

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

DRAFT

TABLE OF CONTENTS

1 INTRODUCTION.....	4
1.1 Purpose.....	4
1.2 Overview	4
1.3 Audience	4
2 APPLICATION MANAGEMENT	5
2.1 Installing.....	5
2.2 Launching	5
2.3 Uninstalling.....	6
3 WORKFLOW 1 – CREATE KEYS FOR A NEW INSTALLATION	7
4 WORKFLOW 2 - LOAD KEYS FROM EXISTING WEB.CONFIG	11
5 WORKFLOW 3 – AD-HOC ENCRYPT.....	12
6 WORKFLOW 4 - AD-HOC DECRYPT.....	14

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.

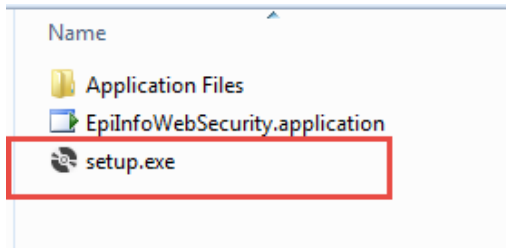
1.3 AUDIENCE

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.

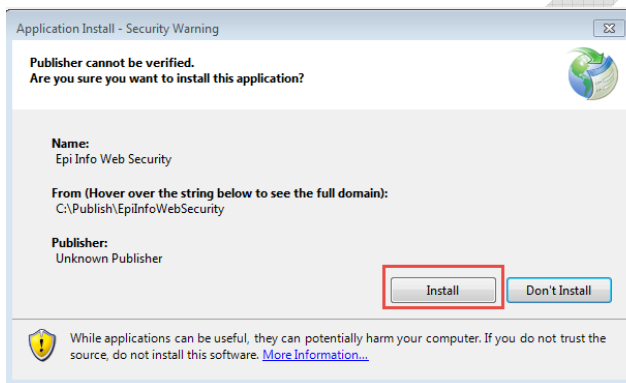
2 APPLICATION MANAGEMENT

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”.

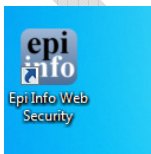


Click on “Setup.exe” and click on “Install” to install Epi Info™ Web Security Utility.

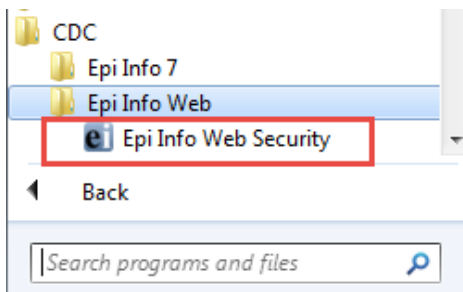


2.2 LAUNCHING

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.

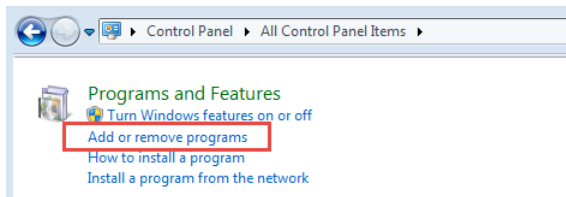


The “Epi Info Web Security” Utility can also be found in All Programs under a folder called “CDC/Epi Info Web”

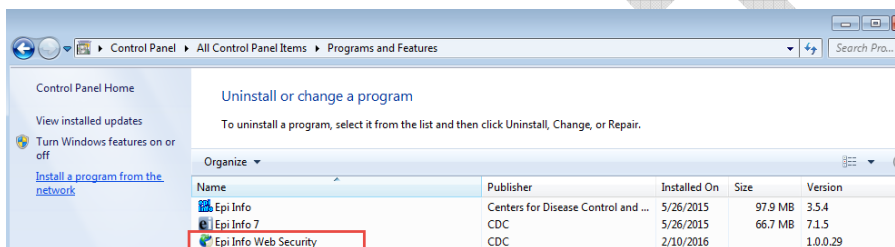


2.3 UNINSTALLING

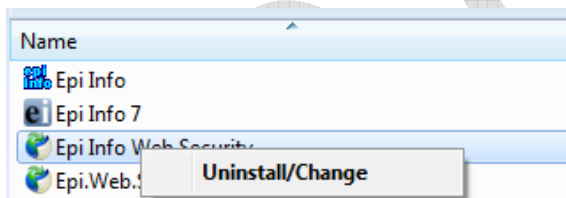
The Epi Info Web Security Utility can be uninstalled by using “Add or remove programs” feature.



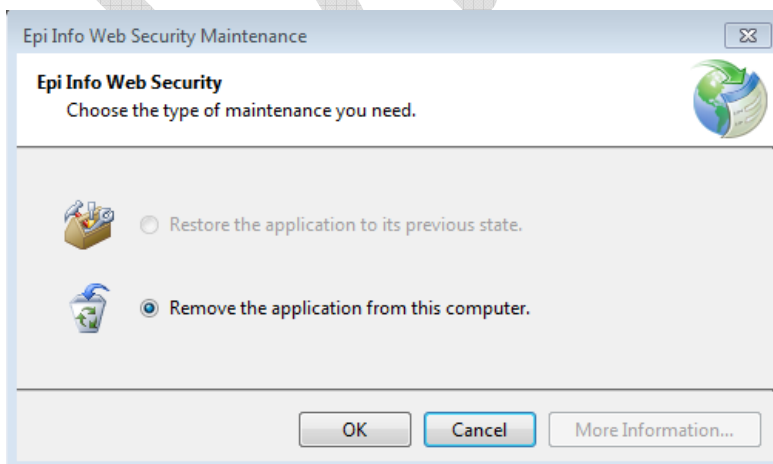
Locate Epi Info Web Security Utility in the list of installed programs



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



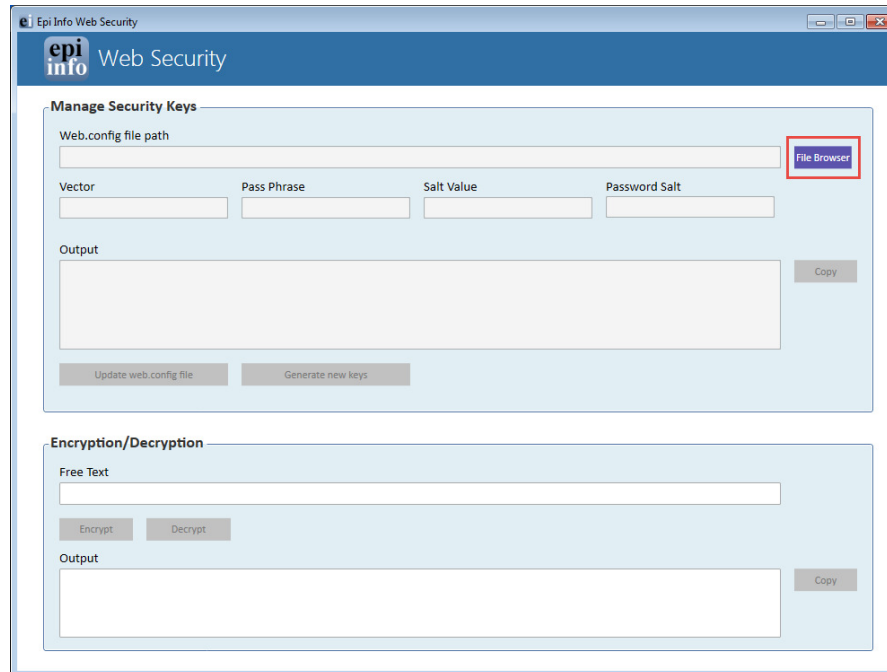
Optionally, you can double click on Epi Info Web Security which will launch the dialog to let you uninstall the application



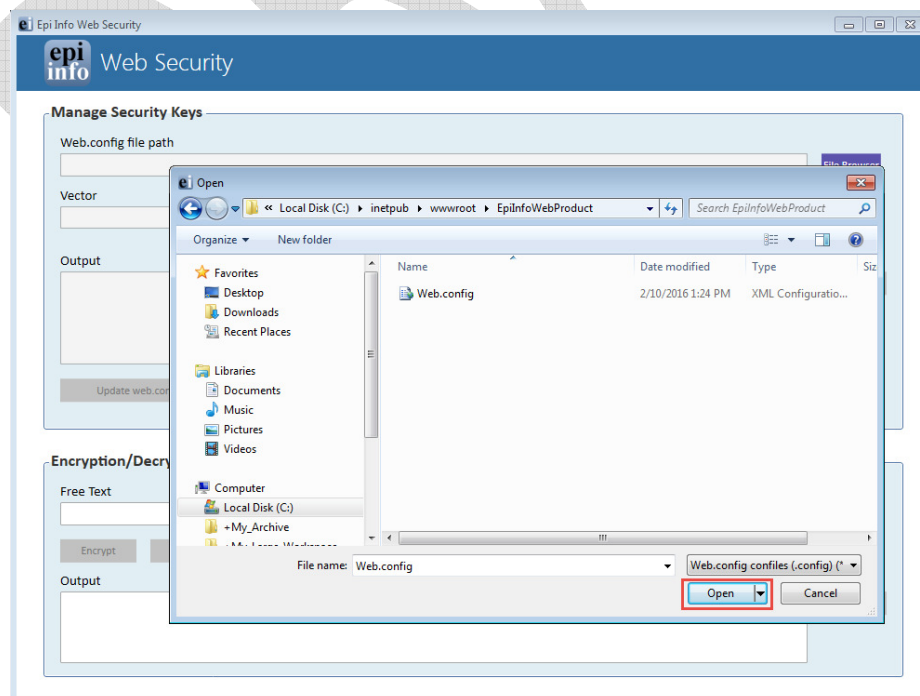
3 WORKFLOW 1 – CREATE KEYS FOR A NEW INSTALLATION

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

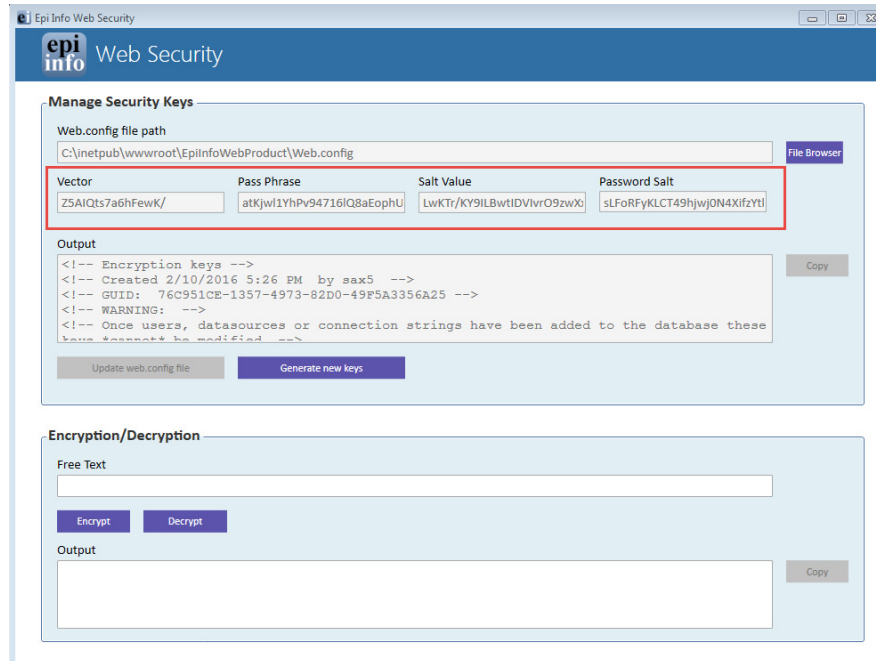
1. Click on “File Browser” button.



2. In the Open file dialog navigate to the location of web.config file which can be found under “inetpub\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.



- 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.



Epi Info Web Security

Manage Security Keys

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

Vector: Z5AIQts7a6hFewK/

Pass Phrase: atKjwl1YhPv94716lQ8aEophU

Salt Value: LwKTr/KY9ILBwtIDVlvrO9zwXc

Password Salt: sLFoRFyKLCT49hjwJON4XifzYtl

Output:

```
<!-- Encryption keys -->
<!-- Created 2/10/2016 5:26 PM by sax5 -->
<!-- GUID: 76C951CE-1357-4973-82D0-49F5A3356A25 -->
<!-- WARNING: -->
<!-- Once users, datasources or connection strings have been added to the database these
keys ***** be modified -->
```

Update web.config file

Generate new keys

Encryption/Decryption

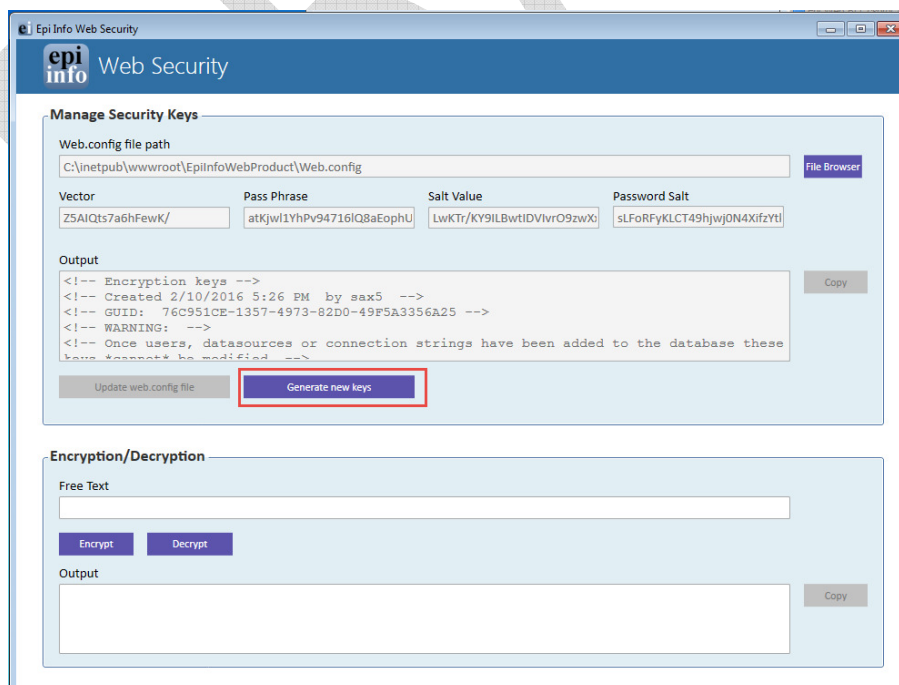
Free Text

Encrypt Decrypt

Output

Copy

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



Epi Info Web Security

Manage Security Keys

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

Vector: Z5AIQts7a6hFewK/

Pass Phrase: atKjwl1YhPv94716lQ8aEophU

Salt Value: LwKTr/KY9ILBwtIDVlvrO9zwXc

Password Salt: sLFoRFyKLCT49hjwJON4XifzYtl

Output:

```
<!-- Encryption keys -->
<!-- Created 2/10/2016 5:26 PM by sax5 -->
<!-- GUID: 76C951CE-1357-4973-82D0-49F5A3356A25 -->
<!-- WARNING: -->
<!-- Once users, datasources or connection strings have been added to the database these
keys ***** be modified -->
```

Update web.config file

Generate new keys

Encryption/Decryption

Free Text

Encrypt Decrypt

Output

Copy

- 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.

Manage Security Keys

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

Vector: HE9Yt55hz8k7q0hG

Pass Phrase: ogNPhFOQ2DeBmhR7hes78rl

Salt Value: 5iqC+OnBfzkiyxcYrcu1lvkmE4i

Password Salt: tmu+zmhHt1oBsmTokEJRSAr

Output:

```
<!-- Encryption keys -->
<!-- Created 2/10/2016 5:30 PM by sax5 -->
<!-- GUID: E3B58527-937C-4218-93B5-26121EEE9AE2 -->
<!-- WARNING: -->
<!-- Once users, datasources or connection strings have been added to the database these keys *must* be modified -->
```

Update web.config file | Generate new keys | Copy

Encryption/Decryption

Free Text:

Encrypt | Decrypt

Output:

Copy

- 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.

Manage Security Keys

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

Vector: HE9Yt55hz8k7q0hG

Pass Phrase: ogNPhFOQ2DeBmhR7hes78rl

Salt Value: 5iqC+OnBfzkiyxcYrcu1lvkmE4i

Password Salt: tmu+zmhHt1oBsmTokEJRSAr

Output:

```
<!-- Encryption keys -->
<!-- Created 2/10/2016 5:30 PM by sax5 -->
<!-- GUID: E3B58527-937C-4218-93B5-26121EEE9AE2 -->
<!-- WARNING: -->
<!-- Once users, datasources or connection strings have been added to the database these keys *must* be modified -->
```

Update web.config file | Generate new keys | Copy

Encryption/Decryption

Free Text:

Encrypt | Decrypt

Output:

Copy

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.

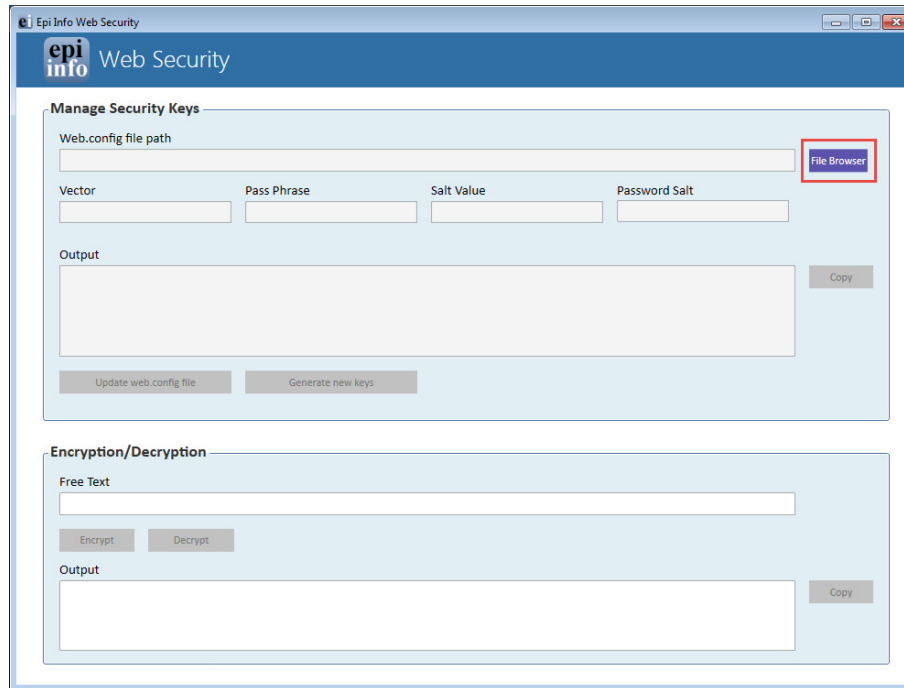
The screenshot shows the 'Epi Info Web Security' application window. The 'Manage Security Keys' section is active, displaying the 'Web.config file path' as 'C:\inetpub\wwwroot\EpiInfoWebProduct\Web.config'. Below this, four input fields are shown: 'Vector' (HE9Yt55hz8k7q0hG), 'Pass Phrase' (ogNPhFOQ2DeBmhr7hes78rt), 'Salt Value' (5iqC+OnBfzkiyxcYrcu1ivkmE4i), and 'Password Salt' (tmu+zmhHt1oBSmTokEJRSAr). An 'Output' section displays XML code for encryption keys, including a GUID and a warning message. At the bottom of this section, the 'Update web.config file' button is highlighted with a red box, and a 'Generate new keys' button is also visible. The 'Encryption/Decryption' section below is empty, with a 'Free Text' input field and 'Encrypt' and 'Decrypt' buttons.

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.

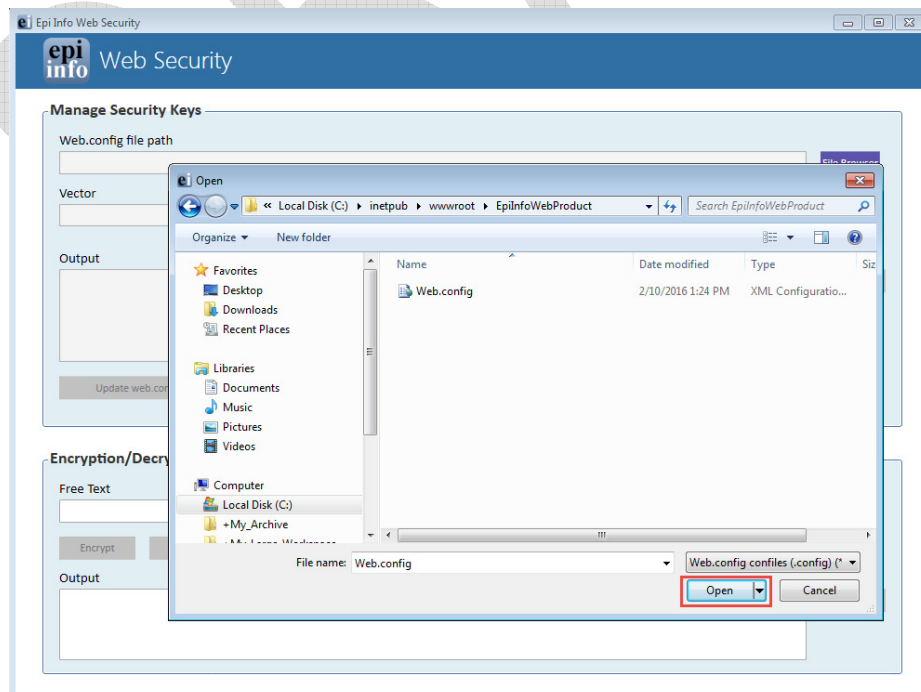
4 WORKFLOW 2 - LOAD KEYS FROM EXISTING WEB.CONFIG

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 “inetpub\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.

The screenshot shows the 'Epi Info Web Security' application window. The 'Manage Security Keys' section is highlighted with a red box. It contains the following fields and values:

Vector	Pass Phrase	Salt Value	Password Salt
Z5AIQt57a6hFewK/	atKjw1YhPv94716IQ8aEophU	LwKTr/KY9ILBwtIDVlvrO9zwXc	sLFoRFyKlCT49hjwJON4XifzYtl

Below the fields is an 'Output' section showing XML code:

```
<!-- Encryption keys -->
<!-- Created 2/10/2016 5:26 PM by sax5 -->
<!-- GUID: 76C951CE-1357-4973-82D0-49F5A3356A25 -->
<!-- WARNING: -->
<!-- Once users, datasources or connection strings have been added to the database these keys cannot be modified -->
```

The 'Encryption/Decryption' section is also visible below, with a 'Free Text' input field and 'Encrypt' and 'Decrypt' buttons.

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

Manage Security Keys

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

Vector: Z5AIQts7a6hFewK/ Pass Phrase: atKjwl1YhPv94716IQ8aEophU Salt Value: LwKTr/KY9ILBwtIDVlvrO9zwXc Password Salt: sLFoRFyKLCT49hJwJON4XfzYtI

Output

```
<!-- Encryption keys -->
<!-- Created 2/11/2016 12:39 PM by sax5 -->
<!-- GUID: F0E80CB1-C97B-43CE-BE92-3651EACAC80F -->
<!-- WARNING: -->
<!-- Once users, datasources or connection strings have been added to the database these
have cannot be modified -->
```

Copy

Update web.config file Generate new keys

Encryption/Decryption

Free Text
Data Source=SQLServer;Initial Catalog=EIW;Persist Security Info=True;User ID=eiw_appuser;Password=P@ssW0rD

Encrypt Decrypt

Output

Copy

3. Click the “Encrypt” button

Manage Security Keys

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

Vector: Z5AIQts7a6hFewK/ Pass Phrase: atKjwl1YhPv94716IQ8aEophU Salt Value: LwKTr/KY9ILBwtIDVlvrO9zwXc Password Salt: sLFoRFyKLCT49hJwJON4XfzYtI

Output

```
<!-- Encryption keys -->
<!-- Created 2/11/2016 12:39 PM by sax5 -->
<!-- GUID: F0E80CB1-C97B-43CE-BE92-3651EACAC80F -->
<!-- WARNING: -->
<!-- Once users, datasources or connection strings have been added to the database these
have cannot be modified -->
```

Copy

Update web.config file Generate new keys

Encryption/Decryption

Free Text
Data Source=SQLServer;Initial Catalog=EIW;Persist Security Info=True;User ID=eiw_appuser;Password=P@ssW0rD

Encrypt Decrypt

Output

Copy

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

The screenshot shows the Epi Info Web Security Utility window. The 'Manage Security Keys' section has a 'Web.config file path' field with the value 'C:\inetpub\wwwroot\EpiInfoWebProduct\Web.config' and a 'File Browser' button. Below are four input fields: 'Vector' (Z5AIQts7a6hFewK/), 'Pass Phrase' (atKjwl1YhPv94716lQ8aEophU), 'Salt Value' (LwKTr/KY9ILBwtIDVlvrO9zwX), and 'Password Salt' (sLFoRFyKLCt49hJwJ0N4XifzYtI). An 'Output' box contains XML-like text: '<!-- Encryption keys -->', '<!-- Created 2/11/2016 12:39 PM by sax5 -->', '<!-- GUID: F0E80CB1-C97B-43CE-BE92-3651EACAC80F -->', '<!-- WARNING: -->', and '<!-- Once users, datasources or connection strings have been added to the database these keys cannot be modified -->'. There are 'Update web.config file' and 'Generate new keys' buttons. The 'Encryption/Decryption' section has a 'Free Text' field with a connection string: 'Data Source=SQLServer;Initial Catalog=EIW;Persist Security Info=True;User ID=eiw_appuser;Password=P@ssW0rD'. There are 'Encrypt' and 'Decrypt' buttons. The 'Output' box shows an encrypted string: 'ZHxkiBbfhIOFhDvj373cAqEvsLbPDuCESEnxBbJutn7+UTSPNivFug5bVl8cA3d61FL+5Zsh9Ht9OWpJfKz2H0xZllzXkSrZAdFq79cNPZIEbx7HOyLc+MojNJBk57HkfqkOPNCWUMHZ+0jhWdQJg=='. A red box highlights the encrypted output.

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

6 WORKFLOW 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

Epi Info Web Security

Manage Security Keys

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

Vector: Z5AIQts7a6hFewK/ Pass Phrase: atKjwl1YhPv94716lQ8aEophU Salt Value: LwKTr/KY9iLBwtlDVlvrO9zwXc Password Salt: sLFoRFyKlCT49hjwJON4XifzYtI

Output

```
<!-- Encryption keys -->
<!-- Created 2/11/2016 1:12 PM by sax5 -->
<!-- GUID: E21645BB-28C2-4B51-B479-7A47D83AD294 -->
<!-- WARNING: -->
<!-- Once users, datasources or connection strings have been added to the database these keys cannot be modified -->
```

Update web.config file Generate new keys Copy

Encryption/Decryption

Free Text

ZHxklBbfhiOFhDvjJ373cAqEvsLbPDuCESENxBbjutn7+UTSPNivFug5bVl8cA3d61FL
+5Zsh9Ht9OWpJfKz2H0xZlZkSrZAdFq79cNPZlEbx7HOyLc+MojNJBk57HkfKOPNCWUMHZ+0JhWdQJg==

Encrypt Decrypt

Output

Copy

- Click the “Decrypt” button.

Epi Info Web Security

Manage Security Keys

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

Vector: Z5AIQts7a6hFewK/ Pass Phrase: atKjwl1YhPv94716lQ8aEophU Salt Value: LwKTr/KY9iLBwtlDVlvrO9zwXc Password Salt: sLFoRFyKlCT49hjwJON4XifzYtI

Output

```
<!-- Encryption keys -->
<!-- Created 2/11/2016 1:12 PM by sax5 -->
<!-- GUID: E21645BB-28C2-4B51-B479-7A47D83AD294 -->
<!-- WARNING: -->
<!-- Once users, datasources or connection strings have been added to the database these keys cannot be modified -->
```

Update web.config file Generate new keys Copy

Encryption/Decryption

Free Text

ZHxklBbfhiOFhDvjJ373cAqEvsLbPDuCESENxBbjutn7+UTSPNivFug5bVl8cA3d61FL
+5Zsh9Ht9OWpJfKz2H0xZlZkSrZAdFq79cNPZlEbx7HOyLc+MojNJBk57HkfKOPNCWUMHZ+0JhWdQJg==

Encrypt Decrypt

Output

Copy

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

The screenshot displays the Epi Info Web Security Utility application window. The title bar reads 'Epi Info Web Security'. The main window has a blue header with the 'epi info' logo and the text 'Web Security'. Below the header, there are two main sections: 'Manage Security Keys' and 'Encryption/Decryption'.

Manage Security Keys

Web.config file path: [File Browser](#)

Vector	Pass Phrase	Salt Value	Password Salt
<input type="text" value="ZSAIQts7a6hFewK/"/>	<input type="text" value="atKjwl1YhPv94716iQ8aEophU"/>	<input type="text" value="LwKTr/KY9ILBwtIDVivrO9zwX0"/>	<input type="text" value="sLFoRFyKLCT49hjwj0N4XifzYtl"/>

Output:

```
<!-- Encryption keys -->
<!-- Created 2/11/2016 1:12 PM by sax5 -->
<!-- GUID: E21645BB-28C2-4B51-B479-7A47D83AD294 -->
<!-- WARNING: -->
<!-- Once users, datasources or connection strings have been added to the database these keys cannot be modified -->
```

[Update web.config file](#) [Generate new keys](#) [Copy](#)

Encryption/Decryption

Free Text:

[Encrypt](#) [Decrypt](#)

Output:

[Copy](#)

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