Create new web application with Kerberos Authentication

1. Open your central admin site
2. You can either convert your existing web application to Kerberos or you can enable Kerberos when you create your application for the first time.
3. On web application creation page. Select Kerberos as authentication mode if you are creating a new web application.



1. If you are dealing with existing web application, select Authentication Providers, click on Default and change the authentication mode to Kerberos as shown above
2. Make a note of your web application URL, we will be using it when we are configuring the Service Principle Name.

AD Configurations

1. Go to Start -> Administrative Tools.
2. Open Active Directory Users and Computers.
3. Expand your Fully Qualified Domain Name on left panel. Click on Computers folder. If in case you do not find your Server listed, then right click on your Fully Qualified Domain Name and click on Find and search Computer Name.
4. Right click on the Server where you need to trust your Server for delegating the services.
5. Click on Properties.
6. On the Delegation tab, select "Trust this computer for delegation to any service ( Kerberos only) option.
7. In case if your server is installed with Active Directory, most likely you will find the name in domain controllers, verify the above setting.

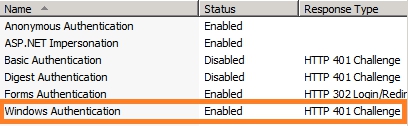
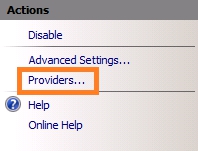
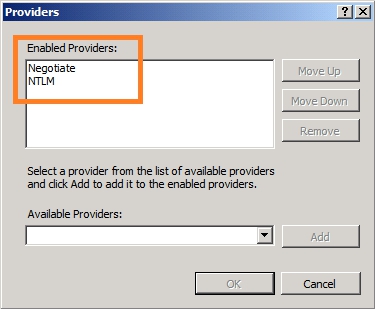
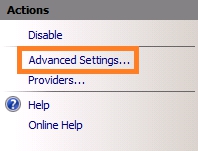
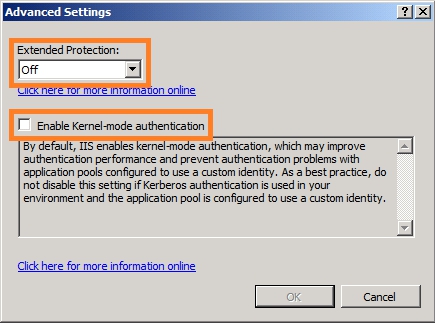
Creating SP Name

1. Open command prompt and run the below command
   1. setspn -L “IIS application pool account” (for example SPAdmin) – this step is to verify if there are any SPN’s already registered for this account
   2. setspn -S HTTP/spn host name <space>App pool service account – now register the service

|  |
| --- |
| C:\Users\SPAdmin>setspn -L SPAdmin  Registered ServicePrincipalNames for CN=SPAdmin,CN=Users,DC=MySharePoint,DC=com:  C:\Users\SPAdmin>setspn -S HTTP/mysharepoint:80 SPAdmin  Checking domain DC=MySharePoint,DC=com  Registering ServicePrincipalNames for CN=SPAdmin,CN=Users,DC=MySharePoint,DC=com  HTTP/mysharepoint:80  Updated object  C:\Users\SPAdmin>setspn -S HTTP/mysharepoint SPAdmin  Checking domain DC=MySharePoint,DC=com  Registering ServicePrincipalNames for CN=SPAdmin,CN=Users,DC=MySharePoint,DC=com  HTTP/mysharepoint  Updated object  C:\Users\SPAdmin>setspn -L SPAdmin  Registered ServicePrincipalNames for CN=SPAdmin,CN=Users,DC=MySharePoint,DC=com:  HTTP/mysharepoint  HTTP/mysharepoint:80 |

IIS Configurations

To verify the IIS Web Site Authentication settings, follow the below steps in IIS.

1. Click Start -> Administrative Tools -> Internet Information Services (IIS) Manager.
2. Click on Server Name- on left panel.
3. Expand Sites folder and locate the web application.
4. Select the web application - and in the middle pane, double click on Authentication under IIS section.  
     
   
5. In the Authentication dialog, select Windows Authentication.  
     
   
6. Click on Providers in the right actions pane.  
     
   
7. Verify that Negotiate and NTLM are listed. Note that Negotiate option should be on the top.  
     
   
8. Click Cancel and then again in the right actions pane, click on Advanced Settings.   
     
   
9. Verify in the Advanced Settings dialog that Extended Protection is Off and that "Enable Kernel-mode" authentication is unchecked.  
     
   
10. Click Cancel.

Validation : Access the application in browser and go to command prompt and type “klist”.