EPI INFO^{TM} WEB ANALYTICS AND VISUALIZATION

MICROSOFT AZURE DEPLOYMENT GUIDE

Version 1.0

04/25/2014

VERSION HISTORY

Version #	**Implemented By**	**Revision Date**	**Comments**
1.0	Sachin Agnihotri	04/25/2014	Version 1.0 of the document

TABLE OF CONTENTS

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 in Microsoft Azure environment and will provide analytical and visualization capability for large public health datasets hosted in Microsoft Azure environment. The product also provides 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.
- **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.
    - **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.
    - **Encapsulated working environment:** Users from one organization can work on data sources in isolation from other groups.
    - **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: A Microsoft Azure Virtual Server with Windows server 2008/2008 R2 /2012/2012 R2
- Database server: Only needed if Meta database is configured on a SQL Server on a Windows Server 2008/2008 R2/2012/2012 R2 virtual machine in Microsoft Azure cloud.

Note: The system is designed to do all the processing and computations on the server. You will have to plan for server capacity both for Web Server and Database server depending on several factors including number of user expected to use the system, kind of reporting to be performed and the size of data sources you plan to use.

Software:

- On Microsoft Azure Virtual Server acting as the Web server:
  - Internet Information Services (IIS) 7.0 or higher
  - .NET 4.0/4.5
  - Microsoft Silverlight 5.0 (optional)
- Database server
  - No software needed if meta database is created as a SQL Database on Microsoft Azure SQL Databases Server
  - No software needed if data sources are configured as Mobile Service databases or as SQL Database on Microsoft Azure
  - SQL Server 2008/2008 R2/2012/2012 R2 database on Microsoft Azure SQL Server virtual machine if data sources are hosted on an independent virtual machine.
- Client
  - Microsoft Silverlight 5.0 runtime
- SMTP Server
  - Provide the name of an SMTP service such as GMAIL etc.

Operational activities:

- A system engineer, IT engineer with administrative access to Microsoft Azure Portal and Azure virtual server to configure the application.
- A system engineer/database administrator with administrative access on the Microsoft Azure portal to configure SQL Database and Azure SQL Server virtual machine if needed.

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 of 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 on the web server, 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 in Microsoft Azure SQL Databases, Mobile Services or Microsoft Azure virtual SQL Server machine that are accessible for analysis.

The diagram below summarizes these components and their interactions.

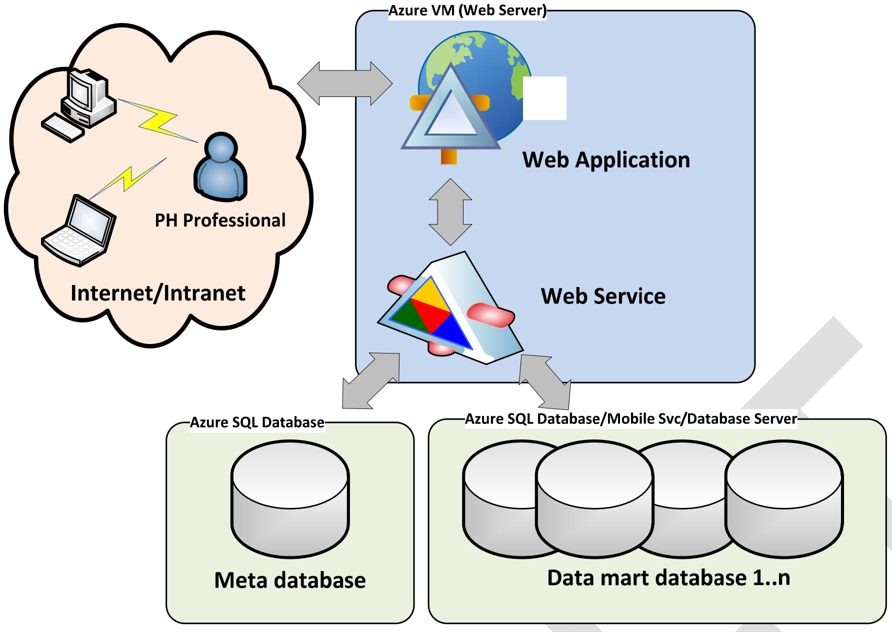


Figure 1: Overview of Epi Info™ Web Analytics & Visualization

The product may be configured for usage as a public facing internet application. The diagram below show the configuration for the product deployed as an application in Microsoft Azure environment.

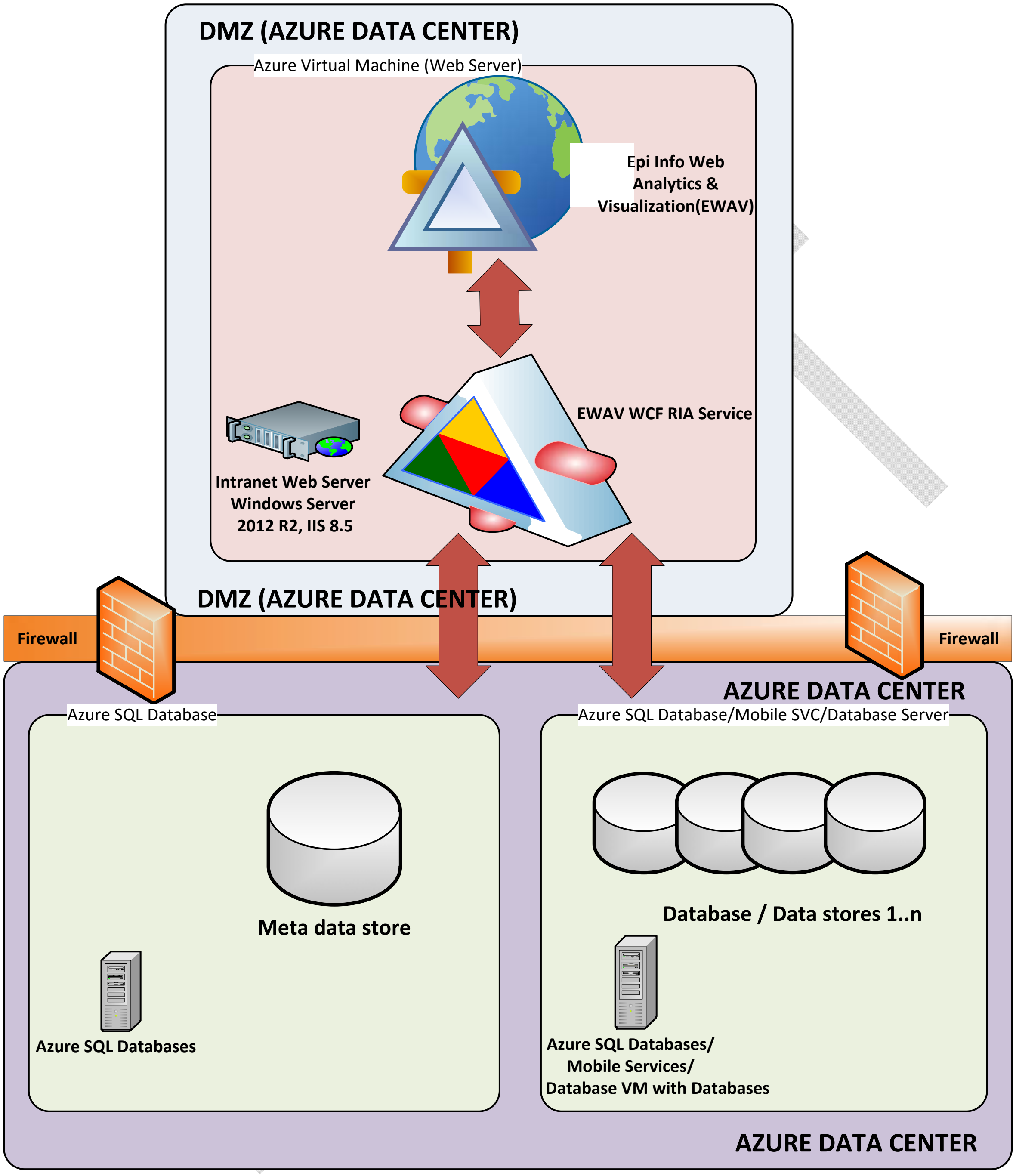

DMZ (AZURE DATA CENTER)
Azure Virtual Machine (Web Server)
Epi Info Web Analytics & Visualization(EWAV)
EWAV WCF RIA Service
Intranet Web Server Windows Server 2012 R2, IIS 8.5
DMZ (AZURE DATA CENTER)
Firewall
Firewall
AZURE DATA CENTER
Azure SQL Database
Meta data store
Azure SQL Databases
Azure SQL Database/Mobile SVC/Database Server
Database / Data stores 1..n
Azure SQL Databases/ Mobile Services/ Database VM with Databases
AZURE DATA CENTER

Figure 2: Configuration of EWAV in Azure Data Center

3. APPLICATION INSTALLATION

3.1 ACCESS CONTROLS

3.1.1 Database

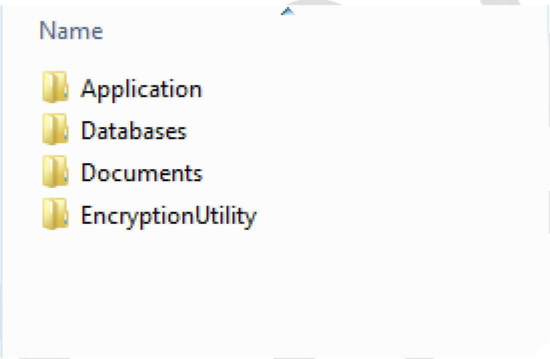
The person creating and configuring the database should have a Microsoft Azure Portal account with the ability to create SQL Databases in the Portal along with knowledge on how to create and configure the database in the Portal. afafafafafa

3.1.2 Application and Services

The person installing and configuring the application and services should have administrative access on the Microsoft Azure virtual machine to configure the server, install Internet Information Services (IIS) and create the application.

3.2 INSTALLATION

The installation can be done using the **EWAV_Azure** 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.



Name

- Application
- Databases
- Documents
- EncryptionUtility

Figure 3: File system showing components in the EWAV Package

3.3 CONFIGURATION

3.3.1 Database Configuration

The deployment package comes with “Databases” folder containing scripts to configure Meta database as a SQL Database in Microsoft Azure SQL Databases server needed by the application.

3.3.1.1 Prerequisites for database configuration

Following prerequisites must be in place to be able to configure the Meta database for EWAV application.

1. A SQL Database in Microsoft Azure Portal
2. Connection string for the SQL database created in Microsoft Azure Portal.
3. Access to tools to execute scripts for SQL Database in Microsoft Azure. Some options are SQL Server 2008/2008 R2/2012/2012 R2 management studio or access to Visual Studio 2012 or 2013. More information can be found at: http://msdn.microsoft.com/en-US/library/azure/ee621784.aspx#ssms

3.3.1.2 Configuring SQL Server database

The prerequisite step created an empty SQL Database which does not have any database objects. The configuration process will create the schema, user and assign necessary privileges for the application to be able to work with the database. Follow the steps outlined below to configure the SQL Database:

1. Provide following information to connect to SQL Database in Windows Azure.

  a. Server type: Database Engine

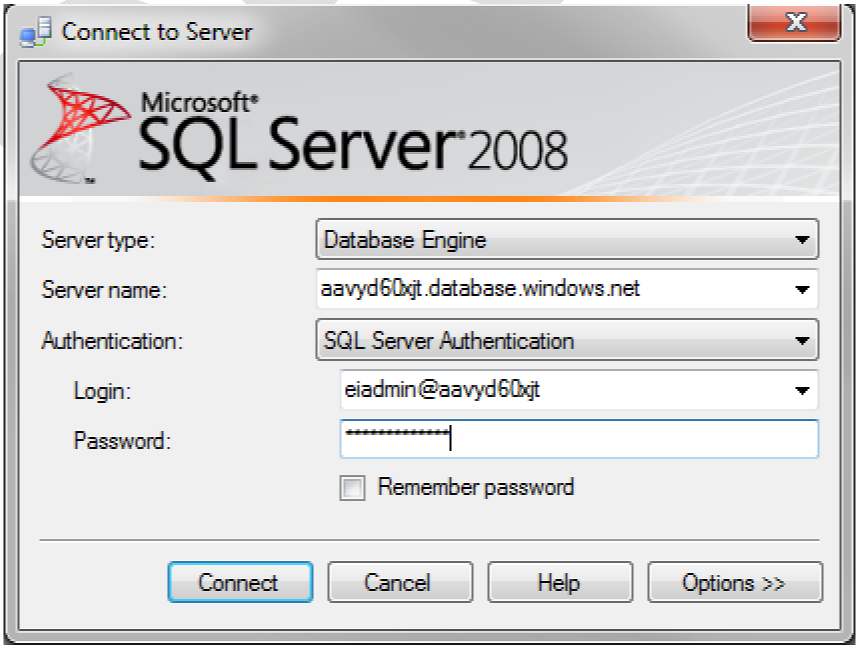
  b. Server name: SQL Database server name. Port number does not need to be specified

    ☐ Example: aavyd60xjt.database.windows.net

  c. Authentication: SQL Server Authentication

    ☐ Login: User ID provided in connection string.

    ☐ Password: Password created during database creation



Server type: Database Engine

Server name: aavyd60xjt.database.windows.net

Authentication: SQL Server Authentication

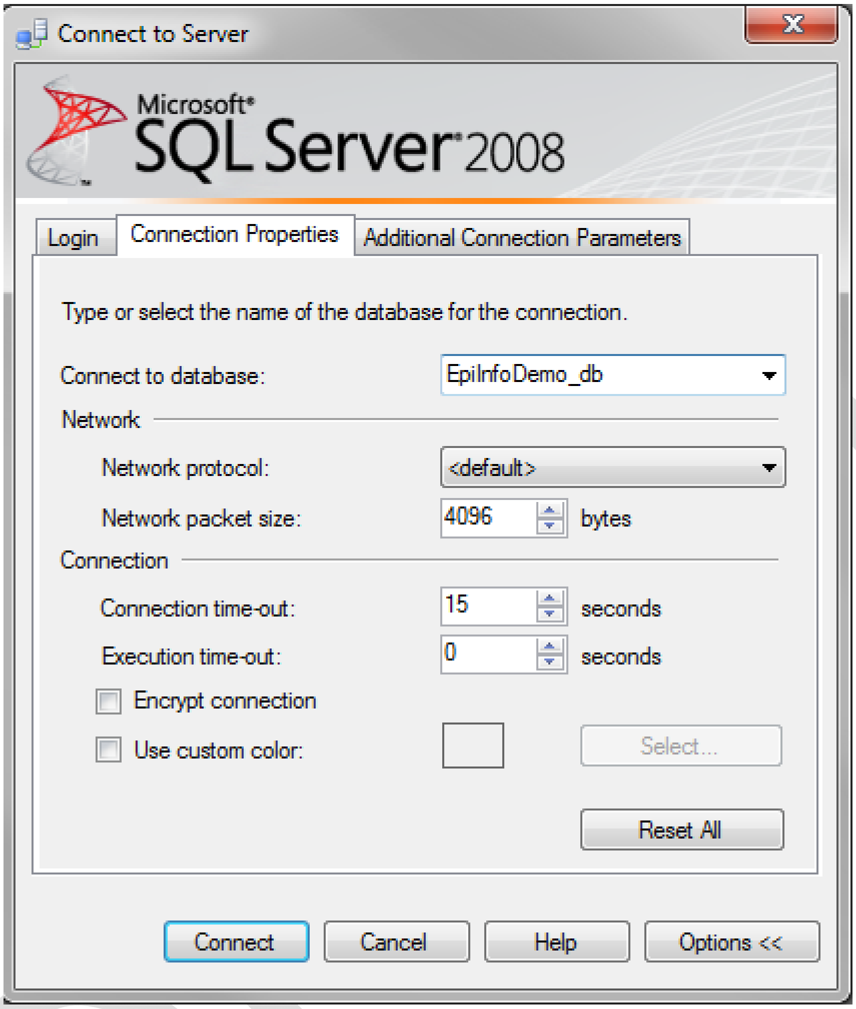
Login: eiadmin@aavyd60xjt

Password: **************

☐ Remember password

Figure 4: SQL Server connection dialog to connect to SQL Databases server in Azure

2. Click on Options and provide the name of the database to connect to. This name should match the name provided in the connection string. Click on Connect to connect to the database.



Type or select the name of the database for the connection.

Connect to database: EpiInfoDemo_db

Network

Network protocol: <default>

Network packet size: 4096 bytes

Connection

Connection time-out: 15 seconds

Execution time-out: 0 seconds

☐ Encrypt connection

☐ Use custom color:

Figure 5: SQL Server connection properties specifying SQL Database to connect to in Azure SQL Databases

3. Open the provided script name “01CreateSchema_Azure.sql” in SQL Server Management Studio or your tool of choice.

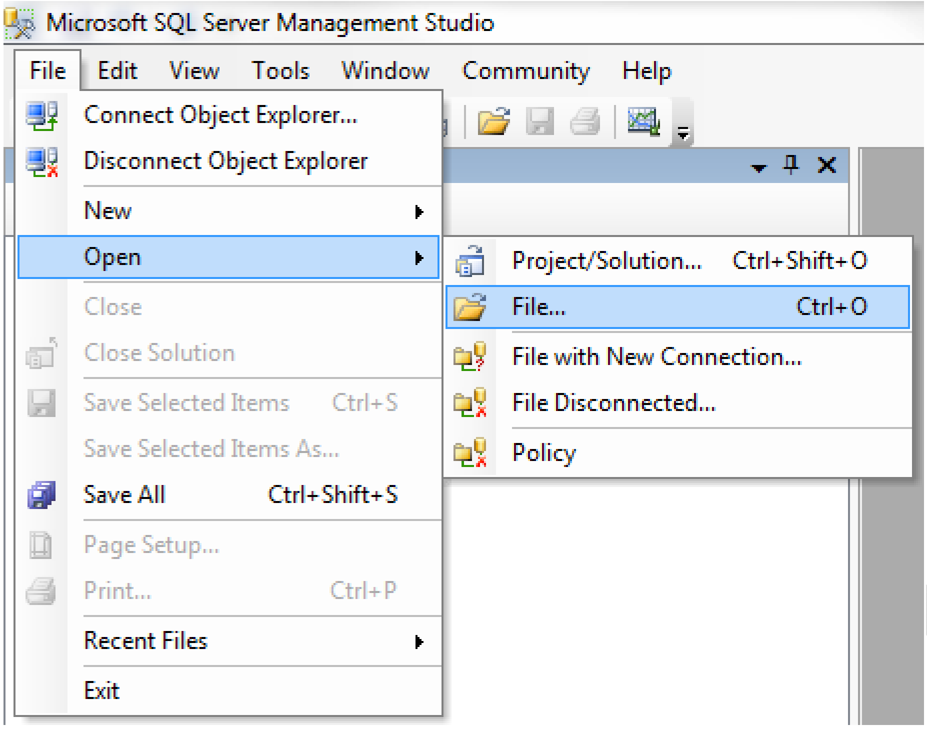

Microsoft SQL Server Management Studio
File
Edit
View
Tools
Window
Community
Help
Connect Object Explorer...
Disconnect Object Explorer
New
Open
Close
Close Solution
Save Selected Items Ctrl+S
Save Selected Items As...
Save All Ctrl+Shift+S
Page Setup...
Print... Ctrl+P
Recent Files
Exit
Project/Solution... Ctrl+Shift+O
File... Ctrl+O
File with New Connection...
File Disconnected...
Policy

Figure 6: File menu to open the database script file for SQL Server

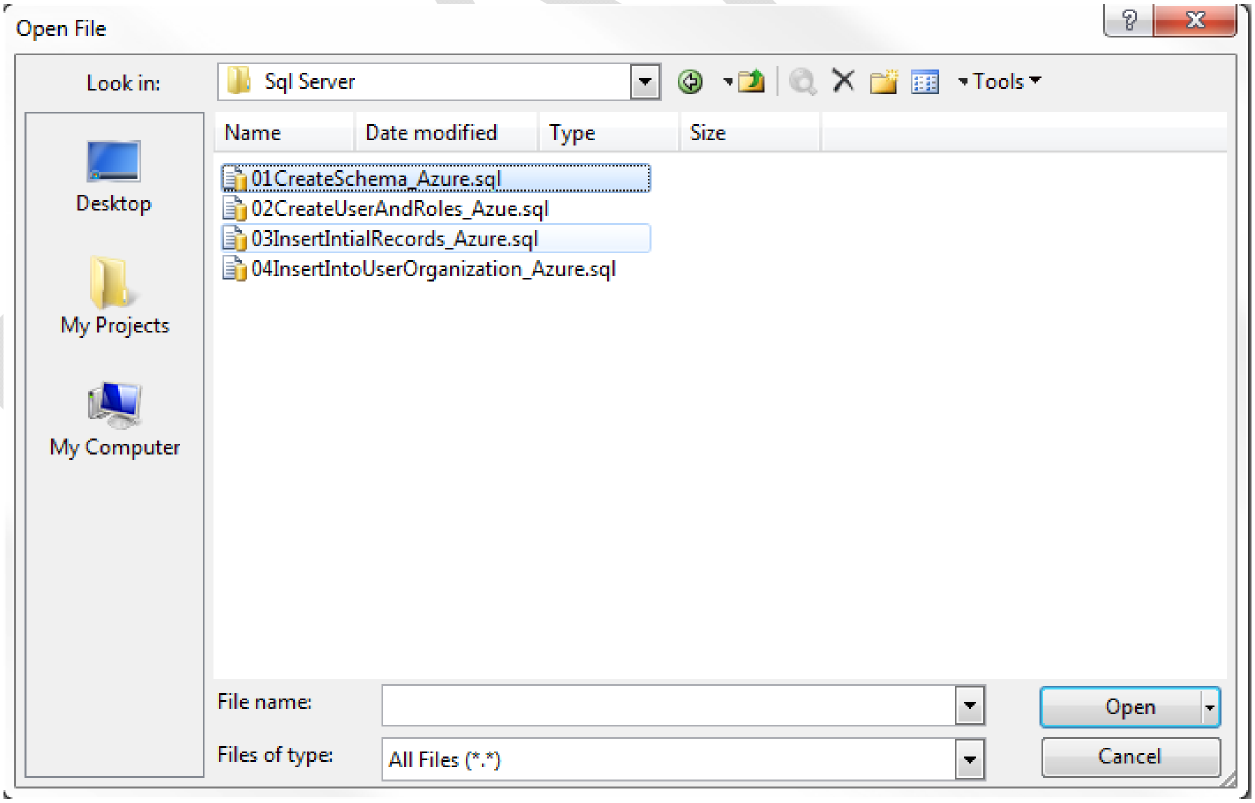
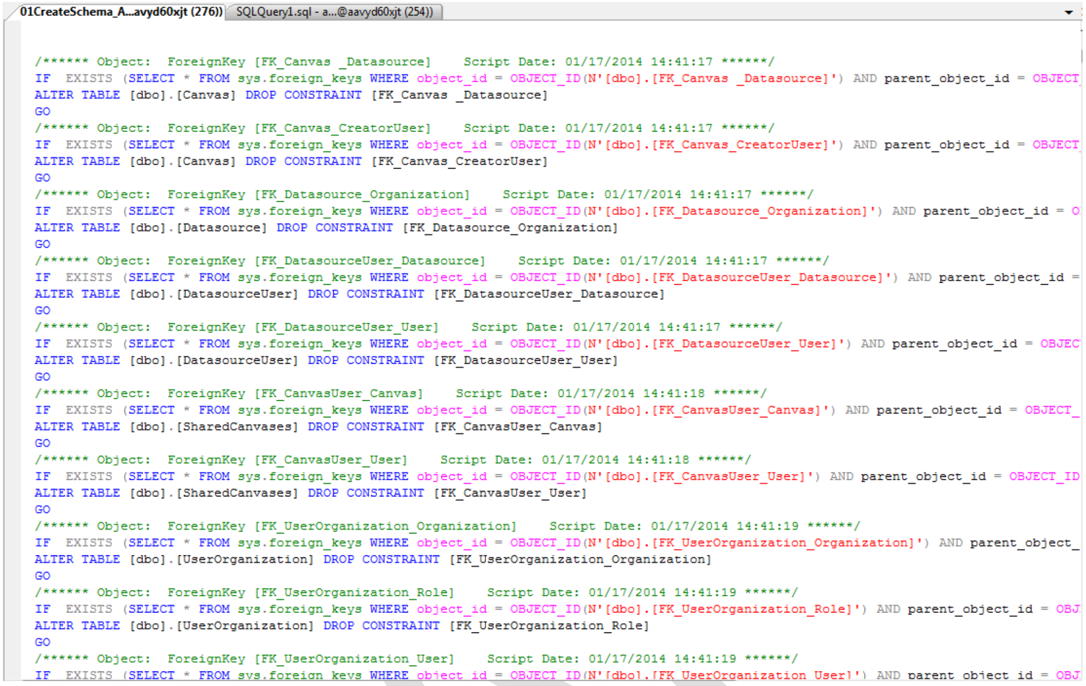


Figure 7: Open File dialog showing the available script for SQL Database in Microsoft Azure

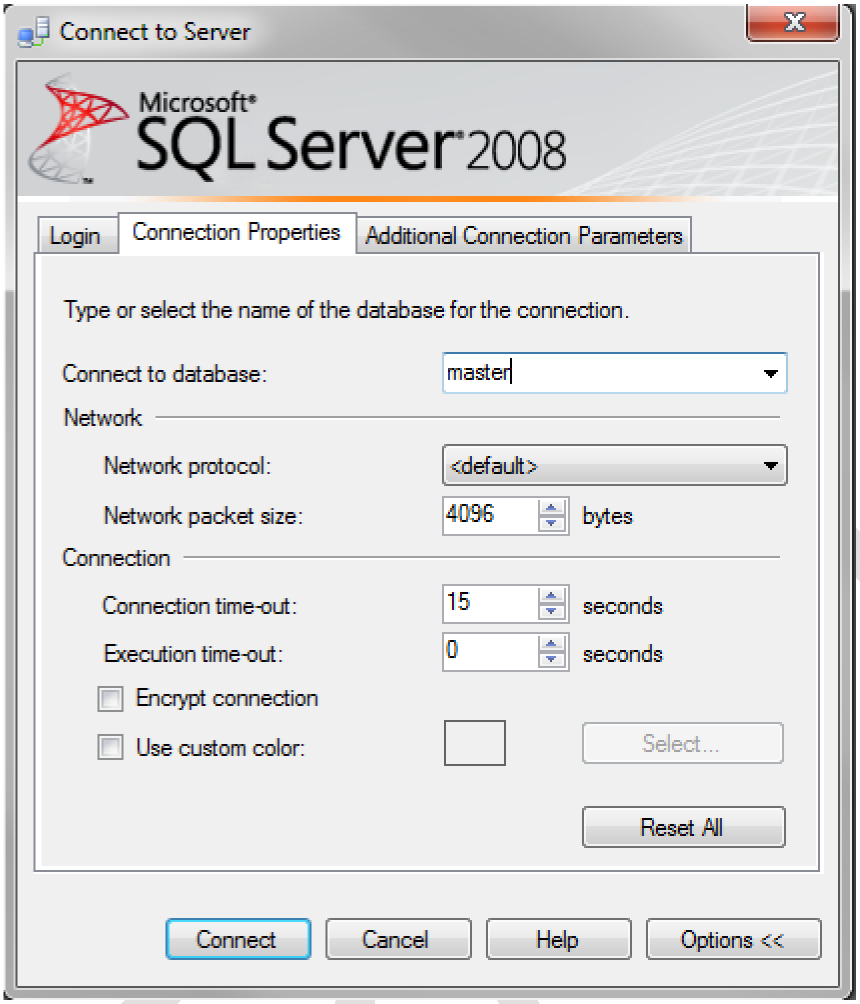
4. Execute the script 01CreateSchema_Azure.sql to create the schema in SQL database in Microsoft Azure.


01CreateSchema_A...avyd60xjt (276))
SQLQuery1.sql - a...@aavyd60xjt (254))

```
/****** Object:  ForeignKey [FK_Canvas _Datasource]    Script Date: 01/17/2014 14:41:17 ******/
IF  EXISTS (SELECT * FROM sys.foreign_keys WHERE object_id = OBJECT_ID(N'[dbo].[FK_Canvas _Datasource]') AND parent_object_id = OBJECT
ALTER TABLE [dbo].[Canvas] DROP CONSTRAINT [FK_Canvas _Datasource]
GO
/****** Object:  ForeignKey [FK_Canvas_CreatorUser]    Script Date: 01/17/2014 14:41:17 ******/
IF  EXISTS (SELECT * FROM sys.foreign_keys WHERE object_id = OBJECT_ID(N'[dbo].[FK_Canvas_CreatorUser]') AND parent_object_id = OBJECT
ALTER TABLE [dbo].[Canvas] DROP CONSTRAINT [FK_Canvas_CreatorUser]
GO
/****** Object:  ForeignKey [FK_Datasource_Organization]    Script Date: 01/17/2014 14:41:17 ******/
IF  EXISTS (SELECT * FROM sys.foreign_keys WHERE object_id = OBJECT_ID(N'[dbo].[FK_Datasource_Organization]') AND parent_object_id = O
ALTER TABLE [dbo].[Datasource] DROP CONSTRAINT [FK_Datasource_Organization]
GO
/****** Object:  ForeignKey [FK_DatasourceUser_Datasource]    Script Date: 01/17/2014 14:41:17 ******/
IF  EXISTS (SELECT * FROM sys.foreign_keys WHERE object_id = OBJECT_ID(N'[dbo].[FK_DatasourceUser_Datasource]') AND parent_object_id =
ALTER TABLE [dbo].[DatasourceUser] DROP CONSTRAINT [FK_DatasourceUser_Datasource]
GO
/****** Object:  ForeignKey [FK_DatasourceUser_User]    Script Date: 01/17/2014 14:41:17 ******/
IF  EXISTS (SELECT * FROM sys.foreign_keys WHERE object_id = OBJECT_ID(N'[dbo].[FK_DatasourceUser_User]') AND parent_object_id = OBJEC
ALTER TABLE [dbo].[DatasourceUser] DROP CONSTRAINT [FK_DatasourceUser_User]
GO
/****** Object:  ForeignKey [FK_CanvasUser_Canvas]    Script Date: 01/17/2014 14:41:18 ******/
IF  EXISTS (SELECT * FROM sys.foreign_keys WHERE object_id = OBJECT_ID(N'[dbo].[FK_CanvasUser_Canvas]') AND parent_object_id = OBJECT_
ALTER TABLE [dbo].[SharedCanvases] DROP CONSTRAINT [FK_CanvasUser_Canvas]
GO
/****** Object:  ForeignKey [FK_CanvasUser_User]    Script Date: 01/17/2014 14:41:18 ******/
IF  EXISTS (SELECT * FROM sys.foreign_keys WHERE object_id = OBJECT_ID(N'[dbo].[FK_CanvasUser_User]') AND parent_object_id = OBJECT_ID
ALTER TABLE [dbo].[SharedCanvases] DROP CONSTRAINT [FK_CanvasUser_User]
GO
/****** Object:  ForeignKey [FK_UserOrganization_Organization]    Script Date: 01/17/2014 14:41:19 ******/
IF  EXISTS (SELECT * FROM sys.foreign_keys WHERE object_id = OBJECT_ID(N'[dbo].[FK_UserOrganization_Organization]') AND parent_object_
ALTER TABLE [dbo].[UserOrganization] DROP CONSTRAINT [FK_UserOrganization_Organization]
GO
/****** Object:  ForeignKey [FK_UserOrganization_Role]    Script Date: 01/17/2014 14:41:19 ******/
IF  EXISTS (SELECT * FROM sys.foreign_keys WHERE object_id = OBJECT_ID(N'[dbo].[FK_UserOrganization_Role]') AND parent_object_id = OBJ
ALTER TABLE [dbo].[UserOrganization] DROP CONSTRAINT [FK_UserOrganization_Role]
GO
/****** Object:  ForeignKey [FK_UserOrganization_User]    Script Date: 01/17/2014 14:41:19 ******/
IF  EXISTS (SELECT * FROM sys.foreign_keys WHERE object_id = OBJECT_ID(N'[dbo].[FK_UserOrganization_User]') AND parent_object_id = OBJ
```

Figure 8: Snapshot of a portion of 01CreateSchema_Azure script for SQL Server

5. Open Script titled “02CreateUserAndRoles_Azure.SQL” in your editor of choice. There are multiple scripts provided in this file to be executed in the order specified.
6. Connect to master database using the admin login account that was used to connect to your SQL Database.



Type or select the name of the database for the connection.

Connect to database: master

Network

Network protocol: <default>

Network packet size: 4096 bytes

Connection

Connection time-out: 15 seconds

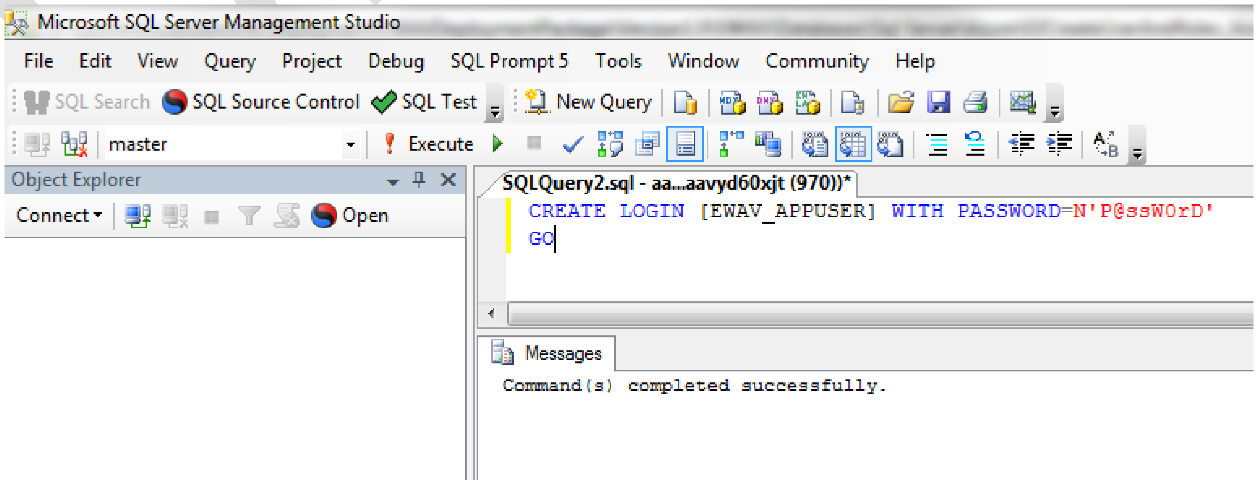
Execution time-out: 0 seconds

☐ Encrypt connection

☐ Use custom color:

Figure 9: Connection Properties specifying connecting to master database in SQL Databases server in Azure

7. Replace the Password with a strong password that meets your organization’s password policy. Execute the first script to create a new Login named EWAV_APPUSER.

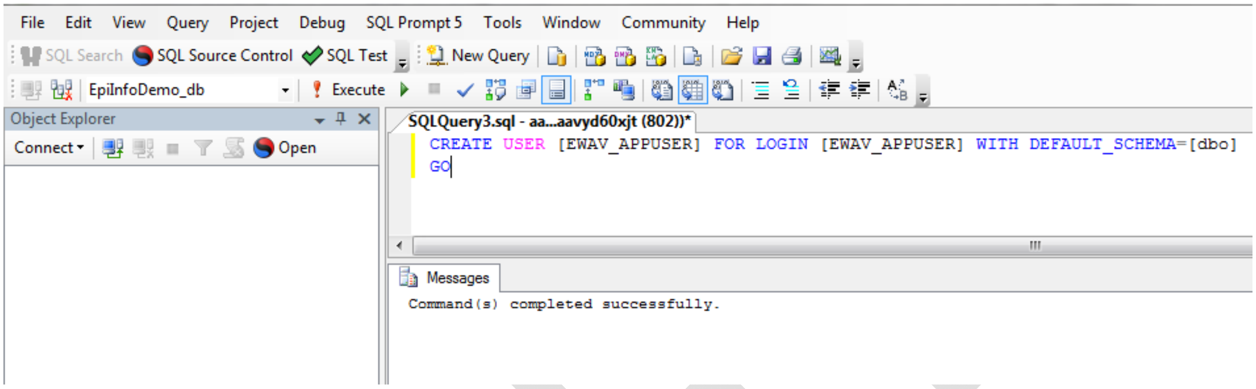


```
CREATE LOGIN [EWAV_APPUSER] WITH PASSWORD=N'P@ssW0rD'
GO
```

```
Command(s) completed successfully.
```

Figure 10: Executing the script to create Login in master database

8. Disconnect from the master database and connect back again to your SQL Database and create the user for the new login along with assigning it the dbo role.

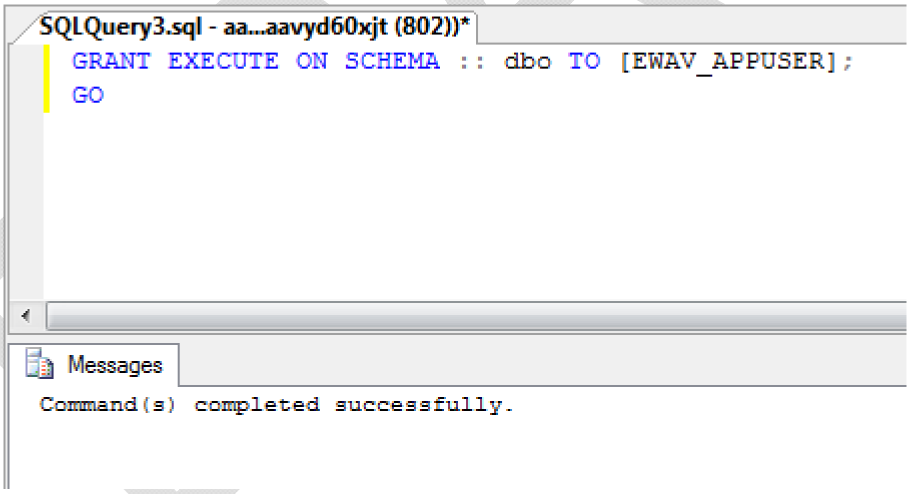


```
CREATE USER [EWAV_APPUSER] FOR LOGIN [EWAV_APPUSER] WITH DEFAULT_SCHEMA=[dbo]
GO
```

```
Command(s) completed successfully.
```

Figure 11: Executing the script to create user

9. Execute the script to grant execute permission to newly created user on dbo schema.

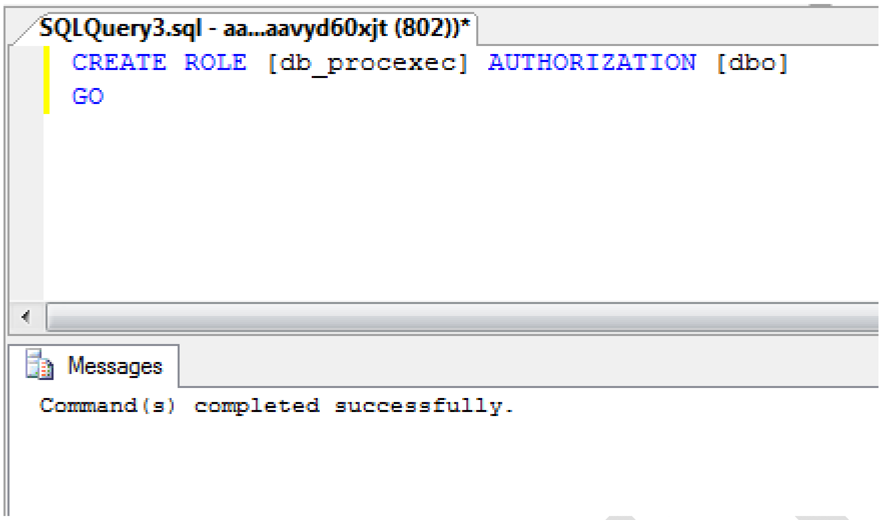


```
GRANT EXECUTE ON SCHEMA :: dbo TO [EWAV_APPUSER];
GO
```

```
Command(s) completed successfully.
```

Figure 12: Executing the script to grant execute permission

10. Execute the script to create a role called db_procexec.

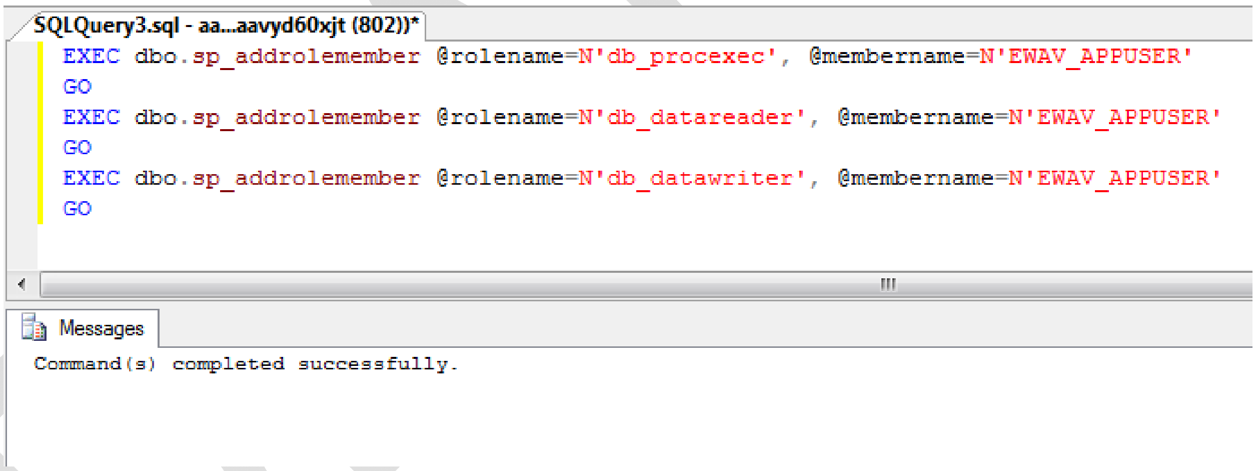


```
CREATE ROLE [db_procexec] AUTHORIZATION [dbo]
GO
```

```
Command(s) completed successfully.
```

Figure 13: Executing the script to create role

11. Execute the remaining three scripts for assigning privilege to user EWAV_APPUSER.



```
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
```

```
Command(s) completed successfully.
```

Figure 14: Executing the script to assign privileges

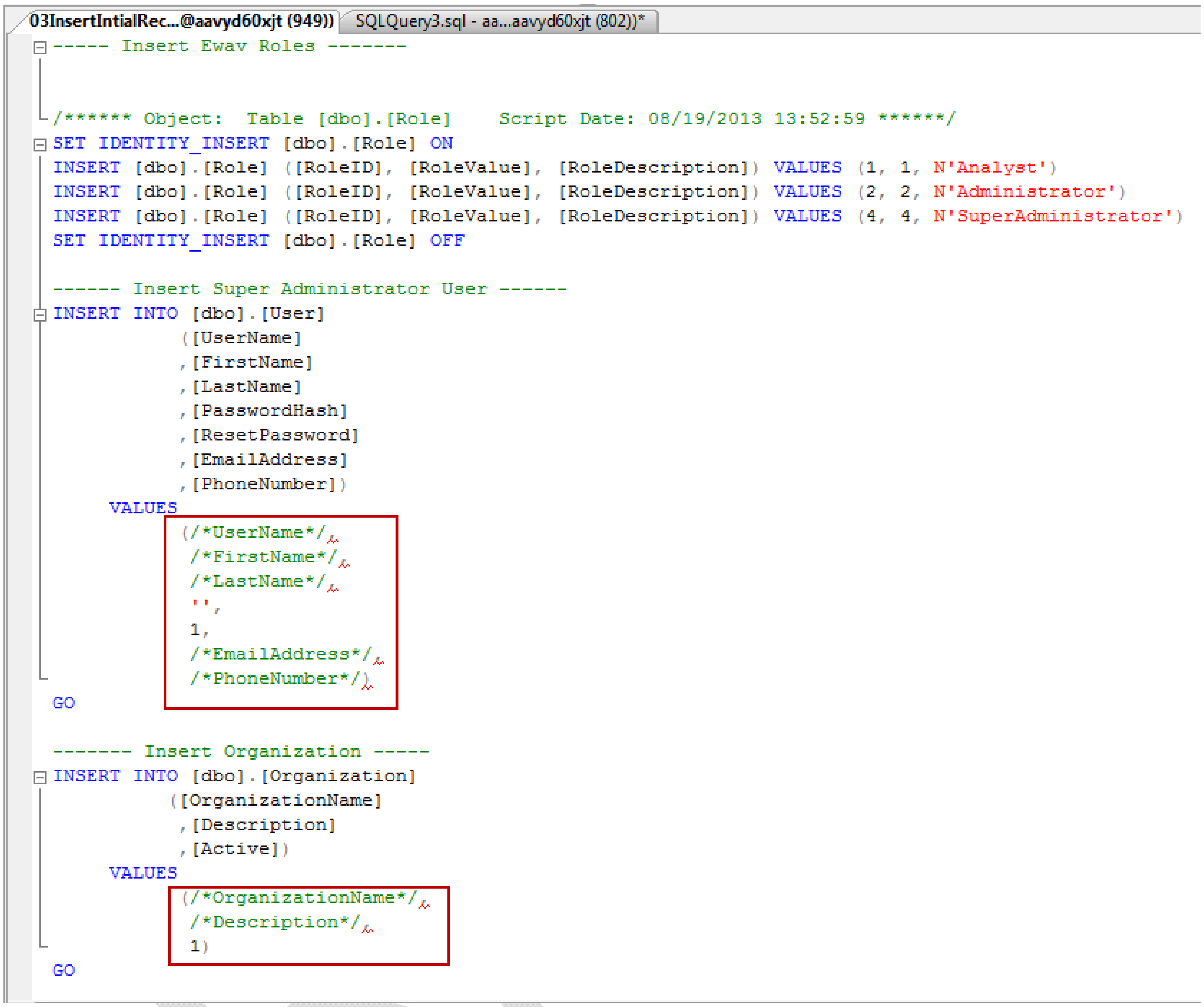
Note: The application can connect to SQL Database using either SQL Database credential used so far or EWAV_APPUSER account with its password. Provide the complete connection string to the person configuring the application on the web server.

12. Open script “03InsertInitialRecord_Azure.sql”. 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 a valid Email address.
    - /*FirstName*/
    - /*LastName*/
    - /*EmailAddress*/
    - /*PhoneNumber*/

    For Organization, replace following placeholders with relevant values:

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


03InsertIntialRec...@aavyd60xjt (949))
SQLQuery3.sql - aa...aavyd60xjt (802))*

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

/****** 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 [dbo].[User]
           ([UserName]
           ,[FirstName]
           ,[LastName]
           ,[PasswordHash]
           ,[ResetPassword]
           ,[EmailAddress]
           ,[PhoneNumber])
     VALUES
           (/*UserName*/,
            /*FirstName*/,
            /*LastName*/,
            '',
            1,
            /*EmailAddress*/,
            /*PhoneNumber*/)
GO

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

Figure 15: Snapshot of a portion 03InsertInitialRecord script for SQL Server

Sample script is provided below:

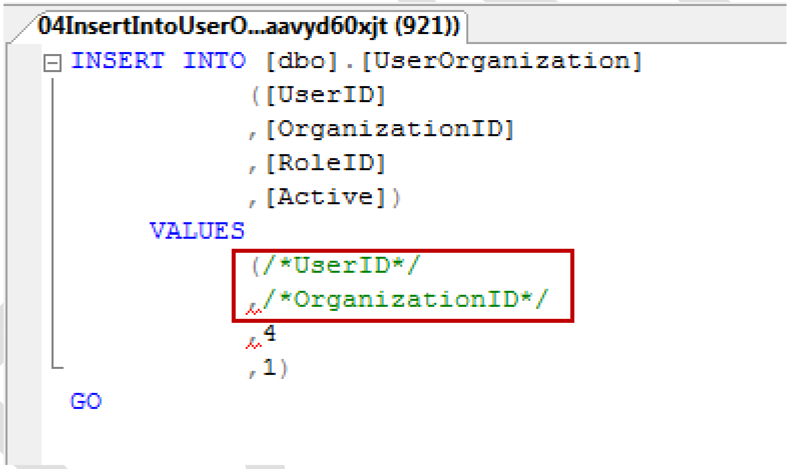
```
INSERT INTO [dbo].[User]
           ([UserName]
           ,[FirstName]
           ,[LastName]
           ,[PasswordHash]
           ,[ResetPassword]
           ,[EmailAddress]
           ,[PhoneNumber])
VALUES
           ('useremail@org.gov'
           ,'UserFirstName'
           ,'UserLastName'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

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

GO
```

13. Open script “04InsertIntoUserOrganization_Azure.sql”. 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:

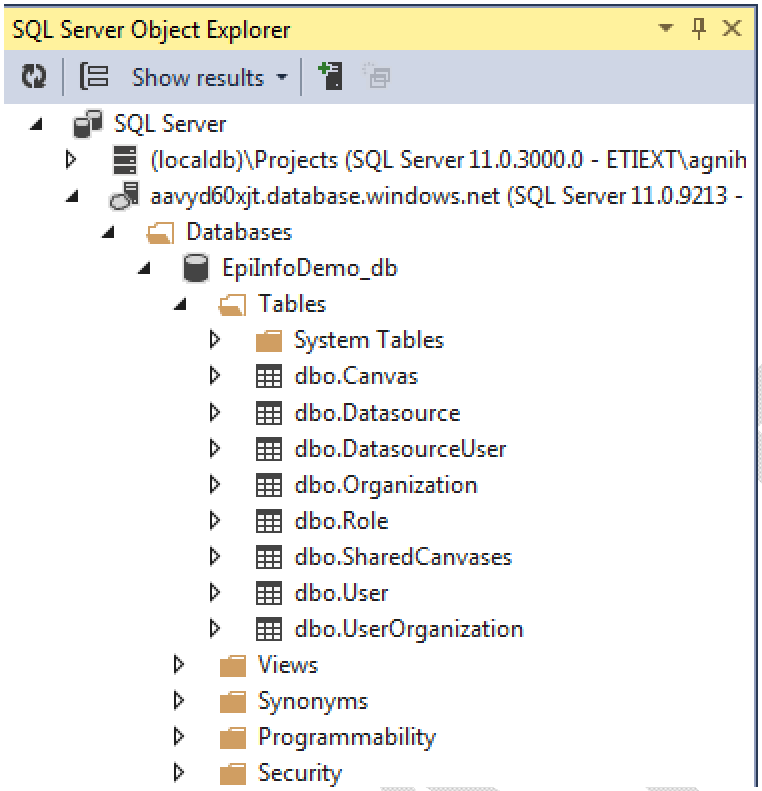
    - /*UserID*/
    - /*OrganizationID*/



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

Figure 16: Snapshot of a portion 03InsertInitialRecord 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. Open the database table in SQL Server Object Explorer of your choice or in the tool you have used so far to run the scripts.



- SQL Server
  - (localdb)\Projects (SQL Server 11.0.3000.0 - ETIEXT\agnih
  - aavyd60xjt.database.windows.net (SQL Server 11.0.9213 -
    - Databases
      - EpiInfoDemo_db
        - Tables
          - System Tables
          - dbo.Canvas
          - dbo.Datasource
          - dbo.DatasourceUser
          - dbo.Organization
          - dbo.Role
          - dbo.SharedCanvases
          - dbo.User
          - dbo.UserOrganization
        - Views
        - Synonyms
        - Programmability
        - Security

Figure 17: Object explorer showing tables created in SQL Databases server in Microsoft Azure

Sample script is provided below:

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

3.3.2 Application Configuration

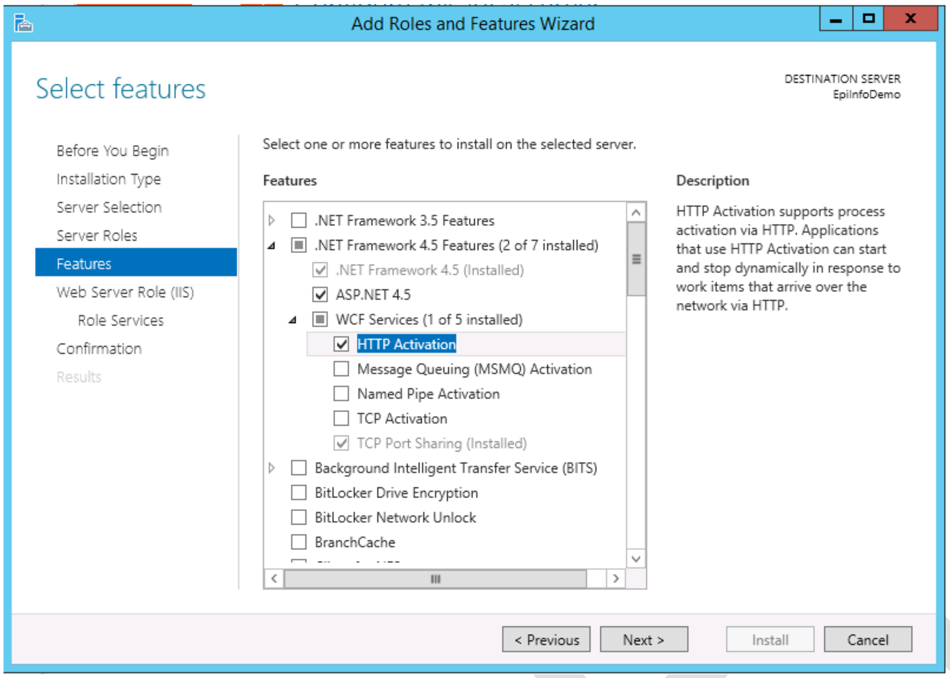
The deployment package comes with “Application” folder containing all the files needed for configuration of Epi Info Web Analytics and Visualization product on Microsoft Azure virtual machine web server. In Microsoft Azure environment the application is deployed as an outward facing application as Forms authenticated application that prompts the user to provide username and password before using the application.

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.

3.3.2.1 Prerequisites for Application configuration

Following prerequisites must be completed before configuring the application.

1. Microsoft Azure virtual machine
    a. Create a Windows Server 2012/2012 R2 virtual machine using Microsoft Azure portal
    b. Open port 8443 for remote desktop, port 80 for inbound and outbound web traffic and port 1433 for communication with database.
2. Install Internet Information Service (IIS) Web Server with needed features
    a. While Installing IIS make sure .NET Framework 4.5 is already installed.
    b. While Installing IIS in the Features selection step make sure you have chosen ASP.NET 4.5 and HTTP Activation under WCF Services.



Select features

DESTINATION SERVER
EpiInfoDemo

Select one or more features to install on the selected server.

Features

- ☐ .NET Framework 3.5 Features
- ▣ .NET Framework 4.5 Features (2 of 7 installed)
  - ☑ .NET Framework 4.5 (Installed)
  - ☑ ASP.NET 4.5
  - ▣ WCF Services (1 of 5 installed)
    - ☑ HTTP Activation
    - ☐ Message Queuing (MSMQ) Activation
    - ☐ Named Pipe Activation
    - ☐ TCP Activation
    - ☑ TCP Port Sharing (Installed)
- ☐ Background Intelligent Transfer Service (BITS)
- ☐ BitLocker Drive Encryption
- ☐ BitLocker Network Unlock
- ☐ BranchCache

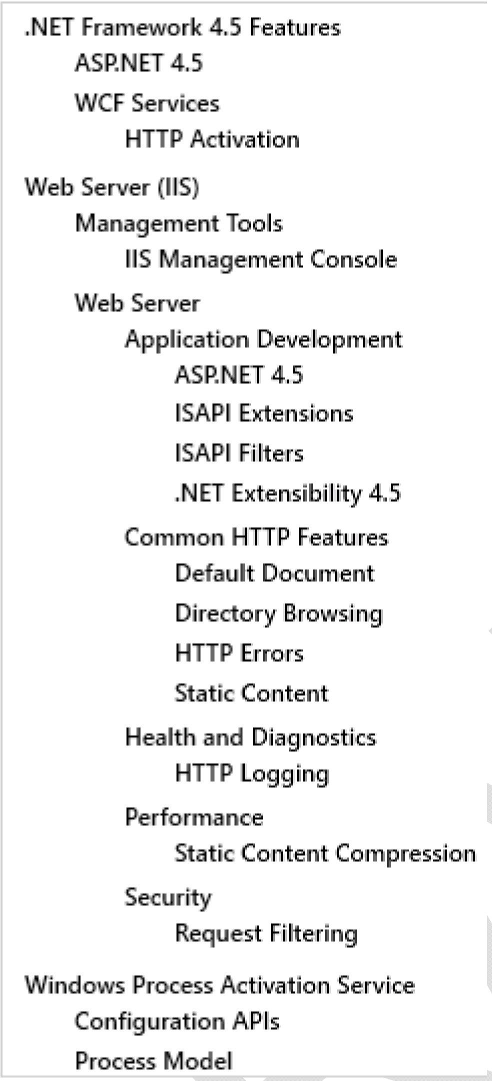
Description

HTTP Activation supports process activation via HTTP. Applications that use HTTP Activation can start and stop dynamically in response to work items that arrive over the network via HTTP.

Figure 18: List of features to be enabled during IIS Web Server install

c. Information on how to install IIS on Windows Server 2012 can be found at: http://www.iis.net/learn/install/installing-iis-85/installing-iis-85-on-windows-server-2012-r2

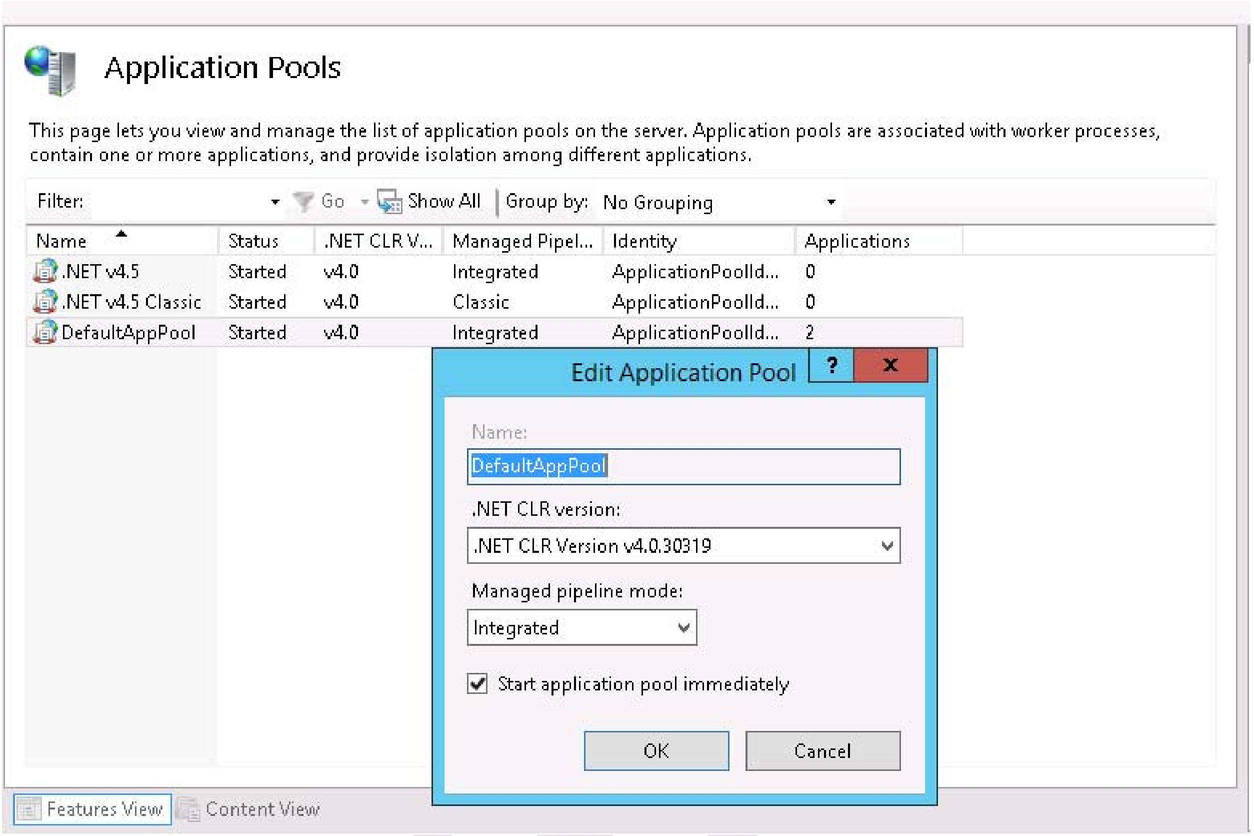
d. Below is a complete list of components and features that should be installed as part of IIS install



- .NET Framework 4.5 Features
  - ASP.NET 4.5
  - WCF Services
    - HTTP Activation
- Web Server (IIS)
  - Management Tools
    - IIS Management Console
  - Web Server
    - Application Development
      - ASP.NET 4.5
      - ISAPI Extensions
      - ISAPI Filters
      - .NET Extensibility 4.5
    - Common HTTP Features
      - Default Document
      - Directory Browsing
      - HTTP Errors
      - Static Content
    - Health and Diagnostics
      - HTTP Logging
    - Performance
      - Static Content Compression
    - Security
      - Request Filtering
- Windows Process Activation Service
  - Configuration APIs
  - Process Model

Figure 19: List of all features installed presented after IIS Web Server install

3. Configure IIS Web Server
   1. Application Pool.
      1. You can create a new application pool that uses .NET 4.0 or can use one of the default application pool that uses .NET 4.0
      2. Confirm that the application pool uses the Managed pipeline mode of integrated



Application Pools

This page lets you view and manage the list of application pools on the server. Application pools are associated with worker processes, contain one or more applications, and provide isolation among different applications.

Name	Status	.NET CLR V...	Managed Pipel...	Identity	Applications
.NET v4.5	Started	v4.0	Integrated	ApplicationPoolId...	0
.NET v4.5 Classic	Started	v4.0	Classic	ApplicationPoolId...	0
DefaultAppPool	Started	v4.0	Integrated	ApplicationPoolId...	2

Edit Application Pool

Name: DefaultAppPool

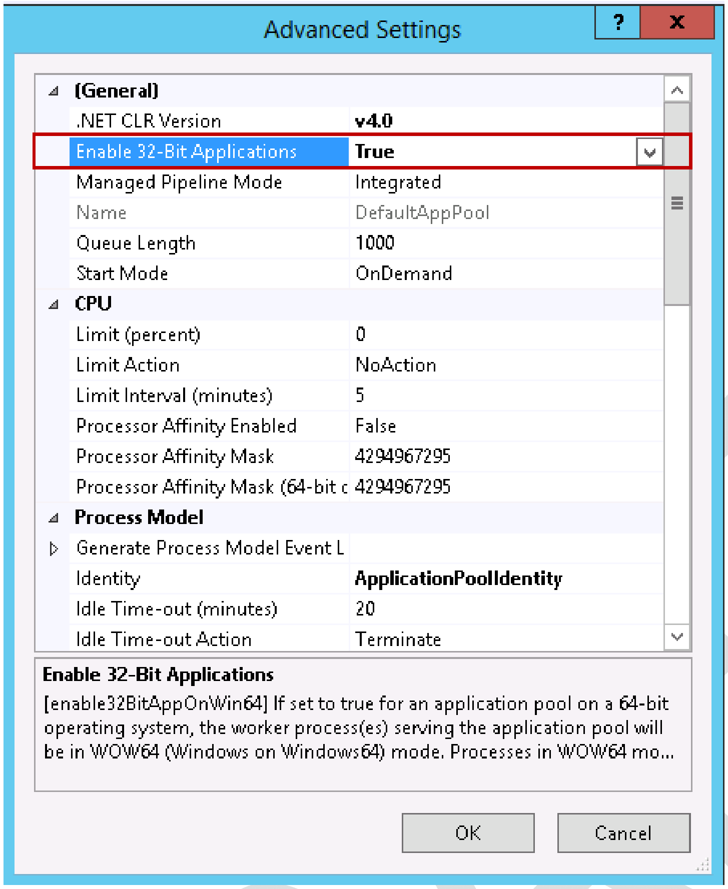
.NET CLR version: .NET CLR Version v4.0.30319

Managed pipeline mode: Integrated

☑ Start application pool immediately

Figure 20: Confirming .NET version and managed pipeline mode

iii. Set 32-Bit applications feature on for the chosen application pool by opening the Advance Settings for the application pool. The screenshot below shows Advanced Settings for application pool named “DefaultAppPool”.



(General)	
.NET CLR Version	**v4.0**
Enable 32-Bit Applications	**True**
Managed Pipeline Mode	Integrated
Name	DefaultAppPool
Queue Length	1000
Start Mode	OnDemand
CPU	
Limit (percent)	0
Limit Action	NoAction
Limit Interval (minutes)	5
Processor Affinity Enabled	False
Processor Affinity Mask	4294967295
Processor Affinity Mask (64-bit c	4294967295
Process Model	
Generate Process Model Event L	
Identity	**ApplicationPoolIdentity**
Idle Time-out (minutes)	20
Idle Time-out Action	Terminate

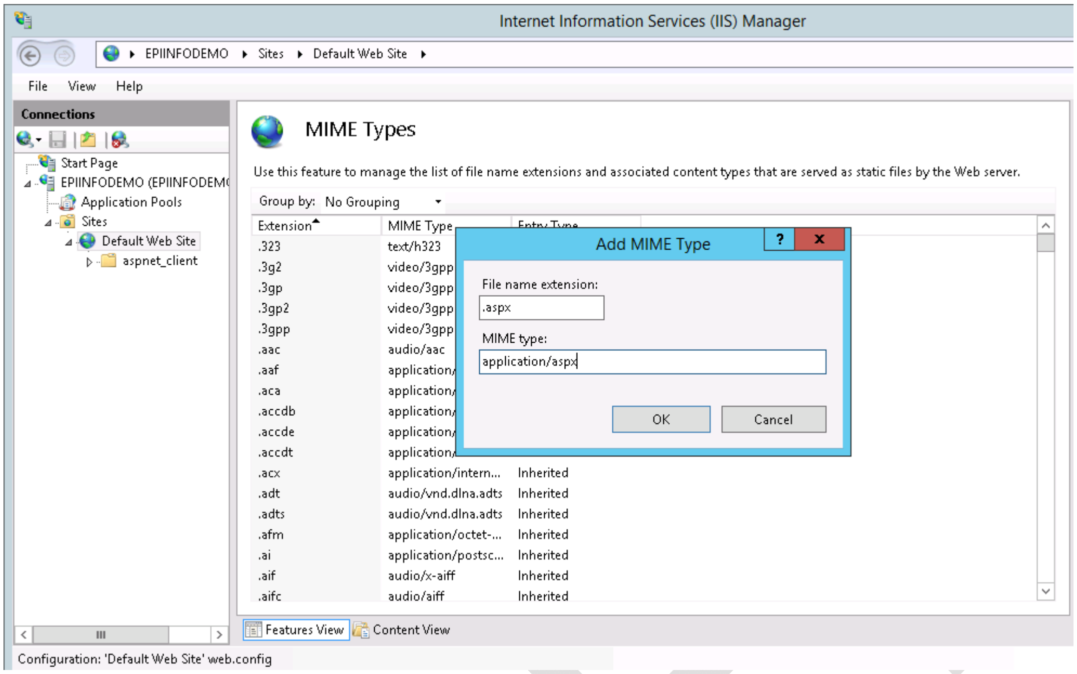
Enable 32-Bit Applications

[enable32BitAppOnWin64] If set to true for an application pool on a 64-bit operating system, the worker process(es) serving the application pool will be in WOW64 (Windows on Windows64) mode. Processes in WOW64 mo...

Figure 21: Enabling 32-bit for application pool

b. Configure MIME Types

   i. Add the MIME type ".aspx" if not already present for Default Web Site by providing value of ".aspx" for File name extension and value of "application/aspx" for MIME type.



Use this feature to manage the list of file name extensions and associated content types that are served as static files by the Web server.

Extension	MIME Type	Entry Type
.323	text/h323	
.3g2	video/3gpp	
.3gp	video/3gpp	
.3gp2	video/3gpp	
.3gpp	video/3gpp	
.aac	audio/aac	
.aaf	application/	
.aca	application/	
.accdb	application/	
.accde	application/	
.accdt	application/	
.acx	application/intern...	Inherited
.adt	audio/vnd.dlna.adts	Inherited
.adts	audio/vnd.dlna.adts	Inherited
.afm	application/octet-...	Inherited
.ai	application/postsc...	Inherited
.aif	audio/x-aiff	Inherited
.aifc	audio/aiff	Inherited

File name extension: .aspx

MIME type: application/aspx

Configuration: 'Default Web Site' web.config

Figure 22: Adding MIME type for handling ASPX pages

3.3.2.2 Configure EWAV on Web Sever

The EWAV configuration deploys the application as a single integrated application on the Internet Information Services (IIS) web server with both the application and its services under one site.

The prerequisite step installed Internet Information Services (IIS) and other needed components and set up the application pool to be used by the application. Follow the steps provided below to configure EWAV application:

1. Create a folder called “EWAV” under “intepub\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

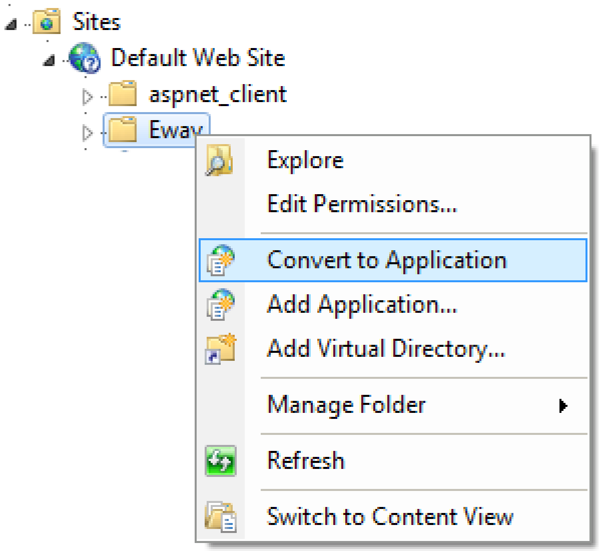
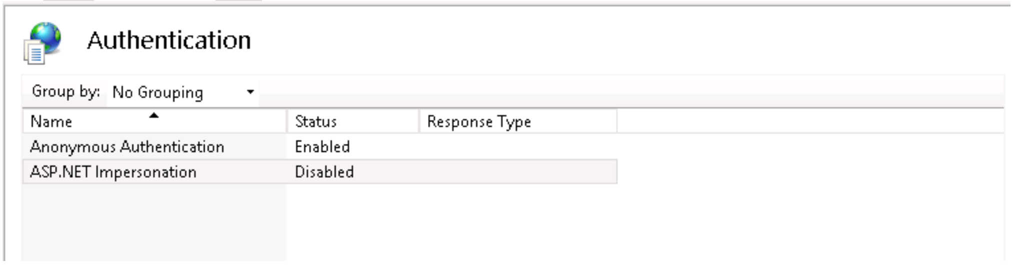


Figure 23: Converting EWAV to application in IIS

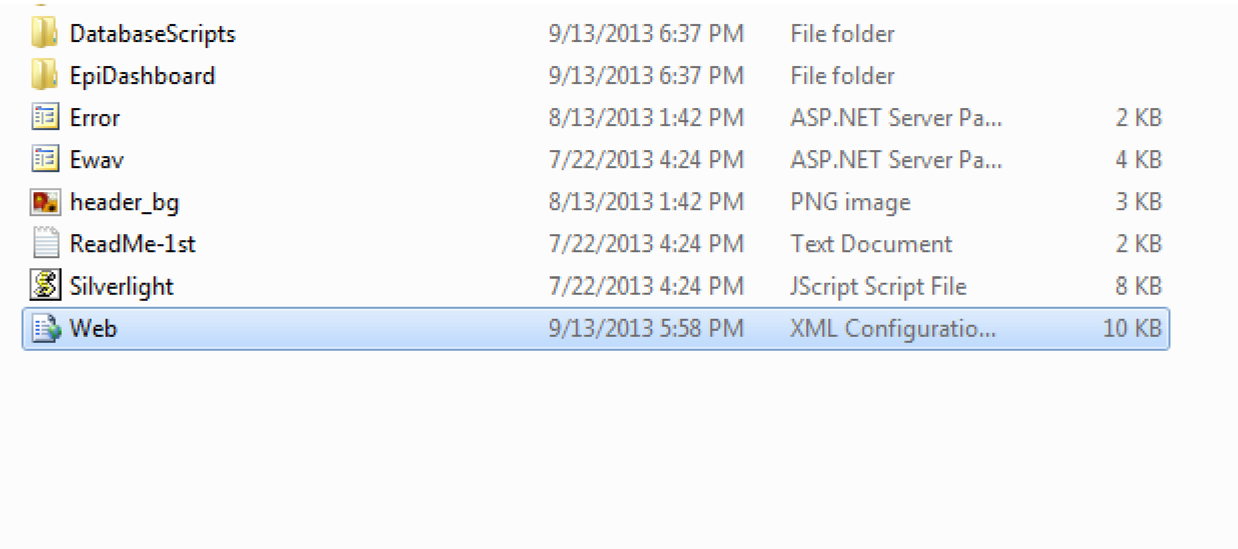
4. Make sure that the site is configured to run on the Application pool that you have configured to be used by the application in the prerequisites process
5. Once the site is converted to application, make sure the site uses Anonymous authentication only. This is the default setting when the site is configured in IIS.



Name	Status	Response Type
Anonymous Authentication	Enabled	
ASP.NET Impersonation	Disabled	

Figure 24: Confirming EWAV site uses Anonymous authentication

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



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 25: Web.config file for a forms authentication application

7. 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">
```

8. 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="XXXXXXXXXXXXXX"/>
<add key="EMAIL_TO" value="XXXXXXXXXXXXXX"/>
<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.

For Simple scenarios a GMAIL account can be used in Microsoft Azure environment for sending an email. If using GMAIL account meets your need then below is an example of the email setting configured using GMAIL. Replace the credential information with your credential.

```
<add key="EMAIL_USE_AUTHENTICATION" value="TRUE"/>
<add key="EMAIL_USE_SSL" value="TRUE"/>
<add key="EMAIL_SUBJECT" value="Subject Line"/>
<add key="EMAIL_FROM" value="GmailID@gmail.com"/>
<add key="EMAIL_PASSWORD" value="GmailAccountPassword"/>
<add key="EMAIL_TO" value="Administrators@YourOrganization.gov"/>
<add key="SMTP_PORT" value="587"/>
<add key="SMTP_HOST" value="smtp.gmail.com"/>
```

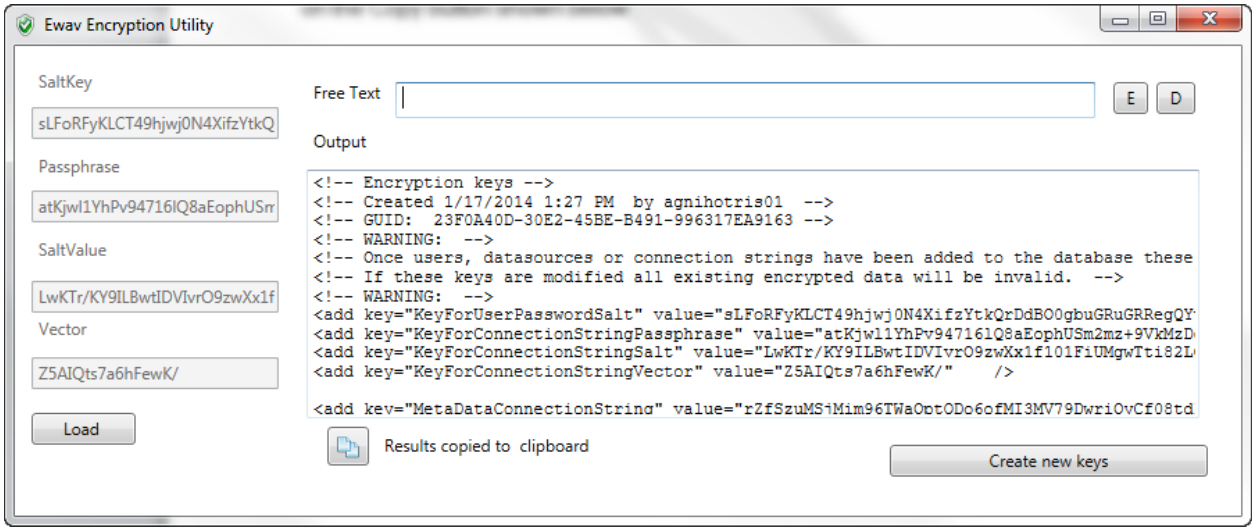
9. Update the password policy section to reflect the password policy for your organization. This policy will be used by users created in the EWAV system.

```
<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 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.

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



SaltKey: sLFoRFyKLCT49hjwj0N4XifzYtkQ

Passphrase: atKjwl1YhPv94716lQ8aEophUSm

SaltValue: LwKTr/KY9ILBwtIDVIvrO9zwXx1f

Vector: Z5AIQts7a6hFewK/

Free Text:

Output

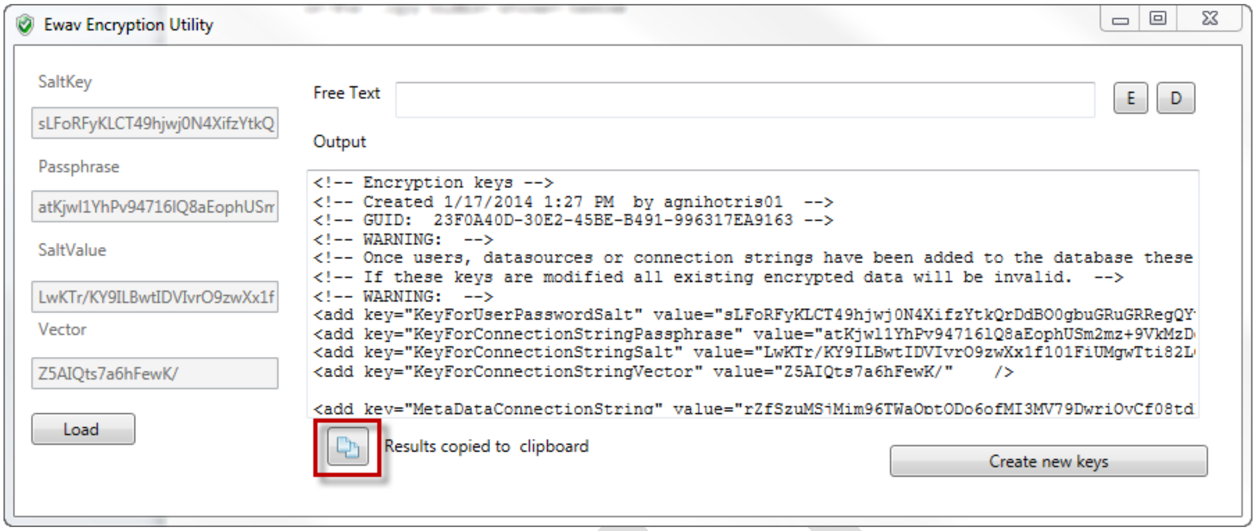
```
<!-- Encryption keys -->
<!-- Created 1/17/2014 1:27 PM  by agnihotris01  -->
<!-- GUID:  23F0A40D-30E2-45BE-B491-996317EA9163 -->
<!-- WARNING:  -->
<!-- Once users, datasources or connection strings have been added to the database these
<!-- If these keys are modified all existing encrypted data will be invalid.  -->
<!-- WARNING:  -->
<add key="KeyForUserPasswordSalt" value="sLFoRFyKLCT49hjwj0N4XifzYtkQrDdBO0gbuGRuGRRegQY
<add key="KeyForConnectionStringPassphrase" value="atKjwl1YhPv94716lQ8aEophUSm2mz+9VkMzD
<add key="KeyForConnectionStringSalt" value="LwKTr/KY9ILBwtIDVIvrO9zwXx1f101FiUMgwTti82L
<add key="KeyForConnectionStringVector" value="Z5AIQts7a6hFewK/"    />

<add key="MetaDataConnectionString" value="rZfSzuMSjMim96TWaQptODo6ofMI3MV79DwriOvCf08td
```

Results copied to clipboard

Figure 26: Generating the application encryption keys using EWAV Encryption utility for forms authentication application

11. 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.



SaltKey: sLFoRFyKLCT49hjwj0N4XifzYtkQ

Passphrase: atKjwl1YhPv94716lQ8aEophUSm

SaltValue: LwKTr/KY9ILBwtIDVIvrO9zwXx1f

Vector: Z5AIQts7a6hFewK/

```
<!-- Encryption keys -->
<!-- Created 1/17/2014 1:27 PM  by agnihotris01  -->
<!-- GUID:  23F0A40D-30E2-45BE-B491-996317EA9163 -->
<!-- WARNING:  -->
<!-- Once users, datasources or connection strings have been added to the database these
<!-- If these keys are modified all existing encrypted data will be invalid.  -->
<!-- WARNING:  -->
<add key="KeyForUserPasswordSalt" value="sLFoRFyKLCT49hjwj0N4XifzYtkQrDdBO0gbuGRuGRRegQY
<add key="KeyForConnectionStringPassphrase" value="atKjwl1YhPv94716lQ8aEophUSm2mz+9VkMzD
<add key="KeyForConnectionStringSalt" value="LwKTr/KY9ILBwtIDVIvrO9zwXx1f101FiUMgwTti82L
<add key="KeyForConnectionStringVector" value="Z5AIQts7a6hFewK/"    />

<add key="MetaDataConnectionString" value="rZfSzuMSjMim96TWaOptODo6ofMI3MV79DwriOvCf08td
```

Results copied to clipboard

Figure 27: 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="sLFoRFyKLCT49hjwj0N4XifzYtkQrDd
BO0gbuGRuGRRegQYv4EydWV5Q5yGV0ECoTYoq5a0UbbRIh81xQbDuQWjYf6Vk4gLg/1dQCuutN9i
VtDZQbe8dlJL0aAhLbFantM013g=="    />
    <add key="KeyForConnectionStringPassphrase" value="atKjwl1YhPv94716lQ8aE
ophUSm2mz+9VkMzDgzRgscoPsRYJ2/vRs7eJTf43X6r/PiBQS2Pb99lzoA0DAVxfmwToq1QXDgov
FCZP+axtINlw9vbidyz9cG0Ty3LNjxCYuMoIw=="    />
    <add key="KeyForConnectionStringSalt" value="LwKTr/KY9ILBwtIDVIvrO9zwXx1
f101FiUMgwTti82LCY0Erdrrdu45vaVQntXe6kD0JjK1RXkLL8HdmuzPSEYsvtIKDJQ8SGdAtzHW
pYrpkdXmcd5bi/pLO4UdL1H3f2ZfpZg=="    />
    <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.

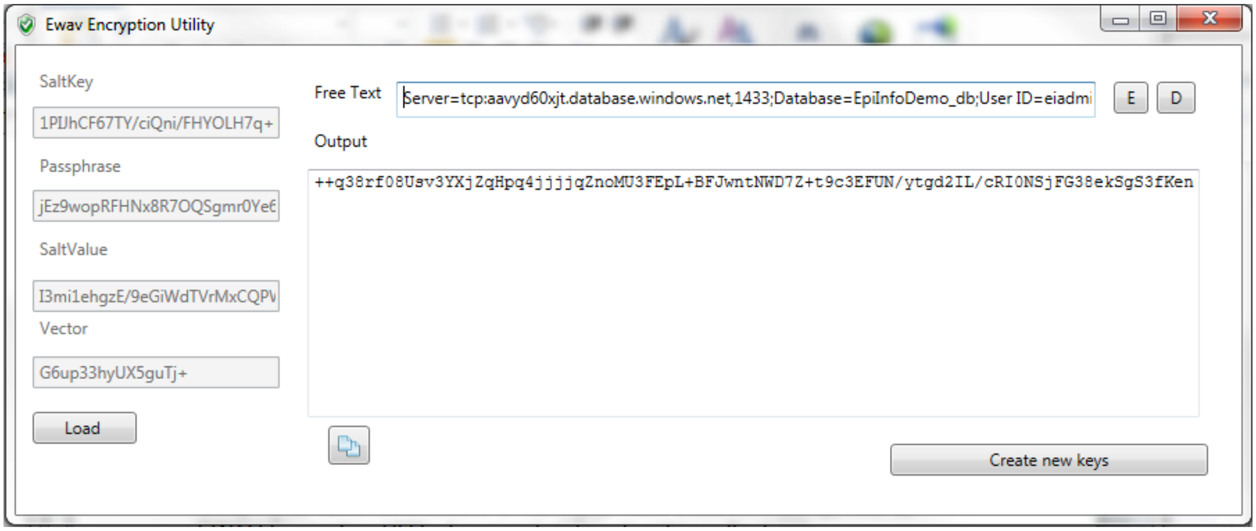
12. Create a MetaDataConnectionString for SQL Database that you configured in Microsoft Azure Portal by replacing the section provided below or optionally you can use the connection string as provided in Portal.

    Server= DATABASE_SERVER_NAME;Database= DATABASE_NAME;User ID= SQL_DATABASE_ACCOUNT;Password= PASSWORD_FOR_ACCOUNT;Trusted_Connection=False;Encrypt=True; Connection Timeout=30;

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

    Server=tcp:aavyd60xjt.database.windows.net,1433;Database=EpiInfoDemo_db;User ID=eiadmin@aavyd60xjt;Password=J*p2leO4>F;Trusted_Connection=False;Encrypt=True;Connection Timeout=30;

13. 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.



SaltKey: 1PIJhCF67TY/ciQni/FHYOLH7q+

Passphrase: jEz9wopRFHNx8R7OQSgmr0Ye

SaltValue: I3mi1ehgzE/9eGiWdTVrMxCQP

Vector: G6up33hyUX5guTj+

Free Text: Server=tcp:aavyd60xjt.database.windows.net,1433;Database=EpiInfoDemo_db;User ID=eiadmi

Output:

```
++q38rf08Usv3YXjZqHpq4jjjjqZnoMU3FEpL+BFJwntNWD7Z+t9c3EFUN/ytgd2IL/cRI0NSjFG38ekSgS3fKen
```

Figure 28: Encrypting connection string using EWAV Encryption utility for forms authentication application

14. 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)" />
```

3.3.2.3 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