EPI INFO™ WEB SECURITY UTILITY HELP DOCUMENT

Version 1.0

02/10/2016

VERSION HISTORY

Version #	Implemented By	Revision Date	Reason
1.0	Mohammed Lamtahri	2/9/2016	Version 1.0 of the document
1.0	Sachin Agnihotri	2/10/2016	Version 1.0 review and updates
1.0	Sachin Agnihotri	8/26/2016	Version 1.0 screen updates

TABLE OF CONTENTS

1 INTRODUCTION

1.1 PURPOSE

The purpose of this document is to provide an overview of the key functionalities of the Epi Info™ Web Security Utility. This document is to be used during the deployment of any of the Epi Info Web Products namely Epi Info™ Web Survey (EIWS), Epi Info™ Web Enter (EWE) and Epi Info™ Web Analytics and Visualization (EWAV). This document goes hand in hand with deployment document for EIWS, EWE and EWAV. The configuration of web Products on the web server cannot be completed without this document.

1.2 OVERVIEW

The Epi Info™ Web Security Utility allows configuration of security keys used by cryptographic algorithm used by Epi Info™ Web Products. The web.config file provided in the Epi Info Web Products package is shipped with default security keys. It is highly recommended to update the default keys with new keys using the Epi Info™ Web Security Utility for enhanced security. The keys that are provided in the web.config file are provided below.

a. KeyForConnectionStringVector – This key corresponds to “Vector” field in Epi Info™ Web Security Utility. This key is applicable to all Epi Info Web Products.

b. KeyForConnectionStringPassphrase – This key corresponds to “Pass Phrase” field in Epi Info™ Web Security Utility. This key is applicable to all Epi Info™ Web Products.

c. KeyForConnectionStringSalt – This key corresponds to “Salt Value” field in Epi Info™ Web Security Utility. This key is applicable to all Epi Info™ Web Products.

d. KeyForUserPasswordSalt – This key corresponds to “Password Salt” field in Epi Info™ Web Security Utility. This key is applicable to EWAV and EWE product only.

In addition to being used by cryptographic algorithm these keys allow you to encrypt connection string and administration key (applicable to EIWS only) that are saved in web.config file.

Note: The screenshots provided in this document shows all four keys in the Epi Info™ Web Security Utility. When configuring Epi Info™ Web Survey product “Password Salt” key will not be available.

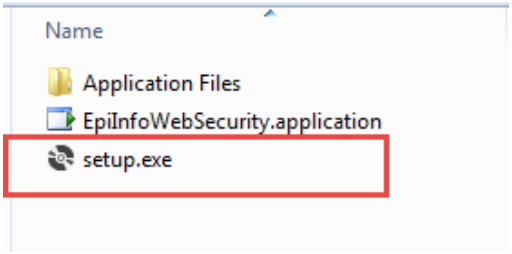
1.3 AUDIENCE

The audience for this document is an Administrator, a Manager or a person responsible for managing any Epi Info™ Web product on the web server.

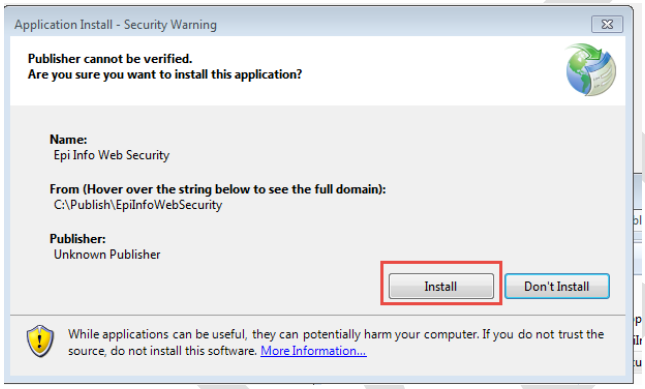
2 APPLICATION MANAGEMENT

2.1 INSTALLING

The installer for Epi Info™ Web Security Utility is provided inside the folder "EpiInfoWebSecurity". It can be installed on web server at the time of configuration of any Epi Info™ Web product using the provided "Setup.exe".



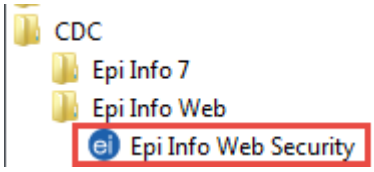
Click on "Setup.exe" and click on "Install" to install Epi Info™ Web Security Utility.



2.2 LAUNCHING

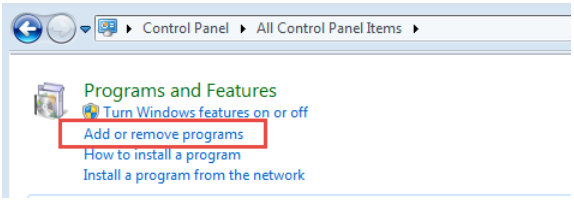
After installation you'll find a shortcut on desktop for "Epi Info Web Security". The Utility can be launched by clicking on the shortcut icon.

The "Epi Info Web Security" Utility can also be found in All Programs under a folder called "CDC/Epi Info Web"

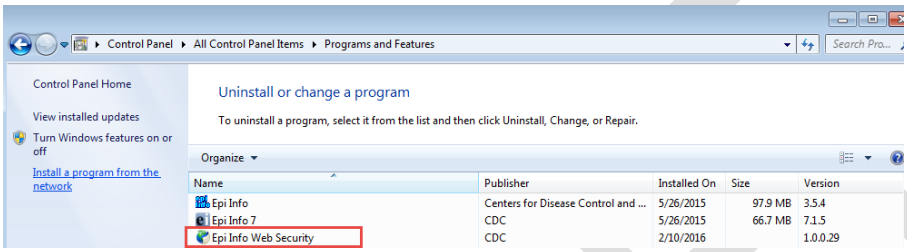


2.3 UNINSTALLING

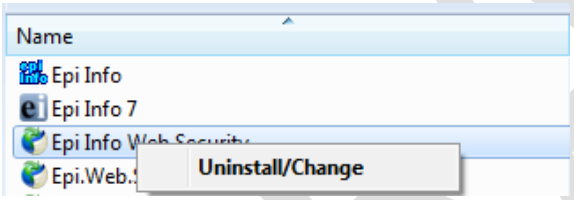
The Epi Info Web Security Utility can be uninstalled by using “Add or remove programs” feature.



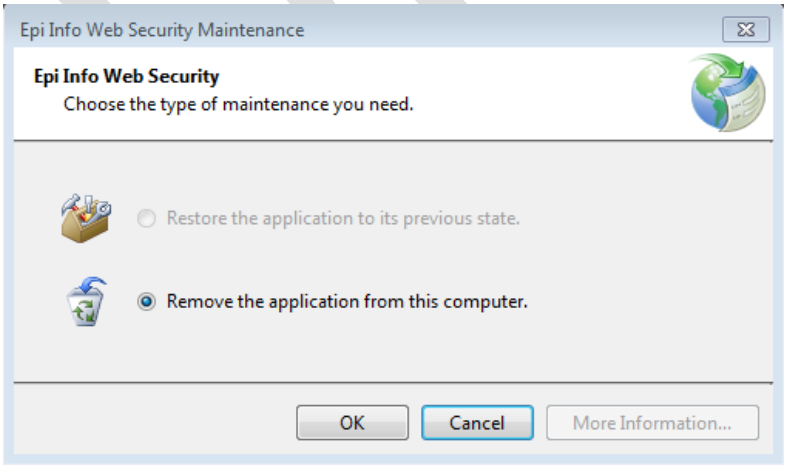
Locate Epi Info Web Security Utility in the list of installed programs



Uninstall by right clicking on Epi Info Web Security and clicking on “Uninstall/Change”



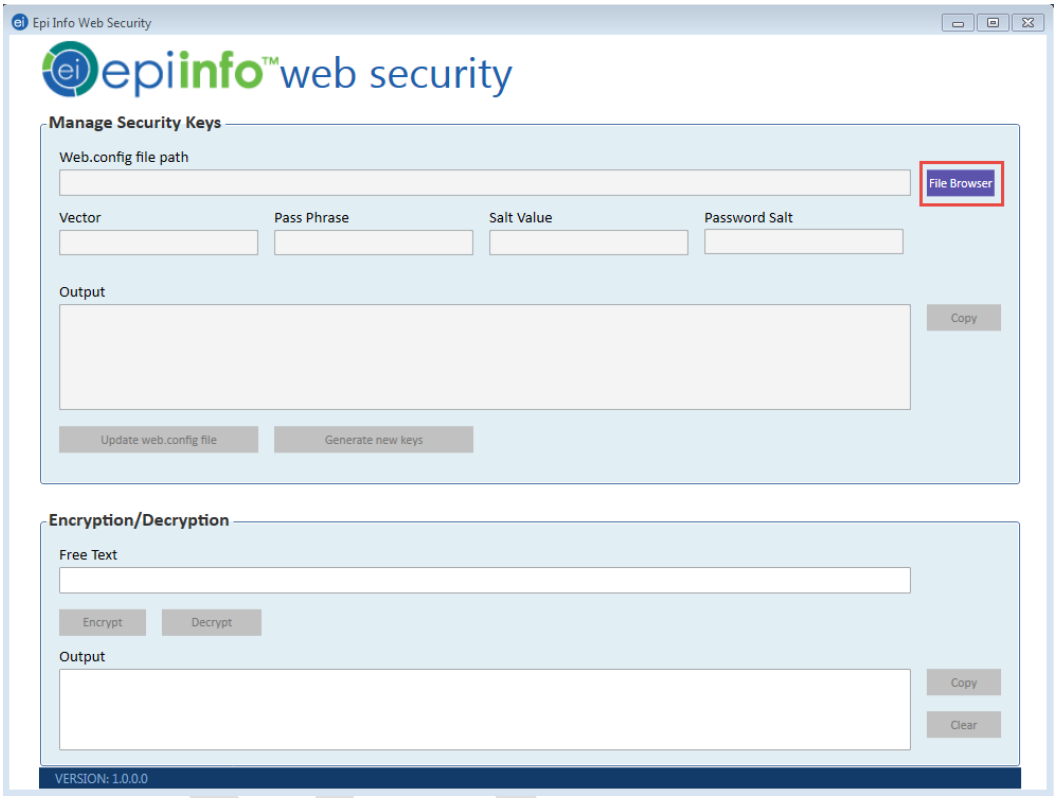
Optionally, you can double click on Epi Info Web Security which will launch the dialog to let you uninstall the application



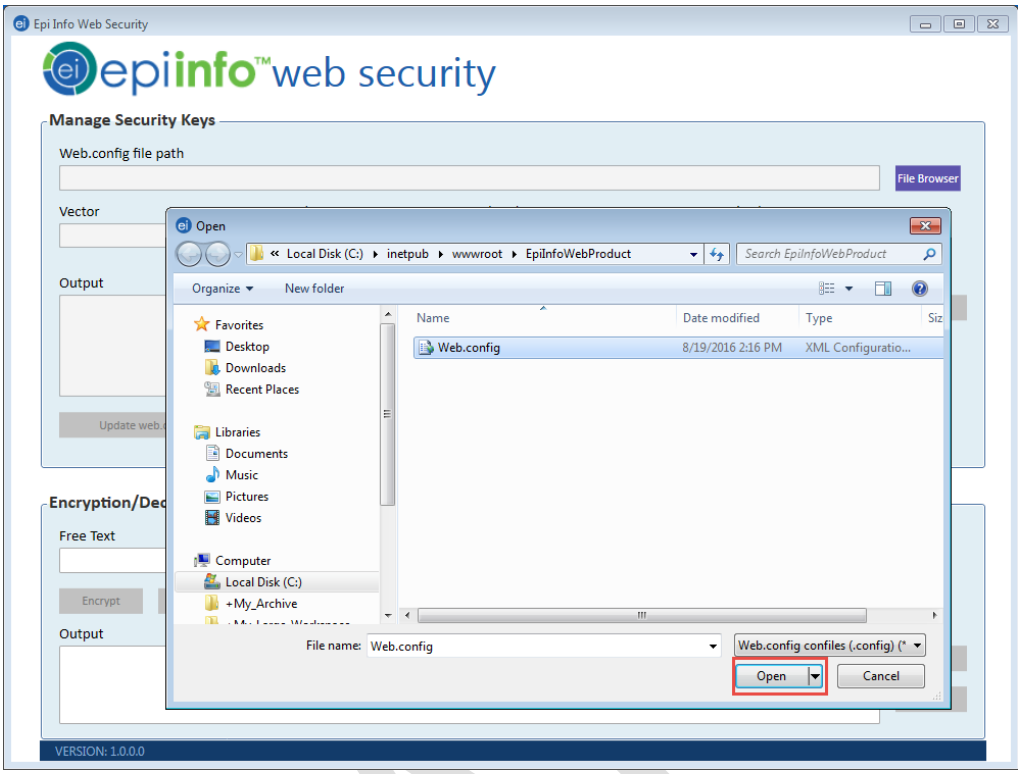
3 WORKFLOW 1 – CREATE KEYS FOR A NEW INSTALLATION

Perform following steps to create security keys for Epi Info™ Web Product being installed.

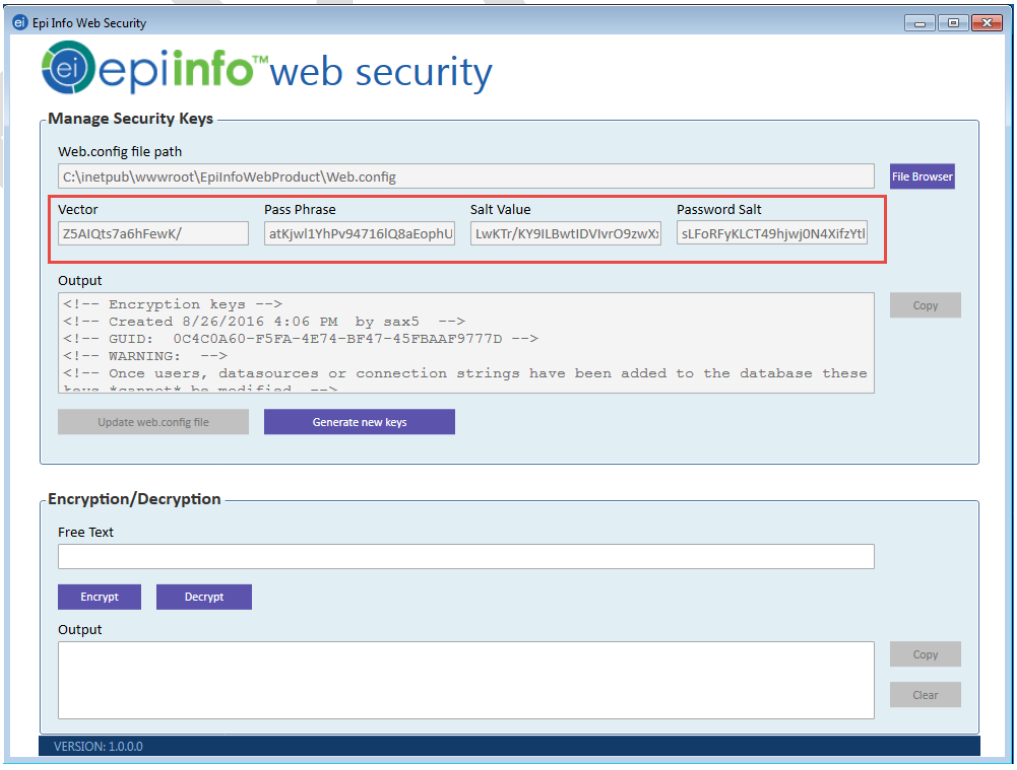
1. Click on “File Browser” button.



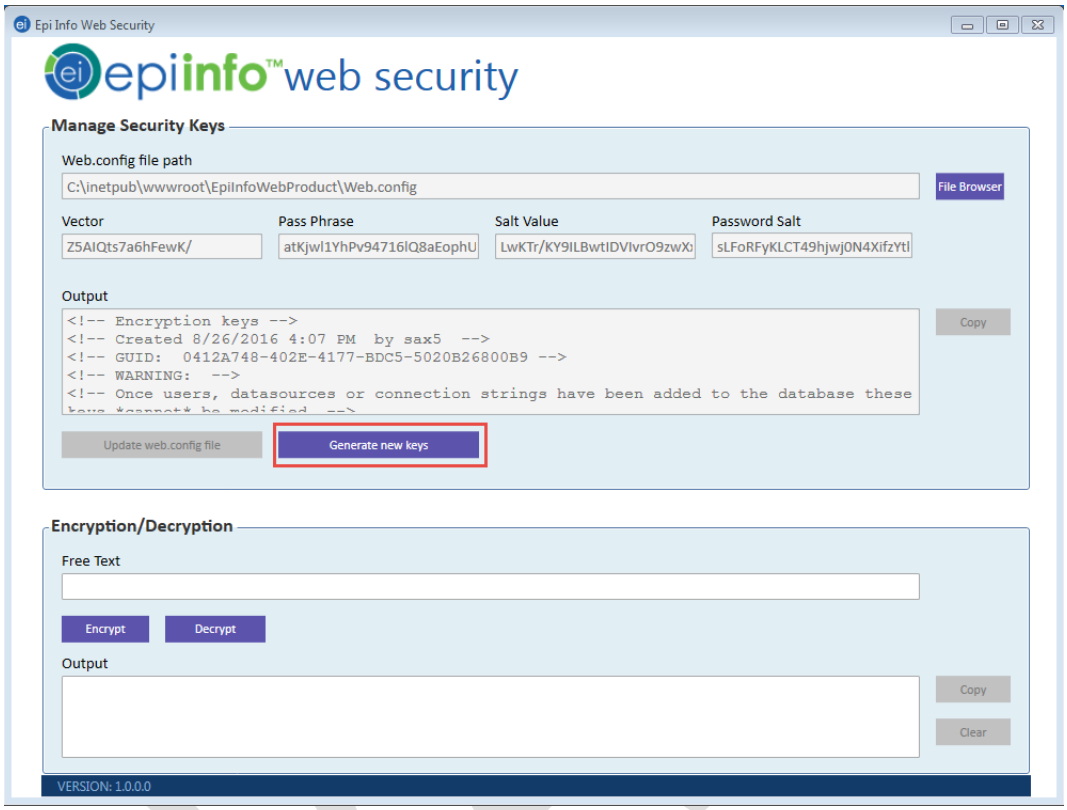
2. In the Open file dialog navigate to the location of web.config file which can be found under “intepub\wwwroot\<EpiInfoWebProduct>. <EpiInfoWebProduct> would be replaced by the name of the folder you have created for installing the Epi Info™ Web Product. Select web.config file and click open.



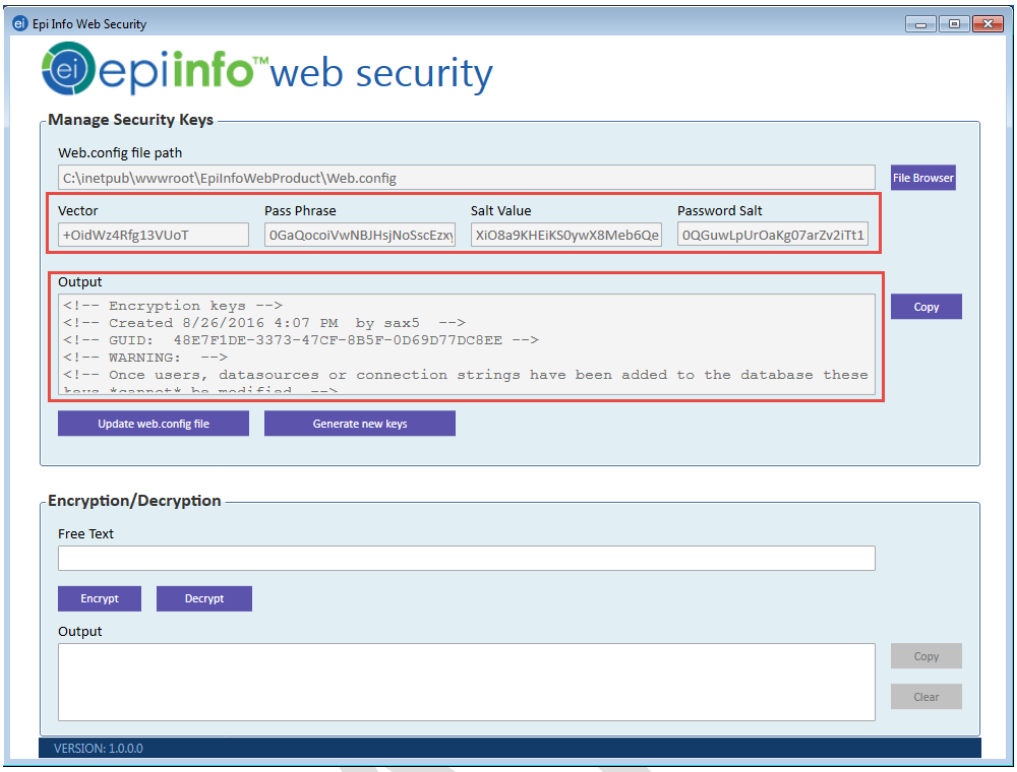
3. The Epi Info™ Web Security Utility displays the default security keys read from the web.config file in Manage Security Keys group and populated in Vector, Pass Phrase, Salt Value and Password Salt (not applicable to Epi Info Web Survey product) text box. The Output text box shows Encryption keys section as is present in the web.config file.



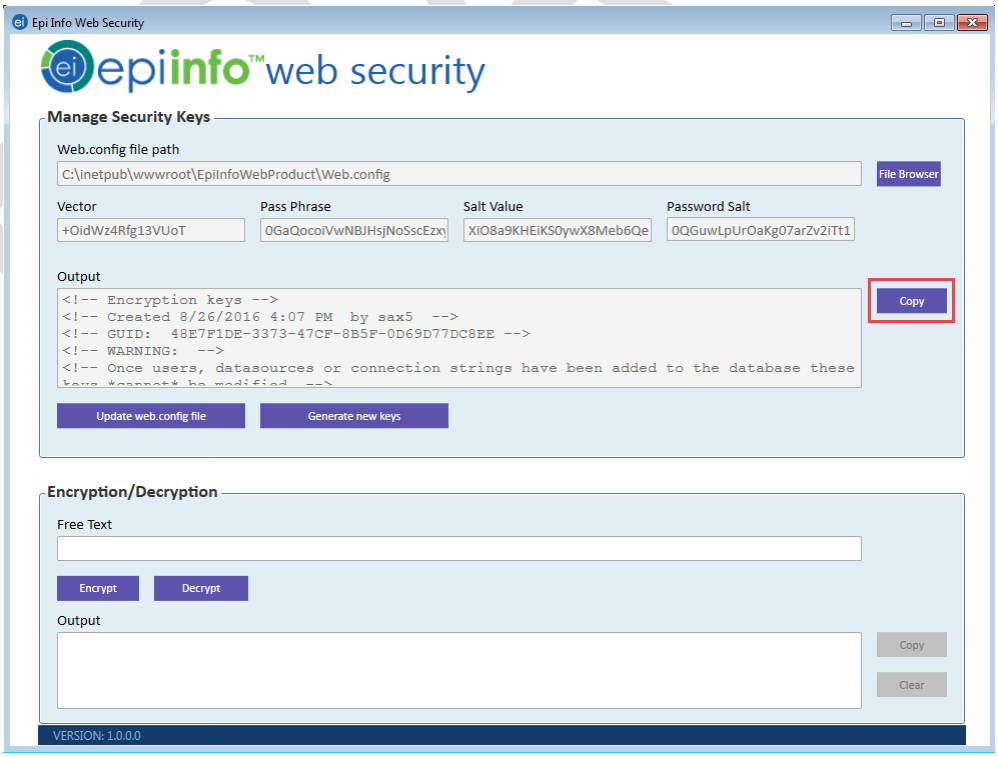
4. Click the “Generate new keys” button in Epi Info Web Security Utility to generate new security keys



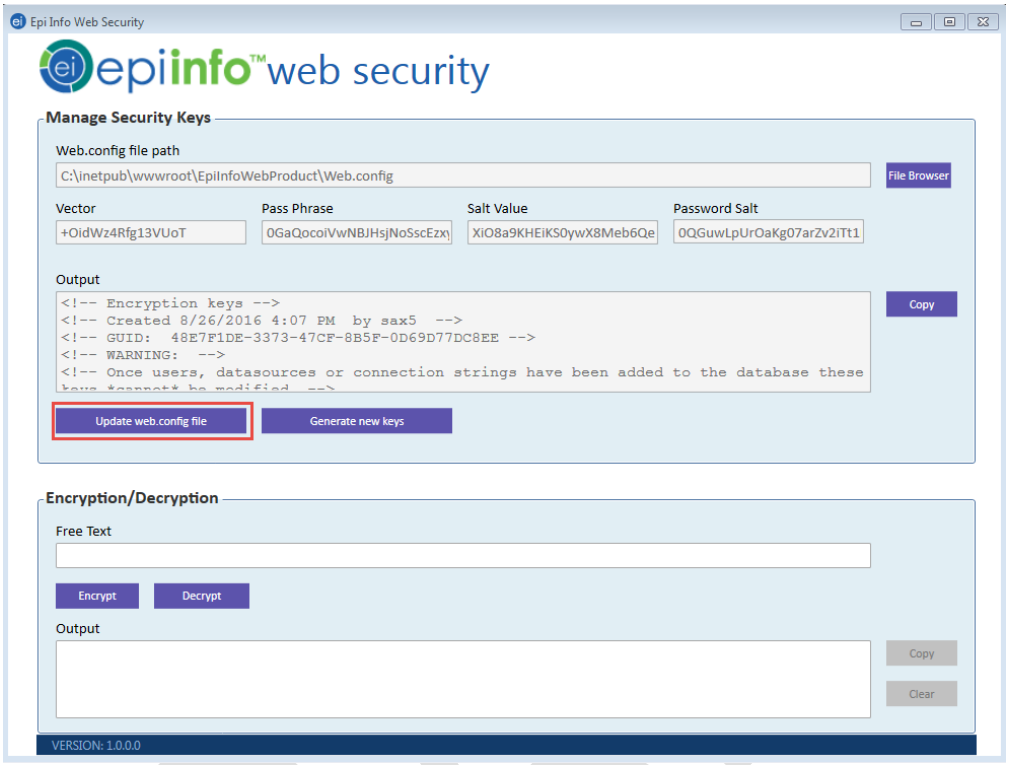
5. The new security keys are generated and displayed in text boxes for security keys. The Output text box has the content that needs to be persisted to web.config file in order to use the newly generated keys instead of the default keys.



6. Copy the newly created keys key by clicking on the Copy button and save it in document of your choice in a location of your choice as a backup in case the keys in web.config file are distorted for any reason.



7. Update the web.config file with the newly generated security keys by clicking on “Update web.config file” button. This action will change the security keys from the default keys provided with the package to the newly generated keys.

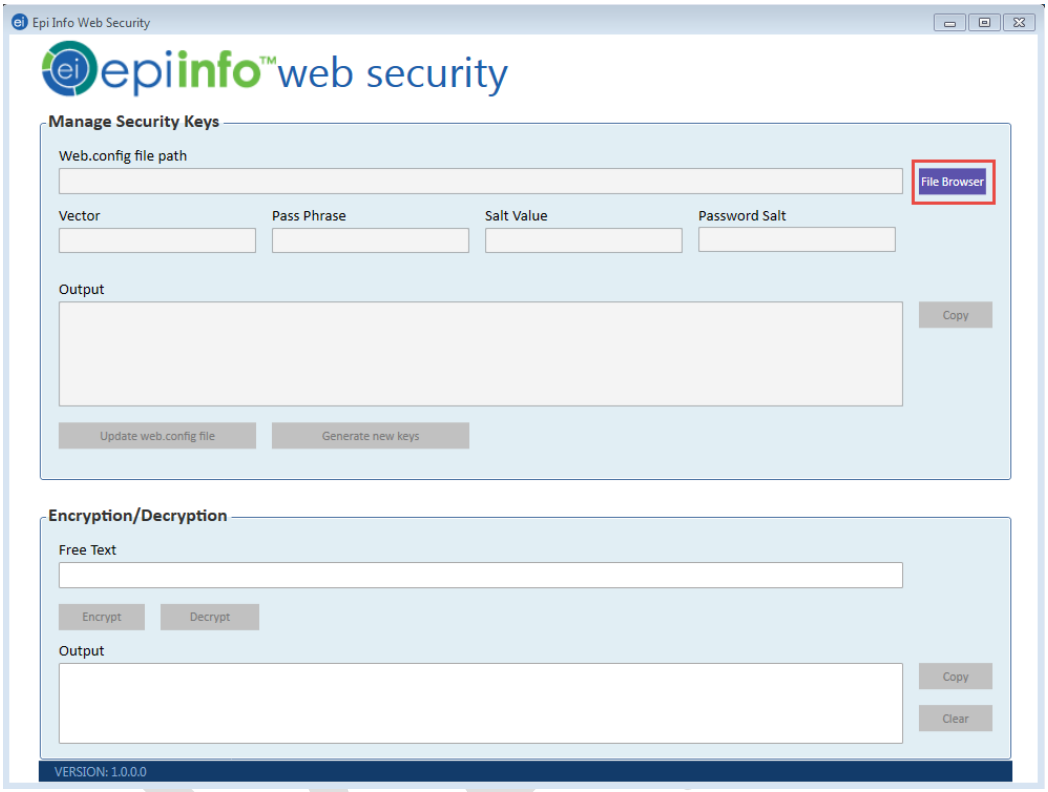


Note: This action should be performed only once during the life of the Epi Info Web product and at the time of initial configuration. Once the data is entered in the database through the application, altering this key will prevent the application from reading the save data.

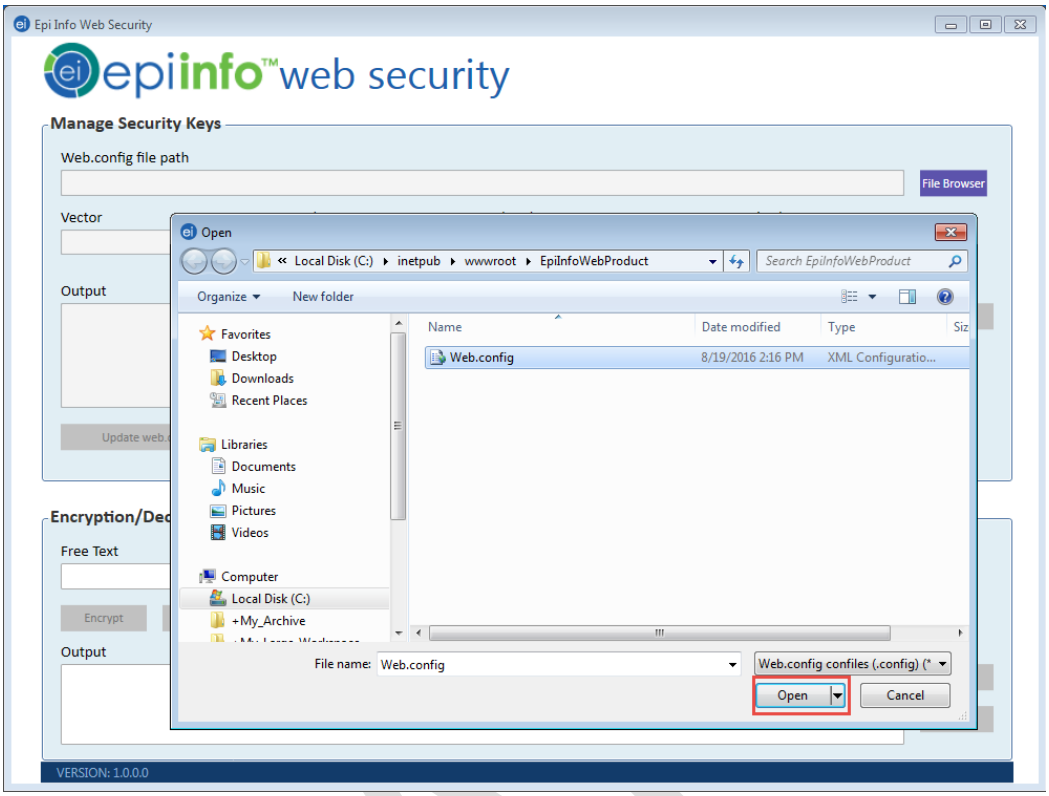
4 WORKFLOW 2 - LOAD KEYS FROM EXISTING WEB.CONFIG

Perform following steps to read security keys for the Epi Info web Product.

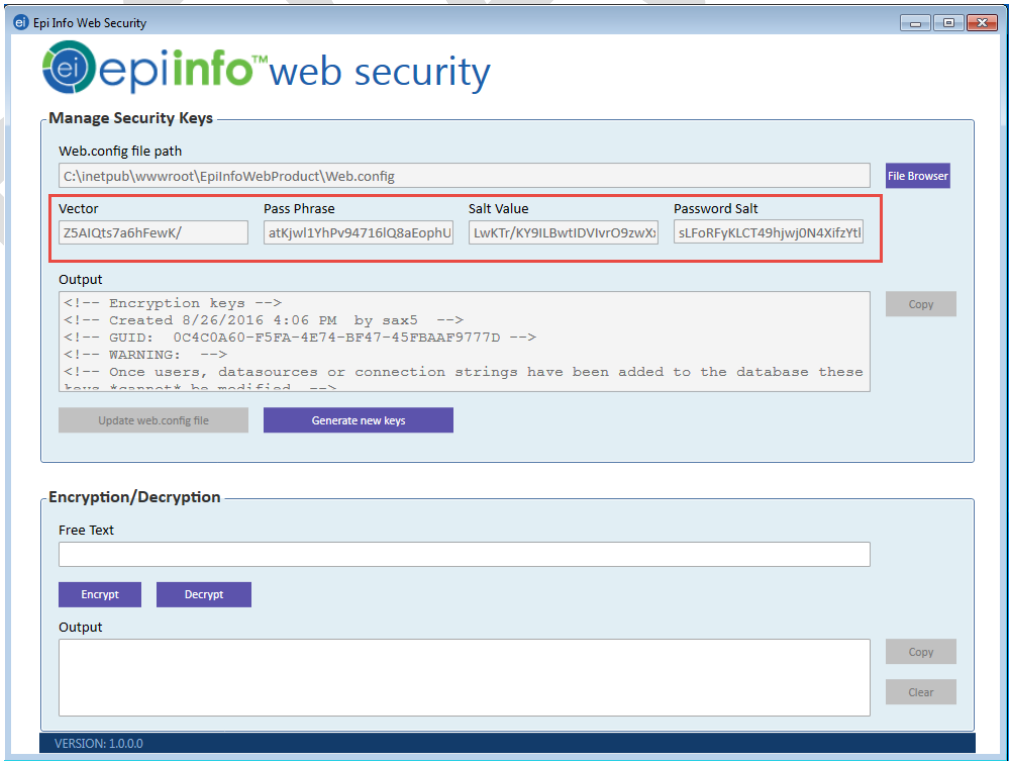
1. Click on “File Browser” button.



2. In the Open file dialog navigate to the location of web.config file which can be found under “intepub\wwwroot\<EpiInfoWebProduct>. <EpiInfoWebProduct> would be replaced by the name of the installed Epi Info Web Product. Select web.config file and click open.



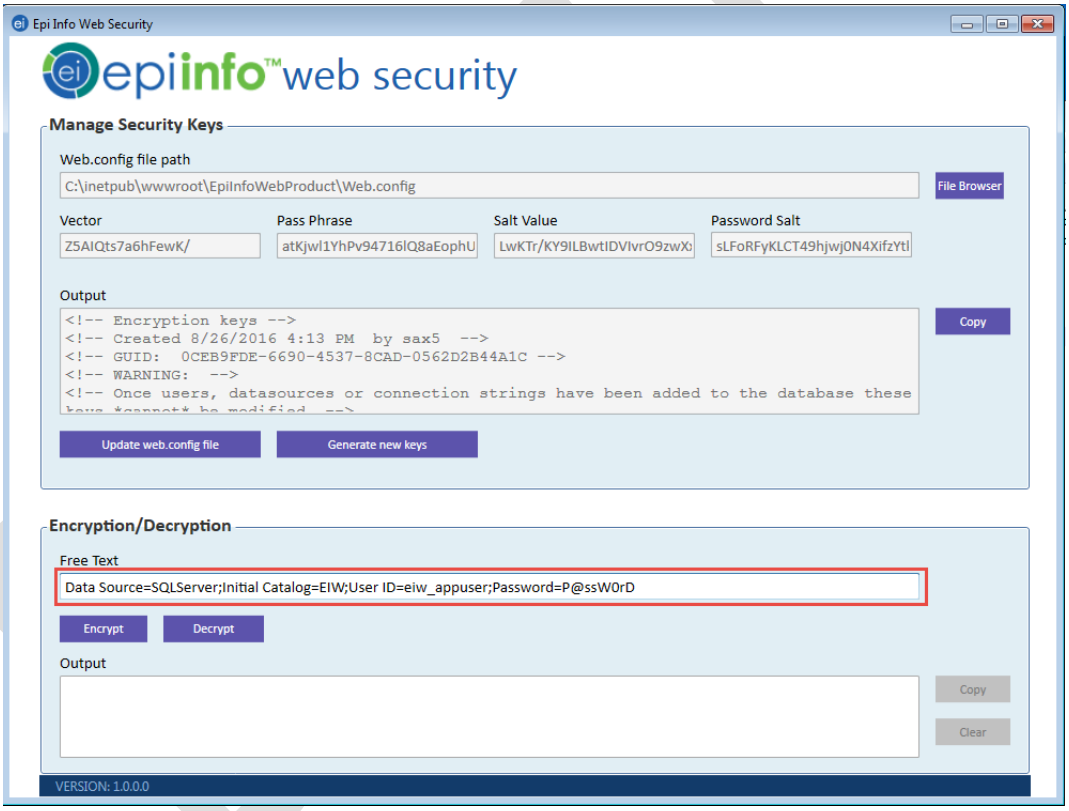
3. The Epi Info Web Security Utility will read the existing security keys from web.config file and populate them in Vector, Pass Phrase, Salt Value and Password Salt (not applicable to Epi Info Web Survey Product) text box.



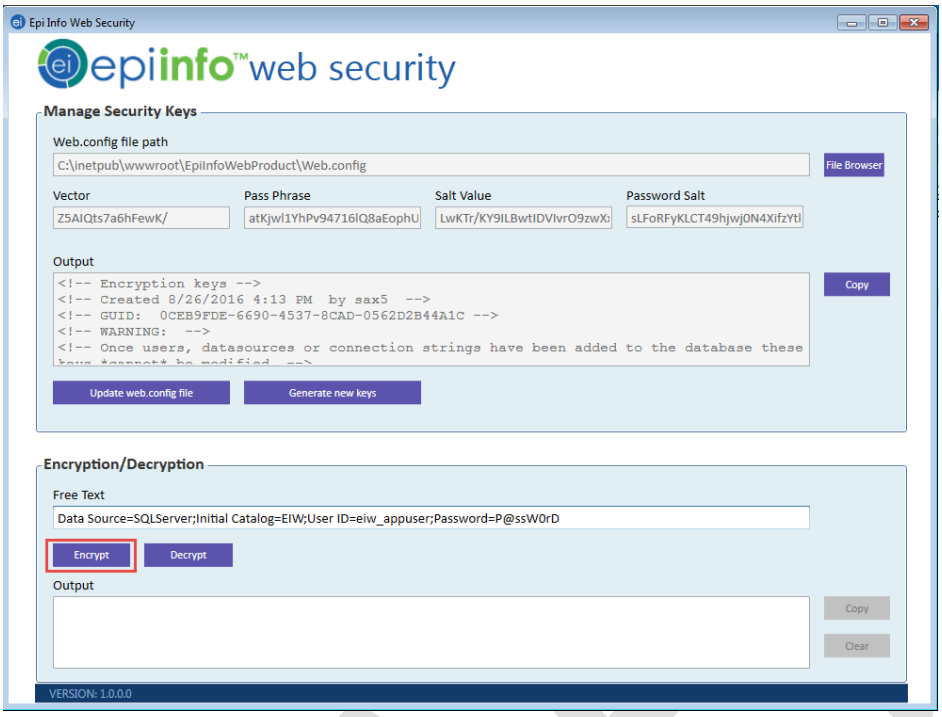
5 WORKFLOW 3 – AD-HOC ENCRYPT

This functionality is to be used to encrypt the database connection string for the database and/or administration key (applicable only to Epi Info Web Survey Product). The encrypted connection string and/or administration key can be used to update the sample encrypted connection string and/or administration key provided in the web.config file. The steps below shows how connection string can be encrypted. The exact connection string should be created using the structure specified in the Epi Info Web Product deployment document.

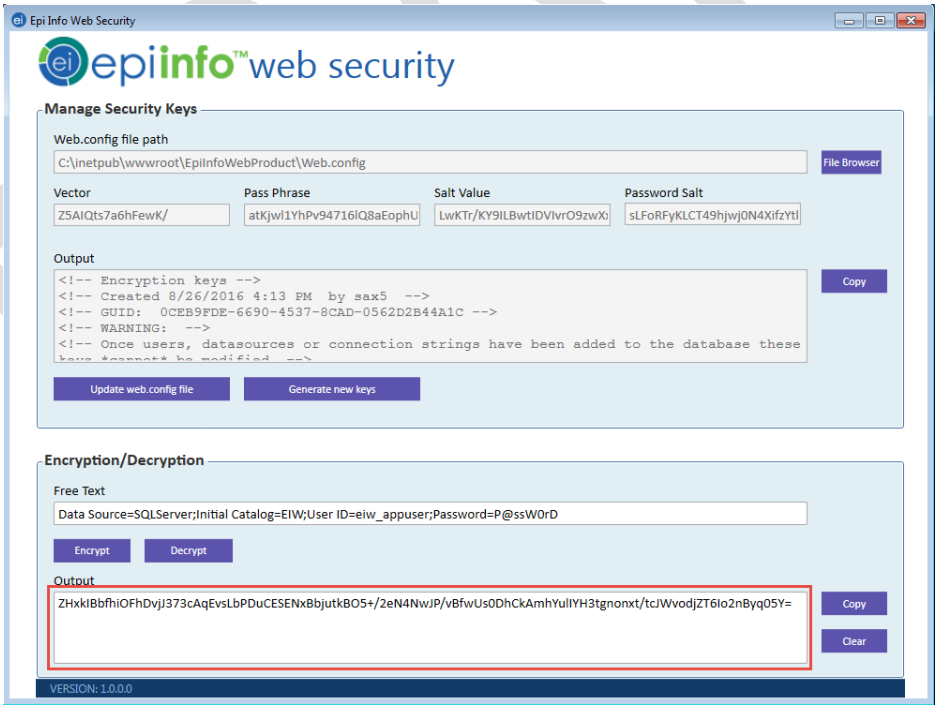
1. Follow steps of workflow 2
2. Paste an unencrypted string into the “Free text” text box



3. Click the “Encrypt” button



4. Use the Encrypted string provided in output textbox to update the relevant connection string in the web.config file.

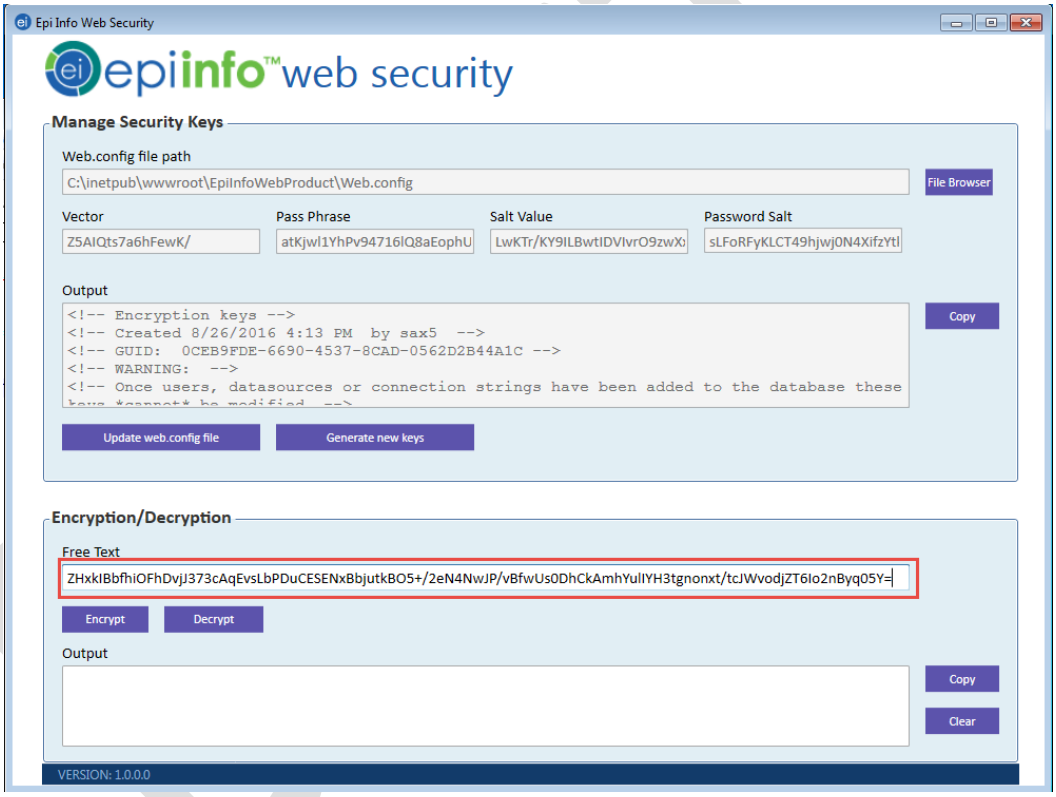


Note: The same workflow can be used to encrypt the Administration key by replacing the connection string with Admin Key.

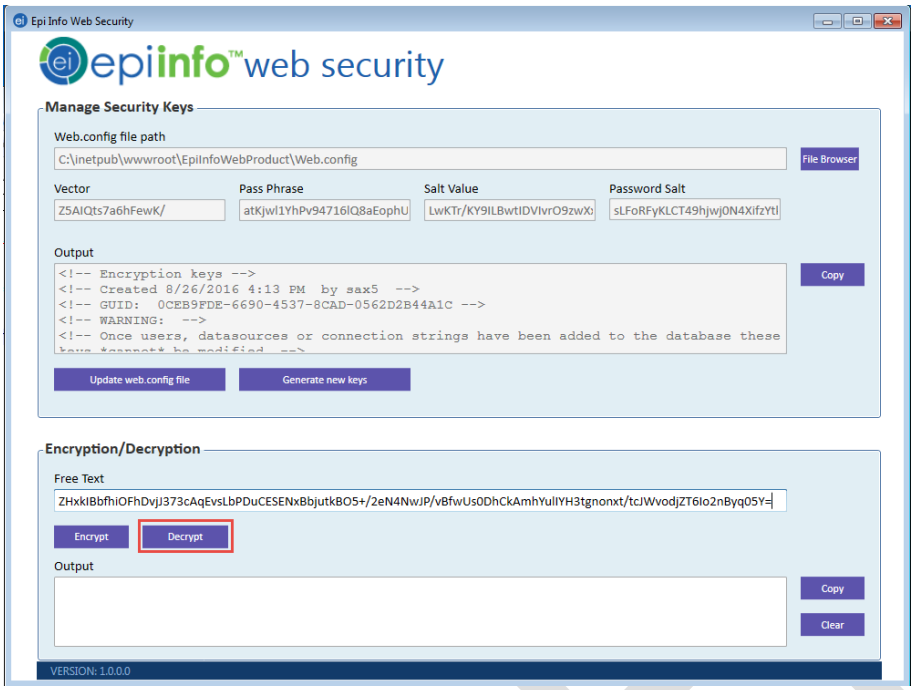
6 WORFLOW 4 - AD-HOC DECRYPT

This functionality can be used to decrypt the connection string or administration key (applicable only to Epi Info Web Survey product) present in the web.config file. Decrypting the connection string is needed in case the application is not able to connect to the database. When resolving connection issues the connection string can be inspected after decryption and updated as needed to resolve database connection problem. The steps below show how connection string can be decrypted.

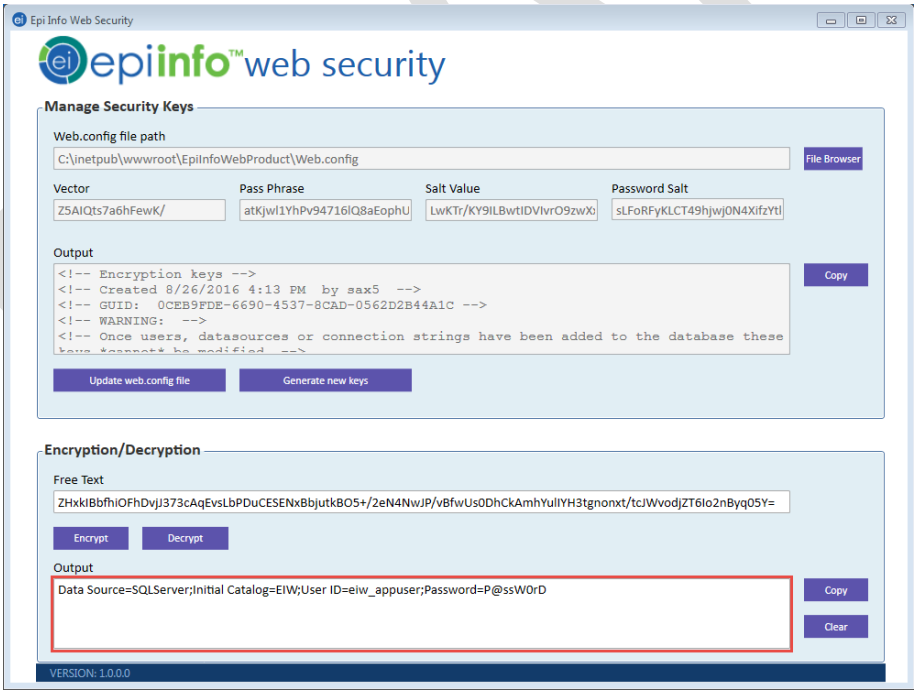
1. Follow steps of workflow 2
2. Paste the encrypted connection string that was previously encrypted using the security keys into the “Free text” text box



3. Click the “Decrypt” button.



4. Use the decrypted string provided in output textbox to debug the issues if any encountered during the application configuration



Note: The same workflow can be used to decrypt the Administration key by replacing the connection string with Admin Key.