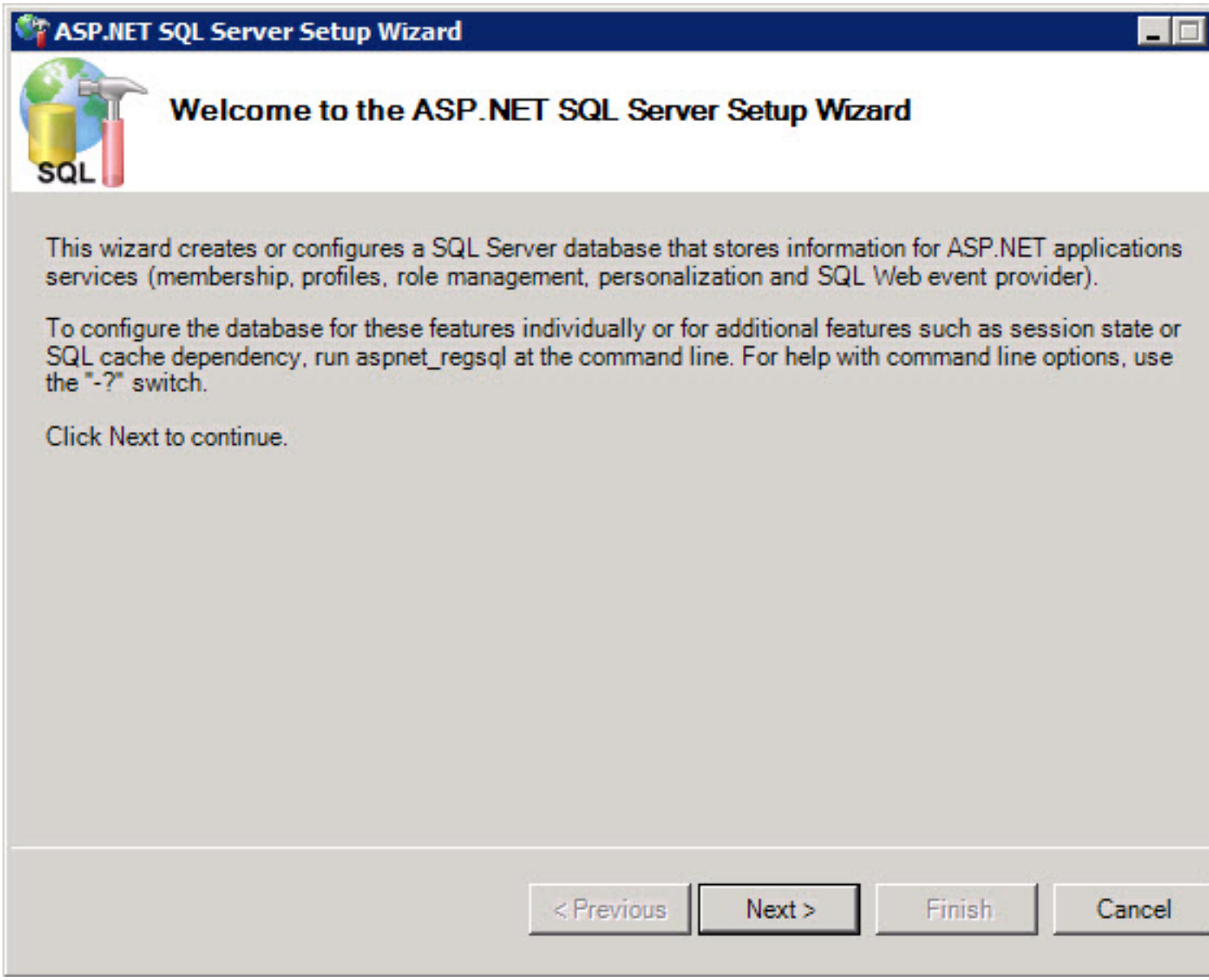
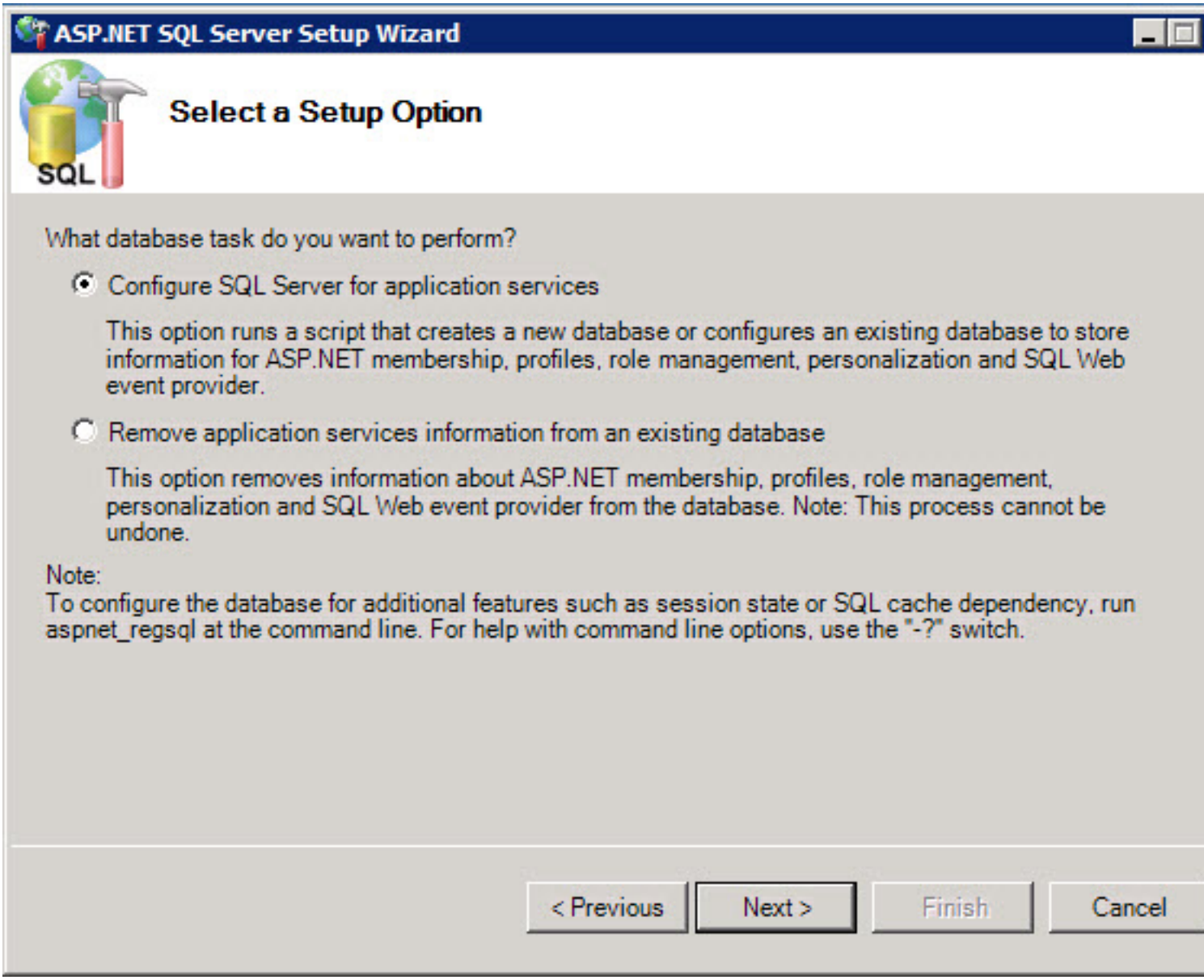
عنوان: **احراز هویت مبتنی بر فرم در شیرپوینت**
نویسنده: میثم نوایی
تاریخ: ۱۳۹۲/۰۶/۱۹ ۱۶:۵۵
آدرس: www.dotnettips.info
برچسب‌ها: SharePoint, FBA

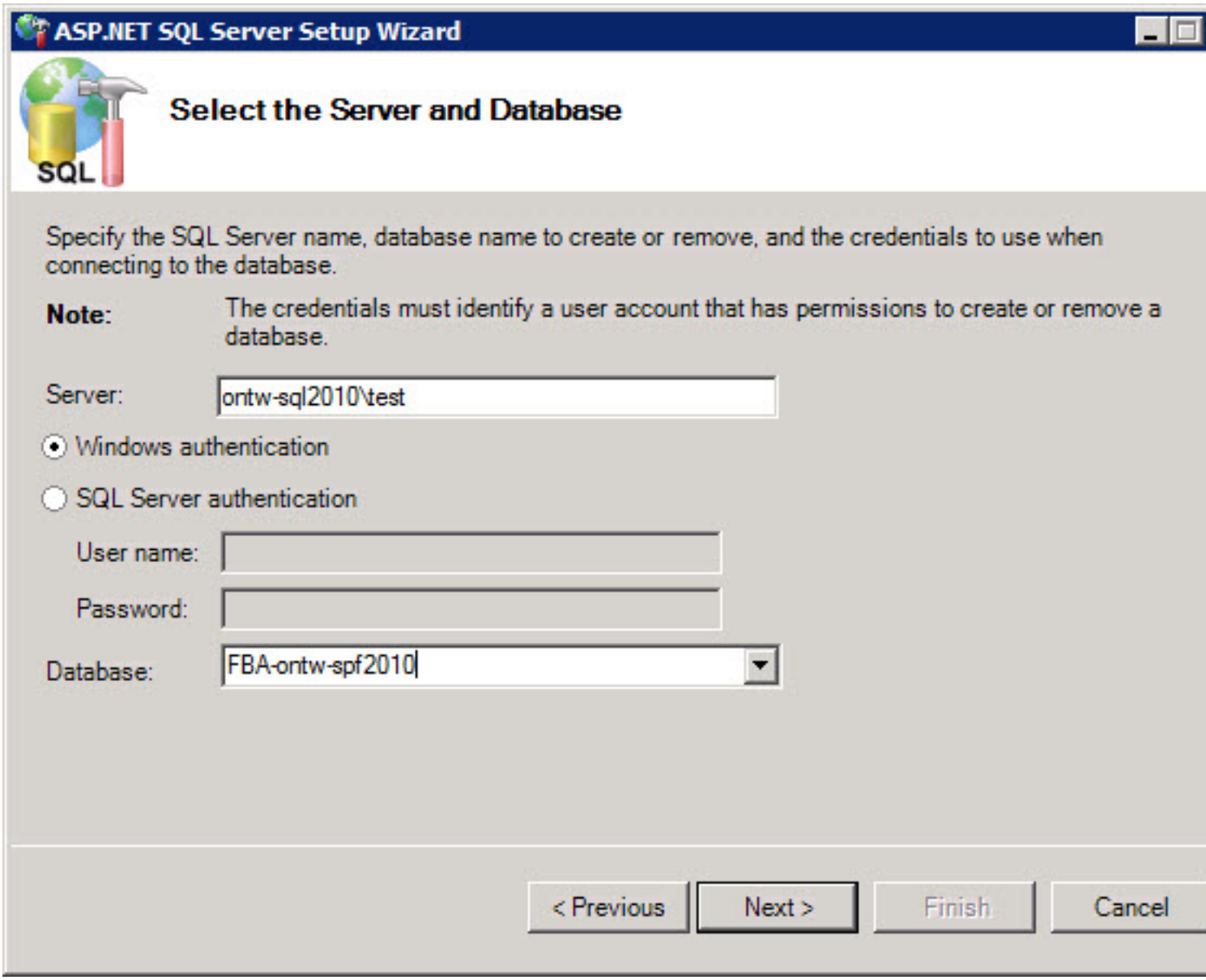
از دغدغه‌های همیشگی در راه اندازی پرتال‌های مبتنی بر شیرپوینت سیستم احراز هویت آن است. این سیستم بصورت پیش فرض بر مبنای Windows Authentication است و ناگفته پیداست این نوع احراز هویت تنها در شبکه‌های محلی کاربرد دارد آنهم در صورتی که همه کاربران و سطوح دسترسی، بدرستی در AD تعریف شده باشد و نیز
یک سری 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 نَصاب(!) 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.
متاسفانه 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 معمولا 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.

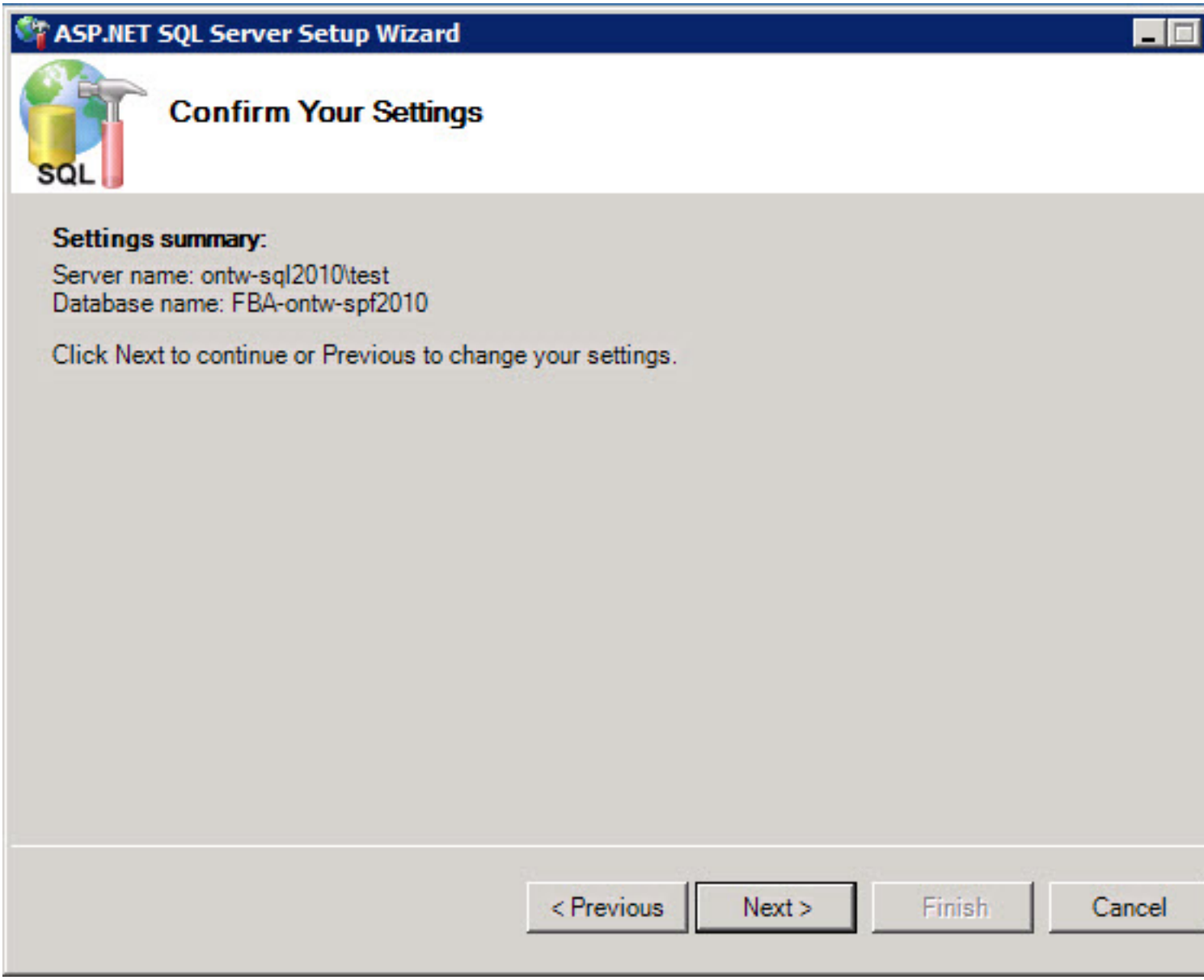
1. ساخت بانک اطلاعاتی FBA بر روی MSSQL

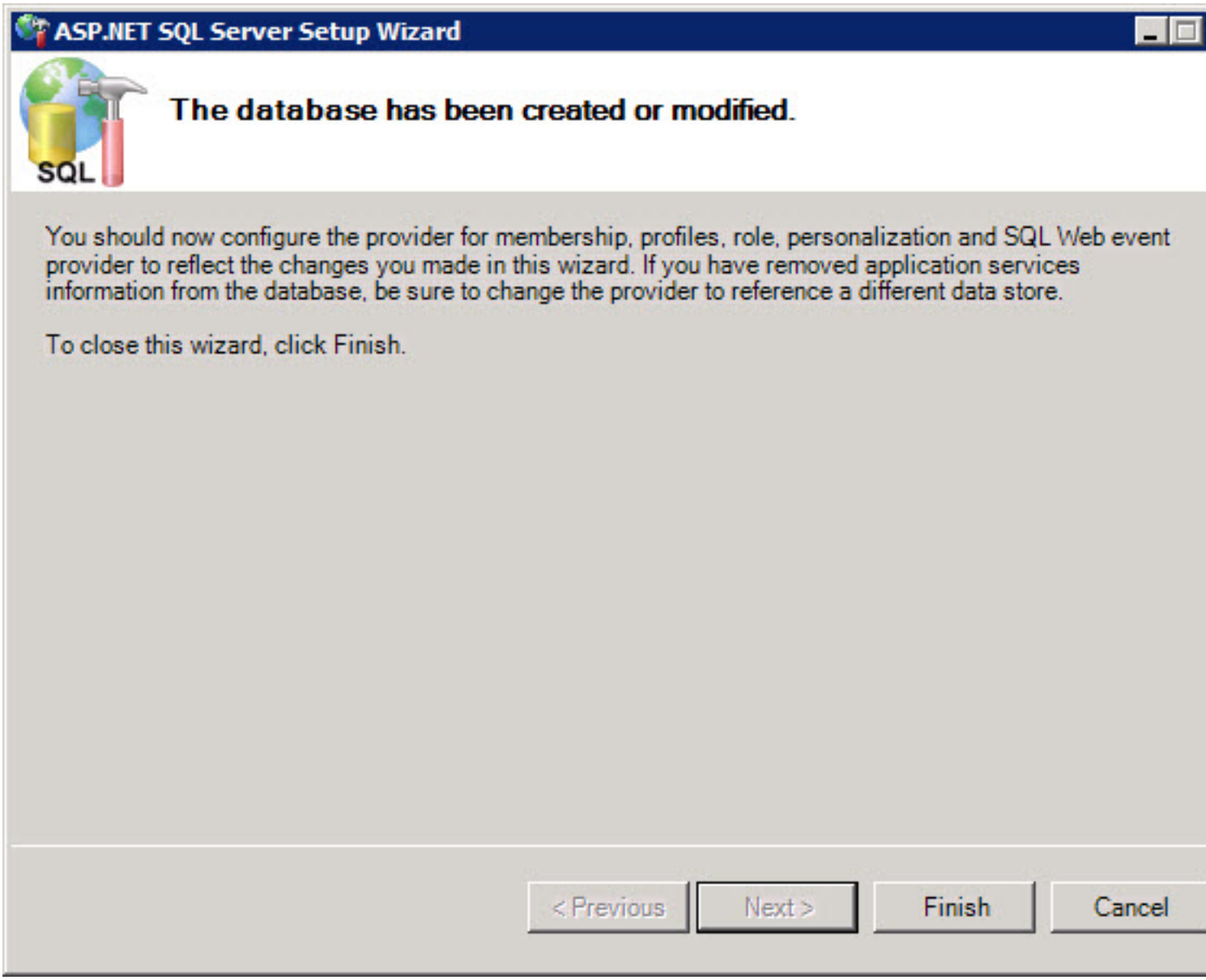
بانک اطلاعاتی FBA ساختار مشخصی از جداول و SPها دارد که تا حد امکان بهتر است در ساختار پیش فرض آن تغییری ایجاد نکنیم. برای ایجاد این بانک کافی است به محل نصب دات نت فریم 2.0 که بصورت پیش فرض در مسیر"C:\Windows\Microsoft.NET\Framework64\v2.0.50727 " قرار دارد بروید و روی فایل "aspnet_regsql.exe " کلیک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


ASP.NET SQL Server Setup Wizard
Welcome to the ASP.NET SQL Server Setup Wizard
SQL
This wizard creates or configures a SQL Server database that stores information for ASP.NET applications services (membership, profiles, role management, personalization and SQL Web event provider).
To configure the database for these features individually or 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.
Click Next to continue.
< Previous
Next >
Finish
Cancel

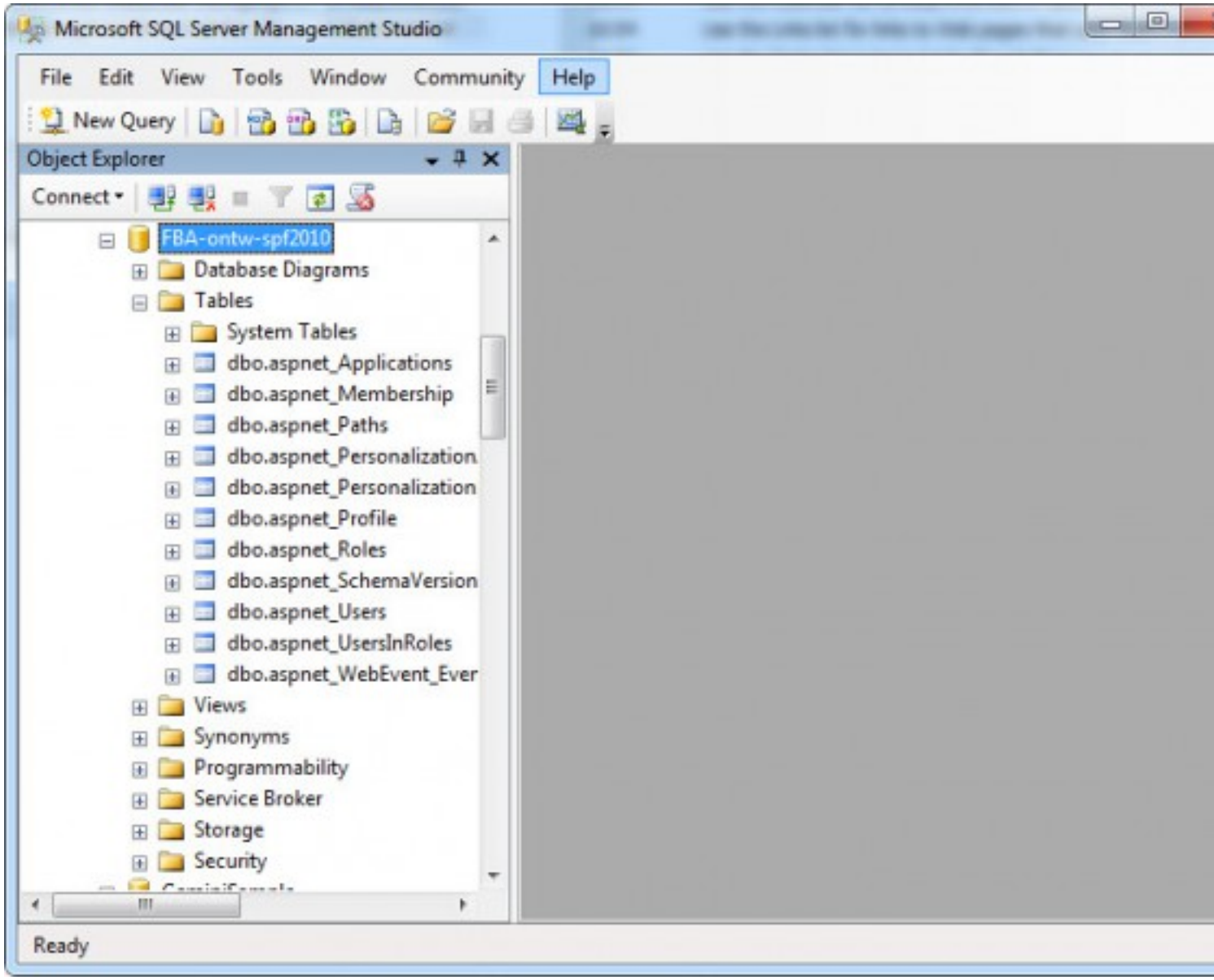

ASP.NET SQL Server Setup Wizard
Select a Setup Option
SQL
What database task do you want to perform?
Configure SQL Server for application services
This option runs a script that creates a new database or configures an existing database to store information for ASP.NET membership, profiles, role management, 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


ASP.NET SQL Server Setup Wizard
Select the Server and Database
SQL
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:
ontw-sql2010\test
Windows authentication
SQL Server authentication
User name:
Password:
Database:
FBA-ontw-spf2010
< Previous
Next >
Finish
Cancel


ASP.NET SQL Server Setup Wizard
Confirm Your Settings
SQL
Settings summary:
Server name: ontw-sql2010\test
Database name: FBA-ontw-spf2010
Click Next to continue or Previous to change your settings.
< Previous
Next >
Finish
Cancel

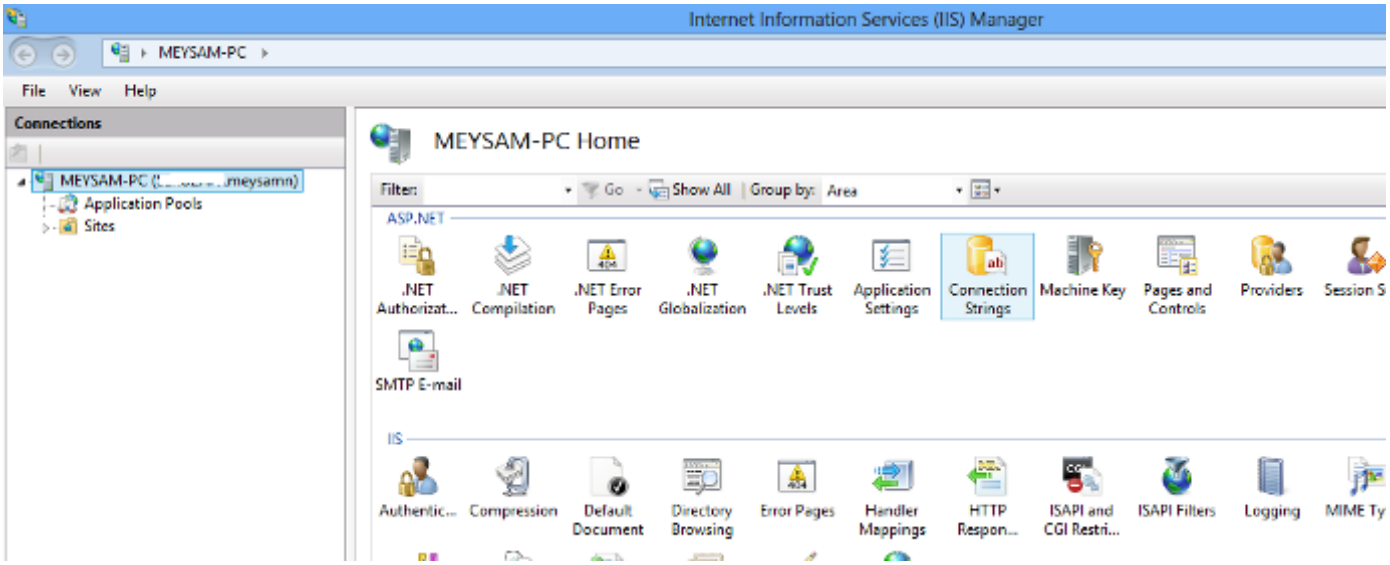


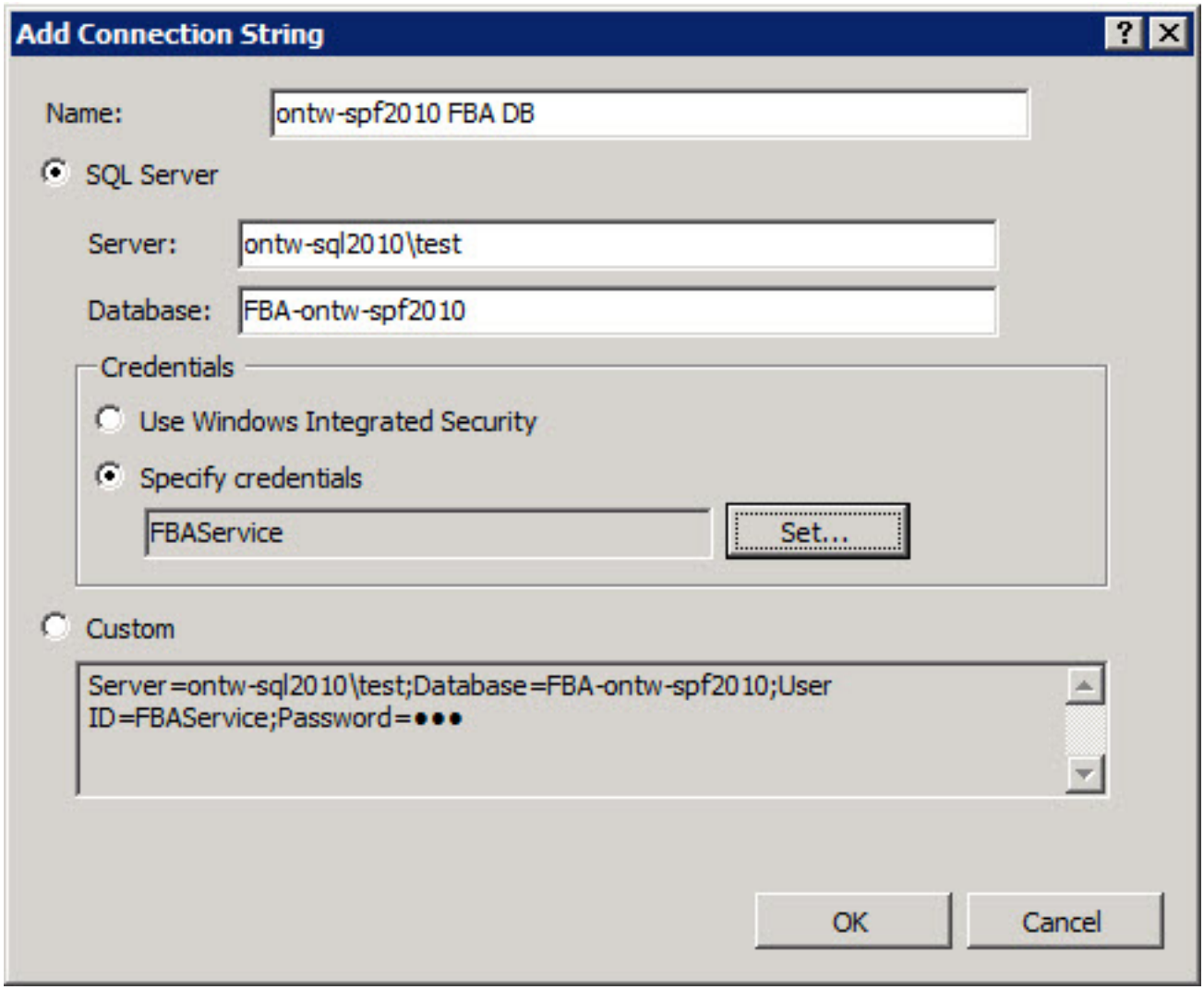
در ادامه MSSQL را باز کنید و مطئمن شوید که بانک FBA به درستی ایجاد شده باشد.

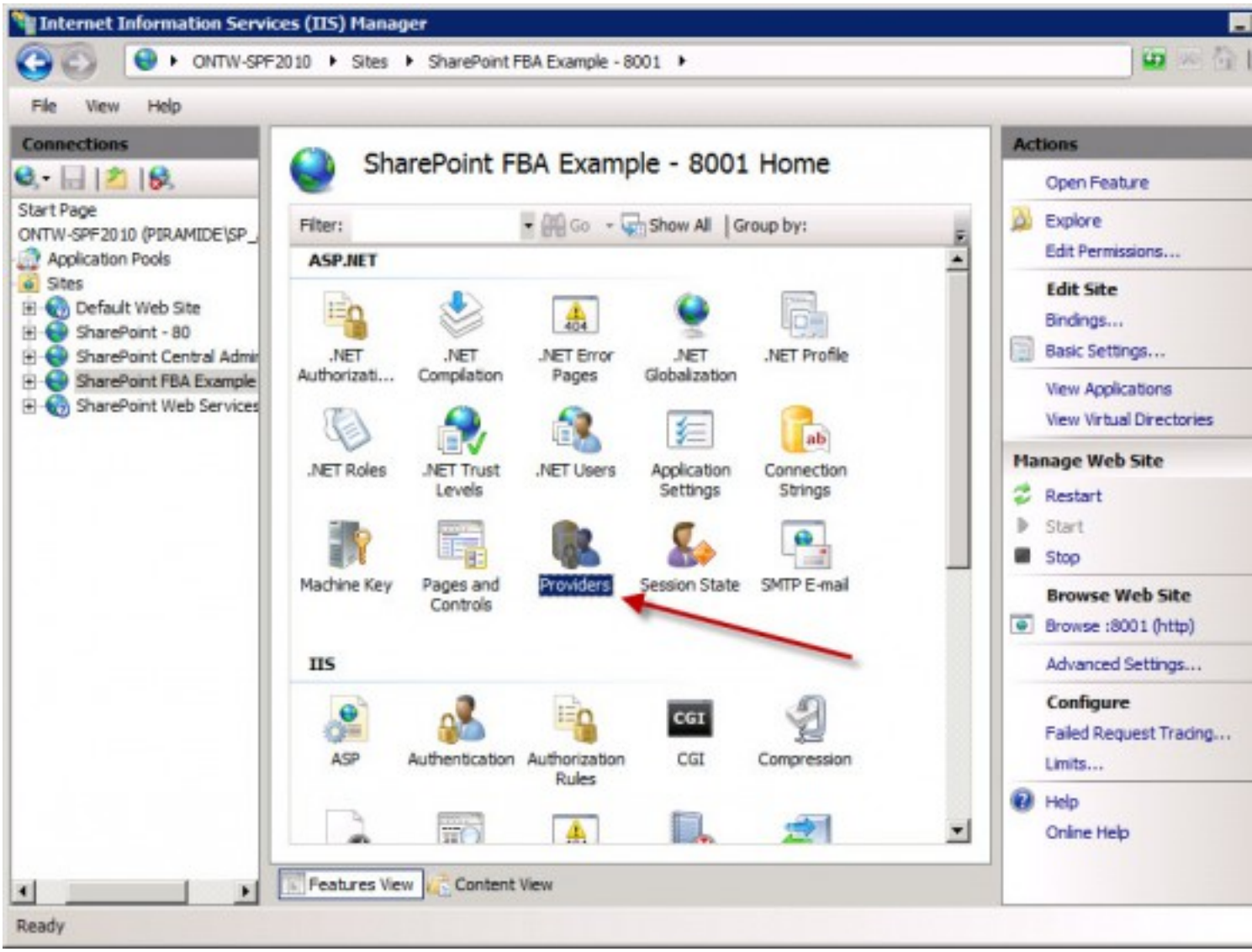


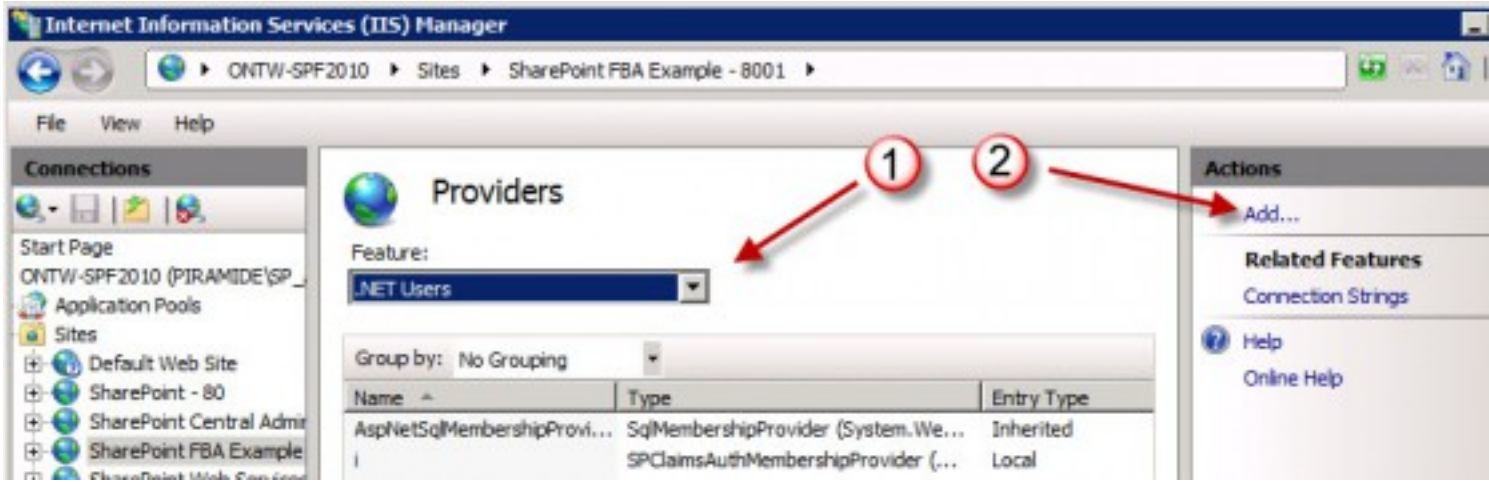
2.وارد IIS شده و در بخش روت سرور ،توجه شود که حتما این تغییرات در روت سرور اعمال شود تا همه سایت‌ها از آن ارث بری کنند و تنظیمات شما یکسان در همه Web Applicationها اعمال شود.

این مرحله Connection String و Role provider و Membership provider مورد نظرتان را اضافه کنید.

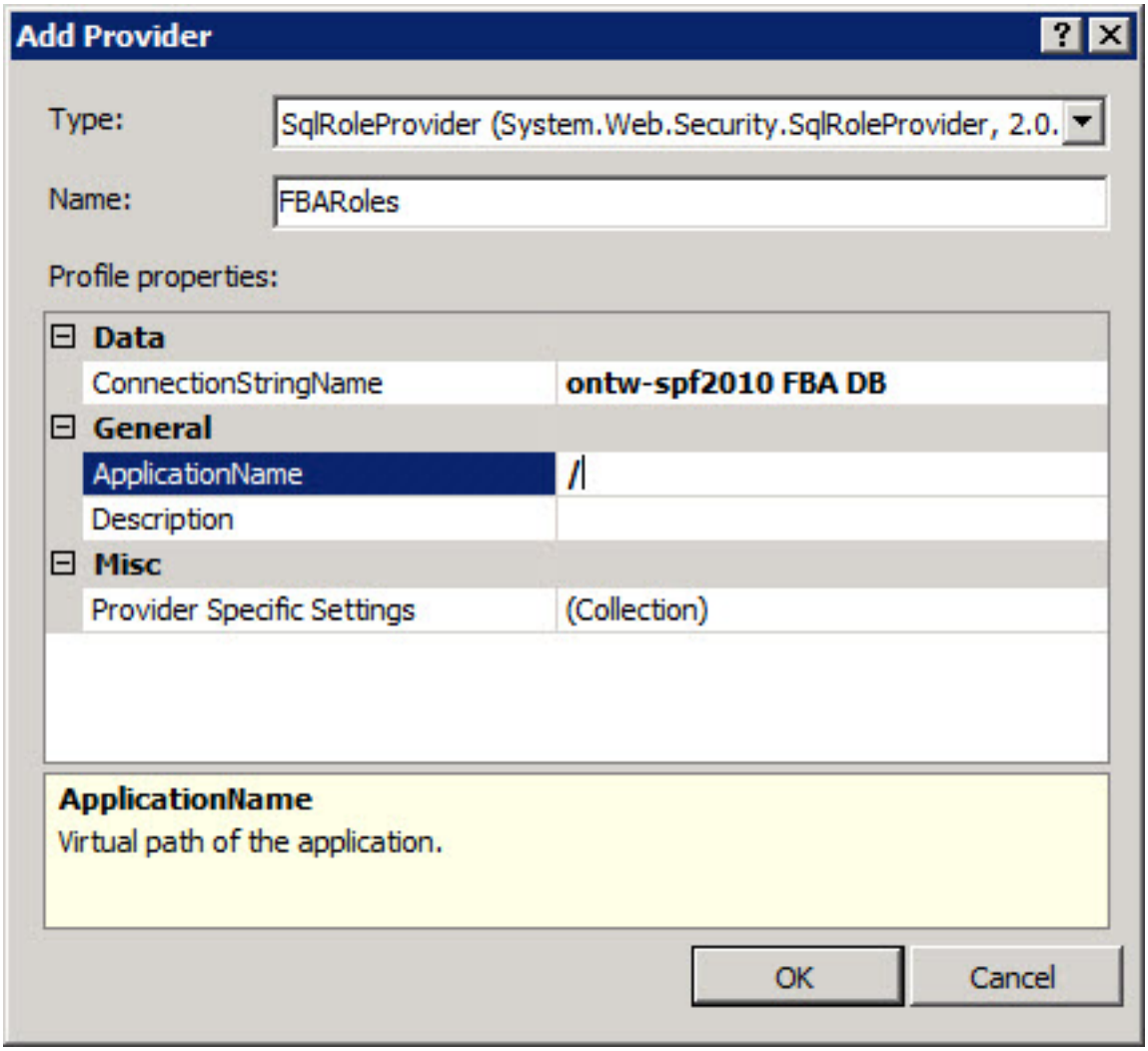

Internet Information Services (IIS) Manager
MEYSAM-PC
File View Help
Connections
MEYSAM-PC (...meysamn)
Application Pools
Sites
MEYSAM-PC Home
Filter:
Go
Show All
Group by: Area
ASP.NET
.NET Authorizat...
.NET Compilation
.NET Error Pages
.NET Globalization
.NET Trust Levels
Application Settings
Connection Strings
Machine Key
Pages and Controls
Providers
Session S
SMTP E-mail
IIS
Authentic...
Compression
Default Document
Directory Browsing
Error Pages
Handler Mappings
HTTP Respon...
ISAPI and CGI Restri...
ISAPI Filters
Logging
MIME Ty


Add Connection String
Name:
ontw-spf2010 FBA DB
SQL Server
Server:
ontw-sql2010\test
Database:
FBA-ontw-spf2010
Credentials
Use Windows Integrated Security
Specify credentials
FBAService
Set...
Custom
Server=ontw-sql2010\test;Database=FBA-ontw-spf2010;User ID=FBAService;Password=●●●
OK
Cancel

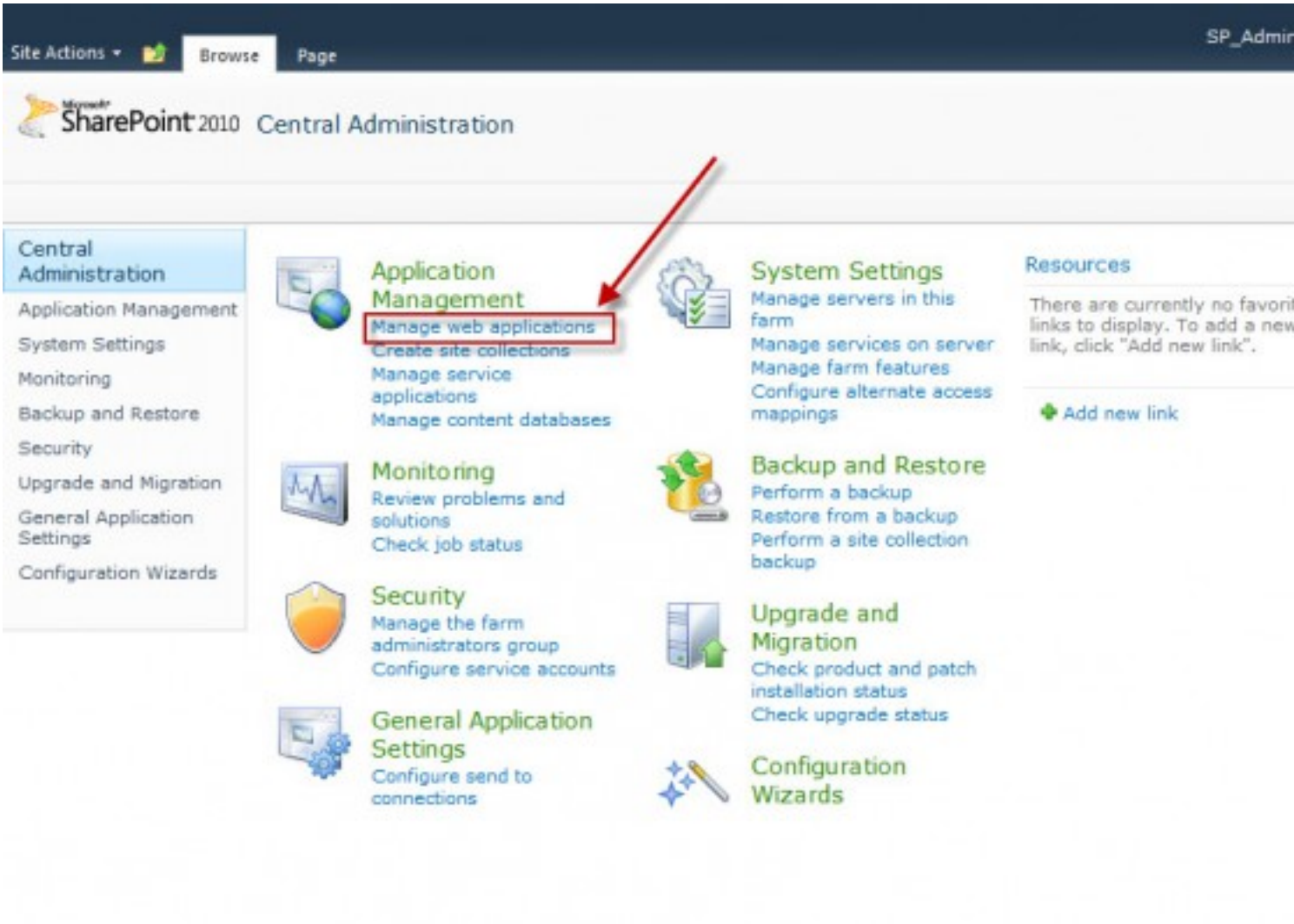




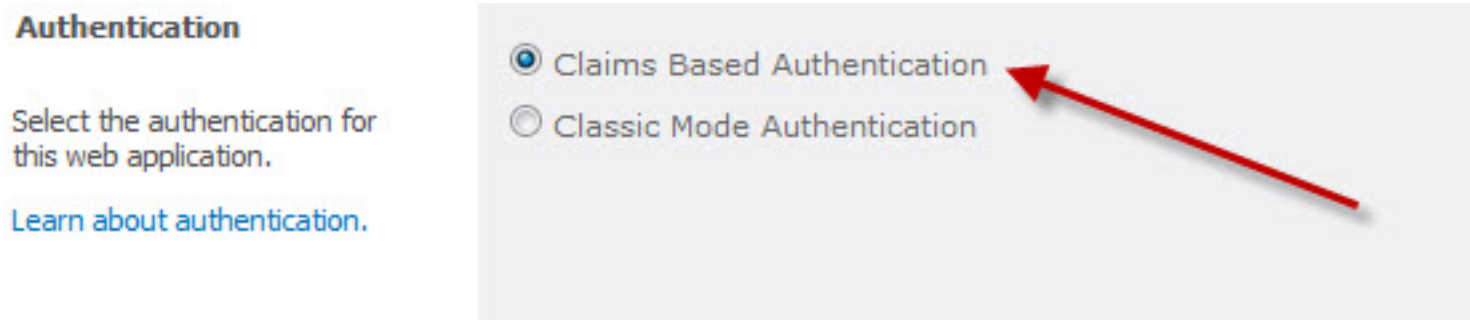
موقع اضافه کردن Providerها باید توجه داشت که Application Name برابر "/" قرار داده شود.



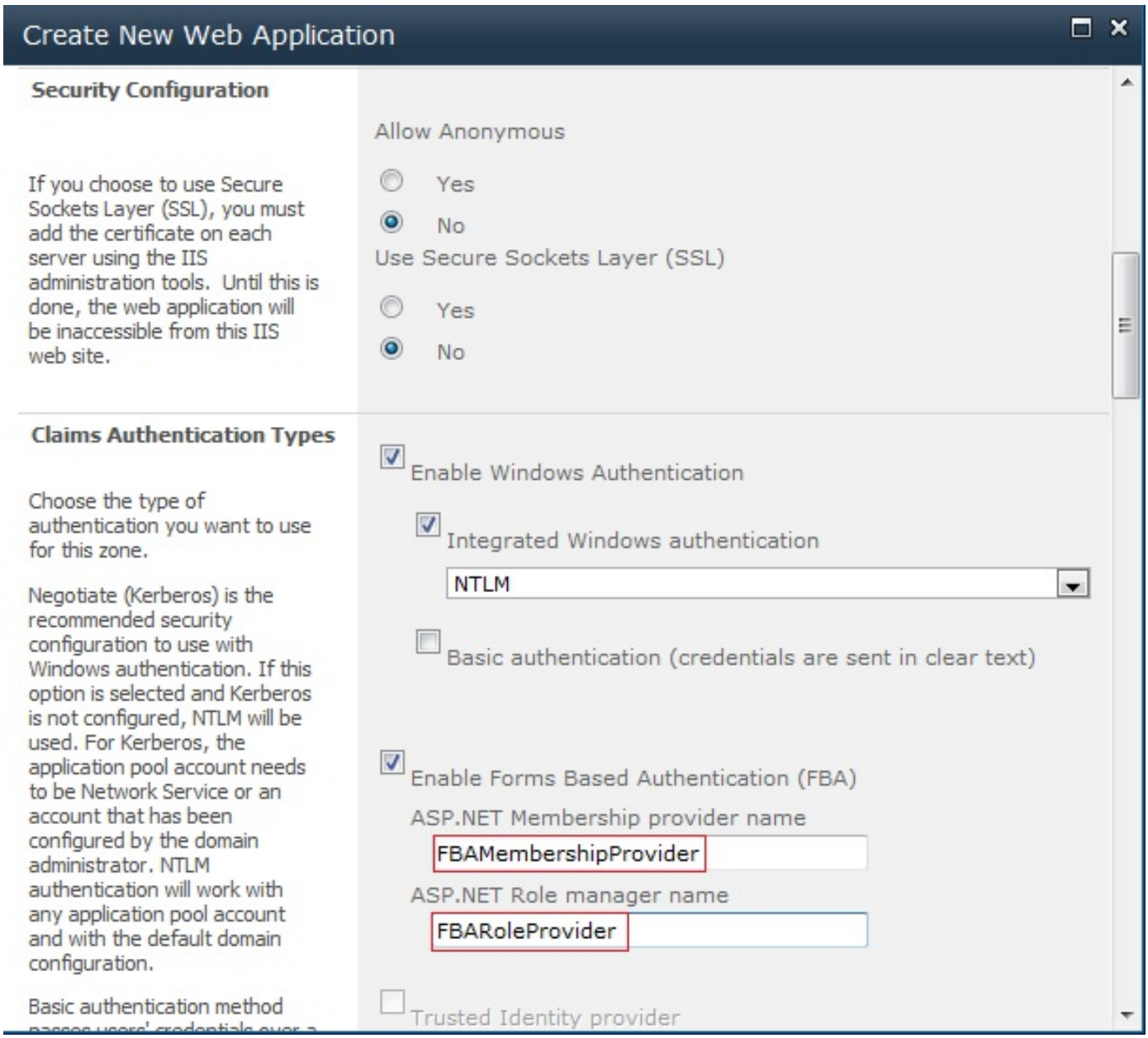
3.به بخش مدیریت شیرپوینت رفته و یک WebApplication جدید ایجاد کنید.



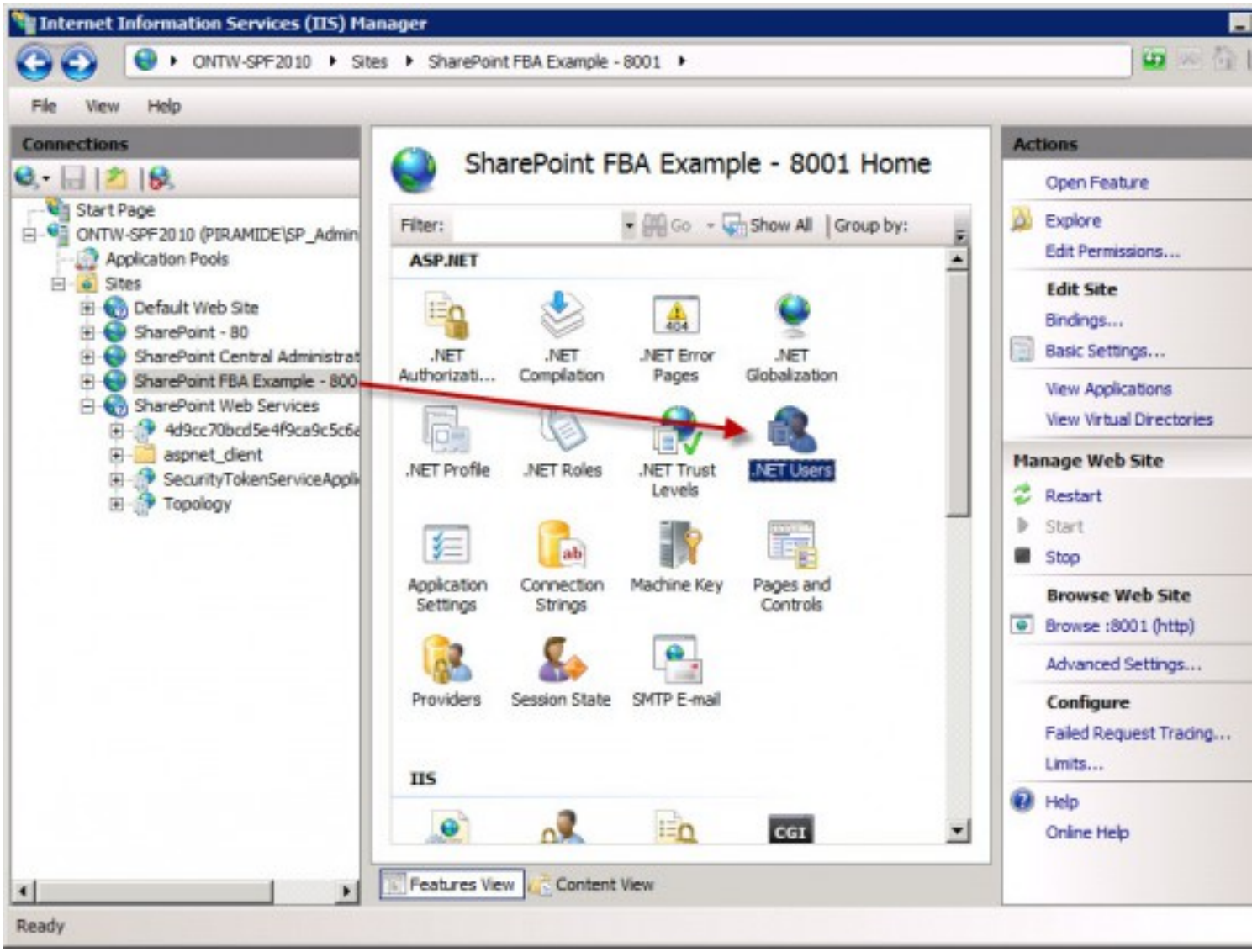
توجه داشت که در بخش Authentication بایدگزینه Claims Authentication را انتخاب کنید.



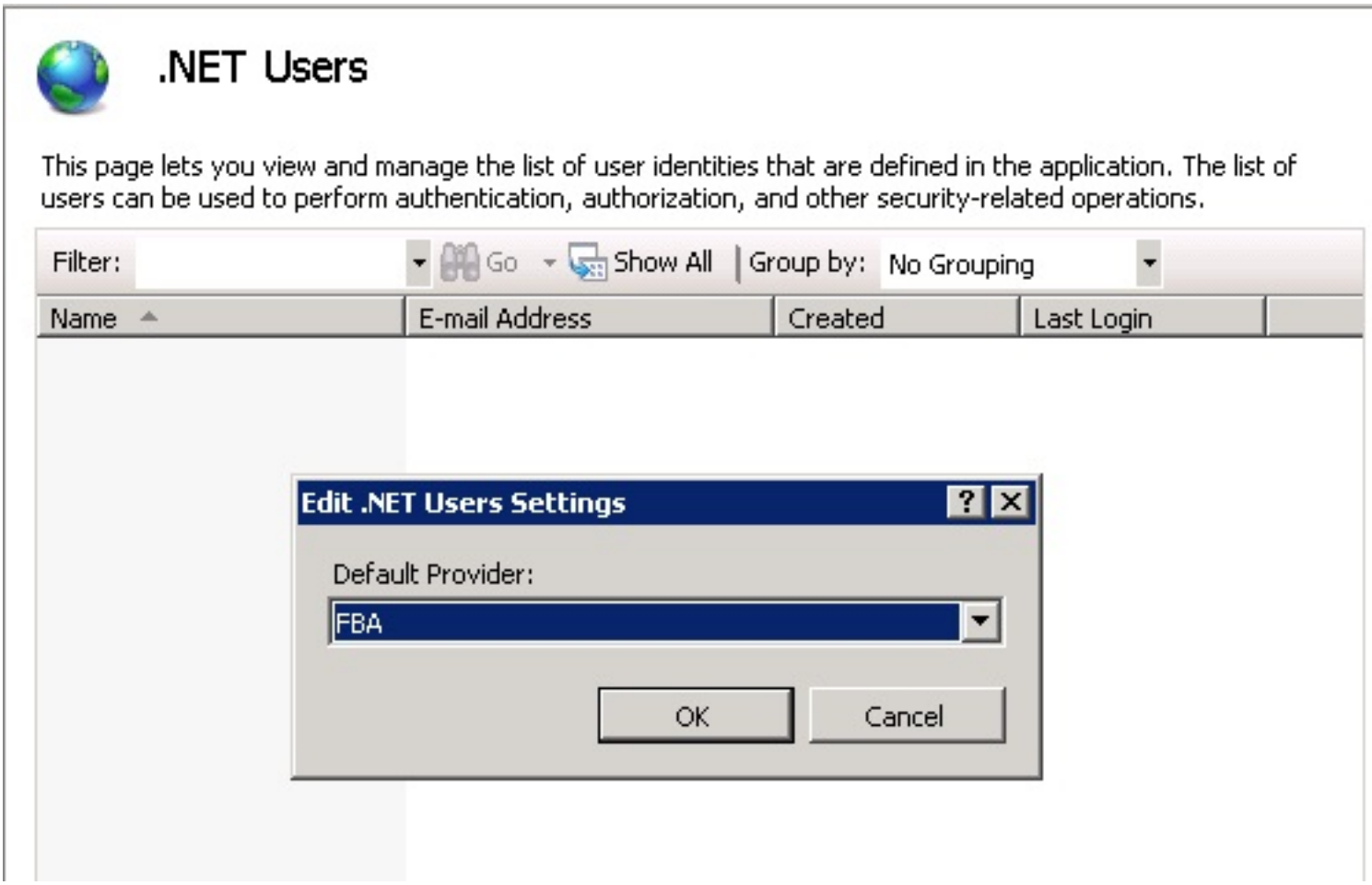
و نیز برای تنظیمات مربوط به FBA باید نام Provider هایی را که در مرحله قبل ایجاده کرده بودید را در این بخش قرار دهید.
اگر پرتال شما بازدید کننده‌های ناشناس(بازدید کنندگانی که عضو نیستند و در سیستم FBA نام کاربری ندارند) را نیز پشتیبانی میکند باید گزینه اول(Allow anonymous) را Yes کنید.
اگر تمایلی ندارید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



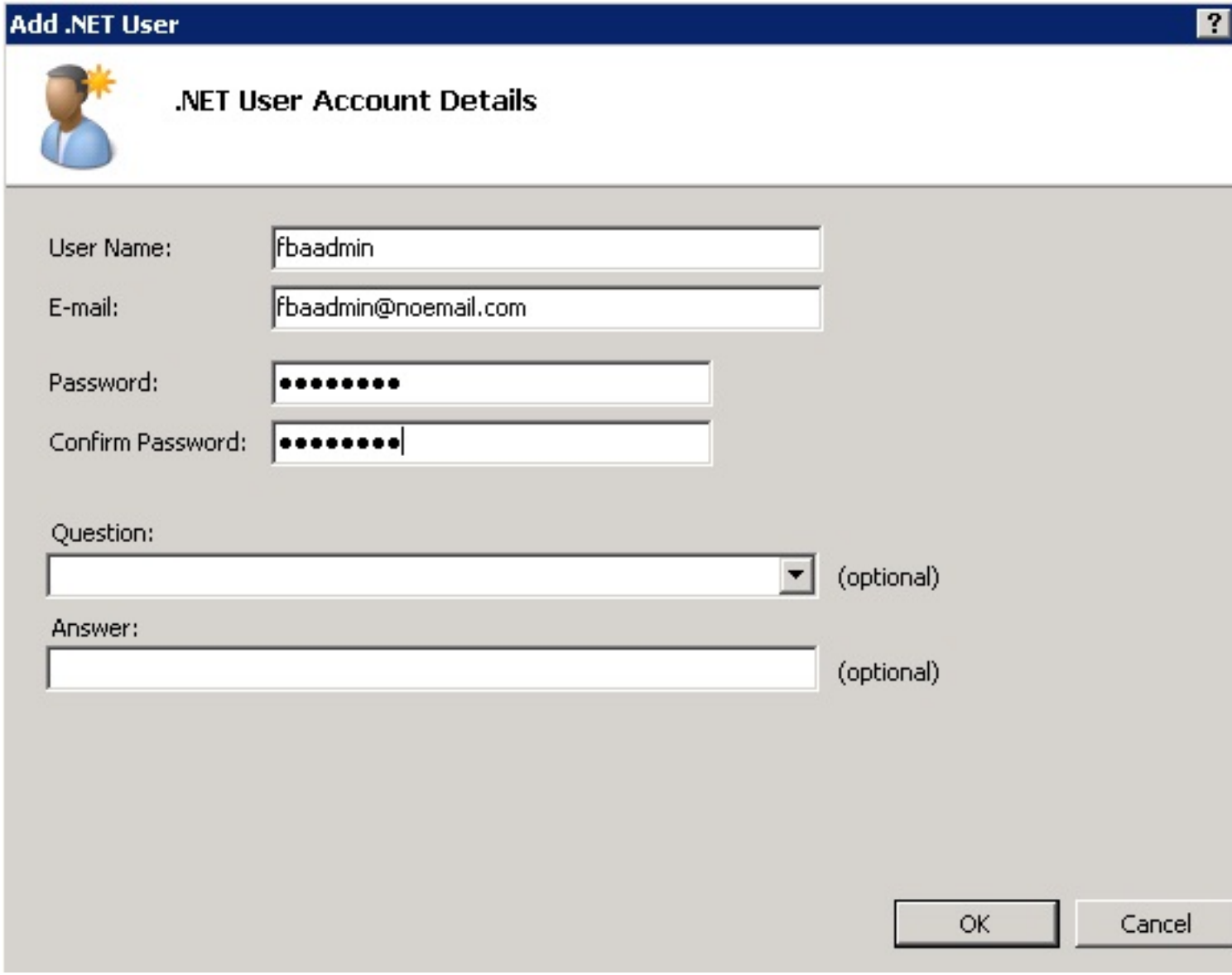
4.حال دوباره سراغ IIS میرویم و روی وب جدیدی که ایجاد کرده ایم کلیک میکنیم و سپس روی آیکون Net Users کلیک میکنیم



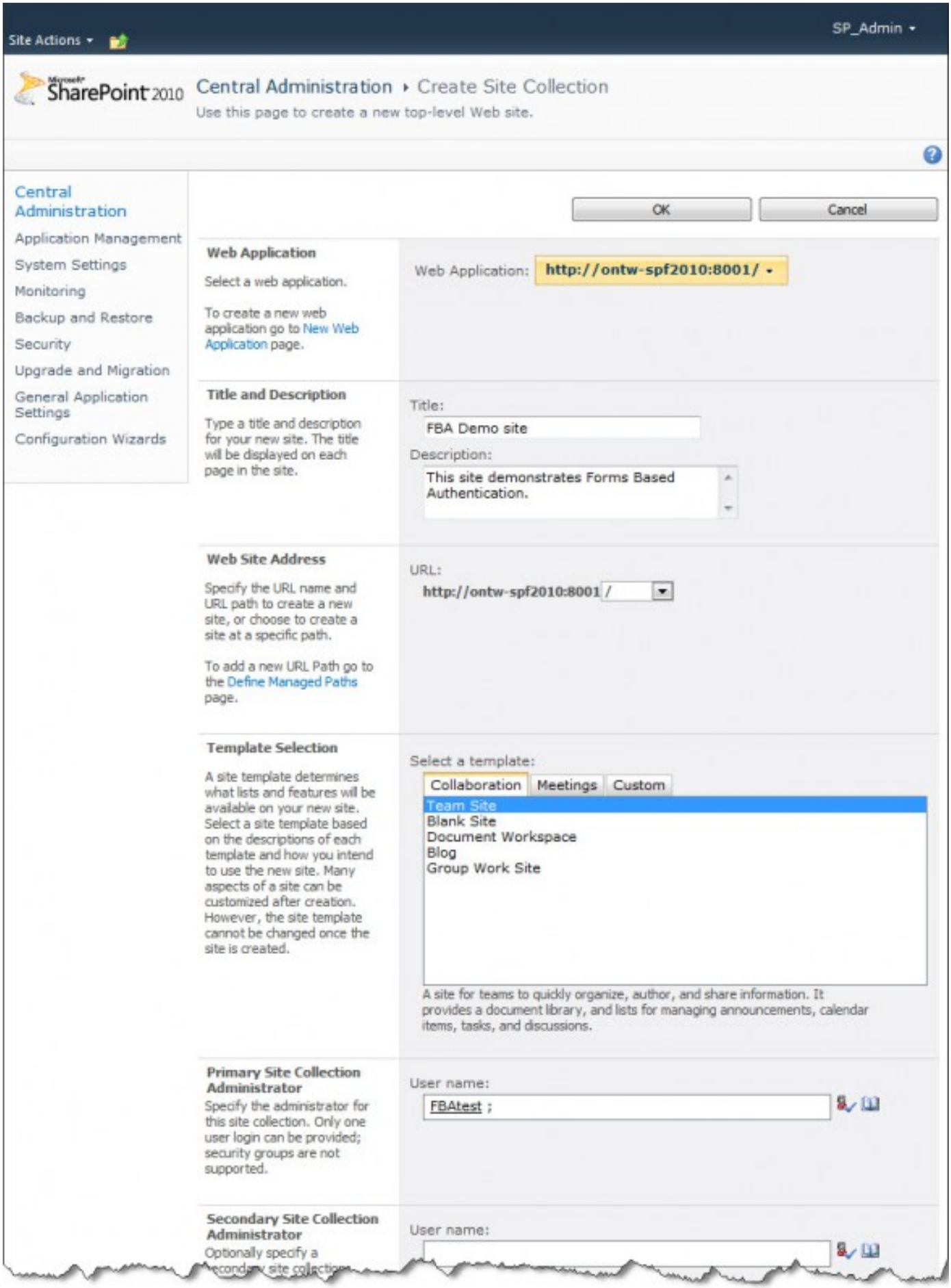
اگر با پیغامی مبنی بر تعیین Provider پیش فرض مواجه شدیم مقادیر پیش فرض Providerها را برابر با نام Provider هایی که خودمان تعریف کرده ایم قرار میدهیم.



در ادامه چند کاربر و رول هم به عنوان کاربران اولیه و مدیران پرتال ایجاد میکنیم .



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


Site Actions
SP_Admin
SharePoint 2010
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
OK
Cancel
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:
FBA Demo site
Description:
This site demonstrates Forms Based Authentication.
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:
Collaboration
Meetings
Custom
Team Site
Blank Site
Document Workspace
Blog
Group Work Site
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.
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:
FBAtest ;
Secondary Site Collection Administrator
Optionally specify a
User name:

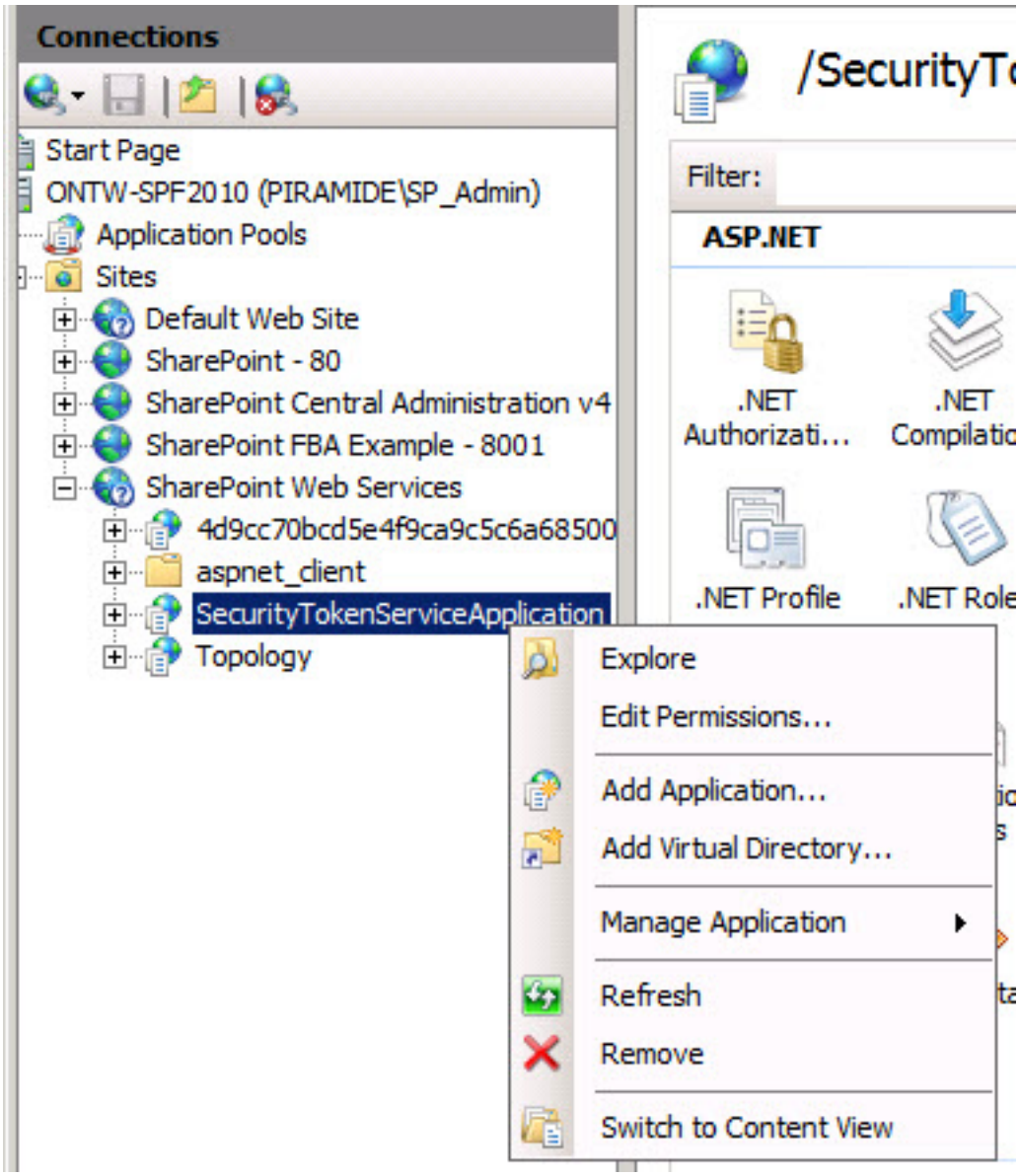
در اینجا بهتر است مدیر اول را از کاربران ویندوزی انتخاب کرد و مدیر دوم را از بخش کاربران FBA

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.

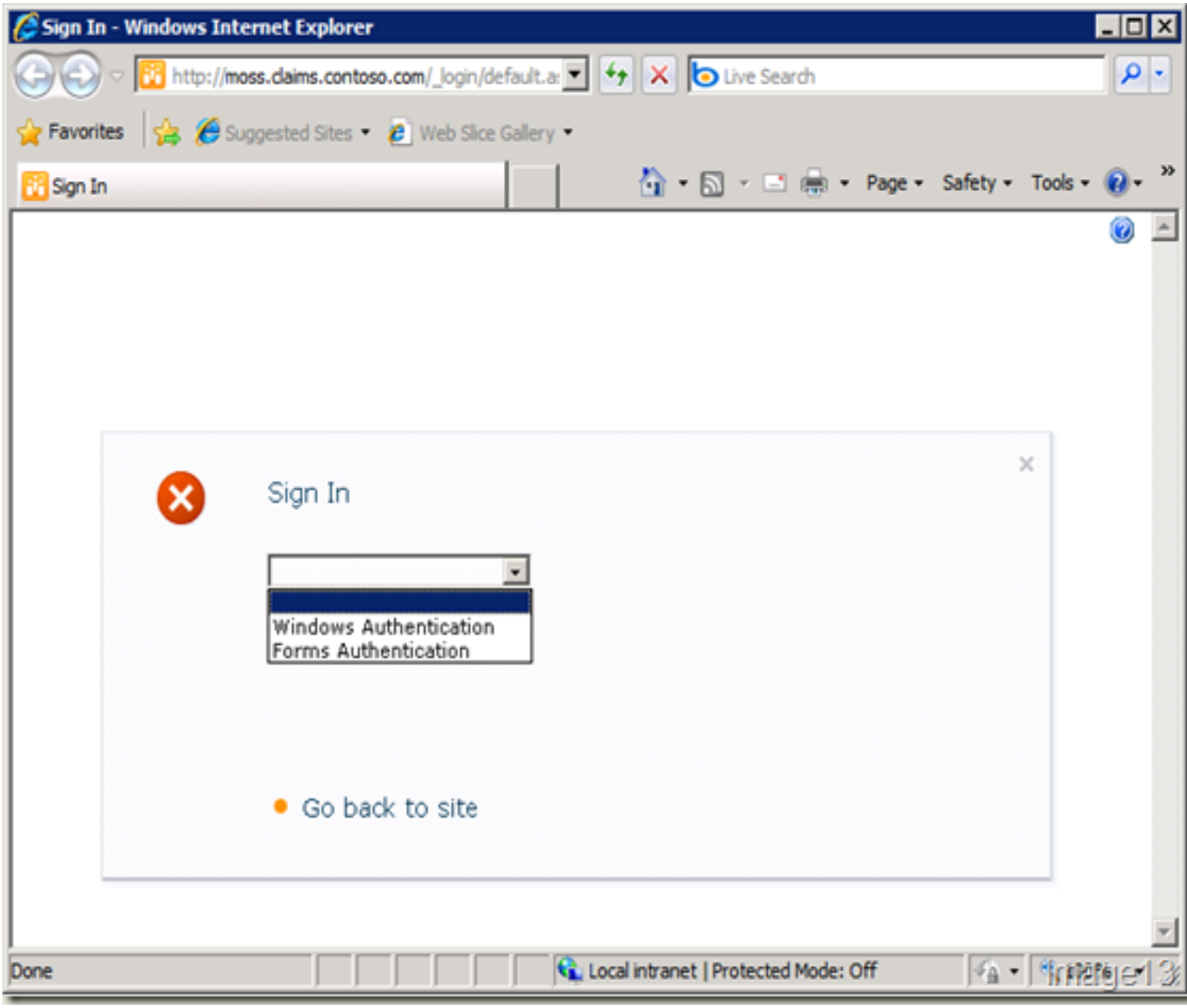


در ادامه تنها کافی است Connection string را جهت اتصال به بانکی که در ابتدا ساختیم ایجاد کرده و Providerها را نیز مطابق قبل اضافه کنیم. فقط توجه شود Connection string و Providerها همنام قبلی‌ها نباشند ولی Application Name همچنان برابر با "/" مقدار دهی شود.

هیچ تغییر دیگری در این Application ایجاد نشود. **مثلا Authentication به هیچ وجه تغییر نکند و در حالت ویندوزی باقی بماند.**

کار تقریبا به پایان رسیده است،میتوانید در پرتال لاگین کنید!

آنچنانکه که در تصویر می‌بینید هر دو حالت ویندوزی و FBA برای احراز هویت فعال می‌باشد.



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 خودداری 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