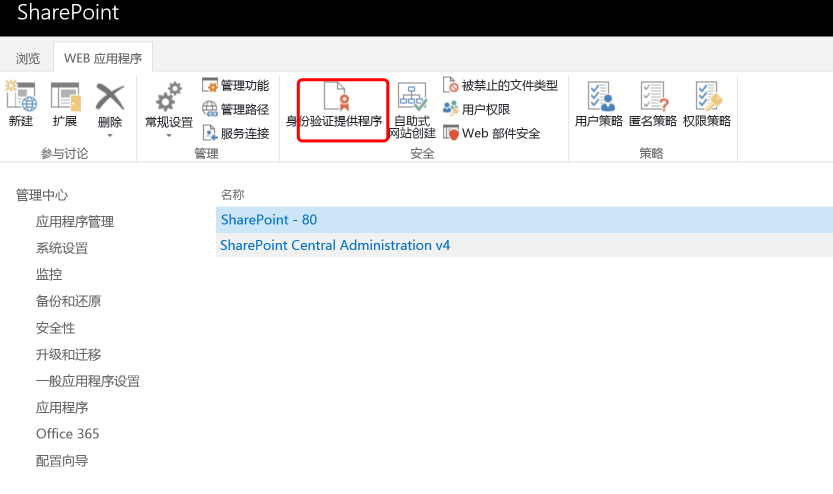
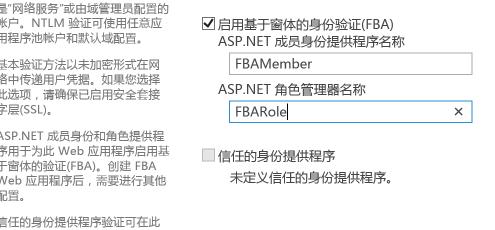
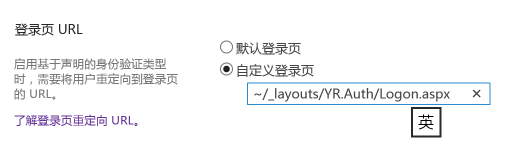
**FBA with LDAP provider**

**Click on authentication provider**

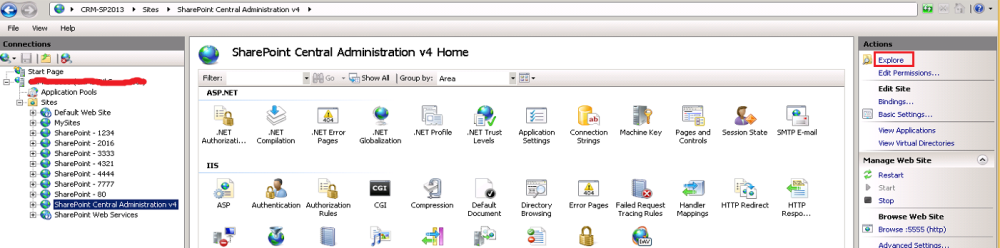


**Enable the FBA check box and give provider and role manager name**





**To configure the Central Administration Web.Config file**

1. Press windows key + R and type **inetmgr.**Click OK.
2. In the console tree, open the server name, and then **Sites**.
3. Right-click the **SharePoint Central Administration v4** site, and then click **Explore**.
4. In the folder window, double-click the Web.Config file.
5. In the  section, find the  section and add the following example entry:

|  |
| --- |
| <membership>  <providers>  <add name="FBAMember"  type="YR.Auth.FBAMember, YR.Auth, Version=1.0.0.0, Culture=neutral, PublicKeyToken=9fd324319561fbd8"  server="sp.datawhy.com"  port="389"  useSSL="false"  userDNAttribute="distinguishedName"  userNameAttribute="sAMAccountName"  userContainer="CN=Users,DC=datawhy,DC=com"  userObjectClass="person"  userFilter="(|(ObjectCategory=group)(ObjectClass=person))"  scope="Subtree"  otherRequiredUserAttributes="sn,givenname,cn" />  </providers>  </membership>  <roleManager>  <providers>  <add name="FBARole"  type="YR.Auth.FBARole, YR.Auth, Version=1.0.0.0, Culture=neutral, PublicKeyToken=9fd324319561fbd8"  server="sp.datawhy.com"  port="389"  useSSL="false"  groupContainer="CN=Users,DC=datawhy,DC=com"  groupNameAttribute="cn"  groupMemberAttribute="member"  userNameAttribute="sAMAccountName"  dnAttribute="distinguishedName"  groupFilter="(ObjectClass=group)"  scope="Subtree"/>  </providers>  </roleManager> |

In the preceding entry, substitute the following:

* The name of your membership provider in <add name="membership"**.**
* The fully qualified domain name (FQDN) of your domain controller (your LDAP server) in server="yourserver.com"**.**
* The distinguished name of your user container in userContainer="OU=UserAccounts,DC=internal,DC=yourcompany,DC=distinguishedName (of your userContainer)".
* The name of your role manager in <add name="roleManager"**.**
* The distinguished name of your group container in groupContainer="DC=internal,DC=yourcompany,DC=distinguishedName (of your groupContainer)"**.**

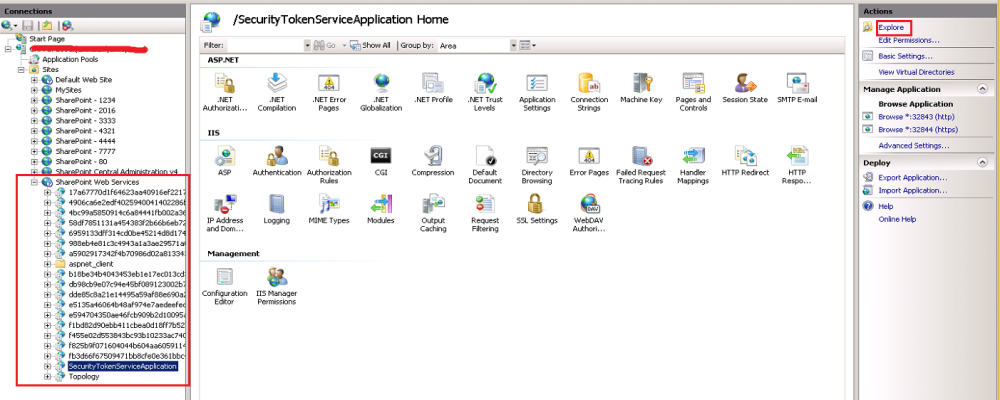
After you add this entry, save and close the Web.Config file.

**Configure the Security Token Service Web.Config file**

The following procedure configures the Security Token Service to recognize and use the new forms-based membership provider and role manager.

**To configure the Security Token Service Web.Config file**

1. In the console tree of Internet Information Services (IIS) Manager, open the **SharePoint Web Services** site.
2. In the console tree, right-click **SecurityTokenServiceApplication**, and then click **Explore**.



1. In the folder window, double-click the Web.Config file.
2. In the <Configuration> section, create a new <system.web> section and add the following example entry:

|  |
| --- |
| <system.web>  <membership defaultProvider="FBAMember">  <providers>  <add name="FBAMember"  type="YR.Auth.FBAMember, YR.Auth, Version=1.0.0.0, Culture=neutral, PublicKeyToken=9fd324319561fbd8"  server="sp.datawhy.com"  port="389"  useSSL="false"  userDNAttribute="distinguishedName"  userNameAttribute="sAMAccountName"  userContainer="CN=Users,DC=datawhy,DC=com"  userObjectClass="person"  userFilter="(|(ObjectCategory=group)(ObjectClass=person))"  scope="Subtree"  otherRequiredUserAttributes="sn,givenname,cn" />  </providers>  </membership>  <roleManager defaultProvider="FBARole" enabled="true" cacheRolesInCookie="true" cookieName=".PeopleDCRole">  <providers>  <add name="FBARole"  type="YR.Auth.FBARole, YR.Auth, Version=1.0.0.0, Culture=neutral, PublicKeyToken=9fd324319561fbd8"  server="sp.datawhy.com"  port="389"  useSSL="false"  groupContainer="CN=Users,DC=datawhy,DC=com"  groupNameAttribute="cn"  groupMemberAttribute="member"  userNameAttribute="sAMAccountName"  dnAttribute="distinguishedName"  groupFilter="(ObjectClass=group)"  scope="Subtree"/>  </providers>  </roleManager>  </system.web> |

In the preceding entry, substitute the following:

* The name of your membership provider in <add name="membership".
* The FQDN of your domain controller (your LDAP server) in server="yourserver.com"**.**
* The distinguished name of your user container in userContainer="OU=UserAccounts,DC=internal,DC=yourcompany,DC=com"**.**
* The name of your role manager in <add name="roleManager"**.**
* The distinguished name of your group container in groupContainer="DC=internal,DC=yourcompany,DC=com"**.**

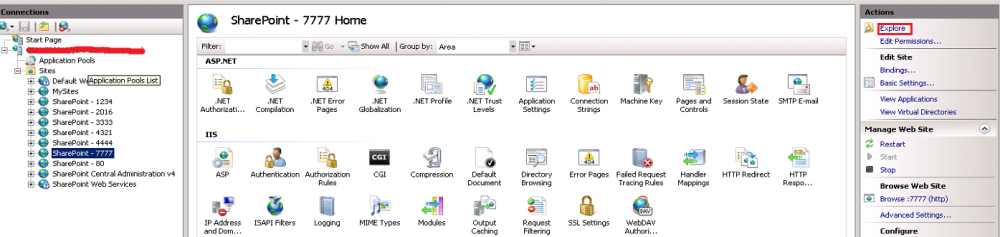
After you add this entry, save and close the Web.Config file.

**Configure the new web application Web.Config file**

The following procedure configures the new web application to recognize and use the new forms-based membership provider and role manager.

**To configure the new web application Web.Config file**

1. In the console tree of Internet Information Services (IIS) Manager, right-click the site that corresponds to the name of the web applications that you just created, and then click **Explore**.



1. In the folder window, double-click the Web.Config file.
2. In the <Configuration> section, find the <system.web> section.
3. Find the <membership defaultProvider="i"> section and add the following example entry to the <Providers> section:

|  |
| --- |
| <add name="FBAMember"  type="YR.Auth.FBAMember, YR.Auth, Version=1.0.0.0, Culture=neutral, PublicKeyToken=9fd324319561fbd8"  server="sp.datawhy.com"  port="389"  useSSL="false"  userDNAttribute="distinguishedName"  userNameAttribute="sAMAccountName"  userContainer="CN=Users,DC=datawhy,DC=com"  userObjectClass="person"  userFilter="(|(ObjectCategory=group)(ObjectClass=person))"  scope="Subtree"  otherRequiredUserAttributes="sn,givenname,cn" /> |

In the preceding entry, substitute the following:

* The name of your membership provider in <add name="membership"**.**
* The FQDN of your domain controller (your LDAP server) in server="yourserver.com".
* The distinguished name of your user container in userContainer="OU=UserAccounts,DC=internal,DC=yourcompany,DC=com"

Find the **<roleManager defaultProvider="c" enabled="true"cacheRolesInCookie="false">**section and add the following example entry to the <Providers> section:

|  |
| --- |
| <add name="FBARole"  type="YR.Auth.FBARole, YR.Auth, Version=1.0.0.0, Culture=neutral, PublicKeyToken=9fd324319561fbd8"  server="sp.datawhy.com"  port="389"  useSSL="false"  groupContainer="CN=Users,DC=datawhy,DC=com"  groupNameAttribute="cn"  groupMemberAttribute="member"  userNameAttribute="sAMAccountName"  dnAttribute="distinguishedName"  groupFilter="(ObjectClass=group)"  scope="Subtree"/> |

In the preceding entry, substitute the following:

* The name of your role manager in <add name="roleManager"**.**
* The FQDN of your domain controller (your LDAP server) in server="yourserver.com"**.**
* The distinguished name of your group container in groupContainer="DC=internal,DC=yourcompany,DC=com"**.**

After you add the preceding entry, save and close the Web.Config file.