



EPI INFO™ WEB ANALYTICS AND VISUALIZATION DEPLOYMENT GUIDE

Version 1.0
05/08/2014

VERSION HISTORY

Version #	Implemented By	Revision Date	Comments
1.0	Mohammad Usman, Daniel Shorter, Sachin Agnihotri	09/25/2012	Version 1.0 of the document
1.0	Mohammad Usman, Daniel Shorter, Sachin Agnihotri	01/17/2014	Review and updates to Version 1.0 of the document
1.0	Sachin Agnihotri	03/12/2014	Updates to Version 1.0 of the document
1.0	Sachin Agnihotri	05/08/2014	Updates to Version 1.0 of the document

TABLE OF CONTENTS

1. INTRODUCTION	4
1.1 PURPOSE	4
1.2 AUDIENCE	4
2. SYSTEM DESCRIPTION	4
2.1 KEY FEATURES.....	4
2.2 INVENTORY	5
2.3 ENVIRONMENT	5
2.4 SYSTEM OPERATIONS	6
2.5 SYSTEM ARCHITECTURE	6
3. APPLICATION INSTALLATION	10
3.1 PREREQUISITES.....	10
3.2 ACCESS CONTROLS	10
3.3 INSTALLATION.....	10
3.4 CONFIGURATION.....	11
APPENDIX A: REFERENCES.....	53
APPENDIX B: TABLE OF FIGURES.....	54

1. INTRODUCTION

1.1 PURPOSE

Epi Info™ Web Analytics & Visualization is an open source project in the popular Epi Info™ suite of tools. The web product can be deployed as an internet or intranet application and will provide analytical and visualization capability for large public health datasets within an organization. The product will also provide a collection of relevant public health related tools that can be used by Epidemiologists or other public health professionals to analyze data.

1.2 AUDIENCE

The audience for this document includes system administrators, database administrators, and information technology personnel who will be configuring the system on web and database servers.

The person creating and configuring the database should have full administrative access to the database server and rights and privileges to create a database, create database users, and grant access to the database.

2. SYSTEM DESCRIPTION

2.1 KEY FEATURES

The Epi Info™ Web Analytics & Visualization system enables the following functionalities on the web:

- **Dashboard functionality on Web:** Provides Epi Info™ 7 dashboard-like functionality, enabling users to use gadgets, charts and calculators via the Web.
- **Configuration for Windows- and Form-based Authentication:** System Administrators have a choice to choose the mode of the deployment.
- **Admin tools:** Provides the means for administrators to create users, control user access, create connections to different data sources, and in some cases, create more organizations.
 - o **Role-based access to application features:** Application features available to a user are determined by their role which is one of super administrator, administrator and user.
 - o **Encapsulated working environment:** Users from one organization can work on data sources in isolation from other groups.
 - o **Creation of data sources:** Admins have authority to create data sources for the users.
- **Capability of Saving/Opening Canvas:** Users can save canvases with selected gadgets, data sources and layouts; then open them later in the previously saved state.

2.2 INVENTORY

The deployment package consists of a compressed folder structure having three sub folders namely: Database, Application and Documents. The database scripts are present in the Database folder. All files needed for deployment of the web product are provided in Application folder. All the documentation for the web product is present in Documents folder.

2.3 ENVIRONMENT

Below is a list of hardware and software requirements, and operational activities needed for the deployment of the Epi Info™ Web Analytics & Visualization system:

Hardware:

- Web server: Windows server 2008 or Windows Server 2008 R2
- Database server: Windows Server 2008 or Windows Server 2008 R2

Note: The system is designed to do all the processing and computations on the server. You will have to plan for server capacity depending on the size of data sources you plan to use and the number of user expected to be use the system.

Software:

- Web server:
 - Internet Information Services (IIS) 7.0 / 7.5
 - .NET 4.0
 - Microsoft Silverlight 5.0
- Database server
 - SQL Server 2008
 - PostgreSQL 9.1 and later
 - MySql
- Client
 - Microsoft Silverlight 5.0 runtime
- SMTP Server
 - The application would need to know the name of an SMTP server within the network that it can use.

Operational activities:

- A system engineer, IT engineer with administrative access on the web server configures the application.
- A database administrator with administrative access on the database server configures the database. This application can be configured for SQL Server 2008, MySql or PostgreSQL 9.1 or later.

2.4 SYSTEM OPERATIONS

The system will be used for:

- Creating Gadgets, Charts and Calculators.
- Saving Gadgets and Charts on canvas.
- Opening the saved canvas and sharing with others
- Defining organization that will be using the system
- Defining data sources to be used by the product
- Defining users in the organization that will use the system and the data sources they have access to.

2.5 SYSTEM ARCHITECTURE

The system comprises a web application where the user will be able to choose the dataset they want to analyze. Once the dataset is chosen, the Public Health user can choose from any number of visualization gadgets and/or charts to start analyzing the data. Behind the scenes, the user interface interacts with a web service that does all the processing, and returns the computed data back to the user interface to be displayed. The web service interacts with a Meta database that has information on how to connect to various databases that a data mart, a data warehouse or a database server may allow access to for analysis.

The diagram below summarizes these components and their interactions.

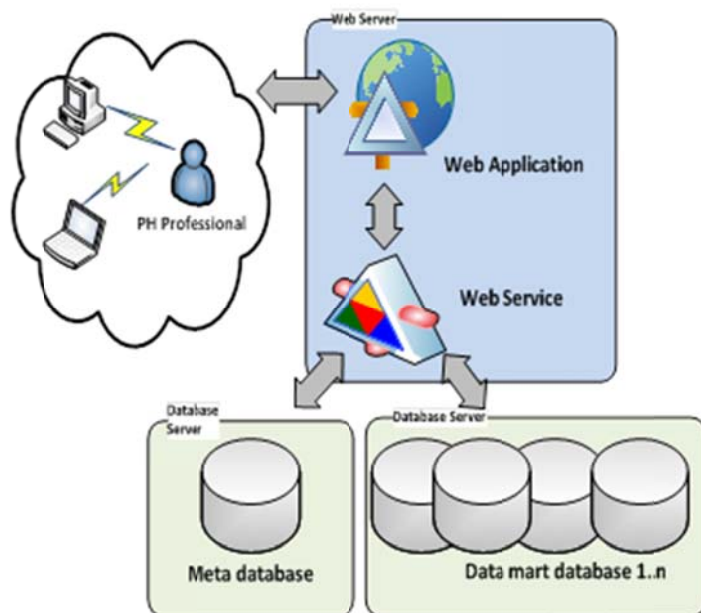


Figure 1: Overview of Epi Info™ Web Analytics & Visualization

The product may be configured for usage as a public facing internet application or as an intranet application within an organization's network, behind the firewall. The diagram below shows the configuration for the product deployed as an intranet application.

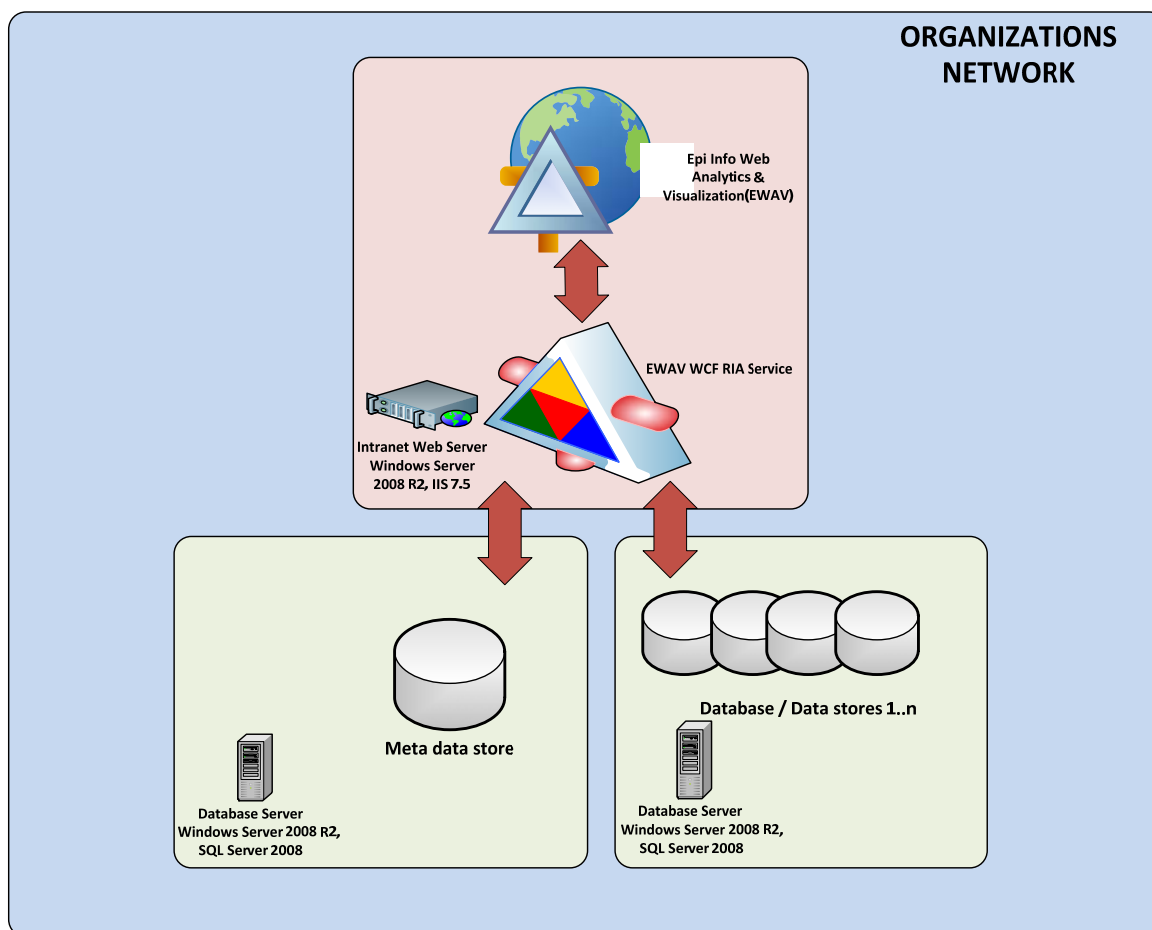


Figure 2: Intranet Configuration

The diagram below show the configuration for the product deployed as an internet application.

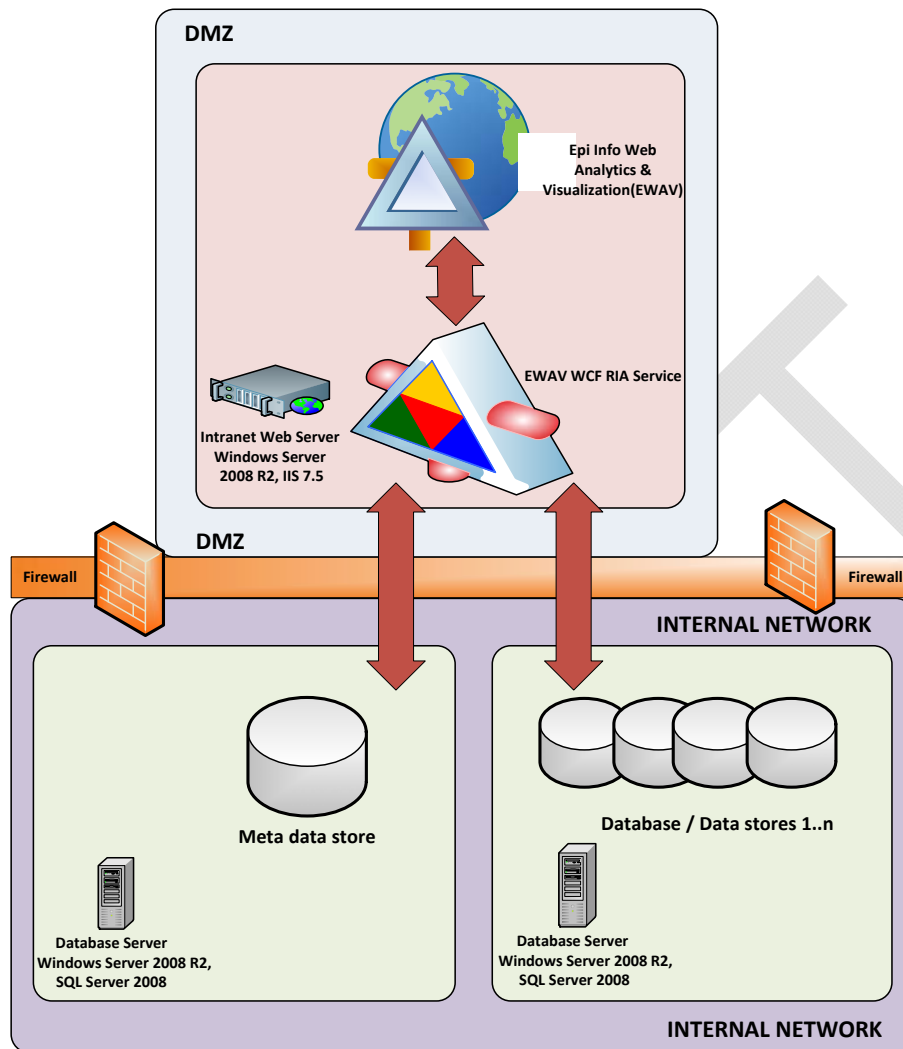


Figure 3: Internet Configuration

3. APPLICATION INSTALLATION

3.1 PREREQUISITES

In order to use the Epi Info™ Web Analytics & Visualization (EWAV) system, encryption keys must be created. These encryption keys are used to encrypt the meta database connection string, external database connection strings, and user passwords. For instructions on how to create these keys, refer to the “EWAV Encryption Utility Help” document included in the Documents folder of this package.

3.2 ACCESS CONTROLS

3.2.1 Database

The person creating and configuring the database should have full administrative access on the database server and rights and privileges to create a database, create database users, and grant access to the database.

3.2.2 Application and Services

The person installing and configuring the application and services should have administrative access on the web server and should have full access and privileges to create a web application in Internet Information Services (IIS).

3.3 INSTALLATION

The installation can be done using the **EWAV** package. The package for installation of the system consists of three items: 1) the database in the **Database** folder; 2) the application and services in the **Application** folder; and 3) the required documentation in the **Documents** folder. The Configuration section describes how these items are used.

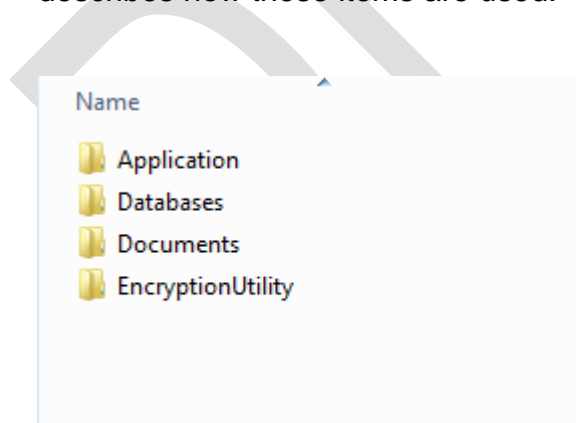


Figure 4: File system showing components in the EWAV Package

3.4 CONFIGURATION

3.4.1 Database Configuration

The deployment package comes with “Databases” folder containing scripts to configure three types of databases namely SQL Server, MySQL and PostgreSQL. Choose the script for database type to configure as per your organizations need. Scripts provided in this package are for deploying the metadata database needed by the application. The instructions for configuring different database types are provided in three sub sections following this section:

- Setting up SQL Server metadata database – Section 3.4.1.1
- Setting up MySQL metadata database – Section 3.4.1.2
- Setting up PostgreSQL metadata database – Section 3.4.1.3

3.4.1.1 Set up EWAV for SQL Server

1. Log in to the database server using an account which has administrative privileges to create the database.
2. Open the provided script name “01CreateSchema.sql” in SQL Server Management Studio.

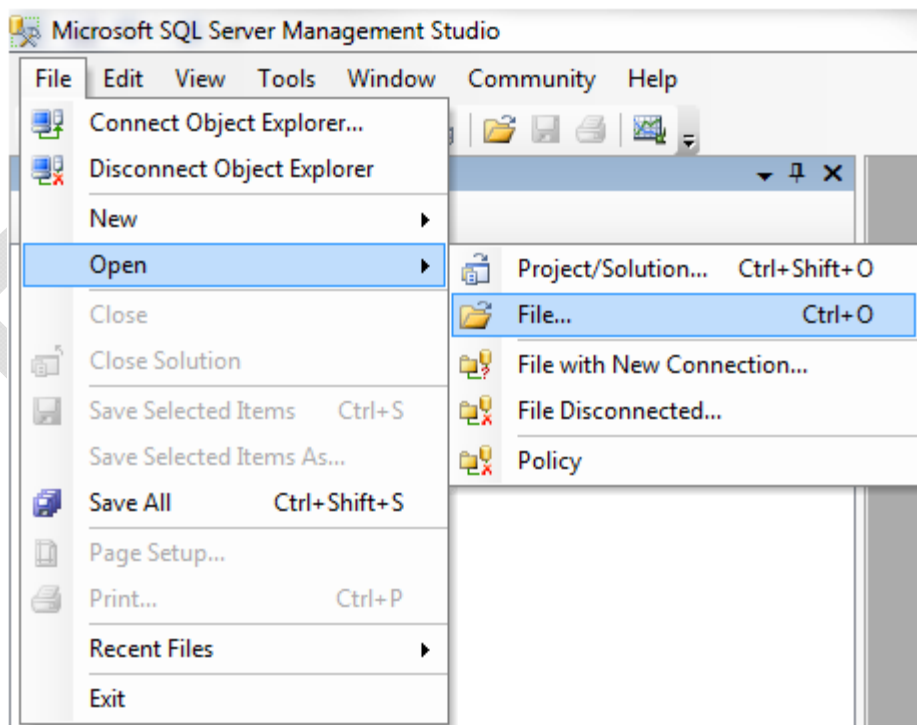


Figure 5: File menu to open the database script file for SQL Server

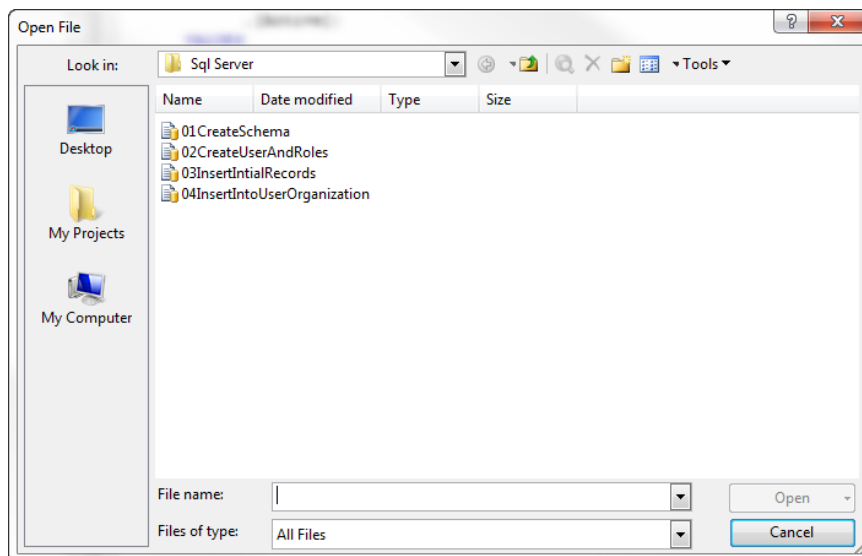


Figure 6: Open File dialog showing the available script for SQL Server.

3. Execute the script 01CreateSchema to create the database and the schema for the database.

```
USE [master]
GO

/***** Object: Database [EWAV] Script Date: 01/17/2014 10:13:24 *****/
CREATE DATABASE [EWAV] ON PRIMARY
( NAME = N'EWAV', FILENAME = N'D:\Databases\EWAV_new.mdf' , SIZE = 23552KB , MAXSIZE = UNLIMITED, FILEGROWTH = 1024K
LOG ON
( NAME = N'EWAV_log', FILENAME = N'D:\Databases\EWAV_new_log.ldf' , SIZE = 219264KB , MAXSIZE = 2048GB , FILEGROWTH
GO

ALTER DATABASE [EWAV] SET COMPATIBILITY_LEVEL = 100
GO

IF (1 = FULLTEXTSERVICEPROPERTY('IsFullTextInstalled'))
begin
EXEC [EWAV].[dbo].[sp_fulltext_database] @action = 'enable'
end
GO

ALTER DATABASE [EWAV] SET ANSI_NULL_DEFAULT OFF
```

Figure 7: Snapshot of a portion of 01CreateSchema script for SQL Server

Note: If you receive an error at this point upon execution, check to see if your hard-coded paths (tied directly to your machine) have the appropriate path pointing to the location where databases are created.

4. Open Script titled “02CreateUserAndRoles”. Replace the Password with a strong password that meets your organization’s password policy. Execute the script. This will create the Application User Account and will grant execute permissions on stored procedures.

```

-----Create Database User And Role

USE [ EWAV ]

GO

CREATE LOGIN [EWAV_APPUSER ] WITH PASSWORD=N'P@ssW0rd', DEFAULT_DATABASE=[EWAV ],
    DEFAULT_LANGUAGE=[us_english], CHECK_EXPIRATION=OFF, CHECK_POLICY=OFF

GO

CREATE USER [EWAV_APPUSER ] FOR LOGIN [EWAV_APPUSER ] WITH DEFAULT_SCHEMA=[dbo]

GO

GRANT EXECUTE ON SCHEMA :: dbo TO [EWAV_APPUSER ];

GO

CREATE ROLE [db_procexec] AUTHORIZATION [dbo]

GO

EXEC dbo.sp_addrolemember @rolename=N'db_procexec', @membername=N'EWAV_APPUSER'

GO

EXEC dbo.sp_addrolemember @rolename=N'db_datareader', @membername=N'EWAV_APPUSER'

GO

EXEC dbo.sp_addrolemember @rolename=N'db_datawriter', @membername=N'EWAV_APPUSER'

GO

```

Figure 8: Snapshot of a portion of 02CreateUserAndRoles script for SQL Server

Note: EWAV_APPUSER is the application account that is used by the application to connect to the database. Provide username and the password to the person configuring the application on the web server along with the Database server name and the Database name.

5. Open script “03InsertInitialRecord”. This script will add initial records for the system to work. It adds the roles used by the product; creates the Super Administrator user; and first organization. Before executing the script, you must update the sections marked in red, “Inserting Super Administrator user” and “Organization”. For Super Administrator, replace following placeholders with relevant values:

- /*UserName*/
 - UserName has to be valid Email address. For Windows deployed mode, this email has to be the part of Active Directory.

- /*FirstName*/
- /*LastName*/
- /*EmailAddress*/
- /*PhoneNumber*/

For Organization, replace following placeholders with relevant values:

- /*OrganizationName*/
- /*Description*/ - This is optional

```

----- Insert Ewav Roles -----

USE [EWAV]
GO
/***** Object: Table [dbo].[Role]      Script Date: 08/19/2013 13:52:59 *****/
SET IDENTITY_INSERT [dbo].[Role] ON
INSERT [dbo].[Role] ([RoleID], [RoleValue], [RoleDescription]) VALUES (1, 1, N'Analyst')
INSERT [dbo].[Role] ([RoleID], [RoleValue], [RoleDescription]) VALUES (2, 2, N'Administrator')
INSERT [dbo].[Role] ([RoleID], [RoleValue], [RoleDescription]) VALUES (4, 4, N'SuperAdministrator')
SET IDENTITY_INSERT [dbo].[Role] OFF

----- Insert Super Administrator User -----
INSERT INTO [EWAV].[dbo].[User]
    ([UserName]
    , [FirstName]
    , [LastName]
    , [PasswordHash]
    , [ResetPassword]
    , [EmailAddress]
    , [PhoneNumber])
VALUES
    (/*UserName*/,
    /*FirstName*/,
    /*LastName*/,
    '',
    1,
    /*EmailAddress*/,
    /*PhoneNumber*/)
GO

----- Insert Organization -----
INSERT INTO [EWAV].[dbo].[Organization]
    ([OrganizationName]
    , [Description]
    , [Active])
VALUES
    (/*OrganizationName*/,
    /*Description*/,
    1)
GO

```

Figure 9: Snapshot of a portion 03InsertInitialRecord script for SQL Server

Sample script is provided below:

```

INSERT INTO [EWAV].[dbo].[User]
    ([UserName]
    ,[FirstName]
    ,[LastName]
    ,[PasswordHash]
    ,[ResetPassword]
    ,[EmailAddress]
    ,[PhoneNumber])
VALUES
    ('useremail@org.gov'
    ,'UserFirstName'
    ,'UserLastName'
    ,''
    ,1
    ,'useremail@org.gov'
    ,'111-111-1111')
GO

INSERT INTO [EWAV].[dbo].[Organization]
    ([OrganizationName]
    ,[Description]
    ,[Active])
VALUES
    ('Organization Name'
    ,'Description'
    ,1)
GO

```

6. Open script “04InsertIntoUserOrganization”. This script creates the relationship between User and Organization for the recently added Super Administrator and Organization. The first user is being assigned the role of Super Administrator, which has a RoleId of 4. To execute the script replace following placeholders with relevant values:

- /*UserID*/
- /*OrganizationID*/

```

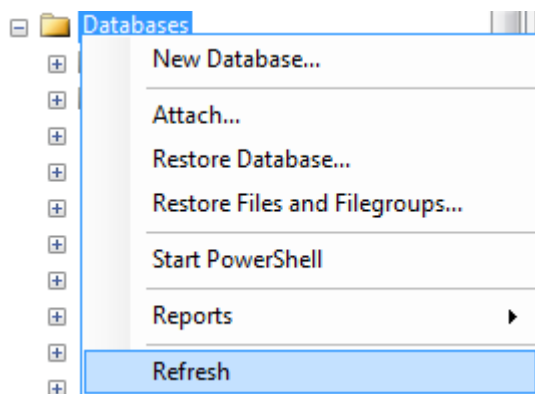
INSERT INTO [EWAV].[dbo].[UserOrganization]
    ([UserID]
    ,[OrganizationID]
    ,[RoleID]
    ,[Active])
VALUES
    (/*UserID*/
    ,/*OrganizationID*/
    ,4
    ,1)
GO

```

Figure 10: Snapshot of a portion 04InsertIntoUserOrganization script for SQL Server

Value of UserID can be retrieved by opening the User table. Value of OrganizationID can be retrieved by opening the Organization table

Note: - If database is not visible, Right click the Databases folder and click Refresh. It should appear.



Sample script is provided below:

```
INSERT INTO [EWAV].[dbo].[UserOrganization]
    ([UserID]
    ,[OrganizationID]
    ,[RoleID]
    ,[Active])
VALUES
    (1
    ,1
    ,4
    ,1)
GO
```


Set up EWAV for MySQL

1. Log in to the database server using an account which has admin privileges to create the database.
2. Open the provided script namely “01CreateSchema.sql” in MySQL Workbench

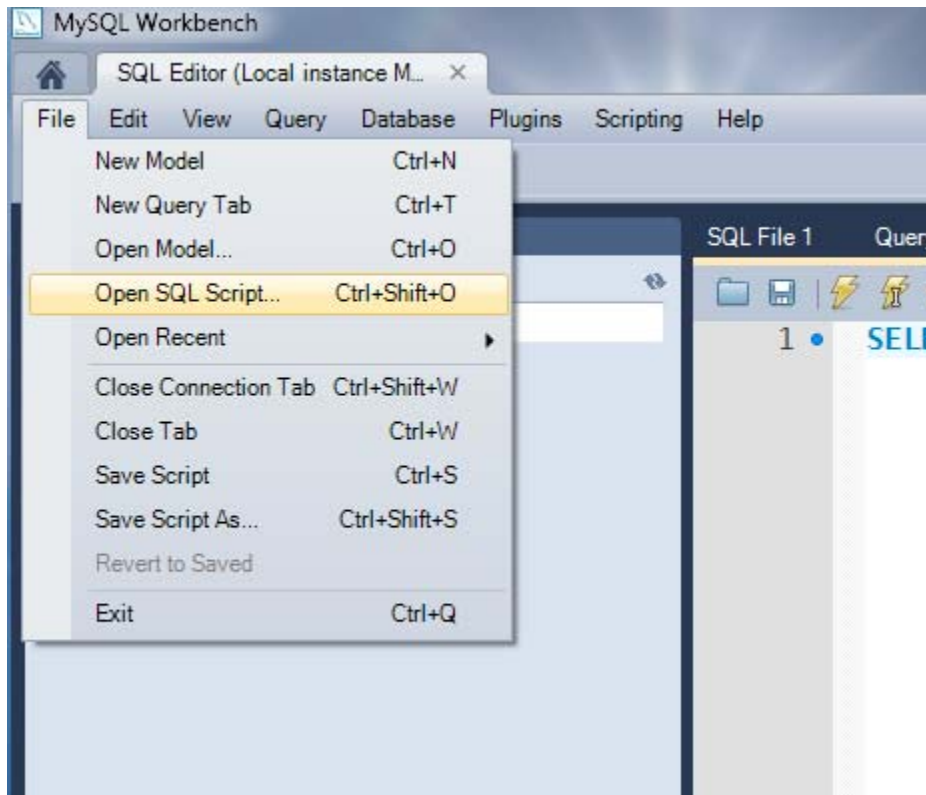


Figure11: File menu to open the database script file for MySQL

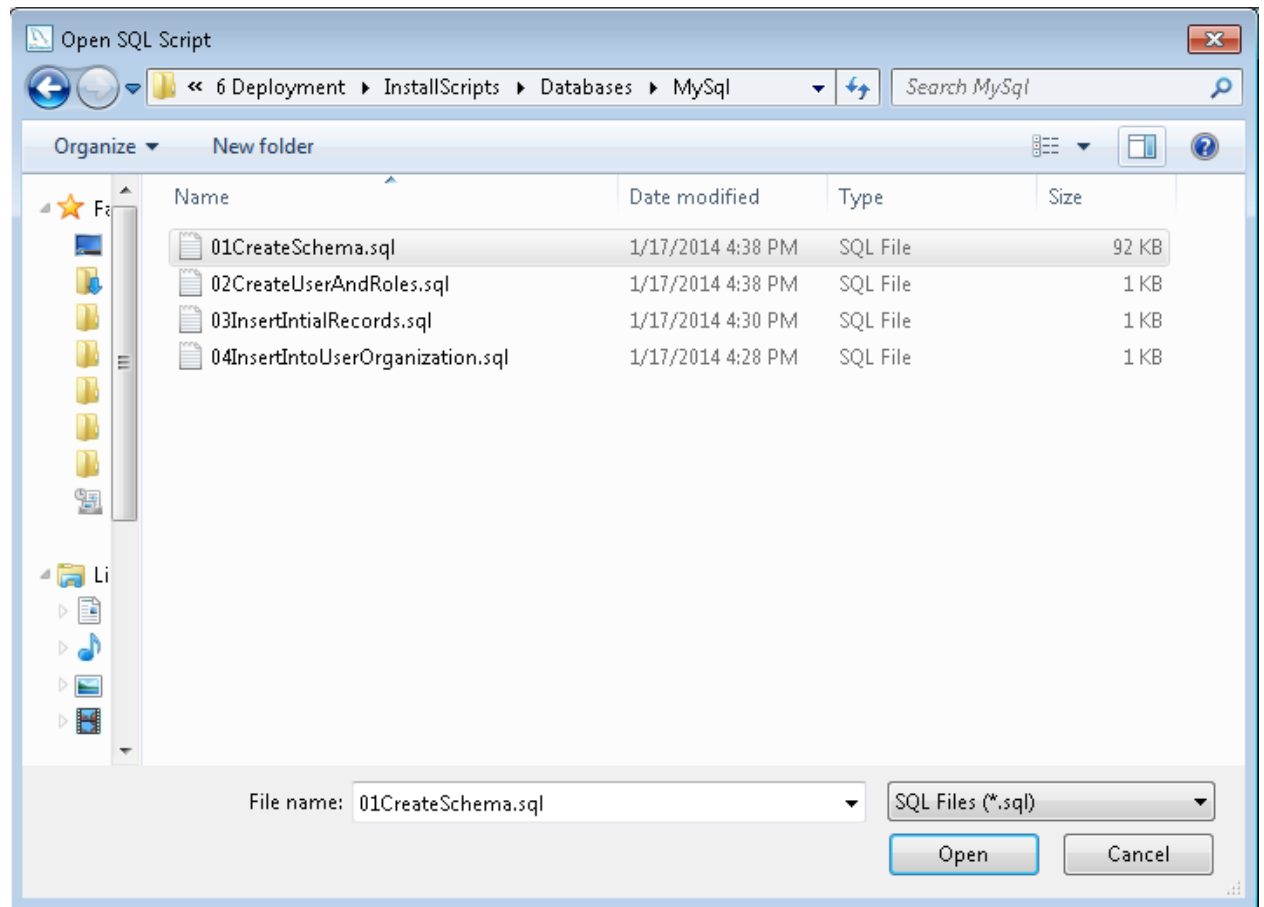
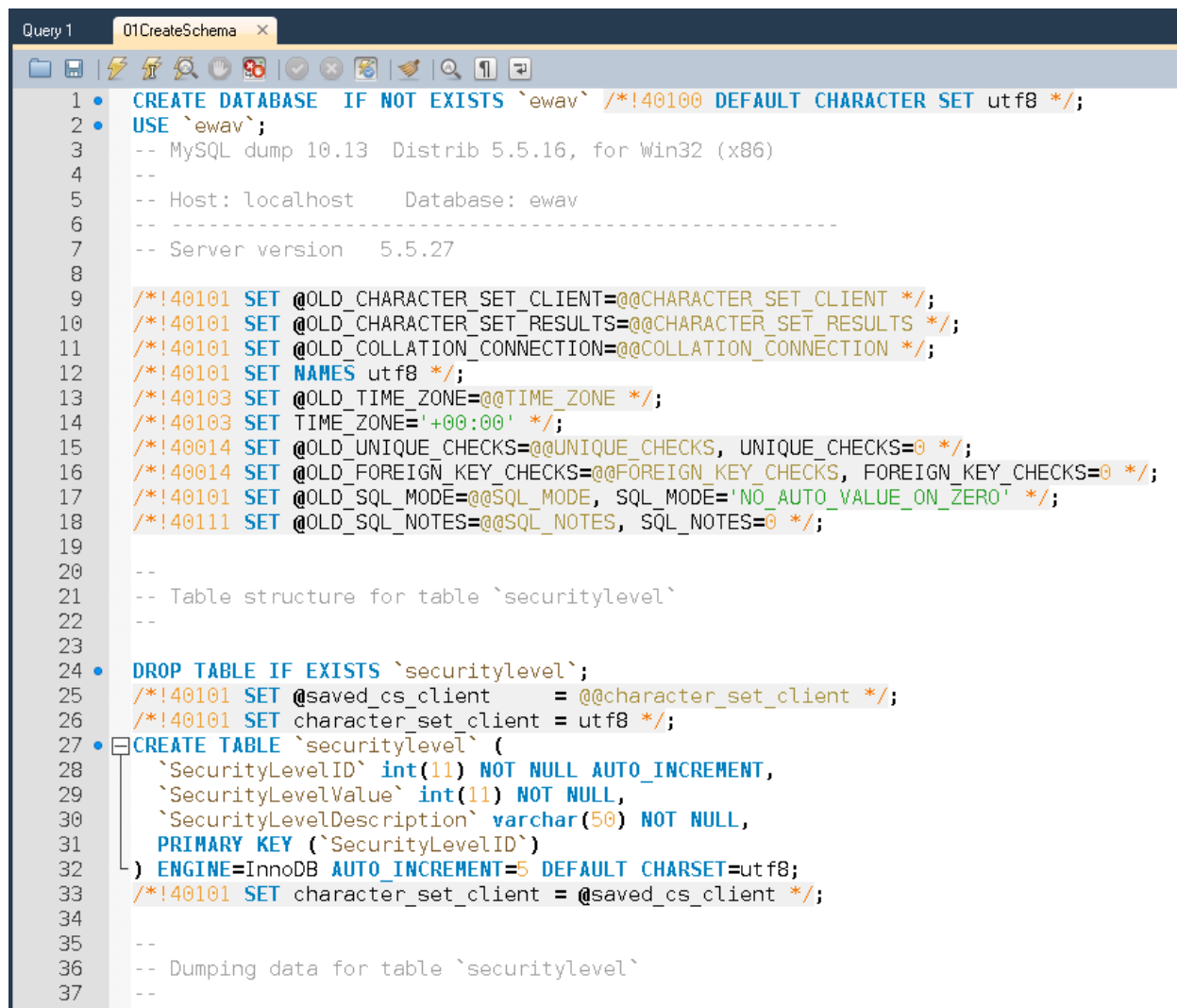


Figure 12: Open File dialog showing the available script for MySQL

3. Execute the script "01CreateSchema" to create the database and the schema for the database



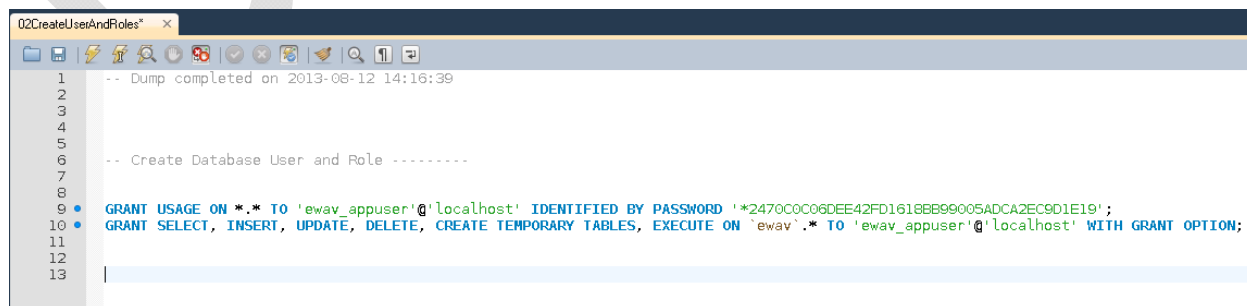
```

Query 1    01CreateSchema
1  CREATE DATABASE IF NOT EXISTS `ewav` /*!40100 DEFAULT CHARACTER SET utf8 */;
2  USE `ewav`;
3  -- MySQL dump 10.13  Distrib 5.5.16, for Win32 (x86)
4  --
5  -- Host: localhost    Database: ewav
6  --
7  -- Server version  5.5.27
8  --
9  /*!40101 SET @OLD_CHARACTER_SET_CLIENT=@@CHARACTER_SET_CLIENT */;
10 /*!40101 SET @OLD_CHARACTER_SET_RESULTS=@@CHARACTER_SET_RESULTS */;
11 /*!40101 SET @OLD_COLLATION_CONNECTION=@@COLLATION_CONNECTION */;
12 /*!40101 SET NAMES utf8 */;
13 /*!40103 SET @OLD_TIME_ZONE=@@TIME_ZONE */;
14 /*!40103 SET TIME_ZONE='+00:00' */;
15 /*!40014 SET @OLD_UNIQUE_CHECKS=@@UNIQUE_CHECKS, UNIQUE_CHECKS=0 */;
16 /*!40014 SET @OLD_FOREIGN_KEY_CHECKS=@@FOREIGN_KEY_CHECKS, FOREIGN_KEY_CHECKS=0 */;
17 /*!40101 SET @OLD_SQL_MODE=@@SQL_MODE, SQL_MODE='NO_AUTO_VALUE_ON_ZERO' */;
18 /*!40111 SET @OLD_SQL_NOTES=@@SQL_NOTES, SQL_NOTES=0 */;
19
20 --
21 -- Table structure for table `securitylevel`
22 --
23
24 DROP TABLE IF EXISTS `securitylevel`;
25 /*!40101 SET @saved_cs_client = @@character_set_client */;
26 /*!40101 SET character_set_client = utf8 */;
27 CREATE TABLE `securitylevel` (
28   `SecurityLevelID` int(11) NOT NULL AUTO_INCREMENT,
29   `SecurityLevelValue` int(11) NOT NULL,
30   `SecurityLevelDescription` varchar(50) NOT NULL,
31   PRIMARY KEY (`SecurityLevelID`)
32 ) ENGINE=InnoDB AUTO_INCREMENT=5 DEFAULT CHARSET=utf8;
33 /*!40101 SET character_set_client = @saved_cs_client */;
34
35 --
36 -- Dumping data for table `securitylevel`
37 --

```

Figure 13: Snapshot showing portion of 01CreateSchema script for MySQL

4. Open Script titled “02CreateUserAndRoles”. Execute the script. This will create the Application User Account and will grant needed permissions.



```

02CreateUserAndRoles
1  -- Dump completed on 2013-08-12 14:16:39
2
3
4
5
6  -- Create Database User and Role -----
7
8
9  GRANT USAGE ON *.* TO 'ewav_appuser'@'localhost' IDENTIFIED BY PASSWORD '*2470C0C06DEE42FD1618BB99005ADCA2EC9D1E19';
10 GRANT SELECT, INSERT, UPDATE, DELETE, CREATE TEMPORARY TABLES, EXECUTE ON `ewav`.* TO 'ewav_appuser'@'localhost' WITH GRANT OPTION;
11
12
13

```

Figure 14: Snapshot showing portion of 02CreateUserAndRoles script for MySQL

After executing the script, change the password for “ewav_appuser” account using Server Administration. Provide the “ewav_appuser” username, the password, server name and database name to the person configuring the web application.

Note: EWAV_APPUSER is the application account that is used by the application to connect to the database. Provide username and the password to the person configuring the application on the web server along with the Database server name and the Database name.

5. Open script “03InsertInitialRecord”. This script will add initial records for the system to work. It adds the roles used by the product; creates the Super Administrator user; and first organization. Before executing the script update sections marked in red for Inserting Super Administrator user and Organization. For Super Administrator replace following placeholders with relevant values:

- /*UserName*/
 - UserName has to be valid Email address. For Windows deployed mode, this email has to be the part of Active Directory.
- /*FirstName*/
- /*LastName*/
- /*EmailAddress*/
- /*PhoneNumber*/

For Organization replace following placeholders with relevant values:

- /*OrganizationName*/
- /*Description*/ - This is optional

```
-- Insert Ewav Roles -----
USE ewav;

INSERT INTO `ewav`.`Role` (RoleID , RoleValue , RoleDescription ) VALUES (1, 1, 'Analyst');
INSERT INTO `ewav`.`Role` (RoleID , RoleValue , RoleDescription ) VALUES (2, 2, 'Administrator');
INSERT INTO `ewav`.`Role` (RoleID , RoleValue , RoleDescription ) VALUES (4, 4, 'SuperAdministrator');

-- Insert Super Administrator --
INSERT INTO `ewav`.`User`
  (UserName
  ,FirstName
  ,LastName
  ,PasswordHash
  ,ResetPassword
  ,EmailAddress
  ,PhoneNumber )
VALUES
  (/*UserName*/x,
  /*FirstName*/x,
  /*LastName*/x,
  'x',
  1,
  /*EmailAddress*/x,
  /*PhoneNumber*/x);

-- Insert Organization --
INSERT INTO `ewav`.`Organization`
  (OrganizationName
  ,Description
  ,Active )
VALUES
  (/*OrganizationName*/x,
  /*Description*/x,
  1);
```

Figure 15: Snapshot showing portion of 03InsertInitialRecord script for MySQL

Sample script is provided below:

```
INSERT INTO `ewav`.`user`
  (`EmailAddress`,
  `FirstName`,
  `LastName`,
  `PasswordHash`,
  `PhoneNumber`,
  `ResetPassword`,
  `UserID`,
  `UserName`)
VALUES
  (
  'useremail@org.gov',
  'UserFirstName',
  'UserLastName',
  'x',
  '111-111-1111',
  1,
```

```
'useremail@org.gov',
'UserName'
);
```

```
INSERT INTO `ewav`.`organization`
(`Active`,
`Description`,
`OrganizationID`,
`OrganizationName`)
VALUES
(
1,
'Description',
1,
'Organization Name'
);
```

6. Open script “04InsertIntoUserOrganization”. This script creates the relationship between User and Organization for the recently added Super Administrator and your Organization. The first user is being assigned the role of Super Administrator that has a RoleId of 4. To execute the script replace following placeholders with relevant values:

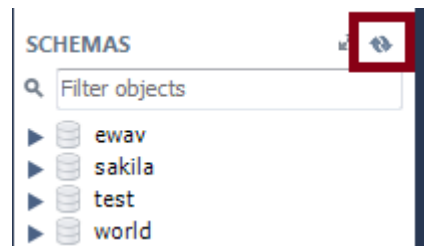
- /*UserID*/
- /*OrganizationID*/

```
INSERT INTO `ewav`.`userorganization`
(`Active`,
`OrganizationID`,
`RoleID`,
`UserID`)
VALUES
(
1,
/*OrganizationID*/,
4,
/*UserID*/
);
```

Figure 16: Snapshot showing portion of 04InsertInitialRecord script for MySQL

Value of UserID can be retrieved by opening the User table. Value of OrganizationID can be retrieved by opening the Organization table.

Note: - If database is not visible, refresh the SCHEMAS folder. Database should appear as shown below:-



Sample script is provided below:

```
INSERT INTO `osels_ewav`.`userorganization`  
(`Active`,  
`OrganizationID`,  
`RoleID`,  
`UserID`)  
VALUES  
(  
1,  
1,  
4,  
1);
```

3.4.1.2 Set up EWAV for PostgreSQL

1. Log in to the database server using an account which has admin privileges to create the database.
2. Right click on Databases under the server and click on New Databases in context menu

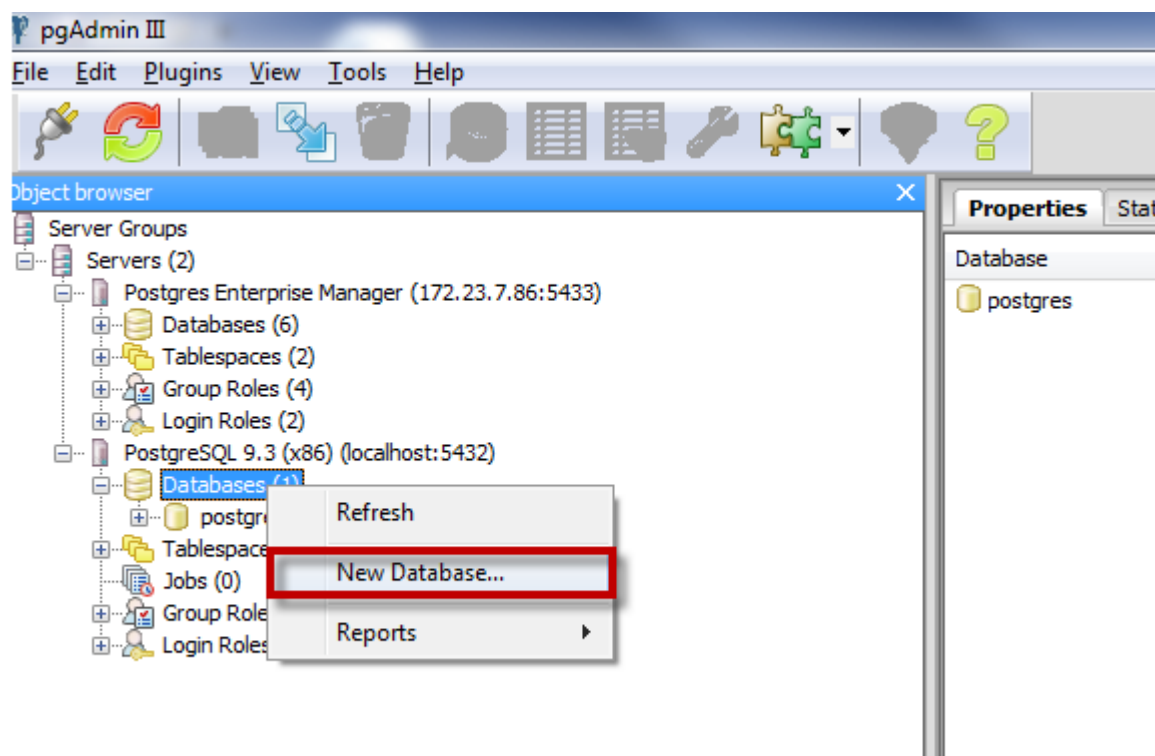


Figure 17: Create new database context menu for PostgreSQL

3. Specify the name of the database as “EWAV” and owner as “postgres” and click Ok. This should create a new database.

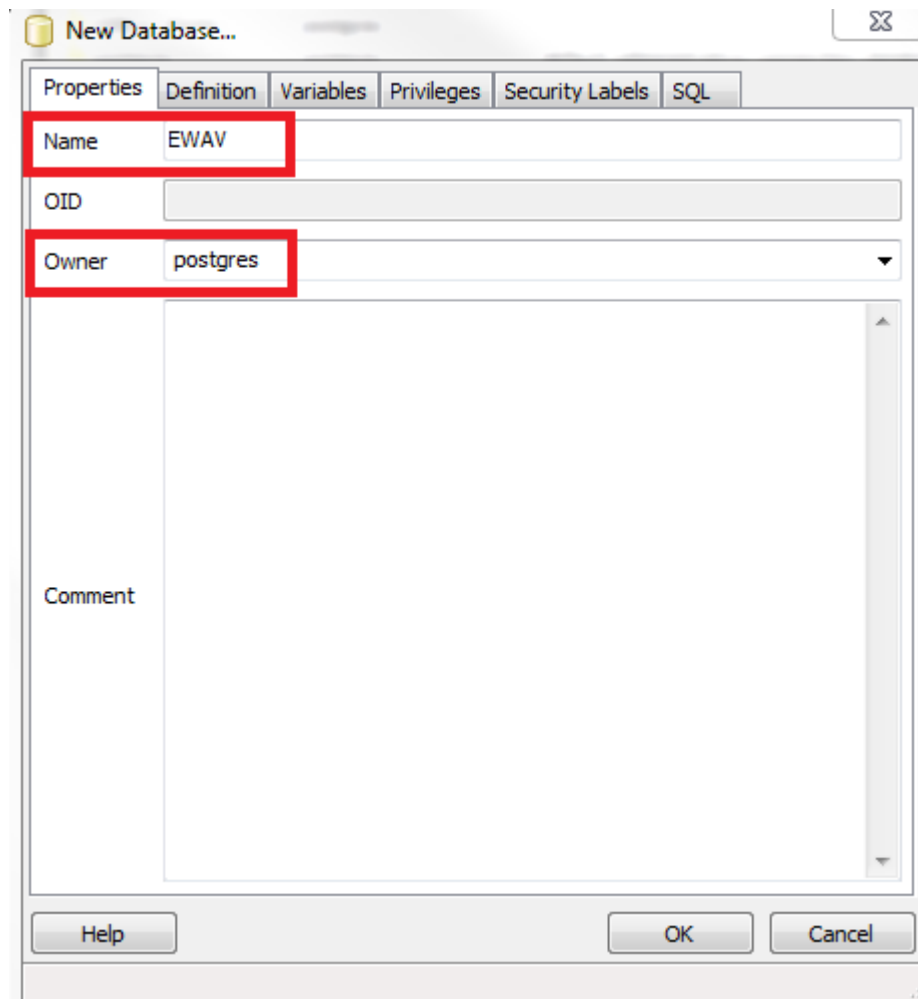


Figure 18: Create new database dialog for PostgreSQL

4. Highlight EWAV database under Databases tree and select SQL Editor. This shall open a new window as shown in the figure below to be used for other steps.

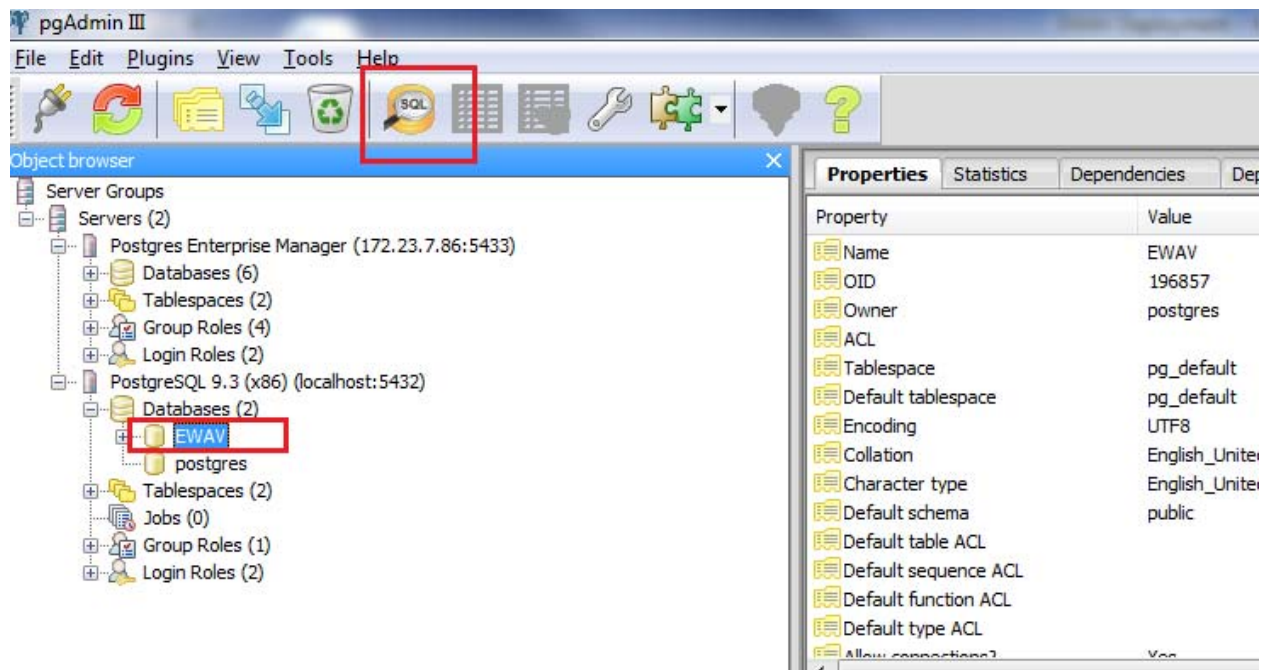


Figure 19: Confirmation of EWAV database creation in PostgreSQL

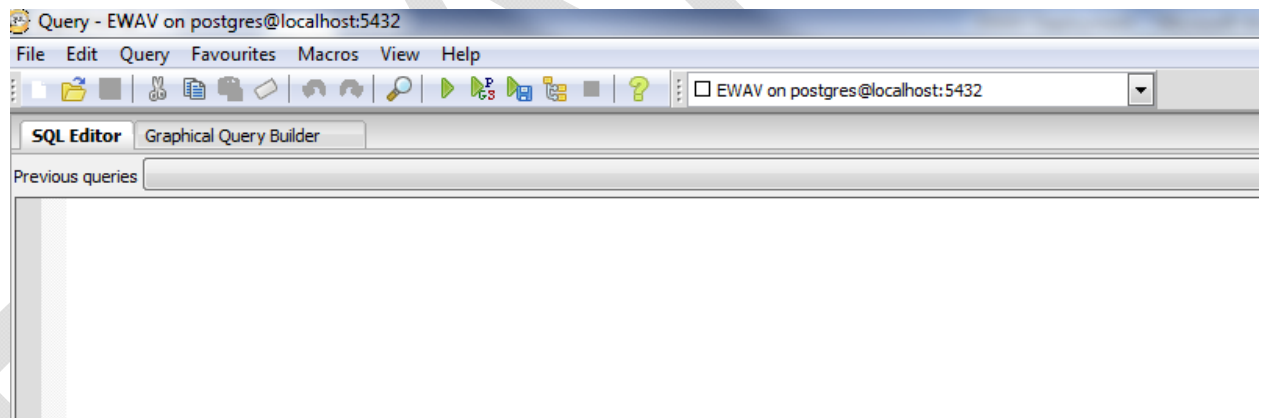


Figure 20: SQL Editor windows for PostgreSQL

5. Open the provided script namely 01CreateSchema.sql in relevant database management IDE/Utility. The diagram below is a snapshot of PG Admin III for Postgres

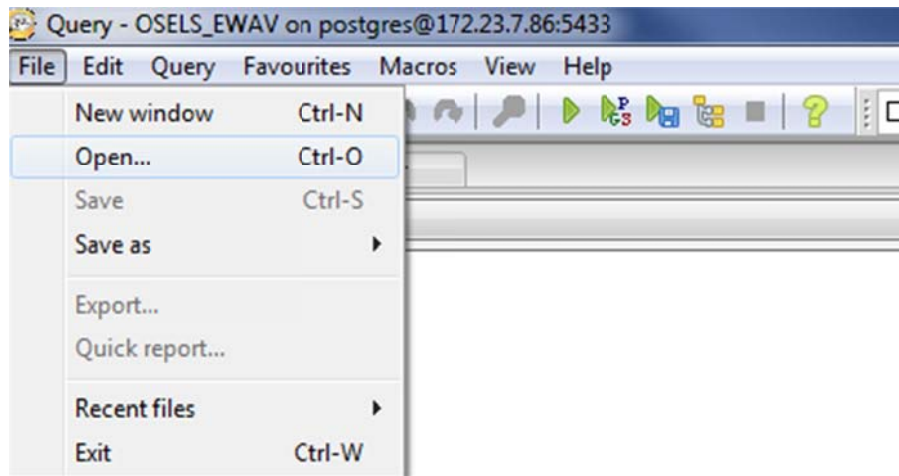


Figure 21: File menu to open the database script file for PostgreSQL

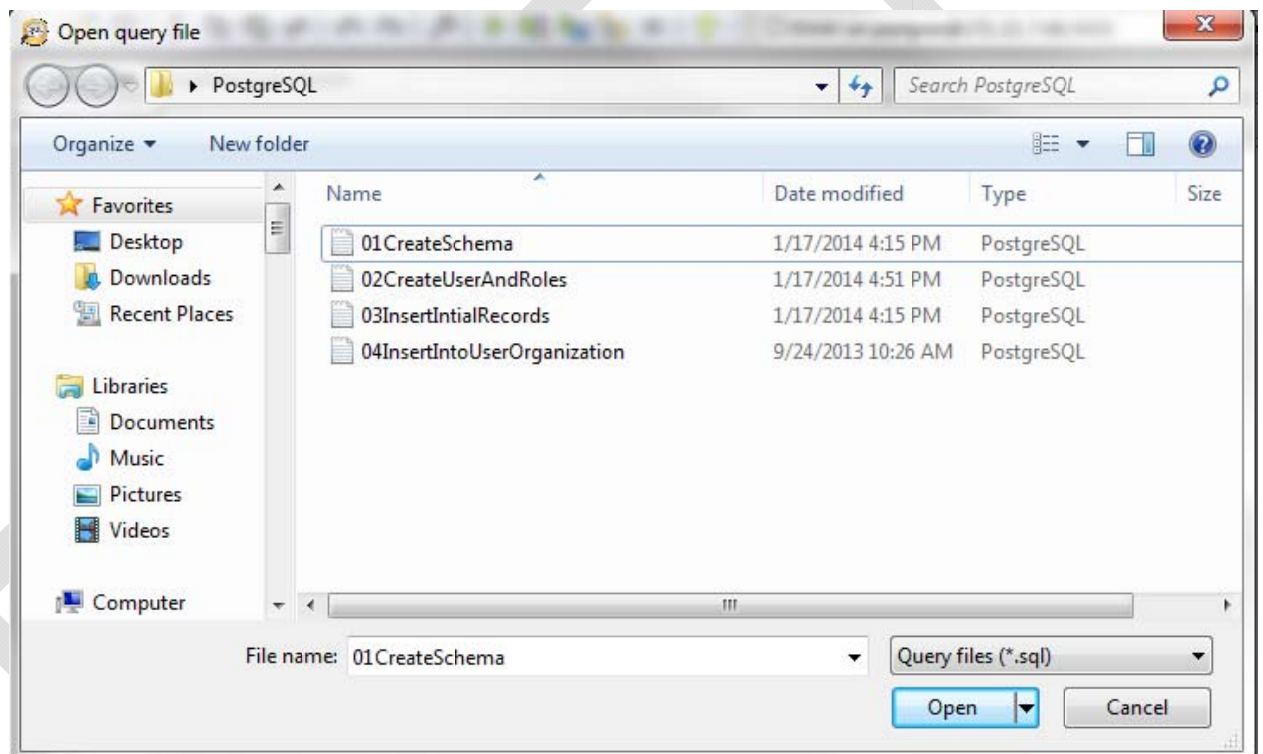


Figure 22: Open File dialog showing the available script for PostgreSQL

- Click on the button shown below to execute the script to create the schema for the database



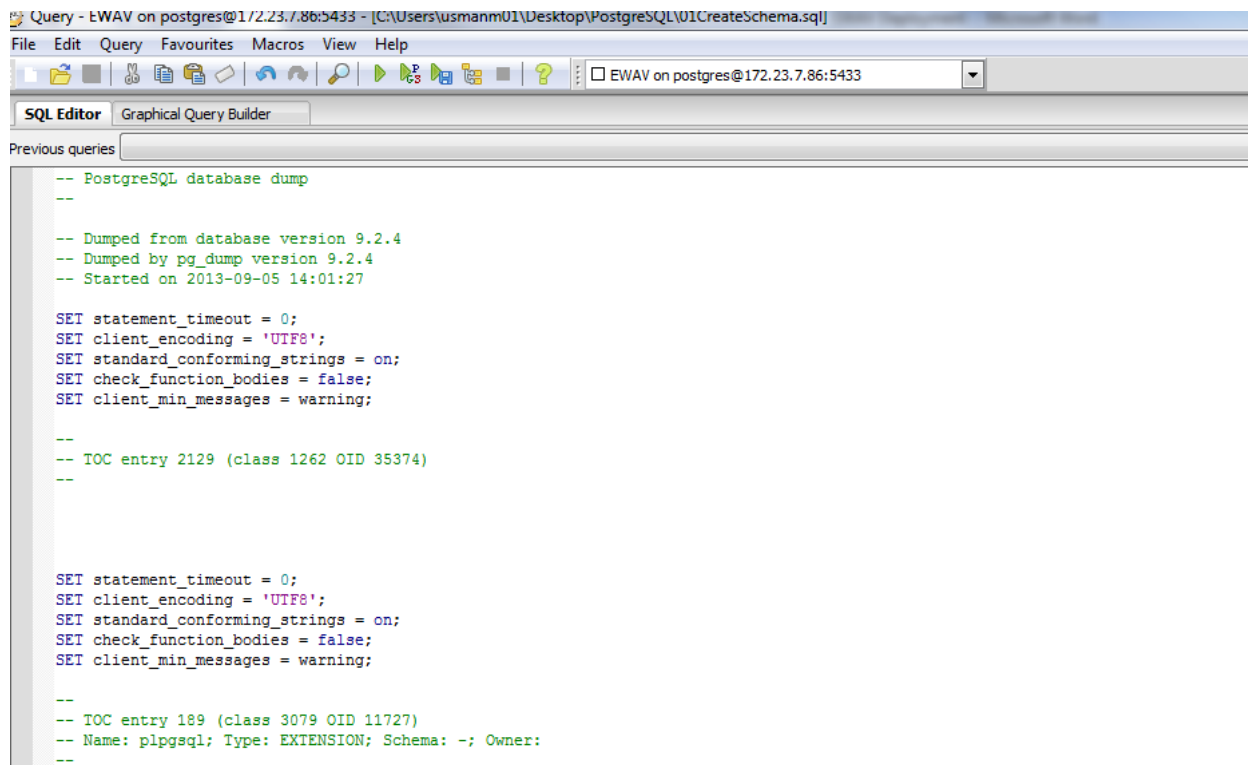


Figure 23: Snapshot showing portion of 01CreateScheam script for PostgreSQL

- Open the script titled “02CreateUserAndRoles”. Replace the Password with a strong password that meets your organization’s password policy. Execute the script by clicking on the button shown below. This will create the Application User Account and will grant execute permissions on stored procedures.



```

-----Create Database User And Role -----

-- Role: dbo
-- DROP ROLE dbo;

CREATE ROLE dbo
    NOSUPERUSER INHERIT NOCREATEDB NOCREATEROLE NOREPLICATION;

-- Role: ewav_appuser
-- DROP ROLE "ewav_appuser ";

CREATE ROLE "ewav_appuser" LOGIN
    PASSWORD 'P@ssW0rd!'
    NOSUPERUSER INHERIT NOCREATEDB NOCREATEROLE NOREPLICATION;
GRANT dbo TO "ewav_appuser";

```

Figure 24: Snapshot showing portion of 02CreateUserAndRoles script for PostgreSQL

Note: EWAV_APPUSER is the application account that is used by the application to connect to the database. Provide username and the password to the person configuring the application on the web server along with the Database server name and the Database name.

8. Open script “03InsertInitialRecord”. Execute this script by clicking on the button shown below. This script will add initial records for the system to work. It adds the roles used by the product; creates the Super Administrator user; and first organization. Before executing the script update sections marked in red for inserting Super Administrator user and Organization. For Super Administrator replace following placeholders with relevant values:

- /*UserName*/
 - UserName has to be valid Email address. For Windows deployed mode, this email has to be the part of Active Directory.
- /*FirstName*/
- /*LastName*/
- /*EmailAddress*/
- /*PhoneNumber*/

For Organization, replace following placeholders with relevant values:

- /*OrganizationName*/
- /*Description*/ - This is optional

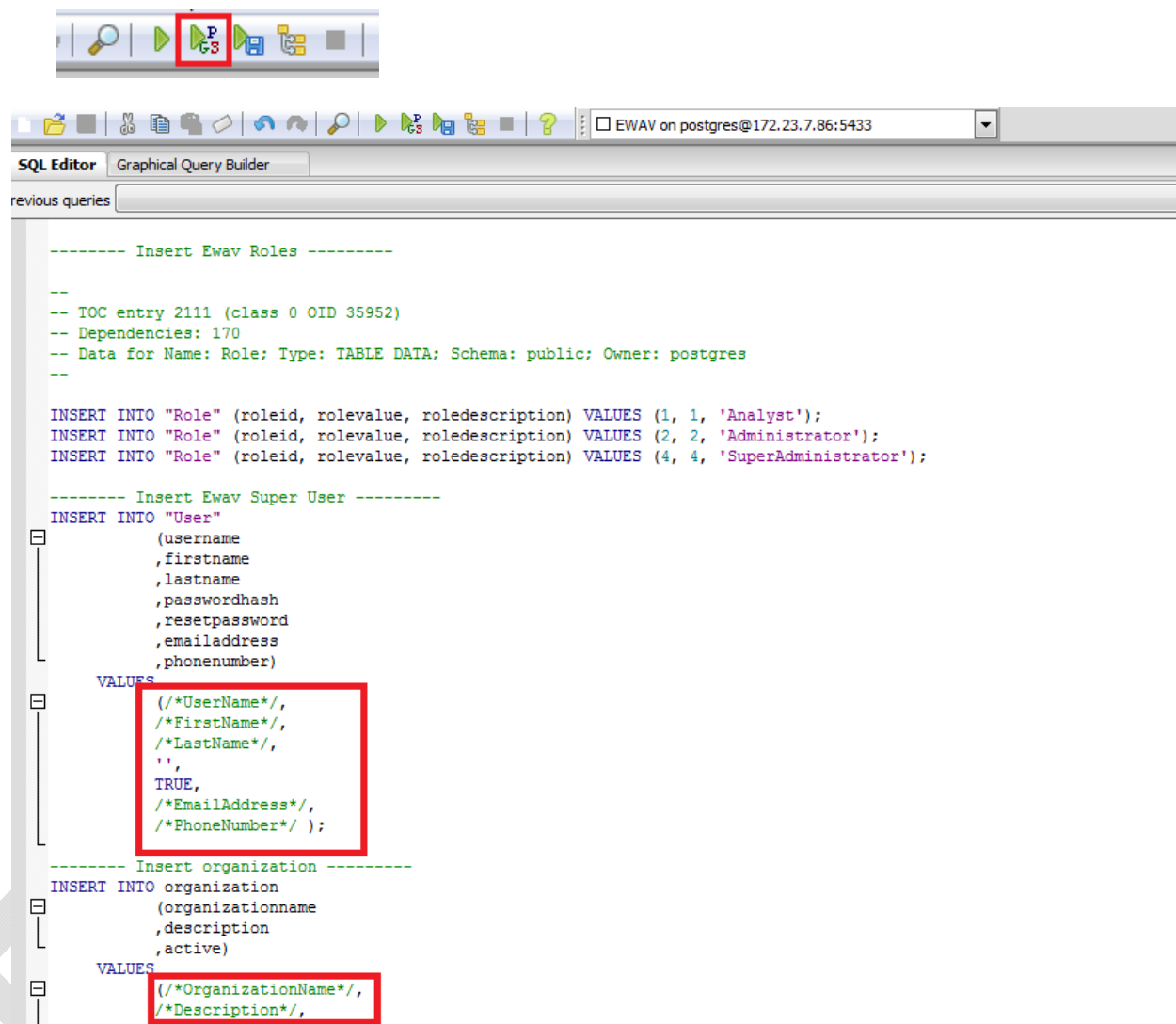


Figure 25: Snapshot showing portion of 03InsertInitialRecord script for PostgreSQL

Sample script is provided below:

```

INSERT INTO "User"
    (username
    ,firstname
    ,lastname
    ,passwordhash
    ,resetpassword
    ,emailaddress
    ,phonenummer)
VALUES
    ('useremail@org.gov'
  
```

```

        , 'UserFirstName'
        , 'UserLastName'
        , ''
        , TRUE
        , 'useremail@org.gov'
        , '111-111-1111' );

INSERT INTO organization
(organizationname
,description
,active)

VALUES
( 'Organization Name'
, 'Description'
, TRUE );

```

9. Execute 04InsertIntoUserOrganization script; this script will create the relationship between User and Organization. By default the user created will be super administrator with RoleId '4'. This authority is needed for a user to add other organizations and users. Like other scripts, place holders need to be changed here as well. These place holders are UserId and OrganizationId. Value of UserId can be retrieved from User table and value of OrganizationId can be retrieved from Organization table.

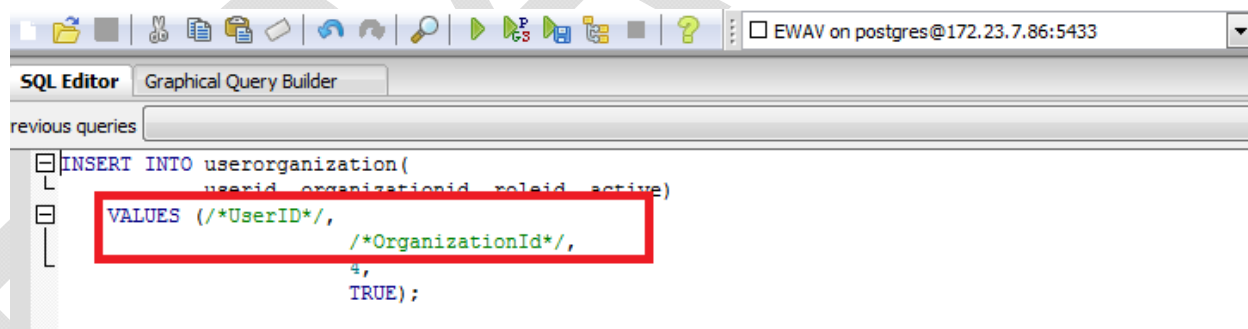
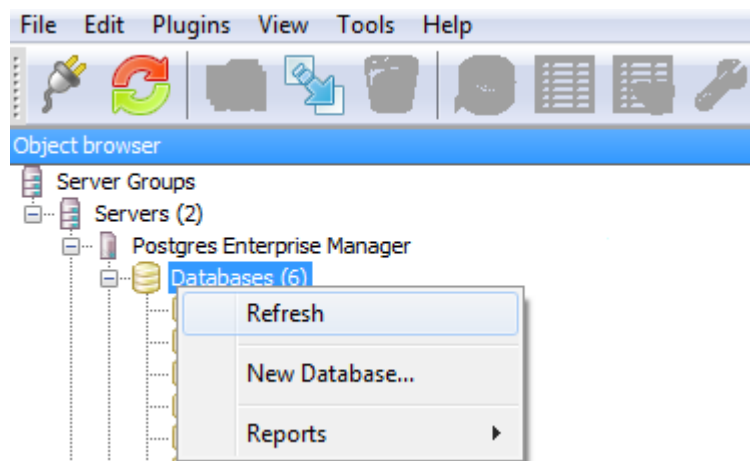


Figure 26: Snapshot showing portion of 04InsertIntoUserOrganization script for PostgreSQL

Note: if Database is not visible. Right click on Databases folder and click Refresh. It should appear as shown below:-



Sample script is provided below:

```
INSERT INTO userorganization(  
    userid,  
    organizationid,  
    roleid,  
    active)  
VALUES (1,  
    1,  
    4,  
    TRUE);
```

3.4.2 Application setup

The deployment package comes with “Application” folder containing all the files needed for configuration of Epi Info Web Analytics and Visualization product on the web server. The product can be configured to work as an Intranet application that uses Windows Authentication for authenticating the user. In case you plan to deploy the product as an outward facing application on public facing server then the product can be configured as Forms authenticated application that prompts the user to provide username and password before using the application. Once you have made the decision about the type of configuration needed for your organization the instructions for configuration are provided in the sub sections provided below:

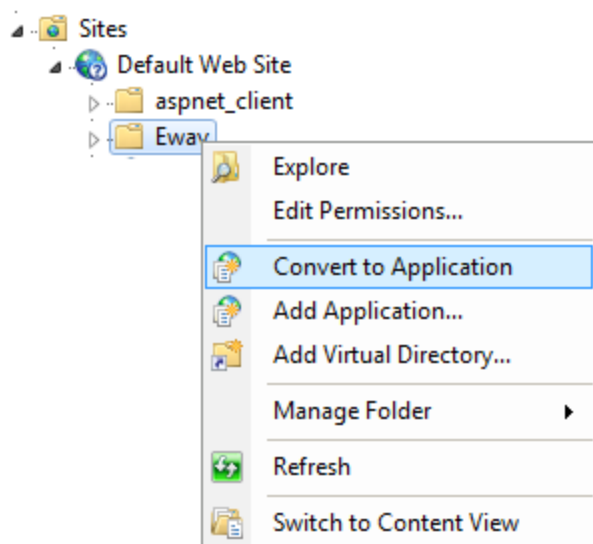
- Configure the application for Windows Authentication - Section 3.4.2.1
- Configure the application for Forms Authentication – Section 3.4.2.2

3.4.2.1 Configure the Application for Windows Authentication

The person installing and configuring the application should have administrative access on the web server and should have full access and privileges to create a web application in Internet Information Services (IIS).

The application and services configuration results in Epi Info™ Web Analytics & Visualization Web product being configured as a web application on the Internet Information Services (IIS).

1. Create a folder called “EWAV” under “inetpub\wwwroot.”
2. Copy the content of the folder “EWAV\Application” (and not the folder itself) to the “inetpub\wwwroot\Ewav” folder.
3. Create an application named “EWAV” in IIS by right clicking on “EWAV” folder under Sites and select Convert to Application



4. Make sure that the site is configured to run on an Application pool that is configured to use .NET 4.0. You can use one of the default application pools called Default Web Site or Default AppPool. This application pool uses a Managed Pipeline Mode of Integrated Authentication.

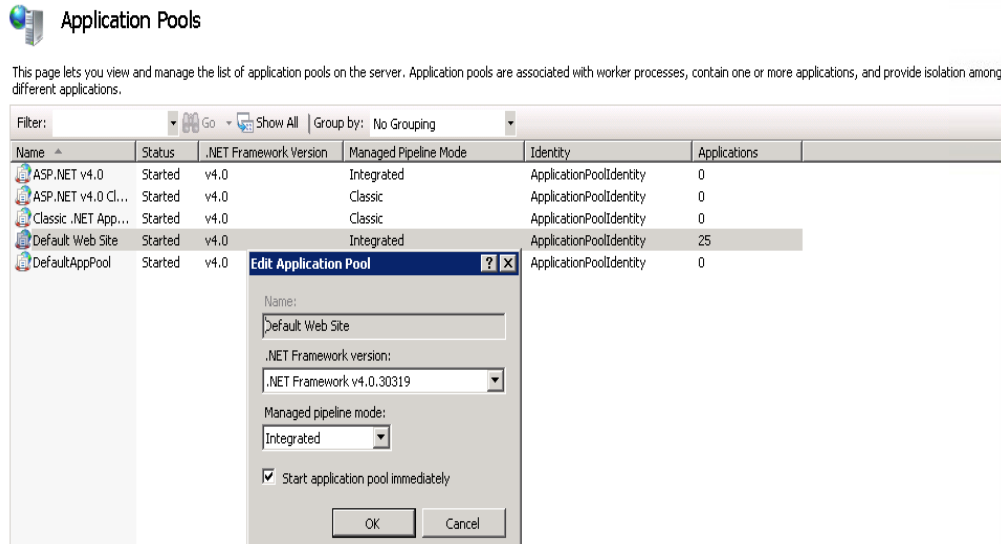


Figure 27: Application pool configured using .NET 4.0

5. Follow the steps provided below to configure application to run using Windows Authentication by configuring the settings of the application pool the application will use.
 - a. Highlight the application pool.
 - b. Click on advanced settings on right hand side of the IIS Manager.

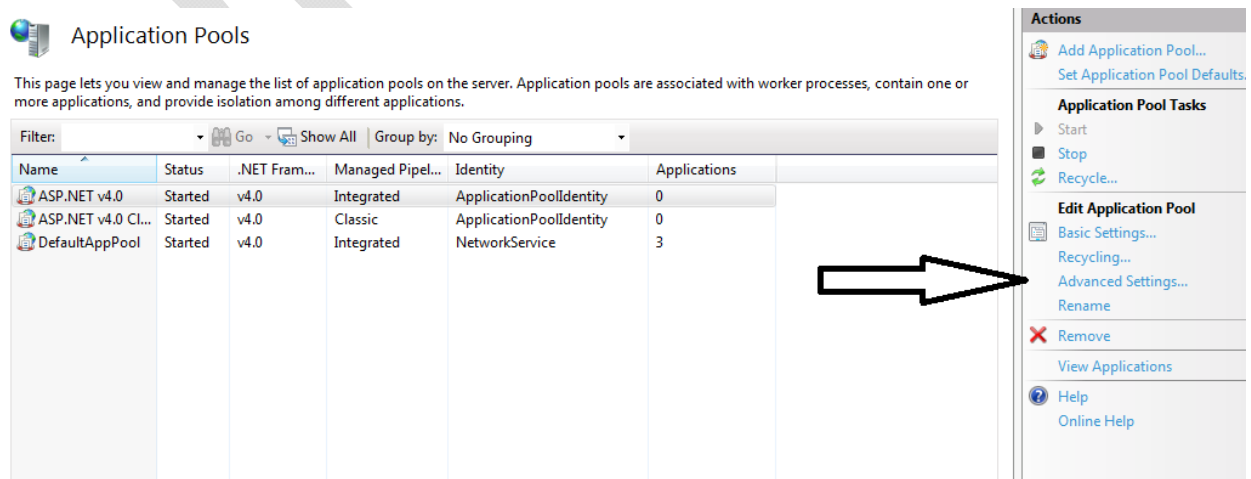


Figure 28: Application pool properties for windows authentication site

- c. Under Process Model section click on Identity value. A popup will appear as shown below. Select Network Service and Click OK.

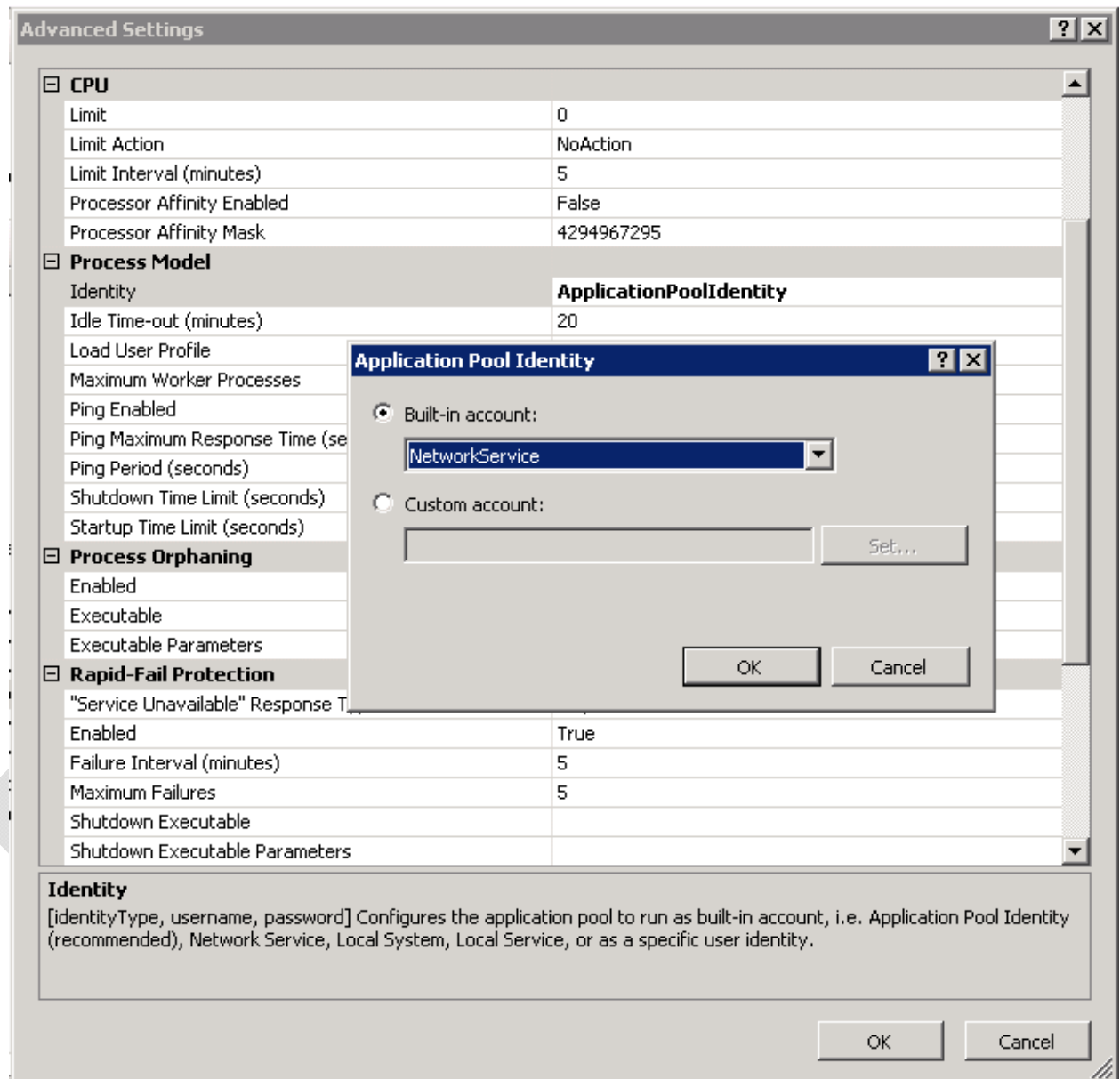


Figure 29: Setting Identity value for windows authentication application

6. For the application pool set 32-bit applications feature to on (True) in the Advance Settings as shown the screenshot below.

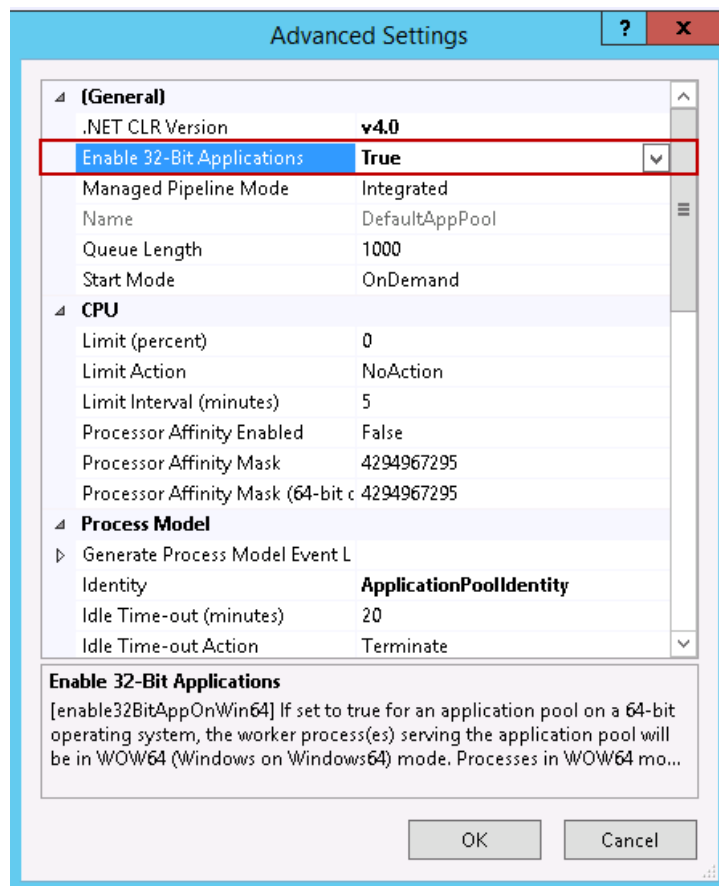


Figure 30: Setting Identity value for windows authentication application

- Make sure the site uses Windows authentication only. For this select the site under Default Web Site and click on Authentication in the Features View.

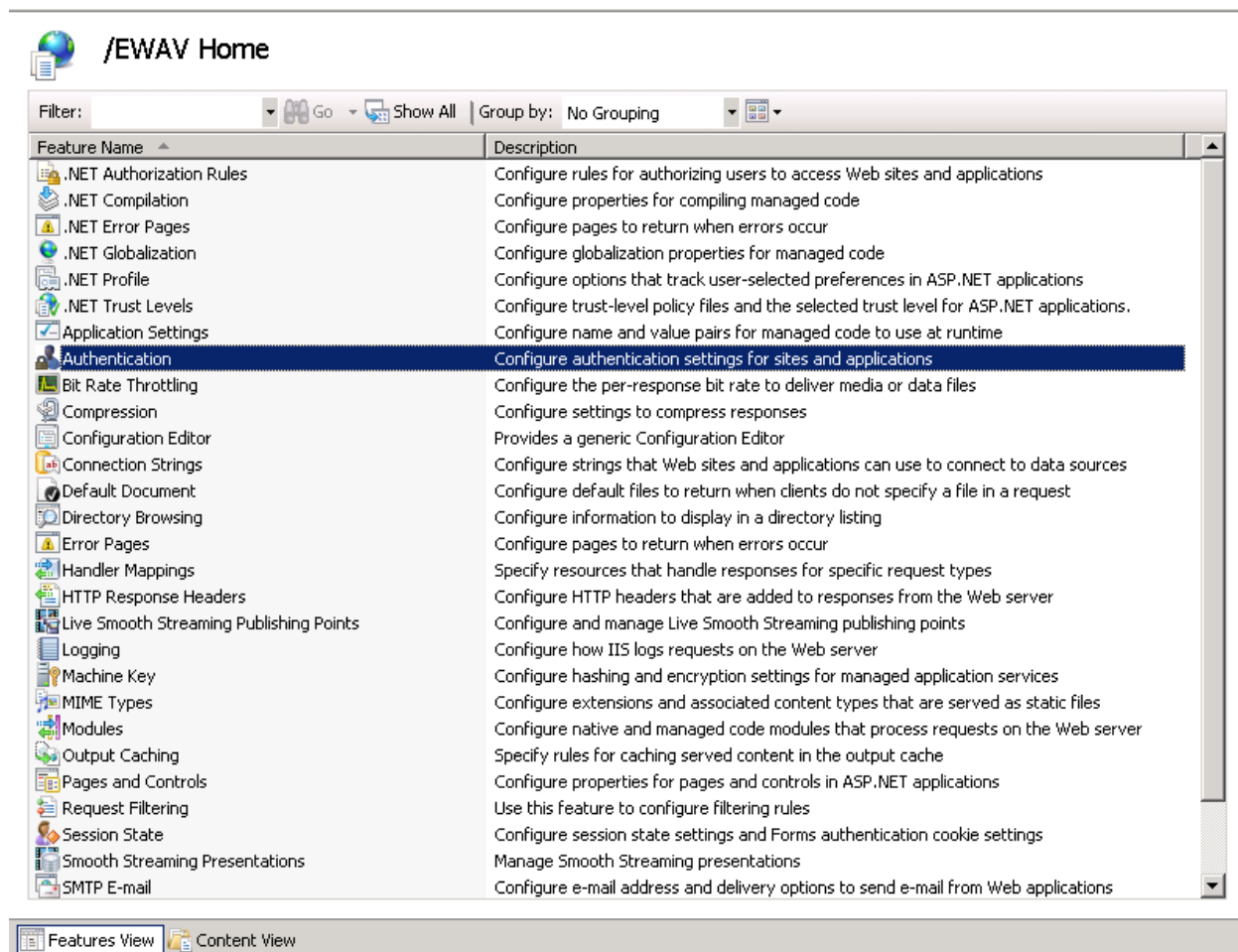


Figure 31: Choosing authentication setting

- In the Authentication View, click on Windows Authentication and then click on Enable in Actions on right hand side.

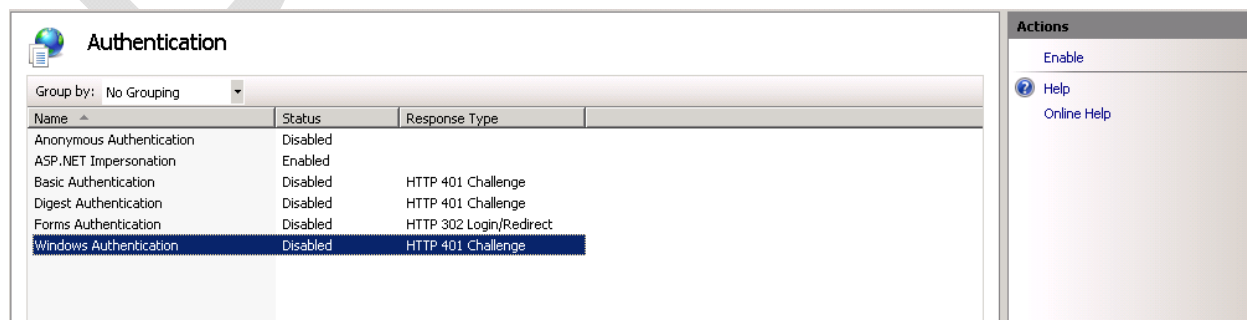


Figure 32: Enabling windows authentication setting

9. If Forms Authentication is "Enabled", make sure that it is set to "Disabled". Also disable Anonymous Authentication, Basic Authentication and Digest Authentication if present. Once the site has been configured to use Windows Authentication the Authentication View may look like the Figure shown below:

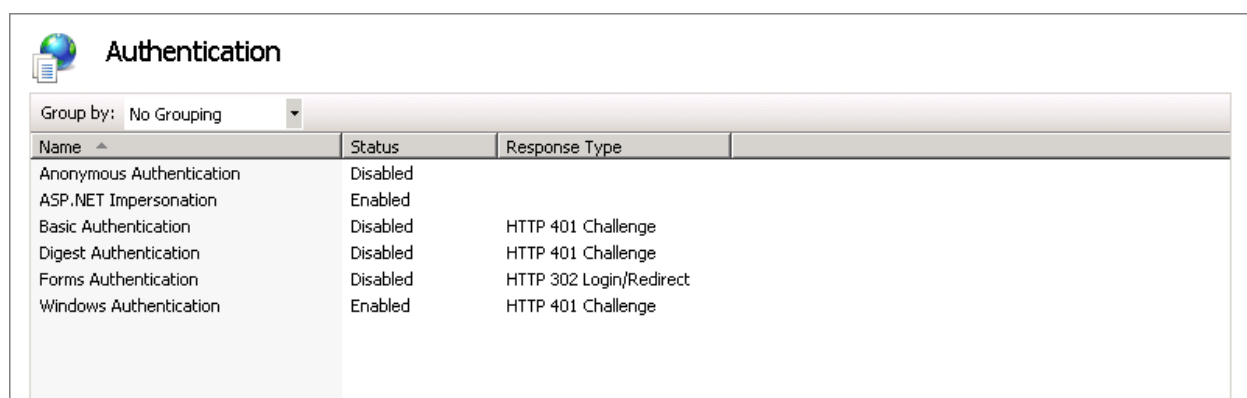


Figure 33: Confirming enabled and disabled authentication types

10. Open the web.config file in EWAV folder under "inetpub/wwwroot/EWAV" for editing in your preferred editor.

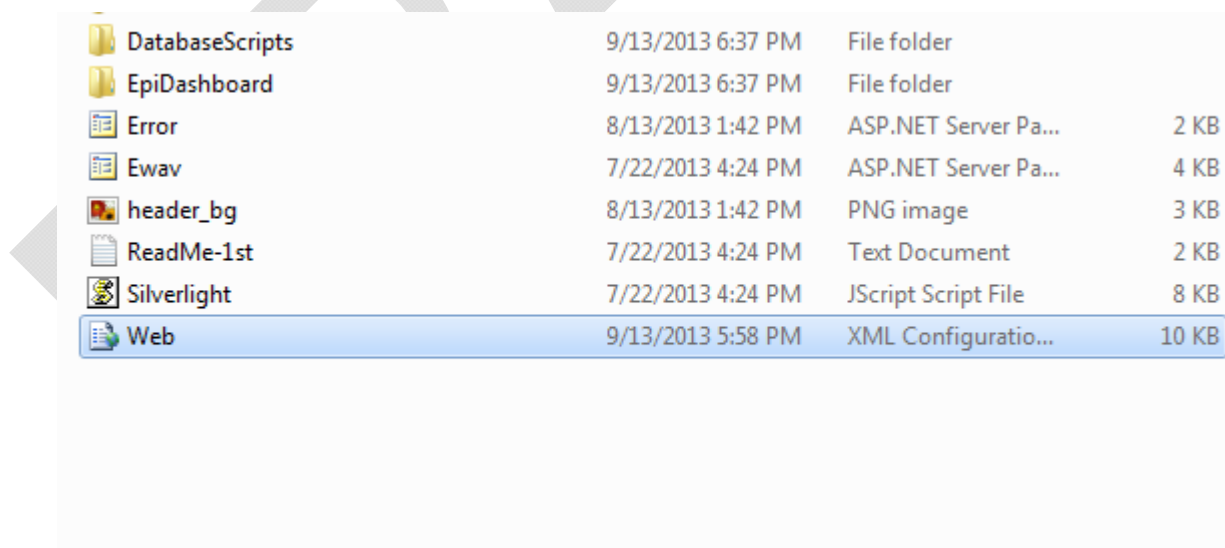


Figure 34: Web.config file for an integrated application under the file system of the web server

11. Validate that the authentication mode is set to “Windows” in the web.config file in the following section

```
<!-- Only valid values for authentication are Windows, Forms-->
<authentication mode="Windows">
```

12. Update Email notification section in the web.config file.

```
<!--Email notification-->
<add key="EMAIL_USE_AUTHENTICATION" value="FALSE"/>
<add key="EMAIL_USE_SSL" value="FALSE"/>
<add key="EMAIL_SUBJECT" value="XXXXXXXXXXXXX"/>
<add key="EMAIL_FROM" value="XXXXXXXXXXXXXXXXXX"/>
<add key="EMAIL_PASSWORD" value="XXXXXXXXXXXXX"/>
<add key="EMAIL_TO" value="XXXXXXXXXXXXX"/>
<add key="SMTP_PORT" value="XXXXXXXXXX"/>
<add key="SMTP_HOST" value="XXXXXXXXXXXXX"/>
```

- EMAIL_USE_AUTHENTICATION: The default value is FALSE. Change this to TRUE if authentication is used.
- EMAIL_USE_SSL: The default value is FALSE. Change this to TRUE if SSL is used.
- EMAIL_FROM: Provide an email address that can be used for the FROM part of the email.
- EMAIL_PASSWORD: A value needs to be provided here only if the EMAIL_USE_AUTHENTICATION is TRUE in step 6a above.
- SMTP_PORT: The system uses the default value of 25. Only provide a port number if the port number is other than 25.
- SMTP_HOST: This value has to be provided. This should be the name of the SMTP server used by the organization.

13. Update the password policy section to reflect the password policy for your organization. This policy will be used by users created in EWAV system. Following is the example of default password policy.

```
<add key="PasswordMinimumLength" value="6" />
<add key="PasswordMaximumLength" value="10" />
<add key="NumberOfTypesRequiredInPassword" value="3" />
<add key="TotalNumberOfTypesInPassword" value="4" />
<add key="UseNumbers" value="true" />
<add key="UseUpperCase" value="true" />
<add key="UseLowerCase" value="true" />
<add key="UseSymbols" value="true" />
<add key="Symbols" value="@#${}^" />
<add key="RepeatCharacters" value="true" />
<add key="ConsecutiveCharacters" value="false" />
<add key="UseUserIdInPassword" value="false" />
<add key="UseUserNameInPassword" value="false" />
```

- PasswordMinimumLength: The default minimum length is 6. Change this to meet your organizations requirements.
- PasswordMaximumLength: The default maximum length is 10. Change this to meet your organizations requirements.
- NumberOfTypesRequiredInPassword: The default value is 3. Change this to meet your organizations requirements.
- TotalNumberOfTypesInPassword: The system supports alphanumeric characters and symbols making a total of 4 types, namely numbers, upper case, lower case and symbols.
- UseNumbers: The default value for using numbers 0-9 is "TRUE". Change this to meet your organizations requirements.
- UseUpperCase: The default value for using characters A-Z is "TRUE". Change this to meet your organizations requirements.
- UseLowerCase: The default value for using character a-z is "TRUE". Change this to meet your organizations requirements.
- UseSymbols: The default value for using symbol is "TRUE". Change this to meet your organizations requirements.
- Symbols: The default list of symbols supported by the product is "@#\${}^". Change the symbol list to meet your organizations requirements.
- RepeatCharacters: The default value for repeating characters in the password is "TRUE". Change this to meet your organizations requirements.
- ConsecutiveCharacters: The default value for consecutive characters in the password is "FALSE". Change this to meet your organizations requirements.
- UseUserIdInPassword: The default value for using User Id in password is "FALSE". Change this to meet your organizations requirements.
- UseUserNameInPassword: The default value for using user name in password is "FALSE". Change this to meet your organizations requirements.

14. Use the encryption utility to generate keys Section. Refer to EWAV Encryption Utility Help document for instructions on generating keys



Figure 35: Generating the application encryption keys using EWAV Encryption utility for windows authentication application

15. Copy the section outputted in the Output text box by clicking the copy button shown with red rectangle. Replace the section shown below found under “Encryption Keys” in your web.config file with your copied text.

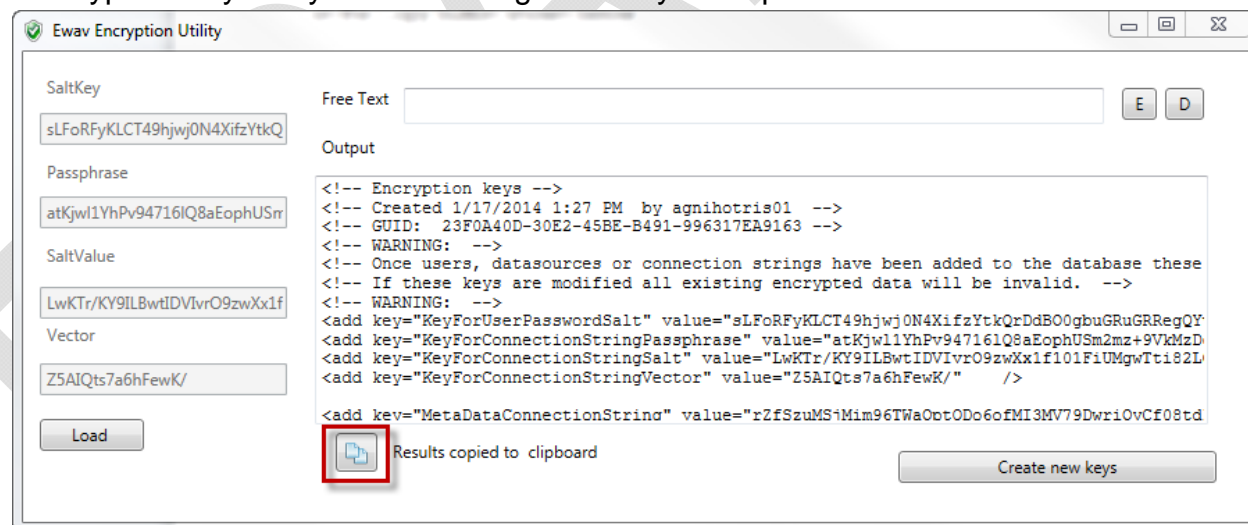


Figure 36: Copying the keys section to update the keys section in the provided web.config file for windows authentication application

```
<!-- Encryption keys -->
<!-- Created 1/17/2014 1:27 PM by user01 -->
<!-- GUID: 23F0A40D-30E2-45BE-B491-996317EA9163 -->
<!-- WARNING: -->
```

```

<!--
Once users, datasources or connection strings have been added to the databa
se these keys *cannot* be modified. -->
<!--
If these keys are modified all existing encrypted data will be invalid. --
>
<!-- WARNING: -->
<add key="KeyForUserPasswordSalt" value="sLFoRFyKLCT49hjwt0N4XifzYtkQrDd
B00gbuGRuGRRRegQYv4EydWV5Q5yGV0ECOTyOq5a0UbbRIh81xQbDuQWjYf6Vk4gLG/1dQCuutN9i
VtDZQbe8d1JL0aAhLbFantM013g==" />
<add key="KeyForConnectionStringPassphrase" value="atKjwl1YhPv94716lQ8aE
ophUSm2mz+9VkmzDgzRgscoPsRYJ2/vRs7eJTf43X6r/PiBQS2Pb99lzoA0DAVxfmwToq1QXDgov
FCZP+axtINlw9vbidyz9cG0Ty3LNjxCYuMoIw==" />
<add key="KeyForConnectionStringSalt" value="LwKTr/KY9ILBwtIDVIvr09zwXx1
f101FiUMgwTti82LCY0Erdrrdu45vaVQntXe6kD0JjK1RXkLL8HdmuzPSEYsvtIKDJQ8SGdAtzHW
pYrpkdXmcd5bi/pL04UdL1H3f2ZfpZg==" />
<add key="KeyForConnectionStringVector" value="Z5AIQts7a6hFewK/" />

```

NOTE: The keys are the most critical piece of the system. Please make an archive of these keys and save it at a safe location in case they are lost/changed/updated in web.config file by mistake

16. Create MetaDataConnectionString for the type of database you are using and replace the relevant section marked in yellow as shown below

a. SQL Server

Data Source= DATABASE_SERVER_NAME;Initial Catalog= DATABASE_NAME;Persist Security Info=True;User ID= APPLICATION_ACCOUNT;Password= PASSWORD_FOR_ACCOUNT

b. MySQL

Server= DATABASE_SERVER_NAME; Port=3306 ;Database= DATABASE_NAME;Uid= APPLICATION_ACCOUNT;Pwd= PASSWORD_FOR_ACCOUNT;

c. PostGreSql

Server= DATABASE_SERVER_NAME;Port=5433;Database= DATABASE_NAME;User Id= APPLICATION_ACCOUNT;Password= PASSWORD_FOR_ACCOUNT;

Below is an example of connection string for SQL Server after removing the sections marked in yellow.

Data Source=SQLServer;Initial Catalog=EWAV;Persist Security Info=True;User ID=ewav_appuser;Password=P@ssW0rD

17. Use the encryption utility to encrypt the values of MetaDataConnectionString created in the step above using the encryption keys you had generated. The encryption keys should still be available in you're the utility if you have not closed it. In case you have closed the utility refer to EWAV Encryption Utility document on how to get back the keys.

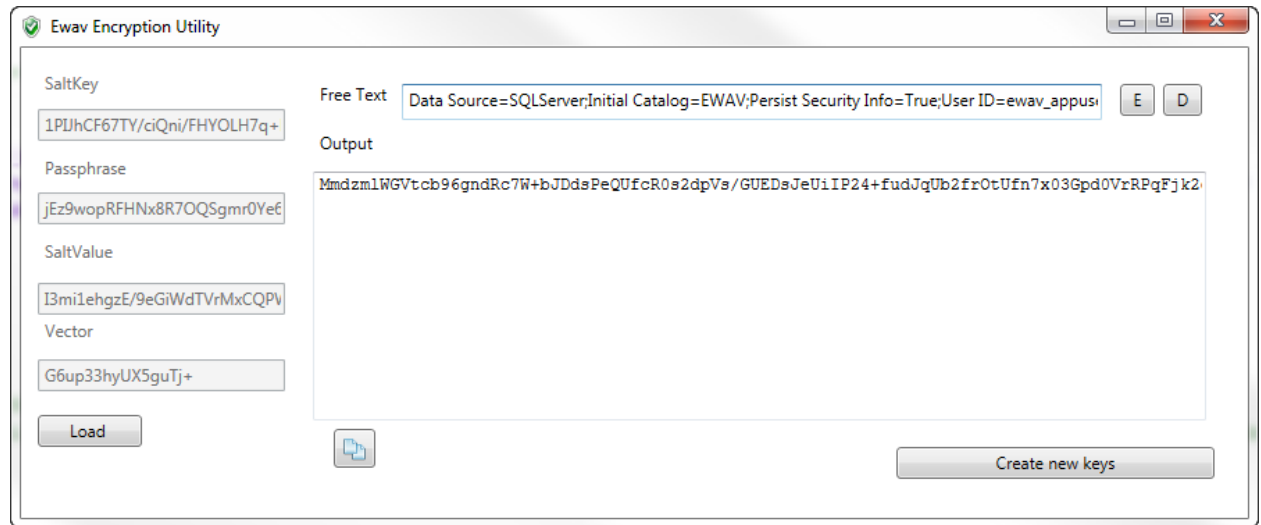


Figure 37: Encrypting connection string using EWAV Encryption utility for windows authentication application

18. Ewav uses the Microsoft Bing Maps API in its Case Cluster Map gadget. You must create a unique key for your web server on Microsoft's Bing Maps portal page here: <http://www.bingmapsportal.com/>. A Microsoft account is required to use the portal page. If you do not have a Microsoft account you will be prompted to register for one.

Once you have created a key for the Bing Maps API the web.config must be updated with this entry:

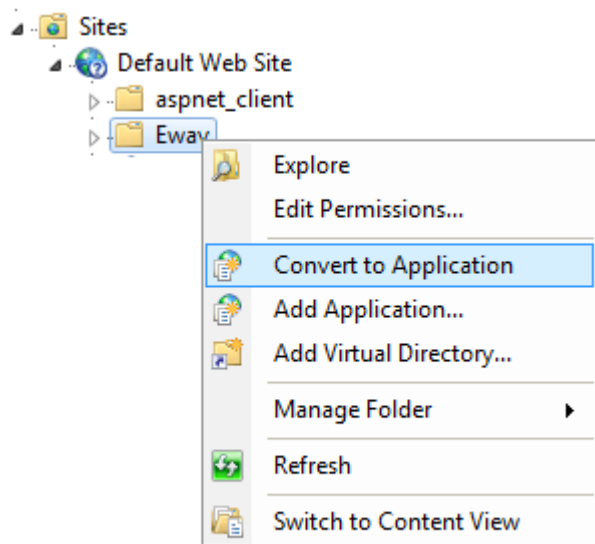
```
<add key="KeyForBingMaps" value="(Your key goes here)" />
```

3.4.2.2 Configure the Application for Forms-based Authentication

The person installing and configuring the application should have administrative access on the web server and should have full access and privileges to create a web application in Internet Information Services (IIS).

The application and services configuration results the Epi Info Web Visualization Web application being configured as a single integrated application on the Internet Information Services (IIS).

1. Create a folder called “EWAV” under “inetpub\wwwroot.”
2. Copy the content of the folder “EWAV\Application” (and not the folder itself) to the “inetpub\wwwroot\Ewav” folder.
3. Create an application named “EWAV” in IIS by right clicking on “EWAV” folder and select Convert to Application



4. Make sure that the site is configured to run on an Application pool that is configured to use .NET 4.0. You can use one of the default application pools called Default Web Site or Default AppPool. This application pool uses a Managed Pipeline Mode of Integrated Authentication.

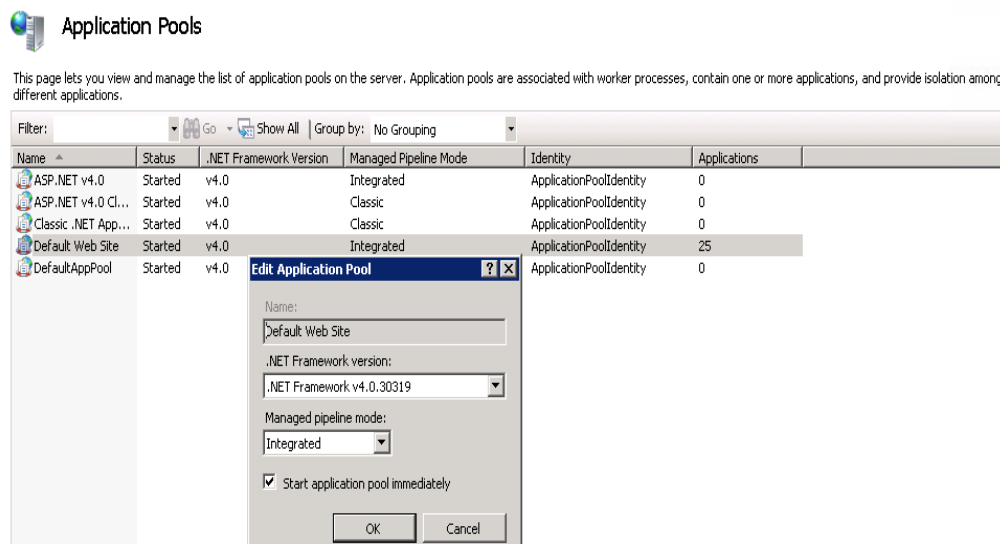


Figure 38: Application pool configured using .NET 4.0

- For the application pool set 32-bit applications feature to on (True) in the Advance Settings as shown the screenshot below.

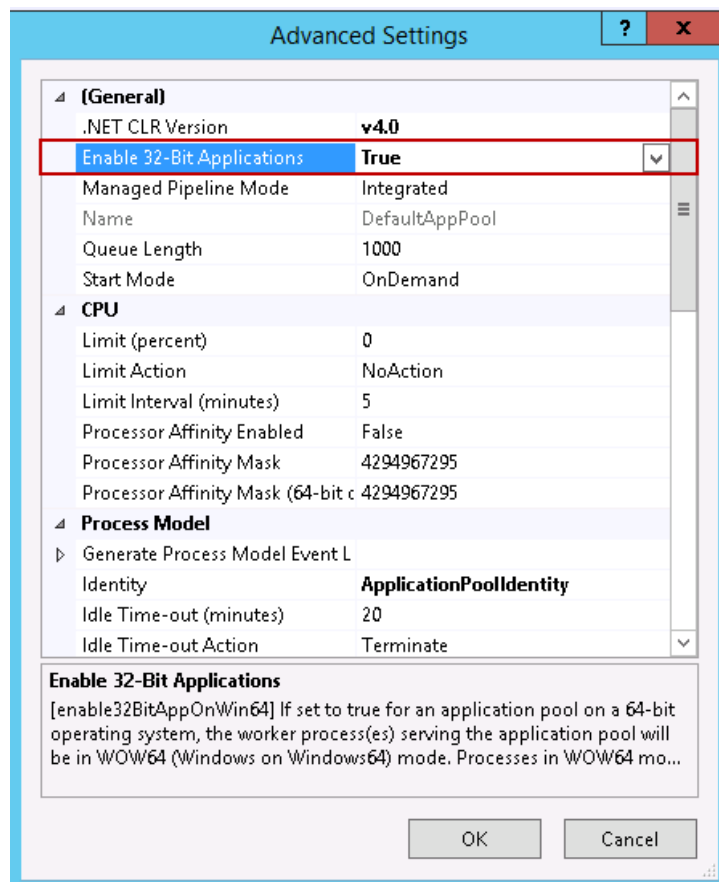


Figure 39: Setting Identity value for windows authentication application

- Make sure the site uses Anonymous authentication only. This is the default setting when the site is configured in IIS.

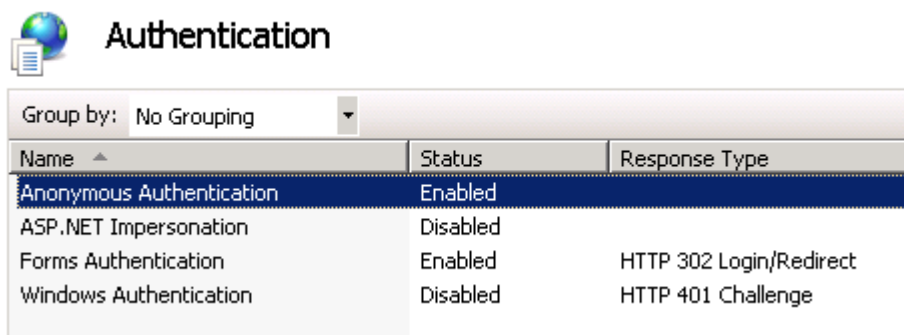


Figure 40: Application configured with Anonymous Authentication Enabled

- Open the web.config file in EWAV folder under “inetpub/wwwroot/EWAV” for editing in your preferred editor.

Name	Modified	Type	Size
DatabaseScripts	9/13/2013 6:37 PM	File folder	
EpiDashboard	9/13/2013 6:37 PM	File folder	
Error	8/13/2013 1:42 PM	ASP.NET Server Pa...	2 KB
Ewav	7/22/2013 4:24 PM	ASP.NET Server Pa...	4 KB
header_bg	8/13/2013 1:42 PM	PNG image	3 KB
ReadMe-1st	7/22/2013 4:24 PM	Text Document	2 KB
Silverlight	7/22/2013 4:24 PM	JScript Script File	8 KB
Web	9/13/2013 5:58 PM	XML Configuratio...	10 KB

Figure 41: Web.config file for a forms authentication application

- Validate that the authentication mode is set to “Forms” in the web.config file in the following section

```
<!-- Only valid values for authentication are Windows, Forms-->
<authentication mode="Forms">
```

- Update Email notification section in the web.config file.

```
<!--Email notification-->
<add key="EMAIL_USE_AUTHENTICATION" value="FALSE"/>
<add key="EMAIL_USE_SSL" value="FALSE"/>
<add key="EMAIL_SUBJECT" value="XXXXXXXXXXXXX"/>
<add key="EMAIL_FROM" value="XXXXXXXXXXXXXXXXX"/>
<add key="EMAIL_PASSWORD" value="XXXXXXXXXXXXX"/>
<add key="EMAIL_TO" value="XXXXXXXXXXXXX"/>
```

```
<add key="SMTP_PORT" value="XXXXXXXXXX"/>
<add key="SMTP_HOST" value="XXXXXXXXXXXXXX"/>
```

- EMAIL_USE_AUTHENTICATION: The default value is FALSE. Change this to TRUE if authentication is used.
- EMAIL_USE_SSL: The default value is FALSE. Change this to TRUE if SSL is used.
- EMAIL_FROM: Provide an email address that can be used for the FROM part of the email.
- EMAIL_PASSWORD: A value needs to be provided here only if the EMAIL_USE_AUTHENTICATION is TRUE in step 6a above.
- SMTP_PORT: The system uses the default value of 25. Only provide a port number if the port number is other than 25.
- SMTP_HOST: This value has to be provided. This should be the name of the SMTP server used by the organization.

10. Update the password policy section to reflect the password policy for your organization. This policy will be used by users created in the EWAV system.

```
<add key="PasswordMinimumLength" value="6" />
<add key="PasswordMaximumLength" value="10" />
<add key="NumberOfTypesRequiredInPassword" value="3" />
<add key="TotalNumberOfTypesInPassword" value="4" />
<add key="UseNumbers" value="true" />
<add key="UseUpperCase" value="true" />
<add key="UseLowerCase" value="true" />
<add key="UseSymbols" value="true" />
<add key="Symbols" value="@#${}^" />
<add key="RepeatCharacters" value="true" />
<add key="ConsecutiveCharacters" value="false" />
<add key="UseUserIdInPassword" value="false" />
<add key="UseUserNameInPassword" value="false" />
```

- PasswordMinimumLength: The default minimum length is 6. Change this to meet your organizations requirements.
- PasswordMaximumLength: The default maximum length is 10. Change this to meet your organizations requirements.
- NumberOfTypesRequiredInPassword: The default value is 3. Change this to meet your organization's requirements.
- TotalNumberOfTypesInPassword: The system supports alphanumeric characters and symbols making a total of 4 types, numbers, upper case, lower case and symbols.
- UseNumbers: The default value for using numbers 0-9 is "TRUE". Change this to meet your organization's requirements.
- UseUpperCase: The default value for using characters A-Z is "TRUE". Change this to meet your organization's requirements.

- UseLowerCase: The default value for using character a-z is “TRUE”. Change this to meet your organization’s requirements.
- UseSymbols: The default value for using symbol is “TRUE”. Change this to meet your organization’s requirements.
- Symbols: The default list of symbols supported by the product is “@#\${}^”. Change the symbol list to meet your organization’s requirements.
- RepeatCharacters: The default value for repeating characters in the password is “TRUE”. Change this to meet your organization’s requirements.
- ConsecutiveCharacters: The default value for consecutive characters in the password is “FALSE”. Change this to meet your organization’s requirements.
- UseUserIdInPassword: The default value for using User Id in password is “FALSE”. Change this to meet your organization’s requirements.
- UserUserNameInPassword: The default value for using user name in password is “FALSE”. Change this to meet your organization’s requirements.

11. Use the encryption utility to generate keys Section. Refer to EWAV Encryption Utility Help document for instructions on generating keys.

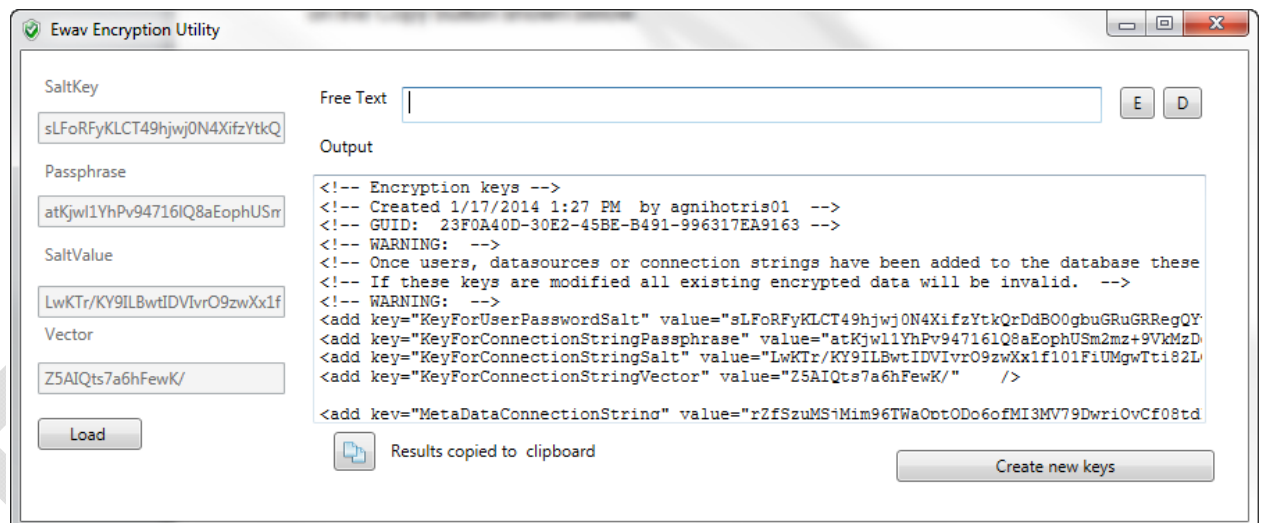


Figure 42: Generating the application encryption keys using EWAV Encryption utility for forms authentication application

12. Copy the section generated in the Output text box by clicking the copy button highlighted in red below. Replace the section shown below found under “Encryption Keys” in your web.config file with your copied text.



Figure 43: Copying the keys section to update the keys section in the provided web.config file for forms authentication application

```
<!-- Encryption keys -->
<!-- Created 1/17/2014 1:27 PM by user01 -->
<!-- GUID: 23F0A40D-30E2-45BE-B491-996317EA9163 -->
<!-- WARNING: -->
<!--
Once users, datasources or connection strings have been added to the databa
se these keys *cannot* be modified. -->
<!--
If these keys are modified all existing encrypted data will be invalid. --
>

<!-- WARNING: -->
<add key="KeyForUserPasswordSalt" value="sLForFyKLCT49hjwt0N4XifzYtkQrDd
B00gbuGRuGRRegQYv4EydWV5Q5yGV0ECOTYq5a0UbbRIh81xQbDuQWjYf6V4gLG/1dQCuutN9i
VtDZQbe8d1JL0aAhLbFantM013g==" />
<add key="KeyForConnectionStringPassphrase" value="atKjw11YhPv94716lQ8aE
ophUSm2mz+9VkmZDgzRgscoPsRYJ2/vRs7eJTF43X6r/PiBQS2Pb991zoA0DAVxfmwToq1QXDgov
FCZP+axtINlw9vbidyz9cG0Ty3LNjxCYuMoIw==" />
<add key="KeyForConnectionStringSalt" value="LwKTr/KY9ILBwtIDVivrO9zwXx1
f101FiUMgwTti82LCY0Erdrrdu45vaVQntXe6kD0Jk1RXkLL8HdmuzPSEYsvtIKDJQ8SGdAtzHW
pYrpkdXmcd5bi/pL04UdL1H3f2ZfpZg==" />
<add key="KeyForConnectionStringVector" value="Z5AIQts7a6hFewK/" />
```

NOTE: The keys are the most critical piece of the system. Please make up an archive of these keys and save it in a safe location, in case they are lost/changed/updated in web.config file by mistake.

13. Create a MetadataConnectionString for the type of database you are using by replacing the section highlighted in yellow, in the plain text connections string.
 - a. SQL Server

Data Source= **DATABASE_SERVER_NAME**;Initial Catalog=**DATABASE_NAME**;Persist Security Info=True;User ID=**APPLICATION_ACCOUNT**;Password= **PASSWORD_FOR_ACCOUNT**

b. MySQL

Server= **DATABASE_SERVER_NAME**; Port=3306 ;Database=**DATABASE_NAME**;Uid= **APPLICATION_ACCOUNT**;Pwd=**PASSWORD_FOR_ACCOUNT**;

c. PostgreSQL

Server= **DATABASE_SERVER_NAME**;Port=5433;Database=**DATABASE_NAME**;User Id= **APPLICATION_ACCOUNT**;Password=**PASSWORD_FOR_ACCOUNT**;

Below is an example of connection string for SQL Server after removing the sections marked in yellow.

Data Source=SQLServer;Initial Catalog=EWAV;Persist Security Info=True;User ID=ewav_appuser;Password=P@ssW0rD

14. Use the encryption utility to encrypt the values of the MetaDataConnectionString created in the step above using the encryption keys generated above. The encryption keys should still be available in the utility if you have not closed it. In case you have closed the utility, refer to EWAV Encryption Utility document on how to retrieve the keys.

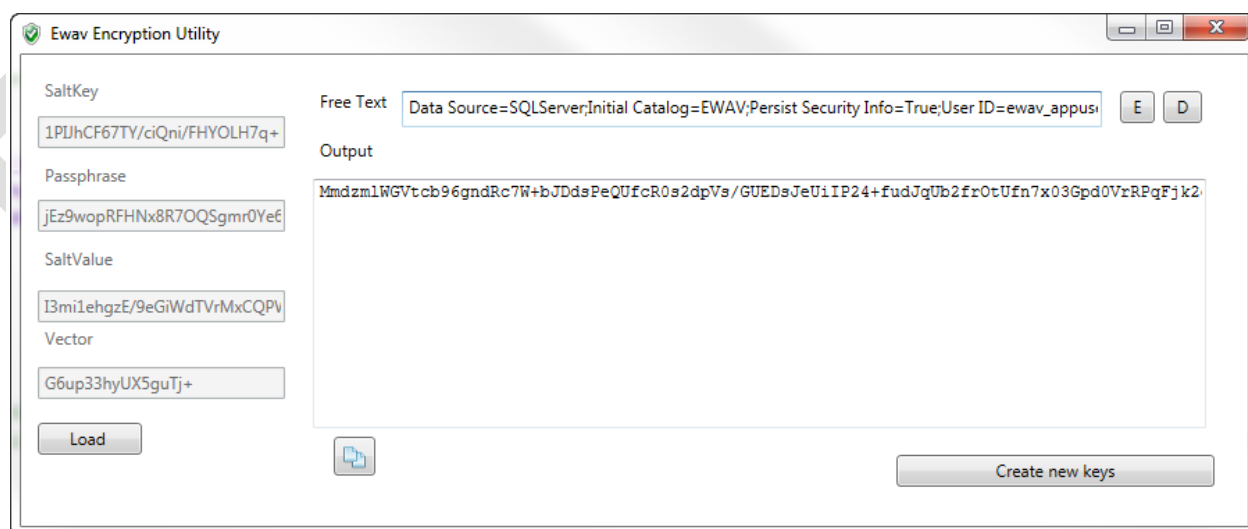


Figure 44: Encrypting connection string using EWAV Encryption utility for forms authentication application

15. EWAV uses the Microsoft Bing Maps API in its Case Cluster Map gadget. You must create a unique key for your web server on Microsoft's Bing Maps portal page here: <http://www.bingmapsportal.com/>. A Microsoft account is required

to use the portal page. If you do not have a Microsoft account you will be prompted to register for one.

Once you have created a key for the Bing Maps API the web.config must be updated with this entry:

```
<add key="KeyForBingMaps" value="(Your key goes here)" />
```

DRAFT

3.4.2.3 Starting the System

To start the system, perform following steps:

1. Navigate to system's URL: http://<SERVER_NAME>/EWAV/Ewav.aspx
2. Click on Forgot password (only for Forms authentication application)
3. Enter the email address which was given during the time of running the initial scripts on the database (only for Forms authentication application)
4. An email will be sent out with temporary password (only for Forms authentication application)
5. Log in using the temporary password and reset your password (only for Forms authentication application)
6. Navigate to Admin tab.
7. Create organization if needed.
8. Create Users/Admins on the current organization.
9. Create at least one data source.
10. Navigate back to dashboard screen.
11. Set a data source.
12. Start adding gadgets.

APPENDIX A: REFERENCES

The following table summarizes the documents referenced in this document.

Document Name and Version	Description	Location
EWAV Admin Help	This document describes the Epi Info™ Web Analytics & Visualization tool.	/Ewav/Documents

APPENDIX B: Table of Figures

Figure 1: Overview of Epi Info™ Web Analytics & Visualization	7
Figure 2: Intranet Configuration	8
Figure 3: Internet Configuration	9
Figure 4: File system showing components in the EWAV Package.....	10
Figure 5: File menu to open the database script file for SQL Server	11
Figure 6: Open File dialog showing the available script for SQL Server.....	12
Figure 7: Snapshot of a portion of 01CreateSchema script for SQL Server	12
Figure 8: Snapshot of a portion of 02CreateUserAndRoles script for SQL Server	13
Figure 9: Snapshot of a portion 03InsertInitialRecord script for SQL Server.....	14
Figure 10: Snapshot of a portion 04InsertIntoUserOrganization script for SQL Server.....	15
Figure 11: File menu to open the database script file for MySQL	17
Figure 12: Open File dialog showing the available script for MySQL.....	18
Figure 13: Snapshot showing portion of 01CreateSchema script for MySQL.....	19
Figure 14: Snapshot showing portion of 02CreateUserAndRoles script for MySQL.....	19
Figure 15: Snapshot showing portion of 03InsertInitialRecord script for MySQL	21
Figure 16: Snapshot showing portion of 04InsertInitialRecord script for MySQL	22
Figure 17: Create new database context menu for PostgreSQL.....	24
Figure 18: Create new database dialog for PostgreSQL	25
Figure 19: Confirmation of EWAV database creation in PostgreSQL.....	26
Figure 20: SQL Editor windows for PostgreSQL	26
Figure 21: File menu to open the database script file for PostgreSQL	27
Figure 22: Open File dialog showing the available script for PostgreSQL.....	27
Figure 23: Snapshot showing portion of 01CreateScheam script for PostgreSQL.....	28
Figure 24: Snapshot showing portion of 02CreateUserAndRoles script for PostgreSQL.....	29
Figure 25: Snapshot showing portion of 03InsertInitialRecord script for PostgreSQL	30
Figure 26: Snapshot showing portion of 04InsertIntoUserOrganization script for PostgreSQL.....	31
Figure 27: Application pool configured using .NET 4.0.....	34
Figure 28: Application pool properties for windows authentication site	34
Figure 29: Setting Identity value for windows authentication application	35
Figure 30: Setting Identity value for windows authentication application	36
Figure 31: Choosing authentication setting.....	37
Figure 32: Enabling windows authentication setting.....	37
Figure 33: Confirming enabled and disabled authentication types.....	38
Figure 34: Web.config file for an integrated application under the file system of the web server	38
Figure 35: Generating the application encryption keys using EWAV Encryption utility for windows authentication application.....	41
Figure 36: Copying the keys section to update the keys section in the provided web.config file for windows authentication application	41
Figure 37: Encrypting connection string using EWAV Encryption utility for windows authentication application	43

Figure 38: Application pool configured using .NET 4.0.....	45
Figure 39: Setting Identity value for windows authentication application	45
Figure 40: Application configured with Anonymous Authentication Enabled	46
Figure 41: Web.config file for a forms authentication application.....	46
Figure 42: Generating the application encryption keys using EWAV Encryption utility for forms authentication application.....	48
Figure 43: Copying the keys section to update the keys section in the provided web.config file for forms authentication application.....	49
Figure 44: Encrypting connection string using EWAV Encryption utility for forms authentication application	50