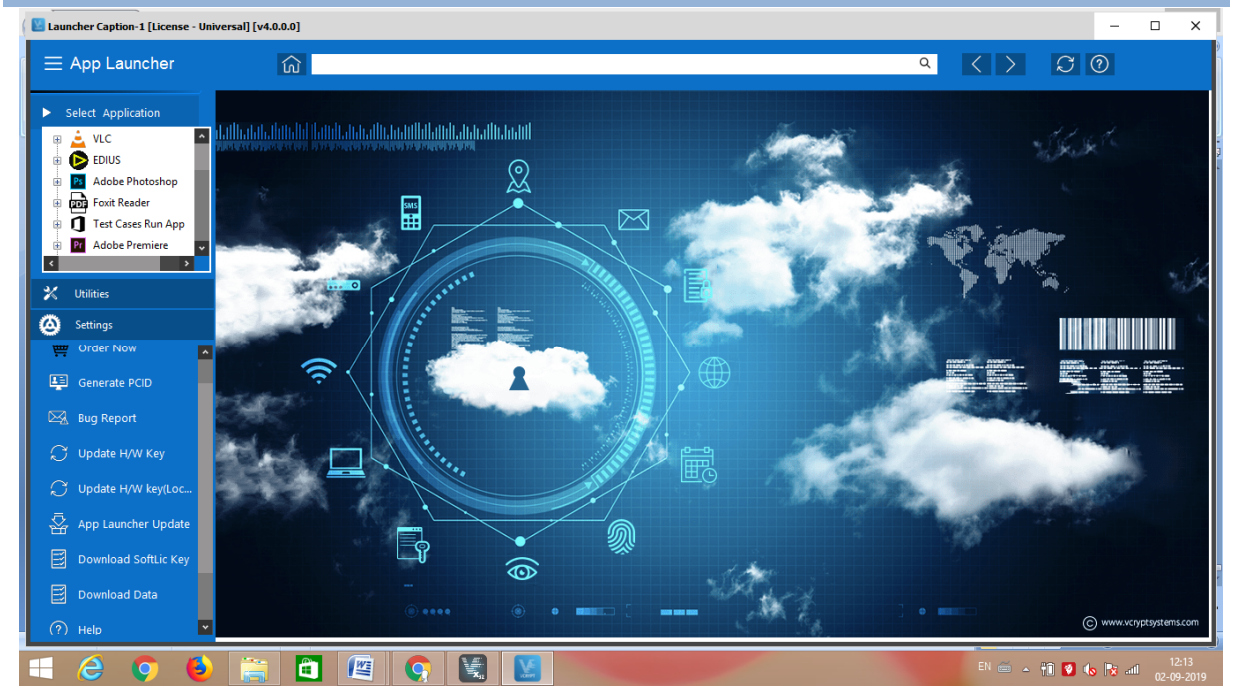

Figure 58 Utilities under app launcher

9.1 Order Now

In order now section User buy application under Package or domains section.

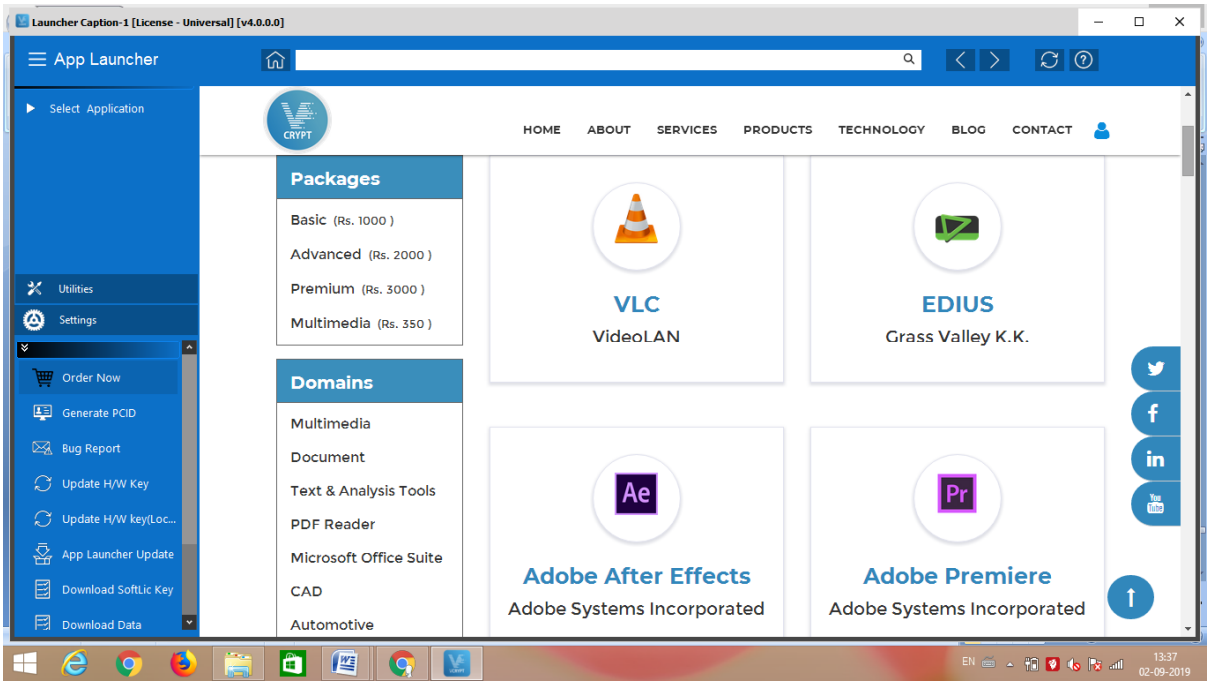

Figure 59 Order Now

9.2 GENERATE PC-ID

Users can generated PC-Info. This section provides detailed information about the PC or device on which VCrypt System application is running.

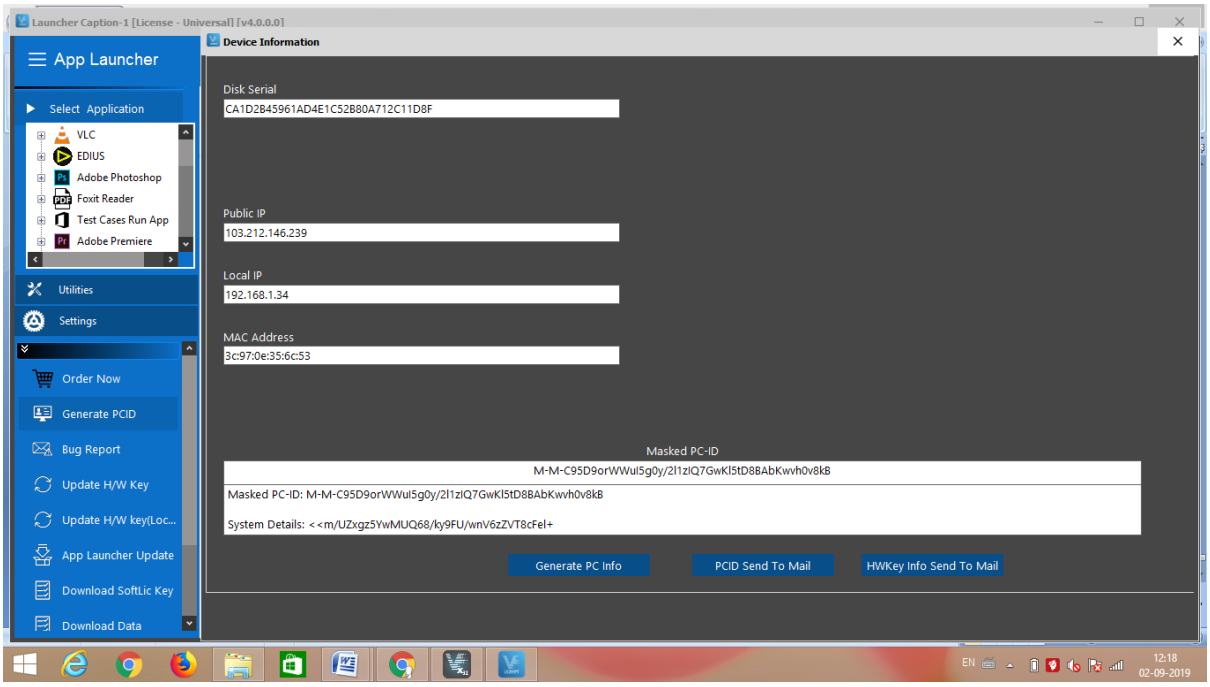

Figure 60 Generate PC-ID

9.3 BUG REPORT

A **bug** is an error, flaw, failure, or fault in a computer program or system that causes it to produce an incorrect or unexpected result or to behave in unintended ways.

If Users found any bug in application system, then he report anytime/anywhere report for bug error. Users fill up bug application form and submit.

9.4 UPDATE H/W KEY

H/W keys can be updated remotely using the built-in Remote Management tool

9.5 UPDATE H/W KEY LOCAL

When h/w key not updated from server then update h/w key through local file. In this section user open the local file situation and update h/w key.

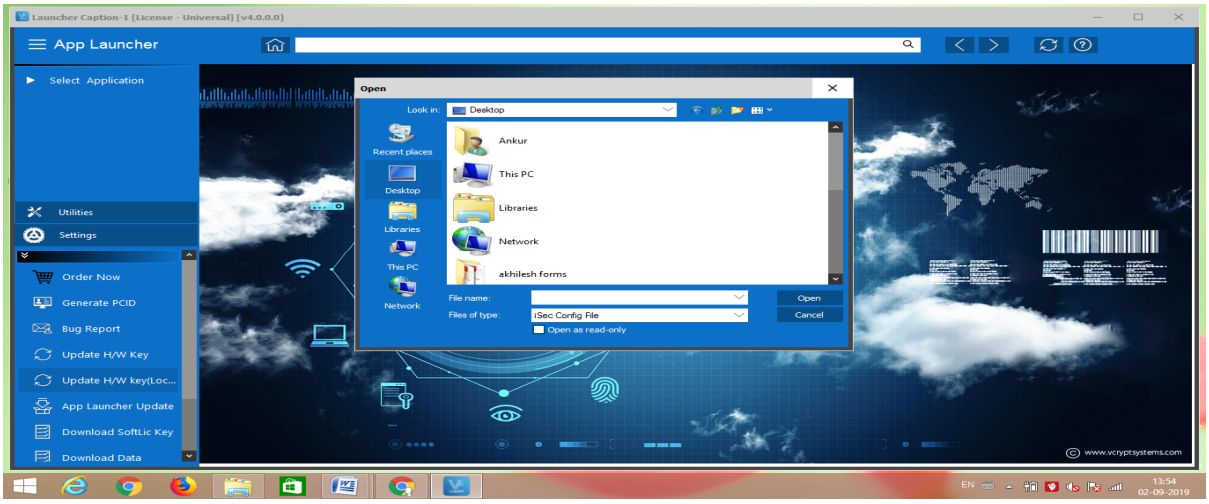

Figure 61 Update H/W key local

9.6 App Launcher Update

App launcher will be auto update at whenever the latest versions are available.

9.7Download Soft License Key

If users delete/not found/forget soft license key then download soft license key through app launcher via utilities.

9.8 Download Data

JSON stands for JavaScript Object Notation. **JSON** is a lightweight format for storing and transporting data. **JSON** is often used when data is sent from a server to a web page.**JSON** is "self-describing" and easy to understand.

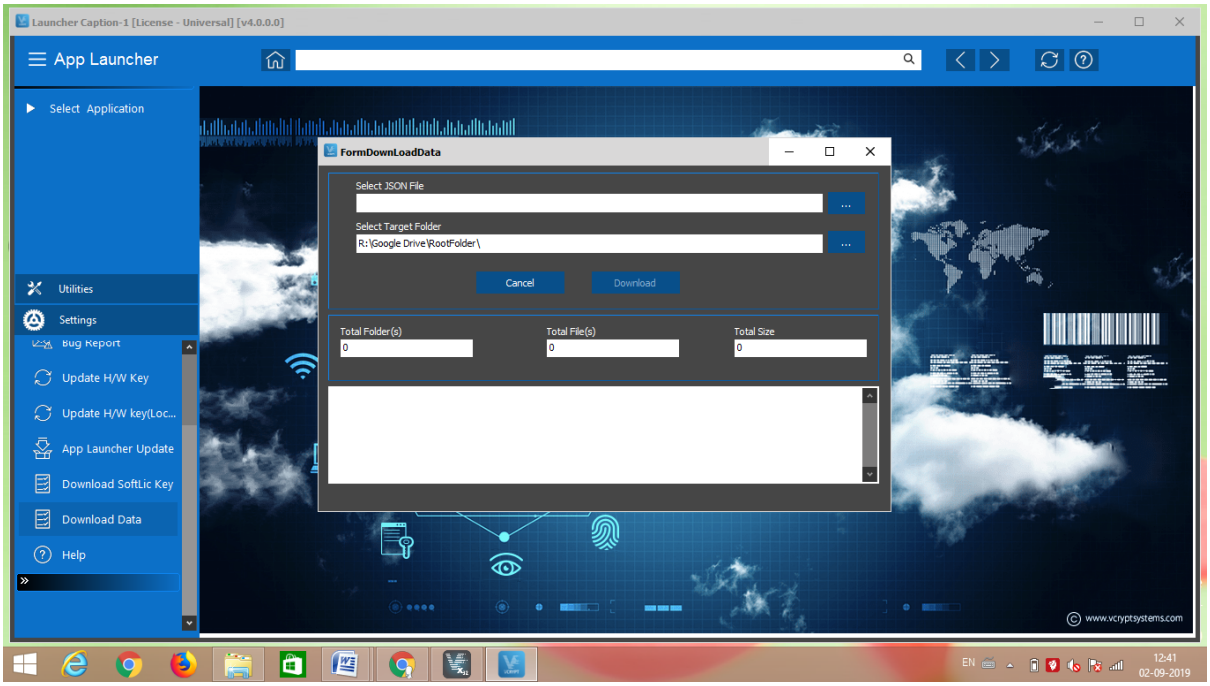

Figure 62 Download data

10. Settings

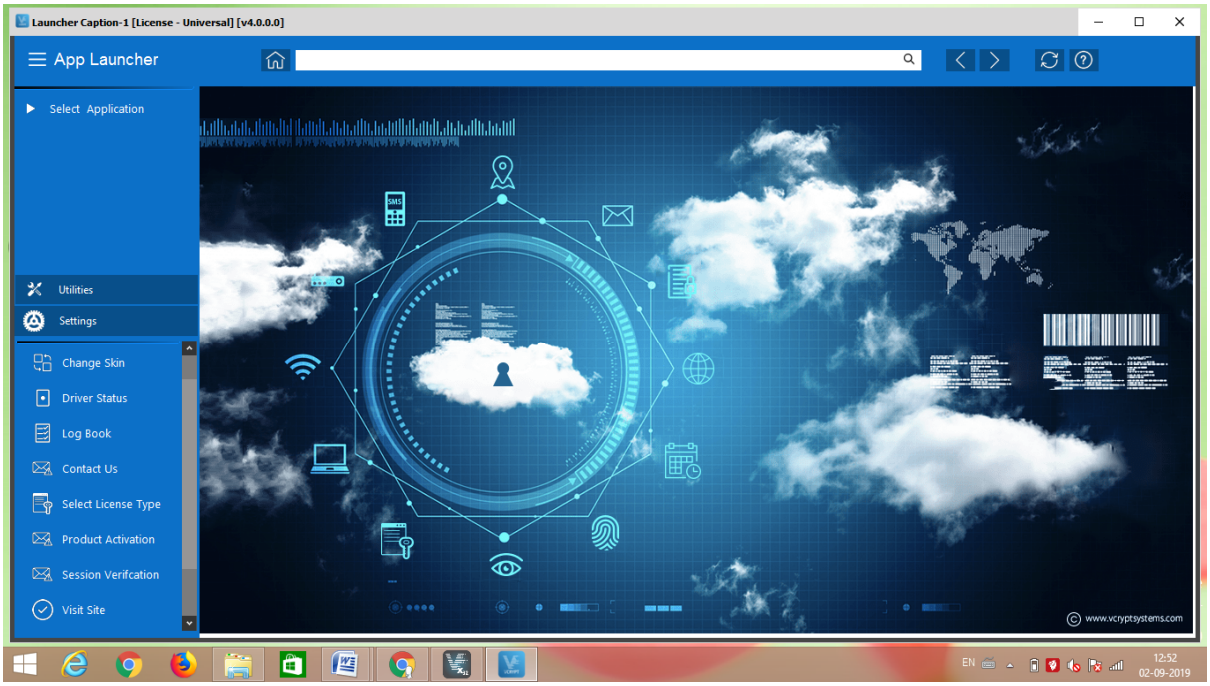

Figure 63 Settings functionality App Launcher

10.1 Change Skin

If user want change the theme from launcher home page then change the theme from change skin option. There are many theme, user select one theme and click on the apply button.

10.2 Log Book

A log book is a book in which someone records details and events relating to something.

10.3 Contact Us

If Users have a any query/problem then contact through mobile number and email-id. Users send a message through fill up form.

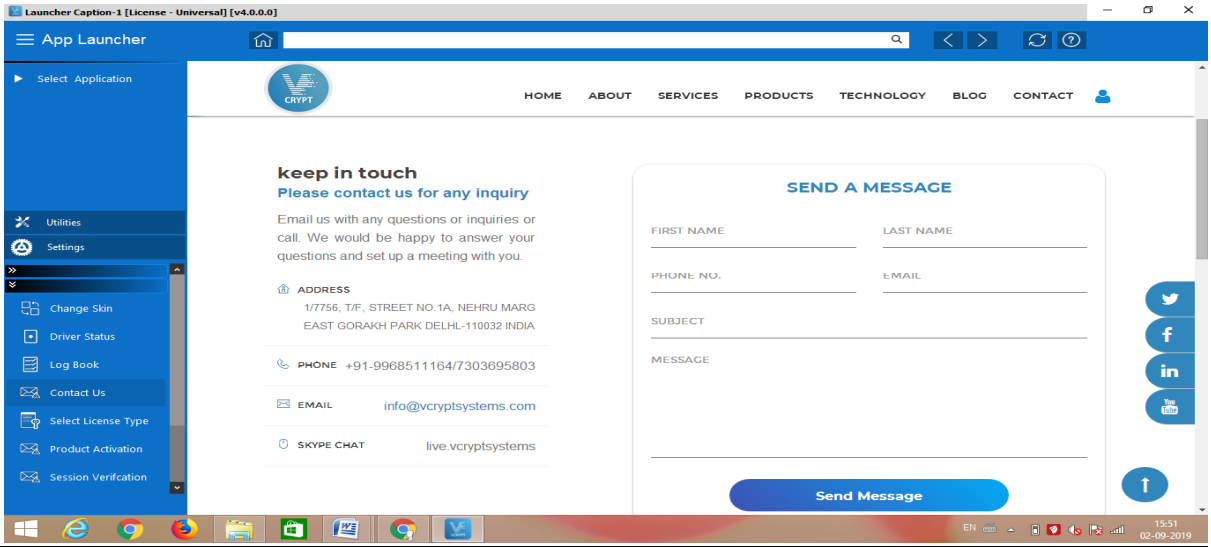

Figure 64 Contact Us

10.4 Select License Type

Users select license type. There are three type of license type:- Universal license, Dongle license and soft key license.

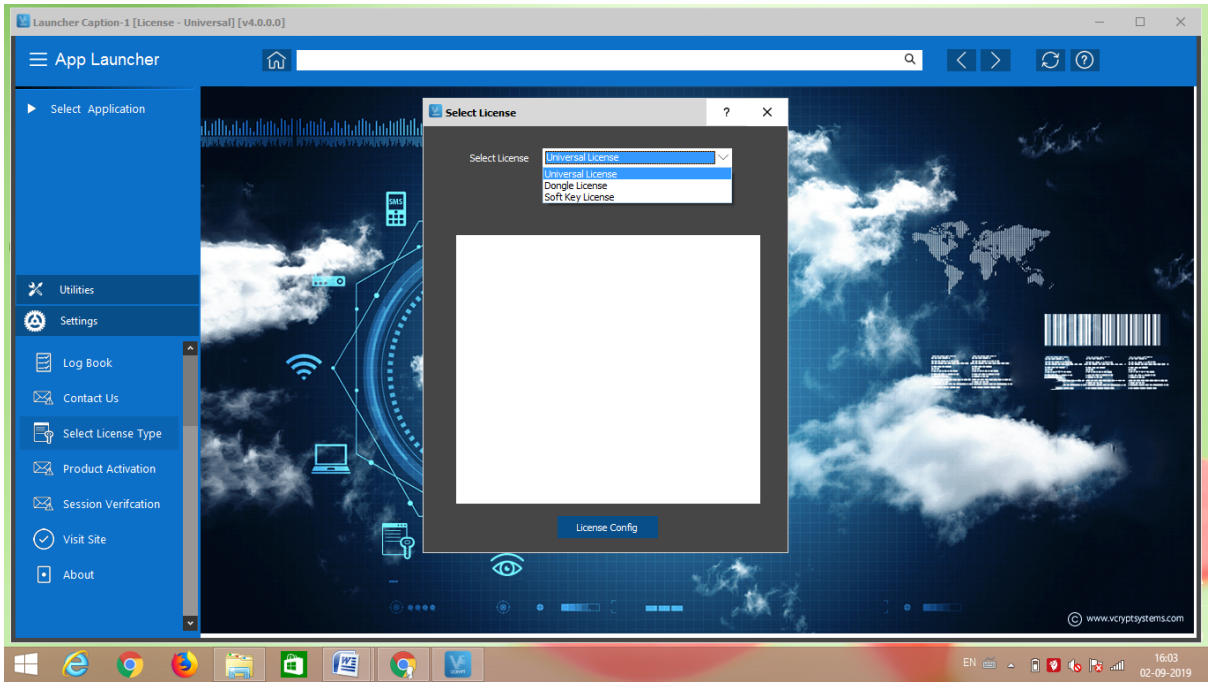

Figure 65 select license type

10.5 Product Activation

Enter the serial key Users activation license key.

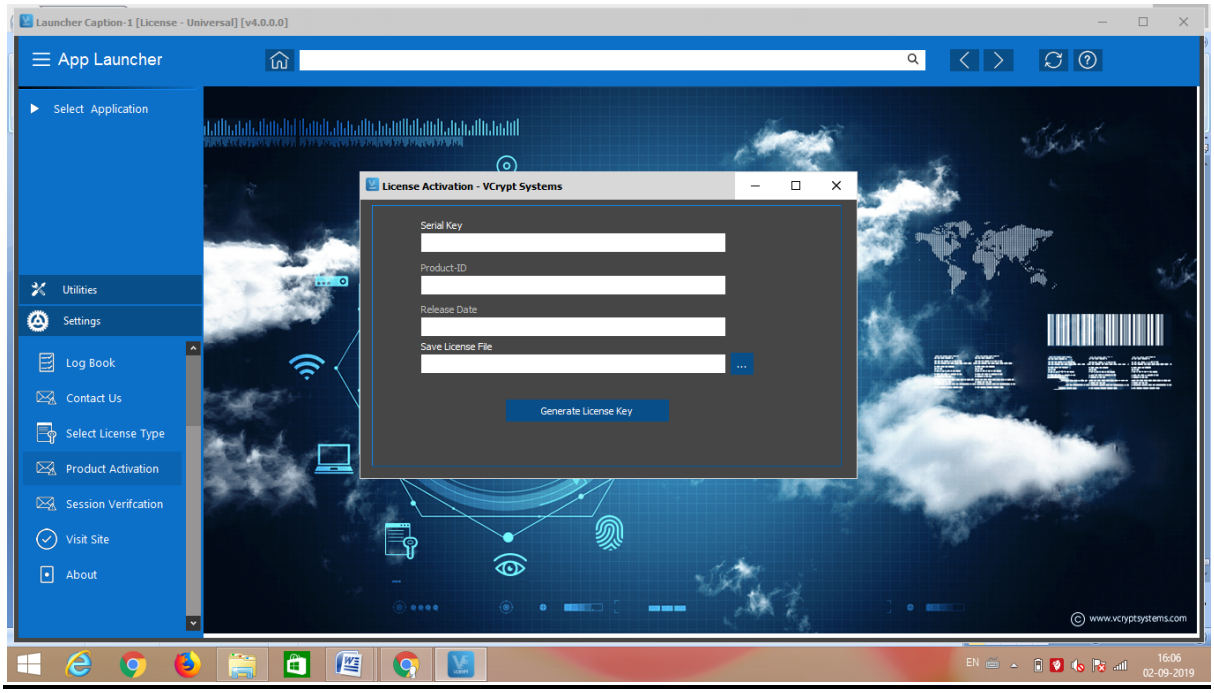

Figure 66 Product Activation

10.6 Visit Site

Users visit site to https://vcryptsystems.com/ for buy a product and details of company.

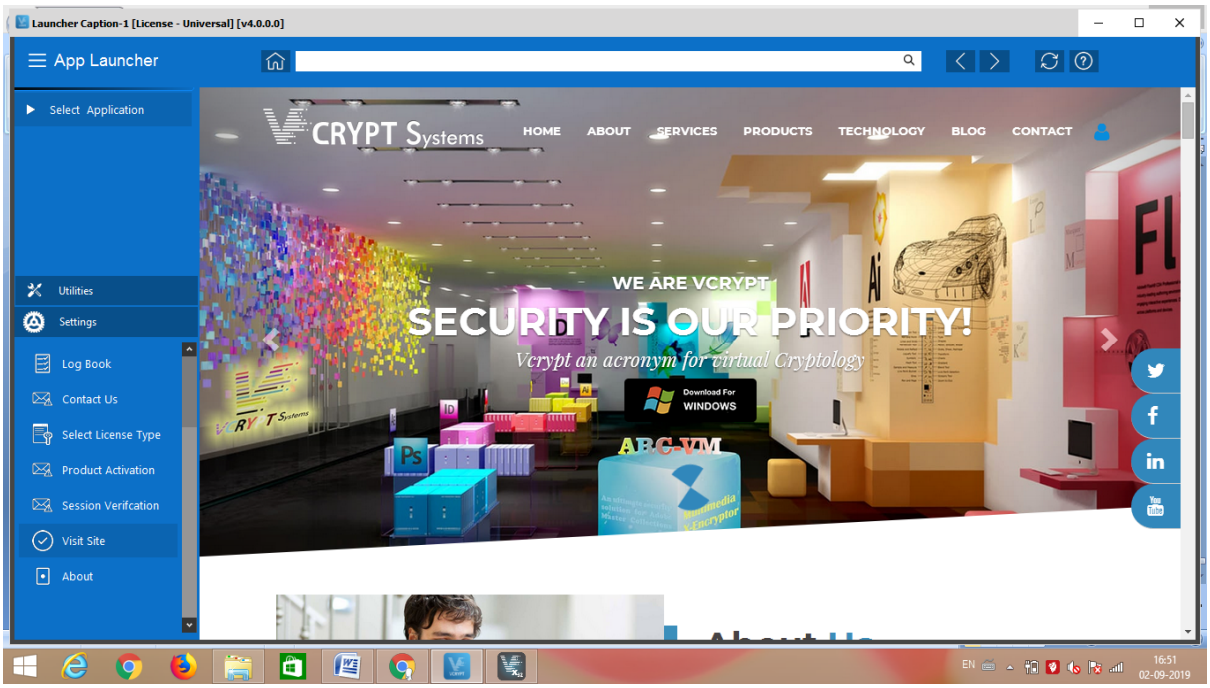

Figure 67 Visit Site

10.7 About

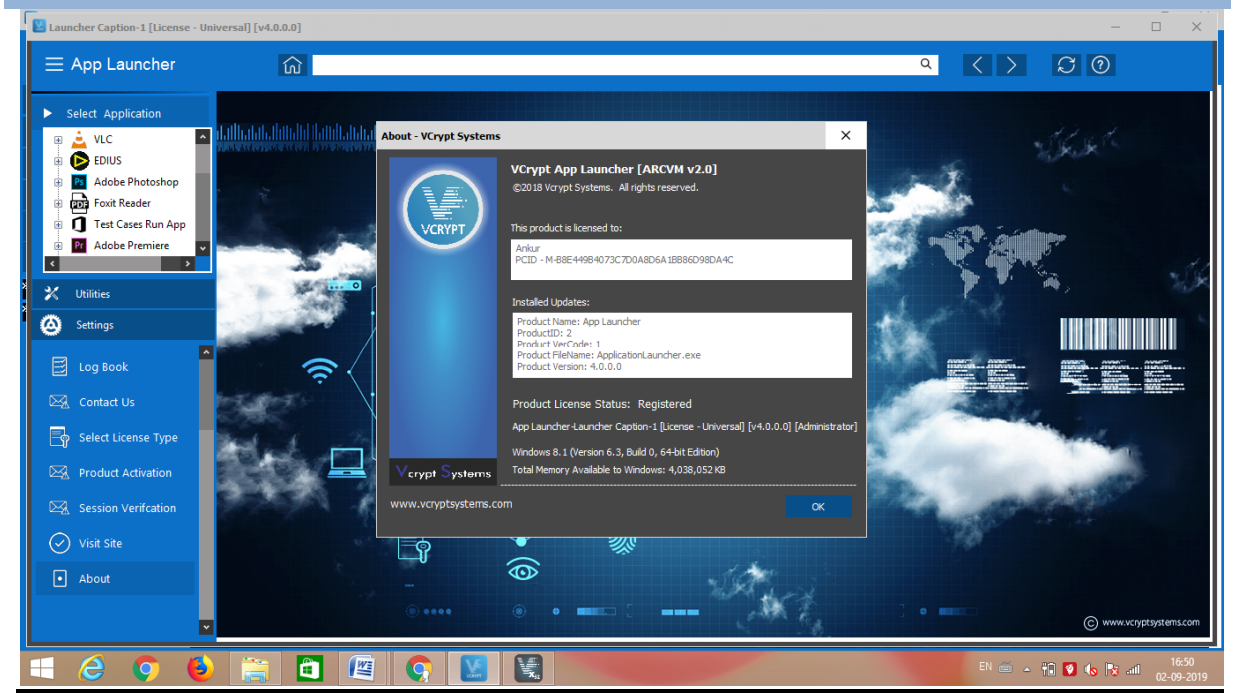

Figure 68 About