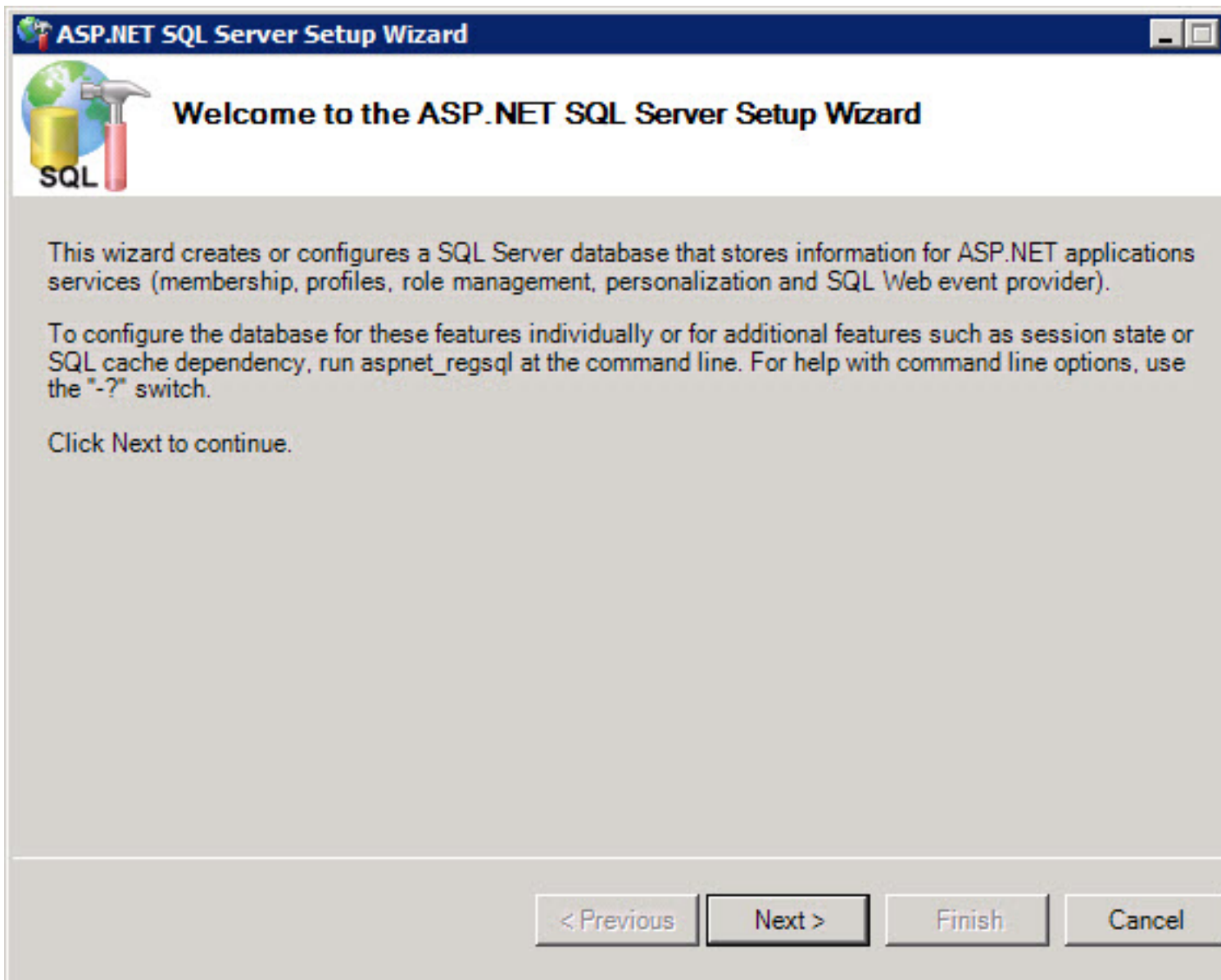
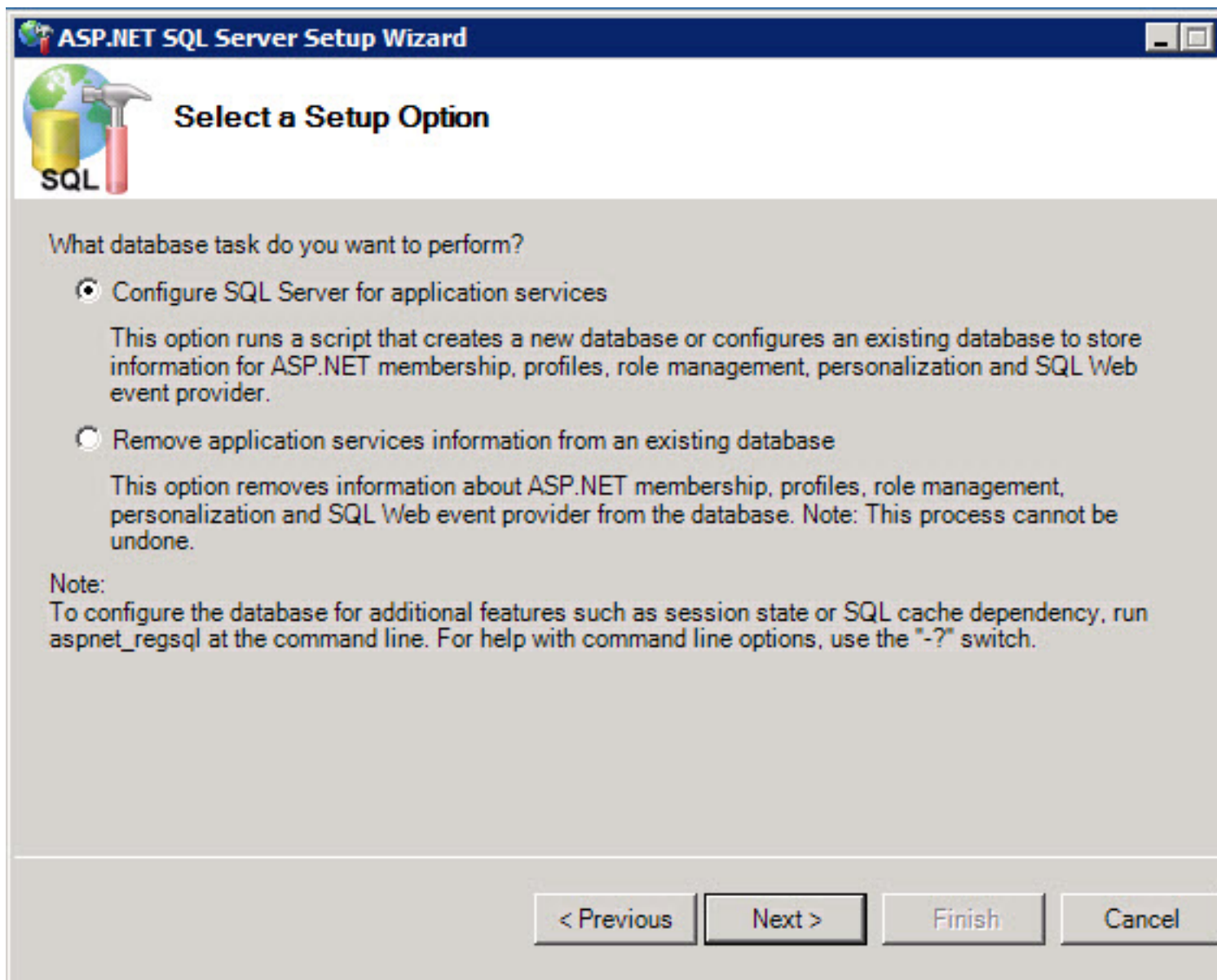


از دغدغه‌های همیشگی در راه اندازی پرتال‌های مبتنی بر شیرپوینت سیستم احراز هویت آن است. این سیستم بصورت پیش فرض بر مبنای Windows Authentication است و ناگفته پیداست این نوع احراز هویت تنها در شبکه‌های محلی کاربرد دارد آنهم در صورتی که همه کاربران و سطوح دسترسی، بدرستی در [AD](#) تعریف شده باشد و نیز یک سری مشکلات دیگر که بیشتر به توسعه شیرپوینت در شرکت و انتقال آن و انطباق آن با محیط پروژه برمیگردد. به عبارت دیگر شما به عنوان یک توسعه دهنده ویا نصاب(!) شیرپوینت خیلی نباید درگیر سیستم احراز هویت پیش فرض مشتری بشوید. برای اینکار بهترین گزینه استفاده از احراز هویت بر مبنای فرم (Form Based Authentication - FBA) است که برای ما برنامه نویسان Asp.net بسیار آشناست؛ سیستم احراز هویتی خوش دست و فراگیر با قاعده‌های مشخص. متأسفانه اکثر راهکارهایی که در وب پیرامون راه اندازی FBA در شیرپوینت معرفی شده‌اند دارای اشکالات ریز و درشتی هستند و یا اینکه یک یا چند گام از فرایند را توضیح نداده‌اند و معمولاً در پایان یکجای کار لنگ میزند و FBA بخوبی عملیاتی نمیشود. بر همین اساس بر آن شدم تا با بررسی چندتا از این مقالات موجود و نیز تجربه عملی خودم این راهکارها را ترکیب کنم که نتیجه اش فرایند شش مرحله ای زیر شده است. برای راه اندازی FBA بر روی SharePoint 2010 باید مراحل زیر را به ترتیب انجام داد.

1. ساخت بانک اطلاعاتی FBA بر روی MSSQL

بانک اطلاعاتی FBA ساختار مشخصی از جداول و SPها دارد که تا حد امکان بهتر است در ساختار پیش فرض آن تغییری ایجاد نکنیم. برای ایجاد این بانک کافی است به محل نصب دات نت فریم 2.0 که بصورت پیش فرض در مسیر "C:\Windows\Microsoft.NET\Framework64\v2.0.50727" قرار دارد بروید و روی فایل "aspnet_regsql.exe" کلیک کنید و مراحل نصب را تا آخر پیش بروید.





The image shows a screenshot of the 'ASP.NET SQL Server Setup Wizard' window. The title bar is dark blue with the text 'ASP.NET SQL Server Setup Wizard' and standard window control buttons. Below the title bar is a header area with a logo on the left (a globe with a hammer and the text 'SQL') and the title 'Select a Setup Option' in bold. The main content area has a light gray background and contains the question 'What database task do you want to perform?'. There are two radio button options: 'Configure SQL Server for application services' (which is selected) and 'Remove application services information from an existing database'. Each option has a descriptive paragraph below it. At the bottom of the window is a gray bar containing four buttons: '< Previous', 'Next >', 'Finish', and 'Cancel'.

ASP.NET SQL Server Setup Wizard

Select a Setup Option

What database task do you want to perform?

☒ **Configure SQL Server for application services**

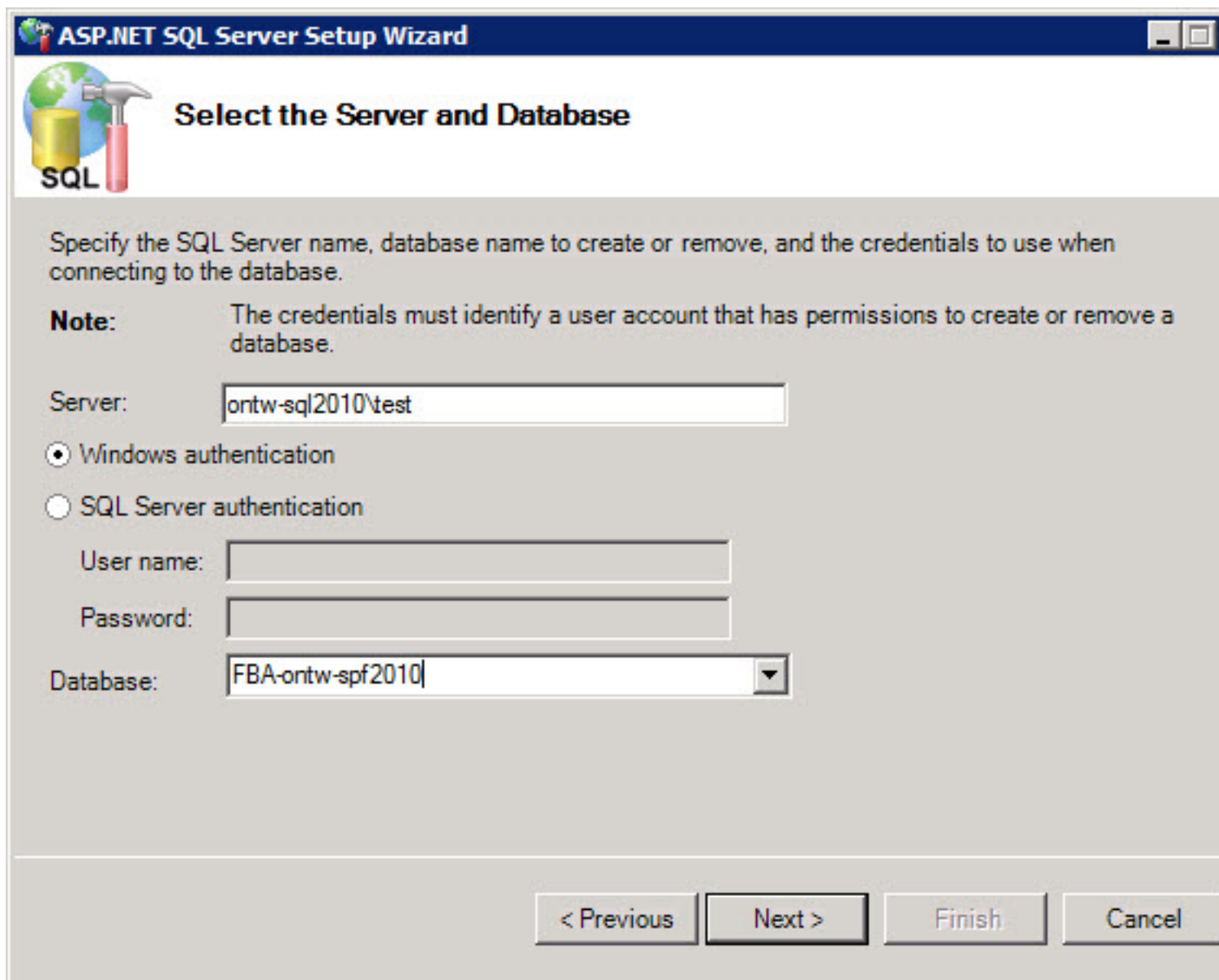
This option runs a script that creates a new database or configures an existing database to store information for ASP.NET membership, profiles, role management, personalization and SQL Web event provider.

☐ **Remove application services information from an existing database**

This option removes information about ASP.NET membership, profiles, role management, personalization and SQL Web event provider from the database. Note: This process cannot be undone.

Note:
To configure the database for additional features such as session state or SQL cache dependency, run aspnet_regsql at the command line. For help with command line options, use the "-?" switch.

< Previous Next > Finish Cancel



The image shows a screenshot of the 'ASP.NET SQL Server Setup Wizard' window. The title bar is dark blue with the text 'ASP.NET SQL Server Setup Wizard' and standard window control buttons. The main area has a light gray background. On the left, there is a logo featuring a globe with a hammer and the text 'SQL'. To the right of the logo, the heading 'Select the Server and Database' is displayed in bold. Below the heading, a paragraph of instructions reads: 'Specify the SQL Server name, database name to create or remove, and the credentials to use when connecting to the database.' A 'Note' section follows, stating: 'The credentials must identify a user account that has permissions to create or remove a database.' The form contains several input fields: 'Server:' with the text 'ontw-sql2010\test', 'User name:' and 'Password:' (both empty), and 'Database:' with a dropdown menu showing 'FBA-ontw-spf2010'. Two radio buttons are present: 'Windows authentication' (selected) and 'SQL Server authentication'. At the bottom right, there are four buttons: '< Previous', 'Next >', 'Finish', and 'Cancel'.

ASP.NET SQL Server Setup Wizard

Select the Server and Database

Specify the SQL Server name, database name to create or remove, and the credentials to use when connecting to the database.

Note: The credentials must identify a user account that has permissions to create or remove a database.

Server:

☒ Windows authentication

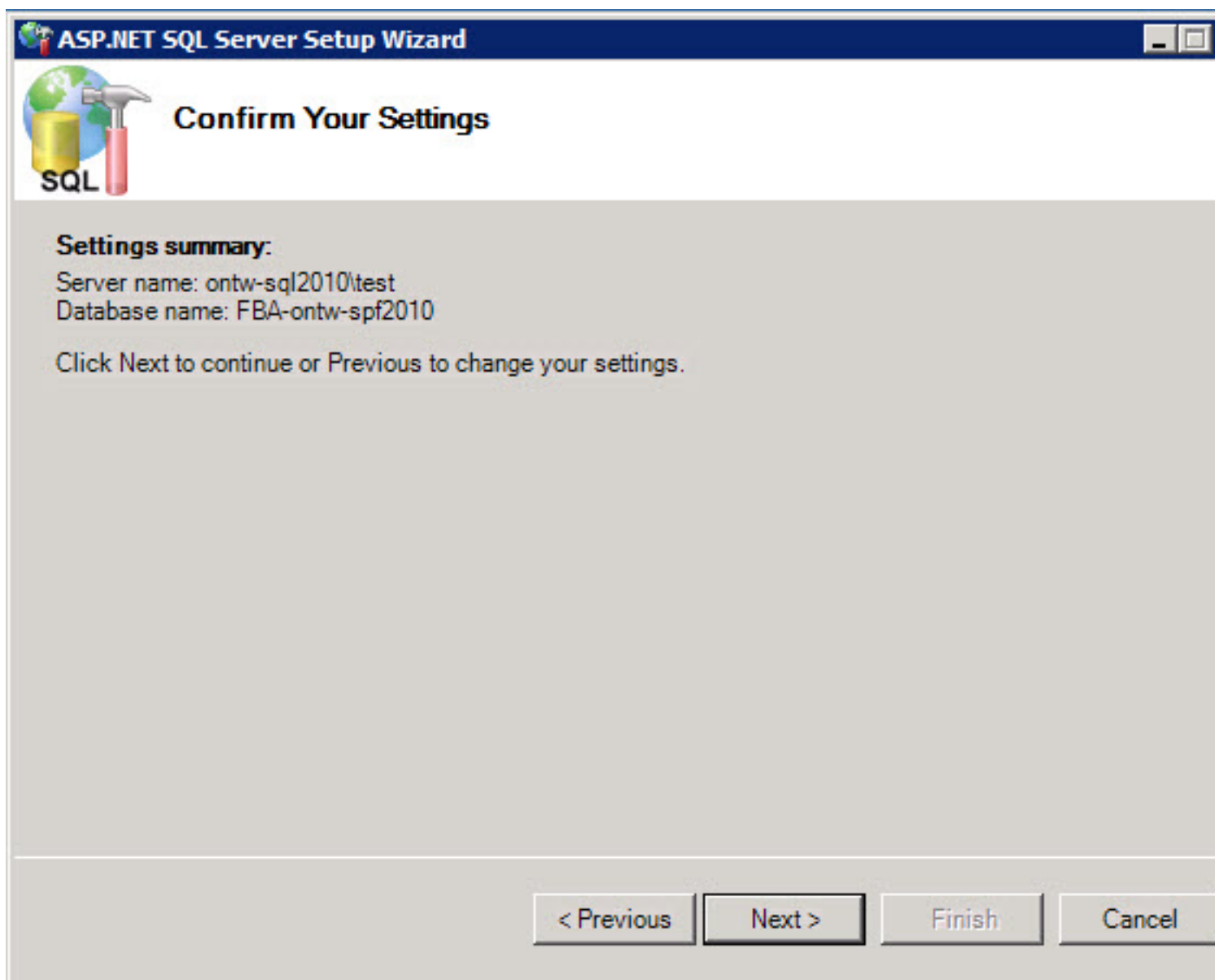
☐ SQL Server authentication

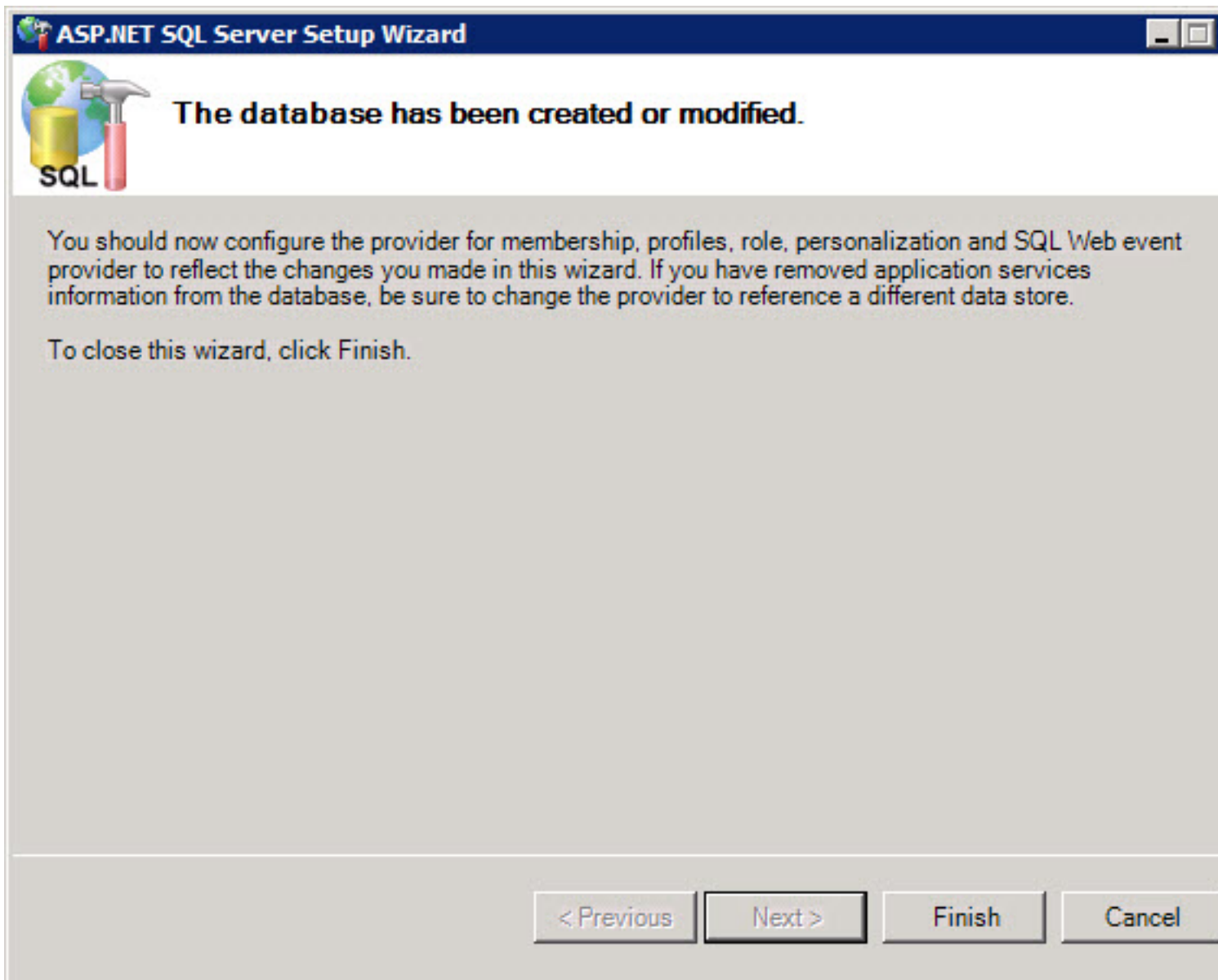
User name:

Password:

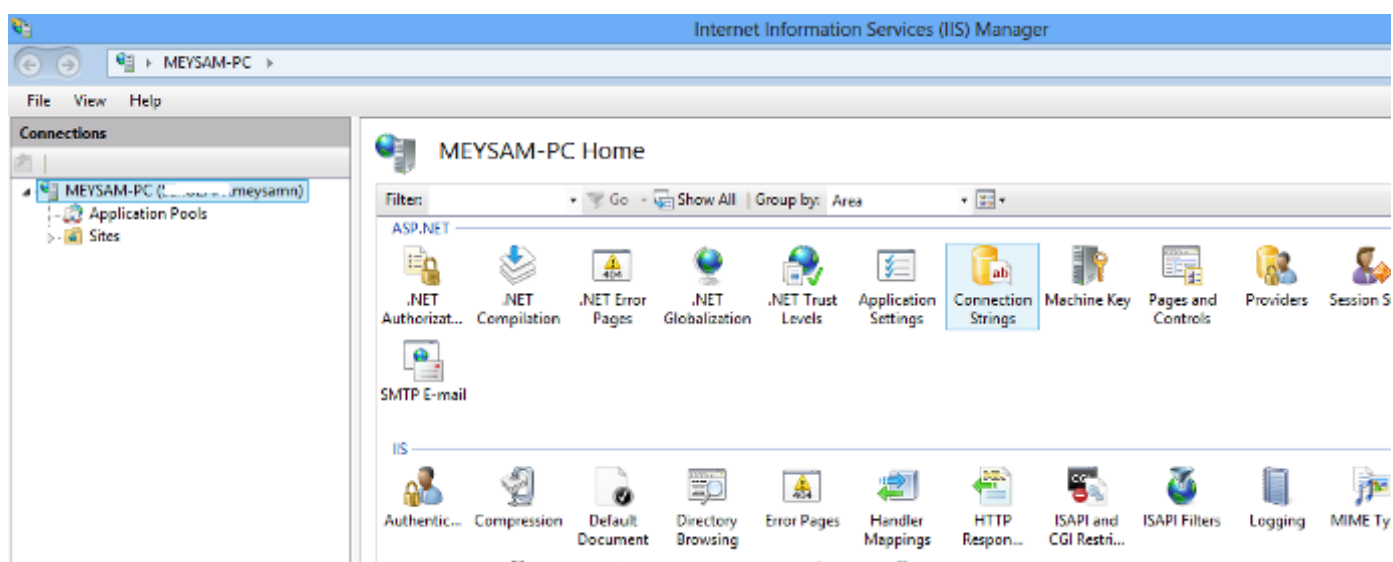
Database:

< Previous Next > Finish Cancel





در ادامه MSSQL را باز کنید و مطمئن شوید که بانک FBA به درستی ایجاد شده باشد.



Add Connection String

Name:

☒ SQL Server

Server:

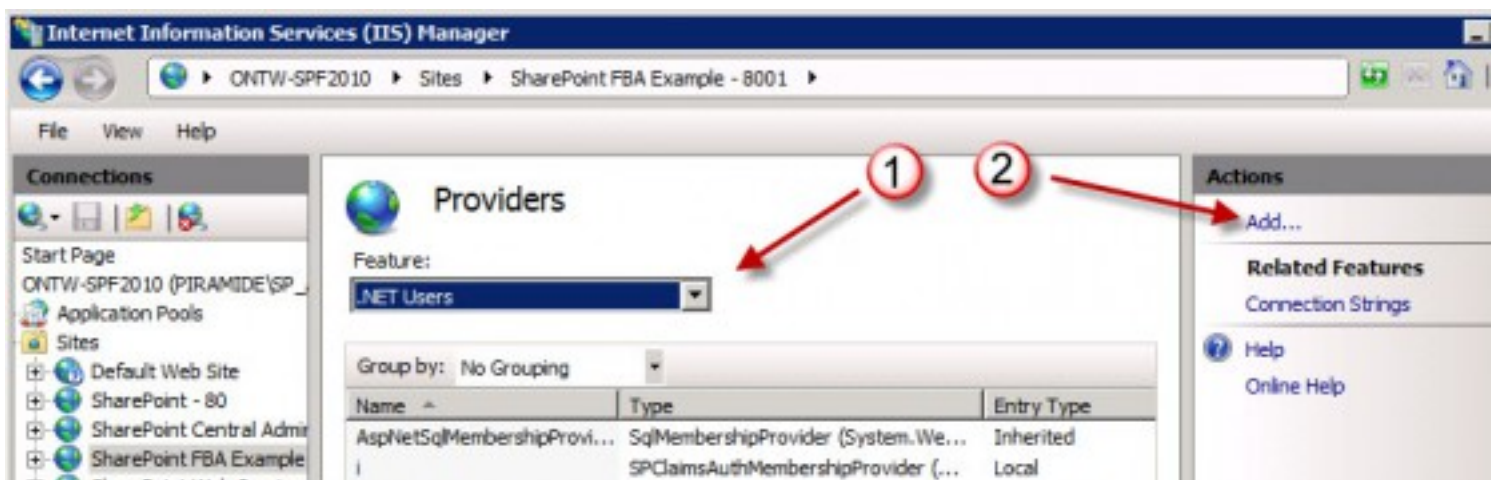
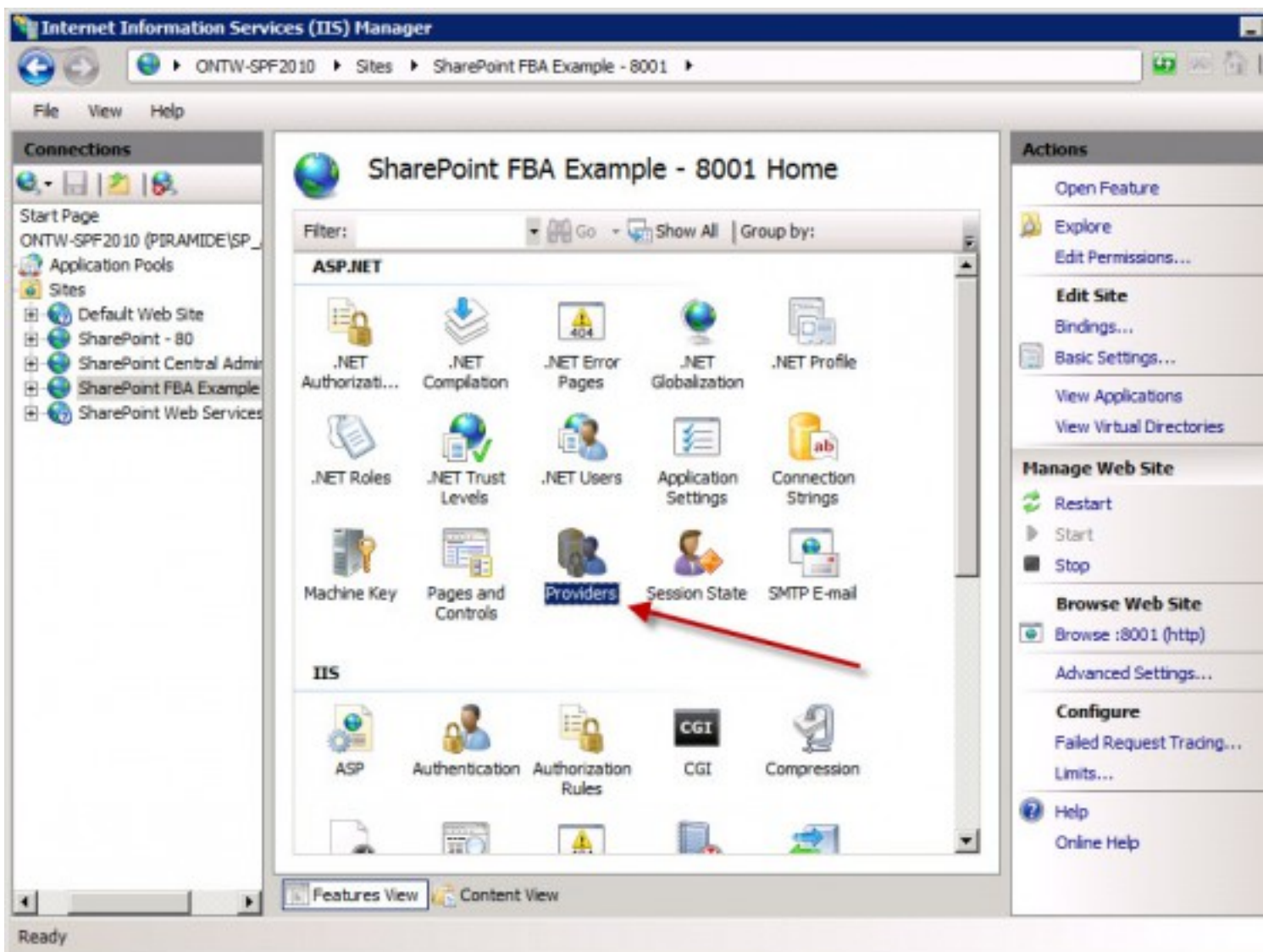
Database:

Credentials

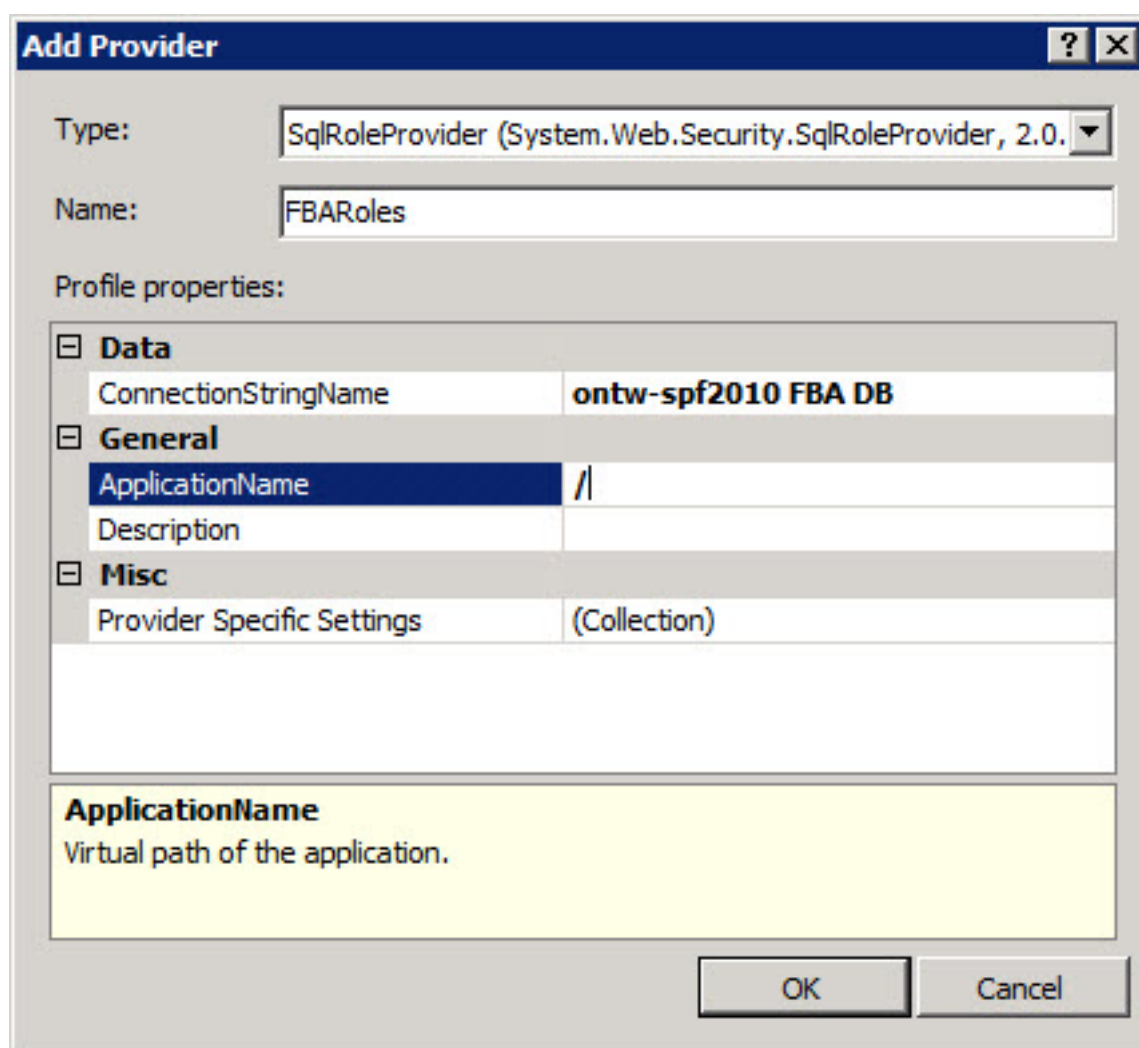
☐ Use Windows Integrated Security

☒ Specify credentials

☐ Custom



موقع اضافه کردن Provider ها باید توجه داشت که Application Name برابر "/" قرار داده شود.

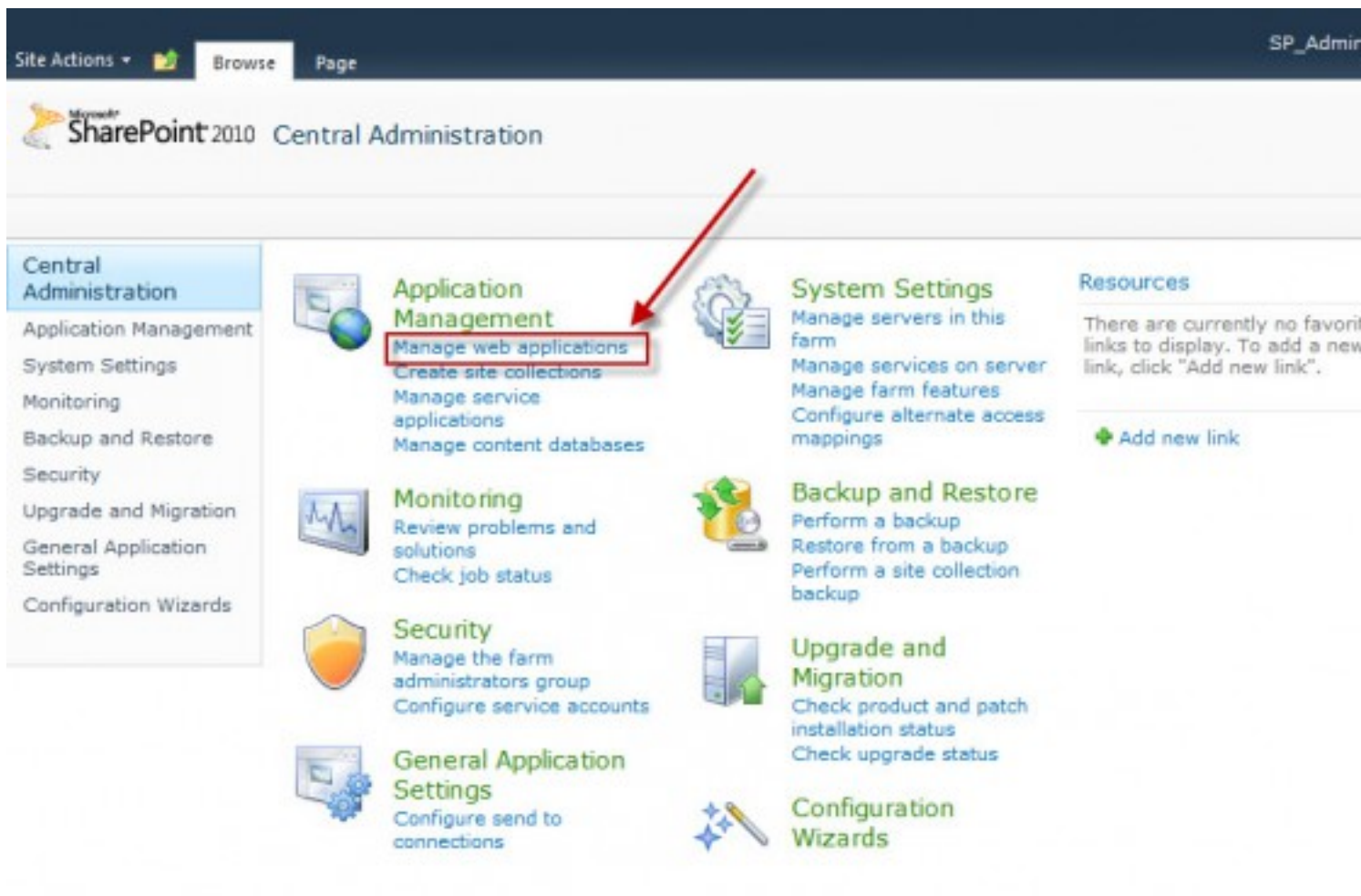


The image shows a Windows-style dialog box titled "Add Provider". It has a standard title bar with a question mark and a close button. The dialog is divided into several sections. At the top, there are two labels: "Type:" and "Name:". The "Type:" label is followed by a dropdown menu showing "SqlRoleProvider (System.Web.Security.SqlRoleProvider, 2.0)". The "Name:" label is followed by a text box containing "FBARoles". Below these is a section labeled "Profile properties:". This section contains three expandable/collapsible categories: "Data", "General", and "Misc". The "Data" category is expanded, showing a table with two columns: "ConnectionStringName" and "ontw-spf2010 FBA DB". The "General" category is also expanded, showing a table with two columns: "ApplicationName" and "/". The "Misc" category is expanded, showing a table with two columns: "Provider Specific Settings" and "(Collection)". Below these categories is a yellow-highlighted section titled "ApplicationName" with the text "Virtual path of the application." At the bottom right of the dialog are two buttons: "OK" and "Cancel".

Profile properties:	
Data	
ConnectionStringName	ontw-spf2010 FBA DB
General	
ApplicationName	/
Description	
Misc	
Provider Specific Settings	(Collection)

ApplicationName
Virtual path of the application.

3. به بخش مدیریت شیرپوینت رفته و یک WebApplication جدید ایجاد کنید.



توجه داشت که در بخش Authentication باید گزینه Claims Authentication را انتخاب کنید.

Authentication

Select the authentication for this web application.

[Learn about authentication.](#)

- ☒ Claims Based Authentication
- ☐ Classic Mode Authentication

و نیز برای تنظیمات مربوط به FBA باید نام Provider هایی را که در مرحله قبل ایجاد کرده بودید را در این بخش قرار دهید. اگر پرتال شما بازدید کننده‌های ناشناس (بازدید کنندگانی که عضو نیستند و در سیستم FBA نام کاربری ندارند) را نیز پشتیبانی میکند باید گزینه اول (Allow anonymous) را Yes کنید. اگر تمایلی ندارید که دیگر احراز هویت مبتنی بر ویندوز فعال باشد تیک Enable Windows Authentication را بردارید.

Create New Web Application

Security Configuration

If you choose to use Secure Sockets Layer (SSL), you must add the certificate on each server using the IIS administration tools. Until this is done, the web application will be inaccessible from this IIS web site.

Allow Anonymous

☐ Yes

☒ No

Use Secure Sockets Layer (SSL)

☐ Yes

☒ No

Claims Authentication Types

Choose the type of authentication you want to use for this zone.

Negotiate (Kerberos) is the recommended security configuration to use with Windows authentication. If this option is selected and Kerberos is not configured, NTLM will be used. For Kerberos, the application pool account needs to be Network Service or an account that has been configured by the domain administrator. NTLM authentication will work with any application pool account and with the default domain configuration.

Basic authentication method passes users' credentials over a

☒ Enable Windows Authentication

☒ Integrated Windows authentication

NTLM

☐ Basic authentication (credentials are sent in clear text)

☒ Enable Forms Based Authentication (FBA)

ASP.NET Membership provider name

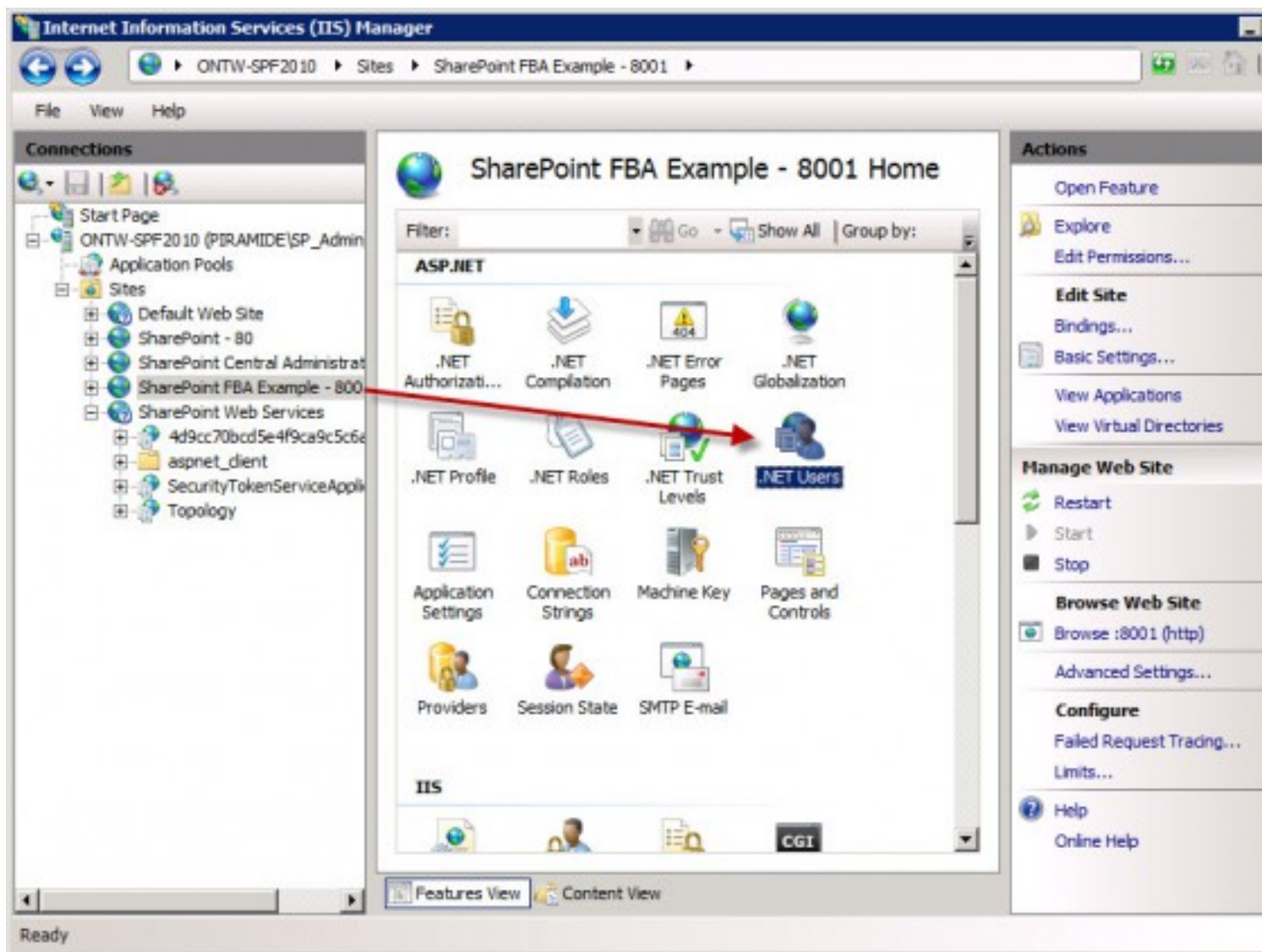
FBAMembershipProvider

ASP.NET Role manager name

FBARoleProvider

☐ Trusted Identity provider

4. حال دوباره سراغ IIS میرویم و روی وب جدیدی که ایجاد کرده ایم کلیک میکنیم و سپس روی آیکون Net Users کلیک میکنیم






اگر با پیغامی مبنی بر تعیین Provider پیش فرض مواجه شدیم مقادیر پیش فرض Provider ها را برابر با نام Provider هایی که خودمان تعریف کرده ایم قرار می‌دهیم.





.NET Users

This page lets you view and manage the list of user identities that are defined in the application. The list of users can be used to perform authentication, authorization, and other security-related operations.

Filter:  Go  Show All | Group by: No Grouping 


Name ▲	E-mail Address	Created	Last Login
--------	----------------	---------	------------

Edit .NET Users Settings  

Default Provider:

در ادامه چند کاربر و رول هم به عنوان کاربران اولیه و مدیران پرتال [ایجاد میکنیم](#).

Add .NET User ?

 **.NET User Account Details**

User Name:

E-mail:

Password:

Confirm Password:

Question:

▼

(optional)

Answer:

(optional)

OK

Cancel

5. حال دوباره به بخش مدیریت برمیگردیم و یک Site Collection جدید روی Web Application مورد نظر ایجاد میکنیم.

Site Actions ▾
SP_Admin ▾

Central Administration ▸ Create Site Collection

Use this page to create a new top-level Web site.

?

Central Administration
 Application Management
 System Settings
 Monitoring
 Backup and Restore
 Security
 Upgrade and Migration
 General Application Settings
 Configuration Wizards

Web Application Select a web application. To create a new web application go to New Web Application page.	Web Application: http://ontw-spf2010:8001/ ▾
Title and Description Type a title and description for your new site. The title will be displayed on each page in the site.	Title: <input style="width: 80%;" type="text" value="FBA Demo site"/> Description: <div style="border: 1px solid #ccc; padding: 2px; min-height: 40px;">This site demonstrates Forms Based Authentication.</div>
Web Site Address Specify the URL name and URL path to create a new site, or choose to create a site at a specific path. To add a new URL Path go to the Define Managed Paths page.	URL: http://ontw-spf2010:8001/ ▾
Template Selection A site template determines what lists and features will be available on your new site. Select a site template based on the descriptions of each template and how you intend to use the new site. Many aspects of a site can be customized after creation. However, the site template cannot be changed once the site is created.	Select a template: <div style="border: 1px solid #ccc; padding: 5px; margin-bottom: 5px;"> Collaboration Meetings Custom </div> <div style="border: 1px solid #ccc; padding: 5px;"> <div style="background-color: #0070c0; color: white; padding: 2px 5px; margin-bottom: 5px;">Team Site</div> <div style="padding: 2px 5px;">Blank Site</div> <div style="padding: 2px 5px;">Document Workspace</div> <div style="padding: 2px 5px;">Blog</div> <div style="padding: 2px 5px;">Group Work Site</div> </div> <div style="font-size: x-small; margin-top: 10px;"> A site for teams to quickly organize, author, and share information. It provides a document library, and lists for managing announcements, calendar items, tasks, and discussions. </div>
Primary Site Collection Administrator Specify the administrator for this site collection. Only one user login can be provided; security groups are not supported.	User name: <input style="width: 80%;" type="text" value="FBAtest;"/>
Secondary Site Collection Administrator Optionally specify a secondary site collection administrator.	User name: <input style="width: 80%;" type="text"/>

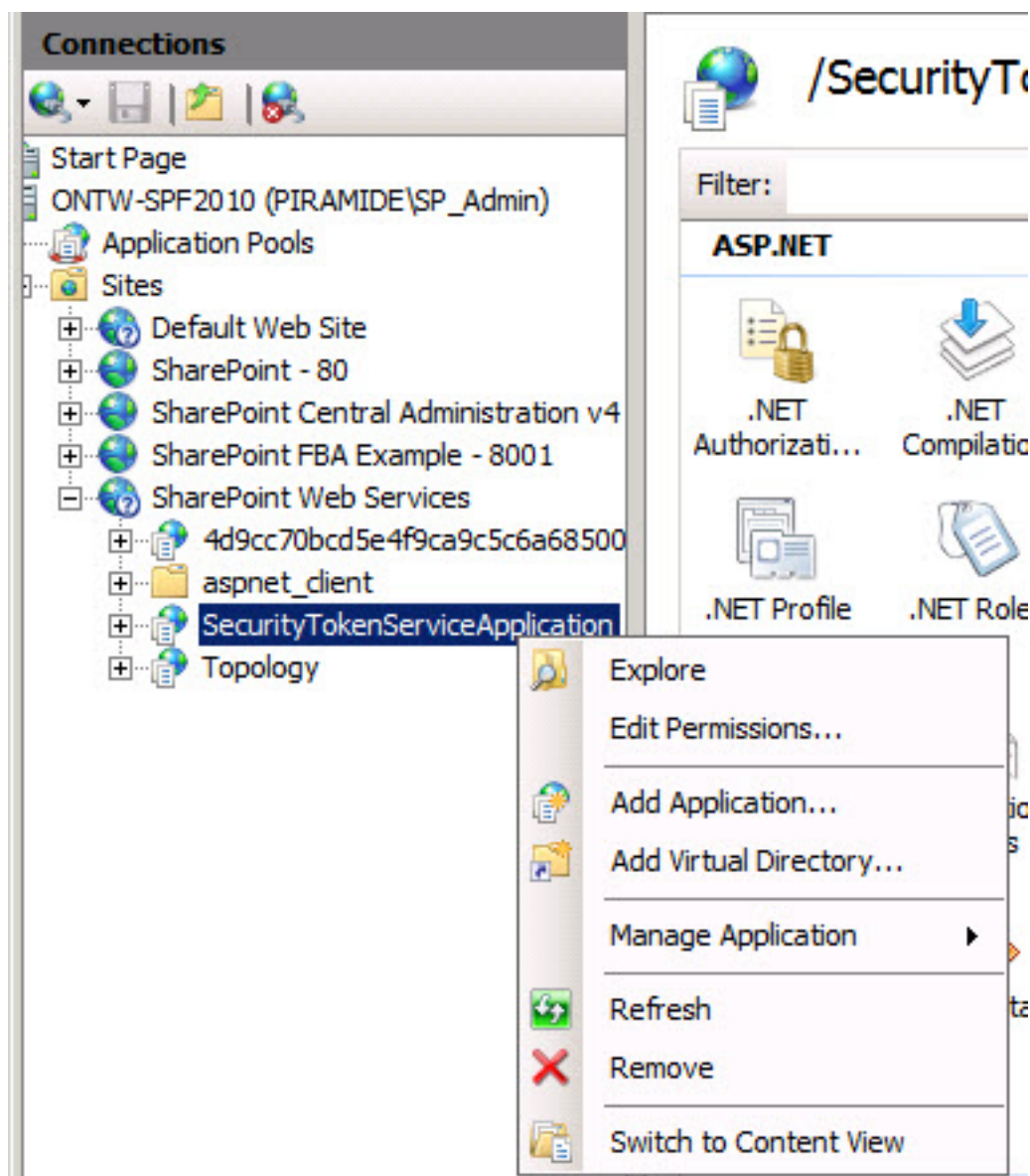
در اینجا بهتر است مدیر اول را از کاربران ویندوزی انتخاب کرد و مدیر دوم را از بخش کاربران FBA

نکته بی ربط: اگر تمپلتی از قبل برای سایتتان دارید در بخش انتخاب نوع سایت بعد از انتخاب زبان باید به تب سوم (Custom) بروید و تنها گزینه موجود را انتخاب کنید. با این کار در مراحل بعد تمپلت مورد نظرتان را در سایت آپلود میکنید و آن را بر سایت جاری اعمال میکنید.

در این مرحله بعد از ایجاد موفقیت آمیز Site collection دوباره به IIS سری بزنید و پس از انتخاب Web Application مورد نظر بروی Authentication کلیک کنید و مطمئن شوید که Form Authentication مقدارش Enable میباشد. در این بخش اگر هر دو حالت Form Base Authentication و Windows Authentication فعال باشد IIS در گوشه سمت راست به شما خطایی نمایش میدهد مبنی بر اینکه شما نباید هر دو حالت را همزمان فعال کنید. البته خیلی این تذکر را جدی نگیرید و بکارتان ادامه دهید و در نهایت بعد از اینکه مراحل را کامل انجام دادید و از اجرای کامل FBA اطمینان حاصل نمودید، میتوانید برگردید و حالت Windows Authentication را غیر فعال کنید.

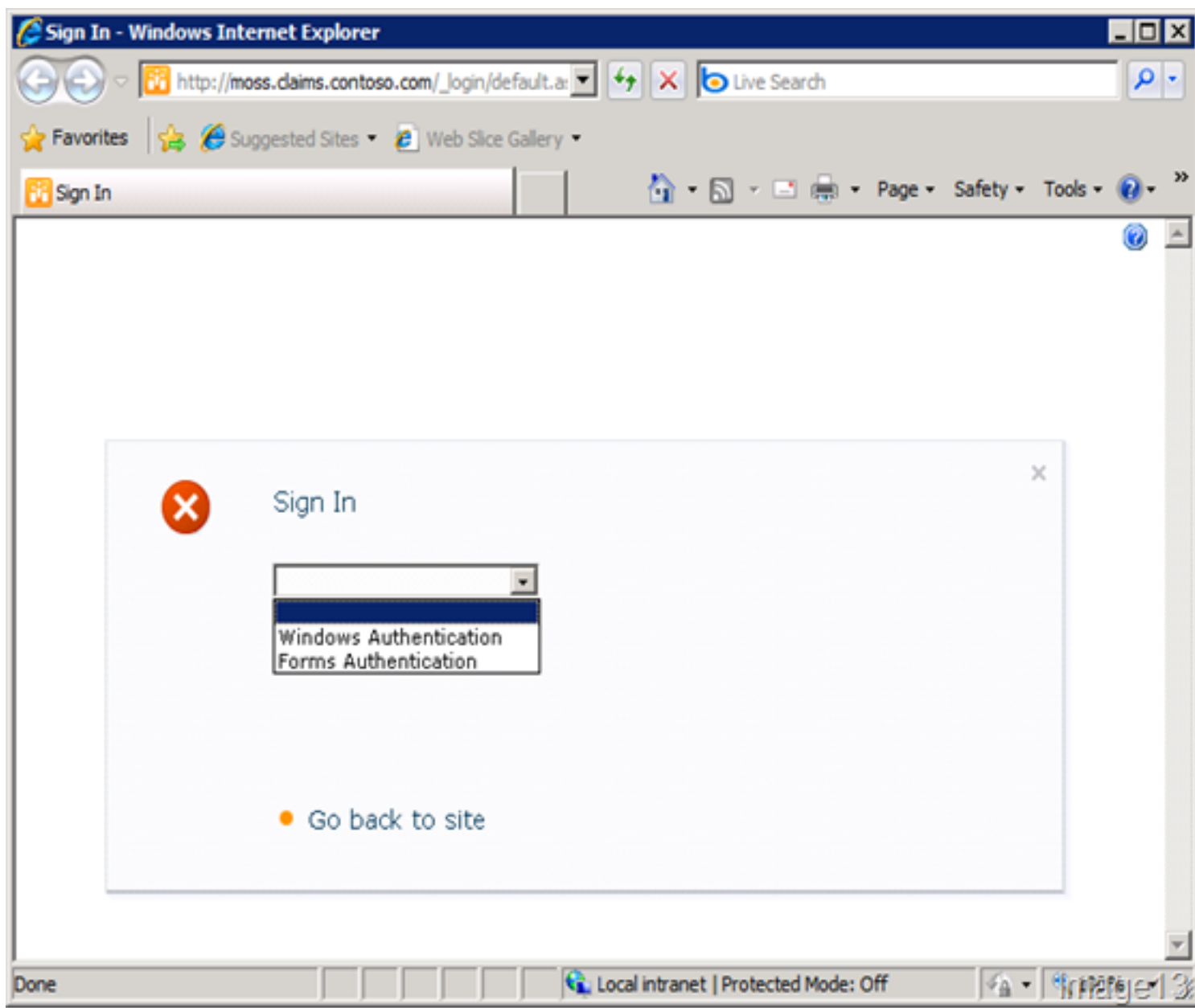
6. تنظیمات STS:


علاوه بر تنظیمات مربوط به بخش Web Application باید تنظیمات FBA را روی Application سرویسها نیز انجام داد تا سرویسهای WCF نیز پشتیبانی از FBA را بپذیرند. برای تنظیمات این بخش روی Security Token Service Application که زیر مجموعه SharePoint Web Services قرار دارد کلیک کنید.



در ادامه تنها کافی است Connection string را جهت اتصال به بانک که در ابتدا ساختیم ایجاد کرده و Provider ها را نیز مطابق قبل اضافه کنیم. فقط توجه شود Connection string و Provider ها همانم قبلی ها نباشند ولی Application Name همچنان برابر با " مقدار دهی شود.

هیچ تغییر دیگری در این Application ایجاد نشود. مثلاً Authentication به هیچ وجه تغییر نکند و در حالت ویندوزی باقی بماند. کار تقریباً به پایان رسیده است، میتوانید در پرتال لاگین کنید! آنچنانکه که در تصویر می بینید هر دو حالت ویندوزی و FBA برای احراز هویت فعال می باشد.





Sign In

Warning: this page is not encrypted for secure communication. User names, passwords, and any other information will be sent in clear text. For more information, contact your administrator.

User name: FBAtest

Password:

☐ Sign me in automatically

پی نوشت:

1. همانطور که احتمالا متوجه شده اید این آموزش با راهکارهای حاضر یک سری تفاوتها داشت که عمدهترین آن عدم تغییر در بخش احراز هویت مدیریت شیرپوینت بود. علت این امر نیز به این خاطر است که اساسا هر کاربری به این بخش دسترسی ندارد و تنها مدیر سیستم است که باید به این بخش دسترسی داشته باشد، بر همین اساس ترجیح میدهم احراز هویت آن به همان شکل اولیه (Windows Authentication) باقی بماند.

2. در این نوشته من از شرح تنظیمات و نکات ریز و بدیهی خوداری کردم با این پیش فرض که خواننده مطلب، بر اصول پایه شیرپوینت و Asp.net آگاهی دارد. در غیر این صورت بهتر است از لینک هایی مرجع زیر کمک بگیرید.

مراجع: <http://technet.microsoft.com/en-us/library/ee806890.aspx>

<http://blog.morg.nl/2011/08/step-by-step-forms-based-authentication-fba-on-sharepoint-2010>

<http://www.codeproject.com/Articles/352841/How-to-Configure-Form-Based-Authentication-FB>

<http://msdn.microsoft.com/en-us/library/bb975136.aspx>

[http://msdn.microsoft.com/en-us/library/gg252020\(v=office.14\).aspx](http://msdn.microsoft.com/en-us/library/gg252020(v=office.14).aspx)