Epi Info^{TM} Web Security Utility

Help Document

Version 1.1

10/25/2017

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
1.1	David Nitschke	10/25/2017	Version 1.1 clarified wording; fixed accessibility issues.

Table Of Contents

1 Introduction

1.1 Purpose

This document provides an overview of the key features of the Epi Info^{TM} Web Security Utility. This utility is to be used during the deployment of any of the Epi Info web products including the Epi Info^{TM} Web Survey (EIWS) system, the Epi Info^{TM} Cloud Data Capture (EICDC) system, and the Epi Info^{TM} Cloud Data Analytics (EICDA) system. This document is a companion to the deployment document for each of those web products. Configuration of the web products on the web server cannot be completed without following the steps described in this document.

1.2 Overview

Use the Epi Info^{TM} Web Security Utility to configure the security keys required by the cryptographic algorithm in the Epi Info™ web products. The web.config file provided in the Epi Info™ web products package is shipped with default security keys. We strongly recommend you update the default keys with new keys using the Epi Info^{TM} Web Security Utility for enhanced security. There are four keys in the web.config file that should be updated. These are described as follows:

a. KeyForConnectionStringVector – This key corresponds to the “Vector” field in the Epi Info^{TM} Web Security Utility.

b. KeyForConnectionStringPassphrase – This key corresponds to the “Pass Phrase” field in the Epi Info^{TM} Web Security Utility.

c. KeyForConnectionStringSalt – This key corresponds to the “Salt Value” field in the Epi Info^{TM} Web Security Utility.

d. KeyForUserPasswordSalt – This key corresponds to the “Password Salt” field in the Epi Info^{TM} Web Security Utility. This key is only applicable to the EICDC and EICDA products. It does not apply to the EIWS product.

In addition to being used by the cryptographic algorithm, these keys allow you to encrypt and decrypt connection strings and other items such as the administration key used in the EIWS product, before these strings are saved in web.config file.

Note: The screenshots provided in this document show all four keys in the Epi Info^{TM} Web Security Utility. However, if you are configuring the EIWS product which does not have a **Password Salt** key, then the text field for this key will appear empty since it is not applicable in EIWS.

1.3 Audience

This document is written for an information technology (IT) administrator, IT manager, web administrator, or anyone responsible for setting up and maintaining any of the Epi Info^{TM} web products on a web server.

2 Application Management

2.1 Prerequisites

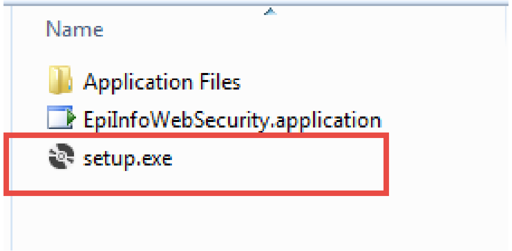
Download the web product deployment package from the Epi Info™ website at the [Epi Info Downloads page (https://www.cdc.gov/epiinfo/support/downloads.html)](https://www.cdc.gov/epiinfo/support/downloads.html). The deployment package is in the form of a compressed (zip) archive.

Extract the contents of the deployment package to a location on your computer.

You will have found these instructions inside the **\Documents** subfolder.

2.2 Installing

The installer for Epi Info^{TM} Web Security Utility is inside the \EpiInfoWebSecurity\ subfolder. The installer is named **setup.exe**. It can be installed on the web server at the time you are configuring any of the Epi Info^{TM} web products.



Name

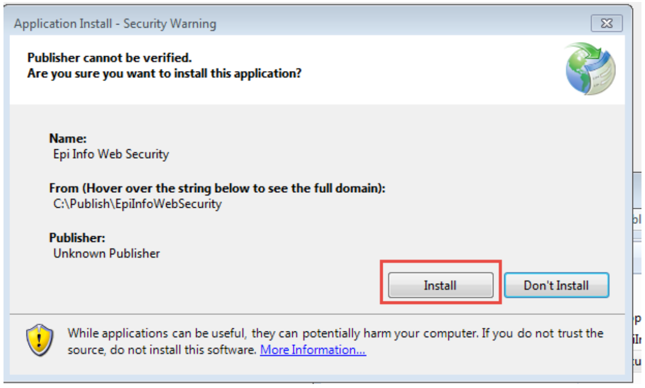
Application Files

EpiInfoWebSecurity.application

setup.exe

Figure 1: EpiInfoWebSecurity folder in Windows Explorer

To install the Epi Info™ Web Security Utility, double-click on **setup.exe**, or right-click **setup.exe** and select **Run as administrator** from the context menu. When the **Application Install – Security Warning** is displayed, click **Install**.



Application Install - Security Warning

Publisher cannot be verified.
Are you sure you want to install this application?

Name:
Epi Info Web Security

From (Hover over the string below to see the full domain):
C:\Publish\EpiInfoWebSecurity

Publisher:
Unknown Publisher

While applications can be useful, they can potentially harm your computer. If you do not trust the source, do not install this software. More Information...

Figure 2: Application installation security warning emphasizing the **Install** button.

2.3 Launching

After installation, you will find a shortcut on the desktop for Epi Info™ Web Security. Launch the utility by double-clicking the shortcut.

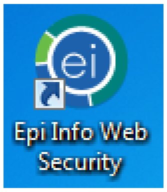


Figure 3: Shortcut icon for the Epi Info™ Web Security Utility

Alternatively, launch the utility by clicking the Epi Info™ Web Security program which is found in the Start Programs menu under a folder named **CDC/Epi Info Web**.

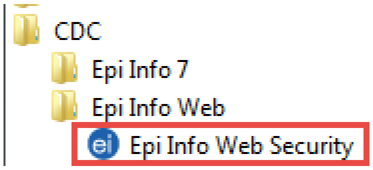


Figure 4: Epi Info™ Web Security Utility shown under the All Programs menu.

2.4 Uninstalling

As with other programs on your Windows computer, you can uninstall the Epi Info™ Web Security Utility using the Windows **Add or remove programs** tool which can be found in the **Control Panel**.

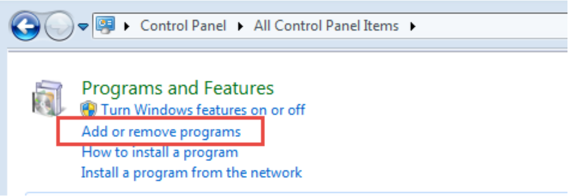
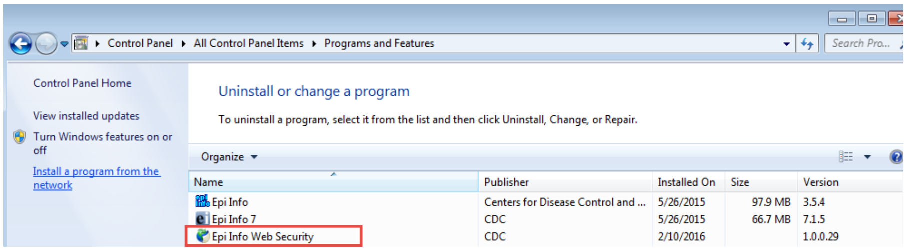


Figure 5: Add or remove programs in Control Panel

Locate **Epi Info Web Security** in the list of installed programs.



Uninstall or change a program

To uninstall a program, select it from the list and then click Uninstall, Change, or Repair.

Name	Publisher	Installed On	Size	Version
Epi Info	Centers for Disease Control and ...	5/26/2015	97.9 MB	3.5.4
Epi Info 7	CDC	5/26/2015	66.7 MB	7.1.5
Epi Info Web Security	CDC	2/10/2016		1.0.0.29

Figure 6: Control Panel, Programs and Features list.

Uninstall by right clicking **Epi Info Web Security** and selecting **Uninstall/Change**.

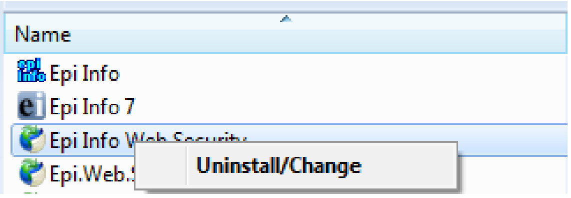
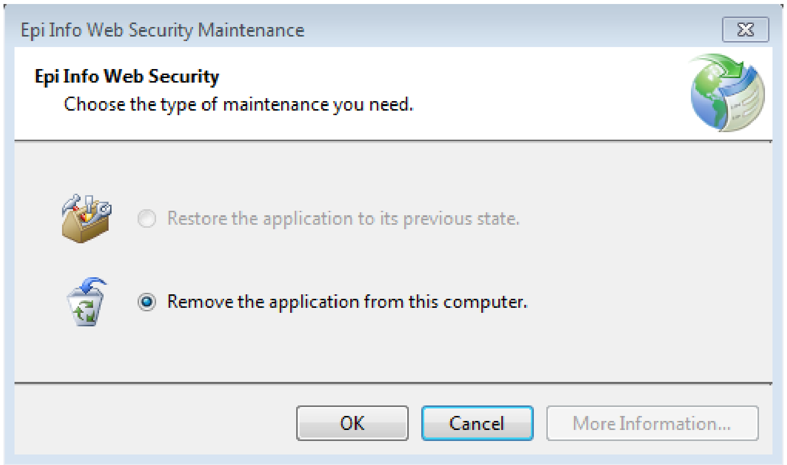


Figure 7: Uninstall/Change context menu after right-clicking on the application

Optionally, you can double-click **Epi Info Web Security** which launches the dialog to let you uninstall the application.



Epi Info Web Security Maintenance

Epi Info Web Security

Choose the type of maintenance you need.

○ Restore the application to its previous state.

● Remove the application from this computer.

Figure 8: Application removal tool.

3 Workflow 1 – Create Keys for a New Deployment

The following steps create new security keys for a new deployment of an Epi Info^{TM} web product.

1. Launch the utility as described in section 2.2. Launching above.
2. Click **File Browser**.

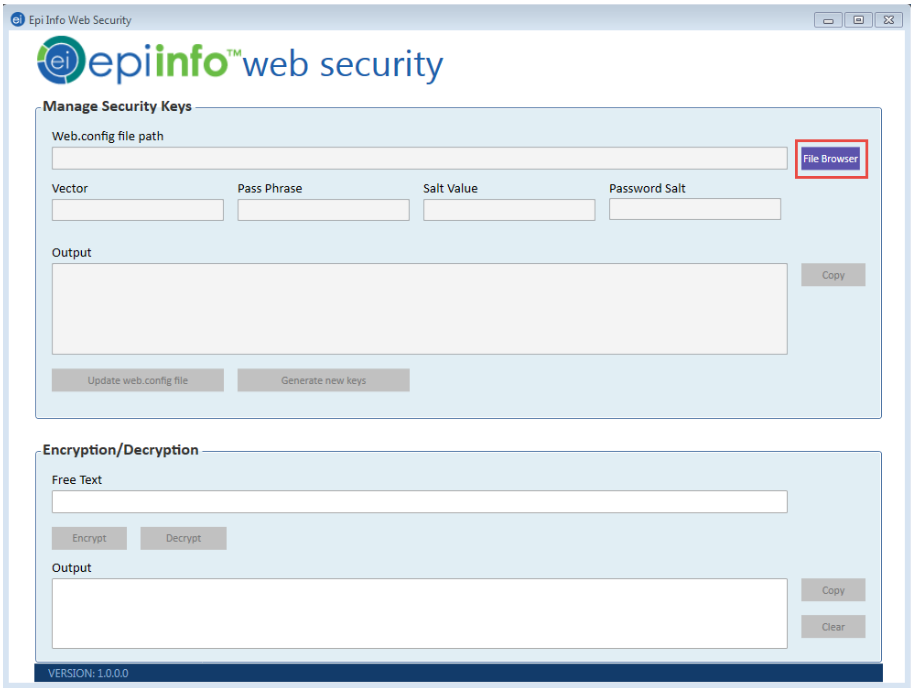
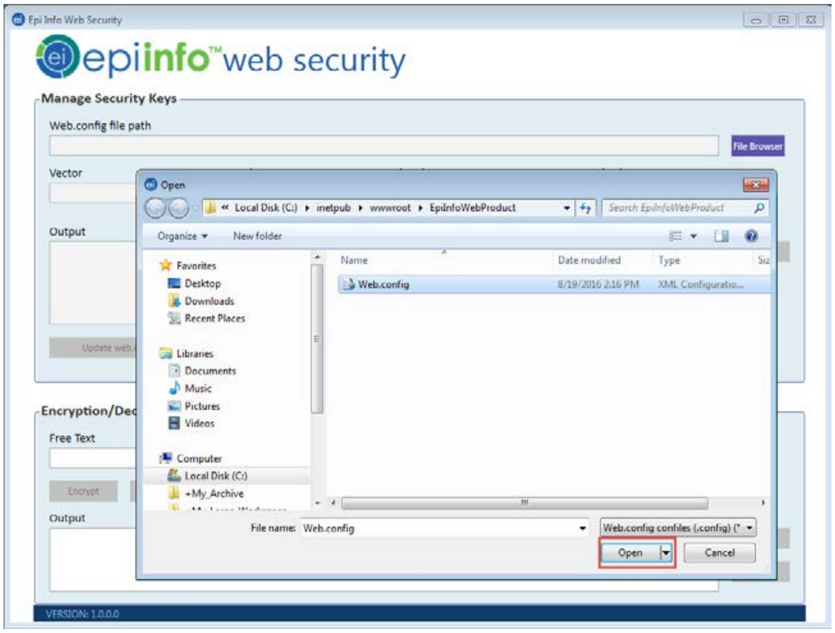


Figure 9: Epi Info™ Web Security Utility main page emphasizing the File Browser button.

3. In the **Open** dialog, navigate to the location of the web.config file which can be found under "inetpub\wwwroot\<EpiInfoWebProduct>, where "<EpiInfoWebProduct>" is replaced by the name of the folder you created for installing it. For example, if you are installing the EICDC product and you

created a folder named **EpiInfoCloudDataCapture**, the web.config file would be found under **inetpub\wwwroot\EpiInfoCloudDataCapture\**.

Select the web.config file and click **Open**.



« Local Disk (C:) ▸ inetpub ▸ wwwroot ▸ EpiInfoWebProduct

Search EpiInfoWebProduct

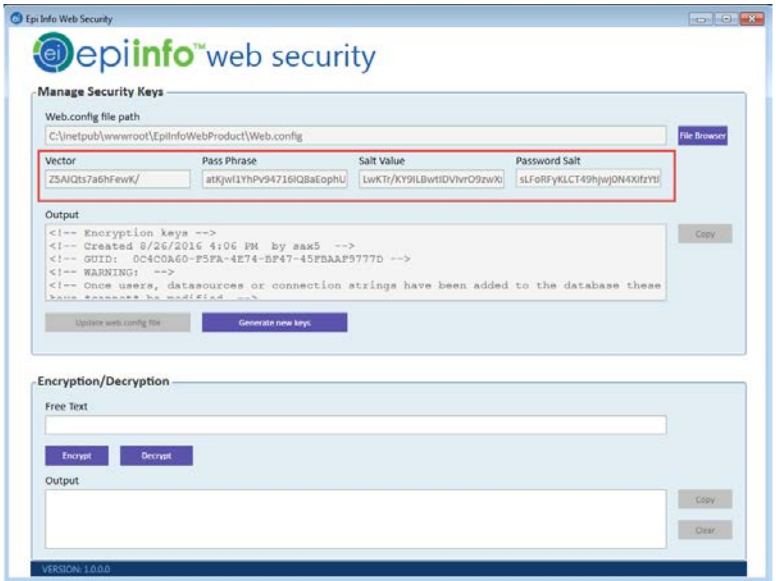
Name	Date modified	Type
Web.config	8/19/2016 2:16 PM	XML Configuratio...

File name: Web.config

Web.config confiles (.config) (*

Figure 10: File browser to open the Web.config file

The Epi Info^{TM} Web Security Utility reads the web.config file and displays the current security keys in the **Manage Security Keys** group. The keys are shown in their respective text fields: **Vector**, **Pass Phrase**, **Salt Value** and **Password Salt** (if applicable). The **Output** text box shows the **Encryption keys** section of the web.config file.



Web.config file path: C:\inetpub\wwwroot\EpiInfoWebProduct\Web.config

Vector: Z5AIQts7a6hFewK/

Pass Phrase: atKjwl1YhPv94716lQBaEophU

Salt Value: LwKTr/KY9ILBwtIDVIvrO9zwXi

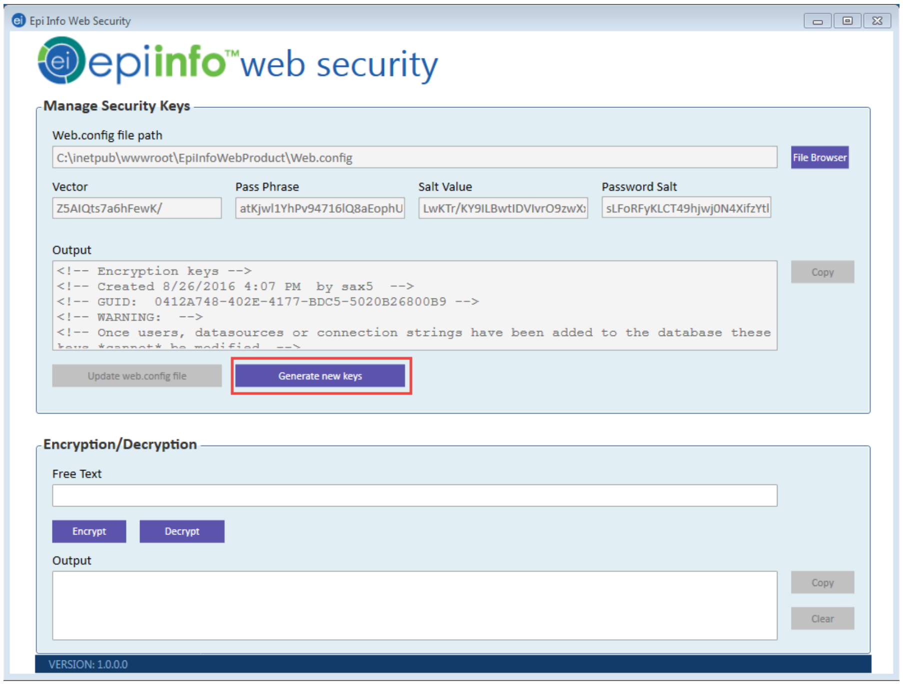
Password Salt: sLFoRFyKLCT49hjwj0N4XifzYtl

Output

```
<!-- Encryption keys -->
<!-- Created 8/26/2016 4:06 PM  by sax5  -->
<!-- GUID:  0C4C0A60-F5FA-4E74-BF47-45FBAAF9777D -->
<!-- WARNING:  -->
<!-- Once users, datasources or connection strings have been added to the database these
have *cannot* be modified  -->
```

Figure 11: Default security keys as read from the web.config file.

4. Click **Generate new keys** to generate new security keys.



Web.config file path: C:\inetpub\wwwroot\EpiInfoWebProduct\Web.config

Vector: Z5AIQts7a6hFewK/

Pass Phrase: atKjwl1YhPv94716lQ8aEophU

Salt Value: LwKTr/KY9ILBwtIDVIvrO9zwX:

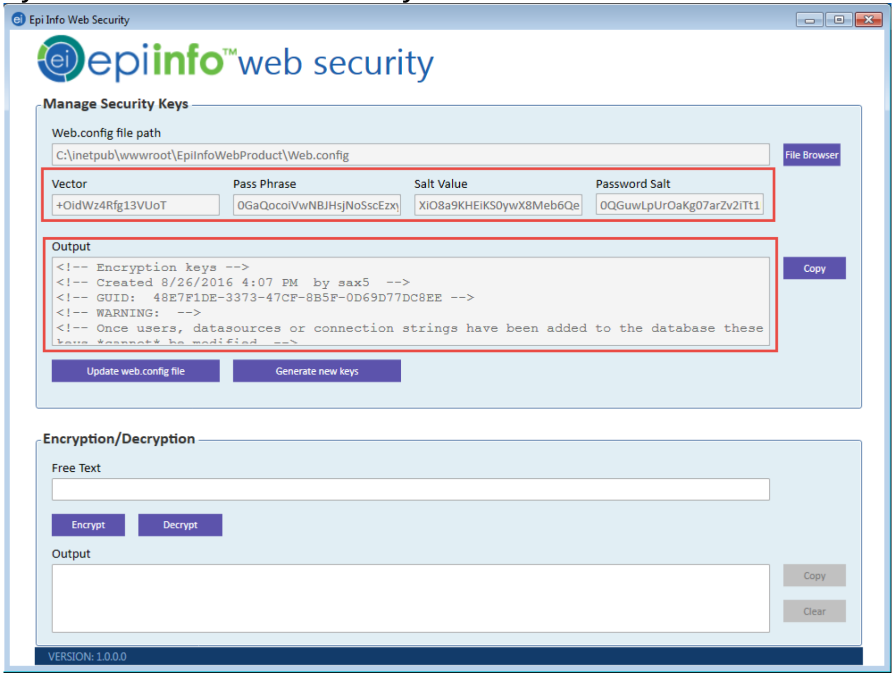
Password Salt: sLFoRFyKLCT49hjwj0N4XifzYtl

Output

```
<!-- Encryption keys -->
<!-- Created 8/26/2016 4:07 PM  by sax5  -->
<!-- GUID:  0412A748-402E-4177-BDC5-5020B26800B9 -->
<!-- WARNING:  -->
<!-- Once users, datasources or connection strings have been added to the database these
keys *cannot* be modified  -->
```

Figure 12: Generate new keys button

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



Web.config file path: C:\inetpub\wwwroot\EpiInfoWebProduct\Web.config

Vector: +OidWz4Rfg13VUoT

Pass Phrase: 0GaQocoiVwNBJHsjNoSscEzxy

Salt Value: XiO8a9KHEiKS0ywX8Meb6Qe

Password Salt: 0QGuwLpUrOaKg07arZv2iTt1

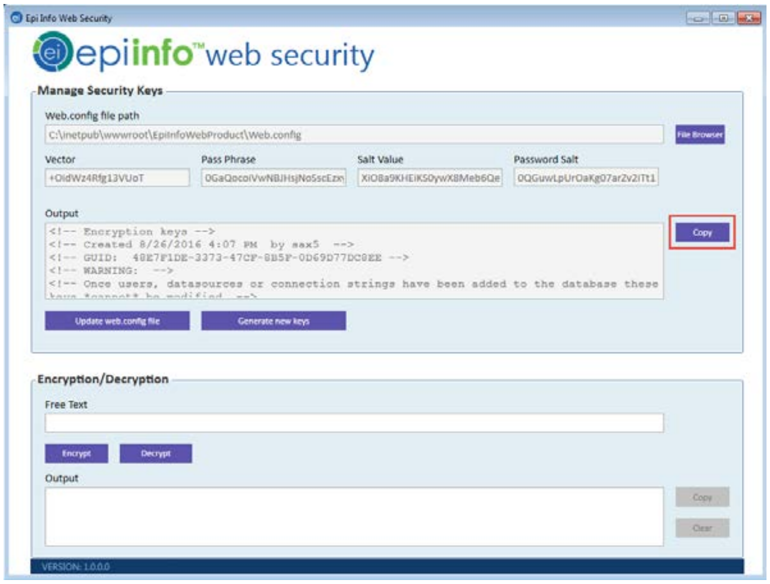
Output

```
<!-- Encryption keys -->
<!-- Created 8/26/2016 4:07 PM  by sax5  -->
<!-- GUID:  48E7F1DE-3373-47CF-8B5F-0D69D77DC8EE -->
<!-- WARNING:  -->
<!-- Once users, datasources or connection strings have been added to the database these
keys *cannot* be modified  -->
```

Figure 13: New security keys and Output box to be saved to web.config

5. Next to the Output text field, click **Copy**. This copies the contents of the Output box to the computer's clipboard.

6. Save the copied contents to a new text file. The text file may be saved in a location of your choice and serves as a backup in case the keys in the web.config file become distorted for any reason.



Web.config file path: C:\inetpub\wwwroot\EpiInfoWebProduct\Web.config

Vector: +OidWz4Rfg13VUoT

Pass Phrase: 0GaQocoiVwNBJHsjNo5scEzx

Salt Value: XiO8a9KHEiKS0ywX8Meb6Qe

Password Salt: 0QGuwLpUrOaKg07arZv2iTt1

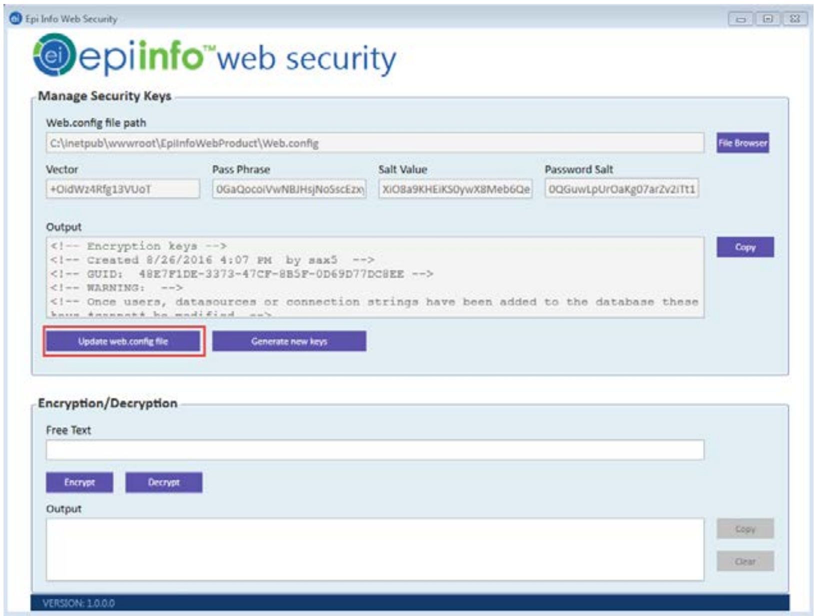
Output

```
<!-- Encryption keys -->
<!-- Created 8/26/2016 4:07 PM  by sax5  -->
<!-- GUID:  48E7F1DE-3373-47CF-8B5F-0D69D77DC8EE -->
<!-- WARNING:  -->
<!-- Once users, datasources or connection strings have been added to the database these
have *cannot* be modified -->
```

Figure 14: Copy button is on the right side of the Output field

7. Click **Update web.config file** to update the web.config file with the newly generated security keys. This action will change the current security keys to the newly generated keys.

Note: This action should be done **only once** during the life of the Epi Info web product and only at the time of initial configuration. Once data are entered in the database through the web product, any change to these keys will prevent the web product from accessing the data.



Web.config file path: C:\inetpub\wwwroot\EpiInfoWebProduct\Web.config

Vector: +OidWz4Rfg13VUoT

Pass Phrase: 0GaQocoiVwNBJHsjNo5scEzx

Salt Value: XiO8a9KHEiKS0ywX8Meb6Qe

Password Salt: 0QGuwLpUrOaKg07arZv2iTt1

Output

```
<!-- Encryption keys -->
<!-- Created 8/26/2016 4:07 PM  by sax5  -->
<!-- GUID:  48E7F1DE-3373-47CF-8B5F-0D69D77DC8EE -->
<!-- WARNING:  -->
<!-- Once users, datasources or connection strings have been added to the database these
have *cannot* be modified -->
```

Figure 15: Update web config file button

4 Workflow 2 – Load Keys from an Existing Web.Config File

The following steps describe how to read the security keys for an existing Epi Info web product from its web.config file.

1. Launch the utility as described in section 2.2. Launching above.
2. Click **File Browser**.

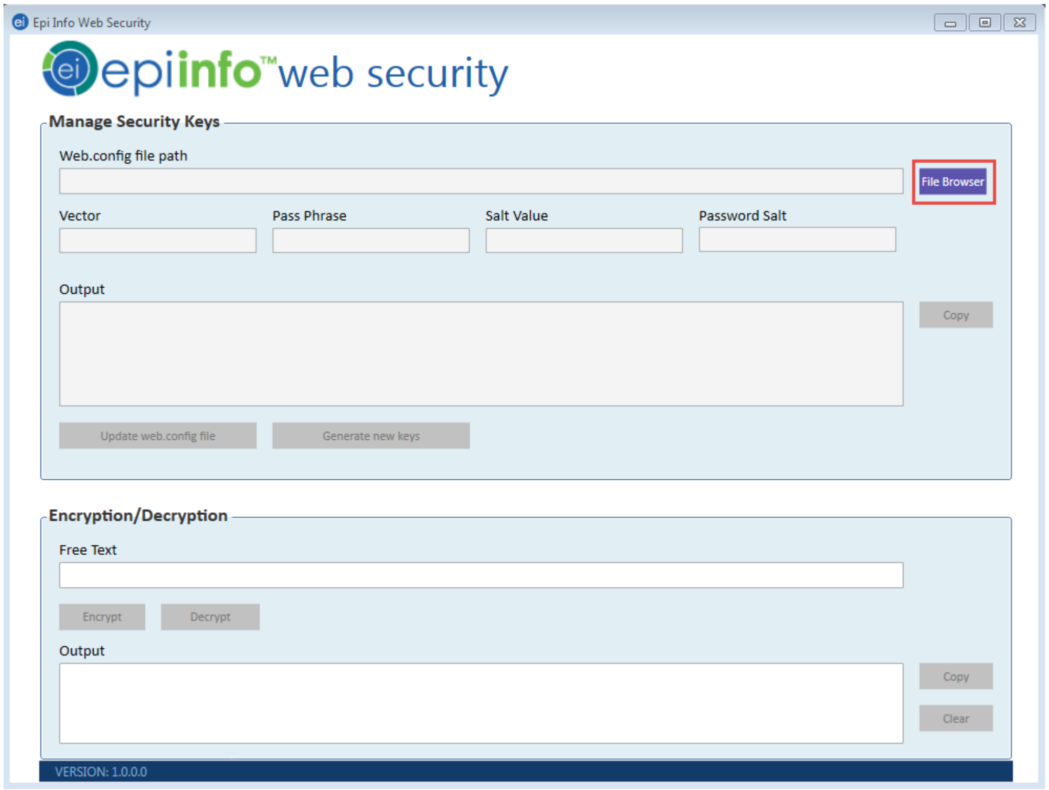


Figure 16: File browser button

3. In the **Open** dialog, navigate to the location of web.config file which can be found under “intepub\wwwroot\<EpiInfoWebProduct>, where "<EpiInfoWebProduct>" is replaced by the name of the folder you created for installing it. For example, if you are installing the EICDC product and you created a folder named **EpiInfoCloudDataCapture**, the web.config file would be found in a under **inetpub\wwwroot\EpiInfoCloudDataCapture\**.

   Select the web.config file and click **Open**.

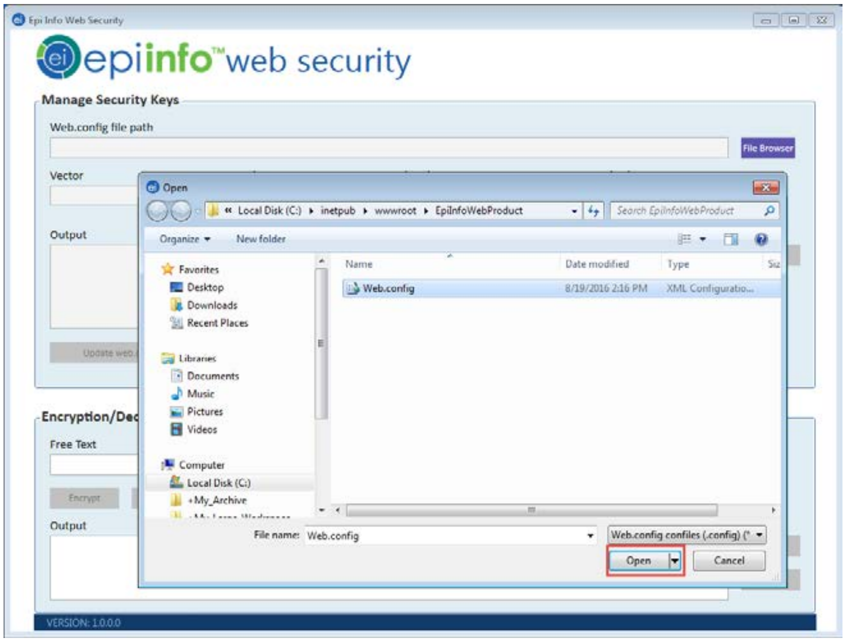
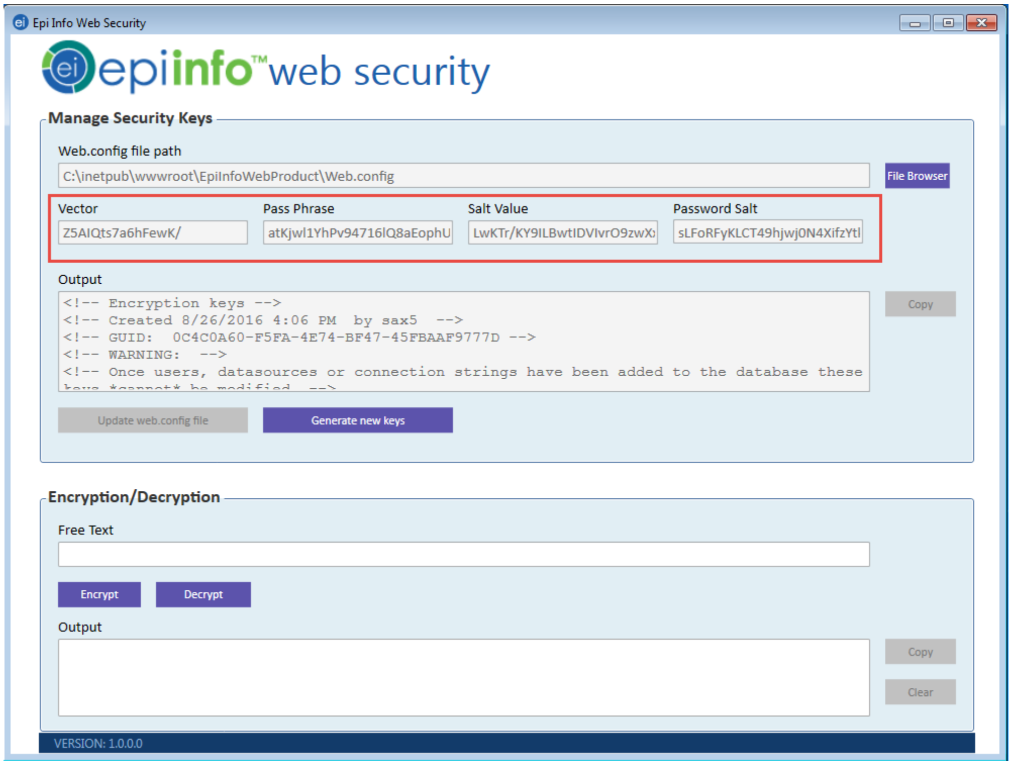


Figure 17: File browser to open the Web.config file

The Epi Info™ Web Security Utility reads the web.config file and displays the current security keys in the **Manage Security Keys** box. The keys are shown in their respective text fields: **Vector**, **Pass Phrase**, **Salt Value** and **Password Salt** (if applicable).



Manage Security Keys

Web.config file path: C:\inetpub\wwwroot\EpiInfoWebProduct\Web.config

Vector: Z5AIQts7a6hFewK/

Pass Phrase: atKjwl1YhPv94716lQ8aEophU

Salt Value: LwKTr/KY9ILBwtIDVIvrO9zwX:

Password Salt: sLFoRFyKLCT49hjwj0N4XifzYtl

Output

```
<!-- Encryption keys -->
<!-- Created 8/26/2016 4:06 PM  by sax5  -->
<!-- GUID:  0C4C0A60-F5FA-4E74-BF47-45FBAAF9777D -->
<!-- WARNING:  -->
<!-- Once users, datasources or connection strings have been added to the database these
keys *cannot* be modified  -->
```

Encryption/Decryption

Free Text

Output

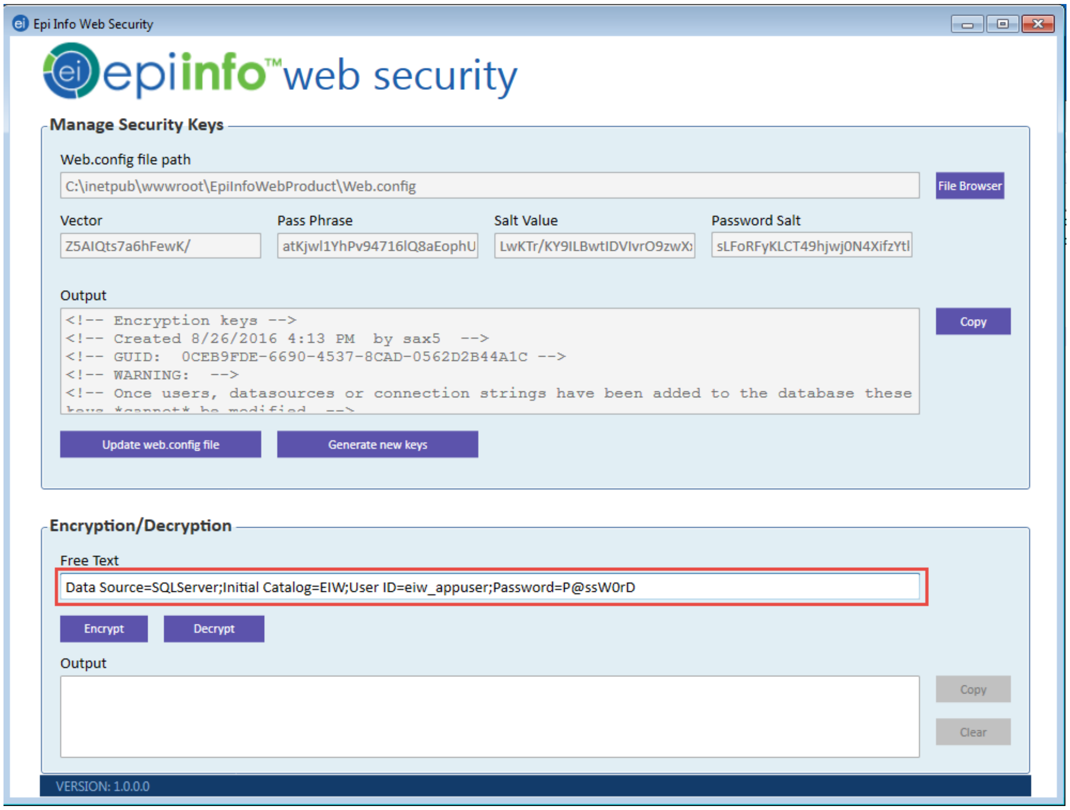
Figure 18: Current security keys as read from the web.config file.

5 Workflow 3 – Ad-Hoc Encryption

The Epi Info™ Web Security Utility allows you to encrypt the database connection string and other items such as the EIWS Administration Key. The encrypted connection string or administration key can be used to update the default encrypted connection string and administration key provided in the deployment package.

The following steps describe how to use the encryption feature with a connection string. The connection string for your installation should be created using the instructions specified in the deployment document that came with your product's deployment package.

1. Complete the steps in section 4. Workflow 2 to load the current encryption keys from the web.config file.
2. In the **Encryption/Decryption** box, paste an unencrypted string into the **Free Text** box.



Manage Security Keys

Web.config file path: C:\inetpub\wwwroot\EpiInfoWebProduct\Web.config

Vector	Pass Phrase	Salt Value	Password Salt
Z5AIQts7a6hFewK/	atKjwl1YhPv94716lQ8aEophU	LwKTr/KY9ILBwtIDVIvrO9zwX:	sLFoRFyKLCT49hjwj0N4XifzYtl

Output

```
<!-- Encryption keys -->
<!-- Created 8/26/2016 4:13 PM  by sax5  -->
<!-- GUID:  0CEB9FDE-6690-4537-8CAD-0562D2B44A1C -->
<!-- WARNING:  -->
<!-- Once users, datasources or connection strings have been added to the database these
keys *cannot* be modified  -->
```

Encryption/Decryption

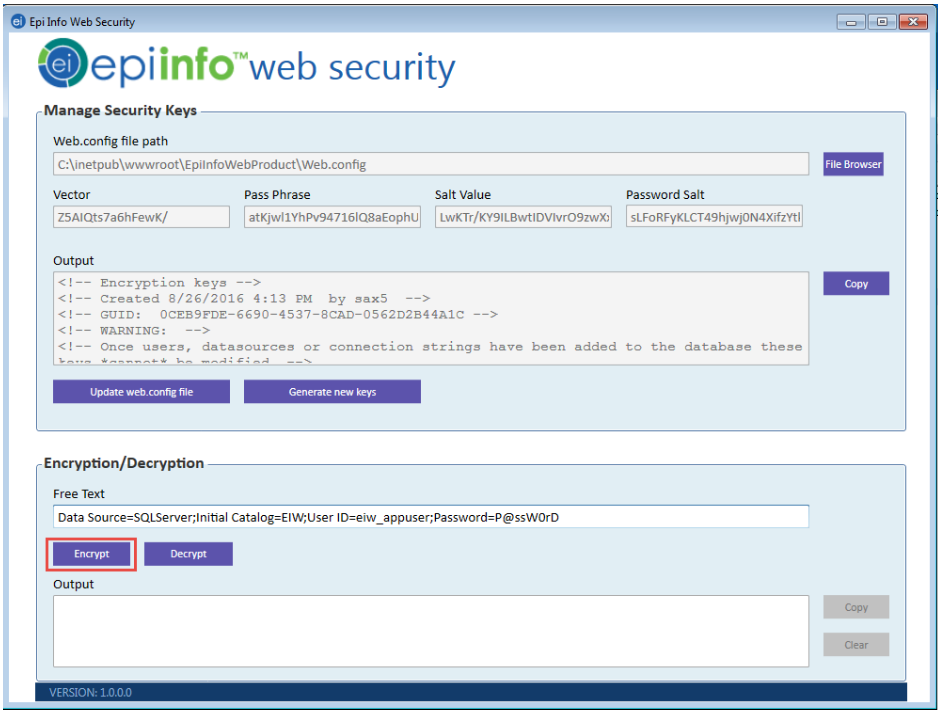
Free Text: Data Source=SQLServer;Initial Catalog=EIW;User ID=eiw_appuser;Password=P@ssW0rD

Output

VERSION: 1.0.0.0

Figure 19: Encryption/Decryption free text field showing an unencrypted connection string

3. Click **Encrypt** to encrypt the string. The utility displays the new encrypted string in the **Output** box.



Manage Security Keys

Web.config file path: C:\inetpub\wwwroot\EpiInfoWebProduct\Web.config

Vector: Z5AIQts7a6hFewK/

Pass Phrase: atKjwl1YhPv94716lQ8aEophU

Salt Value: LwKTr/KY9ILBwtIDVIvrO9zwX

Password Salt: sLFoRFyKLCT49hjwj0N4XifzYtl

Output

```
<!-- Encryption keys -->
<!-- Created 8/26/2016 4:13 PM  by sax5  -->
<!-- GUID:  0CEB9FDE-6690-4537-8CAD-0562D2B44A1C -->
<!-- WARNING:  -->
<!-- Once users, datasources or connection strings have been added to the database these
keys *cannot* be modified  -->
```

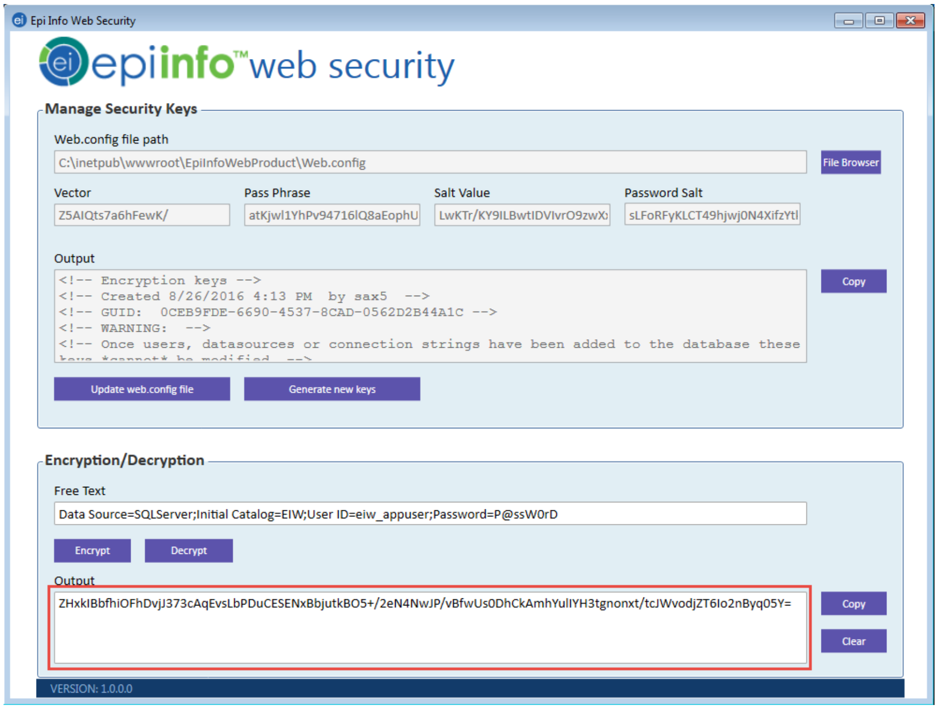
Encryption/Decryption

Free Text: Data Source=SQLServer;Initial Catalog=EIW;User ID=eiw_appuser;Password=P@ssW0rD

Output

Figure 20: Encrypt button below the Free Text field.

4. Use the encrypted string provided in **Output** to update the connection string in the web.config file.



Manage Security Keys

Web.config file path: C:\inetpub\wwwroot\EpiInfoWebProduct\Web.config

Vector: Z5AIQts7a6hFewK/

Pass Phrase: atKjwl1YhPv94716lQ8aEophU

Salt Value: LwKTr/KY9ILBwtIDVIvrO9zwX

Password Salt: sLFoRFyKLCT49hjwj0N4XifzYtl

Output

```
<!-- Encryption keys -->
<!-- Created 8/26/2016 4:13 PM  by sax5  -->
<!-- GUID:  0CEB9FDE-6690-4537-8CAD-0562D2B44A1C -->
<!-- WARNING:  -->
<!-- Once users, datasources or connection strings have been added to the database these
keys *cannot* be modified  -->
```

Encryption/Decryption

Free Text: Data Source=SQLServer;Initial Catalog=EIW;User ID=eiw_appuser;Password=P@ssW0rD

Output

```
ZHxkIBbfhiOFhDvjJ373cAqEvsLbPDuCESENxBbjutkBO5+/2eN4NwJP/vBfwUs0DhCkAmhYulIYH3tgnonxt/tcJWvodjZT6Io2nByq05Y=
```

Figure 21: Output field shows the result of an encryption process.

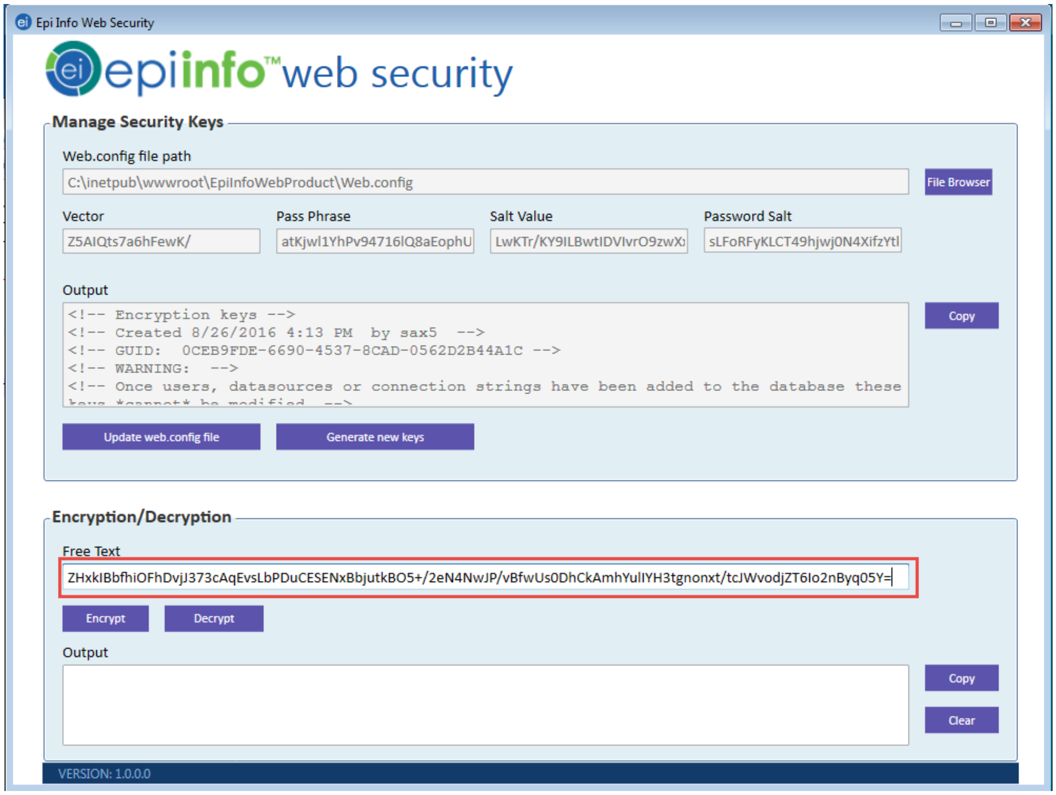
Note: The same workflow can be used to encrypt the Administration key by replacing the connection string with the key.

6 Workflow 4 – Ad-Hoc Decryption

As described above for encryption, the Epi Info™ Web Security Utility also allows you to decrypt items such as encrypted connection strings and keys. This may be needed in order to troubleshoot problems with connecting to the database. When resolving connection issues, the connection string can be inspected after decryption and updated as needed to resolve the problem.

The following steps describe how to use the decryption feature with an encrypted connection string, but the same steps apply for decrypting other items that were encrypted using the keys in the web.config file.

1. Complete the steps in section 4. Workflow 2 to load the current encryption keys from the web.config file.
2. In the **Encryption/Decryption** box, paste the string that was previously encrypted using the current security keys into the **Free Text**.



Web.config file path: C:\inetpub\wwwroot\EpiInfoWebProduct\Web.config

Vector: Z5AIQts7a6hFewK/

Pass Phrase: atKjwl1YhPv94716lQ8aEophU

Salt Value: LwKTr/KY9ILBwtIDVIvrO9zwX

Password Salt: sLFoRFyKLCT49hjwj0N4XifzYtl

Output:

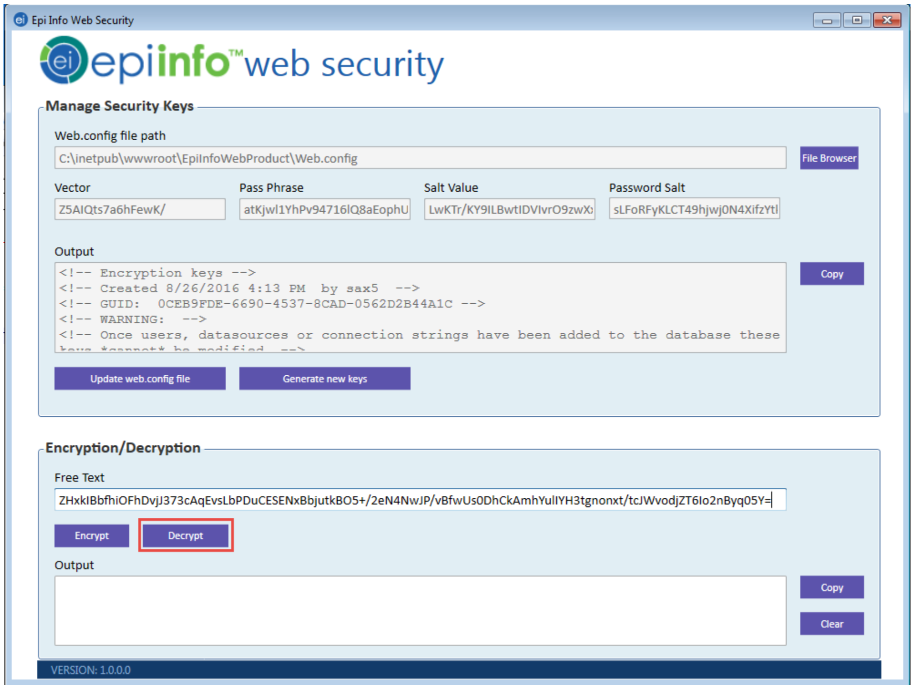
```
<!-- Encryption keys -->
<!-- Created 8/26/2016 4:13 PM  by sax5  -->
<!-- GUID:  0CEB9FDE-6690-4537-8CAD-0562D2B44A1C -->
<!-- WARNING:  -->
<!-- Once users, datasources or connection strings have been added to the database these
keys *cannot* be modified  -->
```

Free Text: ZHxkIBbfhiOFhDvjJ373cAqEvsLbPDuCESENxBbjutkBO5+/2eN4NwJP/vBfwUs0DhCkAmhYulIYH3tgnonxt/tcJWvodjZT6Io2nByq05Y=

Output:

Figure 22: Encryption/Decryption free text field.

3. Click **Decrypt** to decrypt the string. The utility shows the plain text version of the string in the **Output** box.



Manage Security Keys

Web.config file path: C:\inetpub\wwwroot\EpiInfoWebProduct\Web.config

Vector: Z5AIQts7a6hFewK/

Pass Phrase: atKjwl1YhPv94716lQ8aEophU

Salt Value: LwKTr/KY9ILBwtIDVIvrO9zwX

Password Salt: sLFoRFyKLCT49hjwj0N4XifzYtl

Output

```
<!-- Encryption keys -->
<!-- Created 8/26/2016 4:13 PM  by sax5  -->
<!-- GUID:  0CEB9FDE-6690-4537-8CAD-0562D2B44A1C -->
<!-- WARNING:  -->
<!-- Once users, datasources or connection strings have been added to the database these
keys *cannot* be modified  -->
```

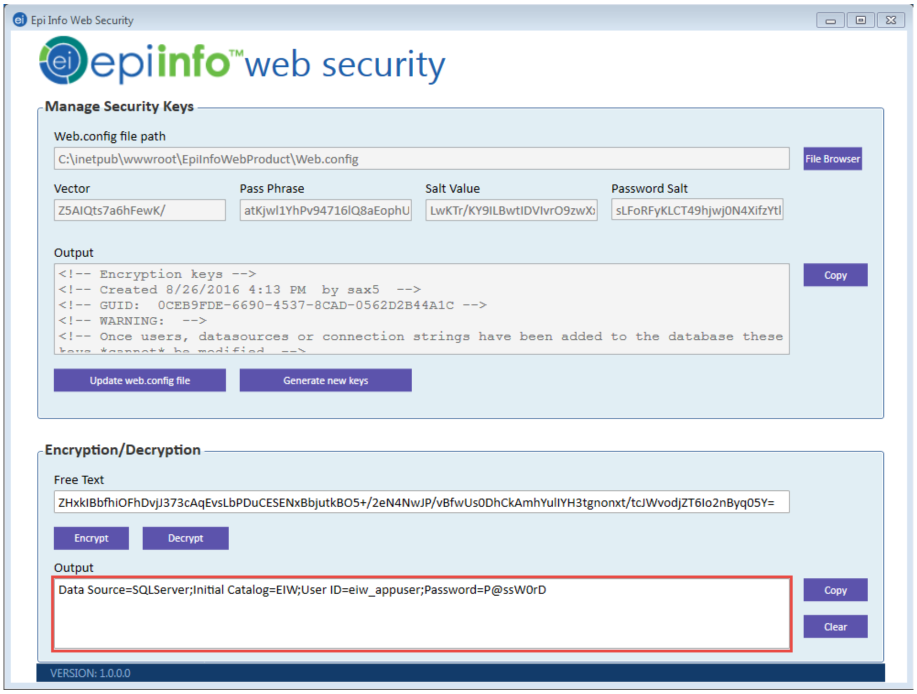
Encryption/Decryption

Free Text: ZHxkIBbfhiOFhDvjJ373cAqEvsLbPDuCESENxBbjutkBO5+/2eN4NwJP/vBfwUs0DhCkAmhYulIYH3tgnonxt/tcJWvodjZT6Io2nByq05Y=

Output

Figure 23: Decrypt button below the Free Text field.

4. Use the decrypted string provided in **Output** to debug the issues if any are encountered during the application configuration process.



Manage Security Keys

Web.config file path: C:\inetpub\wwwroot\EpiInfoWebProduct\Web.config

Vector: Z5AIQts7a6hFewK/

Pass Phrase: atKjwl1YhPv94716lQ8aEophU

Salt Value: LwKTr/KY9ILBwtIDVIvrO9zwX

Password Salt: sLFoRFyKLCT49hjwj0N4XifzYtl

Output

```
<!-- Encryption keys -->
<!-- Created 8/26/2016 4:13 PM  by sax5  -->
<!-- GUID:  0CEB9FDE-6690-4537-8CAD-0562D2B44A1C -->
<!-- WARNING:  -->
<!-- Once users, datasources or connection strings have been added to the database these
keys *cannot* be modified  -->
```

Encryption/Decryption

Free Text: ZHxkIBbfhiOFhDvjJ373cAqEvsLbPDuCESENxBbjutkBO5+/2eN4NwJP/vBfwUs0DhCkAmhYulIYH3tgnonxt/tcJWvodjZT6Io2nByq05Y=

Output

```
Data Source=SQLServer;Initial Catalog=EIW;User ID=eiw_appuser;Password=P@ssW0rD
```

Figure 24: Output field shows the result of the decryption process.

Note: The same workflow can be used to decrypt the administration key by replacing the connection string with an encrypted key string.