EPI INFO™ WEB ANALYTICS AND VISUALIZATION (EWAV) ENCRYPTION UTILITY

HELP DOCUMENT

Version 1.0

01/15/2014

VERSION HISTORY

Version #	Implemented By	Revision Date	Reason
1.0	Daniel Shorter	1/15/2014	Version 1.0 of the document
1.0	Sachin Agnihotri	1/17/2014	Version 1.0 review and updates

TABLE OF CONTENTS

1 INTRODUCTION

1.1 PURPOSE

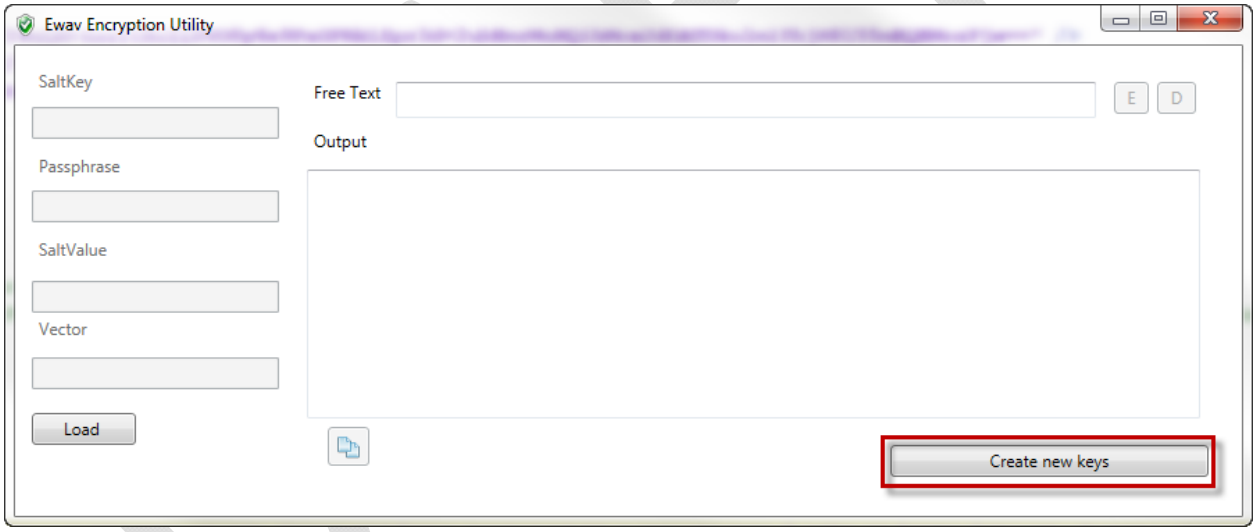
The purpose of this document is to provide an overview of the key functionalities of the Epi Info™ Web Analytics and Visualization (EWAV) Encryption Utility. This document goes hand in hand with the EWAV deployment document. The configuration of EWAV on the web server cannot be completed without this document.

1.2 AUDIENCE

The audience for this document is an Administrator, a Manager or a person responsible for managing the EWAV system.

2 WORFLOW 1 – CREATE KEYS FOR A NEW INSTALLATION

Step 1 – Click the “create new keys” button in EWAV Encryption Utility



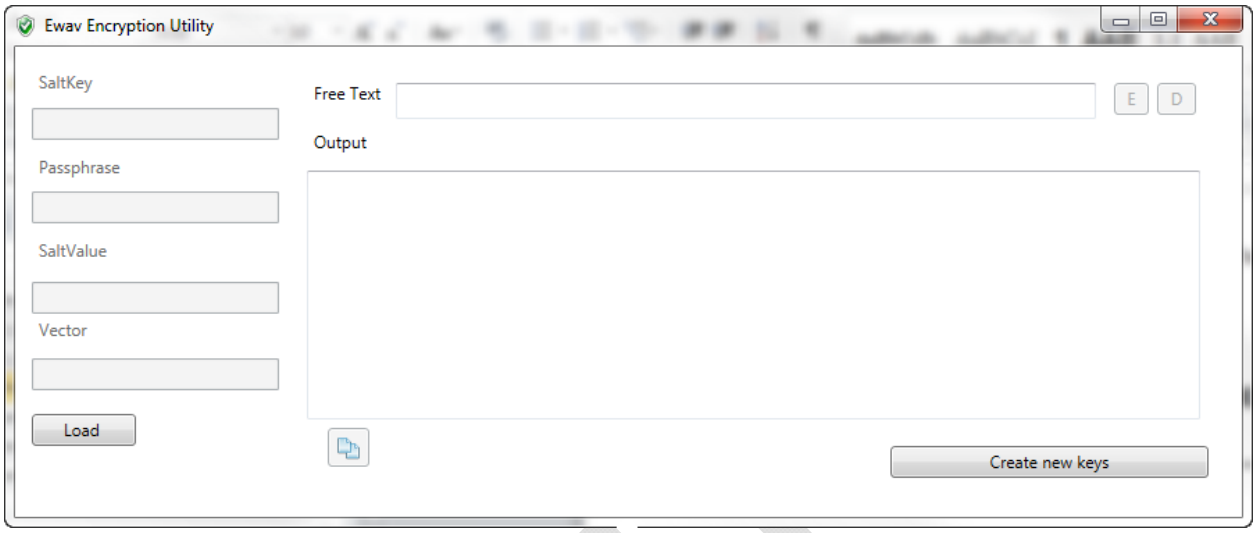
Step 2 - The keys and entries for web.config are generated and displayed in Output textbox.

Step 3 – Copy the newly created section to the application's web.config file by clicking on the Copybutton located in the lower left corner of the dialog box .

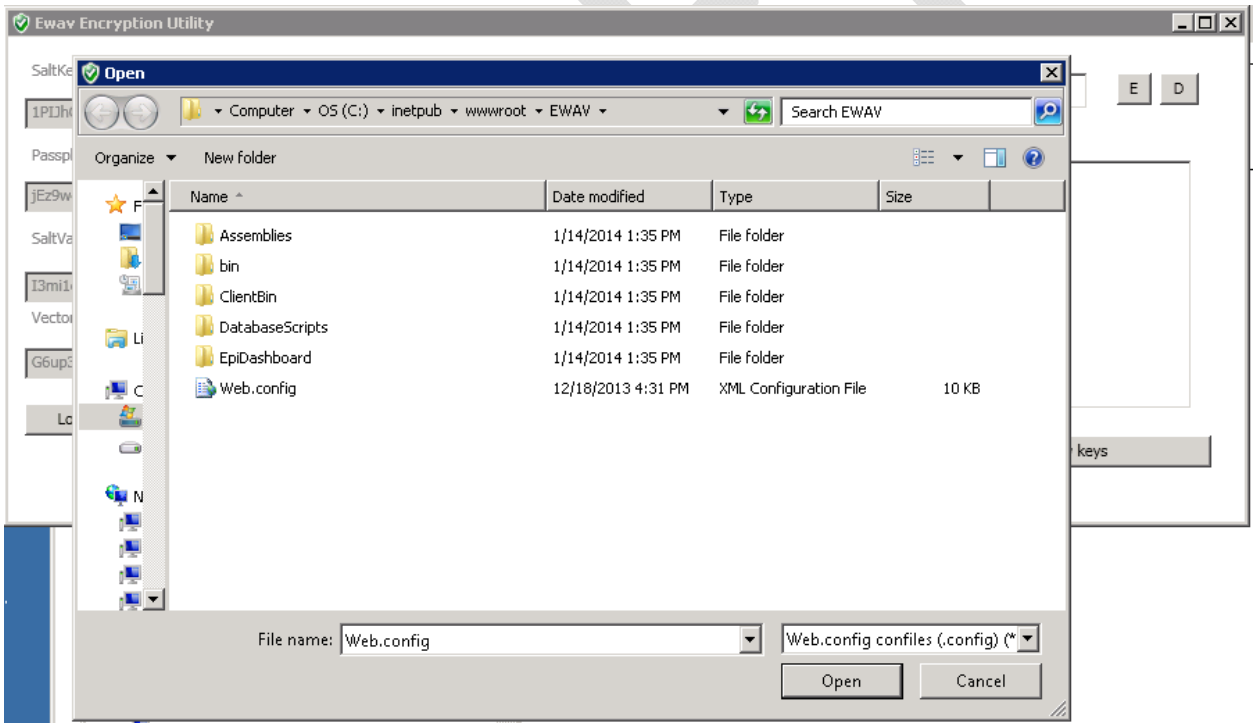
Step 4 – Update the Encryption Keys section of the web.config file with the copied text.

3 WORKFLOW 2 - LOAD KEYS FROM EXISTING WEB.CONFIG

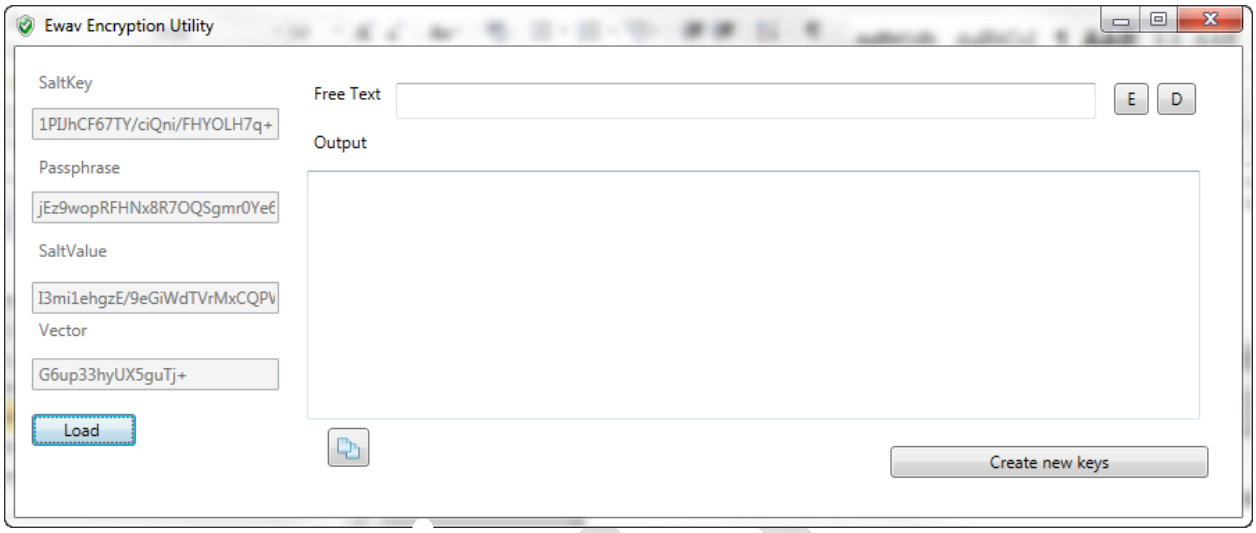
Step 1 – Click the "Load" button



Step 2 – Browse to an existing Ewav web.config file. This should be the location of EWAV on the web server at “inetpub\wwwroot\Ewav”



Step 3 – Click “Open”. The EWAV Encryption Utility will read the existing keys and populate the SaltKey, Passphrase, SaltValue and Vector text box which are disabled.

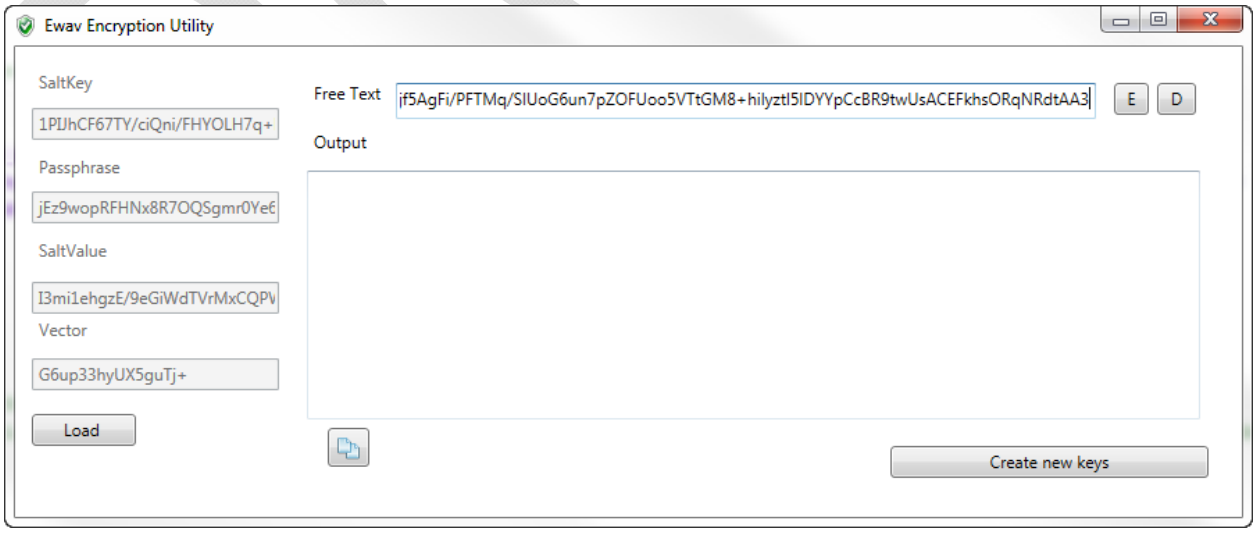


4 WORFLOW 3 - AD-HOC DECRYPT

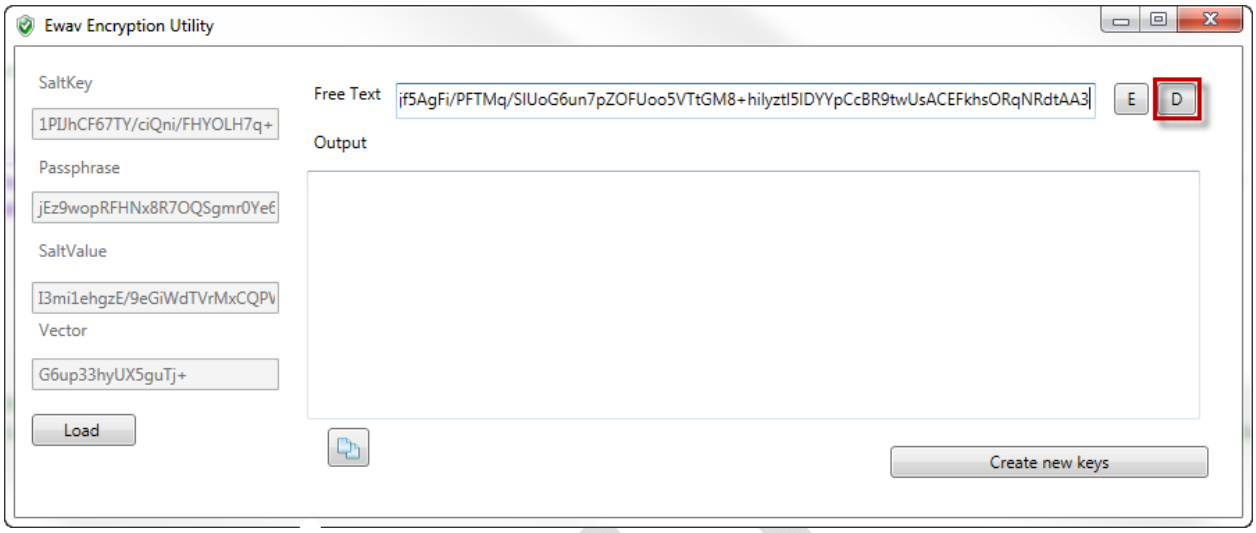
This functionality can be used to decrypt the connection string in the web.config file in case the application is not able to connect to the database. After decryption the connection string can be inspected and updated as needed to resolve database connection problem.

Step 1 – Follow steps of workflow 2

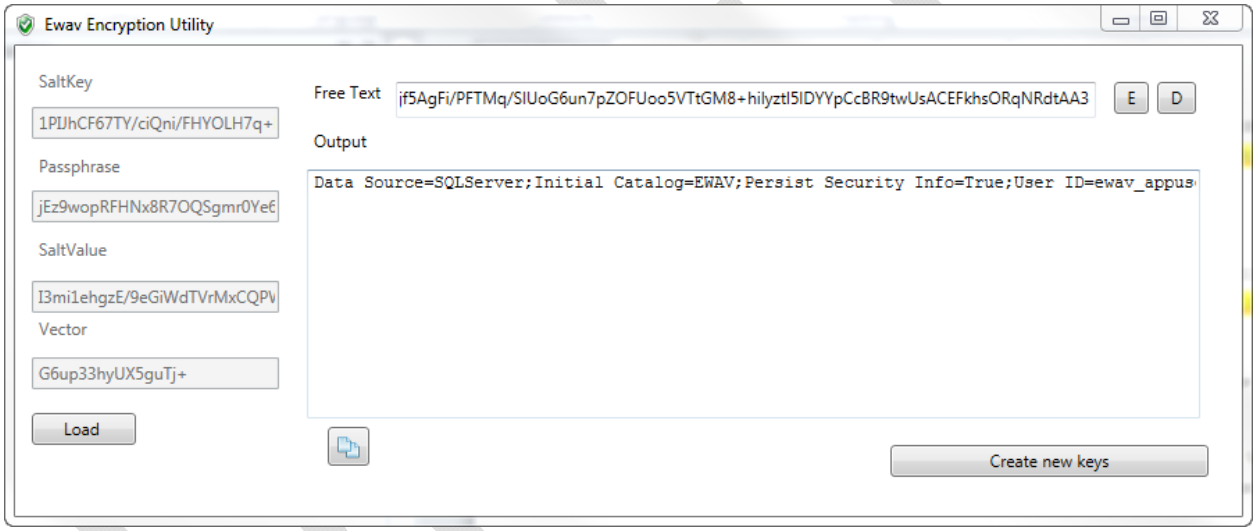
Step 2 – Paste a string that was encrypted with the loaded keys into the “Free text” text box



Step 3 – Click the “D” button



Step 4 – Use the Decrypted string provided in output textbox to debug the issues if any encountered during the application configuration

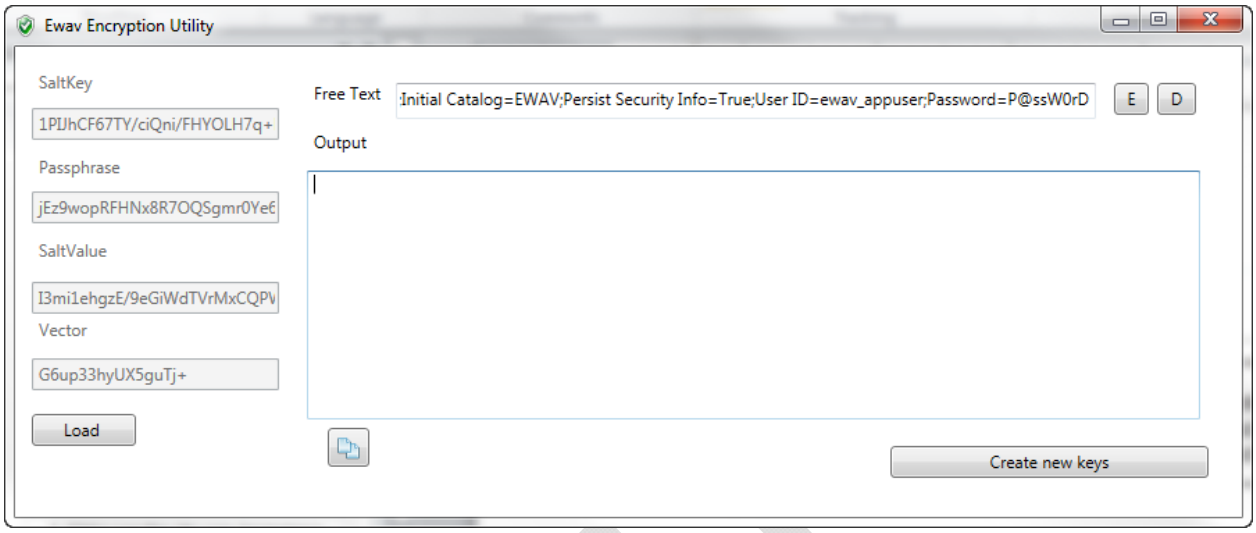


5 WORKFLOW 4 – AD-HOC ENCRYPT

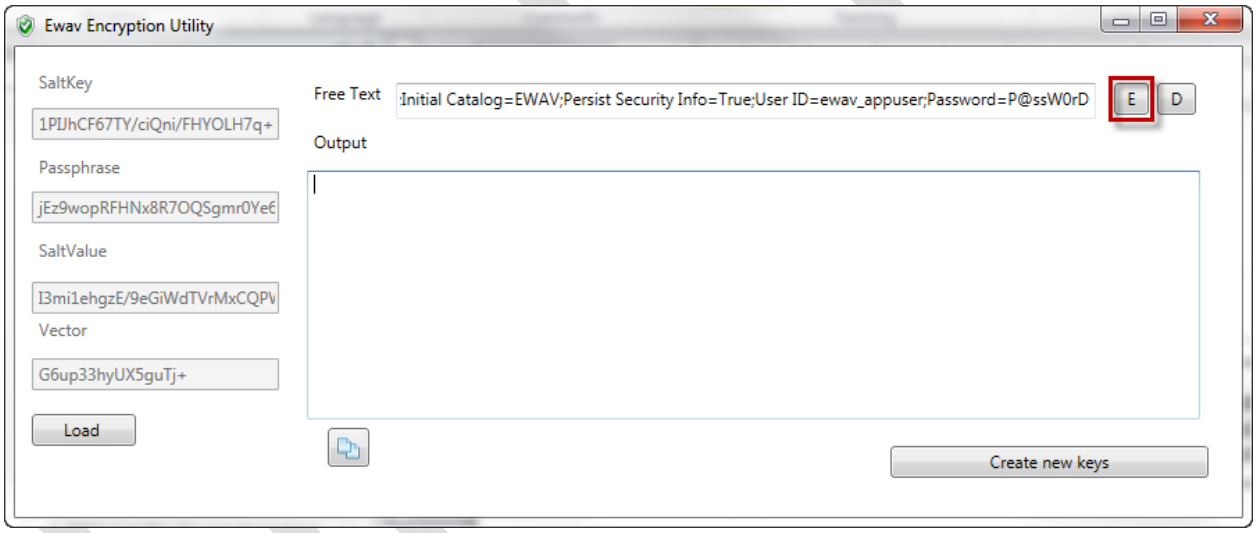
This functionality is to be used to encrypt the connection string for the database type applicable to your organization. Once encrypted update the sample encrypted connection string provided in the web.config file for the database type that is relevant for your deployment.

Step 1 – Follow steps of workflow 2

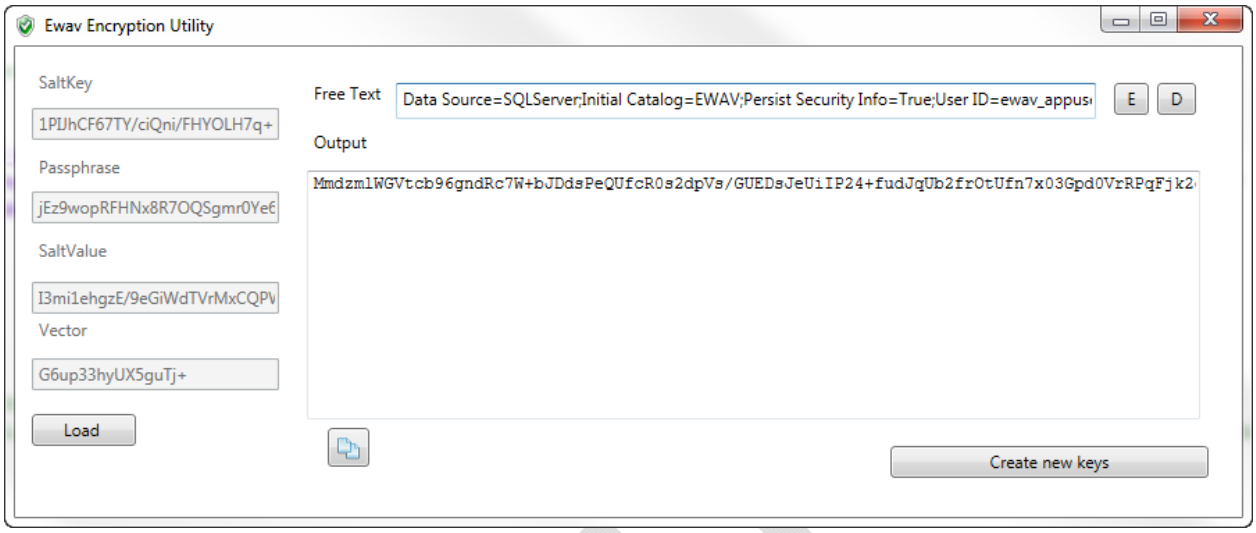
Step 2 – Paste an unencrypted string into the “Free text” text box



Step 3 – Click the "E" button



Step 4 – Use the Encrypted string provided in output textbox to update the relevant connection string for your database type section in the web.config file.


Ewav Encryption Utility
SaltKey
1PlJhCF67TY/ciQni/FHYOLH7q+
Passphrase
jEz9wopRFHNx8R7OQSgmr0Ye6
SaltValue
I3mi1ehgzE/9eGiWdTVrMxCQPv
Vector
G6up33hyUX5guTj+
Load
Free Text
Data Source=SQLServer;Initial Catalog=EWAV;Persist Security Info=True;User ID=ewav_appus
E
D
Output
MmdzmlWGVtcb96gndRc7W+bJDdsPeQUfcR0s2dpVs/GUEDsJeUiIP24+fudJqUb2frOtUfn7x03Gpd0VrRPqFjk2
Create new keys